Private Nutzung von Smartglasses im öffentlichen Raum

Dr. Thomas Schwenke

Creative-Commons-Lizenz: CC BY-NC-ND 4.0

Zitatrecht und Zitiervorschläge:

Die verwendete Lizenz schränkt das geltende Zitatrecht nicht ein. D.h. einzelne Sätze oder Passagen dürfen übernommen werden, solange die Zitierregeln beachtet werden (d.h. die Zitate als Belege für eigene Ausführungen und Gedanken dienen). Bei der Zitierung ist der Verweis auf die Printversion ausreichend:

Als Fußnote:
Schwenke, Private Nutzung von Smartglasses im öffentlichen Raum, S. 1.

Im Literaturverzeichnis:
Schwenke, Thomas, Private Nutzung von Smartglasses im öffentlichen Raum, Edewecht 2016.

Bei Onlinezitaten wird die Verlinkung oder Angabe des Links zur Webseite des Werks unverbindlich empfohlen, z.B.:

Schwenke, Private Nutzung von Smartglasses im öffentlichen Raum, S. 1 <**https://drschwenke.de/smartglasses**>.

Hinweise zum Versionsstand:

Diese elektronische Version der Monographie entspricht der veröffentlichten Printversion, die weiterhin erworben werden kann:
http://olwir.de/?content=reihen%2Fuebersicht&sort=zi-wi-re&isbn=978-3-95599-029-9.

Link zur Website des Werks:

https://drschwenke.de/smartglasses.

Dr. Thomas Schwenke

Private Nutzung von Smartglasses im öffentlichen Raum

Smartglasses erweitern und ergänzen die sinnliche Wahrnehmungsfähigkeit der Menschen und stellen so effiziente Mensch-Maschine-Schnittstellen dar, die Menschen zur Selbstbehauptung in einer datafizierten Welt befähigen. Zu diesem Zweck müssten Smartglasses jedoch die physische Welt möglichst detailreich erfassen, womit Menschen im öffentlichen Raum einer permanenten Beobachtung und einem Verlust von Rückzugmöglichkeiten ausgesetzt sein würden. Dr. Thomas Schwenke untersucht, ob Smartglasses sich angesichts dieser Gefährdung der Privatsphäre in den Alltag von Menschen integrieren und so überhaupt ihre technischen Vorteile ausspielen können.

Die Untersuchung ist durch einen Dreiklang der technischen und gesellschaftlichen Betrachtung sowie deren rechtlicher Würdigung gekennzeichnet. Sie beginnt mit der Darstellung technischer Architektur sowie Funktionen und Einsatzbereichen von Smartglasses. Dabei werden insbesondere die möglichen Einsatzfelder herausgestellt, auf deren Grundlage die schützenswerten Interessen ihrer Nutzer herausgearbeitet werden. Für die Zwecke der Veranschaulichung werden Beispiele konkreter Geräte vorgestellt, und es wird auch ein Ausblick in mögliche künftige Entwicklungen gegeben.

Anschließend widmet sich die Untersuchung den gesellschaftlichen Auswirkungen der Smartglasses-Technologie und den Reaktionen von Menschen auf die „Cyborgs“, wie deren Nutzer häufig bezeichnet werden. Danach werden das Konzept der Privatsphäre, dessen Grundlagen sowie seine historische Entwicklung dargestellt, um die Bedeutung der Privatsphäre sowie ihre Beeinträchtigung, aber auch ihre gegenwärtige und künftige Daseinsberechtigung beurteilen zu können. Im nächsten Schritt wird untersucht, inwieweit die Privatsphäre einen verfassungsrechtlichen Schutz erfahren hat und wie dieser durch den Einsatz von Smartglasses beeinträchtigt wird. Neben der Prüfung des Rechts auf informationelle Selbstbestimmung werden die Kriterien zur Bestimmung der Nützlichkeit und der Eingriffsintensität von Smartglasses zum Zweck der Interessenabwägung auf der Ebene des einfachen Rechts herausgearbeitet. Die rechtliche Prüfung wird durch die Möglichkeiten zur sofortigen Abwehr Betroffener sowie den Einfluss der EU-Datenschutzgrundverordnung auf die gewonnenen Ergebnisse abgeschlossen.

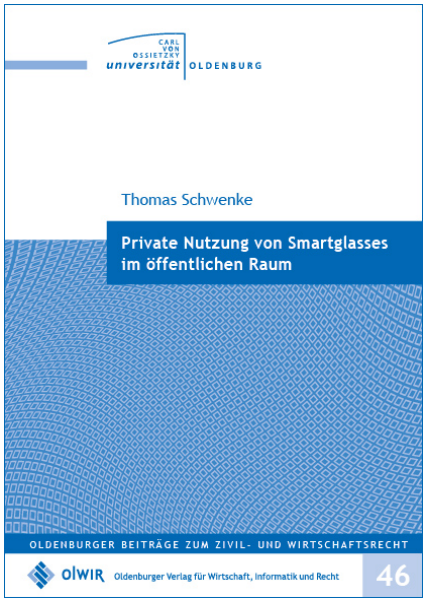
Der Schlußteil der Untersuchung beginnt mit Prognose künftiger technischen und sozialer Entwicklungen. Ihr folgen Vorschläge für Maßnahmen, die eine privatsphärenschonende Nutzung von Smartglasses im öffentlichen Raum ermöglichen sollen.

XXV, 409 S., Edewecht 2016, € 49,80
ISBN 978-3-95599-029-9

OlWIR Verlag –
Oldenburger Verlag für Wirtschaft,
Informatik und Recht
Rudolf-Kinau-Str. 54, 26188 Edewecht

Bestellungen an: mailto:mail@olwir.de

Bestellung über Website:
http://olwir.de/?content=reihen%2Fuebersicht&sort=zi-wi-re&isbn=978-3-95599-029-9



OLDENBURGER BEITRÄGE
ZUM ZIVIL- UND WIRTSCHAFTSRECHT

herausgegeben von

Univ.-Prof. Dr. Jürgen Taeger

Dr. Thomas Schwenke

Private Nutzung von Smartglasses im öffentlichen Raum

olWIR Oldenburger Verlag für Wirtschaft, Informatik und Recht

Bibliografische Information Der Deutschen Nationalbibliothek

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

Zugl.: Oldenburg, Univ., Diss., 2016

Gedruckt auf alterungsbeständigem säurefreiem Papier.

Oldenburger Verlag für Wirtschaft, Informatik und Recht
Rudolf-Kinau-Str. 54, 26188 Edewecht
mail@olwir.de

Edewecht 2016

ISBN: 978-3-95599-029-9

VORWORT

Diese Arbeit wurde im Wintersemester 2015/2016 von der Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften der Carl von Ossietzky Universität Oldenburg als Dissertation angenommen und ist mit Bezug zum Verbundprojekt „Chancen und Risiken von Smartcams im öffentlichen Raum“ (ChaRiSma) entstanden. Die berücksichtigte Literatur, die Rechtsprechung sowie die Sach- und übrige Rechtslage befinden sich auf dem Stand vom 15. Januar 2016.

Mein Dank für die fachlich wertvolle Unterstützung, persönliche Motivation sowie die methodischen und inhaltlichen Freiräume bei der Erstellung dieser Arbeit gilt dem Projektleiter und meinem Doktorvater Prof. Dr. Jürgen Taeger. Ein großer Dank gilt ebenfalls dem Zweitgutachter Prof. Dr. Dr. Volker Boehme-Neßler.

Ebenso möchte ich mich bei dem Heise Zeitschriften Verlag für die technische Unterstützung, insbesondere durch Joerg Heidrich und Jan-Keno Janssen bedanken. Denis Mitlacher schulde ich großen Dank für die Durchsicht des Manuskripts und Vorschläge zu technischen und gesellschaftlichen Aspekten. Dies gilt auch für Hannes Schleeh, dem ich viele Erfahrungen zur Nutzung von Smartglasses verdanke.

Nicht zu Letzt geht der Dank an meinen Podcasts-Partner Marcus Richter und die Zuhörer des Rechtsbelehrung.com-Podcasts, in dessen Rahmen die Idee und die Grundlagen für diese Arbeit gelegt wurden. Für viele Anregungen und Unterstützung möchte ich mich ebenfalls bei meinen Freunden, Followern und Kontakten im Internet bedanken. Meiner Familie und meinem Team bin ich für den Rückhalt ebenfalls zum Dank verpflichtet.

Berlin, im Mai 2016 Thomas Schwenke

INHALTSÜBERSICHT

INHALT

ABKÜRZUNGSVERZEICHNIS

a.A.	andere Ansicht/andere Auffassung
AfP	Archiv für Presserecht
AG	Amtsgericht
AnwZert ITR	AnwaltZertifikatOnline - IT-Recht
AöR	Archiv des öffentlichen Rechts
APR	Allgemeines Persönlichkeitsrecht
AR	Augmented Reality (Erweiterte Wirklichkeit)
ArbRAktuell	Arbeitsrecht Aktuell
BAG	Bundesarbeitsgericht
BAGE	Amtliche Sammlung der Entscheidungen des BAG
BayObLG	Bayerisches Oberstes Landesgericht
BayVBl	Bayerische Verwaltungsblätter
BeckRS	Beck'sche Rechtsprechungssammlung
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des BVerfG
BVerwG	Bundesverwaltungsgericht
BVerwGE	Amtliche Sammlung der Entscheidungen des BVerwG
CR	Computer und Recht
DAR	Deutsches Autorecht
DJZ	Deutsche Juristen-Zeitung
DÖV	Die Öffentliche Verwaltung
DSGVO	Europäische Datenschutz-Grundverordnung

DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
E	Entwurf
EG	Europäische Gemeinschaft
EG-DSRL	Europäische Datenschutzrichtlinie (95/46/EG)
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
FS	Festschrift
GG	Grundgesetz
GRCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtschutz und Urheberrecht
GRUR Int	Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil
GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht Praxis im Immaterialgüter- und Wettbewerbsrecht
GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report
h.M.	herrschende Meinung
Halbs.	Halbsatz
HFR	Humboldt Forum Recht
HRRS	Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht
Hrsg.	Herausgeber
IIC	International Review of Intellectual Property and Competition Law
InTeR	Zeitschrift zum Innovations- und Technikrecht
IR	InfrastrukturRecht
ITRB	Der IT-Rechts-Berater
JA	Juristische Arbeitsblätter

JCMC	Journal of Computer-Mediated Communication
JR	Juristische Rundschau
JS	Juristische Schulung
Jura	Juristische Ausbildung
JuS	Juristische Schulung
JZ	Juristenzeitung
K&R	Kommunikation und Recht
KG	Kammergericht
KommJur	Kommunaljurist
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz)
LAG	Landesarbeitsgericht
LG	Landgericht
LK	Leipziger Kommentar
LKV	Landes- und Kommunalverwaltung
LPG	Landespressegesetz
M.w.N.	Mit weiteren Nachweisen
MDR	Monatsschrift für deutsches Recht
MMR	MultiMedia und Recht
MMR-Aktuell	Newsletter zur Zeitschrift MultiMedia und Recht
Müko	Münchner Kommentar
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NWVBl	Nordrhein-Westfälische Verwaltungsblätter
NZA	Neue Zeitschrift für Arbeitsrecht
NZM	Neue Zeitschrift für Miet- und Wohnungsrecht
NZV	Neue Zeitschrift für Verkehrsrecht

OBA	Online Behavioural Advertising
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
p.	page (Seite in englischsprachigen Zeitschriften)
PNAS	Proceedings of the National Academy of Sciences
RDV	Recht der Datenverarbeitung
RG	Reichsgericht
RGZ	Entscheidungssammlung des Reichgerichts in Zivilsachen
RGSt	Entscheidungssammlung des Reichgerichts in Strafsachen
RL	Richtlinie
Rn.	Randnummer
RStV	Rundfunkstaatsvertrag
SIAM J. Appl. Math.	SIAM (Society for Industrial and Applied Mathematics) Journal on Applied Mathematics
SPIE	The International Society for Optical Engineering (früher: Society of Photographic Instrumentation Engineers)
SSRN	Social Science Research Network
St. Rspr.	Ständige Rechtsprechung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SVR	Straßenverkehrsrecht
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UrhG	Urhebergesetz
U.S.	United States Reports
Var.	Variante
VersR	Versicherungsrecht
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof

VR	Virtual Reality (Virtuelle Realität)
WRP	Wettbewerb in Recht und Praxis
ZD	Zeitschrift fur Datenschutz
ZD-Aktuell	Newsdienst ZD-Aktuett
ZEuP	Zeitschrift für Europäisches Privatrecht
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZRP	Zeitschrift fur Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht
ZUM-RD	Zeitschrift für Urheber- und Medienrecht, Rechtsprechungsdienst
ZWE	Zeitschrift für Wohnungseigentumsrecht

A EINFÜHRUNG UND GRUNDLAGEN DER UNTERSUCHUNG

I. Problemdarstellung und Ziele der Untersuchung

Als Smartglasses werden mobile Computer bezeichnet, die ähnlich einer Korrekturbrille auf dem Kopf getragen werden und mit einer Kamera, Netzwerkanbindung und einer Ausgabeeinheit über ähnliche technische Funktionen wie Smartphones verfügen.[1] Anders als Smartphones sollen Smartglasses jedoch nicht nur bei Bedarf in die Hand genommen werden, sondern ihren Nutzern ähnlich wie traditionelle Korrekturbrillen permanent zur Verfügung stehen.[2]

Welche Bedeutung dieser Unterschied hat, zeigte sich in den Reaktionen auf die ersten einer breiteren Öffentlichkeit vom Unternehmen Google vorgestellten Smartglasses mit der Bezeichnung „Glass".[3] Das Gerät polarisierte wie selten eine neue Technologie zuvor.[4] Viele Nutzer zeigten sich begeistert und lobten eine Befreiung ihrer Hände vom Smartphone, effektive Informationsvermittlung und den schnellen Kamerazugriff.[5] Auf der anderen Seite sahen Kritiker in „Glass" ein Potenzial zur massiven Verletzung der Privatsphäre, die sie mit Begrifflichkeiten, wie

---

1 Der Begriff "Smart Glasses" wird im Rahmen dieser Untersuchung synonym mit dem, im deutschen Sprachraum verbreiteten Begriff "Datenbrille" verwendet; die innerhalb der Untersuchung verwendeten personenbezogenen Begrifflichkeiten (z.B. "Nutzer" oder "Betroffener") sind geschlechtsneutral zu verstehen.

2 *Schart/Tschanz*, Augmented Reality, 2015, S. 110.

3 Synonym wird auch von "Google Glass" gesprochen; *Heinrich*, AnwZert ITR 2014, 10/2014, Anm. 2; *Schwenke*, K&R 2013, S. 685; *Solmecke/Kocatepe*, ZD 2014, S. 22.

4 *Schwenke*, K&R 2013, S. 685.

5 Das Datum des letzten Abrufs von Onlinequellen wird nachfolgend in der Klammer an deren Ende angegeben; Google Glass - One Year On, hypernetec, http://hypernetec.com/glass-one-year/(7.9.2015); Good camera, great internet but poor speaker, Mail Online, http://www.dailymail.co.uk/news/article-2402934/Google-Glass-users-experience-having-Internet-eyesocket.html (7.9.2015); *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (7.9.2015); *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Scobble*, Google Glass is still misunderstood, says the guy who wore them in the shower, CNET, http://www.cnet.com/news/google-glass-is-still-misunderstood-says-the-guy-who-wore-them-in-the-shower/(7.9.2015); *Topolsky*, I used Google Glass, The Verge, http://www.theverge.com/2013/2/22/4013406/i-used-google-glass-its-the-future-with-monthly-updates (7.1.2015).

„Waffe zur Verletzung von Persönlichkeitsrechten“ oder „Werkzeug des Bösen“ unterstrichen.[6]

Die Reaktionen auf Google Glass zeigen, wie groß die Bandbreite zwischen Hoffnungen und Befürchtungen sind, die Smartglasses entgegengebracht werden. Da die Geräte zudem eine Verschmelzung zwischen Menschen und Maschinen manifestieren, rufen sie tiefgehende existentielle Ängste hervor.[7] Den Menschen ist zwar bewusst, dass der technologische Fortschritt ihren Alltag verändert, doch bisher fand das im Hintergrund statt und die negativen Auswirkungen waren nur mittelbar spürbar.[8] Die wirtschaftliche Verwertung ihres Verhaltens zu Werbezwecken, Videoüberwachung, staatliche Überwachung oder Datenschutzskandale sind jedoch anders als die Vorteile neuer Technologien nur selten als Folgen unmittelbar wahrnehmbar.[9] D.h., Menschen machen sich um ihre Privatsphäre zwar Sorgen, gewichten die unmittelbaren Vorteile sozialer Interaktion, Bequemlichkeit, Unterhaltung und Effizienz jedoch höher (sog. „Privacy Paradoxon“).[10]

Diese Vorteile moderner Technologien werden auch durch Smartglasses versprochen.[11] Dabei sollen Smartglasses jedoch nicht nur einen Einblick in die virtuelle Welt gewähren, sondern als effektive Schnittstellen die virtuelle und die physische Realität vor den Augen ihrer Träger zu einer

---

6 *von Gehlen*, Datenbrillen - Werkzeug des Bösen, SZ, http://www.sueddeutsche .de/digital/datenbrillen-werkzeug-des-boesen-1.1871620 (26.1.2014); Thilo Weichert: „Google Glass ist eine Waffe“, heise online, http://www.heise.de/newsticker/meldung/ Thilo-Weichert-Google-Glass-ist-eine-Waffe-2176677.html (15.6.2014).

7 *Sacasas*, Preserving the Person in the Emerging Kingdom of Technological Force, The Frailest Thing, http://thefrailestthing.com/2014/08/21/preserving-the-person-in-the-emerging-kingdom-of-technological-force/(22.8.2014).

8 *Barnes*, First Monday 2006, Vol. 11, Nr. 9, http://firstmonday.org/article/view/1394/ 1312 (3.10.2014); *Tufekci*, Bulletin of Science, Technology & Society 2008, Vol. 28, Nr. 1, p. 20.

9 *Bernau*, Daten gehackt?, Fazit - das Wirtschaftsblog, https://blogs.faz.net/fazit/2015/ 09/10/experiment-zu-datenschutz-und-datensicherheit-6470/(14.9.2015); *Lobo*, S.P.O .N. - Die Mensch-Maschine, Spiegel Online, http://www.spiegel.de/netzwelt/web/sascha-lobo-ueber-gescheiterte-deutsche-netzpolitik-a-1038117.html(15.9.2015); *Mann* , IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10 (13) f.; *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (258).

10 *Barnes*, First Monday 2006, Vol. 11, Nr. 9, http://firstmonday.org/article/view /1394/13 12 (3.10.2014); vgl. *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/ Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (41); *Tufekci*, Bulletin of Science, Technology & Society 2008, Vol. 28, Nr. 1, p. 20.

11 Schwenke, DuD 2015, 166; *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015).

Wirklichkeit verschmelzen lassen.[12] Als „Gegenleistung“ wird von den Nutzern gefordert, dass sie den Smartglasses erlauben, die physische Wirklichkeit in deren Blickfeld zu kartieren.[13] Aber anders als bei der gegenwärtig oft nicht unmittelbar wahrnehmbaren Videoüberwachung und Datenverarbeitung im Hintergrund,[14] wird diese Art der Erfassung durch die der Blickrichtung ihrer Träger folgenden und mit Kameras ausgestatteten Geräte nicht nur deutlich, sondern drängt sich geradezu auf.[15] Es wäre an dieser Stelle jedoch zu kurz gedacht, davon auszugehen, dass Smartglasses nur Ablehnung finden werden und daher als Technologie keine Zukunft haben.[16] Dabei würde man außer Acht lassen, welches Potenzial sie für die Selbstbefähigung von Menschen in einer Informationsgesellschaft bieten.

Aufgrund dieser technischen und sozialen Zwänge darf sich eine rechtliche Würdigung von Smartglasses nicht auf die Geräte selbst beschränken, sondern muss auch deren technologisches und gesellschaftliches Umfeld mit berücksichtigen. Zwar mögen Smartglasses derzeit noch viele Menschen abschrecken, doch zeigte z.B. der Straßenpanoramadienst „Street View“, wie schnell sich Proteste in Akzeptanz wandeln können.[17] Zwar sind Smartglasses intrusiver als statische Straßenpanoramen.[18] Dennoch ist es auch in ihrem Fall vorstellbar, dass ihr Nutzen die Furcht um die Privatsphäre ebenfalls in den Hintergrund treten lassen wird.[19]

D.h. nicht, dass Smartglasses von einem Tag auf den anderen im öffentlichen Raum akzeptiert werden. Die durchmischten Erfahrungen mit

---

[12] *Mann/Niedzviecki*, Cyborg, 2002, S. 32; *Schart/Tschanz*, Augmented Reality, 2015, S. 11, 110; *Schwenke*, DuD 2015, S. 161 (162); der Begriff "physisch" wird im Rahmen der Untersuchung i.S.v. körperlich, greifber, stofflich und mit Menschlichen Sinnen ohne Hilfsmittel wahrnehmbar, verstanden.

[13] Die virtuelle Abbildung der Welt ist für eine Verbindung der physischen mit der virtuellen Welt essentiell, *Schart/Tschanz*, Augmented Reality, 2015, S. 5.

[14] *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (41); *Mann/Niedzviecki*, Cyborg, 2002, S. 27; *Sofsky*, Verteidigung des Privaten, 2007, S. 13 f.

[15] *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Janssen*, Warum Glass (noch) nicht funktioniert, c't, http://www.heise.de/ct/artikel/Warum-Glass-noch-nicht-funktioniert-1897211.html (16.8.2014).

[16] *Schwenke*, DuD 2015, S. 161 (166).

[17] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 267.

[18] *Schwenke*, K&R 2013, S. 685.

[19] Dafür spricht bereits jetzt ein hohes Interesse an der Nutzung von Smartglasses (38% von 1014 befragten Bundesbürgern ab 14 Jahren), Großes Interesse an den Funktionen von Smart Glasses, BITKOM, https://www.bitkom.org/Presse/Presseinformation/Grosses-Interesse-an-den-Funktionen-von-Smart-Glasses.html (14.11.2015).

Google Glass scheinen ganz im Gegenteil die Folge zu haben, dass Smartglasses nunmehr mit Blick auf den Einsatz in beruflichen oder heimischen Bereichen entwickelt werden.[20] Doch wenn sie in diesen Bereichen essentiell sowie optisch unaufdringlicher werden, ist mit einem steigenden Bedürfnis nach deren Nutzung im öffentlichen Raum zu rechnen.[21] Der öffentliche Raum gilt jedoch als eine essentielle Grundlage einer auf einen zwischenmenschlichen Meinungsaustausch und Selbstentfaltung bedachten freiheitlich-demokratischen Gesellschaft, sodass er als eine rote Linie für den Einsatz von Smartglasses begriffen werden kann.[22] Jedoch ist zu befürchten, dass ein Festhalten am vollständigen Verbot von Smartglasses an der Lebensrealität vorbei und zu einem rechtlich unsicheren Bereich zwischen Legalität und der Legitimität der Nutzung von Smartglasses führen kann. Als Folge könnten Unsicherheiten und Konflikte zwischen Nutzern von Smartglasses und Betroffenen entstehen.[23]

Vor dem Hintergrund der potenziellen Vorteile und Gefahren von Datenbrillen liegt das Ziel dieser Untersuchung daher zuerst darin, einen rechtlichen Rahmen für die Nutzung von Smartglasses aufzuzeigen. Die so gewonnenen Erkenntnisse sollen anschließend als Grundlage für Vorschläge dienen, mit denen das Spannungsverhältnis zwischen dem Bedürfnis nach der Nutzung von Smartglasses und der Privatsphäre aufgelöst werden kann. Als Ergebnis sollte dabei langfristig eine Kultur der persönlichkeitsrechtsschonenden Datenbrillennutzung rechtlich verbindlich etabliert werden. Diese Kultur wird spätestens dann relevant, wenn Smartglasses weiter so miniaturisiert werden, dass man sie nicht mehr (als solche) erkennen kann.

II. Thesen der Untersuchung

Die folgenden Thesen sollen bei der nachfolgenden Untersuchung als Orientierungspunkte dienen und helfen, die an Smartglasses gestellten Erwartungen sowie die ihnen entgegengestellte Kritik zu überprüfen:

---

[20] Google Glass „Enterprise Edition" is foldable, more water resistant, rugged for the workplace, 9to5Google, http://9to5google.com/2015/07/21/google-glass-enterprise-edition-is-foldable-water-resistant-rugged-for-the-workplace/(14.9.2015); Windows 10 und «HoloLens», sueddeutsche.de, http://www.sueddeutsche.de/news/wirtschaft/computer-windows-10-und-hololens-microsoft-will-wieder-cool-werden-dpa.urn-newsml-dpa-com-20090101-150122-99-04014 (14.2.2015); *Nelson*, Epson Moverio BT-200 Augmented Reality Glasses Review, Tom's Hardware, http://www.tomshardware.com/rev iews/epson-moverio-bt-200-augmented-reality-glasses,3923.html (8.9.2015).

[21] Vgl. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 23 f.

[22] Vgl. BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (44); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 78; *Spiecker genannt Döhmann*, CR 2010, S. 311 (315).

[23] Vgl. *Schwenke*, K&R 2013, S. 685 (691); *Solmecke/Kocatepe*, ZD 2014, S. 22 (26).

These 1: Smartglasses verfügen über das Potenzial, sich zu integralen Teilen des menschlichen Alltags zu entwickeln, da sie mit ihren Funktionen die Bedürfnisse der Informationsgesellschaft nach Effizienz, Sicherheit und Bequemlichkeit befriedigen.

These 2: Smartglasses bergen aufgrund fehlender Transparenz der Informationserfassung sowie mangelnder Kontrolle anschließender Informationsverarbeitung eine erhebliche Gefahr der Beeinträchtigung der Privatsphäre und damit rechtlich verbürgter Persönlichkeitsrechte der von ihnen erfassten Personen. Die Gefahren gehen weit über die bisher verwendeten Arten der optischen, akustischen und elektronischen Informationserfassung, z.B. durch Videoüberwachung oder Smartphones mit Kameras, hinaus.

These 3: Aufgrund der wahrnehmbaren Auswirkungen auf die Privatsphäre wird der Einsatz von Smartglasses im öffentlichen Raum zu Konflikten zwischen ihren Nutzern und den betroffenen Personen führen, der einen Bedarf nach unmittelbaren und sofortigen Schutzmöglichkeiten der Betroffenen mit sich bringen wird.

These 4: Smartglasses sind lediglich der Bestandteil einer viel umfassenderen technologischen und sozialen Veränderung, die nicht aufgehalten werden kann. Ein langfristiges Verbot von Smartglasses ist aufgrund ihres Nutzens in einer zunehmend verdateten Gesellschaft nicht durchführbar.

These 5: Die gegenwärtige Privatsphäre im öffentlichen Raum wird zwar zugunsten von Smartglasses Einschränkungen hinnehmen müssen, darf jedoch nicht aufgegeben werden. Es wird ein Miteinander des Rechts und der Technik erforderlich, um die Nutzung von Smartglasses im öffentlichen Raum zu ermöglichen.

III. Methodik der Untersuchung

Die im Rahmen dieser Untersuchung eingesetzten Methoden orientieren sich an den Regeln der juristischen Technikfolgenabschätzung. Bei der Technikfolgenabschätzung handelt es sich um eine Sammelbezeichnung, die eine Reihe von interdisziplinären Verfahren umschließt, die der sozialwissenschaftlichen, ethischen, theologischen oder natur- sowie ingenieurwissenschaftlichen „Reflexion über Voraussetzungen, Wirkungen und Folgen der technikinduzierten Gestaltung moderner Gesellschaften“ dienen.[24] Dabei werden die gesellschaftlichen Folgen der Technik im Hinblick auf deren mögliche primäre und unmittelbare Folgen, seien sie ge-

[24] *Westphalen*, Einführung in die Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 9.

wollt oder ungewollt, singulär, kumulativ oder synergetisch betrachtet.[25] Zuvor müssen jedoch die Wertgrundlagen, auf die sich die Abschätzung bezieht, offengelegt werden.[26]

1. Ziel der präventiven Technikfolgenabschätzung

Das Ziel der rechtlichen Technikfolgenabschätzung besteht in der Erkennung, Bewertung und Beeinflussung der Veränderungskraft technischer Entwicklungen.[27] Im Rahmen der Technikfolgeabschätzung wird vor allem ein „technikoptimistisches Fortschrittsverständnis" kritisch hinterfragt, das die zeitlich letzte Stufe einer gesellschaftlichen Entwicklung als ihre beste und erstrebenswerte Form ansieht.[28]

Einer der Hauptpunkte der Kritik gegenüber dem Fortschrittsbegriff ist die Selbstverständlichkeit, mit der technische Innovationen mit einer Verbesserung von Lebensumständen der Menschen gleichgesetzt werden.[29] Denn isoliert betrachtet ist der technische Fortschritt für sich betrachtet rational, direkt und aggressiv.[30] D.h., der eigene Maßstab für die Güte einer technischen Entwicklung ist der Grad, mit dem diese den ihr vorbestimmten Zweck erfüllt. Moralische und normative Werte, wie z.B. der Unterschied zwischen „gut" und „richtig", sind grundsätzlich keine funktionalen Anforderungen und daher nur von Relevanz, wenn sie als Ziele in die technische Entwicklung implementiert werden.[31]

Um die negativen Folgen des technischen Fortschritts zu verhindern und die positiven Entwicklungsaspekte zu fördern, ist es notwendig, „präventive Gedankenexperimente" bereits durchzuführen, bevor sich technische Innovationen etablieren.[32] Hierbei ist zu fragen, welchen Einfluss die

---

[25] Ebenda, 9.

[26] Ebenda.

[27] *Roßnagel*, Die Rolle des Rechts im Prozeß der Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 222 (223).

[28] *Westphalen*, Einführung in die Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 9 (10).

[29] Ebenda.

[30] Vgl. *Ellul*, The Technological Society, 1967, S. 142 f.

[31] Vgl. *Beck*, Das Zeitalter der Nebenfolgen und die Politisierung der Moderne, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 19 (71); *Ellul*, The Technological Society, 1967, S. 96 ff.; *Hornung*, ZD 2011, S. 51 (52); *Moglen*, Privacy under attack: the NSA files revealed new threats to democracy, The Guardian, http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy (10.6.2014); so bereits Mitte des 20sten Jahrhunderts, *Wiener*, Kybernetik, 1963, S. 62; *Wrede*, ZD 2012, S. 321 (322).

[32] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 111; *Roßnagel*, Die Rolle des Rechts im Prozeß der Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 222 (223 f.).

technischen Innovationen auf das gegenwärtig rechtlich verankerte Interessengefüge haben werden und wie sie dessen Verwirklichungsmöglichkeiten beeinflussen werden. Denn nur bei einer rechtzeitig vorweggenommenen Prüfung können gesellschaftliche Lernprozesse beeinflusst und Vorschläge zur Technikgestaltung ausgearbeitet werden.[33] Im optimalen Fall beeinflusst das Recht die Technik, indem es deren Entwicklung steuert und so die Gefahren für die Schutzgüter verhindert sowie die gewünschten Entwicklungschancen fördert.[34]

2. Methoden der Technikfolgenabschätzung

Der erste Schritt der Technikfolgenabschätzung besteht in einer Abschätzung des Einflusses der untersuchten Technologie auf die gesellschaftlichen Prozesse.[35] Zu beachten ist, dass die aufgestellten Prognosen und die ihnen folgenden Handlungsvorschläge auf einem möglichen Kausalverlauf basieren, dessen Ausgangspunkt der gegenwärtige technologische, gesellschaftliche und rechtliche Entwicklungsstand ist. Der Fortschritt bietet jedoch viele „historische Verzweigungssituationen", welche sich erst dann ergeben, wenn die Technologie sich in die Gesellschaft eingebettet hat.[36] Damit zwingt der technologische Fortschritt zugleich auch dem Recht einen „ständigen Reformbedarf" auf, da einmalige Festlegungen nur eine begrenzte zeitliche Wirkung haben.[37]

Der zweite Schritt der Technikfolgenabschätzung besteht in der Bewertung der Technikfolgen. Dabei wird die Rechtsverträglichkeit der durch die untersuchte Technik zu erwartenden Folgen im Hinblick auf bestimmte Ziele des Rechts, hier die Privatsphäre und die von ihr geschützten Rechtsgüter, als Maßstab geprüft.[38]

Im dritten Schritt werden mögliche Maßnahmen erörtert, die dazu beitragen sollen, die herausgestellten Gefahren für die in das Zentrum der Untersuchung gestellten Rechtsgüter zu verhindern.[39] Die eigentliche Regelung der technischen Entwicklung kann wiederum durch Normsetzung, technische Maßnahmen oder die Kombination beider Mittel erfol-

---

[33] *Roßnagel*, Die Rolle des Rechts im Prozeß der Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 222 (224).

[34] Ebenda, 230 f.

[35] Ebenda, 225.

[36] Ebenda, 226 f.

[37] *Piltz*, Soziale Netzwerke im Internet, 2013, S. 281; *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 11 f.

[38] Vgl. *Roßnagel*, Die Rolle des Rechts im Prozeß der Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 222 (228 f.).

[39] Vgl. Ebenda, 230 f.

gen.[40] Dabei liegt die Hypothese der Techniksteuerung in der Annahme, dass Technik sich nicht schicksalhaft entwickelt, sondern durch eine Vielzahl von Interessen, insbesondere ökonomischer, wissenschaftlicher oder bürokratischer Art gesteuert wird.[41] D.h., es ist nicht ungewöhnlich, dass mögliche Innovationen nicht vollumfänglich umgesetzt werden.[42]

3. Mittel und Umfang der Untersuchung

Aufgrund der Geschwindigkeit des technischen Fortschritts bezieht sich diese Untersuchung auf die Funktionen sowie mögliche künftige Entwicklungen von Smartglasses und weniger auf konkrete Geräte.

Zu den wesentlichen Grundlagen dieser Arbeit gehören ebenfalls soziologische Betrachtungen, die einen Ausgangspunkt für die rechtliche Würdigung und die mit ihr zu erreichenden Ziele darstellen. Damit soll vor allem erreicht werden, dass die rechtliche Prüfung sich stets an einer objektiv und wissenschaftlich erfassten Lebenswirklichkeit orientiert.[43] Daher ist eine Maßgabe dieser Untersuchung, offen für mögliche Entwicklungen zu sein, auch wenn diese den traditionellen Schutz von Individuen durch die Privatsphäre hinterfragen und gesellschaftlich als unbequem oder unerwünscht betrachtet werden sollten.[44]

Die Neuartigkeit von Smartglasses als Untersuchungsgegenstand führt dazu, dass die meisten technischen und gesellschaftlichen Informationen im Bezug auf aktuelle Entwicklungen aus Onlinequellen und der allgemeinen Presse stammen. Jedoch wurde auf die Verifikation der Quellen durch Übereinstimmung unterschiedlicher Berichte und die berechtigte Erwartung einer redaktionell-journalistischen Kontrolle geachtet.

---

[40] Vgl. Ebenda, 231; *Saeltzer*, DuD 2015, S. 103; *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 3 ff.; *Schulz*, CR 2012, S. 204; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 3a, Rn. 4 f.

[41] Vgl. *Roßnagel*, Die Rolle des Rechts im Prozeß der Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 222 (230 f.).

[42] Als Beispiel ist der Einsatz von Gesichtserkennungstechnologien zu nennen, die von Unternehmen u.a. wegen der beängstigenden Wirkung, die sich zudem wirtschaftlich niederschlagen könnte, nicht eingesetzt werden (sog. "Creep-Faktor" der Technik), *O'Reilly*, The Creep Factor, Forbes, http://www.forbes.com/sites/oreillymedia/2014/03/06/the-creep-factor-how-to-think-about-big-data-and-privacy/(12.2.2015).

[43] Zum anderen sollen allgemeinsprachliche und unwissenschaftliche Begriffsbedeutungen sowie Ungenauigkeiten die Untersuchung nicht beeinflussen.

[44] Die Vorbehalte von Menschen gegenüber künftigen Entwicklungen, müssen vor dem Hintergrund möglicher kollektiver Auswirkungen gewürdigt werden, *Murswiek*, Technische Risiken, in: *Westphalen*, Technikfolgenabschätzung, 1997, S. 238 (247) f.; vielfach resultieren die Vorbehalte aus der Bequemlichkeit und dem Widerwillen sich auf neue Gegebenheiten einzustellen, *Canton/Groot/Nahuis*, CentER Discussion Paper, Tilburg University, Centre for Economic Research 1999, Vol. 106, p. 1 (3).

Ferner ist zu beachten, dass die Untersuchung vor dem Hintergrund des westlichen Kulturraums und im Speziellen der deutschen Gesellschaft und des deutschen Rechts erfolgt. Sie bezieht jedoch auch ausländische Quellen ein, soweit deren Aussagen und Erkenntnisse übertragbar oder wie insbesondere im Falle des Unionsrecht sogar maßgeblich sind.

IV. Begriffsdefinitionen

Im Rahmen dieser Untersuchung werden bestimmte Begrifflichkeiten wiederkehrend verwendet, die über eine gewisse Ambiguität verfügen, sodass deren Bedeutungsinhalt für die Untersuchung eindeutig festgelegt werden muss. Sie sollen nachfolgend nicht nur „vor die Klammer gezogen werden", sondern auch eine technische, gesellschaftliche und rechtliche Basis schaffen, auf der diese Untersuchung aufbaut.

1. Informationsgesellschaft

Die Menschheit befindet sich in einem radikalen gesellschaftlichen Wandel, der vor allem durch die Entwicklung neuer digitaler und vernetzter Technologien angetrieben wird.[45] Die für diese Untersuchung maßgeblichen technisch-sozialen Veränderungen nahmen vor allem Mitte der 1990er Jahre zu, als die Informations- und Kommunikationstechnologien verschmolzen, das Internet zu einem Massenphänomen wurde und entwickelten sich ab ca. dem Jahr 2005 mit sozialen Medien und als „intelligent" bzw. „smart" bezeichneten Geräten (z.B. Smartphones) zu ihrer gegenwärtigen Form.[46]

Als Bezeichnung für die vielfältigen Änderungen kristallisiert sich der Begriff der „Informationsgesellschaft" heraus, der die radikal zunehmende Bedeutung von „Informationen" für mediale, kulturelle, soziale, politische, wirtschaftliche und individuelle Entwicklungen unterstreicht.[47] Der Begriff der Informationsgesellschaft ist jedoch weniger eine allumfassende und auf einheitlicher Theorie basierende Gesellschaftstheorie, sondern vielmehr als ein gemeinsamer Nenner einer vielfältigen Zahl unterschiedlicher Ansichten der gegenwärtigen gesellschaftlichen Änderungen zu verstehen.[48] Sie alle behandeln unterschiedliche Aspekte eines durch

---

[45] *Webster*, Theories of the Information Society, 2014, S. 1 ff.

[46] Vgl. Ebenda, 12.

[47] *Hotter*, Privatsphäre, 2011, S. 114; bereits in den 1980er Jahren sprach man von einer "Explosion von Informationen", *Schiller*, Columbia Journal of World Business 1983, Vol. 18, Nr. 1, p. 86 (88); *Steinbuch*, GRUR 1987, S. 579; *Webster*, Theories of the Information Society, 2014, S. 1 ff.

[48] *Hotter*, Privatsphäre, 2011, S. 102; *Webster*, Theories of the Information Society, 2014, S. 2.

Informationen angetriebenen gesellschaftlichen Wandels und dessen prägender Auswirkungen.[49]

2. Daten, Informationen und Wissen

Der Informationsgesellschaft liegt die Information, als deren Dreh- und Angelpunkt, zugrunde. Auch Smartglasses sind konzeptionell darauf ausgelegt, als Werkzeuge der Informationserfassung, -verarbeitung und -ausgabe zu dienen. Genauso geläufig und für diese Untersuchung bedeutend sind die mit Informationen im engen Zusammenhang stehenden und oft synonym verwendeten Begriffe „Daten" (bzw. das seltener verwendete Singular „Datum") und Wissen.

Daten sind als Elemente zu verstehen, die der Unterscheidung dienen und über zwei unterschiedliche Zustände, wie „ja" oder „nein" bzw. „1" oder „0" verfügen können.[50] Sie sind für sich noch keine Informationen, da sie ohne einen Bezugspunkt keine Aussage haben.[51] Erst wenn Bezugspunkte existieren, die dazu führen, dass Daten eine bestehende Informationsordnung (bezeichnet als Wissen) verändern, werden sie selbst zu Informationen.[52] Dadurch erlangt ein Datum, das lediglich über eine „syntaktische Dimension" verfügt, in Form der Information eine „semantische Dimension", also eine Bedeutung.[53]

---

[49] Mit Theorien sollen im Rahmen dieser Untersuchung alle Ansichten, Konzepte und Gesellschaftsmodelle verstanden werden, vgl. *Ketzer*, Securitas ex Machina, 2005, S. 32, Fn. 83; *Webster*, Theories of the Information Society, 2014, S. 2.

[50] Vgl. *Gumm/Sommer*, Einführung in die Informatik, 2012, S. 4 f.; *Negroponte*, Total digital, 1997, S. 22; *Wiener*, Kybernetik, 1963, S. 38.

[51] *Seemann*, Das neue Spiel, 2014, S. 18; ähnlich wirkungsorientiert wird die "Information" in den Fachbereichen der Informatik und der Kybernetik, vereinfacht ausgedrückt, als Kenntnis eines bestimmten Empfängers über Sachverhalte und Vorgänge definiert, *Sieber*, NJW 1989, S. 2569 (2572); auch die Informationstheorie versteht die Information eine Teilmenge an Wissen, die ein Sender dem Empfänger mittels Signalen über ein bestimmtes Medium, den Informationskanal, vermitteln kann, vgl. *Steinmüller*, Informationstechnologie und Gesellschaft, 1993, S. 189 ff.

[52] "Information kann als eine Nachricht definiert werden, die für den Empfänger eine Bedeutung hat; durch ihre Aufnahme wird der Empfänger in aller Regel verändert", *Klaus*, Der Grosse Bruder, 1980, S. 15; die Bedeutung der Information kann wiederum zu "Einsichten" oder "Wahrheiten" oder "Entscheidungen" führen, wobei es sich um wachsende Komplexitätsgrade und Ordnungen von Informationen handelt, *Steinbuch*, GRUR 1987, S. 579 (581); *Stonier*, Information und die innere Struktur des Universums, 1991, S. 11.

[53] *Sieber*, NJW 1989, S. 2569 (2572); *Steinmüller*, Informationstechnologie und Gesellschaft, 1993, S. 202 f.

3. Die Verdatung der Welt

Die Bedeutung von Daten als Träger von Informationen ist in der digitalen und vernetzten Welt offensichtlich.[54] Ihre Bedeutung nimmt jedoch mit der Zunahme des Potenzials der Datenverarbeitungstechnologien und der steigenden Menge von Daten weiterhin zu. Entsprechend dem im Jahr 1965 als heuristische Faustformel aufgestellten „Moor'schen Gesetz" verdoppelt sich die Rechnerleistung alle 18-24 Monate,[55] was auch der ungefähren Verdopplung der Datenmenge entspricht.[56] Die dabei entstehenden Datendimensionen liegen weit jenseits des von Menschen begreifbaren Volumens.[57]

Doch es ist nicht nur die bloße Datenmenge, nach der Menschen streben, sondern das Wissen, das aus deren Analyse gewonnen werden kann. So lassen sich Wechselbeziehungen, sog. Korrelationen, offenlegen, die bei einer auf Hypothesen basierenden Herangehensweise erst gar nicht in Betracht gezogen werden.[58] Zusammengefasst kann die unter den Begriffen „Verdatung" oder „Datafizierung" beschriebene Veränderung der

---

[54] Zur Funktion von Daten als Trägermedium, vgl. *Gumm/Sommer*, Einführung in die Informatik, 2012, S. 4 f.; *Stonier*, Information und die innere Struktur des Universums, 1991, S. 11.

[55] *Fabian*, TAUCIS - Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, ULD und Institut für Wirtschaftsinformatik der HU Berlin, 75, ULD und Institut für Wirtschaftsinformatik der HU Berlin, 2006, S. 64; *Moore*, Proceedings of the IEEE 1998, Vol. 86, Nr. 1, p. 82.

[56] EMC, The EMC Digital Universe study, 2014, http://www.emc.com/leadership/digital-universe/index.htm (2.1.2015); Zuckerberg's Law of Information Sharing, Bits Blog, http://bits.blogs.nytimes.com/2008/11/06/zuckerbergs-law-of-information-sharing/ (2.1.2015); *Geis*, ZD 2013, S. 591.

[57] So betrug die Datenmenge im Jahr 2005 rund 130 Exabyte, im Jahr 2015 sollen fast 9.000 Exabyte (d.h. 9 Zetabyte) erreicht werden, was eine Steigerung um das 2.250-fache in 10 Jahren bedeutet, Prognose zum Volumen der jährlich generierten digitalen Datenmenge weltweit in den Jahren 2005 bis 2020, Statista, http://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/ (12.8.2014); dabei enthält ein Exabyte 108 Bytes, d.h. eine Milliarde Gigabyte oder ungefähr die 2.500-fache Datenmenge aller je geschriebenen Bücher, *Anderson*, The End of Theory, WIRED, http://www.wired.com/science/discoveries/magazine/16-07/pb_theory (12.10.2013); *Floridi*, The Ethics of Information, 2013, S. 5; *Siegel*, Predictive Analytics, 2013, S. 37.

[58] *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 72 f.; *Siegel*, Predictive Analytics, 2013, S. 12.

Quantität der Daten zu einer Veränderung ihrer Qualität führen.[59] Dieses Potenzial von Daten wird gegenwärtig unter dem Schlagwort „Big Data" diskutiert.[60] Der Begriff fasst dabei nicht nur die technische Seite der Erkenntnisgewinnung aus Daten zusammen, sondern wird auch als ein gesellschaftliches Paradigma verstanden, das eine neue Ära der menschlichen Entwicklung einläutet.[61] Big Data wird nach diesem Verständnis als das gesehen, was man mit Daten „im großen, aber nicht im kleinen Maßstab tun kann, um neue Erkenntnisse zu gewinnen oder neue Werte zu schaffen, so dass sich Märkte, Organisationen, die Beziehungen zwischen Bürger und Staat und vieles mehr verändern".[62] Nach dieser Ansicht wird sich das „Big Data"-Prinzip auf die Blickweise des Menschen auf die Welt, seine Art, Entscheidungen zu treffen, und die menschliche Lebensweise auswirken.[63] Vor allem wirtschaftlich betrachtet gilt Big Data als ein „Versprechen, dass unerschöpfliche Datenfelder brachliegen, die nur auf die richtigen Techniken warten, um eingefahren, analysiert und kommerziell

---

[59] *Hill*, 2014, Vol. DÖV, S. 213 (213 f.); die Qualität von Datenanalysen hängt nicht nur von der Qualität der Daten, sondern auch deren Quantität ab, da sich hierdurch (Un)regelmäßigkeiten mit algorithmischen Methoden einfacher entdecken lassen, vgl. *Kreye*, Bedeutung von Algorithmen, SZ, http://www.sueddeutsche.de/digital/bedeutung-von-algorithmen-neue-weltsprache-1.2051528 (13.8.2014); *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 50; *Sieber*, NJW 1989, S. 2569 (2573); *Siegel*, Predictive Analytics, 2013, S. 49.

[60] *Hill*, 2014, Vol. DÖV, S. 213 (216 ff.); ursprünglich wurde mit dem Begriff eine große Datenmenge bezeichnet, die zu groß für den Arbeitsspeicher des zu verarbeitenden Computers war, *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 13; nunmehr wird unter "Big Data" das Prinzip, große Datenmengen, aus einer Vielzahl unterschiedlicher Datenquellen, mit einer hohen Verarbeitungsgeschwindigkeit zum Zwecke der optimalen Ausnutzung des Datenpotentials zu verarbeiten (englisch zusammengefasst mit den Begriffen "Volume, Variety, Velocity"), Big-Data-Technologien – Wissen für Entscheider, BITKOM, http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Big-Data-Technologien-Wissen_fuer_Entscheider_Febr_2014.pdf (18.7.2014); *Hoeren/Sieber/Holznagel*, Multimedia-Recht, Teil 16.7, Rn. 1–5; *Lanley*, Gartner Shares Findings from North Pole Inc. Big Data Assessment, Doug Laney, http://blogs.gartner.com/doug-laney/ (21.7.2014); das "3 V-Modell" wird vielfach um ein viertes "V", "Veracity" ergänzt, welches für die Zuverlässigkeit, bzw. Wahrhaftigkeit von Daten steht, IBM Institute for Business Value/Saïd Business School, University of Oxford, Analytics: The real-world use of big data, 2013, http://www.ibm.com/smarterplanet/global/ files/se__sv_se__intelligence__Analytics_-_The_real-world_use_of_big_data.pdf (21.7.2014), S. 5.

[61] So auch Geis, der eine gesellschaftliche und rechtliche Umwälzung durch Big Data vorhersieht, *Geis*, ZD 2013, S. 591; *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 13, Fn. 5; *Weichert*, ZD 2013, S. 251 (253) f.

[62] *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 13.

[63] Ebenda.

verwertet zu werden".[64] Das Potenzial der Informationsgewinnung aus Daten wird sogar mit einem Instrument verglichen, das, ähnlich wie das Fernrohr den Kosmos erschloss und das Mikroskop die Welt der Mikroben, den Blick auf systematische Zusammenhänge in der Welt eröffnen wird.[65]

Zusammengefasst entspringt das Streben nach der Verdatung dem Wunsch des Menschen, die Welt zu entdecken, zu verstehen und zu beherrschen. Während Materie und Energie die äußeren Strukturen der Welt darstellen, stellen Informationen deren innere Struktur dar.[66] An dieser Stelle ist es ein logischer Folgegedanke, dass die Herrschaft über die inneren Strukturen der Welt zugleich die Herrschaft über ihre Verkörperungen bedeuten könnte.[67]

4. Der Cyberspace

Der „Cyberspace" ist ein etwas aus der Mode gekommener Begriff, der ein Synonym für den mittels Computertechnik erzeugten virtuellen Raum ist.[68] In seiner Bedeutung steht der Cyberspace jedoch nicht nur für eine

---

64 "Data is at the centre of the future knowledge economy and society", Eurpean Commission, Towards a thriving data-driven economy, COM(2014) 442, 2014, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6210, S. 4 ff.; Zum wirtschaftlichen Potential, S. auch *Boie*, Algorithmen sind das neue Gold, SZ, http://www.sueddeutsche.de/digital/algorithmen-kontinent-der-zahlen-1.2052884 (13.8.2014); *Geis*, ZD 2013, S. 591.

65 *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 13 f.; Siegel nennt Daten in diesem Zusammenhang als "Quintessenz dessen, worum es geht", *Siegel*, Predictive Analytics, 2013, S. 42.

66 *Sieber*, NJW 1989, S. 2569 (2572); erst mit dem Aufkommen der Computertechnologie wurde es den Menschen bewusst, dass Informationen eine eigene Existenz haben, *Stonier*, Information und die innere Struktur des Universums, 1991, S. 14; zwar können Informationen Produkte des menschlichen Geistes sein, jedoch ebenso wie Materie und Energie unabhängig vom Menschen existieren, Ebenda, 385 ff.; d.h., die Information wird neben der Materie und Energie zu den elementaren Bausteinen der Welt gezählt und während Materie und Energie die äußere Struktur des Universums bilden, bestimmt die Information dessen innere Struktur; Ebenda, 2 ff.; dementsprechend fasste der Begründer der Kybernetik, Norbert Wiener, den Stellenwert der Information Mitte des zwanzigsten Jahrhunderts im Hinblick auf die Computertechnik mit den folgenden Worten zusammen: "Das mechanische Gehirn scheidet nicht Gedanken aus - wie die Leber ausscheidet - wie frühere Materialisten annahmen, noch liefert sie diese in Form von Energie aus, wie die Muskeln ihre Aktivität hervorbringen. Information ist Information, weder Materie noch Energie", *Wiener*, Kybernetik, 1963, S. 192.

67 Vgl. *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 215 ff.; vgl. *Siegel*, Predictive Analytics, 2013, S. 37.

68 Der Begriff wurde wörtlich zum ersten Mal 1981 in der Kurzgeschichte "Burning Chrome" des amerikanischen Science-Fiction-Autors William Gibson verwendet, *Griffiths*, Virtual Ascendance, 2013, S. 165; *Lessig*, Code, 2006, S. 9.

Welt der Daten- und Maschinenkommunikation, sondern auch für einen Lebensraum für Menschen, die virtuell miteinander oder mit Maschinen in Verbindung treten.[69] Damit steht der Cyberspace als ein lediglich auf Information basierender Raum im Kontrast zum physischen Raum, der aus Materie (z.B. aus ertastbaren Gegenständen) oder aus Energie (z.B. aus wahrnehmbarem Licht) besteht.[70]

Der Begriff des Cyberspace geht auf die Kybernetik zurück, ein im Jahr 1948 durch den Mathematiker Norbert Wiener begründetes Wissenschaftsfeld, das sich mit Informationen als Mittel zur Steuerung und Regelung von Maschinen, Organismen sowie sozialen Systemen beschäftigt.[71] Vereinfacht gesagt benannte Wiener den Prozess von Feedbackschleifen und Rückkopplungsmechanismen, in denen Nachrichten in einem menschlichen Wesen, in Computern oder deren Verbund verarbeitet werden.[72] Schon vor der Entstehung des heutigen Verständnisses für den „Cyberspace" bereitete Wieners Arbeit den Weg für die Idee eines einheitlichen kybernetischen Systems, in dem Menschen in einem Verbund mit Computern existieren würden.[73]

Ein Beispiel des „Cyberspace" als virtueller Lebensraum sind die sozialen Netzwerke, die sowohl dem sozialen Miteinander von Menschen als auch den wirtschaftlichen Interessen ihrer Betreiber dienen.

5. Soziale Netzwerke

Als soziale Netzwerke werden Plattformen bezeichnet, auf denen Menschen miteinander sozial interagieren, kollaborieren und Inhalte wie z.B. Texte, Bilder oder Videos produzieren (als Oberbegriff für die aktive Teilhabe der Nutzer wird in Abgrenzung zu den ersten statischen Webseiten

---

[69] *Lessig*, Code, 2006, S. 83; so auch *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 106.

[70] *Schwenke*, DuD 2015, S. 161 (162); *Stonier*, Information und die innere Struktur des Universums, 1991, S. XI.

[71] *Mann/Niedzviecki*, Cyborg, 2002, S. 52; Wiener, zitiert in: *Kuhns*, The Post-industrial Prophets, 1971, S. 218.

[72] *Mann/Niedzviecki*, Cyborg, 2002, S. 52; die Kybernetik umschreibt also die Fähigkeit zur Selbstregulierung, -steuerung und Kontrolle, was der Name zum Ausdruck bringt, der sich von dem Wort "kybernetes" ableitet, welches "Steuermann" bedeutet, *Wiener*, Kybernetik, 1963, S. 39.

[73] *Mann/Niedzviecki*, Cyborg, 2002, S. 53.

die Bezeichnung „Web 2.0“ verwendet).[74] Die sozialen Netzwerke bilden dabei in Teilen soziale Strukturen ab, indem Nutzer öffentliche oder semi-öffentliche Profile anlegen und sich mit bestimmten anderen Nutzern enger vernetzen (u.a. bezeichnet als „Kontakte“ oder „Freunde“).[75] Bei sozialen Netzwerken handelt es sich mehrheitlich um kommerziell betriebene Dienste, die Nutzern zwar ohne eine Gebühr, aber im Tausch gegen die Berechtigung deren Daten wirtschaftlich nutzen zu dürfen, bereitgestellt werden.[76]

Insgesamt sind rund 80% aller Internetnutzer in mindestens einem sozialen Netzwerk angemeldet.[77] Der Branchenprimus „Facebook“ soll mit über 1,3 Milliarden Mitgliedern[78] über die Kenntnisse von ca. zehn Prozent der Weltbevölkerung verfügen.[79] Die Nutzer selbst greifen zunehmend mit mobilen Geräten auf die Netzwerke zu und stellen laut eigenen Angaben von Facebook täglich rund 350 Millionen neue Fotografien auf der Plattform ein.[80]

6. Internet der Dinge

Während die soziale Vernetzung der Menschen bereits fortgeschritten ist, beginnt unter dem Begriff „Internet der Dinge“ auch eine zunehmende Vernetzung von Gegenständen und damit eine Vernetzung und Verdatung

---

74 *Bruns*, Blogs, Wikipedia, Second Life, and Beyond, 2008, S. 21 f.; *Erd*, NVwZ 2011, S. 19; *Fuchs u.a.*, Introduction, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 1 (3) f.; *Lützeler/Bissels*, ArbRAktuell 2011, S. 499; *Piltz*, Soziale Netzwerke im Internet, 2013, S. 1 ff.; *Rosenbaum/Tölle*, MMR 2013, S. 209; *Taeger/Schmidt*, in: *Taeger/Gabel*, BDSG, Einführung, Rn. 2; die Nutzer welche in sozialen Netzwerken zugleich Produzenten und Konsumenten von Informationen sind, werden als "Prosumer" bezeichnet, *Toffler*, Die dritte Welle, 1980, S. 272 ff.

75 *Boyd/Ellison*, JCMC 2007, Vol. 13, Nr. 1, p. 210; *Oberwetter*, NJW 2011, S. 417, ausführlich zur Ausgestaltung und Funktion sozialer Netzwerke, *Piltz*, Soziale Netzwerke im Internet, 2013, S. 19 ff.

76 *Erd*, NVwZ 2011, S. 19 (19 f.); *Fuchs*, Critique of the Political Economy of Web 2.0 Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 31 (pasimo); *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 117 ff.; *Piltz*, Soziale Netzwerke im Internet, 2013, S. 23 f.; *Schultze-Melling*, ZD 2013, S. 570.

77 Soziale Netzwerke – dritte, erweiterte Studie, BITKOM, http://www.bitkom.org/de/markt_statistik/64018_77778.aspx (12.8.2014).

78 "Facebook Reports Second Quarter 2014 Results", Investor Relations, Facebook, http://investor.fb.com/(12.8.2014); Soziale Netzwerke – dritte, erweiterte Studie, BITKOM, http://www.bitkom.org/de/markt_statistik/64018_77778.aspx (12.8.2014).

79 *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 117 f.

80 A Focus on Efficiency, 2014, https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-ash3/851560_196423357203561_929747697_n.pdf (7.1.2014), S. 33; täglich werden mehr Bilder hergestellt, als in den letzten 100 Jahren der Fotografie, *Siegel*, Predictive Analytics, 2013, S. 77.

des physischen Lebensraums von Menschen. Unter dem Begriff „Internet der Dinge“ wird die „Verknüpfung eindeutig identifizierbarer physischer Objekte (engl. ‚Things‘, also ‚Dinge‘) durch deren eindeutige virtuelle Repräsentation in einer Internet-ähnlichen Struktur“ bezeichnet.[81]

Grundlage des „Internets der Dinge“ sind „smarte“, bzw. „intelligente“ Objekte, d.h. Gegenstände, die um Informations- und Kommunikationstechnologien erweitert sind.[82] Die smarten Objekte zeichnen sich insbesondere dadurch aus, dass sie identifiziert, lokalisiert und adressiert werden können, über Sensoren Informationen über ihren eigenen Zustand und den der Umwelt sammeln, dank Effektoren den eigenen Zustand oder die Umwelt beeinflussen können, Benutzerschnittstellen bieten und untereinander sowie mit Menschen kommunizieren können.[83]

Das „Internet der Dinge“ kommt dabei in verschiedenen Teilbereichen des menschlichen Wirkens zum Ausdruck, von denen mit „Smart Homes“,[84] „Industrie 4.0“[85] und „Smart Cars“[86] drei Beispiele genannt werden können.[87] Zusammengefasst zeigen alle smarten Technologien vor allem, dass Computer nicht mehr eigenständige „Computergeräte“ dar-

---

[81] Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, WP 223, 2014, p. 4 f.; *Bräutigam/Klindt*, NJW 2015, S. 1137; *Mattern/Flörkemeier*, Informatik-Spektrum 2010, Vol. 33, Nr. 2, S. 107; *Uckelmann/Harrison/Michahelles*, Architecting the Internet of Things, 2011, S. 2.

[82] *Mattern/Flörkemeier*, Informatik-Spektrum 2010, Vol. 33, Nr. 2, S. 107; *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 122.

[83] *Mattern/Flörkemeier*, Informatik-Spektrum 2010, Vol. 33, Nr. 2, S. 107 (108 f.); Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland, BITKOM, http://www.bitkom.org/de/themen/74736_79154.aspx (11.8.2014).

[84] Gemeint ist die Informatisierung von Wohnräumen und derer Komponenten mit dem Ziel einer erhöhten Wohnqualität, Sicherheit und effizienter Energienutzung auf Grundlage vernetzter und fernsteuerbarer sowie automatisch funktionierender Geräte, vgl. Verband Der Elektrotechnik Elektronik Informationstechnik E.V. (VDE), Die Deutsche Normierungs-Roadmap „Smart Home + Building“, 2013, http://www.dke.de/de/Documents/Deutsche%20Normungs-Roadmap%20Smart%20Home%20+%20Building.pdf (11.8.2014), S. 9; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 53 ff.

[85] *Bräutigam/Klindt*, NJW 2015, S. 1137; *Geis*, ZD 2013, S. 591; die Versionierung "4.0" soll verdeutlichen, dass es sich bei dem "Internet der Dinge", um die vierte industrielle Revolution handelt, nach der Mechanisierung mit Kraft von Wasser- und Dampf (1.), der Elektrifizierung und Massenfertigung (2.), und der Digitalisierung (3.), Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland, BITKOM, http://www.bitkom.org/de/themen/74736_79154.aspx (11.8.2014) f., 17.

[86] *Lüdemann*, ZD 2015, S. 247; *Mattern/Flörkemeier*, Informatik-Spektrum 2010, Vol. 33, Nr. 2, S. 107 (111); *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 58 ff.; *Weichert*, SVR 2014, S. 201.

[87] *Grünwald/Nüßing*, MMR 2015, S. 378 ff.; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 58 ff.

stellen, sondern zu integralen Bestandteilen des menschlichen Lebensumfelds werden.

7. Macht

Im Zusammenhang mit den gesellschaftlichen Aspekten der Informationsgesellschaft wird vor allem der facettenreiche Begriff der Macht relevant. Im Hinblick auf diese Untersuchung soll der Fokus vor allem auf den Zusammenhang zwischen Informationen und Macht gelegt werden, wie er sich in der geläufigen Redewendung „Wissen ist Macht" wiederfindet.[88] Gemeint ist damit, dass die Verfügungsgewalt über Informationen deren Inhaber die Fähigkeit verleiht, künftige soziale oder wirtschaftliche Entwicklungen beeinflussen zu können.[89]

Aus diesem Grund suchen Menschen nach objektiven Mitteln, die es ihnen erlauben, künftige soziale oder wirtschaftliche Entwicklungen einschätzen und beeinflussen zu können.[90] Als solches Machtmittel gewinnen vor allem Informationen an Relevanz. Denn mit der Zunahme der Komplexität der Welt und dem Rückgang unmittelbarer menschlicher Interaktionen als Grundlage des sozialen Lebens wird der Eintritt künftiger Ereignisse von einer Vielzahl von Faktoren beeinflusst, die kaum von einzelnen Personen überblickt werden können.[91]

8. Überwachung und Kontrolle

Der Begriff der Überwachung ist eng mit dem Begriff der Macht verknüpft und wird im Rahmen dieser Untersuchung in seiner soziologischen Ausprägung verwendet, die Überwachung als eine Form sozialer Kontrolle versteht (die Begriffe der Überwachung und der Kontrolle werden daher oft synonym verwendet).[92]

Die Überwachung ist demnach ein gesellschaftliches Konzept und kann dem Wortlaut entsprechend als ein Beobachten von oben und im neutralen Sinne als jede auf persönliche Details gerichtete Aufmerksamkeit zum Zwecke der Einflussnahme, Verwaltung oder Kontrolle verstanden werden.[93] Dabei überprüft eine gesellschaftliche Seite, ob die Istwerte der

---

[88] Das Idiom "Wissen ist Macht" von Francis Bacon hat sich aus der Redewendung "Messen ist Wissen" entwickelt, *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 46.

[89] *Hotter*, Privatsphäre, 2011, S. 89; *Sofsky*, Verteidigung des Privaten, 2007, S. 107.

[90] Vgl. *Luhmann*, Vertrauen, 2000, S. 7.

[91] Vgl. Ebenda, 12.

[92] Umgekehrt Kontrolle als Überwachung definierend, *Ketzer*, Securitas ex Machina, 2005, S. 14; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 9.

[93] *Lyon*, Surveillance Society, 2001, S. 2; *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (257).

überwachten Seite mit den Sollwerten übereinstimmen.[94] Hierdurch gewinnt die überwachende Seite Informationen, die es ihr erlauben, ihr Verhalten anzupassen und auf die überwachten Personen Einfluss zu nehmen, also über sie zu herrschen.[95]

Damit befähigt die Überwachung die überwachende Seite, auf zukünftige Ereignisse Einfluss zu nehmen, und ist somit ein Mittel zur Machtgewinnung. Die Überwachung geht daher über eine reine Wahrnehmung von Personen oder Geschehnissen hinaus. Überwachung erfordert eine gewisse Zielsetzung der Wahrnehmung, d.h. eine Beobachtung oder ein Abhören.[96]

Dabei ist es ausreichend, wenn die Überwachung nur kurzzeitig und stichprobenartig ist.[97] Es ist nicht notwendig, dass die Überwachung wiederholt wird, kontinuierlich erfolgt oder einem übergeordneten Plan folgt.[98] Zum Teil wird bereits jede Art der systematischen Datensammlung als Überwachung betrachtet.[99] Dementsprechend wird nach einer vor allem im englischsprachigen Raum vertretenen Differenzierung der Begriff der „Überwachung“ (engl. Surveillance) als eine Sammlung und Organisation von Informationen verstanden, die zur Beobachtung der Aktivitäten von Menschen eingesetzt wird (engl. Monitoring), um deren Beaufsichtigung in einer bestimmten sozialen Umgebung zu erlauben (engl. Supervision).[100] Die Überwachung im soziologischen Sinn zeichnet sich zudem häufig durch eine asymmetrische Machtverteilung zwischen den Überwachenden und der überwachten Seite aus.[101]

9. Öffentlicher Raum

Die mit Smartglasses einhergehenden rechtlichen Probleme werden vor allem im öffentlichen Raum zu erwarten sein, wo Personen ungewollt in das „Blickfeld“ von Smartglasses geraten können. Der öffentliche Raum

---

94 *Ketzer*, Securitas ex Machina, 2005, S. 15.

95 Ebenda.

96 Ebenda; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270.

97 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 9 f.; a.A. wonach unter unter Überwachung die wiederholte Beobachtung von bestimmten Verhalten zu verstehen ist, *Weber*, How Does Privacy Change in the Age of the Internet, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 273 (274).

98 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 9 f.

99 *Fuchs*, Critique of the Political Economy of Web 2.0 Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 31 (62).

100 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 9.

101 Vgl. *Fuchs*, Ethics and Information Technology 2010, Vol. 12, Nr. 2, S. 171 (174); *Fuchs*, Critique of the Political Economy of Web 2.0 Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 31 (62).

verfügt je nach wissenschaftlicher Disziplin und allgemeinem Verständnis über abweichende Definitionen.[102] Maßgeblich für die vorliegende Untersuchung ist ein Begriffsverständnis, das sich an einer räumlichen Exklusivität des Zugangs als Definitionskriterium orientiert. „Raum" in diesem Sinne soll als physischer Raum verstanden werden (d.h., der virtuelle Cyberspace wird nicht als Raum i.d.S. verstanden).[103] Ferner ist es irrelevant, ob dieser Raum umschlossen oder überdacht ist.[104]

Der Raum gilt als „öffentlich", wenn er nach dem erkennbarem Willen der berechtigten Personen von jedermann betreten werden kann oder der Öffentlichkeit kraft eines Aktes oder gewohnheitsrechtlich gewidmet ist.[105] Das ist typischerweise bei Straßen, Plätzen, Wäldern oder Fußgängerzonen der Fall.[106] Wesentlich ist, dass der Raum durch die Verfügungsberechtigten tatsächlich zur Nutzung eröffnet und damit einem unbestimmten Personenkreis oder einer nach allgemeinen Merkmalen bestimmbaren Personengruppe zugänglich ist.[107] Auf die tatsächliche Zugänglichkeit kann dagegen nicht abgestellt werden, da z.B. eine offenstehende Wohnhaustür nicht bedeutet, dass die sich darin aufhaltenden Personen mit dem Zutritt durch jedermann rechnen müssen.[108]

Zum öffentlichen Raum gehören auch für den Publikumsverkehr geöffnete Bereiche, wie Bahnhöfe, Flughäfen, Tankstellen, Restaurants oder Schwimmhallen.[109] Umgekehrt sind Wohnhäuser typischerweise keine öffentlichen Räume, was auch für die durch die Bewohner gemeinschaftlich genutzten Teile eines Mehrparteiengrundstücks gilt.[110] Dagegen stellen die Eingangsbereiche von Häusern einen jedermann zugänglichen und

---

[102] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 5; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 12.

[103] Wobei auch ein "öffentlicher virtueller Raum" definiert werden könnte, z.B. als Zugangsmöglichkeit zu bestimmten Informationen, wie es z.B. in sozialen Netzwerken der Fall ist, in denen Nutzer geschlossene Freundeskreise pflegen können, vgl. *Piltz*, Soziale Netzwerke im Internet, 2013, S. 194 f.

[104] *Gola/Schomerus*, BDSG, §6 b, Rn. 8; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 23.

[105] *Gola/Schomerus*, BDSG, §6 b Rn. 8; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 14; thematisch am nahesten erscheint die Definition der "öffentlicher Räumlichkeiten" im § 6b Abs. 1 BDSG; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b Rn. 23.

[106] *Scholz*, in: *Simitis*, BDSG, § 6b Rn. 43.

[107] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 5; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 14; *Scholz*, in: *Simitis*, BDSG, § 6b Rn. 42.

[108] *Gola/Schomerus*, BDSG, §6 b, Rn. 8.

[109] OVG Lüneburg, Urt. v. 29.9.2014 (11 LC 114/13), NJW 2015, 502 (505); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 15; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b Rn. 23.

[110] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 15.

damit einen öffentlichen Raum dar.[111] Das gilt auch für die durch jedermann betretbaren Treppenhäuser in gemischt zu Wohn- und Geschäftszwecken genutzten Häusern, in denen sich z.B. Arztpraxen oder Anwaltskanzleien befinden.[112] Oft kommt es dabei auf die tatsächlichen Gegebenheiten, wie Schilder oder Zäune an, aus denen sich ein Betretungsverbot ergibt.[113]

Die Eigentumsverhältnisse, d.h. die Frage, ob der Raum der öffentlichen Hand oder Privatpersonen gehört, sind dagegen für das Vorliegen eines öffentlichen Raums irrelevant.[114]

Ebenso ist das allgemeine Merkmal der „Privatheit" für die Abgrenzung zwischen öffentlichen und nicht öffentlichen Räumen ungeeignet und allenfalls indiziell.[115] So wäre ein abgelegener nicht privater Strand, bei dem nicht mit anderen Personen zu rechnen ist, trotzdem jedermann zugänglich und damit ein öffentlicher Raum. Dagegen könnte sich eine sich dort befindliche Person dort vor der Beobachtung Dritter sicher wähnen, sodass es sich zugleich um eine räumliche Privatsphäre handeln würde.[116] Dasselbe gälte im Fall eines Separés in einem Restaurant.[117]

Zugangsschranken zu räumlichen Bereichen schließen deren öffentlichen Charakter nicht aus, solange sie einer nach allgemeinen Kriterien bestimmten Zahl von Personen den Zugang gewähren.[118] Zwar sind diese Bereiche nur einer bestimmten Zahl von Personen zugänglich, deren Zahl ist jedoch aus der Sicht der Zugangsberechtigten unbestimmt. Das gilt z.B. im Fall einer Altersbeschränkung, vorherigen Anmeldung, Zahlung eines Tickets, um in Veranstaltungshallen, Museen oder einen Check-in-Bereich eines Flughafens zu gelangen.[119] D.h., dass der Zugang zu einem öffentlichen Raum nur im geringen Maße von individuellen

---

[111] Ebenda.

[112] Auch außerhalb der Geschäftszeiten, wenn mit Personenverkehr zu rechnen ist, OVG Lüneburg, Urt. v. 29.9.2014 (11 LC 114/13), NJW 2015, 502 (505); *Gola/Schomerus*, BDSG, §6 b, Rn. 8; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 15.

[113] *Scholz*, in: *Simitis*, BDSG, § 6b Rn. 48; a.A. *Gola/Schomerus*, BDSG, §6 b, Rn. 9.

[114] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 14; vgl. *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b Rn. 23.

[115] So im Ergebnis auch, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 6; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 14.

[116] LG Hamburg, Urt. v. 8.5.1998 (324 O 736/97), ZUM 1998, 852 (859).

[117] Vgl. BVerfG, Urteil v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (368); *Taeger*, ZD 2013, S. 571 (574); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b Rn. 23.

[118] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 14; *Scholz*, in: *Simitis*, BDSG, § 6b Rn. 45.

[119] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 17.

Kriterien abhängt und die zugangsberechtigten Personen nach abstrakt-generellen Kriterien ausgewählt werden.[120]

Zusammenfassend wird ein öffentlicher Raum im Rahmen dieser Arbeit als ein räumlich-physischer Bereich verstanden, zu dem jedermann oder ein nur nach allgemeinen Merkmalen bestimmter Personenkreis Zugang hat.

10. Privatpersonen

Die vorliegende Untersuchung widmet sich der Nutzung von Smartglasses durch natürliche Privatpersonen. Damit sind öffentlich-rechtliche Akteure, juristische Privatpersonen oder Gesellschaften von der Prüfung ausgeschlossen. Auch spezielle Probleme, wie z.B. die Nutzung von Smartglasses in Arbeitsverhältnissen, werden ausgeklammert.[121] Der Nutzer im Sinne diese Untersuchung verwendet Smartglasses folglich für private Zwecke, wie z.B. Sport, Hobbies, Unterhaltung, Kommunikation, Teilnahme am Straßenverkehr oder Eigensicherung, aber nicht für geschäftliche und berufliche Zwecke, z.B. als Mitarbeiter eines Lieferdienstes.

V. Gang der Untersuchung

Die Untersuchung ist durch einen Dreiklang der technischen und gesellschaftlichen Betrachtung sowie deren rechtlicher Würdigung gekennzeichnet. Das Kapitel B. dient dementsprechend der Darstellung technischer Architektur sowie von Funktionen und Einsatzbereichen von Smartglasses. Dabei werden insbesondere die möglichen Einsatzfelder herausgestellt, auf deren Grundlage die schützenswerten Interessen ihrer Nutzer herausgearbeitet werden. Für die Zwecke der Veranschaulichung werden Beispiele konkreter Geräte vorgestellt als auch ein Ausblick in mögliche künftige Entwicklungen gegeben.

Das Kapitel C. wird sich wiederum den gesellschaftlichen Auswirkungen der Smartglasses-Technologie widmen und die Reaktionen von Menschen auf Smartglasses untersuchen.

Im Kapitel D. werden das Konzept der Privatsphäre, dessen Grundlagen sowie seine historische Entwicklung dargestellt, um die Bedeutung der Privatsphäre sowie ihre Beeinträchtigung, aber auch ihre gegenwärtige und künftige Daseinsberechtigung beurteilen zu können.

---

[120] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 6; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 15 ff.

[121] Nichtsdestotroz werden viele der gewonnenen Erkenntnisse auch auf die geschäftliche Nutzung von Smart Glasses übertragbar sein.

Im Kapitel E. wird untersucht, inwieweit die Privatsphäre einen verfassungsrechtlichen Schutz erfahren hat und wie dieser durch den Einsatz von Smartglasses beeinträchtigt wird. Den zentralen Punkt dieses Kapitels wird die Prüfung des Rechts auf informationelle Selbstbestimmung darstellen. Daneben werden Kriterien zur Bestimmung der Eingriffsintensität und der Bedeutung der Interessen an der Nutzung von Smartglasses zum Zweck der Interessenabwägung herausgearbeitet.

Im Kapitel F. werden die widerstreitenden Interessen der Nutzer von Smartglasses und der Betroffenen auf Grundlage des einfachen Rechts untersucht. Dabei werden insbesondere die Ansprüche der Betroffenen sowie deren Möglichkeiten zur sofortigen Abwehr geprüft.

Soweit internationale Rahmenbedingungen für die Untersuchung maßgeblich sind, werden sie jeweils an den einschlägigen Stellen berücksichtigt. Eine Übersicht der internationalen Rahmenbedingungen findet sich ferner im Kapitel G. Sie dient dort vor allem als Grundlage für die Einschätzung, inwieweit die geplante EU-Datenschutzgrundverordnung Einfluss auf die Ergebnisse dieser Untersuchung haben könnte.

Beginnend mit Prognosen für die Zukunft der Smartglasses werden im Kapitel H. vor allem Maßnahmen vorgeschlagen, die eine rechtskonforme Nutzung von Smartglasses im öffentlichen Raum ermöglichen sollen.

Die Untersuchung endet im Kapitel I., welches die eingangs aufgestellten Thesen auf ihre Richtigkeit überprüft sowie die Ergebnisse und Erkenntnisse der Untersuchung zusammenfasst.

B SMARTGLASSES-TECHNOLOGIE

Die Geschichte von Smartglasses reicht in das Jahr 1965 zurück, als der Computerwissenschaftler Ivan Sutherland eine helmartige Vorrichtung mit binokularen Bildschirmen, die direkt vor den Augen des Trägers platziert waren, vorstellte.[122] Die Besonderheit des als „ultimatives Display" angepriesenen Gerätes bestand in der Fähigkeit, computererzeugte Gitternetzgrafiken so auf die beiden Bildschirme zu projizieren, dass der Nutzer sie als Teil der visuellen vernommenen Realität wahrnahm.[123] Doch Sutherlands Erfindung hatte den Nachteil, dass sie wegen ihres Gewichts unter der Decke befestigt wurde, was ihr die Bezeichnung als „The Sword of Damocles" einbrachte.[124] Auch die nachfolgenden Vorläufer von Smartglasses waren technisch limitiert.[125] Erst mit der Miniaturisierung und Mobilität von Computern beschleunigte sich ihre Entwicklung bis zur Gegenwart, in der Smartglasses an der Schwelle zur Massenmarkttauglichkeit stehen.[126]

Aufgrund der gegenwärtig rasanten Entwicklung der Smartglasses-Technologie wird das Augenmerk dieser Untersuchung nicht auf konkrete Modelle gelegt, sondern auf deren generelle Funktionen und Nutzungsmöglichkeiten. Auf ihrer Grundlage werden Smartglasses als Untersuchungsobjekt sowie deren typische Verwendungsmöglichkeiten für die Zwecke der rechtlichen Untersuchung festgelegt. Des Weiteren werden die Vorzüge von Smartglasses vorgestellt, um die Interessen ihrer Nutzer als Abwägungskriterium gegenüber den Privatsphäreninteressen Dritter bestimmen zu können.

---

[122] *Kipper/Rampolla*, Augmented Reality, 2012, S. 8; *Sutherland*, Proceedings of AFIPS 1968, p. 506 (757 ff.).

[123] *Sutherland*, Proceedings of AFIPS 1968, p. 506 (758 ff.); Sutherland, Proceedings of IFIP 1965, Vol.2, 757, 506 ff.

[124] Entwicklung, *Kipper/Rampolla*, Augmented Reality, 2012, S. 8; *Schart/Tschanz*, Augmented Reality, 2015, S. 26.

[125] M.w.N. zur Entwicklung, *Kipper/Rampolla*, Augmented Reality, 2012, S. 8; *Schart/Tschanz*, Augmented Reality, 2015, S. 25 ff.

[126] Mit der technischen Massentauglichkeit von Smartglasses wird innerhalb eines Zeitraums von ca. 10 Jahren gerechnet, Gartner's 2015 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business, Gartner, http://www.gartner.com/newsroom/id/3114217 (18.8.2015); *Kipper/Rampolla*, Augmented Reality, 2012, S. 8; *Mann/Niedzviecki*, Cyborg, 2002, S. 4; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 139; *Preuß*, Augmented Reality, 2014, S. 13.

I. Ubiquitous Computing, Mobile Computing und Wearable Technology

Um die Bedeutung von Smartglasses verstehen zu können, müssen diese vor dem Hintergrund der gegenwärtigen technologischen Strömungen betrachtet werden, die vor allem durch das Konzept des „Ubiquitous Computing" bestimmt werden.[127] Der Begriff „Ubiquitous Computing" wurde durch den Informatiker Mark Weiser geprägt und beschreibt eine Allgegenwart von Rechnern an jedem Ort, zu jeder Zeit, in jeder Situation und jedem Format.[128] Diesem Konzept liegt die Annahme zugrunde, dass die Computertechnologie erst dann ihr volles Potenzial entfalten kann, wenn Menschen ihr nicht mehr mit Argwohn begegnen oder sie hinterfragen.[129] Mit Blick auf bereits dermaßen integrierte Technologien wie Mechanik, Elektronik oder die Schrifttechnik, wird als notwendig erachtet, dass Computer ebenso zu einem nicht wahrnehmbaren Teil der Lebenswirklichkeit von Menschen werden müssen.[130] Das Ziel des „Ubiquitous Computing" ist daher nicht lediglich Computer als separate Geräte mobiler zu machen, sondern sie vielmehr zu integralen Bestandteilen von Geräten, Anwendungen und Funktionen zu machen, ohne dass sie als „Computergeräte" in den Vordergrund treten.[131]

Als Voraussetzung ubiquitärer Computertechnologien werden zum einen das „Mobile Computing", d.h. die ständige und überall vorhandene Computerunterstützung, und das „Pervasive Computing", d.h. eine

---

[127] *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 9 ff.; *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 13; *Weiser*, Scientific American 1991, Vol. 265, Nr. 3, p. 94 (94 ff.).

[128] *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 9 ff.; *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 13; *Weiser*, Scientific American 1991, Vol. 265, Nr. 3, p. 94 (94 ff.).

[129] *Weiser*, Scientific American 1991, Vol. 265, Nr. 3, p. 94 (94 ff.).

[130] Ebenda, 94 ff.

[131] Diese Entwicklung erinnert an das "dritte Clarksche Gesetz" mit dem der Science Fiction Autor Arthur C. Clarke die Integration und Autonomie moderner Technologien beschrieb: "Jede hinreichend fortschrittliche Technologie ist von Magie nicht zu unterscheiden", Arthur C. Clarke zitiert in, *Assmann*, Der Begriff des kulturellen Gedächtnisses, in: *Dreier*, Kulturelles Gedächtnis im 21. Jahrhundert: Tagungsband des internationalen Symposiums, 23. April 2005, Karlsruhe, 2005, S. 21 (39); *Weiser*, Scientific American 1991, Vol. 265, Nr. 3, p. 94; Eric Schmidt, exekutives Vorstandsmitglied von Google, verglich die Entwicklung mit Integration des Kraftfahrzeugen in den Lebensalltag von Menschen und sieht sie für das Internet kommen, *Worstal*, Eric Schmidt's Quite Right The Internet Will Disappear; All Technologies Do As They Mature, Forbes, http://www.forbes.com/sites/timworstall/2015/01/24/eric-schmidts-quite-right-the-internet-will-disappear-all-technologies-do-as-they-mature/(25.1.2015).

durchdringende Datenverarbeitung, bezeichnet.[132] Ferner müssen die Schnittstellen zwischen Menschen und Computern effektiver gestaltet werden und weniger Aufmerksamkeit der Nutzer erfordern.[133] Ebenso sollen die sensorische Erfassung sowie die Verarbeitung von Daten entsprechend dem Nutzungskontext und den Nutzerpräferenzen automatisiert werden.[134] Als technische Voraussetzungen dieser Ziele werden die Miniaturisierung von Computern, ihre Vernetzung sowie Interoperabilität als auch ein Anstieg ihrer algorithmischen Fähigkeiten betrachtet.[135]

Der gegenwärtige technologische Fortschritt folgt dem Prinzip von „Ubiquitous Computing", was sich nicht nur an der Zunahme der algorithmischen Fähigkeiten zur Auswertung von Daten zeigt.[136] Auch die Mobilität von Computergeräten nahm mit Smartphones rasant zu.[137] Diese Entwicklung scheint sich mit dem Aufkommen von „Wearable Technologies", d.h. am Körper getragenen Technologien in Form von Kleidungsstücken oder Accessoires wie Smartwatches (sog. „Wearables"), noch weiter zu beschleunigen.[138] Auch Smartglasses gehören zu der Kategorie der Wearables und fügen sich nahtlos in das Konzept einer allgegenwärtigen Computertechnologie ein, indem sie dank ihrer kompakten

---

[132] Fabian/Hansen in: *Fabian*, TAUCIS - Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, ULD und Institut für Wirtschaftsinformatik der HU Berlin, 75, ULD und Institut für Wirtschaftsinformatik der HU Berlin, 2006, S. 12 ff.

[133] Fabian/Hansen in: Ebenda.

[134] Fabian/Hansen in: Ebenda.

[135] Fabian/Hansen in: Ebenda; *Weiser*, Scientific American 1991, Vol. 265, Nr. 3, p. 94 (105 ff.).

[136] Vgl. A IV. 3, S. 10.

[137] Faszination Mobile Verbreitung, Nutzungsmuster und Trends, Bundesverband Digitale Wirtschaft, 2014, http://www.bvdw.org/mybvdw/media/view?media=5727 (zuletzt abgerufen am: 7.1.2014); *Bliem*, Wearable Computing, 2007, S. 47; *Berg*, Smartphones und Tablets, 2013, S. 2; Infografik, Spiegel Online, http://www.spiegel.de/netzwelt/web/infografik-mobile-nutzung-von-nachrichten-angeboten-in-europa-a-823293.html (5.10.2013); *Hansen*, DuD 2015, S. 435; *Mattern/Flörkemeier*, Informatik-Spektrum 2010, Vol. 33, Nr. 2, S. 107; *Weichert*, SVR 2014, S. 201; *Schart/Tschanz*, Augmented Reality, 2015, S. 59.

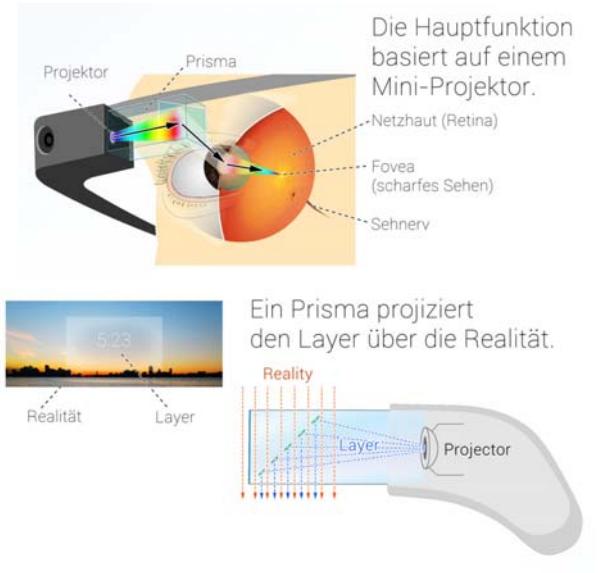
[138] Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, WP 223, 2014, p. 4; *Mann/Niedzviecki*, Cyborg, 2002, S. 3 ff.; m.w.N. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 40 ff. ; *Miller*, Project Glass and the epic history of wearable computers, The Verge, http://www.theverge.com/2012/6/26/2986317/google-project-glass-wearable-computers-disappoint-me (8.7.2013); *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 68 ff.; *Schart/Tschanz*, Augmented Reality, 2015, S. 110; *Thompson*, Googling Yourself Takes on a Whole New Meaning, The New York Times, http://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html (7.9.2013).

Bauweise dazu bestimmt sind, ihre Träger permanent zu begleiten und als effektive Schnittstellen zwischen Menschen und Computern zu dienen.[139]

II. Definition von Smartglasses als Untersuchungsgegenstand

Sowohl der Begriff „Smartglasses“ als auch sein deutsches Pendant „Datenbrillen“ sind nicht genau definiert und werden zu Marketingzwecken auch für Brillen verwendet, die lediglich über eine Videoaufnahmefunktion verfügen.[140] Es ist daher erforderlich, die technischen Eigenschaften von Smartglasses, wie sie im Rahmen der vorliegenden Untersuchung verstanden werden, festzulegen.

1. Technisch vorausgesetzte Eigenschaften



Die Grafik zeigt die Funktionsweise des durchsichtigen Displays bei Google Glass, auf dem mittels einer semipermeablen Spiegeltechnik die Informationen ausgegeben werden und zusammen mit dem Abbild der physischen Welt im Auge des Trägers eintreffen (Bild: „Google Glass Querschnitt“ von Martin Missfeldt, http://brille-kaufen.de/google-brille/, CC-BY http://creativecommons.org/licenses/by/4.0/).

Die grundlegende technische Voraussetzung für Smartglasses ist die Fähigkeit, das Blickfeld ihrer Träger um virtuelle Informationen erweitern zu können. Dies geschieht bei den meisten heutigen Geräten mittels eines durchsichtigen Displays, das vor den Augen der Betrachter auf einem brillenähnlichen Gestell platziert wird. Die Trage- und Darstellungsvor-

---

[139] *Hansen*, DuD 2015, S. 435 (437); *Krombholz u.a.*, Ok Glass, Leave Me Alone, in: *Brenner u.a.*, Financial Cryptography and Data Security, 2015, S. 247 (247); *Schwenke*, DuD 2015, S. 161.

[140] *Feldman*, Epiphany Eyewear, L.A. Weekly, http://www.laweekly.com/news/epiphany-eyewear-like-google-glass-but-maybe-even-better-4440837 (7.9.2015).

richtung wird als Einheit mit dem Begriff „Optical Head Mounted See-Through-Display“ umschrieben (Abb. 1).[141] Noch im experimentellen Stadium befinden sich Geräte, die Informationen statt auf ein Display mittels Laserstrahlen direkt auf die Retina projizieren.[142] Viel weiter am Anfang der Entwicklung befinden sich Kontaktlinsen, in denen die Informationsausgabe mithilfe von LEDs direkt auf die Kontaktlinse oder auf die Netzhaut projiziert werden soll (dabei müsste entsprechend der gängigen Nomenklatur von „Smartlenses“ gesprochen werden).[143] Ebenfalls weit in die Zukunft reicht die Vorstellung von „bionischen Augen“, bei denen elektronische Implantate im Auge Informationen direkt an das Nervensystem übermitteln sollen.[144] Jedoch werden bereits heute im medizinischen Bereich sub-retinale Implantate getestet, um beschädigte Sehnerven ersetzen zu können.[145]

Ferner verfügen Smartglasses im Sinne dieser Untersuchung über eine zur Aufnahme von Fotografien und Videos fähige Kamera, die durch ein Mikrofon unterstützt wird. Weitere Sensoren, wie z.B. Trägheitssensorgen oder Standortbestimmung, werden nicht vorausgesetzt, können jedoch hinzukommen.[146] Ebenso kann die Kamera optional über spezielle Qualitäten, wie z.B. Thermalsicht, verfügen.[147]

---

[141] *Broll*, Augmentierte Realität, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 241 (271); *Klein*, Visual Tracking for Augmented Reality, 2009, S. 76; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 45; *Tonnis*, Augmented Reality, 2010, S. 21 f.

[142] *Broll*, Augmentierte Realität, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 241 (275); *Mann/Niedzviecki*, Cyborg, 2002, S. 9.

[143] *Parviz*, Augmented Reality in a Contact Lens, IEEE Spectrum, http://spectrum.ieee.org/biomedical/bionics/augmented-reality-in-a-contact-lens/0 (4.3.2015); Technik geht ins Auge: Der Trend zur elektronischen Kontaktlinse | heise online, http://www.heise.de/newsticker/meldung/Technik-geht-ins-Auge-Der-Trend-zur-elektronischen-Kontaktlinse-2098418.html (29.1.2014); *Schart/Tschanz*, Augmented Reality, 2015, S. 50; die Erfassung kann mit einer Kamera erfolgen, die ebenfalls direkt auf der Kontaktlinse integriert werden kann, *Kipper/Rampolla*, Augmented Reality, 2012, S. 137 f.; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 45; das Unternehmen Google hat eine entsprechende Kameravorrichtung auf einer Kontaktlinse in den USA patentiert, *Donath*, Wearables: Google patentiert Kontaktlinsen mit Kamera, Zeit Online, http://www.zeit.de/digital/mobil/2014-04/google-kontaktlinse-kamera-patent (16.4.2014).

[144] *Kipper/Rampolla*, Augmented Reality, 2012, S. 138 f.

[145] *Palanker u.a.*, Journal of Neural Engineering 2005, Vol. 2, Nr. 1, p. 105; *Young*, Zweite künstliche Netzhaut erhält Zulassung, Technology Review, http://www.heise.de/tr/artikel/Zweite-kuenstliche-Netzhaut-erhaelt-Zulassung-1920781.html (12.8.2014).

[146] *Schart/Tschanz*, Augmented Reality, 2015, S. 42 ff.

[147] Vgl. *Giger*, Street View mit Infrarotkamera, 2012, passim; *Maerian*, Smart glasses let nurses see veins through skin, Computerworld, http://www.computerworld.com/article/2486116/emerging-technology/smart-glasses-let-nurses-see-veins-through-skin.html (24.9.2015).

Notwendig ist dagegen, dass Smartphones Sende- oder Empfangseinrichtungen darstellen, damit die Daten ohne Verbindungsleitungen zu anderen Geräten übertragen werden können.[148] Dies kann z.B. mittels WLAN, Mobilfunk oder Nahfeldtechnologien erfolgen. Jedoch ist es ausreichend, wenn Smartglasses sich dazu mit einem Smartphone verbinden müssen, um dessen Sende- und Empfangstechnik zu nutzen.[149] Ferner zeichnen sich Smartglasses durch eine Computereinheit aus, die jedoch bereits für die Darstellung von Informationen im Blickfeld der Nutzer notwendig sein wird.

Durch die vorgenommenen technischen Einschränkungen scheiden Geräte mit undurchsichtigen Displays, welche lediglich der Informationsausgabe dienen, als Untersuchungsobjekte aus. Hierzu gehören insbesondere Videobrillen, mit denen z.B. Filme geschaut werden können, oder Virtual-Reality-Brillen, in denen computererzeugte Inhalte, wie z.B. Computerspiele, ablaufen.[150] Ebenfalls sind reine Kamera-Brillen ausgeschlossen, die über keine Bildschirme verfügen, sondern lediglich dazu bestimmt sind, Fotografien oder Videos aus der Augenperspektive aufzunehmen.[151]

---

[148] Definition entsprechend der "Sendeanlage" im § 90 TKG, auf Grundlage der historischen Definition im § 3 Nr. 4 TKG-1996, welche weiterhin ihre Geltung behalten hat, vgl. *Kalf/Papsthart*, in: *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, § 65 TKG, Rn. 4.

[149] Vgl. *Kastrenakes*, Google launches MyGlass app for iPhone, The Verge, http://www.theverge.com/2013/12/19/5228814/myglass-iphone-app-launches-google-glass-ios-companion (2.7.2015); *Nelson*, Epson Moverio BT-200 Augmented Reality Glasses Review, Tom's Hardware, http://www.tomshardware.com/reviews/epson-moverio-bt-200-augmented-reality-glasses,3923.html (8.9.2015).

[150] Z.B. die Virtual Reality-Brillen "Oculus Rift" oder "Samsung VR", *Kremp*, Samsung Gear VR im Test, Spiegel Online, http://www.spiegel.de/netzwelt/gadgets/samsung-gear-vr-im-test-mit-der-datenbrille-in-eine-virtuelle-welt-a-1013463.html (7.2.2015); *Müller-Jung*, Virtuelle Realität - ein Selbstversuch Die Maske, die die Welt bedeutet, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/feuilleton/oculus-rift-verschmelzen-mit-der-virtuellen-welt-13096319.html (14.8.2014); *Broll*, Augmentierte Realität, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 241 (271); *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 45; *Runde*, Head Mounted Displays & Datenbrillen, Virtual Dimension Center (VDC) Fellbach, 2014, http://www.vdc-fellbach.de/files/Whitepaper/2014_VDC-Whitepaper_Head_Mounted_Displays_&_Datenbrillen.pdf (22.12.2014), S. 3; zu beachten ist jedoch, dass die Grenzen zwischen den Geräten fließend sind, so dass eine als Virtual-Reality-Brille bezeichnete Datenbrille über eine Kamera verfügen kann, die Objekte der Außenwelt, wie z.B. Personen in die virtuelle Welt einbindet (sog. "Augmented Virtuality"), auch wenn von Geräten, die darauf ausgelegt sind Menschen in eine virtuelle Welt einzuschließen, kaum höhere Beeinträchtigungseffekte zu erwarten sind als von Smartphones, vgl. 3D-Hand-Scanner für Oculus Rift und Smartphones, heise online, http://www.heise.de/newsticker/meldung/3D-Hand-Scanner-fuer-Oculus-Rift-und-Smartphones-2301259.html (13.1.2015); *Milgram u.a.*, SPIE 1994, Vol. 2351, p. 282 (283).

[151] *Feldman*, Epiphany Eyewear, L.A. Weekly, http://www.laweekly.com/news/epiphany-eyewear-like-google-glass-but-maybe-even-better-4440837 (7.9.2015).

2. Beispiele für Smartglasses

Die nachfolgend vorgestellten Geräte dienen als Beispiele für die vorstehend definierten Smartglasses. Auf detaillierte technische Daten wird dabei weitestgehend verzichtet, da die Technologie sich rasant entwickelt und diese Angaben nur einen geringen Aussagewert hätten.

a) Google Glass

Googles „Glass" (Bild: Ausschnitt aus „Google Glass auf dem Kopf eines Models" von Tim Reckmann, Wikimedia, CC-BY-SA creativecommons.org/licenses/by-sa/3.0/).

Die von Google im Rahmen einer Testphase in den Jahren 2012 bis Anfang 2015 verkauften Smartglasses mit der Bezeichnung „Glass",[152] zeichnen sich durch ein leicht versetzt über dem rechten Auge platziertes durchsichtiges und quaderförmiges Display, das der Informationsdarstellung dient, aus (Abb. 1 und 2).[153] Neben dem Display befinden sich eine Fünf-Megapixel-Kamera und ein Mikrofon, während im Seitenbügel die einem Smartphone entsprechende Rechen- und Speichereinheit untergebracht ist. Die mit einer Leistung für wenige Stunden ausgestattete Batte-

[152] Das Gerät wird als "Glass" und nicht als "Glasses" (englische Kurzform für Brille) bezeichnet, da es nur vor einem Auge getragen wird; die ebenfalls gängige Bezeichnung ist "Google Glass"; zum Entwicklungsverlauf, *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015).

[153] *Schart/Tschanz*, Augmented Reality, 2015, S. 48; die Auflösung des farbigen Displays betrug 640x360 Pixel und sollte von der Wahrnehmung her in etwa der Darstellung eines 55 cm TV Gerätes in 2,5m Entfernung entsprechen, Tech specs - Google Glass Help, Google Glass, https://support.google.com/glass/answer/3064128?hl=en&ref_topic=3063354 (19.12.2014).

rie befindet sich an dem Ohrbügel.[154] „Glass“ ist zwar mit WLAN und Bluetooth netzwerkfähig,[155] kann den vollen Funktionsumfang jedoch nur in Verbindung mit einem Smartphone entfalten (z.B. um sich in Mobilfunknetze einzuwählen oder mittels GPS-Signalen den Standort zu bestimmen).[156]

„Glass“ kann mittels Berührung der berührungsempfindlichen Verkleidung des Geräts (sog. „Touchpad“) sowie über Sprachbefehle gesteuert werden, die auch bei sehr leiser Aussprache erkannt wurden.[157] So wurde mit den Worten „Ok Glass“ das Menü aufgerufen und mit den Worten „Take a Picture“ ein Bild aufgenommen.[158] Ferner konnte das Gerät die Augenbewegungen des Nutzers über einen Infrarotsensor erfassen und so Bildaufnahmen durch das Zwinkern eines Auges auslösen.[159] In experimenteller Umgebung wurde auch die Möglichkeit vorgestellt, Aufnahmen mittels EEG-Sensoren durch Gehirnimpulse auszulösen.[160]

„Glass“ verfügt über keine Signallampe für die Kameraaktivität. Diese macht sich nur durch die Aktivierung des Displays bemerkbar, was jedoch

---

[154] Lt. Testern, soll die Batterie im Schnitt nur zwei Stunden, bei einer dauerhaften Aufnahme, nur 40 Minuten aushalten, *Janssen*, Warum Glass (noch) nicht funktioniert, c't, http://www.heise.de/ct/artikel/Warum-Glass-noch-nicht-funktioniert-1897211.html (16.8.2014); Google Glass Explorer Edition, CNET, http://reviews.cnet.com/google-glass/(2.7.2013).

[155] *Schart/Tschanz*, Augmented Reality, 2015, S. 48; *Topolsky*, I used Google Glass, The Verge, http://www.theverge.com/2013/2/22/4013406/i-used-google-glass-its-the-future-with-monthly-updates (7.1.2015).

[156] Vgl. *Kastrenakes*, Google launches MyGlass app for iPhone, The Verge, http://www.theverge.com/2013/12/19/5228814/myglass-iphone-app-launches-google-glass-ios-companion (2.7.2015); *Piltz*, Google Glass und MyGlass App, de lege data, http://www.delegedata.de/2013/04/google-glass-und-myglass-app-der-tiefe-blick-in-unsere-handys/(2.7.2013); *Schart/Tschanz*, Augmented Reality, 2015, S. 48.

[157] *Schart/Tschanz*, Augmented Reality, 2015, S. 49; *Topolsky*, I used Google Glass, The Verge, http://www.theverge.com/2013/2/22/4013406/i-used-google-glass-its-the-future-with-monthly-updates (7.1.2015).

[158] *Schart/Tschanz*, Augmented Reality, 2015, S. 49; vgl. *Solmecke/Kocatepe*, ZD 2014, S. 22.

[159] *Cipriani*, How to use the „Wink“ feature on Google Glass, CNET, http://www.cnet.com/how-to/how-to-use-the-wink-feature-on-google-glass/(10.7.2014); *Perlow*, Google Glass, ZDNet, http://www.zdnet.com/article/google-glass-let-the-evil-commence/(2.7.2013); *Welch*, Latest Google Glass update lets you wink to take photos, adds Hangouts and YouTube uploading, The Verge, http://www.theverge.com/2013/12/17/5221320/google-glass-update-lets-you-wink-to-take-photos (8.6.2014).

[160] *Lee*, Google Glass controlled by brainwave, BBC News, http://www.bbc.com/news/technology-28237582 (10.7.2014).

nur aus der Nähe deutlich erkennbar ist und sich optisch nicht von dessen übriger Nutzung, z.B. zum Lesen von Webseiten, unterscheidet.[161]

Als Betriebssystem von „Glass“ dient Googles Betriebssystem „Android“, sodass wie bei Smartphones zusätzliche Applikationen den Funktionsumfang der Datenbrille erweitern können.[162] Zu diesem gehören insbesondere Navigationsfunktionen, die Möglichkeit der Kommunikation mit Dritten, der Aufruf von Webseiten, die Publikation von Bildern in sozialen Netzwerken oder eine Live-Übertragung des Geschehens im Blickfeld von „Glass“ an Dritte.[163]

b) Epson Moverio BT-200

Epsons „Moverio BT-200“ (Bild: Thomas Schwenke, CC-BY-SA creativecommons.org/licenses/by-sa/3.0/).

Die Datenbrille „Moverio BT-200“ des Herstellers Epson kann bereits im Handel von jedermann erworben werden. Das Gerät verfügt im Unterschied zu Google Glass über zwei Displays, die jeweils vor den beiden

---

[161] *Thompson*, Googling Yourself Takes on a Whole New Meaning, The New York Times, http://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html (7.9.2013).

[162] *Tung*, Google Glass owners can now post to Facebook, Twitter, ZDNet, http://www.zdnet.com/google-glass-owners-can-now-post-to-facebook-twitter-7000015533/ (2.7.2013).

[163] *Preuß*, Augmented Reality, 2014, S. 15; dagegen kann Google Glass aufgrund der geringen Bildschirmauflösung nicht das Smartphone ersetzen, wenn es um komplexere Internetrecherchen oder das Betrachten von Videos geht, *Thompson*, Googling Yourself Takes on a Whole New Meaning, The New York Times, http://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html (7.9.2013); *Zota*, Hangout mit Google Glass, heise online, http://www.heise.de/newsticker/meldung/Hangout-mit-Google-Glass-1884927.html (8.9.2015).

Augen des Trägers platziert sind (Abb. 3).[164] Ein weiterer Unterschied zu Google Glass besteht darin, dass bei „Moverio“ der Prozessor, der Speicher und die Batterie in einer externen kabelverbundenen Einheit stecken, die zugleich ein Touchpad enthält, mit dem das Gerät bedient werden kann. Das Gerät verfügt über WLAN und Bluetooth-Anbindung, mit der es auch mit Smartphones verbunden und auf Onlineinhalte zugreifen kann.[165]

Die Aktivität der im Gestell untergebrachten Kamera mit eher geringer Auflösung von 640x480 Pixeln wird mittels einer kleinen grünen Leuchtdiode signalisiert. Moverio BT-200 wird ebenfalls mit dem Betriebssystem Android von Google betrieben und kann durch zusätzliche Applikationen erweitert werden.[166] Verfügbare Anwendungen bestehen derzeit aus Machbarkeitsbeispielen, wie z.B. virtuellen Wartungsanleitungen für Servicetechniker oder Computerspielen.[167] Weitere Anwendungsbeispiele zeigen den Einsatz von Moverio zur Venenerkennung im medizinischen Bereich, individuelle Einblendung von Untertiteln in Filmen oder als Tourguide mit virtuellen Avataren.[168] Wegen seines klobigen Aufbaus, der Kabelverbindung und der Überlagerung des Sichtfelds mit den Projektionsflächen für die Bildausgabe sind Moverio-Smartglasses weniger für den täglichen Einsatz als für spezielle Anwendungen geeignet.[169]

---

[164] Moverio BT-200: Das kann Epsons Computerbrille - SPIEGEL ONLINE, http://www.spiegel.de/netzwelt/gadgets/moverio-bt-200-das-kann-epsons-computerbrille-a-942149.html (8.1.2014).

[165] Moverio BT-200 Smart Glasses, Epson, http://www.epson.com/cgi-bin/Store/jsp/Product.do?sku=V11H560020 (6.9.2015).

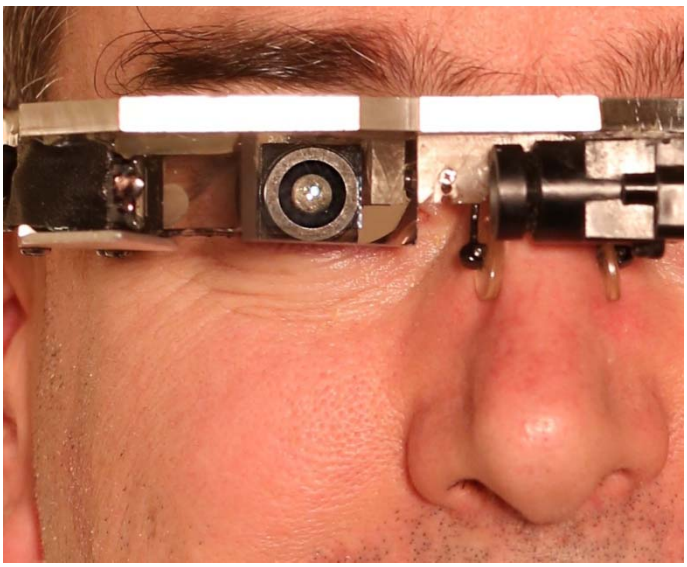
[166] Moverio Developer Program, Epson, http://www.epson.com/cgi-bin/Store/jsp/Landing/moverio_developer-program.do (18.8.2014).

[167] Metaio präsentiert erstmals echte „see-through“ Augmented Reality für Wearables, metaio, http://www.metaio.de/press/press-release/2014/metaio-und-epson-praesentieren-erstmals-echte-see-through-augmented-reality-fuer-wearables-ab-sofort-im-metaio-sdk/(18.8.2014); Augmented Reality SDK for Epson Moverio BT-200, Wikitude, http://www.wikitude.com/products/eyewear/epson-augmented-reality-sdk/(18.8.2014); *Nelson*, Epson Moverio BT-200 Augmented Reality Glasses Review, Tom’s Hardware, http://www.tomshardware.com/reviews/epson-moverio-bt-200-augmented-reality-glasses,3923.html (8.9.2015).

[168] Die Studien beziehen sich auf das Vorgängermodell "Moverio BT-100", Epson’s Moverio Case Studies, Epson, http://www.epson.co.uk/gb/en/viewcon/corporatesite/products/mainunits/overview/12411/casestudies (18.8.2014).

[169] Not quite Google Glass, Engadget, http://www.engadget.com/2014/10/04/epson-moverio-bt-200/(19.12.2014).

c) EyeTap Digital Glass



EyeTap (Bild: Ausschnitt aus „EyeTap wearable computer and Augmediated Reality system“ von Steve Mann, Wikimedia, CC-BY-SA creativecommons.org/licenses/by-sa/3.0/).

Einen Ausblick auf die mögliche Zukunft von Smartglasses zeigt das experimentelle Gerät „EyeTap Digital Glass“ (kurz „EyeTap“) des Smartglasses-Pioniers Steve Mann.[170] Im Unterschied zu Google Glass und Moverio BT-200 ist die Kamera des EyeTap nicht neben, sondern direkt vor dem Auge des Trägers platziert und erfasst die physische Realität damit ohne eine perspektivische Verschiebung.[171] Die visuellen Informationen werden anschließend und nach optionaler Verarbeitung durch die Recheneinheit mithilfe von Laserstrahlen direkt auf die Netzhaut des Trägersprojiziert.[172]

---

[170] *Mann/Niedzviecki*, Cyborg, 2002, S. 9; die vollständige Vermittlung der Wirklichkeit kann auch durch Virtual Reality-Brillen erfolgen, die mit Hilfe einer Kamera die physische Umgebung in die virtuelle Welt einfügen (was als "Augmented Virtuality" bezeichnet wird), jedoch sind die Geräte eher für stationären und nicht den Einstaz im öffentlichen Raum gedacht, 3D-Hand-Scanner für Oculus Rift und Smartphones, heise online, http://www.heise.de/newsticker/meldung/3D-Hand-Scanner-fuer-Oculus-Rift-und-Smartphones-2301259.html (13.1.2015).

[171] *Mann/Niedzviecki*, Cyborg, 2002, S. 9 f.

[172] *Mann*, IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10 (10 ff.); *Mann/Niedzviecki*, Cyborg, 2002, S. 9; mit dem Begriff der "Augmediated Reality" (sinngem. "vermittelte und erweiterte Wirklichkeit") drückt Mann aus, dass die Wirklichkeit durch die Smartglasses vermittelt (engl. "mediated") und dabei durch virtuelle Informationen angereichert (engl. "augmented") wird, *Mann*, IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10.

d) Weitere Smartglasses

Smartglasses können auch für designierte Zwecke, wie z.B. den Einsatz beim Sport[173] oder im Verkehr entwickelt, werden. Z.B. können in Motorradhelmen Armaturenanzeigen, Navigationsinstruktionen als auch mithilfe einer rückseitig platzierten Kamera ein „Rückspiegel" eingeblendet werden. Daneben könnte der Fahrer Fotografien und Videos aufnehmen sowie Standortdaten erfassen.[174] Ähnlich spezifische Funktionen soll z.B. eine im Skifahrerhelm untergebrachte Brille erfüllen, die Pistenhinweise einblenden, einen virtuellen Slalomparcours kreieren, aber auch Aufnahmen und Kommunikation während der Skifahrt ermöglichen kann.[175] Auch der Softwareentwickler Microsoft hat mit „HoloLens" Smartglasses vorgestellt, die als Schnittstelle zu seinem Betriebssystem Windows dienen und mithilfe von Augmented-Reality-Funktionen z.B. die Gestaltung von ausdruckbaren 3D-Gegenständen vereinfachen sollen.[176]

III. Typische Nutzungsarten von Smartglasses

Zusätzlich zu den technischen Eigenschaften sollen der rechtliche Beurteilung von Smartglasses auch deren konkrete Anwendungsmöglichkeiten zugrunde gelegt werden. Zu diesem Zweck werden nachfolgend die typischen Nutzungsarten von Smartglasses in Fallgruppen zusammengefasst.

1. Aufnahme und Speicherung (Augmented Memory)

Im Fall einer Aufnahme werden die audiovisuellen Signale sowie weitere Daten, entsprechend einer regulären Digitalkamera, dauerhaft für die Zwecke einer Reproduktion oder ihrer Verarbeitung gespeichert. Zu den weiteren Daten können z.B. Angaben zur Identität einer Person, der Zeit-

---

[173] *Marker*, Recon Jet, DC Rainmaker, http://www.dcrainmaker.com/2013/08/endurance-sports-display.html (18.8.2014); *Spy*, The smart sunglasses putting sports stars in the shade, http://www.telegraph.co.uk/sponsored/technology/cool-list/10473542/recon-jet-glasses.html (18.8.2014).

[174] *Kim*, 1 Mio. $ in 45 Stunden: Hightech-Motorradhelm Skully bricht IndieGogo-Rekord, Engadget Deutschland, http://de.engadget.com/2014/08/15/1-mio-in-45-stunden-hightech-motorradhelm-skully-bricht-indi/(18.8.2014); *Koesch*, Guardian: Augmented Reality für den Motorradhelm, Engadget Deutschland, http://de.engadget.com/2014/05/30/guardian-augmented-reality-fur-den-motorradhelm-video/(2.6.2014).

[175] *Sturgis*, World's first augmented reality ski goggles up for grabs, Mail Online, http://www.dailymail.co.uk/travel/travel_news/article-2918199/Virtual-reality-SKIING-World-s-augmented-reality-ski-goggles-let-adrenaline-junkies-create-slalom-tracks-follow-video-message-friends-slopes.html (14.2.2015).

[176] Das Gerät scheint jedoch für den heimischen Bereich vorgesehen zu sein, vgl. Windows 10 und «HoloLens», sueddeutsche.de, http://www.sueddeutsche.de/news/wirtschaft/computer-windows-10-und-hololens-microsoft-will-wieder-cool-werden-dpa.urn-newsml-dpa-com-20090101-150122-99-04014 (14.2.2015).

punkt der Aufnahme und Geodaten gehören,[177] die der Lokalisierung der Aufnahme auf einer Stelle der Erdoberfläche dienen.[178] Die Fähigkeit von Smartglasses, die sonst flüchtigen visuellen Informationen schnell und aus dem Blickwinkel der Nutzer festhalten zu können, wird mit dem Begriff der „Augmented Memory", d.h. eines erweiterten Gedächtnisses, umschrieben.[179]

Die Zwecke der Aufnahmen können dabei ebenso vielfältig sein wie bei Fotokameras oder Smartphones. Sie können wie Urlaubsbilder der privaten Erinnerung dienen, aber auch Lebensereignisse permanent in Form von Videos oder in regelmäßigen Zeitabständen ausgelösten Bildaufnahmen festhalten (sog. „Life-Logging" oder „Life-Caching").[180] Ebenso ist es vorstellbar, dass Smartglasses wie mobile Überwachungskameras, z.B. sog. „Dashcams" in Kraftfahrzeugen[181] oder „Bodycams" auf den Schultern von Polizisten,[182] der Steigerung des persönlichen Sicherheitsgefühls

---

[177] Jeder dritte Smartphone-Nutzer teilt seinen Standort mit, BITKOM, http://www.bitkom.org/de/presse/78284_77163.aspx (6.3.2015); *Scellato u.a.*, Proceedings of the 3rd Wonference on Online Social Networks 2010, p. 8.

[178] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 67; Geodaten (bzw. "Standortangaben") dienen der Bestimmung des Entstehungsorts einer Aufnahme auf der Erdoberfläche und können mit Hilfe von satellitengestützten Ortsbestimmungs-Sensoren (am weitesten ist das Ortsbestimmungsangebot "Global Positioning Service" (GPS) verbreitet), Funknetzen oder WLAN-Signalen, erzeugt werden, *Weichert*, DuD 2007, S. 17 (17 f.)

[179] Aufnahmen dieser Art sind jedoch nicht völlig objektiv, sondern durch den Träger der Smartglasses, insbesondere durch die Entscheidung eine Aufnahme auszulösen oder die Wahl der Blickrichtung, subjektiv geprägt, vgl. *Mann/Niedzviecki*, Cyborg, 2002, S. 24 ff.; aus diesem Grund wird im Unterschied zu einer objektiven maschinellen Erinnerung (einer "Computer Memory") von einer durch Computer erweiterten menschlichen Erinnerung (einer "Augmented Memory") gesprochen, *Pedersen*, Ready to Wear, 2013, S. 101 f.

[180] *Schofield*, How to save your life, the Guardian, http://www.theguardian.com/technology/2004/aug/19/onlinesupplement.blogging (12.1.2015).

[181] AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; *Balzer/Nugel*, NJW 2014, S. 1622; *Knyrim/Trieb*, ZD 2014, S. 547; *Lachenmann/Schwiering*, NZV 2014, S. 291.

[182] Mini-Kamera soll Polizei schützen: „Body-Cam-Projekt" wird auf Offenbach ausgeweitet, OP-Online, http://www.op-online.de/lokales/nachrichten/offenbach/mini-kamera-soll-polizei-schuetzen-offenbach-3515776.html (5.7.2014); Bodycams für Hamburgs Polizisten - Innenbehörde Hamburg - FHH, hamburg.de, http://www.hamburg.de/press-archiv-fhh/4366188/2014-09-02-bis-pm-bodycam/(2.10.2014); Innenminister Boris Rhein : „Body-Cam" verhindert Gewalt gegen Polizeibeamte, Hessisches Ministerium des Innern und für Sport, https://innen.hessen.de/presse/pressemitteilung/innenminister-boris-rhein-body-cam-verhindert-gewalt-gegen-polizeibeamte (5.7.2014); *Stoklas*, Datenschutzrechtliche Hürden beim Einsatz von Schulterkameras durch private Sicherheitsdienste, ZD-Aktuell, 2014, Nr. 04388.

und Bekämpfung der Kriminalitätsfurcht dienen können.[183] Dabei soll die Möglichkeit, aufgenommen zu werden, potenzielle Täter wegen des erhöhten Risikos nachträglicher Überführung abschrecken.[184] Neben den präventiven Zwecken können die Aufnahmen generell als Bildbeweise und der Durchsetzung von Ansprüchen jeglicher Art dienen.[185]

2. Übermittlung und Veröffentlichung von Aufnahmen

Die Übermittlung von Aufnahmen muss nicht zwangsläufig präventiven oder repressiven Zwecken dienen. Ähnlich wie bei Smartphones[186] ist damit zu rechnen, dass auch Nutzer von Smartglasses Aufnahmen im großen Umfang an Dritte, z.B. Familie, Freunde und sonstige Kontakte übermitteln oder sie in sozialen Netzwerken veröffentlichen werden.[187]

3. Live-Streaming

Beim Live-Streaming wird das durch die Kamera der Smartglasses erfasste Geschehen direkt an eine beliebige Zahl von Empfängern audiovisuell

---

[183] Die Kriminalitätsfurcht ist als die Manifestation von Angstzuständen zu verstehen und kann sich z.B. darin bemerkbar machen kann, dass bestimmte Orte gemieden werden, *Schwind*, Kriminologie, 2011, § 20 Rn. 12.

[184] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 72 ff.; vorstellbar ist z.B. auch die Aufzeichnung von Polizeiübergriffen bei einer Demonstrationen, *Mann/Niedzviecki*, Cyborg, 2002, S. 178.

[185] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 73.

[186] Alle Smartphone-Nutzer machen Fotos, BITKOM, http://www.bitkom.org/de/presse/8477_79882.aspx (11.8.2014); Faszination Mobile Verbreitung, Nutzungsmuster und Trends, Bundesverband Digitale Wirtschaft, 2014, http://www.bvdw.org/mybvdw/media/view?media=5727 (zuletzt abgerufen am: 7.1.2014); Smartphones werden zur Urlaubskamera, BITKOM, http://www.bitkom-research.de/epages/63742557.sf/de_DE/?ObjectPath=/Shops/63742557/Categories/Presse/Pressearchiv_2013/Smartphones_werden_zur_Urlaubskamera (7.1.2014); das Hochladen der Bilder und Videos gehört bei 58 Prozent der Nutzer zu den meistgenutzten Funktionen sozialer Netzwerke, Soziale Netzwerke – dritte, erweiterte Studie, BITKOM, http://www.bitkom.org/de/markt_statistik/64018_77778.aspx (12.8.2014).

[187] Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 1; vgl. *Tung*, Google Glass owners can now post to Facebook, Twitter, ZDNet, http://www.zdnet.com/google-glass-owners-can-now-post-to-facebook-twitter-7000015533/(2.7.2013).

übertragen.[188] Audio- und/oder Videodaten werden dabei nicht dauerhaft aufgezeichnet, sondern in Echtzeit über die Infrastrukturen Dritter wie Telekommunikationsnetzen bzw. Onlineplattformen an den externen Beobachter übertragen. Dabei kann die Übertragung zu Zwecken der Gleichmäßigkeit der Übertragung zwischengespeichert (sog. „Caching“) werden.[189] Diese Art der Echtzeitübertragung wird als „Live-Streaming“ bezeichnet.[190]

Die Live-Übertragung kann z.B. zu Kommunikationszwecken eingesetzt werden, wenn Nutzer von Smartglasses das Geschehen aus ihrem Blickwinkel mit anderen Personen teilen möchten. Dabei kann es sich um profane Tagesaufgaben handeln, z.B. wenn ein Lebenspartner beim Einkauf den daheimgebliebenen Partner an der Auswahl der Produkte teilhaben lässt.[191] Daneben kann die Öffentlichkeit ähnlich wie bei einer „Webcam“ oder den „Big Brother“-TV-Shows an dem Leben des Trägers von Smartglasses teilnehmen, mit dem Unterschied, dass sie das Geschehen aus dessen Blickwinkel erlebt.[192] Ebenso vorstellbar ist der Einsatz des Live-Streamings zu Präventions- und Nachweiszwecken vorstellbar, wenn Beobachter als Zeugen des Geschehens dienen oder das subjektive Gefühl eines virtuellen Begleiters vermitteln sollen.

4. Biometrische Verfahren

Der Begriff „Biometrie“ bezeichnet die Vermessung des Körpers von Lebewesen und wird primär für Verfahren angewendet, die körperliche Charakteristika zur Identifikation, Verifikation oder Kategorisierung von

---

[188] Dienste wie z.B. Googles "Hangouts on Air" oder "Periscope", erlauben es jedermann kostenlos und ohne wesentliche technische Hürden Live-Übertragungen anzubieten, wie sie zuvor nur Massenmedien vorbehalten waren, *Breithut*, Meerkat versus Periscope, Spiegel Online, http://www.spiegel.de/netzwelt/apps/meerkat-versus-periscope-livestreaming-apps-im-vergleich-a-1025738.html (2.7.2015); *Kwok*, Periscope und Meerkat sind eine Gefahr für unsere Privatsphäre, AndroidPIT, https://www.androidpit.de/ periscope-meerkat-gefahr-fuer-die-privatsphaere (2.7.2015); *Schleeh/Sohn*, Live Streaming mit Hangout On Air, 2014, S. 2 ff.; *Zota*, Hangout mit Google Glass, heise online, http://www.heise.de/newsticker/meldung/Hangout-mit-Google-Glass-1884927.html (8.9.2015).

[189] Das als "Caching" bezeichnete flüchtige Zwischenspeichern ist z.B. im § 44a UrhG geregelt, *Dreier/Schulze*, UrhG, § 44a, Rn. 1.

[190] *Hilgert/Hilgert*, MMR 2014, S. 85 (86); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 66; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 134; *Ensthaler*, NJW 2014, S. 1553.

[191] Good camera, great internet but poor speaker, Mail Online, http://www.dailymail.co.uk/news/article-2402934/Google-Glass-users-experience-having-Internet-eyesocket.html (7.9.2015); *Mann/Niedzviecki*, Cyborg, 2002, S. 16.

[192] *Mann/Niedzviecki*, Cyborg, 2002, S. 129 ff.

Menschen verwenden.[193] Biometrische Daten werden selbst als „biologische Eigenschaften, Verhaltensweisen, physiologische Merkmale, körperliche Erkennungsmerkmale, oder reproduzierbare Handlungen" bezeichnet, die messbar und individuell sind, wobei ein Grad an Wahrscheinlichkeit unschädlich ist.[194] Zu biometrischen Daten gehören insbesondere die Physiognomie, die Art des Gangs oder der Klang der Stimme.[195]

Die besondere Qualität biometrischer Daten besteht darin, dass sie als körperliche Merkmale im Regelfall einer Person dauerhaft anhaften und sie so individualisieren oder verifizieren können.[196] Die häufig zur Zugangskontrolle eingesetzte Verifikation dürfte im Fall der Nutzung von Smartglasses eher eine geringere Rolle spielen, da sie lediglich der Feststellung dient, ob eine Person die ist, als die sie sich ausgibt.[197] Viel relevanter ist die Identifikation von Personen, die z.B. der Anzeige ihres Namens oder weiterer Informationen zur Person dient.[198]

Biometrische Verfahren basieren auf dem Einsatz von sog. „biometrischen Templates“ (bzw. kurz „Templates“), in denen bestimmte biometrische Referenzwerte gespeichert werden.[199] Im Fall von Smartglasses ist dabei insbesondere mit dem Einsatz der Gesichtserkennung zu rechnen,

---

[193] Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 2 ff.; *Busch*, DuD 2013, S. 386; *Gola*, NZA 2007, S. 1139 (1140); *Hornung*, DuD 2004, S. 429.

[194] Art. 29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP193, 00720/12/DE, 2012, S. 3 f.

[195] Ebenda, 2 f.; *Spiecker genannt Döhmann*, K&R 2014, S. 549 (551); *Wrede*, ZD 2012, S. 321 (321 f.).

[196] Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP193, 00720/12/DE, 2012, S. 3; Biometrie - Referenzprojekte, BITKOM, http://www.bitkom.org/de/themen/38337_52490.aspx (13.8.2014).

[197] *Gola*, NZA 2007, S. 1139 (1140); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 16 f.; *Störmer*, Blickrichtungsunabhängige Erkennung von Personen in Bild- und Tiefendaten, 2009, S. 8.

[198] Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 3; *Gola*, NZA 2007, S. 1139 (1140); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 17 f.; *Störmer*, Blickrichtungsunabhängige Erkennung von Personen in Bild- und Tiefendaten, 2009, S. 7 f.

[199] Art. 29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP193, 00720/12/DE, 2012, S. 5; *Karg*, HFR 2012, S. 120 (122).

deren Funktionsweise nachfolgend vorgestellt werden soll.[200] Dabei ist zu bedenken, dass die Effizienz der Gesichtserkennungsverfahren vor allem dank des Einsatzes von lernfähigen neuralen Netzwerken immer weiter zunimmt und zum Teil beinahe humane Fähigkeiten erreicht.[201]

a) Biometrische Gesichtserkennung

Um ein biometrisches Template eines Gesichts des Gegenübers zu erstellen, muss zuerst dessen Abbildung durch die Smartglasses (zumindest zwischenzeitig für diesen Zweck) gespeichert werden. Anschließend werden aus der Aufnahme bestimmte Merkmale des Gesichts extrahiert und gespeichert (sog. „Merkmalsextraktion" bzw. „Enrolment").[202] Dies kann auf Grundlage einer Vielzahl technischer Verfahren erfolgen, wie z.B. des „Elastic Bunch Graph Matching", bei dem ein Raster aus Knoten und Kanten auf ein Gesicht gelegt und damit dessen dreidimensionale Topographie erkannt und gespeichert wird.[203] So können auf Grundlage des Templates auch Gesichter erkannt werden, die durch Mimik verzerrt oder in einem ungewöhnlichen Winkel erfasst wurden.[204] Das Verfahren erlaubt es ferner, Gesichter effektiver in Klassen zu unterteilen, z.B. ent-

---

[200] Biometrische Verfahren wurden z.B. für Google Glass entwickelt, NameTag App, http://www.nametag.ws/(8.6.2014); *Hill*, Google Glass Facial Recognition App Draws Senator Franken's Ire, Forbes, http://www.forbes.com/sites/kashmirhill/2014/02/05/google-glass-facial-recognition-app-draws-senator-frankens-ire/(13.8.2014); *Schulz*, App für Gesichtserkennung „Seien Sie kein Fremder!", Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/feuilleton/medien/app-fuer-gesichtserkennung-seien-sie-kein-fremder-12749493.html (13.8.2014).

[201] Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 1; Art. 29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP193, 00720/12/DE, 2012, S. 3; Datenschutz, Die Zeit, http://www.zeit.de/digital/datenschutz/2015-06/facebook-gesichtserkennung-frisur-kleidung (21.7.2015); *Küchemann*, Gesichtserkennungstechnologie Die Überwachungskamera weiß jetzt, wer du bist, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/gesichtserkennung-aufruestung-der-ueberwachung-13662435.html (21.7.2015); Russakovsky u.a., Cornell University, n.n.v. Studienarbeit 2014, 1, 29; *Taigman u.a.*, IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2014, p. 1701 (7).

[202] Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 2; *Busch*, DuD 2013, S. 386; *Hornung*, DuD 2004, S. 429 (430).

[203] *Wiskott u.a.*, Face Recognition by Elastic Bunch Graph Matching, in: *Jain u.a.*, Intelligent Biometric Techniques in Fingerprint and Face Recognition, 1999, S. 355 (356 ff.).

[204] *Wiskott u.a.*, Face Recognition by Elastic Bunch Graph Matching, in: *Jain u.a.*, Intelligent Biometric Techniques in Fingerprint and Face Recognition, 1999, S. 355 (380 ff.).

sprechend dem Geschlecht, dem Alter oder der Ethnie.[205] Aus Aufnahmen von Gesichtern lassen sich zudem weitere Informationen extrahieren, wie z.B. die Stimmung einer Person (z.B. Trauer oder Freude).[206] Ferner kann die Qualität eines biometrischen Templates verbessert werden, indem es auf Grundlage vieler unterschiedlicher Gesichtsaufnahmen erstellt wird.[207]

Biometrische Templates könnten entsprechend dem Begriff der „Augmented Memory" eingesetzt werden, um sich an den Namen der Person, den Anlass des Kennenlernens sowie weitere Angaben wie „freundlich/unfreundlich" zu erinnern. Findet ein erneuter Kontakt mit der zum Template gehörenden Person statt, könnten die Smartglasses sie automatisch erkennen und dem Nutzer die zu ihr gespeicherten Informationen im Blickfeld einblenden.[208]

Ebenso ist es vorstellbar, dass biometrische Templates innerhalb eines sozialen Netzwerks ähnlich wie Profilbilder gespeichert werden. Dadurch könnten Mitglieder sich mithilfe von Smartglasses automatisch im physischen Raum erkennen lassen und so außerhalb des virtuellen Netzwerks

---

[205] Zur "Kategorisierung", S. Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 3; *DeCarlo/Metaxas*, International Journal of Computer Vision 2000, Vol. 38, Nr. 2, p. 99 (Sec. 46).

[206] *Bundesmann*, Microsoft, heise online, http://www.heise.de/newsticker/meldung/Microsoft-Project-Oxford-soll-Emotionen-auf-Gesichtern-erkennen-2918157.html (16.11.2015); Face Detection Technology Tool Now Detects Your Moods Too, Network World, http://www.networkworld.com/article/2220193/microsoft-subnet/face-detection-technology-tool-now-detects-your-moods-too.html (25.7.2014); Facebook investiert Millionen in Face.com, Welt Online, http://www.welt.de/wirtschaft/webwelt/article 106625878/ Facebook-investiert-Millionen-in-Face-com.html (25.7.2014); SHORE™, Fraunhofer Institute for Integrated Circuits IIS, http://www.iis.fraunhofer.de/en/ ff/bsy/tech/bildanalyse/shore-gesichtsdetektion.html (11.1.2015); *Crowley*, How Germany's Google Glass App Can Help Sufferers Of Autism, Computer Business Review, http://www.cbronline.com/news/social/how-germanys-google-glass-app-can-help-autism-sufferers-4356414 (11.1.2015); *Simonite*, When You're Always a Familiar Face, MIT Technology Review, http://www.technologyreview.com/news/424660/when-youre-always-a-famil iar-face/(17.6.2014); ähnliche Technologie existiert im experimentellen Stadium auf für Googles Datenbrille "Glass", *Anthony*, Real-time emotion detection with Google Glass, ExtremeTech, http://www.extremetech.com/extreme/189259-real-time-emotion-detection-with-google-glass-an-awesome-creepy-taste-of-the-future-of-wearable-computers (11.1.2015).

[207] Face Detection Technology Tool Now Detects Your Moods Too, Network World, http://www.networkworld.com/article/2220193/microsoft-subnet/face-detection-technology-tool-now-detects-your-moods-too.html (25.7.2014); *Karg*, HFR 2012, S. 120 (122); *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 41.

[208] Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 2; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 39.

soziale Kontakte herstellen.[209] Genauso wäre es auch möglich, z.B. eine Template-Datenbank auf Grundlage einer Fahndungsliste anzulegen, um sich potenziell gefährliche Personen im Blickfeld anzeigen zu lassen.[210]

b) Stimm- und Verhaltenserkennung

Neben der Gesichtserkennung kann insbesondere auch die Stimme von Menschen erkannt werden. Die Stimmerkennung ist für Smartglasses, die ohne Hände bedient werden sollen, essentiell.[211] Jedoch basieren die bisher genutzten Stimmerkennungsfunktionen vor allem auf der Erkennung des Inhalts des Gesprochenen, wobei die Feststellung der Identität von Personen zwar möglich ist, bisher jedoch aufgrund der Variabilität der Stimme, der Hintergrundgeräusche und mangels Referenzwerten nur von untergeordneter Bedeutung war.[212] Ferner können Personen aufgrund sonstiger körperlicher Merkmale und Verhaltensmuster, wie der Art zu gehen,[213] erkannt werden.[214] Des Weiteren können die biometrischen Daten miteinander verschnitten werden und so ein sich durch äußere Informationen verdichtendes Profil einer Person ergeben, das einen Rückschluss auf diese alleine aufgrund äußerer Umstände erlaubt.[215]

5. Augmented Reality

Während die bisher behandelten Nutzungen von Datenbrillen lediglich eine graduelle Verbesserung bisheriger Geräte, wie Smartphones oder Überwachungskameras, darstellen, könnte vor allem die Umsetzung von

---

[209] NameTag App, http://www.nametag.ws/(8.6.2014); *Hill*, Google Glass Facial Recognition App Draws Senator Franken's Ire, Forbes, http://www.forbes.com/sites/kashmirhill/2014/02/05/google-glass-facial-recognition-app-draws-senator-frankens-ire/ (13.8.2014); *Schulz*, App für Gesichtserkennung „Seien Sie kein Fremder!", Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/feuilleton/medien/app-fuer-gesichtserkennung-seien-sie-kein-fremder-12749493.html (13.8.2014).

[210] Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 2; vgl. *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 39; Dubai detectives to get Google Glass to fight crime, Reuters, http://www.reuters.com/article/2014/10/02/us-emirates-dubai-google-police-idUSKCN0HR0W320141002 (16.2.2015).

[211] Vgl. B II. 2. a), S. 30.

[212] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 65.

[213] *Greenmeier*, Something in the Way You Move, http://www.scientificamerican.com/article.cfm?id=motion-capture-surveillance (31.1.2015); *Hafner/Bachmann*, 8th IEEE-RAS International Conference on Humanoid Robots - Conference Paper 2008, p. 598; *Spiecker genannt Döhmann*, K&R 2014, S. 549 (551).

[214] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 130 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 66 f.; zur Erkennbarkeit nach körperlicher Konstitution vgl. *Röger/Stephan*, NWVBl 2001, S. 243 (243 ff.)

[215] *Spiecker genannt Döhmann*, K&R 2014, S. 549 (551).

visueller Augmented Reality (deutsch „erweiterte Wirklichkeit“) zu einem Alleinstellungsmerkmal von Smartglasses werden.

Der Begriff „Augmented Reality“ umschreibt die Erweiterung der visuellen Wahrnehmung durch virtuelle Objekte.[216] Dabei wird die von Menschen ohne Hilfsmittel visuell wahrgenommene physische Welt mit virtuellen Informationen, die im Display von Smartglasses ausgegeben werden, zu einer einheitlichen Realitätswahrnehmung vermengt.[217]

a) Grundlagen der Täuschung visueller Wahrnehmung

Die Täuschung der visuellen Wahrnehmung mittels Augmented Reality ist auf die Art und Weise menschlicher Sehfähigkeit zurückzuführen.[218] Die visuelle Wahrnehmung beruht auf Lichtreizen, die Nervenimpulse durch fotochemische Prozesse in den Sinneszellen in der Netzhaut des Auges auslösen.[219] Die Nervenimpulse werden wiederum in diversen Gehirnregionen verarbeitet und durchlaufen verschiedene Stadien, bei denen z.B. zwecks Gefahrvermeidung eine Schnellerkennung erfolgt (z.B. auf mögliche Gefahrenelemente, wie Umrisse eines gefährlichen Tieres), bevor eine langsame sequentielle Aufarbeitung der visuellen Reize und Abgleich mit gespeicherten Mustern erfolgt.[220]

Im Ergebnis erfährt der Mensch eine Wahrnehmung der realen Welt, die nicht unmittelbar ist, sondern stark von seinen kognitiven Prozessen abhängt und damit subjektiv ist.[221] Z.B. kann eine Farbfehlsichtigkeit zu einer unterschiedlichen Farbwahrnehmung führen, obwohl die sie vermittelnden Lichtstrahlen physikalisch keinen Unterschied aufweisen.[222] Fer-

---

[216] *Abawi*, Augmented Reality - die angereicherte Realität, 2008, S. 1; *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (356); *Kipper/Rampolla*, Augmented Reality, 2012, S. 1; *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 14; *Schart/Tschanz*, Augmented Reality, 2015, S. 19.

[217] Auch in diesem Bereich gibt es keine einheitlichen Definitionen, sondern verschiedene Umschreibungskonzepte, *Broll*, Augmentierte Realität, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 241 (245); *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 9.

[218] Neben der visuellen Wahrnehmung, die 70% der Sinneszellen eines Menschen ausmacht und mehr als 40% der Großhirnrinde in Anspruch nimmt, sind weitere Sinne das Hören, Riechen, Schmecken, Erfühlen/Tasten, Gleichgewicht, Körperempfindung, Temperaturgefühl und Schmerzempfindung, *Dörner u.a.*, Einleitung, in: *Dörner u.a.*, Virtual und Augmented Reality, 2013, S. 1 (4).

[219] Ebenda, 2; *Kipper/Rampolla*, Augmented Reality, 2012, S. 30.

[220] *Dörner u.a.*, Einleitung, in: *Dörner u.a.*, Virtual und Augmented Reality, 2013, S. 1 (2).

[221] *Schart/Tschanz*, Augmented Reality, 2015, S. 2.

[222] Ebenda, 62.

ner ist das visuelle Wahrnehmungssystem adaptionsfähig. So hat der Psychologe George M. Stratton Ende des 19. Jahrhunderts eine „Umkehrbrille" getragen, die seine visuelle Wahrnehmung um 180 Grad auf den Kopf stellte.[223] Mit der Zeit gewöhnte sich sein kognitives System an diese Sichtweise und er musste sich erneut anpassen, als er die Umkehrbrille absetzte.[224] Von ähnlichen Erfahrungen berichtet der Forscher Steve Mann, nach dessen Ansicht eine durch Smartglasses vermittelte Realität kognitiv adaptiert wird und nach Abnahme der Datenbrille die unmittelbare Realitätswahrnehmung „unrichtig" wirkt.[225]

Folglich gibt es keinen „festen, eindeutigen und objektivierbaren Zusammenhang zwischen der Realität mit den von ihr auf einen Menschen wirkenden Lichtreizen einerseits und der visuellen Wahrnehmung des Menschen über diese Realität andererseits."[226] Vielmehr lässt diese Art der visuellen Wahrnehmung einen Manipulationsspielraum entstehen, der es erlaubt, die Wahrnehmung der Realität durch den Menschen zu beeinflussen. D.h., wenn künstlich dieselben Reize ausgelöst werden, die von einem realen Objekt ausgehen, wird der Mensch aufgrund dieser Reize annehmen, das reale Objekt zu sehen.[227]

Etwaige Widersprüche aufgrund der Kenntnis, dass die virtuellen Objekte nicht physisch existieren, werden durch das Prinzip der „Willing Suspension of Disbelief" (deutsch „willentliches Ausblenden des Unglaubens") ausgeglichen.[228] Dieser vom Philosophen Samuel T. Coleridge geprägte Begriff umschreibt die Fähigkeit des Menschen, augenscheinliche Widersprüche zwischen Realität und Fiktion auszublenden.[229]

---

[223] *Mann/Niedzviecki*, Cyborg, 2002, S. 199 f.

[224] *Dörner u.a.*, Einleitung, in: *Dörner u.a.*, Virtual und Augmented Reality, 2013, S. 1 (3).

[225] Die von Mann beschriebenen Erfahrungen basieren auf einer Wirklichkeitswahrnehmung, die vollständig durch Smartglasses vermittelt wird und sich besonders stark auswirkt, wenn die Abweichungen zu physischer Realität marginal sind, z.B. das Blickfeld um wenige Grad gedreht wird, *Mann/Niedzviecki*, Cyborg, 2002, S. 209.

[226] *Dörner u.a.*, Einleitung, in: *Dörner u.a.*, Virtual und Augmented Reality, 2013, S. 1 (3); der traditionelle Realitätsbegriff umfasst eine Welt, die in den Dimensionen des dreidimensionalen Raumes und der Zeit existiert, wobei die vielfältigen Konzepte der Physik jedoch zeigen, dass diese Vorstellung keineswegs absolut ist und ganz im Gegenteil Theorien wie die Relativitätstheorie oder Superstring-Theorien davon zeugen, dass die menschliche Realitätswahrnehmung nur ein Ausschnitt eines viel komplexeren Gebildes sein könnte, *Castells*, Das Informationszeitalter, Bd.1, 2001, S. 431.

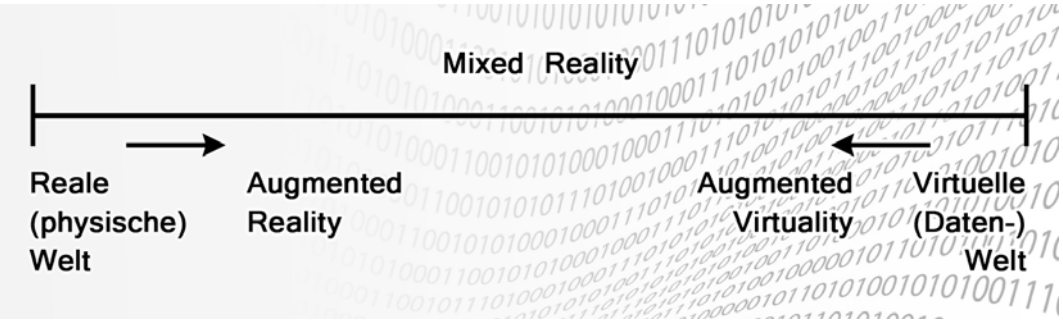
[227] *Dörner u.a.*, Einleitung, in: *Dörner u.a.*, Virtual und Augmented Reality, 2013, S. 1 (3).

[228] Ebenda, 7.

[229] So akzeptieren z.B. Zuschauer eines synchronisierten Films, dass ein englischsprachiger Schauspieler deutsch spricht, ohne sich permanent an diesem Widerspruch zu stören, Ebenda, 8; *Coleridge*, Biographia Literaria, 1965, S. 117.

Zusammengefasst helfen kognitive Wahrnehmungsprozesse, künstlich erzeugte Sinneseindrücke als real zu akzeptieren. Hierdurch eröffnet sich für Menschen ein Illusionsspielraum, der hinter der künstlich gar nicht manipulierten Realitätswahrnehmung beginnt und bis zu einer ausschließlich künstlich erzeugten Realität, der sog. Virtual Reality, reicht.[230]

b) Virtual Reality und Mixed Reality



Die Spannweite des „Mixed Reality"-Kontinuums zwischen physischer und virtueller Welt beinhaltet eine physische Welt, die durch virtuelle Objekte erweitert ist („Augmented Reality"), und eine virtuelle Welt, in welche physische Objekte inkorporiert werden („Augmented Virtuality", wobei dieser Begriff eher selten verwendet wird).[231]

„Virtual Reality" (deutsch „virtuelle Wirklichkeit") steht für die Wirklichkeitswahrnehmung in einer Umgebung, die gänzlich vom Computer in Echtzeit generiert wird.[232] Anders als bei Augmented Reality wird in der Virtual Reality die physische Welt völlig ausgeblendet und vollständig durch eine virtuelle Realität ersetzt.[233]

Dagegen wird in einer Augmented Reality die physische Umgebung nicht ausgeblendet, sondern durch computergenerierte Zusatzobjekte, wie Textanzeigen oder grafische Objekte, angereichert oder überlagert.[234]

---

[230] *Dörner u.a.*, Einleitung, in: *Dörner u.a.*, Virtual und Augmented Reality, 2013, S. 1 (8).

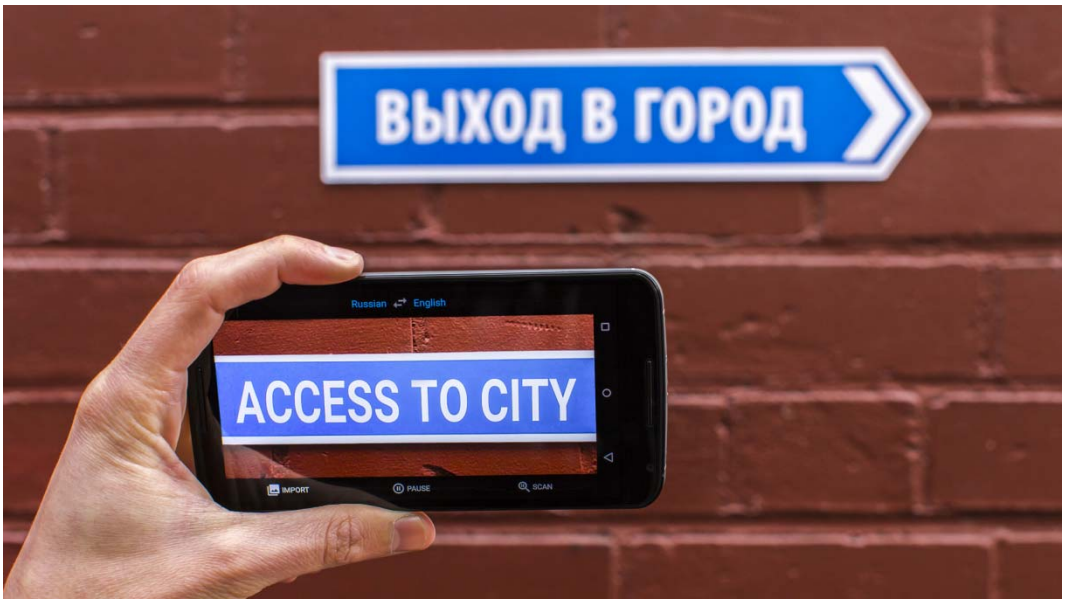
[231] Nach *Milgram u.a.*, SPIE 1994, Vol. 2351, p. 282 (283).

[232] *Kipper/Rampolla*, Augmented Reality, 2012, S. 21 f.; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 46 f.

[233] *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (355 f.); *Klein*, Visual Tracking for Augmented Reality, 2009, S. 1; Zum Begriff der "Immersion", *Milgram u.a.*, SPIE 1994, Vol. 2351, p. 282 (287); *Pratsch*, Auswirkungen einer Aero-Cave Umgebung auf die Orientierung innerhalb einer virtuellen 3D-Umgebung, 2005, S. 16 f.

[234] *Abawi*, Augmented Reality - die angereicherte Realität, 2008, S. 1; *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (356); *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 14; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 39 f.; *Schart/Tschanz*, Augmented Reality, 2015, S. 21 f.

D.h., es wird keine gänzlich neue keine künstliche Welt generiert, sondern die vorhandene, physische Welt wird durch eine virtuelle Realität erweitert.[235] Die Betrachter nehmen dabei die physische und die virtuelle Realität als eine einheitliche Realität wahr (sog. „Mixed Reality", Abb. 5).[236]



Funktionsweise von „Word Lens" mittels eines Smartphones (Bild: Google, Inc.)[237]

Die Funktionsweise von Augmented Reality kann anhand der für Smartphones verfügbaren Applikation „Word Lens" verdeutlicht werden (Abb. 6). „Word Lens" erfasst mithilfe der Smartphone-Kamera fremdsprachige Texte sowie deren Schriftbild.[238] Die Texte werden anschließend übersetzt und auf dem Bildschirm der Geräte über den ursprünglichen Text in dessen Schriftbild platziert. Beim Betrachter entsteht so der Eindruck, dass der Text in der übersetzten Sprache physisch, also „in Wirklichkeit", vorhanden ist.[239]

---

[235] *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (355 f.); *Klein*, Visual Tracking for Augmented Reality, 2009, S. 1; wird die wahrgenommene Realität mehrheitlich durch den Computer kreiert und nur durch einzelne Objekte aus der realen Welt ergänzt, wie z.B. Menschen die in eine virtuelle Umgebung eingefügt werden, spricht man von eine "Augmented Virtuality", *Milgram u.a.*, SPIE 1994, Vol. 2351, p. 282 (283); *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 40.

[236] Zum Begriff "Mixed Reality", S. *Milgram u.a.*, SPIE 1994, Vol. 2351, p. 282 (283).

[237] Ebenda.

[238] "Word Lens" ist z.B. auch für Googles Datenbrille "Glass" verfügbar, *Beiersmann*, Google kauft Entwickler der Übersetzungs-App Word Lens, ZDNet.de, http://www.zdnet.de/88193506/google-kauft-entwickler-der-uebersetzungs-app-word-lens/ (19.12.2014).

[239] *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 80 f.

c) Visuelle Selbstbestimmung durch Mediated Reality

Eine Steigerung von Augmented Reality ist die vollständig durch einen Computer vermittelte und dadurch beliebig manipulierbare Wirklichkeit, die als „Mediated Reality“ bezeichnet wird.[240] D.h., die physische Umgebung wird nur durch Smartglasses unmittelbar visuell erfasst und erst dann an das Auge ausgegeben (vorausgesetzt die Smartglasses übernehmen vollends die visuelle Vermittlung der physischen Welt, s. Abb. 4).[241] Dadurch kann eine höhere Immersionsstufe erreicht werden, die dank visueller Einkapselung dem Menschen ein einheitliches physisch-virtuelles Realitätsgefühl vermittelt.[242] Der Unterschied zwischen Virtual Reality und Mediated Reality besteht darin, dass bei Mediated Reality die Bildausgabe nicht vollends durch den Computer erzeugt, sondern die Wahrnehmung der physischer Welt lediglich bei Bedarf modifiziert wird.

Dank Mediated Reality können Nutzer von Smartglasses nicht nur virtuelle Objekte in physischer Welt platzieren, sondern umgekehrt auch unerwünschte Informationen ausblenden und umgestalten.[243] Z.B. können Nutzer die Welt um sich herum verdunkeln, um sich auf das Lesen eines Textes in der Datenbrille konzentrieren können.[244] Ebenso ist es möglich, den Ton, die Farbe und Kontraste der visuellen Informationen anzupassen oder mithilfe stroboskopischer Filter sich schnell bewegende Objekt optisch zu verlangsamen.[245] Des Weiteren können Werbebotschaften auf Werbetafeln oder in Zeitschriften ausgeblendet werden und Smartglasses die Funktion der aus Internetbrowsern bekannten „AdBlocker“ übernehmen.[246] Ebenso können virtuelle Wände kreiert werden, die dem Träger von Smartglasses ein visuelles Gefühl des Rückzugs, z.B. in einer vollen Wartehalle, verschaffen.[247]

---

[240] *Mann/Niedzviecki*, Cyborg, 2002, S. 32; *Mann*, IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10.

[241] *Mann/Niedzviecki*, Cyborg, 2002, S. 32.

[242] Ebenda.

[243] Vgl. Ebenda, 202 ff.

[244] Ebenda, 203.

[245] Ebenda, 204; Mann beschreibt, dass er mit seiner Datenbrille "EyeTap" z.B. die Schrift auf einem sich drehendem Autoreifen lesen kann, Ebenda, 3.

[246] *Biederbeck*, Die Augmented-Reality-Brille Brand Killer ist der Adblocker für den Alltag, WIRED Germany, https://www.wired.de/collection/latest/die-augmented-reality-brille-brand-killer-ist-der-adblocker-fur-den-alltag (14.2.2015); *Dörner u.a.*, Einleitung, in: *Dörner u.a.*, Virtual und Augmented Reality, 2013, S. 1 (10).

[247] *Mann/Niedzviecki*, Cyborg, 2002, S. 206.

Mediated Reality ist daher als eine Art Filtermechanismus für visuelle Informationen zu verstehen, der Menschen befähigt, die Außenwelt autonom zu interpretieren.[248]

d) Funktionsweise von Augmented Reality in Smartglasses

Augmented-Reality-Anwendungen setzen voraus, dass die reale Umwelt erfasst und um virtuelle Objekte ergänzt wird, bevor sie von den Nutzern wahrgenommen wird. Diese Aufgabe wird durch eine sog. „Tracking Software" oder kurz „Tracker" erfüllt.[249] Die perfekte Illusion für die Nutzer setzt voraus, dass die virtuellen Objekte so zeitnah und räumlich genau wie möglich in dem Abbild der realen Umgebung platziert werden (bezeichnet als deren „Registrierung") und die Registrierung bei dynamischen Umgebungen (z.B. bei einer Kopfbewegung) aufrechterhalten wird.[250]

Während einfaches Tracking mithilfe von im physischen Raum platzierten zweidimensionalen Markern funktioniert (z.B. im Form von graphischen Barcodes),[251] kann das volle Potenzial von Augmented Reality nur dann erreicht werden, wenn die Trackingsoftware den physischen Raum selbst kartieren, also ihr unbekannte Objekte erkennen kann.[252] Ferner funktioniert Augmented Reality desto besser, je mehr Daten über die physische Welt zur Verfügung bereitstehen, da die virtuellen Objekte so qualitativ und quantitativ effektiver in ihr verortet werden können.[253] Dieses Prinzip kann in Anlehnung an das „Ubiquitous Computing" als „Ubiquitous Augmented Reality" bezeichnet werden.[254]

---

[248] Ebenda, 202 f.

[249] *Broll*, Augmentierte Realität, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 241 (252 ff.); *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 27; *Schart/Tschanz*, Augmented Reality, 2015, S. 39; *Tonnis*, Augmented Reality, 2010, S. 40.

[250] *Abawi*, Augmented Reality - die angereicherte Realität, 2008, S. 26 ff.; *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (367 f.); *Broll*, Augmentierte Realität, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 241 (264 ff.); *Kipper/Rampolla*, Augmented Reality, 2012, S. 32 f.; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 27; *Suthau*, See Through Head Mounted Display für die Medizin, 2006, S. 11 f.

[251] Sog. "ID Marker", bzw. "fiducials", *Klein*, Visual Tracking for Augmented Reality, 2009, S. 1 ff.; *Tonnis*, Augmented Reality, 2010, S. 45 ff.

[252] *Klein*, Visual Tracking for Augmented Reality, 2009, S. 27 ff.; Verfahren dieser Art werden z.B. als "Parallel Tracking und Mapping" oder "Simultaneous Localisation and Mapping" bezeichnet; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 37; *Schart/Tschanz*, Augmented Reality, 2015, S. 39 f.

[253] *Schart/Tschanz*, Augmented Reality, 2015, S. 5; *Tonnis*, Augmented Reality, 2010, S. 2.

[254] *MacWilliams*, A Decentralized Adaptive Architecture for Ubiquitous Augmented Reality Systems, 2005, S. 1 ff.; *Tonnis*, Augmented Reality, 2010, S. 162 ff.

Sollen virtuelle Objekte in Abhängigkeit von der Identität einer Person erzeugt werden, kann Augmented Reality mit biometrischer Erkennung verbunden werden. So kann z.B. der Schriftzug mit dem Namen einer Person virtuell an deren physisches Abbild „angeheftet" werden. Bewegt sich die Person im Raum, würde der Schriftzug ihr entsprechend „folgen".[255] Die Technik könnte z.B. eingesetzt werden, um bei einer Veranstaltung Informationen zu anderen Teilnehmern einzublenden oder damit Eltern ihre Kinder inmitten anderer Menschen besser „im Auge behalten" können.

Smartglasses sind für eine Augmented Reality zwar nicht zwingend notwendig, da diese z.B. auch mittels Smartphones erzeugt werden kann (Abb. 6). Jedoch müssen Smartphones vor den Augen der Betrachter in der Hand gehalten werden, was auf Dauer ermüdend und die Präsenz virtueller Objekte zudem auf die Bildschirme der Geräte begrenzt ist. Dadurch wird der Prozess eines „willentlichen Ausblendens des Unglaubens" gestört und die kognitive Verschmelzung der virtuellen mit der physischen Welt erschwert.[256] Dagegen werden virtuelle Objekte mithilfe von Smartglasses permanent im Blickfeld ihrer Nutzer eingeblendet und erleichtern die visuelle Täuschung der visuellen Wahrnehmung.

Je nach Bauweise und Technik können Smartglasses über unterschiedliche Augmented-Reality-Fähigkeiten verfügen. Smartglasses, die nur zweidimensionale Informationen im Blickfeld der Nutzer einblenden, diese jedoch im physischen Raum nicht verorten, sind allenfalls zur „Augmented Reality im weiteren Sinne", also „keiner echten Augmented Reality", fähig.[257] Geräte wie Google Glass, deren Bildschirme nur einen Teilbereich des Blickfeldes einnehmen, haben zumindest ein geringes Potenzial für eine immersive Augmented Reality.[258] Smartglasses wie Moverio

[255] Vgl. *Abawi*, Augmented Reality - die angereicherte Realität, 2008, S. 94 ff.

[256] Vgl. B III. 5. a), S. 43.

[257] Vgl. *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 11.

[258] Zum Begriff der "Immersion" als Umschreibung des "Eintauchens" in eine virtuelle Realität, *Milgram u.a.*, SPIE 1994, Vol. 2351, p. 282 (287); *Pratsch*, Auswirkungen einer Aero-Cave Umgebung auf die Orientierung innerhalb einer virtuellen 3D-Umgebung, 2005, S. 16 f.

BT-200 können dagegen die physische mit der virtuellen Welt effektiv vermengen.[259] Für die höchste Stufe der Augmented Reality, die Mediated Reality, sind dagegen Geräte wie das EyeTap notwendig, bei denen die Kamera direkt vor dem Auge sitzt.[260]

6. Informationsmanagement ohne audiovisuelle Erfassung

Smartglasses können von ihren Nutzern auch nur dazu genutzt werden, um z.B. E-Mails zu lesen, oder gänzlich abgeschaltet sein. D.h., es erfolgen dann keine audiovisuellen Aufnahmen oder sonstige Datenerhebungen. Diese rein auf den Bezug und die Darstellung von Informationen gerichtete Nutzung von Smartglasses wird für deren Anwender bedeutend sein, da die schnelle Informationsvermittlung neben Augmented Reality den wesentlichen Vorteil von Smartglasses darstellt.[261]

Eine solche auf Vermittlung externer Informationen bezogene Nutzung von Smartglasses erscheint im Hinblick auf eine Belastung der Privatsphäre Dritter zuerst als unwesentlich, da mit ihr keine Datenerhebung einhergeht. Jedoch ist es zum einen wahrscheinlich, dass Personen im Erfassungsbereich der Smartglasses nicht wissen werden, ob tatsächlich Aufnahmen erfolgen, sodass sie potenziell von ihnen ausgehen könnten.[262] Folglich ist diese Art des Einsatzes von Smartglasses aufgrund des Anscheins möglicher Aufnahmen, sowohl aus der Sicht ihrer Nutzer, als auch der Betroffenen für diese Untersuchung von großer Relevanz.

IV. Vorteile und Anwendungsmöglichkeiten von Smartglasses

Die vorstehend herausgestellten Nutzungsarten von Smartglasses sollen nachfolgend anhand praktischer Anwendungsmöglichkeiten vorgestellt werden. Dabei wirkt sich neben der schnellen Informationsvermittlung

---

[259] Ein besonderer Vorteil von Smart Glasses bei der nahtlosen "Registrierung" virtueller Objekte liegt in deren Möglichkeit die Pupillen ihrer Träger mit Hilfe eines so genannten "Eye Tracking Devices" zu erfassen und deren Blickrichtung festzustellen, *Grimm u.a.*, VR-Eingabegeräte, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 97 (117 ff.); *Suthau*, See Through Head Mounted Display für die Medizin, 2006, S. 77 ff.; vgl. auch, 31C3, heise online, http://www.heise.de/newsticker/meldung/31C3-Mit-smarten-Brillen-das-Gehirn-ausforschen-2507482.html (11.1.2015).

[260] Vgl. B II. 2. c), S. 34.

[261] *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014).

[262] *Scobble*, Google Glass is still misunderstood, says the guy who wore them in the shower, CNET, http://www.cnet.com/news/google-glass-is-still-misunderstood-says-the-guy-who-wore-them-in-the-shower/(7.9.2015).

und der Handfreiheit vor allem das Augmented-Reality-Potenzial auf den Grad der Nützlichkeit von Smartglasses aus.

1. Echtzeitkriterium beim Informationsmanagement

Neben Augmented Reality stellt die schnelle Informationsvermittlung den wesentlichen Vorteil von Smartglasses dar.[263] Dieser als „Echtzeitkriterium" (bzw. „Time-to-Content-Kriterium") bezeichnete Vorteil ist ein grundlegender Faktor für die Effektivität der Kommunikation zwischen Menschen und Maschinen.[264] Gegenwärtig werden von Computern ausgegebene Informationen vor allem über aufmerksamkeitsfordernde Bildschirme wahrgenommen. Im Vergleich dazu verfügen Smartglasses über eine Ausgabeschnittstelle, die ähnlich einer traditionellen Brille permanent zwischen der Außenwelt und den Nervenzellen des Auges platziert ist, sodass die Informationsausgabe direkt im Blickfeld der Träger erfolgt. Die hieraus resultierenden Vorteile von Smartglasses kommen insbesondere dann zum Vorschein, wenn der Blick auf den Bildschirm die Aufmerksamkeit ablenken würde oder zusätzliche Handlungen, wie z.B. das Hervorholen eines Smartphones, erfordert.[265] So könnte z.B. ein Fahrradfahrer Navigationsinformationen oder Informationen zu eingehenden Anrufen direkt im Blickfeld erhalten, ohne auf ein auf dem Lenkrad montiertes Gerät blicken zu müssen.[266]

Auch bei einer Vielzahl der einzelnen Mikrointeraktionen mit Informationsvermittlungsgeräten sind Nutzer von Smartglasses im Vorteil. Dazu gehören z.B. soziale Interaktionen, wie der Austausch von Nachrichten mit anderen Personen oder die Suche nach Informationen im Internet. Eine Untersuchung zeigt, dass ein Smartphone bis zu 150 Mal an einem Tag hervorgeholt wird, während die durchschnittliche Interaktionszeit bis zu 20 Sekunden betragen kann.[267] Mithilfe von Smartglasses können die-

---

[263] *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014).

[264] *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 55.

[265] *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014).

[266] Es ist jedoch nicht außer Acht zu lassen, dass Datenbrillen auch eine trügerische Sicherheit vermitteln können und zur Nutzung in Situationen, bei denen im Regelfall kein Smartphone verwendet wird, z.B. beim Autofahren, führen können, vgl. *Kipper/Rampolla*, Augmented Reality, 2012, S. 25.

[267] *Bierend*, Google Glass Lead, WIRED, http://www.wired.com/2013/12/the-paradox-of-wearables-close-to-your-body-but-keeping-tech-far-away/(14.12.2014); *Lobe*, Warum wir ständig auf das Smartphone starren, Der Tagesspiegel Online, http://www.tagesspiegel.de/medien/digitale-welt/phubbing-trend-warum-wir-staendig-auf-das-smartphone-starren/10041432.html (14.12.2014); *Meeker/Wu*, 2013 Internet Trends, Kleiner Perkins Caufield & Byers, 2013, http://www.kpcb.com/blog/2013-internet-trends (14.12.2014).

selben Informationen in vielen Fällen innerhalb von zwei Sekunden zugänglich gemacht werden.[268]

2. Mensch-Maschine-Schnittstellen

Smartglasses stellen einen wesentlichen Erfolgsfaktor für die künftige technologische Entwicklung dar, da effektive Benutzerschnittstellen maßgeblich für den Erfolg neuer Technologien sind.[269] Mit der Verbreitung der Computertechnologie wird es für Menschen zunehmen wichtiger, mit und mittels Computer effizient kommunizieren zu können.[270] Dies gilt vor allem im Hinblick auf eine „Smarte Welt", in der Menschen z.B. im Straßenverkehr auf eine effektive Kommunikation mit autonom fahrenden Fahrzeugen angewiesen sein werden.[271] Dank Gesten- oder Spracherkennung können Smartglasses virtuelle Benutzeroberflächen erschaffen, die zweidimensionale Benutzeroberflächen auf Bildschirmen ablösen könnten.[272] So könnten Menschen in Verbindung mit Geräten treten, die wegen ihrer Größe bzw. Relevanz über keine eigenen Bildschirme oder Be-

---

[268] *Bierend*, Google Glass Lead, WIRED, http://www.wired.com/2013/12/the-paradox-of-wearables-close-to-your-body-but-keeping-tech-far-away/(14.12.2014); *Lobe*, Warum wir ständig auf das Smartphone starren, Der Tagesspiegel Online, http://www.tagesspiegel.de/medien/digitale-welt/phubbing-trend-warum-wir-staendig-auf-das-smartphone-starren/10041432.html (14.12.2014); *Meeker/Wu*, 2013 Internet Trends, Kleiner Perkins Caufield & Byers, 2013, http://www.kpcb.com/blog/2013-internet-trends (14.12.2014).

[269] Der Vorteil liegt in der "Usability", d.h. der Benutzerfreundlichkeit, *Dörner u.a.*, Interaktion in Virtuellen Welten, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 157 (158); Benutzerschnittstellen werden als ein Untersystem in einem Mensch-Maschinen-System definiert und haben den Zweck den Nutzern das Steuern, Beobachten oder das Eingreifen in maschinelle Prozesse zu ermöglichen, *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 54 f.; *Negroponte*, Total digital, 1997, S. 115 ff.; Deutsche Akkreditierungsstelle, Leitfaden Usability, 2010, http://www.dakks.de/sites/default/files/71-SD-2-007_Leitfaden%20Usability%201.3.pdf, S. 201; *Richter*, Methoden zur Unterstützung bei der Entwicklung plattformübergreifender Benutzerschnittstellen, 2007, S. XI.

[270] *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 53 f.; unter Kommunikation wird der Austausch von Informationen zwischen einem Sender und einem Empfänger verstanden, die nicht nur zwischen Menschen, sondern auch zwischen Menschen und Maschinen oder jeweils untereinander erfolgen kann (sog. "einstufiges Kommunikationsmodell"), Ebenda.

[271] *Färber*, Kommunikationsprobleme zwischen autonomen Fahrzeugen und menschlichen Fahrern, in: *Maurer u.a.*, Autonomes Fahren, 2015, S. 127 (143 ff.).

[272] *Dörner u.a.*, Interaktion in Virtuellen Welten, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 157; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 70; mit detaillierter Darstellung der Eingabe- und Interaktionsmöglichkeiten, *Tonnis*, Augmented Reality, 2010, S. 95 ff.; eine noch direktere Eingabemöglichkeit wäre die Auswertung von Hirnströmen, *Pratsch*, Auswirkungen einer Aero-Cave Umgebung auf die Orientierung innerhalb einer virtuellen 3D-Umgebung, 2005, S. 20; *Schart/Tschanz*, Augmented Reality, 2015, S. 29.

nutzeroberflächen verfügen. Smartglasses können z.B. die Bequemlichkeit und die Übersicht erhöhen, wenn mit ihnen in einem „Smart Home" das Raumklima gesteuert oder der Verschlussstatus der Fenster überprüft werden könnte.[273] Folglich bieten Smartglasses den Menschen die Möglichkeit, mit der technologischen Entwicklung Schritt zu halten.

3. Anwendungsmöglichkeiten und Einsatzbereiche

Neben dem generellen Nutzen als Mensch-Maschine-Schnittstellen zeigen sich die Vorteile von Smartglasses in vielen konkreten Anwendungsmöglichkeiten und Einsatzbereichen. Deren nachfolgende Darstellung soll jedoch nicht nur deren privaten Nutzen, sondern auch die beruflichen Vorzüge aufzeigen, die zu ihrer Durchsetzung im Alltag von Menschen beitragen können.

a) Lehre, Ausbildung und Forschung

Mithilfe von Augmented Reality kann Wissen dank Visualisierungstechniken anschaulich vermittelt und erlebbar gemacht werden (sog. „Edutainment").[274] So können zu Lernzwecken Explosionszeichnungen eines Motors, d.h. dessen schematische dreidimensionale Darstellung, oder für medizinische Zwecke die eines Körpers in der realen Umgebung eingeblendet, gedreht und von verschiedenen Seiten betrachtet werden.[275] Ebenso kann z.B. ein Arzt Medizinstudenten an einer Operation aus seinem Blickwinkel teilhaben lassen.[276]

b) Kollaboration und Kommunikation in virtueller Welt

Mithilfe von Smartglasses und Augmented Reality können virtuelle Meetings und Unterhaltungen geführt werden, bei denen die Teilnehmer jeweils für das Gegenüber visuell im Raum dargestellt und zusammen z.B. ein virtuell dargestelltes 3D-Modell besprechen können.[277]

---

[273] Infotainmentsystem Erweiterung, auto motor und sport, http://www.auto-motor-und-sport.de/news/infotainmentsystem-erweiterung-bmw-entwickelt-eine-datenbrille-fuer-fahrer-774546.html (19.12.2014); *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (111). *Mann/Niedzviecki*, Cyborg, 2002, S. 29 f., 205; *Kipper/Rampolla*, Augmented Reality, 2012, S. 53; *Tonnis*, Augmented Reality, 2010, S. 148 ff.

[274] *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 116 f.; *Tonnis*, Augmented Reality, 2010, S. 148 ff.

[275] *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (357); *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 94 ff.; *Schart/Tschanz*, Augmented Reality, 2015, S. 30 ff.

[276] *Nosta*, Inside The Operating Room With Google Glass, Forbes, http://www.forbes.com/sites/johnnosta/2013/06/21/google-glass-in-the-operating-room/(9.7.2013).

[277] *Kipper/Rampolla*, Augmented Reality, 2012, S. 78 ff.; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 103 f., 117.

c) Orientierung und Navigation

Smartglasses können wie bisherige Smartphones ihre Nutzer mithilfe von Navigationshinweisen leiten, indem sie z.B. Richtungspfeile oder Markierungen von Gebäuden in deren Blickfeld einblenden.[278]

d) Gesundheitsbereich

Im medizinischen Bereich können Smartglasses mit Augmented Reality im Rahmen eines operativen Eingriffs klinische Informationen (z.B. Computertomographien) für den Chirurgen auf die zu operierenden Stellen des menschlichen Körpers einblenden.[279] Sie können dem Arzt eine Navigations- und Orientierungshilfe bieten und die Operation deutlich einfacher sowie weniger invasiv für die Patienten gestalten.[280]

Smartglasses können insbesondere sehbeeinträchtigten Personen helfen, z.B. indem sie die Umgebung erkennen, diese auf retinalen Implantaten wiedergeben, ihre Nutzer mithilfe akustischer Signale leiten oder auch Texte vorlesen.[281] Ebenso können Psychosen und Phobien mittels visueller Simulationen behandelt werden.[282] Ferner können Smartglasses für Patienten mit motorischen Einschränkungen eine Schnittstelle zur virtuel-

---

[278] *Abawi*, Augmented Reality - die angereicherte Realität, 2008, S. 16; *Kipper/Rampolla*, Augmented Reality, 2012, S. 15; *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 17 f.

[279] *Kipper/Rampolla*, Augmented Reality, 2012, S. 83 ff.; *Suthau*, See Through Head Mounted Display für die Medizin, 2006, S. 1 ff.; *Tonnis*, Augmented Reality, 2010, S. 133 ff.

[280] Google Glass - One Year On, hypernetec, http://hypernetec.com/glass-one-year/ (7.9.2015); mit weiteren Beispielen, *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (356 f.); *Kipper/Rampolla*, Augmented Reality, 2012, S. 83 ff.; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 17; Zu weiteren Beispielen der Anwendung von Augmented Reality in der Medizin, S. *Suthau*, See Through Head Mounted Display für die Medizin, 2006, S. 23 ff.; *Tonnis*, Augmented Reality, 2010, S. 136 f.

[281] *Heinrich*, Retina-Implantate für Blinde, Spiegel Online, http://www.spiegel.de/gesundheit/diagnose/retina-implantate-lassen-blinde-wieder-sehen-a-1042526.html (19.8.2015); *Passary*, Precious Moment, Tech Times, http://www.techtimes.com/articles/28512/20150124/precious-moment-legally-blind-mom-sees-her-son-for-the-very-first-time-video.htm (6.2.2015); *Schwan*, Brille liest für Sehbehinderte, Technology Review, http://www.heise.de/tr/artikel/Brille-liest-fuer-Sehbehinderte-1916999.html (12.8.2013); *Wenleder*, Technik, SZ, http://www.sueddeutsche.de/wissen/technik-sehen-dank-datenbrille-1.2114402 (12.1.2015).

[282] *Botella u.a.*, Behavior Therapy 2010, Vol. 41, Nr. 3, p. 401; *Juan u.a.*, IEEE Comput. Graph. Appl. 2005, Vol. 25, Nr. 6, p. 31; *Kipper/Rampolla*, Augmented Reality, 2012, S. 85.

len Welt darstellen, mit deren Hilfe sie soziale Verbindungen pflegen können.[283]

e) Produktion und Wartung

Augmented Reality kann z.B. bei Reparaturen eingesetzt werden, indem nicht sichtbare Leitungen oder zu wartende Teile samt einer Wartungsanleitung im Blickfeld der Techniker dargestellt werden.[284] Dank diesem „Röntgenblick" sinkt die Fehlerquote, da zu reparierende Stellen und Schritte angezeigt werden, ohne dass Übertragungsfehler beim Blättern in einem Handbuch entstehen.[285]

Augmented Reality kann ebenfalls zu Konstruktionszwecken verwendet werden, um z.B. digitale Prototypen von Fahrzeugen, Kleidung oder Bauobjekten zu erstellen.[286] Es besteht ein deutlicher Vorteil gegenüber rein virtueller Planung auf PC-Bildschirmen, weil die Größenverhältnisse der Objekte auf einem Bildschirm oder deren Wirkung in realer Welt durch Menschen schlecht eingeschätzt werden können.[287]

f) Kultur und Medien

Museen und Ausstellungen können um virtuelle Objekte oder virtuelle Erweiterungen realer Objekte ergänzt und so „zum Leben erwachen und

---

[283] Google Glass - One Year On, hypernetec, http://hypernetec.com/glass-one-year/ (7.9.2015).

[284] *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (359); vgl. *Bockholt u.a.*, Augmented Reality Assistenzsysteme für Wartung und Service in Industrie, Bau und Gebäudemanagement, in: *Schenk*, 16. IFF-Wissenschaftstage 2013. Tagungsband: Digitales Engineering zum Planen, Testen und Betreiben technischer Systeme, 2013, S. 195 (ff.); *Kipper/Rampolla*, Augmented Reality, 2012, S. 81 ff.; *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 19; *Schart/Tschanz*, Augmented Reality, 2015, S. 29.

[285] *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 110.

[286] *Dörner u.a.*, Fallbeispiele für VR/AR, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 295 (306 ff.); *Schart/Tschanz*, Augmented Reality, 2015, S. 30.

[287] Mit weiteren Beispielen, *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (358 f.); *Dörner u.a.*, Fallbeispiele für VR/AR, in: *Dörner u.a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 295 (313 ff.); *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 18 und 11; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 17 ff.; *Tonnis*, Augmented Reality, 2010, S. 127 ff.

eine Geschichte erzählen".[288] Auch können virtuelle Museumsführer eingesetzt werden, die die Besucher leiten und mit Informationen versorgen.[289] Ebenfalls können auf Objekten oder sonstigen Stellen des Raums virtuelle Kunstobjekte platziert oder Graffiti angebracht werden, die ausschließlich im virtuellen Raum existieren.[290]

g) Konsum und Marketing

Im Marketing entsteht das Potenzial von Augmented Reality vor allem mit der Möglichkeit, Werbeinformationen abhängig von den Vorlieben oder dem Standort des Nutzers direkt in den Smartglasses anzuzeigen.[291] Beim Einkauf können z.B. Produkte im Blickfeld erfasst und durch zusätzliche Informationen, wie Nährwert oder Preisangebote, ergänzt werden.[292] Ebenso können Werbetafeln, ähnlich wie es von Bandenwerbung im Fußball bekannt ist, je nach Betrachter mit unterschiedlicher Werbeeinblendung überlagert werden.[293] Vorstellbar ist auch eine virtuelle Anprobe von Kleidungsstücken (sog „Tryvertising") oder die Begehung von Hausobjekten.[294]

h) Tourismus

Touristen können mithilfe von Smartglasses durch fremde Städte navigiert werden, Hinweistafeln übersetzt bekommen, zu Sehenswürdigkeiten oder Attraktionen geführt und mit Informationen zu diesen im Blickfeld

---

[288] Anhand von Beispielen im Guggenheim Museum, *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 111 ff.; *Schart/Tschanz*, Augmented Reality, 2015 , S. 31.

[289] *Tonnis*, Augmented Reality, 2010, S. 154 f.

[290] *Kipper/Rampolla*, Augmented Reality, 2012, S. 16 f.; *Lim/Aylett*, 2004 IEEE International Conference on Multimedia and Expo, 2004. ICME '04 2004, Vol. 2, p. 847.

[291] Hierbei wird jedoch die Befürchtung geäußert, dass ähnlich wie im Internet-Browser, Träger von Smart Glasses durch Werbeeinblendungen im Blickfeld belästigt werden könnten, *Kipper/Rampolla*, Augmented Reality, 2012, S. 25 f.; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 130 f.

[292] *Kipper/Rampolla*, Augmented Reality, 2012, S. 91 f.; *Mattern/Flörkemeier*, Informatik-Spektrum 2010, Vol. 33, Nr. 2, S. 107 (111); *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 120.

[293] *Kipper/Rampolla*, Augmented Reality, 2012, S. 88 ff.; *Schart/Tschanz*, Augmented Reality, 2015, S. 83.

[294] *Kipper/Rampolla*, Augmented Reality, 2012, S. 14; *Ludwig/Reimann*, Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 110 f.; *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 80 f., 103 f.

belehrt werden.[295] Daneben können geschichtsträchtige Orte mit virtuellen Szenen oder Personen virtuell belebt und damit erlebbar gemacht werden.[296] Die für die Darstellung in Augmented Reality benötigten Informationen können dabei aus öffentlich verfügbaren Quellen im Internet bezogen werden.[297]

i) Unterhaltung, Sport und Privatbereich

Die vorbenannten Vorteile von Smartglasses können auch dem privaten Bereich zugutekommen und z.B. den Zusammenbau von Möbeln oder das Warten von Gegenständen mittels virtueller Anleitungen im Blickfeld vereinfachen. [298] Ferner ist es mittels Smartglasses möglich, die Interaktionen zwischen den Mitgliedern sozialer Netzwerke in den physischen Raum zu verlagern. Andere Mitglieder des Netzwerks können z.B. in physischer Welt markiert sowie persönlich als auch mittels privater Nachrichten „angesprochen" werden.[299] Als ein großer Unterhaltungsfaktor könnten sich Augmented-Reality-Spiele herausstellen, bei denen die Spielelemente in der realen Welt platziert werden, die dadurch zu einem Spielfeld wird.

---

[295] *Kipper/Rampolla,* Augmented Reality, 2012, S. 75 ff.; *Schart/Tschanz,* Augmented Reality, 2015, S. 33 f.

[296] *Ludwig/Reimann,* Augmented Reality: Information im Fokus, 2007, http://www.c-lab.de/fileadmin/user_upload/Ueber_Uns/Services_Downloads/C-LAB_Reports/2005/1_C-LAB-TR-2005-1-Augmented_Reality_Information_im_Fokus.pdf (6.8.2014), S. 113.

[297] Vgl. *Azuma,* Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (359).

[298] Die Datenbrille "Moverio" des Herstellers Epson bietet z.B. Anleitungen für den Zusammenbau von LEGO-Spielzeugen, Not quite Google Glass, Engadget, http://www.engadget.com/2014/10/04/epson-moverio-bt-200/(19.12.2014).

[299] *Ferenstein,* Zuckerberg's 3 predictions for what social networks will look like in 10 years, VentureBeat, http://venturebeat.com/2015/01/14/zuckerbergs-3-predictions-for-what-social-networks-will-look-like-in-10-years/(22.8.2015); *Kipper/Rampolla,* Augmented Reality, 2012, S. 65 ff.

V. Hohes Nutzungspotenzial von Smartglasses

Die vorstehende technologische Betrachtung von Smartglasses zeigte deren hohes Potenzial, Menschen bei der Selbstbehauptung in einer informationalisierten Welt zu unterstützen.[300] Als effektive Mensch-Maschine-Schnittstellen erweitern Smartglasses die menschliche Wahrnehmung, helfen bei der Visualisierung komplexer Informationsstrukturen sowie Bewältigung komplexer Aufgaben und minimieren die zur Informationsvermittlung benötigte Zeit.[301]

Dabei hängen die jeweiligen Qualitäten von den konkreten Geräten ab, die vor allem Unterschiede in der Bauweise sowie den Fähigkeiten zur Augmented Reality aufweisen können. Für die Zwecke der vorliegenden Untersuchung werden Smartglasses daher einheitlich als blickdurchlässige oder den Blick auf die physische Welt vermittelnde „Head Mounted Displays" definiert, die über eine Kamera mit Mikrofon verfügen sowie zum Empfang oder zur Sendung digitaler Signale auf kabellosem Weg fähig sind. Zu ihren typischen Nutzungen gehören Live-Übertragungen, visuell-akustische Aufnahmen, ihre Verbreitung und Veröffentlichung ebenso wie Verarbeitung zu Zwecken biometrischer Erkennung oder der Erzeugung einer Augmented Reality.

[300] Vgl. *Tonnis*, Augmented Reality, 2010, S. 148 ff.

[301] *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 22; *Schart/Tschanz*, Augmented Reality, 2015, S. 28 ff.

C GESELLSCHAFTLICHE REAKTIONEN AUF SMARTGLASSES

Für die rechtliche Untersuchung ist neben den technischen Grundlagen von Smartglasses auch deren Wirkung auf Menschen in ihrem Erfassungsbereich sowie die Gesellschaft im Allgemeinen von Bedeutung. Beide zusammen geben die Lebenswirklichkeit wieder, welche der anschließenden juristischen Untersuchung als Grundlage dient.

Die Herausforderung dieser Untersuchung liegt jedoch darin, dass entsprechend ihrem präventiven Charakter noch keine empirischen Erkenntnisse oder Simulationsstudien zur Auswirkung von Smartglasses in der Gesellschaft vorliegen.[302] Die wenigen Einblicke ergeben sich aus den Erfahrungen des Smartglasses-Forschers Steve Mann und der Testphase von Google Glass ab Mitte des Jahres 2012 bis Anfang 2015. Diese Testphase bot neben den technischen Erfahrungen vor allem soziale Erkenntnisse, die sich in der begleitenden medialen Berichterstattung sowie den Erfahrungsberichten widerspiegeln und in Form einer Presseschau gewürdigt werden sollen. Zeitlich umfassender sind die Erfahrungen von Steve Mann, die einen Zeitraum von 30 Jahren umspannen und daher die Langzeitauswirkungen von Smartglasses vermitteln können.

Dabei fällt als erste Gemeinsamkeit auf, dass in sehr vielen Artikeln und Berichten die Nutzer von Smartglasses mit Cyborgs verglichen werden.[303] Zwar kam der „Cyborg"-Begriff nicht erst mit Smartglasses auf, dennoch wurde er im Hinblick auf Nutzer des „Cyberspace" oder Smartphone-Nutzer zumindest nicht in diesem Umfang verwendet. Er scheint daher im Hinblick auf Smartglasses eine besondere Bedeutung zu besitzen, weshalb der „Cyborg"-Begriff im Folgenden dekodiert und in seiner Bedeutung erforscht werden soll.

---

[302] Zum Begriff der Simulationsstudien, S. *Roßnagel*, Die Rolle des Rechts im Prozeß der Technikfolgenabschätzung, in: *Westphalen*, Technikfolgenabschätzung als politische Aufgabe, 1997, S. 222 (226).

[303] U.a. *Beuth*, Google Glass, Die Zeit, http://www.zeit.de/digital/datenschutz/2013-03/stop-the-cyborgs-google-glass (7.9.2015); *Mann/Niedzviecki*, Cyborg, 2002, S. ; *Schwenke*, DuD 2015, S. 161; *Weichert*, Google Glass, IT-Brillen und informationelle Selbstbestimmung, Virtuelles Datenschutzbüro - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutz.de/news/detail/?nid=5865 (7.4.2013).

I. „Cyborg“ als Indikator technologisch-gesellschaftlichen Umbruchs

Der „Cyborg“-Begriff wird im Zusammenhang mit Smartglasses nur selten positiv oder neutral verwendet.[304] In den meisten Fällen wird der Begriff negativ konnotiert und soll Träger von Smartglasses als Menschen, die durch die Technik vereinnahmt werden und dadurch ihre Menschlichkeit verlieren, beschreiben.[305] Dementsprechend muss der „Cyborg“-Begriff von einem technischen und von einem gesellschaftlichen Standpunkt aus betrachtet werden.

1. Technische Dimension des „Cyborg“-Begriffs

Der Begriff „Cyborg“ ist ein Neologismus, den die beiden US-Wissenschaftler Manfred E. Clynes und Nathan S. Kline mit den Worten „kybernetisch“ (englisch: „cybernetic“) und Organismus schufen, während sie im Rahmen der medizinischen Weltraumforschung an der Anpassung des Menschen an die Schwerlosigkeit mithilfe implantierter chemo-elektronischer Systeme arbeiteten.[306] Sie bezeichneten als Cyborg einen „von außen erweiterten organisatorischen Komplex“, der „unterbewusst als ein integriertes homöostatisches System“ funktioniert.[307]

Die grundlegende Idee des „Cyborgs“ liegt also in der optimierten Interaktion des Menschen mit einer Maschine.[308] In diesem Interaktionsprozess verbindet sich der biologische Organismus mit dem künstlichen System derart, dass eine neue, hybride Entität entsteht.[309] Ein Cyborg ist damit entsprechend der Definition eines kybernetischen Systems von Norbert Wiener ein einheitliches Informationssystem, in dem Mensch und Maschine verbunden sind, wodurch die Nachteile rein maschineller Roboter, insbesondere das fehlende Bewusstsein, überwunden werden.[310]

---

[304] Z.B. werden in einem Bericht prominente Fotografen, die mit Google Glass als Kamera experimentieren, wertneutral als "Cyborgs" bezeichnet, *Schmundt/Krug/Sperber*, Google Glass, Spiegel Online, http://www.spiegel.de/netzwelt/gadgets/google-glass-star-fotografen-elliott-erwitt-und-bruce-gilden-testen-a-1015979.html (6.2.2015); auch der Datenbrillenpionier Steve Mann bezeichnet sich selbst als "Cyborg", S. *Mann/Niedzviecki*, Cyborg, 2002, S. 4.

[305] So z.B. eine der bedeutendsten Anlaufplätze für Kritiker der tragbaren Technologien "Stop The Cyborgs", *Beuth*, Google Glass, Die Zeit, http://www.zeit.de/digital/datenschutz/2013-03/stop-the-cyborgs-google-glass (7.9.2015).

[306] *Clynes/Kline*, Astronautics 1960, Nr. 9, p. 26 (27).

[307] Ebenda.

[308] *Friedrich*, Die künstliche Evolution der Cyborgs, 2003, S. 13.

[309] Ebenda, 19 ff.

[310] Vgl. A IV. 4, S. 13; *Mann/Niedzviecki*, Cyborg, 2002, S. 53.

Ab welcher Verschmelzungsstufe von einem Cyborg gesprochen werden kann, ist je nach Wissenschaftsfeld unterschiedlich. Wird der Cyborg als ein strukturell oder funktionell manipulierter Mensch definiert, der sich auf modifizierte Weise an die Umwelt adaptieren kann, können bereits Nutzer von Hilfsmitteln wie traditionellen Brillen unter den Begriff fallen.[311] Erst recht gälte dies für medizinische Hilfsmittel wie z.B. Prothesen oder Herzschrittmacher.[312] Im Fachbereich der Bioinformatik wird ein Cyborg durch eine symbiotische Verbindung zwischen einem lebenden Organismus und einem künstlichen System, die durch interne (d.h. interorganische) Schnittstellen entsteht, definiert.[313] Eine vermittelnde Ansicht stellt ein flexibles „Subkutanitätskriterium“ auf und spricht von „high tech“-Cyborgs, bei denen die Technologie die Hautgrenze unterschreitet, und von „low tech“-Cyborgs, wenn diese Durchdringung des „körperlichen Nahraums“ noch nicht stattgefunden hat.[314]

Smartglasses können demnach wegen ihrer Eigenschaft als ubiquitäre Begleiter von Menschen, die der täglichen Aufgabenwahrnehmung dienen, ihren Nutzern den Charakter von „low tech“-Cyborgs verleihen. Erst mit der Nutzung der retinalen Implantate wird die Stufe zu einem „high tech“-Cyborg überschritten. Diese Einstufung kann z.B. relevant werden, wenn darüber zu entscheiden sein wird, inwieweit die Nutzung von Smartglasses für ihre Nutzer essentiell ist, weil die Geräte als integrale Bestandteile des Körpers verstanden werden müssen.

2. Gesellschaftliche Dimension des „Cyborg“-Begriffs

Der „Cyborg“-Begriff fand als Projektionsfläche für technische, biologische, wirtschaftliche und ethische Herausforderungen sowohl Eingang in

---

311 *Friedrich*, Die künstliche Evolution der Cyborgs, 2003, S. 19 ff.

312 *Pöhl*, Der Cyborg als Medium des Körpers, 2010, S. 3; eine Prothese ist der Ersatz oder Ergänzung von Körperteilen durch künstliche Produkte mit ähnlichen Funktionen, Duden, 2013, Stichwort „Prothese“.

313 Z.B. Neuroimplantate, mit denen Nerven von querschnittsgelähmten Personen stimuliert oder sensorische Fähigkeiten verbessert werden, S. *Friedrich*, Die künstliche Evolution der Cyborgs, 2003, S. 26 ff.; vgl. *Spreen*, Der Cyborg: Diskurse zwischen Körper und Technik, in: *Eßlinger u.a.*, Der Cyborg, 2010, S. 166 (172), 176.

314 Vgl. *Spreen*, Der Cyborg: Diskurse zwischen Körper und Technik, in: *Eßlinger u.a.*, Der Cyborg, 2010, S. 166 (169 f.).

die Wissenschaft als auch in die Kultur.[315] Gesellschaftlich betrachtet werden in den Begriff vor allem aber Ängste und Unbehagen hinein verlegt, die entstehen, wenn die Grenzen zwischen menschlichem Leib und Technik sich aufzulösen beginnen.[316]

Cyborgs sind lebende Wesen, bei denen der Übergang zwischen Mensch und Maschine fließend wird, und damit ethische, philosophische sowie religiöse Denkstrukturen herausgefordert werden.[317] Sie werden als „Signum einer posthumanen Gesellschaft" betrachtet, die einen sozioevolutionären Trend ausdrücken, welcher als „Zeitalter des Posthumanismus", also eine grundlegenden Änderung der Individuen und der gesellschaftlichen Strukturen, beschrieben wird.[318] Diese vielfältig diversifizierenden und durchaus umstrittenen Zukunftsbilder reichen zum Teil bis zu Vorstellungen eines religiös-transzendental geprägten „Transhumanismus", bei dem der Mensch je nach Betrachtung zunehmend mit Maschinen verschmilzt oder in diesen aufgeht.[319]

Geschichtlich betrachtet zeigt sich, dass die Relevanz des „Cyborgs" als Ausdruck gesellschaftlicher Ängste vor allem im Zeitalter revolutionärer technologischer und gesellschaftliche Umbrüche, wenn die Angst der Menschen vor Verlust ihrer existenziellen Grundlagen und gesellschaftli-

[315] Mensch-Maschine-Hybride finden sich in vielen kulturellen Formen wieder, z.B. in Filmen, wie RoboCop, http://www.imdb.com/title/tt0093870 (8.1.2014) oder Cyborg, IMDb, http://www.imdb.com/title/tt0097138 (8.1.2014); oft sind die Grenzen zwischen Cyborgs und sog. "Androiden", bei denen es sich um Roboter handelt, die menschenähnlich aussehen und sich menschenähnlich verhalten, fließend, vgl. *Friedrich*, Die künstliche Evolution der Cyborgs, 2003, S. 47 ff.; ein kulturelles Beispiel für Androiden ist z.B. die Figur "Data" aus der Fernsehserie Star Trek TNG, vgl. The Measure of a Man, IMDb, http://www.imdb.com/title/tt0708807/(8.12.2015).

[316] *Friedrich*, Die künstliche Evolution der Cyborgs, 2003, S. 7 f.; *Hayles*, The Life Cycle of Cyborgs: Writing the Posthuman, in: *Hables-Gray*, The Life Cycle of Cyborgs, 1995, S. 321 (321 ff.); *Spreen*, Der Cyborg: Diskurse zwischen Körper und Technik, in: *Eßlinger u.a.*, Der Cyborg, 2010, S. 166 (166).

[317] *Friedrich*, Die künstliche Evolution der Cyborgs, 2003, S. 8.

[318] *Spreen*, Der Cyborg: Diskurse zwischen Körper und Technik, in: *Eßlinger u.a.*, Der Cyborg, 2010, S. 166 (166 f.).

[319] Laut Wagner ist die Vorstellung der digitalen Unsterblichkeit gepaart mit ökonomischen Faktoren die Triebfeder hinter den maßgeblichen Unternehmen und Entwicklern aus Silicon Valley, *Wagner*, Robokratie, 2015, S. 18 ff.; die Unsterblichkeit als Triebfeder der gegenwärtigen Entwicklung betont auch *Mutschler*, Die Gottmaschine, 1998, S. 91.

cher Stellung zunimmt.[320] Das Modell eines hybriden Wesens wird bemüht, wenn das gegenwärtige ontologische Modell eines Menschen nicht mehr in die gegenwärtige Zeit zu passen scheint.[321] Vor allem die Änderungen in der Lebensumgebung der Menschen, denen sie sich im Rahmen ihrer gesellschaftlichen Behauptung anpassen mussten, rief die Vorstellung einer Aufgabe der (jeweils gegenwärtigen) Menschlichkeit zugunsten des Fortschritts hervor.[322]

So wurden bereits im Zeitalter der industriellen Revolution Befürchtungen geäußert, dass die Effizienz von Maschinen die Menschen dazu zwingen wird, sich ihnen anzupassen und maschinelle Eigenschaften anzunehmen.[323] Zudem wurde die ausgrenzende Überlegenheit derjenigen befürchtet, die Zugang zu den Maschinen hatten.[324] Auch die gesellschaftlichen und technologischen Umwälzungen der Weimarer Zeit brachten die Vorstellungen von hybriden Menschen hervor, die sich mit der Technik verbinden mussten, um ihr gesellschaftliches Fortkommen zu sichern.[325] Hierzu gehörten insbesondere die physische und psychische Desorientierung, die dem Automobil und der Einwirkung von Massenmedien geschuldet war.[326]

---

[320] Diese Stimmung drückt sich u.a. in Prognosen von Stephen Hawkings, Bill Gates oder Elon Musk aus, die neben einer Vielzahl renommierter Akteure der Wissenschaft, Wirtschaft und Politik vor den Gefahren einer ansteigenden künstlichen Intelligenz für den Fortbestand der Menschheit warnen, s. Tausende Unterzeichner - Forscher warnen vor Einsatz selbstständiger Kampfroboter, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/feuilleton/debatten/forscher-wie-stephen-hawking-warnen-vor-kampfroboter-einsatz-13723167.html (22.8.2015); *Cellan-Jones*, Hawking, BBC News, http://www.bbc.com/news/technology-30290540 (6.2.2015); *Gibbs*, Elon Musk: artificial intelligence is our biggest existential threat, the Guardian, http://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat (6.2.2015); *González*, Envisioning Cyborg Bodies: Notes form Current Research, in: *Hables-Gray*, Envisioning Cyborg Bodies, 1995, S. 267 (270); *Holley*, Bill Gates on dangers of artificial intelligence, The Washington Post, http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/28/bill-gates-on-dangers-of-artificial-intelligence-dont-understand-why-some-people-are-not-concerned/(6.2.2015); *Wagner*, Robokratie, 2015, S. 17.

[321] *González*, Envisioning Cyborg Bodies: Notes form Current Research, in: *Hables-Gray*, Envisioning Cyborg Bodies, 1995, S. 267 (270).

[322] Ebenda.

[323] Ebenda, 269; die hybride Form von Maschinen und Menschen war schon lange vor der Entstehung des Begriffs "Cyborg" Gegenstand kultureller Diskussionen, z.B. als "L'Homme Machine" in dem Essay von Julien Offray de La Mettrie aus dem Jahr 1748, S. Ebenda, 268 ff.

[324] *González*, Envisioning Cyborg Bodies: Notes form Current Research, in: *Hables-Gray*, Envisioning Cyborg Bodies, 1995, S. 267 (269).

[325] Vgl. Ebenda, 270 f.

[326] Vgl. Ebenda f.

Ein Ausdruck der Belastung durch den technologischen Fortschritt ist das im Jahr 1921 erschaffene Kunstwerk „Tête Méchanique“ des Dadaisten Raoul Hausmann, der auf dem Kopf eines Mannequins Gegenstände, wie ein Maßband, typografischen Zylinder, Teile einer Uhr und eine Kamera, platzierte.[327] Das Werk sollte einen Menschen repräsentieren, der in einer beunruhigenden und enigmatischen Welt gefangen ist, die er nur mithilfe einer Maske, bestehend aus arbiträren Symbolen wahrnimmt.[328] Es wirkt so, als ob Hausmann mit dem Werk die Cyborg-Diskussion im Zusammenhang mit Smartglasses bereits Anfang des letzten Jahrhunderts vorgeahnt hat.

II. Bisherige Erfahrungen mit Smartglasses

Smartglasses erinnern nicht nur in ihrer Grundidee an das Werk „Tête Méchanique“, sondern lösen bei Menschen auch das gleiche Unbehagen aus, das Hausmann mit seinem Werk seinerzeit konservieren wollte. Dies zeigt sich an dem nachfolgenden Einblick in die Erfahrungen von Steve Mann als auch an den Erkenntnissen aus dem „Google Glass“-Testlauf, der nachträglich als ein „soziales Experiment“ bezeichnet wurde.[329]

1. Langzeiterfahrungen von Steve Mann

Der kanadische Informatiker und Pionier der Erforschung von Smartglasses Steve Mann beschreibt anhand eigener Erfahrungen den Widerstreit zwischen den Vorteilen von Smartglasses und den gesellschaftlichen Vorbehalten ihnen gegenüber.[330] Mann entwickelt bereits seit seiner Jugend Smartglasses, setzte seine Forschung an dem „Massachusetts Institute of Technology“ fort und trägt im Alltag permanent die von ihm als „WearComp“ (Kurzform von „Wearable Computer“, d.h. „ein am Körper getragener Computer“) bezeichneten Geräte.[331] Seine Erfahrungen beziehen sich insbesondere auf die Nutzung der mit der Fähigkeit zur Mediated Reality ausgestatteten Smartglasses „EyeTap“.[332]

Aus diesem Grund wird er nicht nur von anderen Menschen als „Cyborg“ bezeichnet, sondern sieht sich selbst als ein Mensch-Maschine-

---

[327] Ebenda, 271 f.

[328] "[…] a man imprisoned in an unsettling and enigmatic space, 'perceiving the world through a mask of arbitrary symbols.'" von Timothy O. Benson, zitiert in: Ebenda f.

[329] *Nieva*, Lost Explorers, CNET, http://www.cnet.com/news/lost-explorers-the-unrealized-vision-of-google-glass/(7.9.2015).

[330] *Mann/Niedzviecki*, Cyborg, 2002, passim.

[331] Ebenda, 2 f.

[332] Vgl. B II. 2. c), S. 34.

Wesen.[333] Mann bezeichnet den von ihm getragenen WearComp als eine „zweite Haut", die es ihm erlaubt, in einer videographen Welt zu leben und selbst über den visuellen Informationsfluss autonom zu bestimmen.[334] Er versteht sich daher weniger als Träger seines „WearComps", sondern mehr als dessen menschlicher Teil, sieht das Gerät also als einen Teil seines Körpers an.[335]

Bei den negativen Reaktion, die Mann beim Tragen von Smartglasses erfahren hat, unterscheidet er zwischen der „Angst vor Cyborgs" und dem „Neid auf Cyborgs".[336] Den Zwiespalt führt Mann auf einen inneren Kampf der Menschen, die sich weigern zu erkennen, dass der Wandel von Menschen zu Cyborgs bereits begonnen hat, zurück.[337] Es ist seines Erachtens nicht die Frage, ob Menschen zu Cyborgs werden, sondern in welcher Stufe des Cyborg-Daseins sie sich gerade befinden.[338] Nach Manns Ansicht übersehen die Kritiker der Annäherung zwischen Menschen und Maschinen, dass Menschen sich schon immer der Technik angenähert und unter deren Einfluss verändert haben.[339] Dabei müsse man nicht weit zurückblicken und alleine bedenken, dass heutige Menschen, die ständig auf Mobiltelefone „starren", in den 1980er Jahren als unheimlich empfunden worden wären.[340]

Als weiteren Grund für die Abneigung gegen die Vorstellung von Menschen als Cyborgs macht Mann die Neigung von Menschen aus, die Welt in eindeutig gute und schlechte Aspekte zu unterteilen.[341] Technische Innovationen brächten jedoch immer Vor- und Nachteile mit sich, die weder schlechthin gut noch schlechthin schlecht seien, sondern vielmehr komplexe Änderungsprozesse darstellten.[342] Diese Komplexität sieht Mann auch im Hinblick auf die gesellschaftliche Integration von Smartglasses, welche nach seiner Ansicht in der Zukunft von jedermann getragen und unverzichtbar werden.[343] Die Notwendigkeit hierzu sieht Mann in der Ausbreitung der Informationstechnologien auf die gesamte Lebensumgebung von Menschen. Smartglasses werden nach Manns Ansicht

---

333 *Mann/Niedzviecki*, Cyborg, 2002, S. 4.

334 Ebenda, 2.

335 Ebenda, 17.

336 "Cyborg fear" und "Cyborg envy", Ebenda, 77, 79.

337 Ebenda, 98.

338 Ebenda, 7.

339 Ebenda, 92.

340 Ebenda, 93.

341 Ebenda, 99 f.

342 Ebenda.

343 Ebenda, 6.

Menschen dabei helfen, eine Verbindung zu dieser Lebensumwelt zu finden, die er durch die Verbindung der Begriffe „Cyberspace“ und „Cyborg“ als „Cyborgspace“ bezeichnet.[344]

2. Googles Testprojekt „Glass“

Bei „Glass“ handelte es sich zuerst um den Namen eines zuerst geheimen Entwicklungsprojekts für eine neue Generation tragbarer Computer, das von „Google X“, einer experimentellen Abteilung von Google, ab dem Jahr 2009 entwickelt wurde.[345] Laut Presseberichten beschloss Sergey Brin, der Mitbegründer und Geschäftsführer von Google, „Glass“ der Öffentlichkeit vorzustellen und das Feedback der ersten Nutzer für die Entwicklung der Datenbrille zu nutzen.[346] Dies geschah jedoch zu einem Zeitpunkt, als die mit dem Projekt betrauten Entwickler sich selbst noch nicht sicher waren, ob das Gerät nur für spezielle Zwecke eingesetzt werden oder ein Alltagsaccessoire werden sollte.[347] Dementsprechend war das Gerät noch nicht ausgereift, verfügte nur über rudimentäre „Augmented Reality“-Funktionen und diente eher als ein Display zur Anzeige von Informationen sowie als eine Kamera, mit der Fotografien oder Videos schnell und unmerklich erstellt werden konnten.[348]

Trotzdem stieß das neuartige Gerät nach seiner Vorstellung im Juni 2012 auf Begeisterung in den Medien, wurde von Prominenten getragen

---

[344] *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 107.

[345] *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015); *Topolsky*, I used Google Glass, The Verge, http://www.theverge.com/2013/2/22/4013406/i-used-google-glass-its-the-future-with-monthly-updates (7.1.2015).

[346] *Bajarin*, The Debacle of Google Glass, Re/code, http://recode.net/2015/05/12/the-debacle-of-google-glass/(7.9.2015); *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015); die Veröffentlichung von "Glass" als eine noch nicht ausgereifte Hardware war für sich ungewöhnlich, folgte aber den Erfahrungen im Softwarebereich, wo viele Entwicklungen als so genannte "Beta"-Versionen in einem noch nicht fertigem Stadium veröffentlicht werden, um die Erfahrungen der Nutzer in die Entwicklung einzubinden, vgl. *Humble/Farley*, Continuous Delivery, 2010, S. 90.

[347] *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015); *Holly*, There’s still nothing out there quite like Google Glass, Android Central, http://www.androidcentral.com/theres-still-nothing-out-there-quite-google-glass (7.9.2015); *Humble/Farley*, Continuous Delivery, 2010, S. 90.

[348] *Janssen*, Warum Glass (noch) nicht funktioniert, c’t, http://www.heise.de/ct/artikel/Warum-Glass-noch-nicht-funktioniert-1897211.html (16.8.2014); *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (7.9.2015); *Thompson*, Googling Yourself Takes on a Whole New Meaning, The New York Times, http://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html (7.9.2013).

und das „Time Magazine“ zeichnete „Glass“ als eine der besten Erfindungen des Jahres 2012 aus.[349] Die ersten zehntausend Geräte wurden an Entwickler und Journalisten (die von Google als „Explorer“ bezeichnet wurden), beginnend im Jahr 2013 zum Preis von US$ 1.500 ausgegeben.[350] Aufgrund des Marktpotenzials von Google sowie der Ausrichtung auf den Massenmarkt wurde Google Glass von manchen Analysten ein ähnlicher Erfolg bei der Durchsetzung von Smartglasses zugetraut wie zuvor dem Unternehmen Apple mit dem „iPhone“ bei den Smartphones.[351]

Jedoch tauchten zugleich kritische Stimmen auf, die auf die von dem Gerät ausgehende Gefahr für die Privatsphäre hinwiesen.[352] Es wurden Berichte bekannt, in denen Kinos, Restaurants oder Casinos in den USA den Zutritt mit „Glass“ untersagten.[353] Es wurde sogar der Neologismus „Glasshole“ geprägt, der den abfälligen Begriff „Asshole“ als Grundlage nutzte, um auf das im Hinblick auf die Privatsphäre Dritter unsoziale Verhalten der Nutzer von „Glass“ hinzuweisen.[354]

---

[349] *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015); *Holly*, There's still nothing out there quite like Google Glass, Android Central, http://www.androidcentral.com/theres-still-nothing-out-there-quite-google-glass (7.9.2015); Best Inventions of the Year 2012, Time, http://techland.time.com/2012/11/01/best-inventions-of-the-year-2012/slide/google-glass/(6.2.2015).

[350] *Biermann*, Datenbrille, Die Zeit, http://www.zeit.de/digital/mobil/2013-04/google-glass-technische-daten (2.7.2013); *Schart/Tschanz*, Augmented Reality, 2015, S. 48.

[351] *Rosenfelder*, Google und wie wir die Welt sehen werden, Welt Online, http://www.welt.de/kultur/medien/article115301957/Google-und-wie-wir-die-Welt-sehen-werden.html (4.7.2013); Google Glass: What Marketers should know, Forrester Research, Inc., http://www.forrester.com/Google+Glass+What+Marketers+Need+To+Know/fulltext/-/E-RES97141 (8.7.2013).

[352] *Thilo Weichert*: „Google Glass ist eine Waffe“, heise online, http://www.heise.de/newsticker/meldung/Thilo-Weichert-Google-Glass-ist-eine-Waffe-2176677.html (15.6.2014); *Heinrich*, AnwZert ITR 2014, 10/2014, Anm. 2; *Schwenke*, K&R 2013, S. 685; *Solmecke/Kocatepe*, ZD 2014, S. 22.

[353] Umstrittene Datenbrille, Handelsblatt, http://www.handelsblatt.com/panorama/aus-aller-welt/umstrittene-datenbrille-kneipen-gerangel-wegen-google-glass/9545216.html (7.9.2015).

[354] *Greenfield*, The Rise of the Term „Glasshole,“ Explained by Linguists, The Atlantic Wire, http://www.theatlanticwire.com/technology/2013/04/rise-term-glasshole-explained-linguists/64363/(4.7.2013); *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014).

Im Januar 2015 wurde die öffentliche Testphase des Projekts „Glass" schließlich eingestellt.[355] Laut offizieller Begründung des Unternehmens würden ausreichend Informationen gesammelt sein und das Projekt würde nunmehr das experimentelle Stadium verlassen und auf Grundlage der gesammelten Erfahrungen bis zur Marktreife weiterentwickelt werden.[356]

3. Erkenntnisse zur sozialen Wirkung von Google Glass

Es war ein Ansinnen von Google, mit dem öffentlichen Testlauf von „Glass" die Akzeptanz des Gerätes bei den Nutzern zu testen.[357] Die Reaktion der Nutzer war zwar aufgrund der frühen Entwicklungsphase gemischt (z.B. was die Batterielaufzeit und fehlende Anwendungsmöglichkeiten anging), jedoch wurde Smartglasses technisch gesehen generell eine erfolgreiche Zukunft prophezeit.[358]

Doch anders als erwartet, wurde vor allem deutlich, dass es für die Akzeptanz des Gerätes weniger auf die Erfahrungen der Nutzer mit „Glass"

---

[355] Google calls end to Glass experiment, BBC News, http://www.bbc.com/news/technology-30831128 (16.1.2015); *Lindner*, „Glass" Wie geht es mit Googles Datenbrille weiter?, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google/verkauf-von-google-glass-wird-eingestellt-13374767.html (6.2.2015).

[356] *D'Onfro*, Google has hired a bunch of engineers from Amazon's Lab126 for a new wearable tech initiative called „Project Aura", Business Insider, http://uk.businessinsider.com/google-project-aura-revealed-2015-9 (19.9.2015); Google Glass „Enterprise Edition" is foldable, more water resistant, rugged for the workplace, 9to5Google, http://9to5google.com/2015/07/21/google-glass-enterprise-edition-is-foldable-water-resistant-rugged-for-the-workplace/(14.9.2015); Datenbrille vor dem Aus, SZ, http://www.sueddeutsche.de/digital/verkaufsstopp-vater-des-ipods-soll-google-glass-retten-1. 2307044 (6.2.2015); *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015); *Grigoriadis*, Sergey Brin and Amanda Rosenberg, Vanity Fair, http://www.vanityfair.com/style/2014/04/sergey-brin-amanda-rosenberg-affair (6.2.2015); *Schart/Tschanz*, Augmented Reality, 2015, S. 10.

[357] *Bilton*, Why Google Glass Broke, The New York Times, http://www.nytimes.com/2015/02/05/style/why-google-glass-broke.html (6.2.2015); *Bajarin*, The Debacle of Google Glass, Re/code, http://recode.net/2015/05/12/the-debacle-of-google-glass/ (7.9.2015).

[358] Google Glass - One Year On, hypernetec, http://hypernetec.com/glass-one-year/ (7.9.2015); Good camera, great internet but poor speaker, Mail Online, http://www.dailymail.co.uk/news/article-2402934/Google-Glass-users-experience-having-Internet-eyesocket.html (7.9.2015); *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (7.9.2015); *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Scobble*, Google Glass is still misunderstood, says the guy who wore them in the shower, CNET, http://www.cnet.com/news/google-glass-is-still-misunderstood-says-the-guy-who-wore -them-in-the-shower/(7.9.2015); *Topolsky*, I used Google Glass, The Verge, http://www.theverge.com/2013/2/22/4013406/i-used-google-glass-its-the-future-with-monthly-updates (7.1.2015).

selbst ankam. Vielmehr wurde die Trageerfahrung von „Glass“ maßgeblich durch die Reaktion des Umfelds auf das Gerät bestimmt.[359]

Viele Nutzer beschrieben, dass die ungewöhnliche Optik des Gerätes, verbunden mit der direkt im Blickfeld platzierten Kamera eine abschreckende Wirkung auf Personen in deren Umfeld hatte.[360] Hinzu kam das Gefühl der Unterlegenheit, wenn die Personen sich zwischen Trägern von Google Glass als „gewöhnliche Sterbliche“ unter einer „ganz anderen Klasse von superverbundenen Menschen“ fühlten.[361] Dafür fand sich umgekehrt in den Erfahrungen der Träger von „Glass“ ein Gefühl der Überlegenheit wieder. Sie hatten das Gefühl, die Beschränkungen des menschlichen Körpers zu überwinden, selbstbefähigter zu werden und fühlten sich dank der Möglichkeit, jederzeit, schnell und ohne Abwendung des Blicks Informationen zu erhalten, mächtiger.[362] Ein zusätzliches

---

[359] "The most important Google Glass experience is not the user experience – it’s the experience of everyone else", *Hurst*, The Google Glass feature no one is talking about - Creative Good, Creative Good, http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about/(7.1.2015).

[360] *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (7.9.2015); *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab 2013/12/glasshole (2.1.2014); *Janssen*, Warum Glass (noch) nicht funktioniert, c’t, http://www.heise.de/ct/artikel/Warum-Glass-noch-nicht-funktioniert-1897211.html (16.8.2014); *Nieva*, Lost Explorers, CNET, http://www.cnet.com/news/lost-explorers-the-unrealized-vision-of-google-glass/(7.9.2015).

[361] "I felt like a mere mortal among an entirely different class of super-connected humans", *Bilton*, At Google Conference, Cameras Even in the Bathroom, The New York Times - Bits Blog, http://bits.blogs.nytimes.com/2013/05/17/at-google-conference-even-cameras-in-the-bathroom/(7.1.2015); zur Überlegenheit dank künstlichen Sensoren vgl. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 15; *Topolsky*, I used Google Glass, The Verge, http://www.theverge.com/2013/2/22/4013406/i-used-google-glass-its-the-future-with-monthly-updates (7.1.2015); es fällt auf, dass diese Beschreibung an den Begriff der "Informationsdominanz" erinnert, mit dem im militärischen Jargon die auf Mehrwissen basierende operationale Überlegenheit gegenüber dem Gegner beschrieben wird, *Kipper/Rampolla*, Augmented Reality, 2012, S. 102.

[362] Good camera, great internet but poor speaker, Mail Online, http://www .dailymail.co.uk/news/article-2402934/Google-Glass-users-experience-having-Internet-eyesocket.html (7.9.2015); *Arthur*, Google Glass, The Guardian, http://www.guardian .co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy (2.7.2013); "The human body has a lot of limitations", *Bailey*, Google Glass a Hit With 1st Users, Valley News, http://www.vnews.com/news/business/6144267-95/google-glass-a-hit-with-1st-users (7.1.2015).

Machtgefühl vermittelte ihnen die Möglichkeit, Bilder oder Videoaufnahmen schnell und unbeobachtet erstellen zu können.[363]

Der US-Autor David Pogue resümierte daher, dass Google Glass ihren Trägern eine „Kontrollmacht" verleiht.[364] Der Soziologe Michael Sacasas folgerte daraus, dass die Gründe für die Zunahme des Gefühls der Selbstbefähigung im Sinne einer Erweiterung persönlicher Kontrolle darin lägen, dass die Nutzer der Datenbrille „Glass" diese nicht als „Werkzeug" wahrnehmen und nicht „durch Glass" agieren, sondern schlicht „agieren".[365] Dadurch wurde „Glass" zu einer prothetischen Erweiterung des menschlichen Körpers und die Funktionen des Gerätes wurden von den Nutzern als die eigenen wahrgenommen.[366]

Die Unterlegenheit des Smartphone-Nutzers gegenüber Nutzern von Smartglasses kam auch bei Sergey Brin inhaltlich wie symbolisch zum Ausdruck, als er Smartphones im Vergleich zu Smartglasses als „entmannend" bezeichnete.[367] Denn anders als Smartglasses brächten Smartphones ihre Nutzer dazu, den Kopf zum Gerät hin zu beugen und die Konzentration von dem Geschehen um sie herum abzulenken, bevor sie an die gewünschten Informationen gelangen können.[368]

Aufgrund des Unbehagens von Personen im Umfeld der „Glass"-Nutzer fühlten sich einige von ihnen selbst unwohl, wenn sie sich mit aufgesetz-

---

[363] "[…] power to snap pictures with his eyelid", *Bilton*, At Google Conference, Cameras Even in the Bathroom, The New York Times - Bits Blog, http://bits.blogs.nytimes.com/2013/05/17/at-google-conference-even-cameras-in-the-bathroom/(7.1.2015); "I won't lie, it's amazingly powerful (and more than a little scary) to be able to just start recording video or snapping pictures with a couple of flicks of your finger or simple voice commands. […] In the city, Glass make you feel more powerful, better equipped, and definitely less diverted", *Topolsky*, I used Google Glass, The Verge, http://www.theverge.com/2013/2/22/4013406/i-used-google-glass-its-the-future-with-monthly-updates (7.1.2015).

[364] *Pogue*, Why Google Glass Is Creepy, Scientific American, http://www.scientificamerican.com/article/why-google-glass-is-creepy/(7.1.2015).

[365] *Sacasas*, Preserving the Person in the Emerging Kingdom of Technological Force, The Frailest Thing, http://thefrailestthing.com/2014/08/21/preserving-the-person-in-the-emerging-kingdom-of-technological-force/(22.8.2014).

[366] Ebenda.

[367] *Arthur*, Google's Sergey Brin, The Guardian, http://www.theguardian.com/technology/2013/feb/28/google-sergey-brin-smartphones-emasculating (12.10.2013).

[368] Ebenda.

ten Smartglasses in der Öffentlichkeit bewegten.[369] Das Unwohlsein Dritter führte laut manchen Erfahrungsberichten zu offener Ablehnung, Wutausdrücken oder Hausverboten gegenüber den „Glass"-Nutzern.[370] Die soziale Brisanz demonstriert der Fall einer „Glass"-Nutzerin, die in einem Lokal mit rüden Gesten bedacht wurde.[371] Als sie diesen Vorgang zu Nachweiszwecken mit „Glass" auf Video aufnehmen wollte, versuchten die Betroffenen ihr die Datenbrille gewaltsam abzunehmen.[372]

Als weitere Folge der sozialen Entfremdung zwischen „Glass"-Nutzern und ihren Mitmenschen wurde eine Ausgrenzung der „Glass"-Nutzer beobachtet.[373] Denn anders als bei Smartphones ist die Interaktion von Nutzern mit ihren Smartglasses für das Umfeld intransparent.[374] Die „Glass"-Nutzer wurden daher als „abwesend" oder „vor sich hin starrend"

---

[369] Google Glass Experience Review, 1 Year 1/2 Later! DarDadgetZ, YouTube, https://www.youtube.com/watch?v=XNHZlit2Oxw (7.9.2015); *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (7.9.2015); *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Janssen*, Warum Glass (noch) nicht funktioniert, c't, http://www.heise.de/ct/artikel/Warum-Glass-noch-nicht-funktioniert-1897211.html (16.8.2014); *Nieva*, Lost Explorers, CNET, http://www.cnet.com/news/lost-explorers-the-unrealized-vision-of-google-glass/(7.9.2015).

[370] Umstrittene Datenbrille, Handelsblatt, http://www.handelsblatt.com/panorama/aus-aller-welt/umstrittene-datenbrille-kneipen-gerangel-wegen-google-glass/9545216.html (7.9.2015); *Arthur*, Google Glass, The Guardian, http://www.guardian.co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy (2.7.2013); *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (7.9.2015); *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Kooser*, United Airlines to Google Glass wearer, CNET, http://www.cnet.com/news/google-glass-wearer-told-to-take-it-off-on-united-airlines-flight/ (7.9.2015); *Pachal*, Woman Robbed, Assaulted for Wearing Google Glass in a Bar, Mashable, http://mashable.com/2014/02/26/google-glass-assault/(7.9.2015).

[371] *Pachal*, Woman Robbed, Assaulted for Wearing Google Glass in a Bar, Mashable, http://mashable.com/2014/02/26/google-glass-assault/(7.9.2015).

[372] *Slocum*, Assaulted and Robbed at Molotov Bar on Haight St. for Wearing Google Glass, YouTube, https://www.youtube.com/watch?v=BvTrx-i_nB4 (7.9.2015).

[373] "Glass is a class divide in your face", *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Scobble*, Google Glass is still misunderstood, says the guy who wore them in the shower, CNET, http://www.cnet.com/news/google-glass-is-still-misunderstood-says-the-guy-who-wore-them-in-the-shower/(7.9.2015).

[374] *Arthur*, Google Glass, The Guardian, http://www.guardian.co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy (2.7.2013).

beschrieben.[375] Noch relevanter war jedoch, dass die Personen im Blickfeld der Smartglasses nicht wussten, ob ihr Gegenüber nur Informationen bezog oder Aufzeichnungen von ihnen erstellte.[376] Da sie jederzeit hätten aufgezeichnet werden können, fühlten sie sich den „Glass"-Nutzern ausgeliefert.[377] Die Folge war, dass auch manche „Glass"-Träger sich aus Rücksicht oder Angst vor Kritik nur in Abwesenheit von Menschen frei genug fühlten, die Smartglasses zu nutzen und die Geräte zunehmend seltener verwendeten.[378]

Es gab jedoch auch vereinzelte positive Berichte, laut denen „Glass"-Nutzer nur selten negative Erfahrungen gemacht haben.[379] Doch auch in diesen Fällen wurde die Erkennbarkeit der Kamera als Nachteil aufgeführt.[380] Zudem muss berücksichtigt werden, dass Google Glass eine seltene Erscheinung war, die sich allenfalls bei Fachkonferenzen vermehrt gezeigt hat und daher als Kuriosität ein spezielles Interesse hervorrief.[381] D.h., die bisherigen Erkenntnisse geben insbesondere keine Auskunft darüber, welche Wirkung die Omnipräsenz von Smartglasses im öffentlichen Raum hätte. Ebenfalls ist nicht nachvollziehbar, im welchem Umfang die Nutzer von Smartglasses tatsächlich ihre Umwelt erfasst und hierdurch ggf. eine höhere Belastung erzeugt hätten, wenn die Aufnah-

---

375 *Bilton*, At Google Conference, Cameras Even in the Bathroom, The New York Times - Bits Blog, http://bits.blogs.nytimes.com/2013/05/17/at-google-conference-even-cameras-in-the-bathroom/(7.1.2015).

376 *Scobble*, Google Glass is still misunderstood, says the guy who wore them in the shower, CNET, http://www.cnet.com/news/google-glass-is-still-misunderstood-says-the-guy-who-wore-them-in-the-shower/(7.9.2015).

377 *Sacasas*, Preserving the Person in the Emerging Kingdom of Technological Force, The Frailest Thing, http://thefrailestthing.com/2014/08/21/preserving-the-person-in-the-emerging-kingdom-of-technological-force/(22.8.2014).

378 *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Nieva*, Lost Explorers, CNET, http://www.cnet.com/news/lost-explorers-the-unrealized-vision-of-google-glass/(7.9.2015).

379 Google Glass - One Year On, hypernetec, http://hypernetec.com/glass-one-year/ (7.9.2015); Good camera, great internet but poor speaker, Mail Online, http://www.dailymail.co.uk/news/article-2402934/Google-Glass-users-experience-having-Internet-eyesocket.html (7.9.2015); *Holly*, There's still nothing out there quite like Google Glass, Android Central, http://www.androidcentral.com/theres-still-nothing-out-there-quite-google-glass (7.9.2015).

380 Google Glass - One Year On, hypernetec, http://hypernetec.com/glass-one-year/ (7.9.2015).

381 "[…] wearing Glass in public, as like 'seeing a unicorn out in the wild '", Ebenda; *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (7.9.2015); *Swider*, I wore Google Glass for one year and here's what I experienced, TechRadar, http://www.techradar.com/news/wearables/i-wore-google-glass-for-one-year-and-here-s-what-i-experienced-1281372/3 (7.9.2015).

mekapazität von Glass aufgrund der kurzen Batterielaufzeit und internen Speicherbegrenzung nicht limitiert gewesen wäre.[382]

III. Zunahme sozialer Spannungen infolge der Nutzung von Smartglasses

Die Menschen des industriellen Zeitalters hatten die Befürchtung, inmitten einer von effizienten Maschinen beherrschten Umgebung an den sozialen Rand gedrängt zu werden. Dieselbe Angst scheinen auch die Menschen des Informationszeitalters gegenüber Nutzern von Smartglasses als „Mensch-Maschine-Hybriden" zu hegen. Darauf deuten nicht nur die im Rahmen der Nutzung von Smartglasses bisher gewonnenen Erfahrungen hin, sondern auch die Häufigkeit des in diesem Zusammenhang verwendeten „Cyborg"-Begriffs. Der Begriff manifestiert eine radikale technische Veränderung, bei der traditionelle Strukturen der Individualität und des gesellschaftlichen Zusammenlebens herausgefordert werden.

Ein wesentlicher Umstand der Angst vor Smartglasses ist die Angst vor unbefugten Aufnahmen und deren Verwendung, wodurch sich eine große Angst der Menschen vor dem Verlust der Privatsphäre zeigt. Diese Angst hemmt wiederum die Nutzung der als sehr nützlich angepriesenen Smartglasses, wodurch ein hohes Spannungspotenzial zwischen den Interessen ihrer Nutzer und dem Schutz der Privatsphäre Dritter entsteht. Um dieses Spannungsverhältnis aufzulösen, müssen nach der Präsentation von Smartglasses, die mit der Privatsphäre verbundenen Interessen der Betroffenen näher untersucht werden.

[382] *Swider*, I wore Google Glass for one year and here's what I experienced, TechRadar, http://www.techradar.com/news/wearables/i-wore-google-glass-for-one-year-and-heres-what-i-experienced-1281372/3 (7.9.2015).

D KONZEPT UND ENTSTEHUNG DER PRIVATSPHÄRE

Das letzte Kapitel zeigte, dass Menschen alleine aufgrund der Präsenz von Smartglasses große Angst vor der Verletzung ihrer Privatsphäre haben. Um zu prüfen, inwieweit diese Angst eine rechtliche Beachtung findet, ist es erforderlich, die Interessen Betroffener am Schutz ihrer Privatsphäre näher zu beleuchten. Denn trotz bzw. wegen seiner allgemeinsprachlichen Verwendung fehlt es dem Privatsphärenbegriff an einer Konturierung und einheitlicher Verwendung.[383] Er hat unterschiedliche Aspekte und Ausprägungen, je nachdem, wie man ihn soziologisch, philosophisch, politisch, umgangssprachlich oder rechtlich betrachtet.[384] Aus diesem Grund erfordert eine rechtliche Untersuchung der Privatsphäre, dass deren Konzept auf seine rechtliche Bedeutung reduziert wird und so ein klares Verständnis erfährt.[385]

I. Entstehung eines Bedürfnisses nach Schutz der Privatsphäre

Das gegenwärtig geltende Konzept der Privatsphäre, als ein politisch verbrieftes Freiheitsrecht, das jedermann von der Geburt an garantiert wird, entwickelte sich in der durch die Industrialisierung geprägten Moderne.[386]

1. Änderung von Lebensumständen in der Moderne

Mit dem Ende der Feudalherrschaft und dem Aufkommen kapitalistischer Elemente im Merkantilismus der Frühmoderne ab dem 16. Jahrhundert änderte sich das Leben der Menschen wesentlich.[387] Vor allem die ab dem 19. Jahrhundert zunehmenden Errungenschaften der Mobilität, Kommu-

---

[383] Vgl. *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (260 ff.).

[384] *Hotter*, Privatsphäre, 2011, S. 9; *Kang*, Stanford Law Review 1998, Vol. 50, Nr. 4, S. 1193 (1214 f.); *Nebel*, ZD 2015, S. 517.

[385] *Hotter*, Privatsphäre, 2011, S. 13.

[386] Der Begriff der Privatsphäre existierte zwar schon vor der Moderne, hatte jedoch zum Teil abweichende Bedeutungen, z.B. in der Antike als Ausdruck des, im Gegensatz zu der Öffentlichkeit als Ort der Selbstverwirklichung, gesellschaftlich weniger relevanten Bereiches persönlicher Pflichten, vgl. *Habermas*, Strukturwandel der Öffentlichkeit, 1987, S. 15; *Sofsky*, Verteidigung des Privaten, 2007, S. 32.

[387] *Habermas*, Strukturwandel der Öffentlichkeit, 1987, S. 24.

nikation sowie Entstehung einer auf Effizienz ausgerichteten kapitalistischen Marktwirtschaft leiteten einen sozialen Wandel ein.[388]

Der Effizienzgedanke zwang die Marktakteure, sich aus einem örtlich fragmentierten Umfeld zu lösen und der überregionalen Nachfrage nach ihren Leistungen zu folgen.[389] Die Entwicklung führte zur Entstehung von Ballungszentren und zum Wachstum von Großstädten, die als Industrie- und Wirtschaftszentrenten dienten. Dabei wuchs der Anteil der Menschen, die in den Städten lebten, während der industriellen Revolution von 5% auf 60%.[390]

Mit den wirtschaftlichen Änderungen ging ebenfalls ein politischer Wechsel von höfischen und lokal fragmentierten Herrschaftsstrukturen zu einem Nationalstaat, der einen fairen Wettbewerb unter den Bürgern und Teilnehmern der freien Märkte sichern sollte, einher.[391] Zu Zwecken der Wahrung von Sicherheit, Ordnung und sozialer Fürsorge wurde ein effizient agierender bürokratischer Verwaltungsapparat erschaffen, da im Gegensatz zur Vormoderne kein direkter Kontakt mehr zwischen der Herrschaftsmacht und den Beherrschten bestand.[392]

2. Stärkung des Individuums durch Autonomie

Die Lösung der modernen Menschen aus dem örtlich und sozial beschränkten Umfeld beraubte sie eines bestimmten Wertegefüges und klar definierten Handlungshorizontes.[393] Dadurch wurde jedoch zugleich ihre Entwicklung zu rational denkenden Individuen, die sich selbst innerhalb vielschichtiger Sozialstrukturen behaupten mussten, gefördert.[394]

Was die Individuen auszeichnete und bis heute das Kriterium der Individualität definiert, war, dass sie zwar einer Menschengemeinschaft angehörten und mit anderen Menschen viele Merkmale teilten, dennoch für

---

[388] Ebenda, 15.

[389] Ebenda, 17, 28 ff.; *Simmel*, Philosophie des Geldes, 1900, S. 357 ff.

[390] *Mutschler*, Die Gottmaschine, 1998, S. 110.

[391] *Ariès*, Einleitung, in: *Ariès/Duby/Chartier*, Geschichte des privaten Lebens, Bd. 3, 1991, S. 7 (17); *Habermas*, Strukturwandel der Öffentlichkeit, 1987, S. 24 f., 31 ff.; *Hotter*, Privatsphäre, 2011, S. 69 ff.; *Simmel*, Philosophie des Geldes, 1900, S. 371 ff.

[392] *Ariès*, Einleitung, in: *Ariès/Duby/Chartier*, Geschichte des privaten Lebens, Bd. 3, 1991, S. 7 (17); *Habermas*, Strukturwandel der Öffentlichkeit, 1987, S. 24 f., 31 ff.; *Hotter*, Privatsphäre, 2011, S. 69 ff.; *Simmel*, Philosophie des Geldes, 1900, S. 371 ff.

[393] *Giddens*, Modernity and Self-Identity, 1991, S. 20; *Giddens*, Leben in einer posttraditionellen Gesellschaft, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 113 (144).

[394] *Sennett*, Verfall und Ende des öffentlichen Lebens, 2004, S. 166 f.; *Hotter*, Privatsphäre, 2011, S. 74.

sich einzeln waren und sich von anderen Menschen unterschieden.[395] Grundlage dieses Selbstverständnisses war eine Autonomie, die den Menschen erlaubte, kraft eigenen geistigen Bewusstseins die eigene Identität zu wandeln und anzupassen.[396] Nur so konnten sie eine individuelle Identität, die Persönlichkeit, bilden und sich so als ein Individuum in Abgrenzung zu anderen Menschen zu definieren.[397]

Die Autonomie bezeichnet die Fähigkeit des Menschen, sich als ein freies Wesen zu begreifen sowie seine Freiheit entsprechend seinen Überzeugungen und seinem Willen zu handeln. Die Autonomie ist damit die Voraussetzung seiner Individualität.[398] Der Zweck der Autonomie geht also über die Freiheit des Gewissens und der Meinung als innere Werte eines Menschen hinaus und schützt auch ein äußeres Verhalten, das sich an diesen Werten orientiert.[399] Damit ein dementsprechendes äußeres Handeln autonom ist, muss es auf einem freien Willen des Menschen, also unbeeinflusst von äußeren Zwängen, basieren.[400] D.h. jedoch nicht, dass die Autonomie eine völlige Abwesenheit äußerer Einflüsse verlangt, da Menschen ihre eigene Individualität zwangsläufig anhand von Lebens- und Handlungsbildern, die sie um sich herum in der Gesellschaft wahrnehmen, bestimmen.[401] Jedoch dürfen die äußeren Einwirkungen nicht zu Zwängen führen, die z.B. aufgrund der Furcht vor möglichen sozialen Konsequenzen des eigenen Handelns, z.B. der Annahme bestimmter Lebensweisen, entstehen.[402]

Das moderne gesellschaftliche Leben, das innerhalb von Ballungsräumen unter dem Einfluss der moralischen, wirtschaftlichen und staatlichen Interessen stattfand, brachte jedoch vielfältige Zwänge mit sich, die eine autonome Lebensführung der Menschen störten.

---

[395] Lat.: "Individuum", bedeutet "das Unteilbare", Duden, 2013, Stichwort „Individuum“; *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 48 ff.

[396] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 1; *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 49, 55.

[397] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 1; *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 49, 55.

[398] "Autonomie des Willens ist die Beschaffenheit des Willens, dadurch derselbe ihm selbst (unabhängig von aller Beschaffenheit der Gegenstände des Wollens) ein Gesetz ist. Das Prinzip der Autonomie ist also: nicht anders zu wählen, als so, dass die Maximen seiner Wahl in demselben Wollen zugleich als allgemeines Gesetz mit begriffen seien", *Kant*, Grundlegung zur Metaphysik der Sitten, 1786, S. 87.

[399] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 6 ff.

[400] Ebenda, 9.

[401] Ebenda, 12 ff.

[402] *Hotter*, Privatsphäre, 2011, S. 29.

3. Wunsch nach Abgrenzung und Rückzug

Mit der Stellung eines sich im Wettbewerb mit anderen Menschen befindenden Individuums und dem Wachstum der Großstädte änderten sich die Bedingungen und vor allem die Komplexität des Zusammenlebens von Menschen und erforderten einen Schutz ihrer Individualität.[403] Da Menschen nunmehr nicht nur mit einem ihnen vertrauten Umfeld agierten, mussten sie nach einem Kosten-Nutzen-Verhältnis abwägen, welche Informationen sie über sich anderen gegenüber preisgaben.[404] Es entstand die Notwendigkeit, das öffentliche Selbstbild abhängig von Personen und Situationen zu bestimmen, sich also von anderen Gesellschaftsmitgliedern selbstbestimmt abzugrenzen.[405]

Ein weiterer Grund für die Notwendigkeit zur Abgrenzung war die Bewahrung der psychischen Stabilität. Die komplexe wirtschaftlich-soziale Eingliederung brachte eine Vielzahl an äußeren Reizen mit sich, die eine psychische Distanz und Reserviertheit der Menschen zueinander als Selbstschutz vor einer seelischen Überforderung notwendig machte.[406] Anders als in kleinen Gemeinschaften hätte sonst die Vielzahl zwischenmenschlicher Kontakte in einer Großstadt zu einer inneren Reizüberflutung mit der Folge seelischer Überlastung geführt.[407]

Auch die Steigerung differenzierter individueller Ansichten und Vorlieben, welche der zunehmenden Individualisierung der Gesellschaftsteilnehmer geschuldet war, verlangte eine schützende Abschottung von den übrigen Gesellschaftsmitgliedern.[408] Da unterschiedliche Lebensansichten innerhalb der Gesellschaft nur begrenzt toleriert wurden, mussten sie vor den Augen der Öffentlichkeit geschützt werden.[409]

---

[403] "Zu den ärgsten Feinden der Freiheit zählt neben der Macht die soziale Verdichtung", *Sofsky*, Verteidigung des Privaten, 2007, S. 38 ff.

[404] Sennet verglich das Stadtleben mit einer Theaterbühne, in der Menschen ähnlich Schauspielern situationsbedingt verschiedene Rollen einnahmen, *Sennett*, Verfall und Ende des öffentlichen Lebens, 2004, S. 92 ff.; *Sofsky*, Verteidigung des Privaten, 2007, S. 107.

[405] *Hotter*, Privatsphäre, 2011, S. 68; *Simmel*, Philosophie des Geldes, 1900, S. 314.

[406] *Sofsky*, Verteidigung des Privaten, 2007, S. 38 ff.

[407] *Simmel*, Individualismus der modernen Zeit, 2008, S. 325.

[408] *Nagel*, Philosophy & Public Affairs 1998, Vol. 27, Nr. 1, p. 3 (4); So auch, *Simmel*, Die Großstädte und das Geistesleben, in: *Petermann*, Die Großstadt. Vorträge und Aufsätze zur Städteausstellung, 1903, S. 1985 (185 ff.).

[409] "We will never reach a point at which nothing that anyone does disgusts anyone else. […] The boundary between what we reveal and what we do not, and some control over that boundary, are among the most important attributes of our humanity", *Nagel*, Philosophy & Public Affairs 1998, Vol. 27, Nr. 1, p. 3 (4); *Simmel*, Die Großstädte und das Geistesleben, in: *Petermann*, Die Großstadt. Vorträge und Aufsätze zur Städteausstellung, 1903, S. 1985 (185 ff.).

Der moderne Mensch zog sich daher in den Bereich der Kleinfamilie zurück, die im Gegensatz zur vormodernen Großfamilie nicht mehr nur der Sicherheit und dem wirtschaftlichen Fortkommen diente, sondern ein vertrautes Umfeld jenseits des rationalen und risikobehafteten Austausches mit unbekannten Gesellschaftsteilen bot.[410] Der familiäre Raum wandelte sich damit zum Kernbereich der Selbstverwirklichung, der als Zufluchtsort dem staatlichen Zugriff sowie den Blicken der übrigen Gesellschaft entzogen war und der Herstellung psychischer Stabilität diente.[411] Die Familie bot so ein vertrautes Umfeld jenseits des rationalen und risikobehafteten Austausches mit unbekannten Gesellschaftsteilnehmern.[412] Mit dem Rückzug und der Abgrenzung der Gesellschaftsteilnehmer voneinander stieg jedoch zugleich deren Informationsinteresse aneinander.

4. Spannungsverhältnis zwischen Freiheitsräumen und Überwachungsinteressen

Die Abgrenzung der Menschen voneinander als auch vom Staat führte jedoch zugleich zu einem Vertrauensverlust und Misstrauen, das wiederum das Interesse an politischen Vorgängen sowie voyeuristische Interesse an Informationen über die anderen Gesellschaftsteilnehmer verstärkte (und u.a. zur Entstehung von Massenmedien führte).[413]

Das Interesse an der Beobachtung teilten sich die Individuen mit dem bürokratischen Nationalstaat, der zur Wahrung seiner Kontroll-, Ordnungs- und Selbsterhaltungsfunktionen, insbesondere der sozialen Fürsorge sowie Sicherung des fairen Wettbewerbs, wie auch der Rechte der Staatsbürger ebenfalls auf die Kenntnis des Verhaltens und der Ansichten der Gesellschaftsmitglieder angewiesen war.[414]

---

[410] *Giddens*, Leben in einer posttraditionellen Gesellschaft, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 113 (144); *Hotter*, Privatsphäre, 2011, S. 70; *Sennett*, Verfall und Ende des öffentlichen Lebens, 2004, S. 230 f.

[411] Vgl. Aries, der darauf hinweist, dass das Indidivuum in der vorindustriellen Zeit der Großfamilie untergeordnet und sich nur außerhalb dieser entfalten konnte, *Ariès*, Einleitung, in: *Ariès/Duby/Chartier*, Geschichte des privaten Lebens, Bd. 3, 1991, S. 7 (15); vgl. *Habermas*, Strukturwandel der Öffentlichkeit, 1987, S. 45 f.

[412] *Sennett*, Verfall und Ende des öffentlichen Lebens, 2004, S. 230 f.

[413] Vgl. *Hotter*, Privatsphäre, 2011, S. 69 f.; *Sennett*, Verfall und Ende des öffentlichen Lebens, 2004, S. 252 f., 332; *Sofsky*, Verteidigung des Privaten, 2007, S. 107.

[414] *Fuchs*, Critique of the Political Economy of Web 2.0 Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 31 (37); *Hotter*, Privatsphäre, 2011, S. 69 f.; *Sennett*, Verfall und Ende des öffentlichen Lebens, 2004, S. 325; *Simmel*, Über soziale Differenzierung. Soziologische und psychologische Untersuchungen, 1890, S. 120; *Sofsky*, Verteidigung des Privaten, 2007, S. 107, 116 ff.; *Webster*, Theories of the Information Society, 2014, S. 282 ff.

Die bürokratisch organisierten Kontrollmechanismen fanden auch auf in der Privatwirtschaft Anwendung.[415] Nur so konnten die komplexen technisch-wirtschaftlichen Prozesse koordiniert und perfektioniert werden.[416] Nach dem Produktionsprozess erfasste das Überwachungsbedürfnis auch die Produktentwicklung und den Vertrieb.[417] Informationen über Konsumenten wurden für die Marktforschung und den Verkauf von Produkten von Bedeutung. Sie dienten dazu, die Bedürfnisse der Konsumenten zu erfahren, zu wecken und gezielt anzusprechen.[418]

Die vorgenannten und neu entstandenen Bedürfnisse sowie Möglichkeiten der Überwachung führten zur Entstehung einer neuen Form der sozialen Kontrolle, die als „Disziplinargesellschaft“ bezeichnet wird.[419]

5. Panoptische Überwachung und Kontrolle in der Disziplinargesellschaft

Der Begriff der „Disziplinargesellschaft“ beschreibt eine seit dem 18 Jahrhundert stattfindende Weiterentwicklung der auf Strafe und Folter basierenden gesellschaftlichen Kontrolle der Feudalzeit.[420] Die direkte Gewaltanwendung wurde dabei durch mildere Formen der Macht ersetzt, um Menschen zu disziplinieren, zu kontrollieren und zu normalisieren.[421] Um diese neu entwickelten Überwachungsstrukturen zu beschreiben, verwendete der französische Soziologe Michel Foucault mit dem „Panoptikum“ eine Metapher.[422] Mit ihr griff er auf eine von dem englischen Philosophen und Sozialreformer Jeremy Bentham im 18. Jahrhundert entworfene Bauweise für Gefängnisse, Besserungsanstalten oder Fabriken zurück.[423]

Die Besonderheit panoptischer Bauweise liegt darin, dass die Insassen bzw. Arbeiter von einem zentralen Punkt aus beobachtet werden können, aber nicht wissen, ob die die Beobachtung gerade tatsächlich stattfindet.[424] Das Panoptikum brachte den Vorteil mit sich, dass die Beobachte-

---

[415] *Lyon*, Surveillance Studies, 2007, S. 12; *Sofsky*, Verteidigung des Privaten, 2007, S. 120.

[416] Vgl. *Radkau*, Technik in Deutschland, 2008, S. 64.

[417] *Sofsky*, Verteidigung des Privaten, 2007, S. 121 f.

[418] *Lyon*, Surveillance Studies, 2007, S. 40 f.

[419] *Foucault*, Überwachen und Strafen, 1994, S. 263 ff.

[420] *Allmer*, Critical Internet Surveillance Studies, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 124 (126).

[421] Ebenda; zu organisatorischer Disziplin, S. *Marx*, Das Kapital, 1872, S. 440 ff.

[422] *Foucault*, Überwachen und Strafen, 1994, S. 263 ff.

[423] *Bentham*, Das Panoptikum, 2013, passim.

[424] Ebenda; *Foucault*, Überwachen und Strafen, 1994, S. 257 f.; Der Begriff geht auf den griechischen Worte "pãn" für "gesamt" sowie "optikós" für optisch und bedeutet so viel wie "das alles Sehende" oder "Gesamtschau", Duden, 2013, Stichwort „Panoptikon“.

ten sich wegen potenziell permanenter Überwachung selbst disziplinierten und dadurch deren Kontrolle zum einen keiner unmittelbaren Gewaltanwendung bedurfte und zum anderen ökonomischer und „ungeheuer effizient“ wurde.[425]

Übertragen auf die Kontrolle der Gesellschaft bedeutet die panoptische Überwachung, dass die moralischen Werte und sonstigen Normen nicht als unmittelbarer Zwang vermittelt werden müssen, sondern als ein „fester Bestandteil des alltäglichen Lebens akzeptiert werden.“[426] Personen, die sich der Beobachtung ausgesetzt fühlen, haben die Wahl, entweder ständig auf der Hut zu sein, um abweichende innere Gedanken und Ansichten nicht preiszugeben oder die von den beobachtenden Instanzen akzeptierte Meinung als ihre eigene zu verinnerlichen, um so dem Druck der Beobachtung zu entgehen.[427]

Diese Betrachtungen entsprechen den psychologischen Erkenntnissen, die auf der Theorie der objektiven Selbstaufmerksamkeit beruhen.[428] Wenn Menschen nicht ihre Umwelt, sondern sich selbst aus einem objektiven Blickwinkel betrachten, nehmen sie einen Abgleich zwischen ihrem tatsächlichen Verhalten und einem von ihnen erwarteten Idealverhalten vor.[429] Werden sie sich dabei einer Diskrepanz bewusst, müssen sie entscheiden, ob und in welchem Umfang sie diese Diskrepanzen reduzieren.[430]

Sind Menschen sich dabei bewusst, dass ihre Selbstbeobachtung einer Fremdbeobachtung entsprechen kann, dann treffen sie die Entscheidung zum Umgang mit der Verhaltensdiskrepanz nicht mehr autonom, sondern unter Einbeziehung möglicher Sanktionen infolge der Fremdbeobachtung.[431] Denn die Aufrechterhaltung der Verhaltensdiskrepanz könnte

---

[425] *Allmer*, Critical Internet Surveillance Studies, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 124 (127); vgl. *Bentham*, Das Panoptikum, 2013, S. ; *Foucault*, Überwachen und Strafen, 1994, S. 260; *Han*, Transparenzgesellschaft, 2012, S. 75 f.; *Hotter*, Privatsphäre, 2011, S. 91.

[426] *Foucault*, Überwachen und Strafen, 1994, S. 278 f.; *Hotter*, Privatsphäre, 2011, S. 92.

[427] *Sofsky*, Verteidigung des Privaten, 2007, S. 27.

[428] *Fischer/Wiswede*, Grundlagen der Sozialpsychologie, 2009, S. 424.

[429] Ebenda.

[430] *Goffman*, Wir alle spielen Theater, 2003, S. 7 f.; *Wicklund/Frey*, Die Theorie der objektiven Selbstaufmerksamkeit, in: *Frey/Irle*, Theorien der Sozialpsychologie, 1993, S. 155 (155 f.).

[431] *Grötker*, Informationelle Selbstbestimmung, in: *Sokol*, Total transparent, 2006, S. 48 (52).

sonst zu einer psychischen Beeinträchtigung durch geistige Anspannung, Unwohlsein oder Ängste vor Sanktionen führen.[432]

Die nächstliegende und eigener Entscheidungsgewalt unterliegende Möglichkeit zur Reduktion der inneren Diskrepanz, der sog. „kognitiven Dissonanz", ist die Anerkennung des erwarteten Verhaltens als eigenen Wertemaßstab.[433] Diese Aufgabe eigner Subjektivität als Folge der kognitiven Dissonanz birgt nicht nur individuelle Folgen, sondern auch eine Gefahr der Meinungskonformität und damit der Gefährdung einer freiheitlich-demokratischen Gesellschaft.[434] Dabei fällt es desto schwerer, ein abweichendes Selbstbild aufrechtzuerhalten, je genauer und je verbreiteter die Vorstellungen anderer sind, die von einem Gesellschaftsmitglied erwartet werden.[435]

II. Definition, Schutzzwecke und Funktionen der Privatsphäre

Als Folge der zunehmenden staatlichen, wirtschaftlichen und gesellschaftlichen Überwachung fühlten sich die Gesellschaftsteilnehmer in der Entfaltung der Individualität behindert und entwickelten ein Bedürfnis nach einem Schutz vor diesen Eingriffen.[436] Daraus entstand auf Grundlage der Wünsche nach selbstbestimmtem Rückzug aus der Öffentlichkeit sowie einer modulierten Informationspreisgabe das rechtlich verbürgte Schutzgut der Privatsphäre.[437]

1. Entstehung der Privatsphäre als ein negatives subjektives Recht

Die Idee der Privatsphäre als Schutzrecht von Individuen griffen vor allem Gelehrte wie Thomas Hobbes, John Locke und John Stuart Mill auf.[438] Nach ihrer Vorstellung sollte dem einzelnen Menschen ein innerer Bereich verbleiben, innerhalb dessen er frei vom öffentlichen Druck seiner

---

[432] *Geiger*, Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie, 1994, S. 55 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 94.

[433] *Fischer/Wiswede*, Grundlagen der Sozialpsychologie, 2009, S. 357 f.; *Giddens*, Interpretative Soziologie, 1984, S. 112 ff.; *Goffman*, Verhalten in sozialen Situationen, 1971, S. 9.

[434] *Hotter*, Privatsphäre, 2011, S. 79 f.; vgl. *Nagel*, Concealment and Exposure, 2004, S. 21.

[435] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 13.

[436] *Simmel*, Soziologie, 1983, S. 256 ff.

[437] *Hotter*, Privatsphäre, 2011, S. 70.

[438] Ebenda, 15; *Locke/Ebbinghaus*, Ein Brief über Toleranz, 1996, S. XIII u. XXII; *Mill*, Über die Freiheit, 1986, S. 9 f.

inneren Freiheit und der Vernunft folgen kann.[439] Vor allem sollte eine „Tyrannei der Mehrheit" durch öffentlichen Druck auf die Vertreter von Meinungen, die vom gesellschaftlichen Konsens abweichen, vermieden werden.[440]

Immanuel Kant fasste diese liberal freiheitlichen Theorien zu einer Staatslehre zusammen, nach der das Merkmal der bürgerlichen Gesellschaft die Freiheit eines jeden Bürgers ist, eigene Handlungen durch freien Willen bestimmen zu dürfen, solange dabei keine Freiheiten der Mitbürger verletzt werden.[441] Diese Freiheit darf laut Kant nur durch Gesetze beschränkt werden, die vom öffentlichen Gemeinwillen des Volkes legitimiert sind.[442] Damit formulierte Kant eine negative Freiheit, nach der jeder sich kraft freien Willens und nach den Grenzen eigener Vernunft, unabhängig von fremdbestimmten Ursachen gegen oder für moralisches Handeln entscheiden darf.[443]

Der Schutz des Individuums vor Konformität war jedoch nicht nur ein Selbstzweck, sondern diente auch dem objektiven Interesse der pluralistischen Gesellschaft.

2. Objektive Schutzkomponente der Privatsphäre

Pluralistische Gesellschaften zeichnen sich dadurch aus, dass sie dem Individuum eine Rückzugssphäre belassen und diese sogar schützen, damit es Entscheidungen frei von einer öffentlichen Einmischung fällen kann.[444] Sie basieren auf der Idee, dass ihre Mitglieder ihr Glück nur durch die Möglichkeit, sich ständig neu zu finden und zu erfinden und einen „Lebensplan eigenständig zurechtzulegen und zu verfolgen", finden oder bewahren können.[445] Die Privatsphäre schützt damit zugleich die Demokratie, welche auf einem Wettbewerb unterschiedlicher Werte basiert.[446]

Würden Menschen aus Angst vor Konsequenzen nur der öffentlichen, d.h. „sicheren" Meinung folgen, würde der Wertepluralismus kollektivis-

---

[439] *Hobbes*, Leviathan, 2005, S. 179; *Locke/Ebbinghaus*, Ein Brief über Toleranz, 1996, S. XVII ff.; *Mill*, Über die Freiheit, 1986, S. 20.

[440] *Hotter*, Privatsphäre, 2011, S. 19; *Mill*, Über die Freiheit, 1986, S. 10.

[441] *Kant*, Werkausgabe Band 11, 1977, S. 145.

[442] So auch *Hobbes*, Leviathan, 2005, S. 179; *Kant*, Werkausgabe Band 11, 1977, S. 150.

[443] *Kant*, Grundlegung zur Metaphysik der Sitten, 1786, S. 97 ff.

[444] *Westin*, Privacy And Freedom, 1968, S. 26.

[445] Ebenda.

[446] *Ketzer*, Securitas ex Machina, 2005, S. 188.

tischen Tendenzen geopfert werden.[447] Der absoluten Transparenz wohnt nicht die Negativität inne, welche vorhandene politisch-ökonomische Systeme in Frage stellt.[448] Das Fehlen der Privatsphäre stabilisiert dagegen vorhandene Systeme, indem es nur das Existierende bestätigt und optimiert, aber gegenüber dem Außen eines Systems blind ist.[449] Denn nicht Normen und Institutionen konstituieren eine aus Macht erwachsende Herrschaft, sondern der „Konformismus der Menschen".[450]

Um ihrer Funktion als Keimzelle autonom entwickelter Ideen zu dienen, die sich erst im demokratischen Meinungswettbewerb behaupten müssen, ist es notwendig, dass die Privatsphäre negativ ausgestaltet ist, also eine wertneutrale Rückzugssphäre bildet, die keiner Rechtfertigung bedarf.[451] Gerade die Negativität ist ein Raum, in dem „das Neue" und „das ganz Andere" sich entwickeln kann. Dazu bedarf es jedoch eines Scheins, einer „Maske", die es vor „dem Gleichen" schützt.[452]

3. Kritik an positiven Konzepten der Privatsphäre

Im Gegensatz zu einer negativ ausgestalteten Privatsphäre sind Konzepte, welche die Inanspruchnahme der Privatsphäre bestimmten Anforderungen unterwerfen und somit deren Inanspruchnahme einer Rechtfertigungspflicht unterwerfen, kritisch zu betrachten.

Zu diesen Konzepten, die die Privatsphäre bedingen wollen, gehören z.B. feministische Theorien, die eine Privatsphäre formulieren, welche zugleich Rücksicht auf die Freiheits- und Gleichheitsrechte anderer nimmt und z.B. keine Räume für die Benachteiligung der Frauen im häuslichen Bereich bietet.[453] Ähnlich argumentieren die Vertreter des Kommunitarismus, einer sich an moralischen Werten orientierenden Denkbewegung, die Grenzen der individuellen Freiheit beim gesellschaftsschädigenden Verhalten ziehen wollen.[454] Die kommunitaristischen Theorien ähneln dabei den Ideen von Rousseau und Marx, die eine Idee der idealen Gesellschaft vertraten, in welcher der Gemeinwille eine moralisch-

---

[447] *Hotter*, Privatsphäre, 2011, S. 80; "At its worst, this climate demands that people say what they do not believe in order to demonstrate their commitment to the right side […]", *Nagel*, Philosophy & Public Affairs 1998, Vol. 27, Nr. 1, p. 3 (23).

[448] *Han*, Transparenzgesellschaft, 2012, S. 16.

[449] Ebenda.

[450] *Sofsky*, Verteidigung des Privaten, 2007, S. 17.

[451] Vgl. Ebenda, 136 ff.

[452] *Han*, Transparenzgesellschaft, 2012, S. 32 f.

[453] *Kymlicka*, Theorie und Gesellschaft Band 35, 1997, S. 210 ff.; *MacKinnon*, Toward a Feminist Theory of the State, 1989, S. 239; vgl. *Sofsky*, Verteidigung des Privaten, 2007, S. 62.

[454] *Etzioni*, Die Entdeckung des Gemeinwesens, 1998, S. 3, 18, 283.

metaphysische Wesensgleichheit mit der Summe aller individuellen Ansichten der Gesellschaftsmitglieder haben sollte.[455]

Abgesehen von der Frage, wie ein „Gemeinwille" in einer heterogenen Gesellschaft angenommen werden kann, würde eine positive Ausgestaltung der Privatsphäre dazu führen, dass diejenigen, die sich auf sie berufen, zuerst deren Voraussetzungen darlegen müssten.[456] Da sie im Rahmen der Begründung ihres Anspruchs auf die Privatsphäre die Umstände und Grundlagen ihrer Inanspruchnahme darlegen müssten, würde das Konzept der Privatsphäre ad absurdum geführt, da das, was zu verdecken wäre, zuerst gegenüber der Öffentlichkeit offengelegt werden müsste.[457]

Wäre der Umfang einer Privatsphäre von der gesellschaftlichen Kollektivvorstellung abhängig, so könnte dieser Umfang auch auf null schrumpfen, wodurch sich das Individuum dem kollektiven Willen nicht entziehen könnte.[458] Die Folge wäre ein Zwang zur Konformität.[459] Die Konformität würde wiederum verhindern, dass die herrschende kollektive Moral einer Überprüfung unterzogen werden könnte.[460]

Deshalb darf die Privatsphäre auch nicht zulasten der Gleichheit geopfert werden, vielmehr muss die Gleichheit auf Grundlage der Privatsphäre umgesetzt werden.[461] Denn ein demokratischer Diskurs setzt einen geschützten Entwicklungsraum voraus, in dem abweichende politische Ansichten besprochen werden und nach Zuspruch suchen können.[462] Dabei muss auch in Kauf genommen werden, dass diese Gedanken die Demokratie an sich oder das bestehende politische System in Frage stellen dürfen.[463] Sie dürfen erst eingeschränkt werden, wenn nachgewiesen ist, dass sie das Bestehen des freiheitlich-demokratischen Systems, wel-

---

[455] *Fetscher*, Rousseaus politische Philosophie, 1993, S. 127 f.; *Fetscher*, Karl Marx und der Marxismus, 1967, S. 39 f.; *Kymlicka*, Theorie und Gesellschaft Band 35, 1997, S. 134.

[456] Hotter verweist darauf, dass Rousseaus Ideen auf der Vorstellung eines überholten "kollektiven Individualismus" des 18ten Jahrhunderts basierten, der sich mit dem Wechsel zum 20sten Jahrhundert in einen "pluralistischen Individualismus", also dem Aufbau einer großen Bandbreite in Inhalt und Position unterschiedlicher Wertvorstellungen, wandelte, *Hotter*, Privatsphäre, 2011, S. 47 f.

[457] Vgl. Ebenda, 48.

[458] Vgl. *Mill*, Über die Freiheit, 1986, S. 10.

[459] *Hotter*, Privatsphäre, 2011, S. 53 f.

[460] Ebenda, 54.

[461] Ebenda, 57.

[462] *Bennett/Raab*, The Governance of Privacy, 2006, S. 40; *Sofsky*, Verteidigung des Privaten, 2007, S. 136 ff.

[463] *Sofsky*, Verteidigung des Privaten, 2007, S. 137.

ches diese Gedanken überhaupt zulässt, oder die Rechtsgüter Dritter gefährden.[464]

4. Erweiterung des „Rechts alleine gelassen zu werden“ um ein dynamisches Kommunikationskonzept

Auch wenn die Privatsphäre in ihrem Kernbereich auf Grundlage der liberal-freiheitlichen Gedanken als eine Sphäre für autonome Handlungen in ihrem Kernbereich bestimmt wurde, wurde sie erst von den beiden US-Juristen Warren und Brandeis als ein benanntes Recht, das „Recht alleine gelassen zu werden“ (englisch: „the right to be left alone“), definiert.[465] Warren und Brandeis formulierten die Privatsphäre als ein generelles Freiheitsrecht, das sowohl gegenüber dem Staat als auch gegenüber den Mitbürgern gilt. Dabei schufen sie eine Analogie zum Privateigentum, welche sich nicht auf körperliche, sondern auf unkörperliche Güter erstecken sollte.[466]

Neben der Möglichkeit des Rückzugs aus der Gesellschaft bedurften Gesellschaftsmitglieder aber auch einer Möglichkeit, ihre Stellung im Gesellschaftsgefüge durch Kontrolle über den sie betreffenden Informationsfluss zu regulieren.[467] Nur so konnten sie Sicherheit angesichts der veränderten Risikoanforderungen des modernen Lebens gewinnen und einen Einfluss auf ihre Personalität, d.h. die Wahrnehmung durch andere Gesellschaftsmitglieder, nehmen.[468]

Während die Menschen der Vormoderne sich den Naturgewalten und (göttlichem) Schicksal ausgeliefert fühlten, brachte die Moderne von

---

[464] Vgl. *Westin*, Privacy And Freedom, 1968, S. 21 ff.

[465] *Hotter*, Privatsphäre, 2011, S. 12; *Warren/Brandeis*, Harvard Law Review 1890, Vol. 4, Nr. 5, p. 193.

[466] "[…] and now the right to life has come to mean the right to enjoy life, the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession- intangible, as well as tangible", *Warren/Brandeis*, Harvard Law Review 1890, Vol. 4, Nr. 5, p. 193; ähnlich Simmel, der ebenfalls von einem "geistigen Privateigentum" spricht, *Simmel*, Soziologie, 1983, S. 266.

[467] *Sofsky*, Verteidigung des Privaten, 2007, S. 108 ff.; *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (256).

[468] Während die Individualität unmittelbar und aktiv dem Menschen anhaftet, handelt sich bei der Personalität um eine passive Eigenschaft, die sich aus der Stellung des Menschen in der Gesellschaft ergibt und dessen Entscheidung für bestimmte Verhaltensweisen bestimmt werden kann, *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 51; umgekehrt kann die Individualität eines Menschen durch dessen Personalität beeinflusst werden, indem die gesellschaftliche Rollenzuweisung die besonderen subjektiven Merkmale eines Menschen verändern, *Wieczorek*, Persönlichkeitsrecht und Meinungsfreiheit im Internet, 2013, S. 57; vgl. *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 29.

Menschenhand geschaffene Risiken mit sich, die entweder durch Umgang mit anderen Menschen oder abstrakte Systemen (z.B. den Personenverkehr oder Unternehmen) entstanden.[469] Diese Risiken konnten aufgrund ihrer Komplexität nicht vollständig kontrolliert werden und setzten ein Vertrauen unter den Gesellschaftsmitgliedern voraus.[470] Dies setzte wiederum einen Austausch von wechselseitigen Informationen als Grundlage einer sozialen oder wirtschaftlichen Interaktion voraus.[471]

Gleichzeitig bedeutete die von jedermann ausgeübte Informationskontrolle, dass Menschen nicht auf Grundlage ihrer vollständigen Persönlichkeit, sondern nur der über sie bekannten Informationen eingeschätzt wurden.[472] Dadurch konnte das Bekanntwerden gesellschaftlich abweichender Informationen über eine Person auch zu einem Misstrauen führen.[473] Aus diesem Grund bedurfte es Schutzmechanismen, welche den Menschen erlaubten, die über sie in Erfahrung zu bringenden Informationen selbst bestimmen zu können.[474]

Hieraus entstand die Funktion der Privatsphäre als Recht, darüber zu bestimmen, wie viel persönliche Informationen an wen weitergegeben werden und wie sie vorgehalten und verbreitet werden.[475] Dessen Umfang wird dabei in einem dialektischen Prozess bestimmt, in dessen Rahmen zwei widerstreitende psychologische Bedürfnisse einer Person abgewogen werden.[476] Zum einen das Recht auf Rückzug und zum anderen das Bedürfnis nach sozialer Interaktion, die zwingend eine Preisgabe von per-

---

[469] *Beck*, Risikogesellschaft. Auf dem Weg in eine andere Moderne, 1986, S. 254; *Giddens*, Modernity and Self-Identity, 1991, S. 123 f.; *Habermas*, Strukturwandel der Öffentlichkeit, 1987, S. 350 ff.; *Giddens*, Modernity and Self-Identity, 1991, S. 123 f.

[470] "Natürlich ist kein System in der Lage, die wirkliche Welt mit all ihrer unfaßbaren Komplexität in der Vorstellung zu wiederholen […] Im Falle des Vertrauens nimmt diese Komplexitätsreduktion durch Subjektivierung besondere Formen an. […] Das System setzt innere Sicherheit an die Stelle äußerer Sicherheit.", *Luhmann*, Vertrauen, 2000, S. 31 f.

[471] *Giddens*, Konsequenzen der Moderne, 1996, S. 102 ff.

[472] Eine typische Beziehungsform, in der die gegenseitige Einschätzung lediglich auf wenigen Informationen basiert, ist für Simmel die Bekanntschaft, *Simmel*, Soziologie, 1983, S. 264 f.

[473] Ebenda.

[474] "Ein soziales System, das misstrauisches Verhalten seiner Teilnehmer für bestimmte Funktionen benötigt oder nicht vermeiden kann, braucht zugleich Mechanismen, die verhindern, dass das Misstrauen überhandnimmt.", *Luhmann*, Vertrauen, 2000, S. 100; *Sofsky*, Verteidigung des Privaten, 2007, S. 108 ff.

[475] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 13; "[…] the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated", *Westin*, Privacy And Freedom, 1968, S. 7.

[476] *Altman*, The environment and social behavior, 1975, S. 11.

sönlichen Informationen gegenüber Dritten voraussetzt, um eine Nähe zwischen Menschen zu erzeugen.[477]

Der optimale Umfang der Privatsphäre ist damit ein individuelles Equilibrium zwischen dem Wunsch nach Kontrolle persönlicher Informationen und der Bereitschaft, Informationen gegenüber Dritten preiszugeben.[478] Dieses Equilibrium ist selbst nicht starr, sondern abhängig von Situation und Kommunikationspartner.[479] Z.B. ist die Bereitschaft zur Preisgabe von Informationen gegenüber Fremden im öffentlichen Raum geringer als zu Hause gegenüber Familienmitgliedern.

Die Privatsphäre ist also kein absolutes, sondern ein relatives Konzept, das auf der individuellen Wahrnehmung und dem individuellen Verhalten und der Preisgabe persönlicher Informationen beruht und die Relevanz der sozialen Interaktion und zwischenmenschlicher Beziehungen betont.[480]

5. Funktionen der modernen Privatsphäre

Aus den in der Privatsphäre verkörperten Bedürfnissen nach Rückzug sowie dynamischer Informationsregelung muss die Privatsphäre lt. Westin vier wesentliche Funktionen erfüllen:

Zum einen kann die Privatsphäre schlicht zum Zweck des Alleinseins beansprucht werden.[481]

Zum anderen schützt die Privatsphäre auch den Informationsaustausch innerhalb enger zwischenmenschlicher Beziehungen und das Recht zur Bestimmung des Adressaten der eigenen Selbstdarstellung.[482]

---

[477] *Green/Grotz*, Human Communication Research 1976, Vol. 2, Nr. 4, p. 338; *Simmel*, Soziologie, 1983, S. 256.

[478] *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (256).

[479] Ebenda.

[480] *Altman*, The environment and social behavior, 1975, S. 18; *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (257).

[481] "The first state of privacy is solitude", *Westin*, Privacy And Freedom, 1968, S. 31.

[482] "In the second state of privacy, intimacy, the individual is acting as part of a small unit that claims and is allowed to exercise corporate seclusion so that it may achieve a close, relaxed, and frank relationship between two or more individuals", Ebenda.

Die dritte Funktion der Privatsphäre besteht in der Anonymität, also einer Interaktion mit der Außenwelt, die nicht dem agierenden Individuum zugerechnet werden kann.[483] Die Funktion der Privatsphäre wird ebenfalls als eine „öffentliche Privatheit" bezeichnet, da sie auch eine öffentliche, aber anonyme Meinungskundgabe umfasst.[484]

Die vierte Funktion der Privatsphäre ist die Reserviertheit, welche den subtilsten Ausdruck der Privatsphäre darstellt und eine mentale sowie physische Distanz zur sozialen Umwelt umschreibt.[485] Sie wird vor allem als notwendig zur Wahrung einer psychischen Identität in modernen industriellen Gesellschaften und im urbanen Leben betrachtet.[486] Die Reserviertheit kommt daher in Situationen zur Anwendung, die Menschen nicht in Abgeschiedenheit oder Anonymität verbringen (wie die meiste Zeit ihres Lebens), in denen sie aber dennoch bestimmte Teile der Persönlichkeit zurückhalten möchten, weil diese ihnen z.B. zu beschämend oder zu profan sind.[487] D.h., diese Funktion der Privatsphäre wird vor allem zur Lösung der Spannung zwischen der „Selbstoffenbarung und Selbstzurückhaltung" herangezogen.[488]

III. Das moderne Privatsphärenkonzept

Zusammenfassend lässt sich das moderne Konzept der Privatsphäre als ein individueller und wertneutraler Freiraum persönlicher Integrität definieren, der das Individuum vor äußeren Einflüssen bewahrt und ihm innerhalb dieses Bereichs Kontrolle über die eigene Selbstdarstellung bietet, d.h. freie Wahl, welche ihn betreffenden Informationen veröffentlicht werden und welche nicht.[489]

Der Zweck der Privatsphäre besteht in der Sicherung der autonomen Lebensgestaltung.[490] Denn nur wer die Möglichkeit hat, sich äußeren

---

[483] "The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seek, and finds, freedom from identification and surveillance", Ebenda; so auch, *Sofsky*, Verteidigung des Privaten, 2007, S. 39.

[484] "Public Privacy", *Westin*, Privacy And Freedom, 1968, S. 32; Hoeren verweist auf die Anonymität als einen Wert, der es Menschen ab der Neuzeit erlaubte, deren soziale Rollen, Zünfte und Familien verlassen zu können, *Hoeren*, ZRP 2010, S. 251 (251 f.).

[485] "Reserve, the fourth and most subtle form of privacy, is the creation of a psychological barrier against unwanted intrusions; this occurs when the individual's need to limit communication about himself is protected by the willing discretion of those surrounding him.", *Westin*, Privacy And Freedom, 1968, S. 32.

[486] Ebenda; *Simmel*, Soziologie, 1983, S. 269 ff.

[487] *Westin*, Privacy And Freedom, 1968, S. 32; *Simmel*, Soziologie, 1983, S. 269 ff.

[488] *Westin*, Privacy And Freedom, 1968, S. 32; *Simmel*, Soziologie, 1983, S. 269 ff.

[489] *Hotter*, Privatsphäre, 2011, S. 43.

[490] *Pieroth u.a.*, Grundrechte, 2014, Rn. 391.

staatlichen, wirtschaftlichen und moralischen Einflüssen zu entziehen, kann in einer durch äußere Zwänge geprägten Umwelt geistige Entspannung und Freiheit finden.[491] Nur dank der Privatsphäre können Menschen den notwendigen psychischen Ausgleich zu der Notwendigkeit, sich in sozialen Situationen selektiv darzustellen und unterschiedliche, zum Teil widersprechende Rollen zu spielen, finden.[492] Ohne einen privaten Freiraum und die Möglichkeit, „die Hüllen fallen zu lassen", würden Menschen die innere Balance verlieren und psychische sowie physische Probleme bekommen, wodurch ihr Wohlbefinden beeinträchtigt wäre.[493] Ebenso ist Privatsphäre eine notwendige Voraussetzung, damit Menschen „zu sich finden" können, also das Erlebte ohne fremde Einflüsse reflektieren und auf dieser Grundlage sich selbst hinterfragen und definieren, um autonome Entscheidungen für eine authentische Lebensführung treffen zu können.[494] Indem die Privatsphäre einen Raum schafft, der Menschen vor dem Zugriff Dritter bewahrt, wird damit zugleich ein Spielraum für autonome Handlungen eröffnet.[495]

Neben dem Schutz des Individuums dient die Privatsphäre der Sicherung einer meinungsoffenen demokratischen Gesellschaft, indem sie einen Freiraum schafft, in dem sich auch abwegige sowie mit den Mehrheitsmeinungen kollidierende Ansichten entwickeln und in einen demokratischen Prozess eingebracht werden können.[496] Ohne diesen Freiraum wären eine erzwungene Konformität der Meinungen und das Ende des demokratischen Meinungswettbewerbs zu befürchten.[497]

Dabei ist die Privatsphäre kein absolutes Recht, sondern vielmehr ein relativer Wert, der seine Grenzen in den Freiheiten anderer Gesellschaftsteilnehmer findet und darüber hinaus durch die Erfüllung öffentlicher Aufgaben eingeschränkt wird, mit denen die Staatsbürger die demokra-

---

[491] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (383); *Hotter*, Privatsphäre, 2011, S. 29 ff.

[492] "Finaly, emotional release through privacy plays an important part in individual times […]", *Westin*, Privacy And Freedom, 1968, S. 36 ff.

[493] Ebenda, 41 f.

[494] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 9 ff.; "Self-Evaluation. Every Individual needs to integrate his experiences into a meaningful pattern and to exert his individuality on eventS. To carry on such self-evaluation, privacy is essential", *Westin*, Privacy And Freedom, 1968, S. 36 f.

[495] *Hotter*, Privatsphäre, 2011, S. 31 f.

[496] Vgl. BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43); BVerfG, Beschl. v. 12.4.2005 (2 BvR 1027/02), BVerfGE 113, 29 (46); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 35 ff.

[497] *Hotter*, Privatsphäre, 2011, S. 29 ff.

tisch gewählte Staatsgewalt betrauen.[498] Nur wenn die Privatsphäre dazu missbraucht werden sollte, das liberale Systeme an sich oder andere schützenswerte Freiheitswerte Dritter zu verletzen, muss sie eingeschränkt werden.[499] Hierbei gilt jedoch der Grundsatz „in dubio pro libertate", wonach der Beweis der Rechtmäßigkeit demjenigen obliegt, der in ein Freiheitsrecht eingreift.[500]

D.h., wer die Privatsphäre in Anspruch nehmen will, muss dies nicht mit einem schützenswerten Zweck begründen, da die Privatsphäre ein liberaler Selbstzweck ist und mit der Autonomie sowie der Demokratie bereits dem Schutz elementarer gesellschaftlicher Werte dient.[501]

[498] Ebenda, 43.

[499] *Westin*, Privacy And Freedom, 1968, S. 21 ff.

[500] *Hotter*, Privatsphäre, 2011, S. 34.

[501] Ebenda, 33 f.

E VERFASSUNGSRECHTLICHE PRÜFUNG DER NUTZUNG VON SMARTGLASSES

Die herausgearbeiteten Vorzüge von Smartglasses wie auch das Recht auf die Privatsphäre müssen vor dem Hintergrund der technischen Umgebung gegeneinander abgewogen werden. Dies findet nachfolgendend im Wege einer verfassungsrechtlichen Untersuchung statt, die einem durch Grundrechte vorgegebenen Prüfungsrahmen folgt. Dazu wird zuerst der Schutz der Privatsphäre in dem Grundrechtskatalog verortet. Anschließend wird dessen Beeinträchtigung durch die Nutzung der Smartglasses geprüft und auf eine mögliche Rechtfertigung durch die schützenswerten Interessen ihrer Nutzer untersucht. Die verfassungsrechtliche Prüfung ist für die im nächsten Kapitel folgende einfachgesetzliche Prüfung relevant. Denn obwohl eine Interessenabwägung in der Praxis von der einfachgesetzlich zu würdigenden Einzelfallsituation abhängt, wird das Verfassungsrecht dabei dennoch als ein objektiver Verfassungsmaßstab zur Anwendung kommen.[502]

I. Auswirkung der Grundrechte im Verhältnis zwischen Privaten

Grundrechte binden gem. Art. 1 Abs. 3 GG nur „die Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht".[503] Die drei Staatsgewalten müssen jedoch gem. Art. 1 Abs. 3 GG und Art. 20 Abs. 3 GG im Rahmen ihrer Aufgabenerfüllung die Grundrechte der Bürger beachten.[504] Daher entfalten die Grundrechte insoweit eine subjektivrechtliche Wirkung, auf die sich Bürger auch im Verhältnis zu anderen Privatakteuren mittelbar, d.h. über den Staat als Mittler, berufen können.[505] Dazu gehört insbesondere, dass Gerichte unbestimmte Rechtsbegriffe und Interessenabwägungen in einfachgesetzlichen Verfahren unter

---

[502] BVerfGE, Beschl. v. 19.10.1993 (1 BvR 567 u. 1044/89), BVerfGE 89, 214 (229 f.); BVerfG, Beschl. v. 23.4.1986 (2 BvR 487/80), BVerfGE 73, 261 (269); BVerfG, Beschl. v. 3.10.1979 (1 BvR 726/78), BVerfGE 52, 203 (207); BVerfG, Urt. v. 15.1.1958 (1 BvR 400/57), BVerfGE 7, 198 (206 f.); *Herdegen*, in: *Maunz/Dürig*, GG, Art. 1 Abs.3, Rn. 65; *Pieroth u.a.*, Grundrechte, 2014, Rn. 195 ff.

[503] So die h.M., BVerfG, Beschl. v. 23.4.1986 (2 BvR 487/80), BVerfGE 73, 261 (269); BVerfG, Urt. v. 15.1.1958 (1 BvR 400/57), BVerfGE 7, 198 (205); *Merten*, NJW 1972, S. 1799; *Pieroth u.a.*, Grundrechte, 2014, Rn. 191 ff.

[504] *Herdegen*, in: *Maunz/Dürig*, GG, Art. 1 Abs.3, Rn. 64 ff.; *Pieroth u.a.*, Grundrechte, 2014, Rn. 101.

[505] BVerfG, Urt. v. 15.1.1958 (1 BvR 400/57), BVerfGE 7, 198 (206 f.).

Beachtung der Verfassungswerte auslegen müssen.[506] Ferner können auf legislativer Ebene Pflichten zur Schaffung von Schutzgesetzen für Bürger voreinander (sog. primäre Schutzpflichten) und auf exekutiver Ebene Pflichten zu deren Durchsetzung (sog. sekundäre Schutzpflichten) entstehen.[507]

Der Umfang, in welchem die Grundrechte beachtet werden müssen, ist einzelfallbezogen und soll zwar eine Symmetrie herstellen, die den Bürgern gleiche Chancen auf die Verfolgung und Bewahrung ihrer Interessen bietet, darf jedoch nicht in eine Fremdbestimmung umschlagen (sog. Übermaßverbot).[508] Eine Fremdbestimmung wäre vor allem dann anzunehmen, wenn die Regelungen dem Ausgleich von Bagatellbeeinträchtigungen, die sich nicht negativ auf die Subjektivität der Bürger auswirken und sich notwendigerweise durch ein gesellschaftliches Zusammenleben ergeben, dienen würden.[509]

Ob Smartglasses lediglich eine Bagatellbeeinträchtigung darstellen, vermag bereits an dieser Stelle anhand der Schilderung der durch sie Betroffenen bezweifelt werden.[510] Das gilt insbesondere deswegen, weil dem Schutz der Grundrechte gerade vor dem Hintergrund der Bedrohung der Privatsphäre durch den technischen Fortschritt eine besondere Bedeutung beigemessen wird.[511] Angesichts der Vorwürfe, Smartglasses seien „Waffen“ oder „Werkzeuge des Bösen“, die zur Objektivierung von Menschen beitragen, liegt eher die Prüfung eines Verstoßes gegen die, das

---

[506] BVerfGE, Beschl. v. 19.10.1993 (1 BvR 567 u. 1044/89), BVerfGE 89, 214 (229 f.); BVerfG, Beschl. v. 23.4.1986 (2 BvR 487/80), BVerfGE 73, 261 (269); BVerfG, Beschl. v. 3.10.1979 (1 BvR 726/78), BVerfGE 52, 203 (207); BVerfG, Urt. v. 15.1.1958 (1 BvR 400/57), BVerfGE 7, 198 (206 f.); *Pieroth u.a.*, Grundrechte, 2014, Rn. 195 ff.

[507] BVerfG, Urt. v. 25.2.1975 (1 BvF 1 - 6/74), BVerfGE 39, 1 (41); *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 32; *Murswiek*, Technische Risiken, in: *Westphalen*, Technikfolgenabschätzung, 1997, S. 238 (241); *Hesse*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 1995, Rn. 355; *Pieroth u.a.*, Grundrechte, 2014, Rn. 110; *Sofsky*, Verteidigung des Privaten, 2007, S. 102; *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 188.

[508] BVerfGE, Beschl. v. 19.10.1993 (1 BvR 567 u. 1044/89), BVerfGE 89, 214 (232 f.); BVerfG, Beschl. v. 7.2.1990 (1 BvR 26/84), BVerfGE 81, 242 (261 ff.); *Hermes*, NJW 1990, S. 1764 (1766); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 49 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 405; *Pieroth u.a.*, Grundrechte, 2014, Rn. 198.

[509] *Murswiek*, Technische Risiken, in: *Westphalen*, Technikfolgenabschätzung, 1997, S. 238 (240).

[510] Vgl. C II. 3, S. 68.

[511] BVerfG, Beschl. v. 21.1.2007 (1 BvR 382/05), NVwZ 2007, 805; BVerfG, Beschl. v. 29.11.1995 (1 BvR 2203/95), NJW 1996, 651 (651); BVerfG, Urt. v. 8.8.1978 (2 BvL 8/77), BVerfGE 49, 89 (140 ff.); *Pieroth u.a.*, Grundrechte, 2014, Rn. 110 f.

Subjekt schützende Menschenwürde, als die Annahme einer Bagatelle nahe.[512]

II. Beeinträchtigte Interessen der Betroffenen

1. Schutz der Menschenwürde

Der Schutz der Menschenwürde im Art. 1 Abs. 1 GG ist zugleich das oberste Verfassungsprinzip und das oberste Grundrecht.[513] Es gewährleistet den Schutz des Menschen als Individuum, was in mehreren Theorien weiter ausdifferenziert wird. So betont die „Mitgifttheorie" die Qualitäten, die den Menschen als Subjekt ausmachen, d.h. seine Vernunftbegabtheit, seine Willens- und Entscheidungsfreiheit sowie die Gabe zur rationalen und autonomen Selbstbestimmung.[514] Danach existiert der Mensch als Selbstzweck und nicht als Objekt und Mittel für den Staat oder andere Menschen.[515] Die „Leistungstheorie" sieht die Würde des Menschen in seiner Leistung der Identitätsbildung und Selbstdarstellung.[516] Die „Anerkennungstheorie" versteht die Würde als einen „Kommunikationsbegriff", den sich Menschen innerhalb einer Anerkennungs- und Solidargemeinschaft gegenseitig schulden und gewähren.[517]

Alle drei Theorien zeigen, dass die Menschenwürde die menschliche Qualität als Subjekt und insbesondere die seelische Identität und Integrität schützt.[518] Insoweit decken sich die Schutzziele der Menschenwürde mit den Schutzzielen der Privatsphäre.[519] Allerdings stellt der Schutz der Menschenwürde eine absolute Grenze dar, die zwar abhängig von der

---

[512] Thilo Weichert: „Google Glass ist eine Waffe", heise online, http://www.heise.de/newsticker/meldung/Thilo-Weichert-Google-Glass-ist-eine-Waffe-2176677.html (15.6.2014); *von Gehlen*, Datenbrillen - Werkzeug des Bösen, SZ, http://www.sueddeutsche.de/digital/datenbrillen-werkzeug-des-boesen-1.1871620 (26.1.2014); *Sacasas*, Preserving the Person in the Emerging Kingdom of Technological Force, The Frailest Thing, http://thefrailestthing.com/2014/08/21/preserving-the-person-in-the-emerging-kingdom-of-technological-force/(22.8.2014).

[513] BVerfG, Urt. v. 3.3.2004 (1 BvR 2378/98 u. 1 BvR 1084/99), BVerfGE 109, 279 (149 f.); BVerfG, Beschl. v. 24.4.1986 (2 BvR 1146/85), BVerfGE 72, 105 (115); BVerfG, Urt. v. 21.6.1977 (1 BvL 14/76), BVerfGE 45, 187 (227); BVerfG, Urt. v. 16.1.1957 (1 BvR 253/56), BVerfGE 6, 32 (36); BVerfG, Urt. v. 13.6.1952 (1 BvR 137/52), BVerfGE 1, 332 (343).

[514] Vgl. *Hofmann*, AöR 1993, S. 353 (353 ff.).

[515] Vgl. Ebenda.

[516] *Luhmann*, Grundrechte, 1965, S. 53 ff.

[517] *Hofmann*, AöR 1993, S. 353 (364 ff.).

[518] *Pieroth u.a.*, Grundrechte, 2014, Rn. 371a ff.

[519] Vgl. DII.5, S. 86.

konkreten Situation und dem Kontext bestimmt wird, jedoch keine Eingriffe zulässt.[520] Eingriffe in die Menschenwürde sind schlichtweg verboten und stehen nicht unter einem Gesetzesvorbehalt, sodass eine Abwägung oder Kollision mit anderem Verfassungsrecht insgesamt ausscheidet.[521]

D.h., wenn man die Privatsphäre der Menschenwürde gleichsetzen würde, wäre sie vor jeglichen Eingriffen geschützt. Die Privatsphäre ist jedoch ein dynamisches Freiheitsrecht, was bedeutet, dass sie Eingriffen ausgesetzt sein kann, die sich aus dem Umstand des gemeinschaftlichen Zusammenlebens von Menschen ergeben.[522] Dementsprechend unterscheidet sich der Schutzumfang der Privatsphäre von dem der Menschenwürde. Die Menschenwürde ist verletzt, wenn Menschen die Subjektqualität abgesprochen und sie wie Objekte behandelt werden (sog. „Objektformel“).[523] Das ist der Fall, wenn der Mensch „einer Behandlung ausgesetzt wird, die seine Subjektqualität prinzipiell in Frage stellt [oder in der] eine willkürliche Missachtung der Würde des Menschen liegt.“[524] Dabei steigt der Grad der Willkür, je weniger Transparenz, Teilhabe und sonstige Partizipation einem Menschen zugestanden wird.[525] Die Schutzwirkung der Privatsphäre reicht dagegen viel weiter und umfasst auch mildere Verstöße, wie z.B. die Preisgabe zwar vertraulich geführter, aber die persönliche Entfaltung kaum belastender Informationen.[526] Nur bei erheblichen Eingriffen in die Privatsphäre wird zugleich auch die Menschenwürde beeinträchtigt.[527]

Es ist zwar auch im Rahmen dieser Untersuchung zu prüfen, ob die Menschenwürde verletzt ist. Jedoch wird sich diese Prüfung nur der Über-

---

[520] BVerfG, Beschl. v. 11.3.2003 (1 BvR 426/02), BVerfGE 107, 275 (284); BVerfG, Beschl. v. 10.10.1995 (1 BvR 1476/91), BVerfGE 93, 266 (293); *Pieroth u.a.*, Grundrechte, 2014, Rn. 381.

[521] BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274 (335); BVerfG, Beschl. v. 11.3.2003 (1 BvR 426/02), BVerfGE 107, 275 (284); BVerfG, Beschl. v. 10.10.1995 (1 BvR 1476/91), BVerfGE 93, 266 (293); BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367 (373); *Pieroth u.a.*, Grundrechte, 2014, Rn. 381.

[522] Vgl. DII.4, S. 83.

[523] BVerfG, Urt. v. 15.2.2006 (1 BvR 357/05), BVerfGE 115, 751 (153); BVerfG, Urt. v. 5.2.2004 (2 BvR 2029/01), BVerfGE 108, 133 (149 f.); BVerfG, Beschl. v. 20.10.1992 (1 BvR 698/89), BVerfGE 87, 209 (228).

[524] BVerfG, Urt. v. 15.12.1970 (2 BvF 1/69), BVerfGE 30, 1 (26).

[525] *Pieroth u.a.*, Grundrechte, 2014, Rn. 377 f.

[526] Vgl. D II. 5, S. 86.

[527] BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274 (335); BVerfG, Beschl. v. 12.4.2005 (2 BvR 1027/02), BVerfGE 113, 29 (390 f.).

schreitung dieser Schwelle widmen und daher die dynamischen Aspekte der Privatsphäre nicht hinreichend berücksichtigen. Die Abwägung der Interessen der Nutzer von Smartglasses und der Privatsphäre Dritter muss daher innerhalb eines grundrechtlichen Schutzbereiches verortet werden, der wie die Privatsphäre einer Interessenabwägung zugänglich ist.

2. Allgemeines Persönlichkeitsrecht

Auch wenn die Menschenwürde selbst eine absolute Grenze des Subjektschutzes bildet, heißt dies nicht, dass sie darüber hinaus keine Wirkung entfaltet. Ganz im Gegenteilt strahlt sie auf die anderen Grundrechte insoweit aus, als deren Prüfung immer im Lichte und unter Beachtung des Schutzes der Menschenwürde erfolgen muss.[528]

Eine ganz besondere Beziehung geht der Schutz der Menschenwürde mit dem Schutz allgemeinen Handlungsfreiheit gem. Art. 2 Abs. 1 GG ein. Die allgemeine Handlungsfreiheit ist der äußere Ausdruck der inneren Autonomie eines Menschen und Grundlage seiner selbstbestimmten Lebensführung.[529] Art. 2 Abs. 1 GG ist vor allem ein Mittel, um sich in einer Gesellschaft voller Fremdbilder und fremder Lebensweisen die eigenen Lebensvorstellungen bilden und umsetzen zu können.[530] Anders als die Menschenwürde lässt die allgemeine Handlungsfreiheit Eingriffe in ihren Schutzbereich zu, solange diese gem. Art. 2 Abs. 1 GG „nicht die Rechte anderer", „die verfassungsmäßige Ordnung" oder das Sittengesetz verletzen. D.h., die allgemeine Handlungsfreiheit erlaubt einen Privatsphärenschutz, der sich dynamisch im Rahmen eines Ausgleichs mit den Interessen Dritter bildet. Jedoch schützt Art. 2 Abs. 1 GG, anders als die Privatsphäre, jegliches Handeln und Unterlassen.[531] D.h., während die Menschenwürde über einen viel engeren Schutzbereich als die Privatsphäre verfügt, ist der Schutzbereich des Art. 2 Abs. 1 GG viel weiter, da er auch Handlungen ohne jeglichen Bezug zur Privatsphäre schützt. Folglich ist der Schutz der Privatsphäre in der Schnittmenge der Allgemeinen Handlungsfreiheit gem. Art. 2 Abs. 1 GG und der Menschenwürde gem. Art. 1 Abs. 1 GG zu verorten. Da diese Kombination beider Grundrechte sich jeweils von ihrem ursprünglichen Schutzbereich unterscheidet, wird

---

[528] Vgl. BVerfG, Urt. v. 3.3.2004 (1 BvR 2378/98 u. 1 BvR 1084/99), BVerfGE 109, 279 (310); *Herdegen*, in: *Maunz/Dürig*, GG, Art. 1, Rn. 6 ff.; *Pieroth u.a.*, Grundrechte, 2014, Rn. 84; so im Ergebnis *Weichert*, RDV 2009, S. 154 (158 f.).

[529] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 17, 44.

[530] Ebenda, 39.

[531] St. Rspr., BVerfG, Beschl. v. 23.5.1980 (2 BvR 854/79), BVerfGE 54, 143 (144); BVerfG, Urt. v. 16.1.1957 (1 BvR 253/56), BVerfGE 6, 32 (36); *Jarass*, NJW 1989, S. 857; *Pieroth u.a.*, Grundrechte, 2014, Rn. 386 f.

ihr gewohnheitsmäßig unter der Bezeichnung als „Allgemeines Persönlichkeitsrecht“ eine eigenständige Grundrechtsqualität zugesprochen.[532] Der Schutzbereich des Allgemeinen Persönlichkeitsrechts wird hierbei durch den um die Notwendigkeit eines Bezuges zur Menschenwürde eingeschränkten Schutzbereich der allgemeinen Handlungsfreiheit bestimmt.[533]

Wie die Privatsphäre hat auch das Allgemeine Persönlichkeitsrecht je nach Sach- und Interessenlage im Einzelfall einen unterschiedlich starken Bezug zur Menschenwürde und damit einen unterschiedlich weiten Schutzbereich.[534] Insbesondere hat das Allgemeine Persönlichkeitsrecht, anders als der Schutz der Menschenwürde, nicht den absoluten Schutz des Grundrechtsträgers zum Ziel, sondern dient der „Aufrechterhaltung der Grundbedingungen sozialer Beziehungen zwischen dem Grundrechtsträger und seiner Umwelt“.[535] Damit spiegelt sich das Konzept der Privatsphäre als ein relatives, die Relevanz der sozialen Interaktion und zwischenmenschlicher Beziehungen berücksichtigendes Recht im Allgemeinen Persönlichkeitsrecht wider.[536] Dieser Charakter des Allgemeinen Persönlichkeitsrechts als ein „kommunikativoffenes Freiheitsrecht“ erfährt gerade in der digitalen Welt eine besondere Bedeutung.[537]

---

[532] St. Rspr., BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1196); BVerfG, Urt. v. 11.3.2008 (1 BvR 2074/05, 1 BvR 1254/07), BVerfGE 120, 378 (397); BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (197); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1; BVerfG, Urt. v. 5.6.1973 (1 BvR 536/72), BVerfGE 35, 202; BGH, Urt. v. 23.6.2009 (VI ZR 196/08), BGHZ 181, 328; BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284; BGH, Urt. v. 14.2.1958 (I ZR 151/56), BGHZ 26, 349; BGH, Urt. v. 26.11.1954 (I ZR 266/52), BGHZ 15, 249; *Martin*, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, 2007, S. 236; *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823, Rn. 242.

[533] BVerfG, Beschl. v. 3.6.1980 (1 BvR 185/77), BVerfGE 54, 148 (153); *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 41 ff., 59 ff.; *Jarass*, NJW 1989, S. 857 (858); *Pieroth u.a.*, Grundrechte, 2014, Rn. 391.

[534] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 128; *Wieczorek*, Persönlichkeitsrecht und Meinungsfreiheit im Internet, 2013, S. 52.

[535] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (197); *Herdegen*, in: *Maunz/Dürig*, GG, Art. 1 Abs.1, Rn. 34 f.; *Hofmann*, AöR 1993, S. 353 (364).

[536] Vgl. DII.4, S. 83.

[537] *Mann/Ferenbok*, Surveillance and Society 2013, Vol. 11, Nr. 1/2, p. 18 (27); *Wieczorek*, Persönlichkeitsrecht und Meinungsfreiheit im Internet, 2013, S. 54 ff.

a) Fallgruppen des Allgemeinen Persönlichkeitsrechts

Das Allgemeine Persönlichkeitsrecht ist als ein sog. „Rahmenrecht" offen ausgestaltet, was bedeutet, dass sein Schutzbereich und die Rechtswidrigkeit seiner Verletzung in einer einzelfallbezogenen Güter- und Interessenabwägung zu bestimmen sind.[538] Diese Offenheit des Allgemeinen Persönlichkeitsrechts ist vor allem im Hinblick auf den wissenschaftlich-technischen Fortschritt sowie gewandelte Lebensverhältnisse notwendig, um neuartige Gefährdungen der Persönlichkeitsentfaltung erfassen zu können.[539]

Der Nachteil seiner offenen Definition liegt in der Unschärfe des Allgemeinen Persönlichkeitsrechts, weshalb vor allem in der Literatur versucht wird, dem Grundrecht anhand von Fallgruppen eine Kontur zu geben.[540] Die Fallgruppen sind jedoch nicht als starre Gebilde zu verstehen, sondern als aus dem Allgemeinen Persönlichkeitsrecht hergeleitete Prinzipien, die zwar eine Allgemeingültigkeit für sich beanspruchen, jedoch je nach Situation im Einzelfall Abweichungen erfahren und durch zusätzliche Prinzipien ergänzt werden können.[541] Für die Untersuchung der Beeinträchtigung der Privatsphäre ist zum einen mit dem Schutz des räumlichen und thematischen Rückzugsbereichs die Fallgruppe der Selbstbewahrung maßgeblich.[542] Zum anderen wird mit der Fallgruppe der Selbstdarstellung die Verfügungsgewalt Einzelner an nicht öffentlich gespro-

---

[538] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (380); BGH, Urt. v. 5.12.1958 (IV ZR 95/58), BGHZ 29, 33; BGH, Urt. v. 2.4.1957 (VI ZR 9/56), BGHZ 24, 72 (78); *Nink*, in: *Spindler/Schuster*, Recht der elektronischen Medien, § 823 BGB, Rn. 5; *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823, Rn. 242.

[539] BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274 (303); BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (197 f.); BVerfG, Beschl. v. 16.6.2007 (1 BvR 1550/03), BVerfGE 118, 168 (183 f.); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (380); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (41); BVerfG, Beschl. v. 3.6.1980 (1 BvR 185/77), BVerfGE 54, 148 (153).

[540] *Martin*, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, 2007, S. 253.

[541] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 148; *Ehmann*, JuS 1997, S. 193 (194 f.); *Jarass*, NJW 1989, S. 857 (858 f.); *Martin*, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, 2007, S. 256.

[542] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382); BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367 (373 ff.); BVerfG, Beschl. v. 2.3.1977 (2 BvR 1319/76), BVerfGE 44, 197 (203); BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373; *Pieroth u.a.*, Grundrechte, 2014, Rn. 394 ff.

chenen Worten, am eigenen Bild sowie an personenbezogenen Daten umfasst.[543]

Im Rahmen der nachfolgenden Prüfung des Allgemeinen Persönlichkeitsrechts werden zuerst die einzelnen Schutzbereiche der einschlägigen Fallgruppen herausgearbeitet. Anschließend wird deren Beeinträchtigung geprüft, bevor zuletzt die Rechtfertigung der Eingriffe durch die Interessen der Nutzer von Smartglasses untersucht wird. Da diese Interessen sachlich eng mit der Erhebung von Daten mittels von Smartglasses verbunden sind, wird die Prüfung mit dem Schutz personenbezogener Daten durch das Recht auf informationelle Selbstbestimmung begonnen.

aa) Recht auf informationelle Selbstbestimmung

Das Grundgesetz enthält kein benanntes Recht auf Datenschutz, was dem Umstand geschuldet ist, dass die typischen Probleme einer automatischen Verarbeitung von Daten zum Zeitpunkt dessen Inkrafttretens im Jahr 1949 noch keine große Rolle spielten.[544] Erst vor dem Hintergrund der geplanten Volkszählung wurde durch das Bundesverfassungsgericht mit dem „Recht auf informationelle Selbstbestimmung“ im Jahr 1983 die Funktion der Privatsphäre als informatorisches Verfügungsrecht unter Berücksichtigung der technologischen Entwicklung auf alle personenbezogenen Daten erweitert.[545]

Das Bundesverfassungsgericht sah in dem Kontrollverlust über personenbezogene Daten die Gefahr, dass die betroffene Person als „bloßes Informationsobjekt“ verdinglicht und damit in ihrer Selbstbestimmung als Individuum beeinträchtigt wird.[546] Die Gefahr des Kontrollverlusts sah

---

[543] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (39); BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367 (142); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42 ff.); BVerfG, Urt. v. 5.6.1973 (1 BvR 536/72), BVerfGE 35, 202 (220); BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238; *Pieroth u.a.*, Grundrechte, 2014, Rn. 394 ff.

[544] *Klar*, MMR 2012, S. 788 (54); laut Murswiek ist die Technik im Grundgesetz generell nicht unmittelbar normiert, sondern kommt nur in Formen wie dem Fernmeldegeheimnis oder Komponenten wie Luftverkehr oder Straßenverkehr mittelbar zur Geltung, *Murswiek*, Technische Risiken, in: *Westphalen*, Technikfolgenabschätzung, 1997, S. 238 (238); anders als im GG, ist das Recht auf informationelle Selbstbestimmung in manchen Landesverfassungen ausdrücklich verankert, u.a. im Art. 33 der Verfassung von Berlin oder Art. 11 der Verfassung des Landes Brandenburg, Art. 4 Abs. 2 der Verfassung des Landes Nordrhein-Westfalen.

[545] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 ff.; das Urteil wurde mehrfach bestätigt, BVerfG, Beschl. v. 13.6.2007 (1 BvR 1550/03), BVerfGE 118, 168 (183); BVerfG, Urt. v. 27.7.2005 (1 BvR 668/04), BVerfGE 113, 348 (364). BVerfG, Urt. v. 3.3.2004 (1 BvF 3/92), BVerfGE 110, 33 (53 ff.).

[546] Vgl. BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (48).

das Bundesverfassungsgericht gerade im Hinblick auf die modernen technischen Entwicklungen der automatischen Datenverarbeitung, welche es erlaubten, „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person“ technisch gesehen unbegrenzt zu speichern und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abzurufen.[547] Dadurch könnten Daten „zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann.“[548]

Die Gefahr des unkontrollierten Datenumgangs liegt laut dem Bundesverfassungsgericht vor allem darin, dass der Einzelne nicht überschauen kann, wem welche ihn betreffende Informationen in welchem Umfang bekannt sind.[549] Die Folge ist, dass die Betroffenen sich schon alleine wegen der Möglichkeit der öffentlichen Einsicht- und Einflussnahme auf ihre Persönlichkeit und Verhalten einem psychischen Druck ausgesetzt fühlen könnten.[550] Sie müssten befürchten, dass jegliche Verhaltensweisen, die von den sozialen Normen abweichen, „jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden.“[551] Die Betroffenen wären hierdurch unter dem „Druck der öffentlichen Anteilnahme“ in ihrer Freiheit, „aus eigener Selbstbestimmung zu planen oder zu entscheiden“, wesentlich gehemmt.[552] Anstatt frei zu entscheiden, würden Menschen versuchen, sich möglichst unauffällig zu verhalten und nicht aufzufallen.[553] Daher sollte den Betroffenen mit einem Recht auf informationelle Selbstbestimmung die Möglichkeit gegeben werden, zu erfahren, wer was zu welcher Gelegenheit über sie weiß, um auf Grundlage dieses Vorwissens die eigene Rolle in der Gesellschaft annehmen, herausbilden oder wechseln zu können.[554]

Ferner sollte neben dem individuellen Schutz auch die Mündigkeit der Bürger als Voraussetzung ihrer Teilnahme an einem freiheitlich-demokratischen Gemeinwesen gewahrt werden.[555] Ihre Mündigkeit wäre jedoch nicht gewahrt, wenn Menschen auf die Ausübung von Grundrech-

---

[547] Ebenda, 42.

[548] Ebenda.

[549] Ebenda, 43.

[550] Ebenda, 42.

[551] Ebenda, 43.

[552] Ebenda, 42 f.

[553] Ebenda, 43.

[554] Ebenda.

[555] Ebenda; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 110 f.; *Schnabel*, ZUM 2008, S. 657.

ten, die darauf ausgerichtet sind, die soziale Gemeinschaft von Menschen selbstbestimmt zu gestalten, wie z.B. die Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 1. HS GG oder die Versammlungsfreiheit aus Art. 8 GG, wegen möglicher persönlicher Nachteile der fehlenden Informationskontrolle verzichten würden.[556]

(1) Personenbezug von Daten

Nach der Definition des Bundesverfassungsgerichts setzt die Eröffnung des Schutzbereichs des Rechts auf informationelle Selbstbestimmung einen Umgang mit „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person" voraus.[557]

Eine einheitliche verfassungsrechtliche Definition der sich aus „Einzelangaben", „persönlichen" oder „sachlichen Verhältnissen" sowie der „bestimmten oder bestimmbaren Person" zusammensetzenden Tatbestandstrias existiert nicht. Jedoch decken sich diese Begrifflichkeiten, soweit sie im Rahmen dieser Untersuchung maßgeblich sind, mit der Legaldefinition des Personenbezuges im § 3 Abs. 1 BDSG.[558] Als Einzelangaben gelten demnach Informationen, die sich unmittelbar auf ein bestimmtes Individuum beziehen, wie z.B. Name und Adresse, Angaben zu dessen Aktivitäten, als auch Informationen, über die ein unmittelbarer Bezug zu der Person hergestellt wird, wie z.B. eine Telefonnummer.[559] Dagegen scheidet der Personenbezug von Informationen aus, die sich zwar auf eine einzelne Person beziehen, diese Person jedoch nicht identifizierbar ist, wie im Fall anonymer Daten.[560] Dennoch ist zu bedenken, dass auch diese Angaben jederzeit zu Einzelangaben werden können, wenn der Bezug zu einer konkreten Person hergestellt wird, weil diese

---

[556] Vgl. BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43); die Inanspruchnahme der Grundrechte aus Art. 5 Abs. 1 S.1 1.HS oder Art. 8 GG muss jedoch nicht von den Grundrechtberechtigten als Zweck zur Rechtfertigung der informationellen Selbstbestimmung vorgebracht werden, da die informationelle Selbstbestimmung, entsprechend der Privatsphäre, ein Selbstzweck ist und keiner weiteren positiven Rechtfertigung bedarf, vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 172 ff.

[557] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42); *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 175.

[558] Zur Vergleichbarkeit im einfachen Recht, S. *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 175; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 129.

[559] *Buchner*, in: *Taeger/Gabel*, BDSG, § 3, Rn. 4; *Gola/Schomerus*, BDSG, § 3, Rn. 3; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 5; *Brink/Eckhard*, ZD 2015, S. 205.

[560] *Buchner*, in: *Taeger/Gabel*, BDSG, § 3, Rn. 12; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 23; *Forgó/Krügel*, MMR 2010, S. 17 (20); *Gola/Schomerus*, BDSG, § 3, Rn. 3; Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 15.

z.B. als Mitglied einer Personengruppe gekennzeichnet wird und die Daten auf die Einzelperson „durchschlagen“ können.[561]

Einzelangaben treffen Aussagen über „persönliche“ Verhältnisse einer Person, wenn sie eine konkrete Person selbst betreffen und deren unmittelbaren Identifizierung oder Charakterisierung dienen können (z.B. Fotografien, Name, Anschrift, Geburtsdatum, Erscheinungsbild, Gesundheitszustand, Überzeugungen etc.).[562] Zu persönlichen Verhältnissen gehören ferner Fotografien, Fingerabdrücke als auch die Ansichten und Werturteile einer Person.[563]

Als „sachliche Verhältnisse“ werden dagegen Sachverhalte beschrieben, die Angaben enthalten, die einen Bezug auf eine Person erlauben. Zu diesen Daten gehören auch Angaben zum Aufenthaltsort einer Person, dem Zeitpunkt, an dem sie diesen Ort aufgesucht hat, welche Kleidung sie dabei trug und welche Handlungen sie vornahm.[564] Ebenso stellen Angaben zur Inhaberschaft an bestimmten Gegenständen sachliche Verhältnisse dar.[565]

Von dem Punkt des persönlichen oder sachlichen Verhältnisses ist jedoch die Frage abzugrenzen, ob der Bezug zur Person tatsächlich hergestellt werden kann.[566] Dieses Kriterium findet sich auf der Ebene des einfachen Rechts in dem Tatbestandsmerkmal der „Bestimmbarkeit“ von Daten wieder (s. § 3 Abs. 1 BDSG). Nur wenn mithilfe des Datums ein

---

[561] Für einen solchen "Durchschlag" ist es ausreichend, wenn die Einzelangaben rein statistischer Natur sind, auf Durchschnittswerten beruhende und z.B. Personen als potentielle Interessenten für bestimmten Werbemaßnahmen klassifiziert werden, *Arning/Moos*, ZD 2014, S. 242; *Gola/Schomerus*, BDSG, § 3, Rn. 3.

[562] BGH, Urt. v. 23.6.2009 (VI ZR 196/08), MMR 2009, 608 (613); OLG Hamburg, Urt. v. 18.1.2012 (5 U 51/11), MMR 2012, 605 (606); LG Hamburg, Urt. v. 20.9.2010 (325 O 111/10), MMR 2011, 488; LG Göttingen, Urt. v. 16.11.1978 (2 O 152/78), NJW 1979, 601 (602); *Buchner*, in: *Taeger/Gabel*, BDSG, § 3, Rn. 4 f.; *Gola/Schomerus*, BDSG, § 3, Rn. 6.

[563] BGH, Urt. v. 23.6.2009 (VI ZR 196/08), MMR 2009, 608 (613); OLG Hamburg, Urt. v. 18.1.2012 (5 U 51/11), MMR 2012, 605 (606); LG Hamburg, Urt. v. 20.9.2010 (325 O 111/10), MMR 2011, 488; LG Göttingen, Urt. v. 16.11.1978 (2 O 152/78), NJW 1979, 601 (602); *Gola/Schomerus*, BDSG, § 3, Rn. 6.

[564] *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 7 ff.; die genaue Abgrenzung zwischen "persönlichen" und "sachlichen" Verhältnissen ist nicht immer trennscharf möglich und praktisch auch nicht erforderlich, da es im Hinblick auf die Selbstbestimmung einer Person von keiner Relevanz ist, ob eine Beeinträchtigung von einem persönlichen oder sachlichen Verhältnis ausgeht, *Gola/Schomerus*, BDSG, § 3, Rn. 8; vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 152.

[565] BVerfG, Beschl. v. 24.7.1990 (1 BvR 1244/87), MMR 1990, 1162; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 57; *Weichert*, DuD 2007, S. 17 (20).

[566] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 136.

Bezug zu einer konkreten Person hergestellt werden kann, soll diese einen Schutz erfahren.[567] Die Erheblichkeit des Personenbezugs ist hierbei unabhängig von der Qualität eines Datums anzunehmen, wenn mit dessen Hilfe „weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen, als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können".[568]

Im Fall von Smartglasses ist entsprechend den technischen Möglichkeiten und bisherigen Erfahrungen zu erwarten, dass mit den Geräten vor allem audiovisuelle Daten erhoben und mit weiteren Daten wie dem Standort sowie dem Zeitpunkt der Aufnahmen oder Namen der Betroffenen verbunden werden können. Daneben können auch Sachen im öffentlichen Raum, wie z.B. Hausfassaden oder Kraftfahrzeuge, erfasst werden.

(a) Personenbezug von Personenabbildungen

Die Aufnahme einer Person ist zumindest dann eine Einzelangabe über die persönlichen Verhältnisse einer bestimmten Person, wenn diese anhand ihres äußeren Erscheinungsbildes erkannt werden kann.[569] Dabei gilt im Hinblick auf die Bestimmtheit der Person zumindest derselbe Maßstab wie im § 22 KUG, was bedeutet, dass die Bestimmbarkeit, durch Bekannte und Betroffene erkannt zu werden, ausreichend ist.[570]

Ein Personenbezug kann zum einen abgelehnt werden, wenn die Aufnahme ohne jeglichen kontextualen Bezug zur Person und der Möglichkeit ihrer Erkennung gespeichert wäre.[571] Eine solche Annahme erscheint jedoch in der zunehmend verdateten Welt der Smartglasses als praxisfern,

---

[567] *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 20 ff.

[568] BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274 (312); BVerfG, Beschl. v. 13.6.2007 (1 BvR 1550/03), BVerfGE 118, 168 (184 f.); BVerfG, Beschl. v. 4.4.2006 (1 BvR 518/02), BVerfGE 115, 320 (342); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42); zur Frage der Grenzen der Bestimmbarkeit, vgl. *Bergt*, ZD 2015, S. 365 (365 ff.).

[569] EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196); *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 22; Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 4; *Opel/Körffer/Nouak*, DuD 2013, S. 347 (347 f.).

[570] Wohingegen § 22 KUG im Hinblick auf die Bestimmbarkeit einer Person, nicht entsprechung anwendbar ist, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 150; *Opel/Körffer/Nouak*, DuD 2013, S. 347 (347 f.).

[571] Vgl. *Schnabel*, ZUM 2008, S. 657 (694).

sodass ihr an dieser Stelle nicht weiter nachgegangen wird.[572] Ferner wäre ein Personenbezug der Aufnahme allenfalls dann abzulehnen, wenn z.B. die auf einer Aufnahme erfasste Person aufgrund des Blickwinkels oder der Qualität der Aufnahme, bei Berücksichtigung der technisch und sonst zur Verfügung stehenden Möglichkeiten, gar nicht individualisiert werden kann.[573] Ausreichend ist jedoch, wenn die Person erst nach Vergrößerung von Aufnahmen identifizierbar wird.[574] Denn der weitere Umgang mit den Aufnahmen hängt von der Verfügungsgewalt derjenigen, die Zugriff auf die Aufnahme haben, ab, ohne dass die betroffene Person Einfluss hierauf nehmen kann.[575] Ohnehin sind die vorstehenden Einschränkungen vor dem Hintergrund von Webcams oder ähnlichen Übersichtsaufnahmen getroffen worden, die Personen allenfalls von Weitem erfassen.[576]

Smartglasses enthalten jedoch zum einen Kameras mit einer Auflösung, die mit Smartphone-Kameras vergleichbar ist, also sehr detailreich werden kann.[577] Zum anderen werden die Aufnahmen aus dem Blick der Träger der Smartglasses erstellt, sind also genau das Gegenteil von Übersichtsaufnahmen, sodass im Regelfall von einer hinreichenden Auflösung und damit Erkennbarkeit der Personen auszugehen sein wird. Auch wenn Personen nicht direkt aufgrund ihres Gesichts erkennbar sind, z.B. weil sie mit dem Rücken zu den Smartglasses stehen, so können sie auch aufgrund ihrer körperlichen Konstitution, des Verhaltens und anderer Äußerlichkeiten, wie z.B. wegen des Ganges, der Größe, einer Brille sowie weiterer mitgespeicherter Daten identifiziert werden.[578] Zur Bestimmbarkeit einer Person können vor allem Sachen beitragen, die in Verbindung mit

---

[572] Ebenso nur eine geringe Wahrscheinlichkeit der Erkennung für ausreichend haltend, *Buchner*, in: *Taeger/Gabel*, BDSG, § 3, Rn. 15; ebenso, *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 74; a.A. der bei einer Speicherung eines Templates ohne Zuordnung zu einer Person in einer ausreichend großen Datenbank einen Personenbezug zumindest in Frage stellt, *Hornung*, DuD 2004, S. 429 (430).

[573] *Jahn/Striezel*, K&R 2009, S. 753 (758); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 150; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 153; Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 9; Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 4.

[574] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 29.

[575] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 172.

[576] Ebenda.

[577] Vgl. B II. 2. a), S. 30.

[578] Vgl. BIII.4.b), S. 42; LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1068); *Hilpert*, RDV 2009, S. 160 (162); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 130 ff.; *Röger/Stephan*, NWVBl 2001, S. 243 (243 ff.); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 15.

der Person erfasst werden, wie z.B. Kfz-Kennzeichen oder Namensschilder.[579]

(b) Personenbezug von Sachabbildungen

Sachen können aber auch alleine auf die Individualität einer Person hindeuten und somit dem Schutzbereich des Rechts auf informationelle Selbstbestimmung unterfallen.[580] Der Personenbezug drängt sich auch bei Sachabbildungen auf, bei denen er sich direkt aus den Sachen ergibt, wie es z.B. bei einem Namensschild der Fall ist.[581] Auch bei Kraftfahrzeugkennzeichen (oder ähnlichen Charakteristika, wie z.B. Firmenaufklebern auf einem Auto) wird der Personenbezug aufgrund der Möglichkeit, die Fahrzeughalter zu recherchieren, anzunehmen sein.[582]

Jedoch kann sich nicht aus jedem Sachdatum ein sachliches Verhältnis einer Person ergeben, da die Reichweite des Rechts auf informationelle Selbstbestimmung sonst uferlos wäre.[583] Zur Vertiefung dieses Themenbereichs wird auf die Diskussion um den Personenbezug von Hausfassaden und anderen Sachen im öffentlichen Raum verwiesen, die vor dem Hintergrund von Googles Straßenpanoramen-Dienst „Street View" geführt wird.[584]

(c) Geodaten und sonstige Daten

Neben Personen und Sachabbildungen können Smartglasses weitere Daten, wie z.B. den Standort der Aufnahme oder deren Zeitpunkt, speichern.

---

[579] Im Hinblick auf die Übertragung der Erkennbarkeit gem. § 22 KUG, vgl. LG Essen, Urt. v. 10.7.2014 (4 O 157/14), BeckRS 2014, 17008; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 130 ff.

[580] Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 10; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 59.

[581] *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 61.

[582] *Balzer/Nugel*, NJW 2014, S. 1622 (1625); Halterdaten sind gem. § 39 Abs. 1 StVG gegenüber jedermann bereits bei Darlegung berechtigter Interessen zu übermitteln, vgl. *Buschbaum/Rosak*, ZD 2015, S. 354 (355); a.A. unter der Annahme, dass die die vorgenannte Begründung der Auskunft eine hinreichende Hürde für die Herstellung des Personenbezuges darstellt, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 162.

[583] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 135; *Weichert*, DuD 2007, S. 17 (21).

[584] *Ernst*, CR 2010, S. 178; *Forgó*, MMR 2010, S. 217; *Hoffmann*, CR 2010, S. 514; *Jahn/Striezel*, K&R 2009, S. 753; *Klar*, MMR 2012, S. 788; *Lindner*, ZUM 2010, S. 292; *Moos/Zeiter*, ZD 2013, S. 178; *Spiecker genannt Döhmann*, CR 2010, S. 311; *Weber*, NJOZ 2011, S. 673; *Weichert*, Datenschutzrechtliche Bewertung des Projektes „Google Street View", Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/geodaten/20080930-googlestreetview-bewertung.htm (2.1.2015).

Auch diese Daten können der Bestimmung einer Person dienen und zur Beeinträchtigung ihrer informationellen Selbstbestimmung durch Erleichterung der Identifikation oder durch Herstellung eines benachteiligenden Kontexts, wie z.B. bei Aufnahmen einer krankgeschriebenen Person während der Ausübung von Freizeittätigkeiten, beitragen.[585]

Die besondere Relevanz von Geodaten (auch bezeichnet als Standort- oder Lokalisierungsdaten) für die Persönlichkeitsentfaltung von Menschen ergibt sich aus der Bedeutung von Ortsveränderungen als notwendige Voraussetzung des sozialen Lebens, dem sich Menschen nicht entziehen können.[586] Aus diesem Grund werden Menschen Orte meiden, wenn sie aufgrund der Feststellung ihrer dortigen Anwesenheit negative Folgen erwarten, weshalb die Lokalisierung zu ihrer Verhaltensänderung führen kann.[587] Inwieweit Geodaten personenbezogen sind, wurde wie ebenfalls im Fall von Sachaufnahmen mit Bezug zu Street View-Panoramen diskutiert, worauf an dieser Stelle verwiesen wird.[588] Nach den vertretenen Ansichten handelt es sich bei Geodaten um Einzelangaben über ein sachliches Verhältnis von Personen, wenn sie von der für die Verarbeitung verantwortlichen Stelle dazu bestimmt sind, Personen zugeordnet zu werden oder sie in einem Kontext verarbeitet werden, der „die Identität, die Merkmale oder das Verhalten einer Person betrifft, oder in dem sie verwendet werden soll, um zu beeinflussen, wie die Person behandelt oder beurteilt wird".[589] Ferner muss die Person für die verarbeitende Stelle oder auch jeden Dritten ohne unverhältnismäßigen Aufwand bestimmbar sein.[590] Die Bestimmbarkeit wird sich umso leichter ergeben, je näher die Person an einem Ort lokalisiert wurde, an dem sie regelmäßig verkehrt, wie z.B. dem Wohn- oder Berufsort.[591] Dagegen spricht der Aspekt der Georeferenzierung nur eine untergeordnete Rolle, wenn Personen an Orten aufgenommen werden, die keinen Beitrag zur Identifizierbarkeit der Person leisten.[592]

(2) Umgang mit personenbezogenen Daten

Trotz der Parallelen zu einfachem Recht im Rahmen des Personenzuges darf der Anwendungsbereich der informationellen Selbstbestimmung

---

[585] Vgl. LAG Hamm, Urt. v. 11.7.2013 (11 Sa 312/13), ZD 2014, 204.

[586] *Weichert*, DuD 2007, S. 17 (18).

[587] Ebenda.

[588] *Forgó/Krügel*, MMR 2010, S. 17; *Weichert*, DuD 2009, S. 347.

[589] *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 58; *Forgó/Krügel*, MMR 2010, S. 17 (22 f.).

[590] *Forgó/Krügel*, MMR 2010, S. 17 (22 f.).

[591] *Dammann*, in: *Simitis*, BDSG, § 3 Rn. 69; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 152.

[592] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 152.

nicht auf die Anwendungsbereiche der einfachen Datenschutzgesetze beschränkt werden. Vielmehr muss die Erheblichkeit des Datenumgangs am Schutzzweck des Rechts auf informationelle Selbstbestimmung gemessen werden.[593]

Entsprechend seinem Schutzzweck umfasst das Recht auf informationelle Selbstbestimmung daher jegliche Form des Umgangs mit personenbezogenen Daten, sofern dieser sich auf die durch informationelle Selbstbestimmung geschützte Autonomie des Individuums auswirken kann.[594] In dieser Hinsicht ist der Schutzbereich gerade im Hinblick auf mögliche künftige Entwicklungen im Datenumgang sehr weit gefasst.[595] Der schutzbereichsrelevante Datenumgang umfasst sowohl klassische, durch die Kriterien der Unmittelbarkeit und Finalität geprägte Eingriffe als auch jede Form der „Erhebung, schlichter Kenntnisnahme, Speicherung, Verwendung, Weitergabe oder Veröffentlichung von persönlichen – d.h. individualisierten oder individualisierbaren – Informationen".[596] Damit stellen auch beiläufige Erfassungen von Personen einen Umgang mit personenbezogenen Daten i.S.d. Rechts auf informationelle Selbstbestimmung dar, z.B. wenn eine Person per Zufall in den Erhebungsradius von Smartglasses gerät.[597]

Dabei wird der Eingriff in den Schutzbereich nicht davon abhängig gemacht, ob ein Datum den Bereich der Privat- oder gar Intimsphäre betrifft.[598] Vielmehr kann sich eine Beeinträchtigung der Persönlichkeit durch ein einzelnes Datum unabhängig von der qualitativen Aussagekraft ergeben.[599] Auch der Umgang mit „personenbezogenen Daten, die für sich genommenen nur geringen Informationsgehalt haben, kann je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben."[600] Denn gerade mit der modernen Informationstechnologie kann durch die „Synthese aller verfügbaren Daten über eine Person ein umfassendes Persönlichkeitsprofil erschlossen werden".[601]

---

[593] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 175.

[594] Ebenda, 152.

[595] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42).

[596] M.w.N. in Fn. 19, *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 176.

[597] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 156.

[598] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 176.

[599] Ebenda.

[600] BVerfG, Beschl. v. 13.6.2007 (1 BvR 1550/03), BVerfGE 118, 168 (184 f.); BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274 (312).

[601] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 174.

bb) Recht am eigenen Bild

Das Recht am eigenen Bild wurde bereits vorkonstitutionell als eine Ausprägung des Persönlichkeitsrechts entwickelt und 1907 mit dem Kunsturhebergesetz im einfachen Recht kodifiziert.[602] Nachdem es durch den BGH nachkonstitutionell etabliert wurde, wurde das Recht am eigenen Bild auch vom Bundesverfassungsgericht als ein Teil des Allgemeinen Persönlichkeitsrechts bestätigt.[603]

Schutzgegenstand des Rechts am eigenen Bild ist die Abbildung, also das Bildnis einer erkennbaren Person, als Ausdruck des Wesens ihrer Persönlichkeit unabhängig vom Ort sowie den Umständen der Aufnahme, und es „gewährleistet dem Einzelnen Einfluss- und Entscheidungsmöglichkeiten, soweit es um die Anfertigung und Verwendung von Fotografien oder Aufzeichnungen seiner Person durch andere geht".[604] Dabei nimmt das Bundesverfassungsgericht an, dass es keine „neutralen Abbildungen" gibt, sondern ihnen immer eine latente Missbrauchsgefahr innewohnt.[605] Das Gericht begründet diese besondere Gefährlichkeit mit der „Möglichkeit, das Erscheinungsbild eines Menschen in einer bestimmten Situation von diesem abzulösen, datenmäßig zu fixieren und jederzeit vor einem unüberschaubaren Personenkreis zu reproduzieren".[606]

(1) Bestimmung und Beeinträchtigung des Schutzgegenstandes

Die Erkennbarkeit der Person auf der Abbildung kann sich aus den körperlichen Merkmalen sowie zusätzlichen Informationen, die der Erkennbarkeit dienen, wie dem Namen, Kraftfahrzeugkennzeichen oder Angaben

---

[602] Der Auslöser für die Kodifizierung des Rechts am eigenen Bild im § 22 KUG war die Entscheidung des RG über die heimlich vom verstorbenen Reichskanzler Bismarck erstellte Bildaufnahmen, die sich noch auf ein widerrechtliches Eindringen in ein fremdes Besitztum stützte, RG, Urt. v. 28.12.1899 (VI. 259/99), RGZ 45, 170 (173); nach Erlass des KUG verurteile das RG Persönlichkeitsrechtsverstöße durch unerlaubte Bildveröffentlichung auf der Grundlage des § 22 KUG, RG, Urt. v. 28.10.1910 (II 688/09), RGZ 74, 308 (312 f.); RG, Urt. v. 26.6.1929 (I 97/29), RGZ 125, 80; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 1; *Martin*, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, 2007, S. 191.

[603] BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238 (246); BGH, Urt. v. 14.2.1958 (I ZR 151/56), BGHZ 26, 349.

[604] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (381); BGH, Urt. v. 14.2.1958 (I ZR 151/56), BGHZ 26, 349 (351).

[605] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (381).

[606] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (198); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (381); BVerfG, Beschl. v. 14.7.1994 (1 BvR 1595/92 u. 1606/92), BVerfGE 91, 125.

zur Wohnstätte ergeben.[607] Allerdings ist es für eine Erkennbarkeit der Person nicht ausreichend, wenn lediglich ihre Identität bestimmbar ist (z.B. anhand eines Kraftfahrzeugkennzeichens), die Person selbst aber nicht anhand des Bildes erkannt werden kann.[608] Erst recht sind Abbildungen, auf denen nur Sachen zu sehen sind, nicht vom Schutzbereich des Rechts am eigenen Bild erfasst.[609] Dagegen ist es ausreichend, wenn die Person einen begründeten Anlass hat, innerhalb ihres Bekannten- oder Familienkreises erkannt zu werden.[610] Es kommt also erst recht nicht auf die Erkennbarkeit eines durchschnittlichen Betrachters an.[611] Der Personenkreis muss jedoch „unbeherrschbar" sein, sodass die Erkennbarkeit im engsten Freundes- und Familienkreis i.d.R. nicht ausreichend ist.[612]

Der Verlust der Verfügungsgewalt über eine Abbildung kann sich unterschiedlich auswirken. Zum einen kann sich durch die Reproduktionstechnik die Form der Öffentlichkeit verändern, indem z.B. die überschaubare Öffentlichkeit, in der man sich bewegt, durch die Medienöffentlichkeit ersetzt wird.[613] Zum anderen kann durch den Wechsel des Kontexts der Aufnahme deren Sinngehalt geändert werden.[614] Das Gleiche gilt, wenn die Aufnahme selbst manipuliert wird.[615] Aus diesem Grund ist der

---

[607] Vgl. BGH, Urt. v. 9.12.2003 (VI ZR 373/02), GRUR 2004, 438 (440); BGH, Urt. v. 26.6.1979 (VI ZR 108/78), GRUR 1979, 732 (733); OLG Hamburg, Urt. v. 13.1.2004 (7 U 41/03), ZUM 2004, 309; OLG Nürnberg, Urt. v. 26.10.1971 (3 U 68/71), GRUR 1973, 40; LG Essen, Urt. v. 10.7.2014 (4 O 157/14), BeckRS 2014, 17008 (17008); AG Kerpen, Urt. v. 25.11.2010 (102 C 108/10), BeckRS 2011, 10636; *Dreier/Schulze*, UrhG, vor § 22 KUG, Rn. 4; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 24; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 7; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 116 ff.

[608] So mangelt es an der Erkennbarkeit, wenn alleine ein Autokennzeichen auf die Person hinweist, sie aber auf der Abbildung nicht mal an ihren Körperkonturen erkennbar ist, AG Kerpen, Urt. v. 25.11.2010 (102 C 108/10), BeckRS 2011, 10636.

[609] *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 21; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 65.

[610] BGH, Urt. v. 1.12.1999 (I ZR 49/97), BGHZ 143, 214; BGH, Urt. v. 26.6.1979 (VI ZR 108/78), GRUR 1979, 732 (733); OLG Nürnberg, Urt. v. 26.10.1971 (3 U 68/71), GRUR 1973, 40 (41); *Dreier/Schulze*, UrhG, § 22 KUG, Rn.3.

[611] BVerfG, Beschl. v. 14.7.2004 (1 BvR 263/03), NJW 2004, 3619 (3620).

[612] LG Köln, Urt. v. 3.11.2004 (28 O 731/03), ZUM-RD 2005, 351 (353); AG Kerpen, Urt. v. 25.11.2010 (102 C 108/10), BeckRS 2011, 10636.

[613] Das Gericht weist beispielhaft auf den Unterscheid zwischen der Wahrnehmung eines Gerichtsfverfahrens in seiner Gesamtheit durch anwesende Beteiligte und einer durch das Fernsehen hergestellten Medienöffentlichkeit, hin, BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (381).

[614] Ebenda, 381 f.

[615] Vgl. Ebenda, 382.

Schutzbereich des Allgemeinen Persönlichkeitsrechts auch dann eröffnet, wenn die Abbildung nicht im privaten Bereich, sondern in der Öffentlichkeit erfolgt.[616]

(2) Abgrenzung vom Recht auf informationelle Selbstbestimmung

Wird durch Smartglasses eine Person aufgezeichnet, kann die Aufnahme als Bildnis sowohl dem Schutzbereich des Rechts am eigenen Bild als auch als ein personenbezogenes Datum dem Schutzbereich des Rechts auf informationelle Selbstbestimmung unterfallen. Es stellt sich daher die Frage, in welchem Verhältnis die beiden Schutzrechte zueinander stehen. In der Literatur sowie der Rechtsprechung wird dazu überwiegend vertreten, dass das Recht am eigenen Bild einschlägig ist, wenn es um die Veröffentlichung oder Verbreitung von Bildnissen geht, auch wenn diese nicht in körperlicher, sondern in Datenform stattfindet.[617]

Diese Spezialität wird damit begründet, dass das Recht am eigenen Bild in seiner Schutzrichtung den Gefahren des Verfügungsverlustes vorbeugen soll, wenn das Erscheinungsbild von Menschen abgelöst, fixiert und reproduzierbar wird, sodass es in die Öffentlichkeit gebracht oder in einen falschen Kontext gestellt werden kann.[618] Das Recht auf informationelle Selbstbestimmung soll dagegen den Gefahren eines unkontrollierbaren Datenumgangs vorbeugen, die sich insbesondere aus der Speicherung und Verschneidung von Daten und Erstellung von Persönlichkeitsprofilen im Rahmen automatischer Datenverarbeitungsvorgänge ergeben.[619]

Die Spezialisierung des Rechts am eigenen Bild auf die Fälle der Verbreitung und Veröffentlichung von Bildnissen darf jedoch nicht dazu führen, dass Schutzlücken im Allgemeinen Persönlichkeitsrecht entste-

---

[616] Ebenda, 381.

[617] EGMR, Urt. v. 7.2.2012 (40660/08 u. 60641/08), ZUM 2012, 551 (557 ff.); BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07, 1606/07 u. 1626/07), BVerfGE 120, 180 (202 ff.); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (380 ff.); BAG, Urt. v. 11.12.2014 (8 AZR 1010/13), ZUM 2015, 604 (606); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 152; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 12; zum Teil wird jedoch vertreten, dass das Recht am eigenen Bild ein Unterfall, bzw. eine Konkretisierung des Rechts auf informationelle Selbstbestimmung ist und die Verletzung des Rechts am eigenen Bild wird als dessen Nebenerscheinung geprüft, BVerfG, Beschl. v. 23.2.2007 (1 BvR 2368/06), NVwZ 2007, 688 (690 f.); BGH, Urt. v. 14.5.1991 (1 StR 699/90), NJW 1991, 2651; BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); *Büllesfeld*, Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze, 2002, S. 129; *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 193; *Jahn/Striezel*, K&R 2009, S. 753 (759); *Kloepfer/Breitkreutz*, DVBl 1998, S. 1149 (1150 f.); *Schnabel*, ZUM 2008, S. 657 (658).

[618] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07, 1606/07 u. 1626/07), BVerfGE 120, 180 (198); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (381 f.).

[619] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (48 ff.); BVerfG, Beschl. v. 16.7.1969 (1 BvL 19/63), BVerfGE 27, 1 (6).

hen.[620] Das bedeutet, dass sowohl das Recht auf informationelle Selbstbestimmung als auch das Recht am eigenen Bild in Frage kommen, wenn ein einheitlicher Lebenssachverhalt die spezielleren Schutzrichtungen beider Grundrechte berührt.[621]

cc) Recht am nicht öffentlich gesprochenen Wort

Die geschützte Vertraulichkeit des nicht öffentlich gesprochenen Wortes gewährt jedermann als Grundlage der autonomen Persönlichkeitsentfaltung die „Garantie einer ungestörten zwischenmenschlichen Kommunikation" unabhängig von deren Ernsthaftigkeit, Tiefe, Qualität und Effektivität.[622]

(1) Das gesprochene Wort als Schutzgegenstand

Jeder Einzelne soll unbefangen und frei von Argwohn und Misstrauen mit anderen Menschen kommunizieren können, ohne die Befürchtung haben zu müssen, dass vertrauliche Gespräche aufgezeichnet und später veröffentlicht oder gegen ihn verwendet werden können.[623] Insbesondere soll jeder Mensch selbstbestimmt entscheiden können, ob das von ihm Gesagte lediglich von einzelnen Personen, einem Personenkreis oder der Öffentlichkeit vernommen wird.[624] Das gilt auch, wenn die Aufzeichnung des Gesprochenen mittels handelsüblicher Geräte und keiner speziellen Abhöreinrichtung i.S.d. § 201 Abs. 2 Nr. 1 StGB erfolgt.[625]

Der Schutz erstreckt sich auch auf beiläufig aufgezeichnete Gesprächsfragmente, wie einzelne Wort- oder Satzfetzen eines nicht öffentlichen Gesprächs, sofern diese über bloße Laute hinausgehen, die für sich keine

---

[620] Vgl. BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (380); vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 69 f.

[621] So im Ergebnis *Golla/Herbort*, GRUR 2015, S. 648 (651); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 70 f.

[622] BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (286); *Di Fabio*, in: *Maunz/Dürig*, GG, Art.2, Rn. 196; im Hinblick auf den Schutz der Privatsphäre unterscheidet sich der Schutz des Rechts am nichtöffentlich gesprochenem Wort insoweit, als er unabhängig von dem Inhalt und dem Vorliegen eines räumlichen Rückzugsbereichs entsteht, BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (41).

[623] St. Rspr., BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (39); BVerfG, Beschl. v. 19.12.1991 (1 BvR 382/85), NJW 1992, 815; BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238; BGH, Urt. v. 10.3.1987 (VI ZR 244/85), NJW 1987, 2667; BGH, Urt. v. 16.3.1983 (2 StR 775/82), NJW 1983, 1569; BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277; BGH, Urt. v. 14.6.1960 (1 StR 683/59), NJW 1960, 1580; BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284; *Di Fabio*, in: *Maunz/Dürig*, GG, Art.2, Rn. 196.

[624] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (39 f.); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (286).

[625] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (44).

Rückschlüsse auf eine bestimmte Kommunikation erlauben.[626] Denn gerade aus der Aufzeichnung und Wiedergabe einzelner Gesprächsphasen kann sich die Beeinträchtigung des Persönlichkeitsrechts des Sprechers ergeben, wenn die Gesprächsphasen aus dem äußeren und inneren Kontext des Gesprächs herausgelöst werden und in einem anderen Kreis und anderer Situation wiedergegeben werden können.[627]

Auf die Qualität der Gespräche, d.h. besonderen privaten Bezug oder Sensibilität der Inhalte, kommt es für die Eröffnung des Schutzbereichs nicht an.[628] Denn die Bedeutung einzelner Inhalte kann erst im Verlauf des Gesprächs oder in dessen Anschluss eine beeinträchtigende Bedeutung erlangen.[629] Ebenso ist der Schutzbereich nach der neueren Ansicht des Bundesverfassungsgerichts nicht auf bestimmte Arten nicht privater Kommunikationen beschränkt und daher sind auch geschäftliche Unterhaltungen, wenn auch nicht im gleich hohen Umfang wie Privatgespräche, geschützt.[630]

(2) Kriterium der Öffentlichkeit der Kommunikation

Ob eine Kommunikation nicht öffentlich ist, kann nur anhand der berechtigten Erwartungshaltung ihrer Teilnehmer bestimmt werden, die „aufgrund der Rahmenbedingungen begründetermaßen" erwarten dürfen, nicht von Dritten gehört zu werden.[631] So ist eine Kommunikation auch dann öffentlich, wenn deren Teilnehmer Mithörer in ihrer Nähe übersehen oder ihre Lautstärke falsch einschätzen.[632] Umgekehrt kann alleine aus dem Umstand, dass eine Kommunikation im öffentlichen Raum stattfindet, nicht darauf geschlossen werden, dass es den Kommunikationsteilnehmern gleichgültig sei, wer sie mithören kann.[633] Anders als z.B. im Fall visueller Wahrnehmung, ist die akustische Wahrnehmung räumlich

---

[626] Jedoch kann auch die Aufnahme einzelner Laute wie Seufzen oder Schluchzen einen Eingriff in die räumliche oder thematische bestimmte Privatsphäre begründen, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 130.

[627] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (44); BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238 (246); BGH, Urt. v. 10.3.1987 (VI ZR 244/85), NJW 1987, 2667 (2668); BGH, Urt. v. 14.6.1960 (1 StR 683/59), NJW 1960, 1580 (1581); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (287 f.).

[628] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (33).

[629] Ebenda, 41.

[630] Ebenda, 33; BVerfG, Beschl. v. 19.12.1991 (1 BvR 382/85), NJW 1992, 815 (f.); BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238 (248 ff.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 129.

[631] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (40 ff.).

[632] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 129.

[633] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (41).

beschränkt. Daher kann auch bei Gesprächen, die bei angepasster Stimmlautstärke und hinreichendem Abstand an einsehbaren und von Dritten frequentierten Orten geführt werden, berechtigterweise deren Vertraulichkeit angenommen werden kann.[634] Dagegen gilt die Kommunikation als öffentlich, wenn die Teilnehmer sich so verhalten, dass ihre Worte „von unbestimmt vielen Menschen ohne besondere Bemühungen gehört werden können".[635] In diesem Fall haben sich die Kommunikationsteilnehmer das Zuhören Dritter „selbst zuzuschreiben".[636]

Der Annahme der Vertraulichkeit steht jedoch nicht entgegen, dass Betroffene Smartglasses als solche und damit die Möglichkeit einer Aufzeichnung erkennen können. So lässt laut dem Bundesverfassungsgericht die faktische Verbreitung von Mithöreinrichtungen nicht per se darauf schließen, dass mit einem Mithören zu rechnen ist, wenn die Mithöreinrichtung für andere Zwecke, z.B. im Fall von Telefonen zum freihändigen Telefonieren, verwendet werden kann.[637] Dies gilt auch für Smartglasses, die zwar zum freihändigen Telefonieren ebenso wie zur Aufzeichnung von Stimmen eingesetzt werden können, dies jedoch nur optional erfolgt. Würden sich die Smartglasses jedoch in einem Live-Streaming-Modus befinden und wäre dies dem Sprecher bekannt, dann dürfte er sich nicht auf die Nichtöffentlichkeit des Gesprächs berufen.

dd) Das Recht der Selbstbewahrung

Das Recht der Selbstbewahrung spiegelt die klassischen Privatsphärenfunktionen wider, indem es jedermann die Freiheit gewährt, sich zurückziehen, für sich alleine bleiben und sich vor fremder Einflussnahme abschirmen zu dürfen.[638] Die so geschützte Privatsphäre ist sowohl als ein

---

[634] Ebenda.

[635] Ebenda, 40.

[636] Ebenda.

[637] Ebenda, 45 f.; vor diesem Hintergrund erscheinen frühere Rechtsprechung des BGH, wonach der mit dem Mithören durch Dritte über ein Mithörapparat oder einen Lautsprecher zu rechnen sei, wenn ein Ferngespräch von einem im Geschäftszimmer eines Kaufmanns stehenden Fernsprechapparat aus geführt wird, als überholt, BGH, Urt. v. 21.10.1963 (AnwSt (R) 2/63), NJW 1964, 165 (166); dasselbe gilt, wenn ein geschäftliches Gespräch aus einem Hotelzimmer geführt wird, weil wegen der Verbreitung der Mithöreinrichtungen und keines aktiven auf Täuschung angelegten Verhaltens, Mithörer angenommen werden müssen, BGH, Urt. v. 17.2.1982 (VIII ZR 29/81), NJW 1982, 1397 (1398).

[638] BVerfG, Beschl. v. 2.3.1977 (2 BvR 1319/76), BVerfGE 44, 197 (203); BVerfG, Beschl. v. 3.10.1969 (1 BvR 46/65), BVerfGE 27, 71 (6); *Pieroth u.a.*, Grundrechte, 2014, Rn. 394 f.

räumlicher wie auch als ein sozial-thematischer Rückzugsbereich zu verstehen.[639]

(1) Räumlich bestimmte Privatsphäre

Die durch das Recht der Selbstbewahrung geschützte Privatsphäre umfasst räumliche Bereiche, die dem Einzelnen dazu dienen, zu sich zu kommen, sich zu entspannen oder auch sich gehen zu lassen.[640] Dieses Recht auf Einsamkeit, Recht, sich „sich selbst zu besitzen", sich zurückzuziehen und „in Ruhe gelassen" zu werden, ist für eine freie Entfaltung der Persönlichkeit essentiell.[641] Dementsprechend werden räumliche Rückzugsbereiche auch rechtlich als notwendig betrachtet, da das Gefühl, von Dritten möglicherweise beobachtet zu werden, einen „psychischen Druck […] öffentlicher Anteilnahme" ausübt, der zu einer erzwungenen Selbstkontrolle des Einzelnen führen kann.[642]

Der räumliche Schutzbereich der Privatsphäre ist nicht nur auf den häuslich-familiären Bereich beschränkt und setzt nicht zwingend eine Abgrenzung durch Hausmauern oder Grundstücksgrenzen voraus.[643] Vielmehr ist der räumliche Schutz abhängig von dem Ort, der Zeit und der konkreten Situation im Einzelfall, anhand des Willens der betroffenen Person und sowie der äußeren Umstände zu bestimmen.[644] Ausschlaggebend ist, „ob der Einzelne eine Situation vorfindet oder schafft, in der er begründetermaßen und somit auch für Dritte erkennbar davon ausgehen darf, den Blicken der Öffentlichkeit nicht ausgesetzt zu sein."[645] Dagegen ist es nicht ausreichend, dass die Person sich subjektiv unbeobachtet fühlt, während der Raum ihr tatsächlich keinen Privatsphärenschutz bie-

---

[639] BGH, Urt. v. 29.10.2009 (I ZR 65/07), NJW-RR 2010, 855 (855 ff.); BGH, Urt. v. 19.12.1995 (VI ZR 15/95), NJW 1996, 1128 (1129); BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367 (373 ff.); BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373 (379).

[640] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382 f.).

[641] Vgl. D I. 3, S. 75; Ebenda, 383; BVerfG, Beschl. v. 16.7.1969 (1 BvL 19/63), BVerfGE 27, 1 (6 f.).

[642] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (383); BVerfG, Beschl. v. 16.7.1969 (1 BvL 19/63), BVerfGE 27, 1 (6 f.).

[643] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (199); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (383).

[644] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (384 ff.).

[645] EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051 (1052 ff.); BVerfG, Beschl. v. 2.5.2006 (1 BvR 507/01), NJW 2006, 2836 (2837); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (384); BGH, Urt. v. 19.12.1995 (VI ZR 15/95), NJW 1996, 1128 (1129); vgl. Einzelfälle in, Dreier/Schulze in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn.22 ff.

tet.[646] Dabei gibt es Bereiche, in denen typischerweise mit einer optisch-elektronischen und akustischen Erfassung nicht gerechnet wird, wie z.B. in Arztpraxen, Toiletten oder dem Umkleidebereich eines Kaufhauses.[647] Dazu gehören ferner auch Rückzugsorte in einem Restaurant.[648] Die Umschlossenheit eines Raums kann hierbei als ein Indiz dienen, ist aber nicht zwingend, da z.B. auch ein nur per Boot erreichbarer Strand einen Rückzugsbereich konstituieren kann.[649] Umgekehrt bieten sowohl umschlossene Räume als auch öffentliche Plätze, innerhalb derer man sich unter den Augen vieler Personen bewegt, keinen Privatsphärenschutz.[650]

Die Möglichkeit, beobachtet zu werden, muss zudem für die beteiligten Personen erkennbar sein und nicht nur objektiv vorliegen, da die heutigen Aufnahmetechniken die räumliche Abgeschiedenheit unbemerkt überwinden können.[651] Zu bedenken ist jedoch, dass die Verbreitung von Smartglasses im öffentlichen Raum dazu führen kann, dass praktisch überall mit ihnen zu rechnen sein könnte und so das Vertrauen in die räumliche Abgeschiedenheit immer seltener eine Berechtigung fände.[652]

(2) Inhaltlich bestimmte Privatsphäre

Der Schutz der inhaltlich bzw. thematisch bestimmten Privatsphäre umfasst Angelegenheiten, deren Gegenstand oder Informationsgehalt Sachverhalte betrifft, die typischerweise als privat gelten.[653] Dazu gehören insbesondere Aspekte, deren „öffentliche Erörterung als unschicklich gilt, deren Bekanntwerden als peinlich empfunden oder nachteilige Reaktionen

---

[646] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (383 ff.).

[647] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 141; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 40 ff.; m.w.N. *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 31

[648] BVerfG, Urteil v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (368); *Taeger*, ZD 2013, S. 571 (574).

[649] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (384).

[650] Ebenda; LG Hamburg, Urt. v. 8.5.1998 (324 O 736/97), ZUM 1998, 852 (859).

[651] Vgl. BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (384).

[652] Vgl. zu einem solchen "Verlust der Privastphäre", *Brin*, The Transparent Society, 1999, S. passim; *Heller*, Post Privacy, 2011, passim; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 262; *Lyon*, Surveillance Studies, 2007, S. 176; *Schaar*, Das Ende der Privatsphäre, 2007, passim.

[653] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (199); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382); BVerfG, Beschl. v. 5.2.1981 (2 BvR 646/80), BVerfGE 57, 170 (211 ff.); BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373 (380 f.).

der Umwelt“ für die betroffene Person auslösen kann.[654] Dazu gehören vor allem Umstände, die zum Gefühl der Scham führen können, welches als das Gefühl des Privaten schlechthin gilt.[655] Zu diesen Angelegenheiten gehören insbesondere die vertrauliche Kommunikation unter Eheleuten,[656] Bereiche der Sexualität,[657] Krankheiten[658] oder auch sozial abweichendes Verhalten.[659] Würden diese Angelegenheiten nicht vor der unbefugten Kenntniserlangung durch Dritte geschützt sein, wären grundrechtlich geschützte Verhaltensweisen, wie die Auseinandersetzung mit sich selbst, die unbefangene Kommunikation unter Nahestehenden, die sexuelle Entfaltung oder die Inanspruchnahme ärztlicher Hilfe, beeinträchtigt oder unmöglich.[660]

ee) Recht auf Anonymität

Die Anonymität wird im Schrifttum vereinzelt als ein eigenes allgemeingültiges negatives Recht aufgefasst, das dazu berechtigt, eine Fremdvorstellung von der eigenen Person nicht zu erzeugen, also auf eine Selbstdarstellung zu verzichten.[661] Dies ist zwar zutreffend, da auch die Anonymität ein Zweck der Privatsphäre ist. Jedoch findet sich Anonymität, als ein Recht auf Nichtdarstellung in der Öffentlichkeit, bereits in anderen Rechten der Selbstdarstellung und Selbstbestimmung wieder.[662] So ist die Anonymität eine Methode zum Schutz der informationellen Selbstbestimmung, indem sie der Herstellung des Personenbezugs entgegengesetzt werden kann (vgl. § 3 Abs. 6 BDSG).[663] Auch die anderen Fallgruppen des Allgemeinen Persönlichkeitsrechts, wie das Recht am eigenen Bild oder der Schutz des nicht öffentlich gesprochenen Wortes, können

---

[654] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382); BGH, Urt. v. 28.10.2008 (VI ZR 307/07), BGHZ 178, 213; BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367; BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373.

[655] *Sofsky*, Verteidigung des Privaten, 2007, S. 59.

[656] BVerfG, Beschl. v. 15.1.1970 (1 BvR 13/68), BVerfGE 27, 344.

[657] BVerfG, Beschl. v. 11.10.1978 (1 BvR 16/72), BVerfGE 49, 286; BVerfG, Beschl. v. 21.12.1977 (1 BvL 1/75), BVerfGE 47, 46.

[658] BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373; LG Essen, Urt. v. 10.7.2014 (4 O 157/14), BeckRS 2014, 17008; AG Mannheim, Urt. v. 11.7.2008 (3 C 154/08), BeckRS 2008, 13697.

[659] BVerfG, Beschl. v. 24.5.1977 (2 BvR 988/75), BVerfGE 44, 353.

[660] BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382).

[661] *Bizer*, Das Recht auf Anonymität, in: *Bäumler/Mutius*, Anonymität im Internet, 2003, S. 78 (78 f.); *Bökel*, Das Recht auf Anonymität in der Diskussion, in: *Bäumler/Mutius*, Anonymität im Internet, 2003, S. 191 (192 f.)

[662] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 175 f.

[663] *Härting*, NJW 2013, S. 2065.

einen Anspruch auf Anonymität begründen, indem sie z.B. die Veröffentlichung von Abbildungen oder Sprachaufzeichnungen von Teilnehmern einer Kommunikation verhindern. Aus diesem Grund brächte die Anonymität als ein eigenes Recht keine zusätzlichen Vorteile gegenüber der bisherigen Nomenklatur des Privatsphärenschutzes. D.h., die Anonymität ist nicht selbstständig, sondern im Rahmen der Prüfung der Verletzung bisheriger Fallgruppen des Allgemeinen Persönlichkeitsrechts zu berücksichtigen.

b) Beeinträchtigung des Allgemeinen Persönlichkeitsrechts durch Smartglasses

Nach der Festlegung des Schutzbereichs des Allgemeinen Persönlichkeitsrechts muss dessen Beeinträchtigung durch die typischen Arten der Nutzung von Smartglasses geprüft werden.[664] Dabei drängt sich ein solcher Eingriff angesichts der Möglichkeiten jederzeitiger Aufnahme von Personen, der Verarbeitung ihrer Daten sowie der Einschüchterungswirkung von Smartglasses geradezu auf.

aa) Aufnahme und Speicherung

Bei einer Aufnahme werden die durch die Smartglasses elektronisch, visuell und akustisch erfassten Daten innerhalb des Gerätes oder auf ausgelagerten Servern (sog. „Cloud-Servern“)[665] gespeichert und so einer Reproduktion oder anschließenden Auswertung zugänglich gemacht. Können anhand der Aufnahme Personen identifiziert werden, wird es sich dabei insgesamt um einen Umgang mit personenbezogenen Daten und damit zugleich um einen Eingriff in das Recht auf informationelle Selbstbestimmung der Person handeln.[666] Sind die Personen auf den Aufnahmen erkennbar oder werden vertrauliche Gespräche aufgezeichnet, liegt zugleich ein Eingriff in deren Recht am eigenen Bild oder den Schutz des nicht öffentlich gesprochenen Wortes vor, da die Betroffenen mit den Aufzeichnungen die Kontrolle über ihre Bildnisse und die gesprochenen Worte verlieren. Ferner kann je nach Situation und Inhalt der Aufnahme die räumliche oder die inhaltlich bestimmte Privatsphäre verletzt werden, bzw. beide zusammen, wenn z.B. eine Person in einer Umkleidekabine unbekleidet aufgenommen wird.[667]

---

[664] Vgl. BIII, S. 35.

[665] Vgl. zu Cloud-Diensten, *Federrath*, ZUM 2014, S. 1 (1 f.); *Gabel*, in: *Taeger/Gabel*, BDSG, § 11, Rn. 18; *Geis*, ZD 2013, S. 591 (592); *Schulz*, MMR 2010, S. 75.

[666] Vgl. E II. 2. a) aa) (1), S. 98.

[667] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 142.

bb) Übertragung und Veröffentlichung von Aufnahmen

Ein Eingriff in das Recht am eigenen Bild liegt nach einhelliger Meinung dann vor, wenn die Abbildung einer erkennbaren Person veröffentlicht, also einem unbestimmten Personenkreis zur Verfügung gestellt oder verbreitet wird.[668] Unter einer Verbreitung ist eine Zurverfügungstellung der Aufnahme für Dritte oder deren Vervielfältigung zu verstehen, die eine Gefahr einer nicht mehr zur kontrollierenden Möglichkeit der Kenntnisnahme Dritter schafft.[669] Auf den Zweck und die Motivation der Verbreitungs- und Veröffentlichungshandlungen kommt es nicht an.[670] Damit wird es sich bei den typischen Übertragungen von Bildern an Freunde um eine Beeinträchtigung des hier speziell anwendbaren Rechts am eigenen Bild bzw. des Rechts am nicht öffentlich gesprochenen Wort handeln.[671] Das wird erst recht der Fall sein, wenn die Aufnahmen im Internet jedermann zugänglich gemacht werden.[672] Werden personenbezogene Daten übertragen, was z.B. bei Personenaufnahmen im Regelfall anzunehmen sein wird, wird es sich hierbei zugleich um einen Eingriff in das Recht auf informationelle Selbstbestimmung handeln.

cc) Live-Streaming

Beim Live-Streaming mittels Smartglasses wird die Aufnahme nicht dauerhaft fixiert, sondern in Echtzeit an Dritte übermittelt. Im Hinblick auf den Inhalt der beeinträchtigten Informationen unterscheidet sich der Vorgang nicht von einer Aufzeichnung, da dieselben Daten lediglich weitergeleitet statt gespeichert werden. Im Wesentlichen ähnelt die Live-Übertragung einer Verbreitung von Aufnahmen, da sie Dritten auch die Möglichkeit der Verfügungsgewalt über die abgebildeten Personen oder Sachen verschafft. Denn diese können die übermittelten Inhalte z.B. im Wege einer Bildschirmaufnahme oder eines Bildschirmvideos aufzeich-

---

668 BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07, 1606/07 u. 1626/07), BVerfGE 120, 180 (198); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (381); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 66; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 9; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 131.

669 *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 9; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 8.

670 *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 9 f.

671 OLG Frankfurt a.M., Urt. v. 15.6.2004 (11 U 5/04), ZUM-RD 2004, 576 (578); LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14), n.v.; LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 9; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 53; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 8; Ebenda, 120 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 348 ff.

672 *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 121.

nen.[673] Dadurch können die Abbildungen Betroffener, ohne dass dies für sie zu erkennen ist, dauerhaft fixiert werden.[674]

Der Unterschied zur Verbreitung liegt lediglich darin, dass Live-Streaming der Natur nach flüchtiger ist und die Wahrscheinlichkeit einer Aufzeichnung und damit Identifizierung von z.B. schnell vorbeigehenden Personen je nach Situation gering sein kann.[675] Dieser Umstand mag sich zwar auf die Intensität eines Eingriffs auswirken, lässt ihn jedoch nicht entfallen. Wird die Live-Übertragung einer Vielzahl von Personen zur Verfügung gestellt, so erhöht bereits Anzahl der möglichen Zuschauer die Wahrscheinlichkeit der Erkennung einer Person.[676] Ferner werden auch für eine Live-Übertragung Infrastrukturen Dritter verwendet, die zumindest Zugriffe auf die zwischengespeicherten Daten bei den Infrastrukturanbietern oder auf Datenströme durch Dritte möglich machen. So ist es bekannt, dass z.B. Geheimdienste unterschiedlicher Länder nicht nur auf die bei Anbietern gespeicherten Daten, sondern direkt auf die Dateninfrastruktur, wie z.B. Datenknoten, zugegriffen haben.[677]

dd) Biometrische Verfahren

Der Gegenstand eines biometrischen Verfahrens ist der Umgang mit biometrischen Daten, d.h. mit biologischen Eigenschaften einer Person, wie z.B. ihren physiologischen Charakteristika, d.h. der Gesichtsform und den Gesichtszügen, oder reproduzierbaren Handlungen, wie dem Gang oder der Sprechweise.[678] Entsprechend der technischen Darstellung müssen die einzelnen Stufen der biometrischen Verfahren rechtlich gesondert betrachtet werden.[679] Zu den Verfahrensstufen gehören die Aufnahmen von Personen, die Herstellung biometrischer Templates durch Extraktion

---

673 Vgl. *Hilgert/Hilgert*, MMR 2014, S. 85 (87 f.); ein Vergleich mit einem "verlängerten Auge" oder einem Fernglas, wie es im Fall von Überwachunsganlagen ohne Aufzeichnungsmöglichkeit zum Teil angestellt wurde, scheidet daher ebenfalls aus, vgl. *Kloepfer/Breitkreutz*, DVBl 1998, S. 1149 (1152); *Roggan*, NVwZ 2001, S. 134 (135 f.).

674 Sollte eine anschließende Veröffentlichung oder Verbreitung des Bildes erfolgen, würde diese keine neue, sondern die Vertiefung eines bereits vorhandenen Eingriffs darstellen, *Wanckel*, Persönlichkeitsschutz in der Informationsgesellschaft, 1999, S. 183 ff.

675 Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 151.

676 Ebenda, 152 ff.

677 MMR-Aktuell, NSA-Ausschuss: Mängel beim BND-Datenschutz, 2014, Nr. 04356; NSA-Affäre Bericht, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/politik/nsa-affaere-bericht-bnd-leitete-abgezapfte-daten-an-amerikaner-weiter-13011564.html (23.1.2015).

678 Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 01248/07/DE, 2007, S. 9; *Busch*, DuD 2013, S. 386; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 10; *Scholz*, in: Ebenda, § 6b, Rn. 15 f.

679 *Hornung*, DuD 2004, S. 429 (429 ff.); *Karg*, HFR 2012, S. 120 (121 f.).

der biometrischen Merkmale aus den Aufnahmen und der Einsatz von biometrischen Templates für Abgleichzwecke.

(1) Erstellung von Personenaufnahmen

Die Herstellung von Personenaufnahmen stellt grundsätzlich einen Eingriff in das Allgemeine Persönlichkeitsrecht dar. Jedoch könnte ein Eingriff entfallen, wenn die Aufnahmen nur flüchtig für die Zwecke des biometrischen Verfahrens gespeichert und danach sofort gelöscht werden würden.

So liegt nach Ansicht des Bundesverfassungsgerichts keine Persönlichkeitsrechtsbeeinträchtigung bei einem polizeilichen Kennzeichenabgleich vor, bei dem die Aufnahmen von Kraftfahrzeugen im Fall von „Nichttreffern" sofort gelöscht werden.[680] Lediglich bei einem positiven Treffer, d.h. einem erfolgreichen Abgleich, wird ein Eingriff in das Allgemeine Persönlichkeitsrecht angenommen.[681] Diese Entscheidung orientiert sich jedoch am Schutzzweck des Rechts auf Selbstdarstellung, welches vor einem Kontrollverlust über Bildnisse oder personenbezogene Daten schützt.[682] Dementsprechend begründeten die Gerichte einen fehlenden Eingriff im Fall der Kennzeichenerkennung damit, dass die unmittelbare Datenlöschung organisatorisch und technisch gesichert war.[683] Eine solche Annahme kann zwar im Fall eines polizeilichen Verfahrens angenommen werden, jedoch nicht im Fall privater Nutzung von Smartglasses, die im Regelfall keiner zum Schutze der Privatsphäre Dritter ausgerichteten Organisation und Kontrolle unterworfen ist. Zudem kann ein Kennzeichenabgleich vom Grad der Persönlichkeitsrechtgefährdung her sowohl im Hinblick auf den Kontrollverlust über den Inhalt der Abbildung als auch die Einschüchterungswirkung auf Betroffene, nicht mit einer Kennzeichenaufnahme verglichen werden.[684] Folglich wohnt jedem biometri-

---

[680] BVerfG, Urt. v. 11.3.2008 (1 BvR 2074/05, 1 BvR 1254/07), BVerfGE 120, 378 (399); vergleichbar ist die Entscheidung zum Abgleich im Rahmen der Fernemeldeüberwachung, BVerfG, Urt. v. 14.7.1999 (1 BvR 2226/94, 2420/95 u. 2437/95), BVerfGE 100, 313 (366); BVerwG, Urt. v. 22.10.2014 (6 C 7/13), NVwZ 2015, 906 (908); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 161.

[681] BVerfG, Urt. v. 11.3.2008 (1 BvR 2074/05, 1 BvR 1254/07), BVerfGE 120, 378 (399); BVerwG, Urt. v. 22.10.2014 (6 C 7/13), NVwZ 2015, 906 (908); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 161.

[682] Vgl. E II. 2, S. 93.

[683] BVerfG, Urt. v. 11.3.2008 (1 BvR 2074/05, 1 BvR 1254/07), BVerfGE 120, 378 (399); BVerwG, Urt. v. 22.10.2014 (6 C 7/13), NVwZ 2015, 906 (908); so auch *Karg*, HFR 2012, S. 120 (133).

[684] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 63, 240 f.

schen Abgleich von Personen, bereits mit der Erstellung einer Aufnahme für Extraktions- oder Vergleichszwecke, ein Eingriff inne.[685]

(2) Extraktion eines biometrischen Templates

Wird ein biometrisches Template aus der Aufnahme extrahiert, stellt sich zuerst die Frage, ob bereits in diesem Vorgang ein Eingriff in das Allgemeine Persönlichkeitsrecht zu sehen ist. Bei dem biometrischen Template handelt es sich um eine Ansammlung personenbezogener biometrischer Daten, wenn mit deren Hilfe eine Person bestimmt werden kann.[686] Das gilt auch, wenn diese Bestimmung nicht absolut ist, sondern auf Wahrscheinlichkeiten basiert.[687] Biometrische Daten können sowohl den Bezug zu einer bestimmten Person herstellen und sie identifizieren (z.B. „dieses Template eines Gesichts gehört Max Müller") als auch inhaltliche Informationen zu einer Person preisgeben (z.B. „die Person, deren Gesichtszüge dem Gesichtstemplate von Max Müller entsprechen, befand sich an diesem Ort zu diesem Zeitpunkt").[688]

Die Herstellung eines Personenbezuges kann sich zum einen aus der Verknüpfung mit zusätzlichen Informationen, wie z.B. dem Namen der Person oder der Aufnahme, die als Quelle des Templates diente, ergeben.[689] Fehlt ein solcher identifizierender Bezug, wird zum Teil einem isoliert gespeicherten Template kein Personenbezug zugestanden.[690] Dagegen spricht jedoch, dass auch das bloße Template zumindest dadurch Rückschlüsse auf eine Person erlaubt, dass es sie von anderen Personen unterscheidet.[691] So könnte ein Nutzer von Smartglasses mithilfe gespeicherter biometrischer Templates zumindest erkennen, ob er einer Person bereits begegnet ist oder nicht. Ein Personenbezug des Templates wäre daher allenfalls dann abzulehnen, wenn das Template ohne jeglichen kontextualen Bezug zur Person und der Möglichkeit ihrer Erkennung

---

685 Vgl. *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (242).

686 Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 9; vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 158; vgl. *Opel/Körffer/Nouak*, DuD 2013, S. 347 (347 f.).

687 Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 9.

688 Vgl. B III. 4, S. 38; Ebenda.

689 *Karg*, HFR 2012, S. 120 (124); *Opel/Körffer/Nouak*, DuD 2013, S. 347 (348).

690 *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 159.

691 *Karg*, HFR 2012, S. 120 (124).

gespeichert wäre, was jedoch dessen Sinnhaftigkeit beim Einsatz von Smartglasses aufheben würde.[692]

Ferner würden ein Personenbezug und zugleich eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung oder des Rechts am eigenen Bild vorliegen, wenn das biometrische Template selbst die dazugehörigen Personen erkennen lassen würde.[693] In diesem Fall müsste das Template jedoch im Wesentlichen der Originalaufnahme entsprechen, wobei die Erkennbarkeit sich auch ergeben könnte, wenn das Template gröber aufgelöst wäre als die Originalaufnahme. So hat z.B. der BGH die Erkennbarkeit eines Fußballspielers in einer Computerspielfigur bejaht.[694] Eine solche Erkennbarkeit des Templates ist zwar möglich, jedoch nicht zwingend, da die für eine biometrische Erkennung relevante Wahrnehmung eines Computers sich von der menschlichen Wahrnehmung unterscheiden kann.[695]

(3) Personenabgleich mithilfe von Smartglasses

Bei einem Personenabgleich wird zuerst ebenfalls ein biometrisches Template der abzugleichenden Person erstellt und anschließend mit den vorliegenden biometrischen Templates (sog. Referenz-Templates), abgeglichen.[696] Z.B. könnte der Nutzer von Smartglasses auf diese Art und Weise einer Person im Fall positiver Erkennung zusätzliche Informationen, wie ihren Namen, Hobbys oder Anmerkungen Dritter zu der Person, zuordnen.[697] Ein derartiger Abgleich stellt einen Umgang mit biometrischen Templates als personenbezogene Daten dar und ist besonders einschneidend, wenn die betroffene Person positiv mit dem vorliegenden

---

[692] Derart anonyme Speicherung von biometrischen Daten ist in der Praxis z.B. im Rahmen wissenschaftlicher Untersuchungen relevant, *Opel/Körffer/Nouak*, DuD 2013, S. 347 (347 ff.).

[693] Art. 29-Datenschutzgruppe spricht von einem "einem Satz unverwechselbahrer Merkmale einer Person" als Grundlage des Personenbezugs, Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 4; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 73; *Hornung*, DuD 2004, S. 429 (431).

[694] OLG Hamburg, Urt. v. 13.1.2004 (7 U 41/03), ZUM 2004, 309 (310); das Recht am eigenen Bild schützt generell Abbildungen unabhängig von dem Trägermedium, BVerfG, Beschl. v. 25.8.2000 (1 BvR 2707/95), ZUM 2001, 232; m.w.N., *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 1; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 22.

[695] Ein hoch aufgelöstes biometrisches Template kann "wie Eiweiß, das in der Pfanne brutzelt und Blasen wirft" aussehen, *Tanriverdi*, Gesichtserkennung, SZ, http://www.sueddeutsche.de/digital/gesichtserkennung-wie-maschinen-menschen-sehen-1.2272954 (7.9.2015).

[696] Vgl. B III. 4. a), S. 40.

[697] Vgl. B III. 4. a), S. 40.

Template abgeglichen wurde.[698] Aber auch bei Nichttreffern kann ein Abgleich ebenso intensiv beeinträchtigend sein, wenn z.B. das Vertrauen in eine Person davon abhängig gemacht wird, dass sie zum selben sozialen Netzwerk gehört wie der Nutzer der Smartglasses.[699]

Dieses Ergebnis gilt gleichermaßen für einen Personenabgleich, bei dem auf fremde Referenztemplates zugegriffen wird.[700] Das wäre der Fall, wenn anhand der erstellten Personenabbildung eine Internetsuche durchgeführt werden würde. Hierzu würde die Abbildung z.B. an eine Bildersuchmaschine übermittelt, wo sie biometrisch ausgewertet und mit den im Internet zugänglichen Aufnahmen von Personen abgeglichen werden würde.[701] In dieser Konstellation ist erschwerend zu berücksichtigen, dass die Personenabbildung an den Suchanbieter übertragen wird und damit eine Verbreitung erfährt.

(4) Besonderheiten der Stimm- und Verhaltenserkennung

Smartglasses können auch über die Fähigkeit verfügen, Personen anhand ihrer Stimmen oder ihres Verhaltens zu erkennen.[702] Hierzu würden statt körperbezogener biometrischer Templates stimm- oder verhaltensbezogene Templates extrahiert oder abgeglichen.[703] Derartige Verfahren können z.B. der Steuerung von Smartglasses durch Stimmen und Gesten dienen.[704] Sie können aber auch ähnlich wie „smarte Überwachungskameras“

---

[698] BVerwG, Urt. v. 22.10.2014 (6 C 7/13), NVwZ 2015, 906 (908); BVerfG, Urt. v. 11.3.2008 (1 BvR 2074/05, 1 BvR 1254/07), BVerfGE 120, 378 (399); BVerfG, Urt. v. 14.7.1999 (1 BvR 2226/94, 2420/95 u. 2437/95), BVerfGE 100, 313 (366); *Hornung*, DuD 2004, S. 429 (430); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 161.

[699] Darin spiegelt sich die Feststellung des BVerfG wieder, dass kein Datum belanglos ist, BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (45).

[700] Vgl. *Hornung*, DuD 2004, S. 429 (431); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 159.

[701] Vgl. zum Personensuchmaschinen, OLG Köln, Urt. v. 9.2.2010 (15 U 107/09), ZUM 2010, 706; LG Hamburg, Urt. v. 16.6.2010 (325 O 448/09), ZUM-RD 2010, 623; bei der Personensuche im Internet wird nicht nur eine templatebasierte Suche eingesetzt, sondern es werden unterschiedliche Suchverfahren kombiniert, *Gates*, Our Biometric Future, 2011, S. 143; Netzwerke wie Facebook oder Google verfügen bereits heute über die Möglichkeiten der Gesichtserkennung, *Russakovsky u.a.*, Cornell University, n.n.v. Studienarbeit 2014, p. 1 (29); *Küchemann*, Gesichtserkennungstechnologie Die Überwachungskamera weiß jetzt, wer du bist, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/gesichtserkennung-aufruestung-der-ueberwachung-13662435.html (21.7.2015); Datenschutz, Die Zeit, http://www.zeit.de/digital/datenschutz/2015-06/facebook-gesichtserkennung-frisur-kleidung (21.7.2015).

[702] Vgl. B III. 4. b), S. 42.

[703] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 15 f.; *Spiecker genannt Döhmann*, K&R 2014, S. 549 (551); *Wrede*, ZD 2012, S. 321 (321 f.).

[704] Vgl. B II. 2. a), S. 30.

auf ein anormales Verhalten von Personen und damit potenzielle Gefahrenquellen aufmerksam machen.[705]

Generell kann im Hinblick auf die Erstellung sowie Verwendung von biometrischen Stimm- und Verhaltenstemplates auf die gewonnenen Erkenntnisse zum Personenabgleich mithilfe von Smartglasses verwiesen werden.[706] D.h., in jeder Stufe des biometrischen Verfahrens wird ein Eingriff in das Allgemeine Persönlichkeitsrecht anzunehmen sein.[707]

Eine Besonderheit stellt jedoch eine Analyse der Stimme oder der Gesten dar, die nicht der Identifizierung einer Person dient, sondern alleine der Auswertung des Bedeutungsinhalts der Worte oder der Gesten, um etwaige Befehle der Nutzer zu erkennen. Z.B. überwacht Google Glass permanent, ob die Worte „Ok Glass" gesprochen werden (sog. „Hotwords"), die dem Gerät als Hinweis darauf dienen, dass weitere sprachliche Befehle folgen werden.[708] Damit Smartglasses die Hotwords oder Gesten erkennen können, müssen sie permanent die eingehenden akustischen sowie visuellen Informationen aufzeichnen und auswerten. Zwar ist damit zu rechnen, dass die Geräte so gestaltet sein werden, dass generell nur die Eingaben ihrer Nutzer erfasst werden. Dennoch können z.B. laute Stimmen von Personen im Erfassungsbereich der Kamera oder des Mikrofons erfasst und der Auswertung zugeführt werden.

An dieser Stelle könnte zugunsten der Nutzer von Smartglasses ein Vergleich zu einem rein technischen Vorgang gezogen werden, bei dem zwar personenbezogene Daten erfasst werden, diese aber nicht in den Kenntnis- und Verfügungsbereich des Verwenders gelangen und daher deren Erhebung im Sinne eines Datenumgangs in Frage gestellt wird.[709] Das ist z.B. der Fall, wenn Fahrassistenzsysteme von Fahrzeugen zwar mithilfe von Kameras und anderen Sensoren die Umgebung abbilden, diese Aufnahmen jedoch nur von den Fahrassistenzsystemen ausgewertet werden. Darüber hinaus gibt es keine technische Möglichkeit, diese Kamerabilder zu sehen oder anderweitig zu verarbeiten.[710] Bei Smartglasses ist zwar ein vergleichbares Verfahren vorstellbar, jedoch müsste eine ähnliche technisch-organisatorische Sicherheit wie in einem Kraftfahrzeug

---

[705] Vgl. B III. 4. b), S. 42; *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (239 f.); *Spiecker genannt Döhmann*, K&R 2014, S. 549 (551); *Wrede*, ZD 2012, S. 321 (321 f.).

[706] Vgl. E II. 2. b) dd) (1), S. 116; Art. 29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, 00727/12/DE, 2012, S. 2 ff.; *Gola*, NZA 2007, S. 1139 (1140).

[707] Vgl. E II. 2. b) dd) (3), S. 118.

[708] Vgl. B II. 2. a), S. 30.

[709] *Fuchs*, ZD 2015, S. 212 (213).

[710] Ebenda.

bestehen, bei dem ein Fahrer diese Daten nicht ohne Weiteres aus dem Fahrassistenzsystem gewinnen kann.[711] Ferner ist im Fall von Fahrassistenzsystemen, anders als bei Smartglasses und als Folge der technisch-organisatorischen Sicherheit sowie des beschränkten Nutzungszwecks, keine Einschüchterungswirkung auf die Passanten im Wahrnehmungsfeld des Kraftfahrzeugs anzunehmen. Auch ist die Intensität der Beeinträchtigung des Allgemeinen Persönlichkeitsrechts bei Auswertung der Stimme oder des Verhaltens einer bestimmten Person weitaus höher als bei fahrtechnischen Fahrassistenzsystemen, die eine Straßenlage auswerten.

D.h., auch wenn der Zweck der flüchtigen Aufnahme nicht in der Identifizierung der Person liegt, wird sie einen Eingriff in das Allgemeine Persönlichkeitsrecht darstellen. Dasselbe gilt für die folgende inhaltliche biometrische Auswertung der gewonnenen Daten, die einen Umgang mit personenbezogenen Daten bedeutet. Dies gilt auch, wenn eine Erhebung personenbezogener Daten nicht beabsichtigt, sondern nur eine zwingende und unerwünschte Nebenfolge der Erkennungsfunktionen war.[712]

Zusätzlich könnten Stimmbefehle, wie im Fall heutiger Smartphones, an Geräte- oder sonstige Drittanbieter übertragen werden, damit diese die inhaltliche Stimmauswertung durchführen.[713] Im derartigen Fall führt die zusätzliche Übertragung der Stimmaufnahmen wegen des damit einhergehenden Kontrollverlusts über das gesprochene Wort zu einer weiteren Beeinträchtigung des Allgemeinen Persönlichkeitsrechts der Betroffenen. Umgekehrt wäre bei Kenntnis der Betroffenen von den Befehlserkennungsfunktionen (und ggf. auch der Übertragung der Stimmaufzeichnung an Dritte) zu prüfen, ob die trotz der Präsenz von Smartglasses geäußerten Worte nicht von einer Einwilligung gedeckt sind. Das zur Erkennung von Stimmbefehlen Gesagte gilt ferner ebenso für die Erkennung von Steuerungsbefehlen mittels von Gesten.

ee) Augmented-Reality-Funktionen

Auch die Augmented-Reality-Funktionen erfordern, dass der Sichtbereich der Nutzer von Smartglasses zuerst aufgezeichnet wird, bevor er einer Bilderkennungsanalyse zugeführt werden kann, die wiederum notwendig ist, um in der Abbildung der physischen Realität virtuelle Objekte zu

---

[711] Vgl. zur Kennzeichenerkennung durch Polizeibehörden gesagte E II. 2. b) dd) (3), S. 118.

[712] Vgl. *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 105; *Jahn/Striezel*, K&R 2009, S. 753 (755).

[713] ZD-Aktuell, Spracherkennung auf Smartphones, 2012, Nr. 03026; *Martin-Jung*, Siri und Co., SZ, http://www.sueddeutsche.de/digital/digitale-assistenten-berechnende-alltagshelfer-1.2264423 (10.9.2015).

registrieren.[714] Ein solcher Vorgang kann zugleich ein biometrisches Erkennungsverfahren darstellen, wenn z.B. die Ermittlung der Identität einer Person notwendig ist, um ihren Namen virtuell im Sichtfeld des Datenbrillenträgers einzublenden. In diesem Fall kann auf die Ergebnisse zu biometrischen Verfahren verwiesen werden.[715]

Augmented Reality kann jedoch auch ohne die Identifizierung der Person erzeugt werden, wenn Menschen lediglich als solche, aber ohne Einbeziehung identifizierender Merkmale, erkannt werden. Z.B. könnten so Fußgänger bei schlechten Sichtverhältnissen für einen Nutzer von Smartglasses beim Autofahren optisch, z.B. durch einen virtuellen farblichen Rahmen, gekennzeichnet werden.[716] D.h., derartige Verfahren würden keine biometrischen Templates von Personen extrahieren und Menschen lediglich als anonyme Objekte der Klasse „Mensch" behandeln. Jedoch würde auch hierbei zumindest eine Aufnahme der Person erstellt werden, anhand welcher die Personen erkannt oder identifiziert werden könnte. Doch auch die Erkennung und Identifikation der Person könnte verhindert werden, wenn die Person bereits im Zeitpunkt der Aufnahme anonymisiert werden würde.[717] Zwar würde es sich hierbei weiterhin um einen Umgang mit personenbezogenen Daten handeln, da die Anonymisierung erst nach der Stufe der Aufnahme erfolgt, jedoch läge bei sofortiger und effizienter Durchführung der Anonymisierung ohne Speicherung der Rohdaten lediglich eine geringe Beeinträchtigung des Allgemeinen Persönlichkeitsrechts vor.[718]

ff) Modifizierte Wahrnehmung von Menschen durch Mediated Reality

Die Mediated-Reality-Eigenschaften von Smartglasses erlauben ihren Nutzern, die Wirklichkeit nur modifiziert wahrzunehmen und z.B. die Abbildungen von Menschen nur bearbeitet wahrzunehmen oder sie insgesamt auszublenden.[719] So wäre es z.B. möglich, die Gesichter von Men-

---

[714] Zu beachten ist, dass die vorstehenden Ausführungen nicht für "Augmented Reality im Weiteren Sinne" gelten, D.h., die bloße Einblendung von Informationen im Sichtfeld der Nutzer, ohne deren Registrierung im physischen Raum, vgl. B III. 5. d), S. 47.

[715] Vgl. E II. 2. b) dd) (1), S. 116.

[716] Vgl. *Grünweg*, Assistenzsysteme gegen Nachtunfälle, Spiegel Online, http://www.spiegel.de/auto/aktuell/assistenzsysteme-gegen-nachtunfaelle-fussgaenger-im-lichtkegel-a-768526.html (14.11.2015).

[717] Vgl. Information and Privacy Commissioner of Ontario, Anonymous Video Analytics (AVA) technology and privacy, 2011, https://www.ipc.on.ca/images/Resources/AVAwhite6.pdf (2.9.2015), p. 4; *Zscherpe*, DuD 2015, S. 172 (173).

[718] Information and Privacy Commissioner of Ontario, Anonymous Video Analytics (AVA) technology and privacy, 2011, https://www.ipc.on.ca/images/Resources/AVAwhite6.pdf (2.9.2015), p. 4.

[719] Vgl. B III. 5. c), S. 46.

schen ähnlich wie in einer Bildbearbeitungssoftware durch Gesichter anderer Menschen auszutauschen oder zu karikieren. Derartige Modifikationen könnten die Betroffenen als eine Beeinträchtigung ihres Rechts auf Selbstdarstellung empfinden.[720] Jedoch wäre diese gefühlte Beeinträchtigung zumindest so lange rechtlich nicht relevant, wie die Modifikation nicht verbreitet oder Dritten nicht zugänglich gemacht wird und so z.B. einen Verstoß gegen das Recht am eigenen Bild oder eine Ehrverletzung darstellen würde.[721] Denn eine Person darf zwar innerhalb der Grenzen der ihr gewährleisteten Privatsphäre über die sie betreffenden Informationen bestimmen, jedoch nicht darüber, wie diese Informationen von Dritten interpretiert werden.[722] Ganz im Gegenteil ist die Privatsphäre Teil eines freiheitlichen Konzeptes, das die innere Vorstellungswelt einzelner vor Beeinflussung durch Dritte und damit eine modifizierte Wirklichkeitswahrnehmung schützt.[723]

gg) Einschüchterungswirkung durch die bloße Präsenz von Smartglasses

Die bisherigen Reaktionen auf Smartglasses im Alltag zeigten vor allem die Befürchtung Betroffener, dass sie Opfer heimlicher Foto- oder Videoaufnahmen werden.[724] Auf der anderen Seite meinten die Nutzer von Smartglasses, dass sie es gar nicht vorhatten, gegen die Privatsphäre Dritter zu verstoßen und diese gegen ihren Willen aufzuzeichnen.[725] Doch auch wenn man den Trägern von Smartglasses diese Rücksichtnahme unterstellt, kann eine Angst vor permanenter Möglichkeit der Beobachtung, wie sie für eine panoptische Überwachung typisch ist, zu einer Verhaltensanpassung der sich beobachtet fühlenden Person führen.[726]

Es besteht daher ein Anlass, zu prüfen, inwieweit die bloße Präsenz von Smartglasses zu einer Überwachungswirkung führt, deren Einschüchterungseffekt Menschen zur Anpassung ihres Verhaltens und damit der

---

[720] Vgl. B III. 5. c), S. 46.

[721] Vgl. BVerfG, Beschl. v. 14.2.2005 (1 BvR 240/04), NJW 2005, 3271.

[722] Ebenda, 3272; RG, Urt. v. 29.4.1930 (II 355/29), RGZ 128, 330 (343); *Alexander*, ZUM 2011, S. 382 (384).

[723] Vgl. D I. 3, S. 75; würde die veränderte Abbildung Betroffener Dritten zur Verfügung gestellt, dann könnte darin eine Beeinträchtigung des Rechts am eigenen Bild oder der Ehre der betroffenen Person vorliegen, vgl. BVerfG, Beschl. v. 14.2.2005 (1 BvR 240/04), NJW 2005, 3271 (3273); BVerfGE, Beschl. v. 3.6.1987 (1 BvR 313/85), BVerfGE 75, 369 (376 ff.).

[724] Vgl. C II. 3, S. 68.

[725] *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/2013/12/glasshole (2.1.2014); *Swider*, I wore Google Glass for one year and here's what I experienced, TechRadar, http://www.techradar.com/news/wearables/ i-wore-google-glass-for-one-year-and-here-s-what-i-experienced-1281372/3 (7.9.2015).

[726] Vgl. D I. 5, S. 78.

Beeinträchtigung ihrer Autonomie zwingen kann. Dogmatisch wird hierbei vor allem die Frage relevant, an welcher Stelle die bloßen „Überwachungs- und Anpassungseffekte“ im Allgemeinen Persönlichkeitsrecht zu verorten sind.

(1) Rechtliche Anerkennung von Überwachungs- und Anpassungseffekten

Ein „Überwachungs- und Anpassungsdruck“ in Form einer psychischen Zwangswirkung und damit Anpassung des eigenen Verhaltens wird vor allem im Zusammenhang mit der Präsenz von Videoüberwachungskameras im öffentlichen Raum und einem damit einhergehenden Gefühl der latenten Beobachtung gesehen.[727] Dabei wird zur Verdeutlichung der psychischen Effekte der Überwachung häufig auf George Orwells Buch „1984“ zurückgegriffen.[728] In Orwells dystopischem Zukunftsszenario wurden die Menschen dem Gefühl ständiger Überwachung durch optisch-akustische Überwachungsgeräte (sog. „Teleschirme“) in ihren Wohnungen ausgesetzt und so ohne direkte Eingriffe unter dem Motto „Der Große Bruder beobachtet dich“ zur Befolgung der staatlich vorgegebenen Meinungsdoktrin diszipliniert.[729] Auch bei der Auseinandersetzung mit Smartglasses wird der Vergleich mit einem von Orwell beschriebenen Panoptikum häufig aufgegriffen, wobei zum Teil weitaus schlimmere Effekte durch die Dezentralität der Überwachung befürchtet werden.[730]

Als Überwachungs- und Anpassungsdruck ist eine psychische Zwangswirkung zu verstehen, die durch das Gefühl einer latenten Überwachung hervorgerufen wird.[731] Die Zwangswirkung äußert sich in einer Furcht, dass das eigene Verhalten negativ auffallen und sanktioniert werden könnte, weshalb die sich überwacht fühlende Person versucht, ihr Verhalten den vermeintlichen oder tatsächlichen an sie gestellten äußeren Erwartungen anzupassen.[732] Die Person trifft ihre Entscheidungen daher

---

[727] *Horst*, NZM 2000, S. 937; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 91, 108.

[728] *Haggerty/Ericson*, The surveillant assemblage, in: *Hier*, The Surveillance Studies Reader, 2007, S. 104 (605); *Hotter*, Privatsphäre, 2011, S. 92; *Mann/Ferenbok*, Surveillance and Society 2013, Vol. 11, Nr. 1/2, p. 18.

[729] "Big Brother is watching you", *Orwell*, 1984, 1983, S. 21; *Kukkonen u.a.*, The Journal of Sexual Medicine 2007, Vol. 4, Nr. 1, p. 93.

[730] *Sagatz*, Big Brothers Brille, Der Tagesspiegel, http://www.tagesspiegel.de/medien/digitale-welt/google-glass-big-brothers-brille/8124318.html (11.9.2015); *Solmecke/Kocatepe*, ZD 2014, S. 22 (24); *Wagstaff*, Is Google Glass the new Big Brother?, The Week, http://theweek.com/articles/462431/google-glass-new-big-brother (11.9.2015); *Weber*, SSRN Electronic Journal 2012, Nr. 6, p. 1.

[731] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 91.

[732] Ebenda.

nicht unabhängig, sondern unter Einfluss eines äußerlichen Drucks, wodurch ihre Autonomie beeinträchtigt wird.[733]

Die beeinträchtigende Wirkung des Gefühls der Überwachung wurde sowohl, und wie bereits geschildert,[734] wissenschaftlich als auch durch die Rechtsprechung anerkannt.[735] Nach der Begründung des Bundesverfassungsgerichts dient das Recht auf informationelle Selbstbestimmung auch dem Schutz vor der psychischen Zwangswirkung des Überwachungs- und Anpassungsdrucks.[736] „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."[737] Dabei betonte das Bundesverfassungsgericht, dass nicht nur subjektive Rechte, sondern auch die Ausübung kommunikativer sowie politischer Rechte und damit das freiheitlich demokratische Grundwesen beeinträchtigt werden können.[738]

Eine solche psychische Zwangswirkung durch anonyme Kontrolle wurde vor allem beim Einsatz von Videotechnologien zur Überwachung von Arbeitnehmern und Nachbargrundstücken samt öffentlichen Zugangswegen anerkannt.[739] Auch im Fall von Dashcams in Kraftfahrzeugen verwiesen Gerichte auf die Möglichkeit anonymer Kontrolle als beeinträchtigende Wirkung der Geräte.[740] Ähnlich wie im Panoptikum können die Betroffenen in diesen Fällen allenfalls die Überwachungsgeräte erblicken,

---

[733] Vgl. D I. 2, S. 74.

[734] Vgl. D I. 5, S. 78.

[735] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42 f.).

[736] Ebenda.

[737] Ebenda, 43; den Einschüchterungseffekt betonend, BVerfG, Beschl. v. 12.4.2005 (2 BvR 1027/02), BVerfGE 113, 29 (46).

[738] BVerfG, Beschl. v. 12.4.2005 (2 BvR 1027/02), BVerfGE 113, 29 (46); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43).

[739] BVerfG, Beschl. v. 23.2.2007 (1 BvR 2368/06), NVwZ 2007, 688 (690 f.); BGH, Urt. v. 16.3.2010 (VI ZR 176/09), NJW 2010, 1533 (1534); BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955; OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827: OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545 (129); OLG Köln, Urt. v. 13.10.1988 (18 U 37/88), NJW 1989, 720 (721); LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327 (328); LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1068); AG Dinslaken, Urt. v. 5.3.2015 (34 C 47/14), ZD 2015, 531 (532); BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); BAG, Urt. v. 15.5.1991 (5 AZR 115/90), BAGE 68, 52 (58); BVerwG, Urt. v. 31.8.1988 (6 P 35.85), BVerwGE 80, 143 (146); *Geiger*, Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie, 1994, S. 178 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 95, 182.

[740] LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (Rn. 17); AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291.

ohne zu wissen, ob und in welchem Umfang sie überwacht werden.[741] Dementsprechend können bereits Warnhinweise, Schilder oder Attrappen, die auf die Möglichkeit einer potenziellen Überwachung hinweisen, einen solchen Überwachungsdruck erzeugen.[742] Die Folge ist, dass Betroffene ständig mit einer Überwachung rechnen müssen und „in einem optischen Gefängnis" leben.[743]

(2) Schutz vor Überwachungs- und Anpassungseffekten als eigenes Recht

Zwar ist geklärt, dass die bloße Präsenz von Überwachungskameras zur Entstehung von Überwachungs- und Anpassungseffekten führen kann, jedoch ist nicht geklärt, innerhalb welcher Fallgruppe des Allgemeinen Persönlichkeitsrechts diese Effekte zu verorten sind.

Aufgrund der Heranziehung des Überwachungs- und Anpassungsdrucks zur Begründung der informationellen Selbstbestimmung könnte man annehmen, das Bundesverfassungsgericht habe den Schutz vor dem Überwachungs- und Anpassungsdruck insgesamt dem Schutzbereich des Rechts auf informationelle Selbstbestimmung zugeordnet.[744] Jedoch ist der Überwachungs- und Anpassungsdruck ein genereller Schutzzweck der Privatsphäre, sodass diese Herleitung aus der Entscheidung des Bundesverfassungsgerichts nicht zwingend ist.[745] Aus der Aussage des Bundesverfassungsgerichts ist daher lediglich abzuleiten, dass der Schutz vor Überwachungs- und Anpassungsdruck als Nebenfolge des Umgangs mit personenbezogenen Daten auftreten kann, aber nicht, dass er vom Recht auf informationelle Selbstbestimmung ohne einen tatsächlich vorliegenden Datenumgang zwingend erfasst wird.[746]

Im Fall der Videoüberwachung wird dieser Ansicht entgegengehalten, dass Videoüberwachungsmaßnahmen einen einheitlichen Lebensvorgang

---

[741] Als Auslöser für die psychische Zwangswirkung wird vor allem die fehlende Möglichkeit zur Erfassung der technologischen Zusammenhänge und ihrer Folgen ausgemacht, S. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 91.

[742] LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1067 f.); AG Frankfurt a.M., Urt. v. 14.1.2015 (33 C 3407/14 (93)), ZD 215, 280 (280 f.); AG Aachen, Urt. v. 11.11.2003 (10 C 386/03), NZM 2004, 339 (339 f.); BAG, Urt. v. 15.5.1991 (5 AZR 115/90), BAGE 68, 52 (56); *Hilpert*, RDV 2009, S. 160 (162); *Horst*, NZM 2000, S. 937 (941 f.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 182.

[743] OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545 (129); OLG Köln, Urt. v. 13.10.1988 (18 U 37/88), NJW 1989, 720 (721).

[744] BVerfG, Beschl. v. 12.4.2005 (2 BvR 1027/02), BVerfGE 113, 29 (46); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43);.

[745] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 164.

[746] Vgl. LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1068); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 163; *Weichert*, DuD 2000, S. 662 (663).

darstellen, unabhängig davon, ob tatsächlich ein Datenumgang stattfindet oder nicht.[747] Dem ist zuzustimmen, da eine Überwachungseinrichtung häufig zur Videoüberwachung zwar fähig ist, diese aber nur periodisch vornimmt.[748] In diesem Fall würde die Annahme des Überwachungs- und Anpassungsdrucks als eine eigene Fallgruppe des Allgemeinen Persönlichkeitsrechts willkürlich und kaum bestimmbar erscheinen.[749] Diese Ansicht erscheint insbesondere im Hinblick auf Smartglasses überzeugend, da die Geräte praktisch jederzeit fähig sind, zur Beobachtungszwecken eingesetzt zu werden.[750] Z.B. könnte ein Nutzer von Smartglasses seinen Blick spontan auf eine Person heften und ihr mit dem Blick und damit auch mit der aufnahmebereiten Datenbrille visuell „nachgehen". Angesichts des Umstands, dass Menschen im öffentlichen Raum ihre Aufmerksamkeit häufiger anderen Menschen und auch länger als bloß flüchtig widmen, werden solche spontanen Beobachtungsvorgänge häufiger zu erwarten sein. Es wäre dadurch praktisch kaum möglich zu bestimmen, wann ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt und wann ein Verstoß in ein gesondertes „Recht auf Schutz vor Überwachungs- und Anpassungseffekten" gegeben ist.

Ein gesonderter Schutz vor Überwachungs- und Anpassungseffekten erscheint ferner deswegen nicht als eine eigene Fallgruppe notwendig, da ein solches Recht praktisch betrachtet ein Minus zum Recht auf informationelle Selbstbestimmung wäre. D.h., statt eines Datenumgangs und der Einschüchterungswirkung als Nebenfolge würde lediglich die Einschüchterungswirkung den Schutzbereich der neuen Fallgruppe ausmachen. Auch der Zweck des Rechts auf informationelle Selbstbestimmung spricht dafür, dass dessen Schutzbereich auch die bloßen Einschüchterungseffekte möglicher Überwachung mit umfasst. Das Recht soll die Kenntnis Einzelner über den Umgang mit deren personenbezogenen Daten gewähr-

---

[747] *Büllesfeld*, Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze, 2002, S. 124; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 60.

[748] Dies spiegelt sich im § 6 b BDSG wieder, der für eine Videoüberwachung keine durchgehende Beobachtung oder Aufnahme voraussetzt, LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1068); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 250.

[749] Darauf abstellend, dass eine Kamera ohne weitere und erkennbare Maßnahmen zur Videoüberwachung potentiell eingesetzt werden kann, OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827 (182); so auch, LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327 (328).

[750] Die Beobachtung setzt kein zielgerichtetes oder langfristiges Verhalten voraus, vgl. A IV. 8, S. 17.

leisten.[751] Diese Kenntnis ist auch dann beeinträchtigt, wenn ein Betroffener nicht weiß, ob er aufgenommen wurde oder nicht.[752]

Im Ergebnis sind die von Smartglasses ausgehenden Überwachungs- und Anpassungseffekte generell auch ohne tatsächlich stattfindende Aufnahmen als eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung anzusehen. Zu fragen ist jedoch, wann solche Effekte im Fall von Smartglasses angenommen werden können.

(3) Erzeugung eines Überwachungs- und Anpassungsdrucks durch Smartglasses

Nicht jedes Gefühl der Überwachung kann Berücksichtigung finden, da ansonsten die Grenzen des Persönlichkeitsrechtsschutzes konturlos werden würden.[753] Daher darf eine von Smartglasses ausgehende Überwachungs- und Anpassungswirkung erst mit der Überschreitung einer an objektiven Faktoren festzumachenden Erheblichkeitsschwelle angenommen werden. Diese Erheblichkeitsschwelle wird dann überschritten, wenn die Furcht vor Überwachung nicht lediglich irrational, sondern objektiv, z.B. durch Anwesenheit von überwachungstauglichen Geräten, Attrappen oder Hinweisschildern, begründet wird.[754] Ferner ist es nicht notwendig, dass der Überwachungs- und Anpassungsdruck bei einer Vielzahl von Personen entsteht. Denn der Schutz der Privatsphäre soll jedem Individuum und gesellschaftlichen Minderheiten undabhängig von der Quantität Betroffener zugutekommen.[755] Folglich ist es für die Qualifizierung als Beeinträchtigung des Allgemeinen Persönlichkeitsrechts ausreichend, wenn die psychische Belastung nur einzelne Personen betrifft.

Die bisherigen Erfahrungen, die vor allem mit den Reaktionen Dritter auf Smartglasses „Glass“ gemacht wurden, zeigen, dass die Betroffenen sich durch ein Gerät, das als Smartglasses erkennbar ist, überwacht füh-

---

[751] So auch, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 60 f.; dagegen eher eine eigene "Konkretisierung" des Allgemeines Persönlichkeitsrecht vorschlagend, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 181.

[752] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43).

[753] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 182; dagegen ohne weitere Ausführungen zur Erkennbarkeit der Überwachungsmaßnahmen von einem Überwachungsdruck als Folge der Überwachung ausgehend, BVerfG, Urt. v. 14.7.1999 (1 BvR 2226/94, 2420/95 u. 2437/95), BVerfGE 100, 313 (381); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43); BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238 (246 f.).

[754] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 58 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 182.

[755] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2 Abs.2 S.1, Rn. 42.

len.[756] Das Gefühl ist nicht rein subjektiver Natur, sondern geht auf die Erkennbarkeit der Geräte zurück, die durch Betroffene vor allem als eine Kamera wahrgenommen werden.[757] Auch wenn man den Trägern von Smartglasses unterstellt, dass sie Rücksicht auf die Rechte Dritter nehmen wollen, ist angesichts der Vorzüge von Augmented Reality oder Augmented Memory insbesondere mit einem Anstieg von Bild- oder Tonaufnahmen sowie biometrischen Erkennungsvorgängen zu rechnen.

Folglich sind die bei den Betroffenen infolge der Präsenz von Smartglasses entstehenden Überwachungs- und Anpassungseffekte nicht bloß subjektiver Natur, sondern objektiv gerechtfertigt. Die Intensität der psychischen Beeinträchtigung wird von der Konstruktion der jeweiligen Geräte als auch von deren Verbreitung abhängig zu machen sein. Insbesondere wird eine Verbreitung von Smartglasses im Lebensalltag von Menschen dazu führen können, dass das Gefühl der Überwachung auch dann berechtigt ist, wenn Smartglasses aufgrund der Bauweise nicht mehr als solche erkennbar sind. Denn objektive Hinweise auf deren Präsenz werden nicht erforderlich sein, wenn mit der Allgegenwart der Erfassung durch Smartglasses gerechnet werden muss.[758]

(4) Beachtung von Gewöhnungseffekten

Zu beachten ist, dass die vorstehenden Erkenntnisse zur Entstehung von Überwachungs- und Anpassungseffekten durch Smartglasses sich auf wenige Erfahrungsberichte sowie die Erfahrungen mit Überwachungskameras, jedoch nicht auf empirische Erkenntnisse stützen. Diese Erkenntnisse dürfen daher nur als indiziell, aber nicht als zwangsläufig angesehen werden. So können fehlende negative Erfahrungen mit permanenter Präsenz von Überwachungstechnologien zu Gewohnheitseffekten führen, in deren Folge ihre Anwesenheit keine Einschüchterungswirkung und dem-

---

[756] Vgl. C II. 3, S. 68.

[757] *Janssen*, Warum Glass (noch) nicht funktioniert, c't, http://www.heise.de/ct/artikel/Warum-Glass-noch-nicht-funktioniert-1897211.html (16.8.2014); *Sacasas*, Preserving the Person in the Emerging Kingdom of Technological Force, The Frailest Thing, http://thefrailestthing.com/2014/08/21/preserving-the-person-in-the-emerging-kingdom-of-technological-force/(22.8.2014); *Thompson*, Googling Yourself Takes on a Whole New Meaning, The New York Times, http://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html (7.9.2013).

[758] Vgl. im Ergebnis ähnliche Argumentation zu Dashcams, LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (Rn. 17); AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291.

entsprechend keinen psychischen Druck auf die Betroffenen ausübt.[759] Hierbei muss jedoch genau untersucht werden, ob die Gewöhnung nicht bloß Folge einer Verhaltensanpassung durch das Gefühl permanenter Beobachtung ist. In diesem Fall läge eine Verletzung der Privatsphäre vor.[760] Da jedoch erst einmal im Alltag implementierte Technologien selten wieder rückgängig gemacht werden können, müssten mögliche Gewohnheitseffekte zuerst empirisch bestätigt werden, bevor die Nutzung von Smartglasses im öffentlichen Raum in Annahme einer autonomen Gewöhnung der Menschen erlaubt wird.[761]

hh) Beeinträchtigung des Allgemeinen Persönlichkeitsrechts als Regelfall

Als Ergebnis der Prüfung der Auswirkung von Smartglasses auf das Allgemeine Persönlichkeitsrecht ist festzustellen, dass ihre Nutzung im öffentlichen Raum praktisch immer einen Eingriff in das Allgemeine Persönlichkeitsrecht Dritter darstellen wird. Zum einen werden sich deren Beeinträchtigungen durch tatsächlich hergestellte Aufnahmen und sonstige Datenerhebungen, deren Verbreitung, Veröffentlichung sowie Nutzung in biometrischen und Augmented-Reality-Verfahren, ergeben. Denn auch wenn Smartglasses lediglich präsent sind und keine Daten erheben, dürfen Personen in deren Erfassungsbereich berechtigterweise davon ausgehen, dass Aufnahmen von ihnen erstellt oder sonstige Daten erhoben werden.

---

[759] Vgl. BVerwG, Urt. v. 31.8.1988 (6 P 35.85), BVerwGE 80, 143 (148); die Gewohnheitseffekte könnten vor allem bei Personen zu erwarten sein, die mit Überwachungstechnologien aufwachsen und diese als gegeben hinnehmen oder mit ihnen umzugehen lernen, was an die satirische Feststellung des Buchautors Douglas Adams im Hinblick auf die Reaktionen von Menschen auf technische Neuerungen erinnert: "1. Alles, was es schon gibt, wenn du auf die Welt kommst, ist normal und üblich und gehört zum selbstverständlichen Funktionieren der Welt dazu. 2. Alles, was zwischen deinem 15. und 35. Lebensjahr erfunden wird, ist neu, aufregend und revolutionär und kann dir vielleicht zu einer beruflichen Laufbahn verhelfen. 3. Alles, was nach deinem 35. Lebensjahr erfunden wird, richtet sich gegen die natürliche Ordnung der Dinge.", *Adams/Schwarz*, Lachs im Zweifel, 2003, S. 134; Adams' These wird durch eine höhere Zustimmung zu Datenbrillen unter jüngeren Personen bestätigt, Großes Interesse an den Funktionen von Smart Glasses, BITKOM, https://www.bitkom.org/Presse/Presseinformation/Grosses-Interesse-an-den-Funktionen-von-Smart-Glasses.html (14.11.2015); *Mann/Niedzviecki*, Cyborg, 2002, S. 143; vgl. *Wicklund/Frey*, Die Theorie der objektiven Selbstaufmerksamkeit, in: *Frey/Irle*, Theorien der Sozialpsychologie, 1993, S. 155 (169).

[760] Vgl. zu kognitiver Anpassung E IV. 2. c) aa), S. 175; vgl. *Beck*, Das Zeitalter der Nebenfolgen und die Politisierung der Moderne, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 19 (74); vgl. *Sofsky*, Verteidigung des Privaten, 2007, S. 129 f.

[761] *Ellul*, The Technological Society, 1967, S. 85; "Pandora's Box has been opened and it has to be feared that nobody will be able to close it again", *Weber*, SSRN Electronic Journal 2012, Nr. 6, p. 1 (3).

Demzufolge ist nicht von der Hand zu weisen, dass Menschen in der Präsenz von Smartglasses ihr Verhalten anpassen werden, damit sie nicht in Situationen erfasst werden, die sie als unvorteilhaft empfinden oder weil sie sonstige Nachteile durch die Verbreitung, Veröffentlichung oder Verarbeitung der Informationen befürchten. Im öffentlichen Raum kann dies insbesondere bedeuten, dass zulässige, aber von vielen Gesellschaftsteilnehmern kritisierte Handlungen, wie z.B. das Rauchen in der Öffentlichkeit, Kommunikation mit Anhängern kritisch betrachteter politischer Richtungen, die Religionsausübung oder ein unbekleidetes Sonnenbad, angesichts der sozialen Kritik als zu gefährlich betrachtet und unterlassen werden könnten.[762] Damit würde die Privatsphäre ihre Funktion als Schutz vor äußerer Zwangswirkung auf ein moralisch, aber nicht normativ sanktioniertes Verhalten, verlieren.[763] Als Folge wäre der Fortbestand der Individualität und der Meinungspluralität erheblich gefährdet.

c) Schutz der Privatsphäre durch besondere Freiheitsrechte

Neben der Menschenwürde und dem Allgemeinen Persönlichkeitsrecht enthält das Grundgesetz weitere Freiheitsrechte, deren Schutzwirkung auch den Zielen der Privatsphäre entspricht und die durch die Nutzung von Smartglasses beeinträchtigt sein könnten.[764]

aa) Schutz der körperlichen Unversehrtheit aus Art. 2 Abs. 2 Satz 1 GG

Die Funktion der Privatsphäre als Schutz der psychischen Integrität vor Reizüberflutung und Beobachtung persönlicher Vorgänge durch Dritte könnte durch das Recht auf Schutz der körperlichen Unversehrtheit gem. Art. 2 Abs. 2 Satz 1 GG umfasst sein.[765] Die Beeinträchtigung des geistig-seelischen Befindens kann jedoch erst dann als eine körperliche Beeinträchtigung qualifiziert werden, wenn die Einwirkung auf das psychische Wohlbefinden körperlichen Schmerzen oder anderen, auch schmerzfreien, vergleichbaren physischen Wirkungen gleich kommt.[766] Insbesondere ist

---

[762] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 37.

[763] Vgl. D II, S. 80; vgl. *Pieroth u.a.*, Grundrechte, 2014, Rn. 420.

[764] Spezielle Freiheitsrechte sind systematisch grundsätzlich vor dem generelleren Allgemeinen Persönlichkeitsrecht zu prüfen, wurden jedoch im Rahmen dieser Arbeit aufgrund der Fokussierung auf den Schutz der Privatsphäre nachgestellt.

[765] Vgl. D I. 3, S. 75.

[766] BVerfG, Beschl. v. 14.1.1981 (1 BvR 612/72), BVerfGE 56, 54 (57); BVerfG, Beschl. v. 25.7.1979 (2 BvR 878/74), BVerfGE 52, 131 (171 ff.); BVerwG, Urt. v. 29.4.1988 (7 C 33/87), NJW 1988, 2396 (f.); BVerwG, Urt. v. 27.5.1983 (4 C 40, 44 u. 45/81), BVerwGE 67, 206 (213); *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2 Abs.2 S.1, Rn. 56.

die Störung eines sozialen Wohlbefindens nicht bereits als eine Beeinträchtigung der psychischen Integrität einzustufen.[767]

Daher führt das allgemeine Unwohlsein beim Gedanken, Objekt der Videoüberwachung oder biometrischer Auswertung zu werden, noch nicht zur Beeinträchtigung der körperlichen Integrität.[768] Nur eine dauerhafte und systematische und vor allem mobile Videoüberwachung kann zum Auftreten seelisch-psychologischer Pathologien führen, die sich bei hyperüberwachten Menschen mit Neurosen und fehlender Selbstständigkeit auswirken können.[769] Dazu muss der Raum für einen psychischen Rückzug soweit zurückgehen, dass ein Mensch sich nicht hinreichend zurückziehen kann, um seine innere Balance zu finden.[770]

Ein solcher pathologischer Zustand ist abhängig von den Einzelfällen, jedoch durchaus vorstellbar, wenn Smartglasses an Verbreitung im öffentlichen Raum gewinnen und Menschen, vorbehaltlich etwaiger Gewohnheitseffekte, keine Möglichkeit haben werden, ihnen auszuweichen. Ferner kann sich eine psychisch relevante Belastung ergeben, wenn Nutzer von Smartglasses anderen Personen nachstellen und so bei diesen einen psychologischen Überwachungs- und Verfolgungsdruck aufbauen.[771]

bb) Freiheit der Person aus Art. 2 Abs. 2 Satz 2 GG und Freizügigkeit aus Art. 11 GG

Art. 2 Abs. 2 Satz 2 GG gewährleistet die körperliche Bewegungsfreiheit, welche auch dann beeinträchtigt werden kann, wenn eine Person faktisch oder rechtlich daran gehindert oder umgekehrt dazu gezwungen wird, einen bestimmten Ort aufzusuchen.[772] Diese Freiheit soll jedoch nur vor körperlichen Beeinträchtigungen schützen und bezieht eine psychische Zwangswirkung allenfalls vor dem Hintergrund physischer Folgen, wie z.B. eines durch Festnahme bedrohten Zutrittsverbotes, ein.[773] Insbeson-

---

[767] BVerfG, Beschl. v. 14.1.1981 (1 BvR 612/72), BVerfGE 56, 54 (57); BVerfG, Beschl. v. 25.7.1979 (2 BvR 878/74), BVerfGE 52, 131 (171 ff.); BVerwG, Urt. v. 29.4.1988 (7 C 33/87), NJW 1988, 2396 (f.); BVerwG, Urt. v. 27.5.1983 (4 C 40, 44 u. 45/81), BVerwGE 67, 206 (213); *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2 Abs.2 S.1, Rn. 56.

[768] BVerfG, Beschl. v. 14.1.1981 (1 BvR 612/72), BVerfGE 56, 54 (74).

[769] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 188.

[770] Vgl. *Hotter*, Privatsphäre, 2011, S. 153; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 188.

[771] Auch wenn der Schwerpunkt der Belastung eher in dem Nachstellen selbst, als in dem Einsatz von Smartglasses zu sehen sein wird und es sich nicht um eine originäre Gefahr von Smartglasses handelt, da sie auch beim Einsatz klassischer Videokameras entstehen könnte, vgl. *Eisele*, in: *Schönke/Schröder*, StGB, § 238, Rn. 8.

[772] *Pieroth u.a.*, Grundrechte, 2014, Rn. 442.

[773] Ebenda, Rn. 443 ff.

dere wird kein Recht auf eine Körperbewegung, die frei von jeglicher Angst und Furcht ist, gewährleistet.[774] Auch etwaige Betretungsverbote müssen einem Hausarrest gleichkommen, um eine Freiheitsbeschränkung i.S.d. Art. 2 Abs. 2 Satz 2 GG darzustellen.[775] Dementsprechend stellt die Nutzung von Smartglasses im öffentlichen Raum generell keinen Eingriff in die Fortbewegungsfreiheit dar, weil dadurch Personen nicht physisch an der Fortbewegung gehindert werden.[776]

Die Freizügigkeit gem. Art. 11 GG gewährleistet die Freiheit, an jedem Ort innerhalb des Bundesgebiets Aufenthalt oder Wohnsitz zu nehmen.[777] Anders als im Fall der allgemeinen Videoüberwachung, wo eine Verletzung des Schutzbereichs z.B. durch die Verdrängung von Obdachlosen besprochen wird,[778] ist dessen Beeinträchtigung beim Einsatz von Smartglasses nicht einschlägig. Denn anders als bei festinstallierten Videokameras erfolgt die typische Erfassung durch Smartglasses vorübergehend und beeinträchtigt nicht die auf eine gewisse Dauer angelegten Niederlassungen von Menschen in Form von Wohnung oder Aufenthaltsstätte.[779]

cc) Allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG

Art. 2 Abs. 1 GG schützt als allgemeine Handlungsfreiheit jegliches menschliche Verhalten, ohne dass dessen Schutzbereich auf bestimmte Lebensbereiche beschränkt wäre.[780] In ihrer Weite ist die allgemeine Handlungsfreiheit als ein nachrangiges Auffanggrundrecht zu verstehen, das nur dann zur Anwendung kommt, wenn kein Schutzbereich eines spezielleren Grundrechts einschlägig ist.[781] Folglich ist Art. 2 Abs. 1 GG vorliegend gegenüber dem vorliegend einschlägigen Allgemeinen Persönlichkeitsrecht subsidiär.

dd) Sonstige Freiheitsrechte

Im Weiteren können Betroffene aufgrund der Präsenz von Smartglasses in der Wahrnehmung anderer Freiheiten, wie z.B. der Religionsfreiheit gem. Art. 4 GG, der Meinungsfreiheit gem. Art. 5 Abs. 1 Satz 1 HS. 1 GG, der

---

[774] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2 Abs.2 S.2, Rn. 24.

[775] Ebenda, Art. 2 Abs.2 S.2, Rn. 28.

[776] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 187.

[777] BVerfG, Urt. v. 17.3.2004 (1 BvR 1266/00), BVerfGE 110, 177 (190); *Pieroth u.a.*, Grundrechte, 2014, Rn. 856.

[778] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 187.

[779] Zur Notwendigkeit einer gewissen Dauer des Verweilens, vgl. *Pieroth u.a.*, Grundrechte, 2014, Rn. 858.

[780] BVerfG, Beschl. v. 14.12.2000 (2 BvR 1741/99, 2 BvR 276/00 u. 2 BvR 2061/00), BVerfGE 103, 29 (45); *Pieroth u.a.*, Grundrechte, 2014, Rn. 386.

[781] BVerfG, Urt. v. 16.1.1957 (1 BvR 253/56), BVerfGE 6, 32 (37); *Pieroth u.a.*, Grundrechte, 2014, Rn. 387.

Versammlungsfreiheit gem. Art. 8 Abs. 1 GG oder der Vereinigungsfreiheit aus Art. 9 GG, beeinträchtigt werden. Dabei würde es sich um Auswirkungen handeln, die auch das Bundesverfassungsgericht als mögliche Folge der Beeinträchtigung der informationellen Selbstbestimmung sah.[782] Im Hinblick auf die Privatsphäre als Gegenstand dieser Untersuchung müssen zwar die möglichen Folgen ihrer Verletzung berücksichtigt werden, jedoch würde die Vertiefung aller möglicherweise betroffenen Grundrechte den Rahmen der Untersuchung übersteigen.

d) Einwilligung und Grundrechtsverzicht der Betroffenen

Die bisher festgestellten Eingriffe in die Persönlichkeitsrechte Betroffener beruhen auf der Annahme ihres entgegenstehenden Willens. Es ist jedoch, z.B. wie im Fall gewöhnlicher Foto- oder Videoaufnahmen vorstellbar, dass Betroffene mit der Erfassung durch Smartglasses einverstanden sind und ihre Grundrechte daher nicht beeinträchtigt werden.[783] Ob eine derartige Einwilligung vorliegt, kann zwar nur im Einzelfall geprüft werden, jedoch können bereits auf der verfassungsrechtlichen Ebene die Grenzen und Grundlagen einer zulässigen Einwilligung festgelegt werden.[784]

aa) Zulässigkeit und Reichweite des Grundrechtsverzichts

Die Frage, ob und inwieweit eine Einwilligung der Beeinträchtigung von Grundrechten entgegensteht, wird unter dem Aspekt des Grundrechtsverzichts diskutiert.[785] So spricht die Funktion der Grundrechte als subjektive Rechte dafür, dass ein Grundrechtsträger auf deren Wahrnehmung als Akt der Freiheitsausübung und Akt autonomer Persönlichkeitsentfaltung verzichten kann.[786] Ferner kann sich eine Einwilligung im Rahmen der mittelbaren Geltung von Grundrechten auch im Verhältnis zwischen zwei Privatpersonen auswirken.[787] Daher kommt auch für die durch die Nutzung von Smartglasses betroffenen Fallgruppen des Allgemeinen Persönlichkeitsrechts eine Einwilligung generell in Frage. So könnte z.B. ein

---

[782] Vgl. BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43).

[783] Vgl. zum Wegfall des Eingrffs bei Einwilligung *Jarass*, NJW 1989, S. 857 (860); *Pieroth u.a.*, Grundrechte, 2014, Rn. 156.

[784] Vgl. *Geiger*, NVwZ 1989, S. 35 (36 f.); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 21, 43 ff.

[785] *Geiger*, NVwZ 1989, S. 35 (36 f.); *Pieroth u.a.*, Grundrechte, 2014, Rn. 146.

[786] BVerfG, Beschl. v. 25.3.1992 (1 BvR 1430/88), BVerfGE 85, 386 (398); *Dürig*, AöR 1956, S. 117 (152); *Geiger*, NVwZ 1989, S. 35 (37); *Jarass*, NJW 1989, S. 857 (860); *Pieroth u.a.*, Grundrechte, 2014, Rn. 152.

[787] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 229.

Verzicht auf das Recht am gesprochenen Wort oder auf das Recht auf informationelle Selbstbestimmung ausgeübt werden.[788]

Jedoch ist zu beachten, dass der Verzicht auf die Menschenwürde und deren Gehalt in anderen Grundrechten unzulässig ist.[789] Da das Allgemeine Persönlichkeitsrecht neben einer subjektiven Schutzfunktion auch die Funktionsfähigkeit einer Meinungspluralität in einem demokratischen Staat sichern soll, dürfen sich dessen Bürger nicht selbst ihrer Mündigkeit begeben.[790] D.h., der einwilligenden Person muss eine Sphäre der Privatheit verbleiben, in der sie sich unbeeinflusst von der Öffentlichkeit autonom, d.h. ohne moralische oder rechtliche Konsequenzen zu befürchten, eine freie Meinung bilden kann.[791]

Bei der Beurteilung, wann die Schwelle einer Verletzung der Menschenwürde überschritten wird, werden im Wesentlichen die Dauer und die Schwere der Beeinträchtigung der Privatsphäre eine Rolle spielen.[792] Insbesondere darf sich eine Person dem Einwilligungsempfänger nicht auf „Gedeih und Verderb ausliefern".[793] Eine Einwilligung ist daher unbeachtlich, wenn die einwilligende Person ohne Rücksicht auf ihre eigene personale Identität zum Mittel instrumentalisiert wird.[794] Dies wurde z.B. bei einer „entpersonifizierenden Vermarktung der Frau" in einer „Peep Show"-Kabine bejaht, die Männern einen einseitigen Blickkontakt durch Sichtfenster gegen Münzeinwurf gewährte.[795]

Vor dem Hintergrund der Videobeobachtung wird die Möglichkeit des Grundrechtsverzichts in Bereichen enger persönlicher Sphäre, wie z.B. Toiletten oder Umkleideräumen, oder Fällen dauerhafter Beobachtung in voyeuristischen Fernsehunterhaltungsshows wie „Big Brother" diskutiert.[796] Dabei wird der Möglichkeit, sich der Videobeobachtung zu entziehen, ein entscheidender Wert beigemessen. So waren die Teilnehmer der TV-Show „Big Brother" der als Showkonzept eingesetzten Kameraüberwachung nicht ausgeliefert, da sie die Show jederzeit verlassen konn-

---

[788] Vgl. BVerfG, Beschl. v. 11.6.1991 (1 BvR 239/90), BVerfGE 84, 192 (194); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43); *Geiger*, NVwZ 1989, S. 35 ff.

[789] *Pieroth u.a.*, Grundrechte, 2014, Rn. 152.

[790] Vgl. D II. 2, S. 81.

[791] Vgl. D I. 2, S. 74.

[792] *Pieroth u.a.*, Grundrechte, 2014, Rn. 154.

[793] *Schmitt Glaeser*, ZRP 2000, S. 395 (399).

[794] BVerwG, Urt. v. 15.6.1999 (2 WD 34/98), BVerwGE 113, 340 (341 f.); BVerwG, Urt. v. 15.12.1981 (1 C 232/79), BVerwGE 64, 274 (279).

[795] BVerwG, Urt. v. 15.12.1981 (1 C 232/79), BVerwGE 64, 274 (278 f.).

[796] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 194; *Schmitt Glaeser*, ZRP 2000, S. 395.

ten.[797] Auch eine Einwilligung zur Erfassung durch Smartglasses wird typischerweise keine Auslieferung oder Aufgabe der Privatsphäre der Einwilligenden darstellen und damit grundsätzlich zulässig sein. Erst wenn die einwilligende Person im Sonderfall in eine lückenlose und unausweichliche Überwachung einwilligen würde, wäre ihre Einwilligung unzulässig.[798]

bb) Einwilligungsfähigkeit und Freiwilligkeit

Voraussetzung eines Grundrechtsverzichts und damit einer wirksamen Einwilligung ist die Einwilligungsfähigkeit des Grundrechtsträgers. D.h., er muss sich ihrer vollen Tragweite, vor allem der möglichen Folgen der Einwilligung, bewusst sein.[799] Die Einwilligungsfähigkeit kann z.B. bei stark betrunkenen Personen fehlen, die nicht in der Lage sind, zu erkennen, dass eine Videoaufnahme an Dritte weitergegeben oder zu deren Belustigung dienen kann.[800] Ebenso wird ein genereller als auch ein pauschaler und zeitlich unbefristeter Grundrechtsverzicht nicht alle unvorhersehbaren Situationen und Rechtsfolgen einschließen können und wird daher unwirksam sein.[801] Jedoch können Einwilligungen für überblickbare konkrete Situationen und Konstellationen zulässig sein.[802] Aber auch dann ist zur Prüfung der Reichweite einer Einwilligung darauf abzustellen, inwieweit die einwilligende Person die Tragweite ihrer Entscheidung erkennen konnte, was im Wege einer Auslegung zu ermitteln ist.[803] Weitere Voraussetzung für eine wirksame Einwilligung ist, dass sie freiwillig, also nicht unter Druck oder infolge einer Täuschung, geleistet wird.[804]

Zwar wird eine Einwilligung gegenüber den Nutzern von Smartglasses selten infolge einer Druckausübung oder bewussten Täuschung abgegeben werden. Jedoch wird aufgrund des hohen Aufklärungsbedarfs über die Reichweite der Erfassung, ihre Folgen und Risiken eine Einwilligung bei der Nutzung von Smartglasses im Alltag derzeit nur in seltenen Fällen,

---

797 *Schmitt Glaeser*, ZRP 2000, S. 395 (399).

798 Vgl. BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 95 f.

799 BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42); *Jarass*, NJW 1989, S. 857 (860); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 197; *Schmitt Glaeser*, ZRP 2000, S. 395 (399).

800 OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087.

801 *Schmidt*, in: *Dieterich u.a.*, ErfK, Einleitung, Rn. 65.

802 *Jarass*, NJW 1989, S. 857 (860).

803 Ebenda.

804 BVerfG, Beschl. v. 18.8.1981 (2 BvR 166/81), NJW 1982, 375; *Geiger*, NVwZ 1989, S. 35 (37); *Jarass*, NJW 1989, S. 857 (860).

z.B. im Rahmen beschränkter Veranstaltungen oder Örtlichkeiten oder im Verhältnis zu nahestehenden Personen, zu erwarten sein.

III. Interessen der Nutzer von Smartglasses

Nach der Feststellung der Beeinträchtigung der Grundrechte Betroffener ist zu prüfen, ob die Eingriffe nicht durch höherrangige Interessen der Nutzer von Smartglasses gerechtfertigt sind. Allerdings müssen zuerst die verfassungsrechtlich geschützten Interessen der Datenbrillennutzer herausgearbeitet werden, bevor die Interessen beider Seiten gegeneinander abgewogen werden können. Da Smartglasses jedoch in fast jedem Lebenskontext eingesetzt werden können und eine erschöpfende Übersicht aller Rechtsgüter den Rahmen dieser Untersuchung sprengen würde, werden im Folgenden nur die typischerweise zu erwartenden Interessen berücksichtigt.

1. Kommunikationsfreiheiten aus Art. 5 Abs. 1 GG

Bei der Erstellung von Aufnahmen, Gewinnung sonstiger Informationen oder deren Verbreitung und Veröffentlichung handelt es sich um Nutzungen von Smartglasses, die typischerweise in den Schutzbereich der grundgesetzlich geschützten Kommunikationsfreiheiten fallen.[805] Dabei wird der Schwerpunkt der rechtlichen Relevanz der Kommunikationsfreiheit im Rahmen dieser Prüfung vor allem in der Aufnahme von Informationen liegen.

a) Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 HS. 1 GG

Die Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 HS. 1 GG gewährleistet jedermann, sich aus allgemeinen Quellen zu unterrichten, sei es durch passive oder durch aktive Informationsaufnahme.[806] Systematisch wird die Informationsfreiheit im Verbund mit der Meinungs- und Medienfreiheit betrachtet, welche die Verarbeitung und Entäußerung von Tatsachen und Meinungen gewährleistet, während die Informationsfreiheit deren Beschaffung schützt.[807]

---

[805] Zur Klassifizierung und Gruppierung der Kommunikationsfreiheiten, Vgl. *Pieroth u.a.*, Grundrechte, 2014, Rn. 591.

[806] BVerfG, Beschl. v. 3.10.1969 (1 BvR 46/65), BVerfGE 27, 71 (82 f.); *Pieroth u.a.*, Grundrechte, 2014, Rn. 610.

[807] *Grabenwarter*, in: *Maunz/Dürig*, GG, Art.5, Rn. 76; *Köppen*, Das Grundrecht der Informationsfreiheit unter besonderer Berücksichtigung der neuen Medien, 2004, S. 41 ff.

aa) Art, Qualität sowie Bestimmung der Informationen und ihrer Quellen

Als Informationsquelle kommt sowohl jeder denkbare Träger von Informationen als auch der Gegenstand der Information selbst in Betracht.[808] D.h., es ist nicht nur die Unterrichtung aus einer Quelle, wie z.B. Presseerzeugnissen, Fernsehen, Rundfunk oder dem Internet, geschützt, sondern auch die Unterrichtung an der Quelle selbst.[809] Folglich können alle Daten, auch solche, die personenbezogen sind, Informationsquellen i.S.d. Informationsfreiheit sein.[810] Dementsprechend kommen sowohl einzelne Personen als auch deren Anwesenheit an einem bestimmten Ort, ihr Verhalten, das Aussehen oder ihre Äußerungen als Informationsquellen in Frage.[811]

Wegen der systematischen Einordnung der Informationsfreiheit als ein Vorfeldrecht der Meinungsfreiheit könnten jedoch Informationen, die rein technischen Vorgängen dienen, aus dem Schutzbereich der Informationsfreiheit ausgeschlossen sein. Dazu könnten z.B. Aufnahmen von Personen gehören, die primär nicht meinungsbildenden, sondern biometrischen Vorgängen oder der Registrierung von virtuellen Objekten in einer Augmented Reality dienen.[812] Gegen eine solche Einschränkung der Informationsfreiheit spricht jedoch, dass Smartglasses als Alltagsbegleiter von Menschen generell dazu dienen, ihnen eine breitere Tatsachenbasis zu verschaffen.[813] Daher sind i.d.R. alle Informationen unter die Meinungsfreiheit zu subsumieren, wenn der Rezipient sie nach eigenen Kriterien sichten und bewerten kann.[814] Dazu kann z.B. gehören, dass dank Augmented Reality der Informationsmehrwert von physischen Objekten

---

[808] *Pieroth u.a.*, Grundrechte, 2014, Rn. 606.

[809] BVerfG, Beschl. v. 24.1.2001 (1 BvR 2623/95 u. 1 BvR 622/99), BVerfGE 103, 44 (60); zum Fernsehen als Informationsquelle; BVerfG, Beschl. v. 27.3.1973 (2 BvR 684/72), BVerfGE 35, 307 (309); *Fink*, in: *Spindler/Schuster*, Recht der elektronischen Medien, VerfassungsR, Rn.12; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 73.

[810] Vgl. *Gallwas*, NJW 1992, S. 2785 (2787); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 73; *Pieroth u.a.*, Grundrechte, 2014, Rn. 609.

[811] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 74, 82; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 190.

[812] Vgl. B III. 5. d), S. 47.

[813] Zum Einsatz technischer Geräte als Grundlage der Informationsbeschaffung, vgl. "Parabolantenne", BVerfG, Beschl. v. 9.2.1994 (1 BvR 1687/92), BVerfGE 90, 27 (32 f.); "Fernsehgerät", BVerfG, Beschl. v. 27.3.1973 (2 BvR 684/72), BVerfGE 35, 307 (309).

[814] BVerfG, Urt. v. 5.8.1966 (1 BvR 586/62, 1 BvR 610/63 u. 1 BvR 512/64), BVerfGE 20, 162 (174 f.); *Fink*, in: *Spindler/Schuster*, Recht der elektronischen Medien, VerfassungsR, Rn.12; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 74.

durch virtuelle Informationen gesteigert wird. Es kann sich hierbei auch um so profane Dinge handeln wie z.B. die Einblendung von Nährwerten eines Lebensmittels als Grundlage einer der Kaufentscheidung vorgehenden Meinungsbildung.

Vor dem Hintergrund der eigenen Würdigung der erfassten Informationen durch die Nutzer von Smartglasses stellt sich ferner die Frage, ob sie sich auch im Fall des Live-Streamings auf die Informationsfreiheit berufen können. In dieser Konstellation können die Aufnahmen nicht für die Nutzer von Smartglasses, sondern nur für bestimmte Personen oder Webcam ähnlich für die Wahrnehmung durch die Öffentlichkeit bestimmt sein. Würde man jedoch beim Live-Streaming die Berufung auf die Informationsfreiheit verneinen, müsste man sie konsequenterweise auch den Medientätigen bei Live-Übertragung im Fernsehen oder Radio absprechen. Eine solche Sichtweise wäre jedoch vor dem Hintergrund der Meinungs- und Medienfreiheit nicht haltbar. Bereits die Entscheidung, ob ein Geschehen erfasst wird, in welchem Umfang, aus welchem Winkel etc., stellt eine würdigende und meinungsprägende Handlung des Datenrillenbrillennutzers dar.[815] Er ist also mehr als eine „Kamera", die objektiv ein Geschehen „durchleitet", sondern stellt eine selbstbestimmte und subjektive Sicht auf die Dinge dar.[816] Folglich können sich Nutzer von Smartglasses auch beim Live-Streaming auf die Informationsfreiheit berufen.

bb) Allgemeine Quellen

Die Informationsfreiheit erhält eine Limitierung, indem sie nur ein Recht auf Unterrichtung aus allgemein zugänglichen Quellen gewährt.[817] Allgemein zugänglich bedeutet, dass die Quelle der Öffentlichkeit gewidmet oder dazu bestimmt ist, einem individuell nicht bestimmten Personenkreis von ihrem Inhalt Kenntnis zu verschaffen.[818] Maßgeblich ist dafür die tatsächliche bzw. technische Zugänglichkeit der Informationen, die

---

[815] So auch im Hinblick auf Panoramastraßenansichten, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 80.

[816] *Mann/Niedzviecki*, Cyborg, 2002, S. 24.

[817] Aufgrund des fehlenden Rechts auf die Schaffung von Informationsquellen, sondern Beschränkung auf die Abwehr der Beschränkungen des Zugangs zu bestehenden allgemeinen Informationsquellen, wir die Informationsfreiheit insoweit nicht als ein umfassendes, sondern nur ein abwehrendes Grundrecht betrachtet, *Bohne*, NVwZ 2007, S. 656 (658); *Roßnagel*, MMR 2007, S. 16 (17).

[818] St. Rspr., BVerfG, Beschl. v. 24.1.2001 (1 BvR 2623/95 u. 1 BvR 622/99), BVerfGE 103, 44 (60); BVerfG, Beschl. v. 3.10.1969 (1 BvR 46/65), BVerfGE 27, 71 (83); BVerwG, Urt. v. 3.12.1974 (I C 30.71), BVerwGE 47, 247 (252).

nach objektiven Kriterien zu beurteilen ist und zudem durch Gesetze oder behördliche Entscheidungen festgelegt werden kann.[819]

Im Fall der Nutzung von Smartglasses ist vor allem zu fragen, ob die visuell, akustisch oder elektronisch erfassten Informationen dazu bestimmt waren, jedermann als eine Informationsquelle zur Verfügung zu stehen. Hierbei muss vor allem berücksichtigt werden, ob Informationen Zugangsschranken unterliegen, die deren Wahrnehmung durch jedermann verhindern sollen. Hierbei kann die bereits zur Bestimmung der Grenzen des öffentlichen Raums getroffene Unterscheidung zwischen abstrakten Zugangshindernissen (z.B. Eintrittsgeldern) und konkreten Zugangshindernissen (z.B. Betriebszugehörigkeit, Ladung zu einer Veranstaltung) angewandt werden.[820] Während eine abstrakte Beschränkung jedermann Zutritt gewährt, schließt eine konkrete Zugangsschranke die allgemeine Zugänglichkeit der hinter ihr befindlichen Informationen aus.[821]

Dementsprechend stellt der öffentliche Raum generell eine allgemeine Informationsquelle dar, weil er einen Raum des sozialen Lebens darstellt und dementsprechend jedermann als Informationsquelle dient.[822] Dagegen werden nicht öffentliche Räume, wie z.B. Wohnungen oder nicht dem Publikumsverkehr gewidmete Geschäftsräumlichkeiten, die der Dispositionsbefugnis ihrer Bewohner oder Eigentümer gem. Art. 13 Abs. 1 GG oder Art. 14 Abs. 1 GG unterfallen, generell nicht allgemein zugänglich sein.[823] Das wird auch dann anzunehmen sein, wenn Nutzer von Smartglasses in fremde Räumlichkeiten, z.B. durch geöffnete Fenster, hineinbli-

---

[819] BVerfG, Beschl. v. 24.1.2001 (1 BvR 2623/95 u. 1 BvR 622/99), BVerfGE 103, 44 (59 ff.); BVerfG, Beschl. v. 16.7.1969 (1 BvL 19/63), BVerfGE 27, 1 (83 ff.); BVerwG, Urt. v. 16.9.1980 (1 C 52/75), BVerwGE 61, 15 (22); *Pieroth u.a.*, Grundrechte, 2014, Rn. 608; Ebenda, Rn. 608; *Roßnagel*, MMR 2007, S. 16 (17).

[820] Vgl. A IV. 9, S. 18.

[821] Vgl. A IV. 9, S. 18.

[822] Der Mensch ist im sozialen Kontext zwangsläufig ein Informationsgeber, BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (44); Eigentümer von Gebäuden haben es nach dem BGH zu dulden, wenn deren Fassaden vom öffentlichen Raum aus fotografiert werden, auch wenn die Fotografien geschäftlich verwertet werden, BGH, Urt. v. 17.12.2010 (V ZR 45/10), GRUR 2011, 323 (324); BGH, Urt. v. 9.3.1989 (I ZR 54/87), NJW 1989, 2251 (2252); *Jahn/Striezel*, K&R 2009, S. 753 (756); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 78; *Spiecker genannt Döhmann*, CR 2010, S. 311 (315).

[823] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 79.

cken können, da die Fenster den Bewohnern zum Hinaus-, aber nicht jedermann zum Hineinblicken dienen (anders als z.B. Schaufenster).[824]

Die Zugänglichkeit einer Informationsquelle für die Allgemeinheit könnte jedoch entfallen, wenn es sich um einen Raum des Rückzugs handeln würde, der als Grundlage einer räumlichen Privatsphäre geeignet wäre.[825] Ebenso könnten Umstände, die der inhaltlichen Privatsphäre unterfallen, wie z.B. die Nacktheit der Menschen an einem Badestrand, gegen deren allgemeine Zugänglichkeit als Informationsquellen sprechen.[826] Eine solche Beschränkung würde jedoch die im Art. 5 Abs. 2 GG vorgesehene Abwägung der Privatsphäreninteressen mit der Informationsfreiheit vorwegnehmen oder sie gar unmöglich machen.[827] So könnten z.B. für die Öffentlichkeit sehr relevante Informationen über einen Politiker generell nicht verwertet werden, wenn deren privater Charakter ein kategorisches Verwertungsverbot darstellen würde.[828] Folglich gebietet die gesetzliche Zielsetzung der Informationsfreiheit, den öffentlichen Raum insgesamt als allgemein zugänglich zu betrachten und etwaige Interessen der Betroffenen auf der Rechtfertigungsebene des Art. 5 Abs. 2 GG auszugleichen.

Neben den räumlichen Zugangsschranken können sich Schranken auch aus der persönlichen Natur von Informationen ergeben. Z.B. ist zu fragen, ob die Wärmebilderfassung von Personen im öffentlichen Raum der Informationsfreiheit unterfällt. Dafür spräche zunächst, dass Menschen sich in der Öffentlichkeit bewegen und damit sich objektiv bewusst sind, von Dritten wahrnehmbare Informationen „auszustrahlen".[829] Auf der anderen Seite rechnet bei objektiver Betrachtung niemand mit einer Erfassung der körperlichen Vorgänge, die unter die äußerlich mit den Augen sichtbare „Hülle" des Menschen reicht.[830] Ferner spricht gegen eine allgemeine Zugänglichkeit jenseits der äußeren Wahrnehmung die Ausstrahlungswirkung der Menschenwürde, nach der die inneren körperlichen Vorgänge oder die Nacktheit eines Menschen dem Privat- oder sogar dem Intim-

---

[824] Im Fall der Street View-Aufnahmen wurde die allgemeine Zugänglichkeit z.T. dort verneint, wo die auf dem Dach der Erfassungsfahrzeuge in ca. 3-4m Höhe angebrachten Kameras, über das den Menschen zugängliche Straßenniveau von ca. 2m blicken und so z.B. Sichtschutz in Form von Hecken überwinden konnten, S. *Spiecker genannt Döhmann*, CR 2010, S. 311 (315).

[825] Vgl. E II. 2. a) dd) (1), S. 110.

[826] Vgl. E II. 2. a) dd) (2), S. 112.

[827] So im Ergebnis *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 6; ebenso *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 14.

[828] Vgl. BGH, Urt. v. 30.9.2014 (VI ZR 490/12), ZD 2015, 227 (228) ff.

[829] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 78.

[830] *Busche*, DÖV 2011, S. 225 (230).

sphäre zuzuordnen sind.[831] Es wäre vor diesem Hintergrund widersinnig, wenn das Innere einer Wohnung nicht allgemein zugänglich wäre, die inneren körperlichen Vorgänge des Menschen dagegen schon.[832]

cc) Aufzeichnung und Verwendung der Informationen

Der Begriff der Unterrichtung aus allgemein zugänglichen Quellen umfasst notwendigerweise die Erhebung von Informationen. Daneben wird aber auch die Speicherung der Informationen als ein denknotwendiger Schritt bejaht, da die Informationsfreiheit sonst ihrer Funktion als Grundlage der Meinungsbildung nicht gerecht werden könnte.[833] Eine verantwortliche Meinung kann nur gebildet werden, wenn die erhobenen Informationen betrachtet und bewertet werden können, was deren nicht flüchtiges Vorliegen erfordert.[834]

Die weitere Verwendung der Informationen unterfällt dagegen nicht der Informationsfreiheit, sondern kann nur durch andere, sachnähere Grundrechte geschützt werden.[835] Hierzu gehören z.B. die Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 HS. 2 GG und die Medienfreiheiten aus Art. 5 Abs. 1 Satz 2 GG. Aufgrund dieser sachlichen Grenzen und aufgrund der Beschränkung auf allgemeine Informationsquellen wird das Verständnis der Informationsfreiheit als ein allgemeines Datenumgangsrecht abgelehnt.[836]

Im Fall von Smartglasses bedeutet dies, dass die Erhebungs- und Speicherungsvorgänge, gleich welchen Zwecks, von dem Schutzbereich der Informationsfreiheit erfasst werden. Dagegen muss deren Veröffentlichung, Verbreitung oder sonstige Nutzung durch speziellere Grundrechte gerechtfertigt werden. Im Hinblick auf die Gewinnung weiterer Daten aus den bereits erfassten Informationen, wie z.B. die biometrische Auswertung von Videoaufnahmen, ist jedoch wiederum der Schutz der Informationsfreiheit einschlägig, da es sich hierbei um eine weitere Stufe der „Unterrichtung“ handelt.

---

831 Vgl. E II. 2. b) aa), S. 113.

832 Vgl. zu der Frage des Eindringens in die Privatsphäre durch Thermalbeobachtung die US-Entscheidung, Kyllo v. United States, 533 U.S. 27 (2001), 28.

833 *Fink*, in: *Spindler/Schuster*, Recht der elektronischen Medien, VerfassungsR, Rn.20; *Köppen*, Das Grundrecht der Informationsfreiheit unter besonderer Berücksichtigung der neuen Medien, 2004, S. 122; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 189.

834 *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 75.

835 Ebenda, 76.

836 Ebenda, 77.

dd) Sousveillance

Steve Mann setzte sich im Rahmen der Entwicklung von Smartglasses auch mit deren Einfluss auf die Gesellschaft auseinander und vertritt die Ansicht, dass Smartglasses ein Abwehrmittel gegen die zunehmende „orwellsche" Überwachung durch wirtschaftliche oder staatliche Institutionen darstellen.[837] Dieses Konzept bezeichnet Mann als „Sousveillance", also eine Beobachtung „von unten" (als Kontrast zur Überwachung „von oben", die im englischsprachen Raum als „Surveillance" bezeichnet wird).[838]

Laut Mann ist diese Form der „Zurückbeobachtung" notwendig, da die derzeitigen Formen der Überwachung „von oben" zu einer asymmetrisch verteilten Macht führen.[839] Dabei sind laut Mann die Grenzen der Focault'schen Metapher des Panoptikums längst überschritten, da diese nicht mehr ausreichend ist, die Machtverteilung zu beschreiben, welche durch mobile und ubiquitäre Rechner entstanden ist.[840] Als Beispiel für Sousveillance dient z.B. das sog. „cop watching", d.h. die Videoaufzeichnung und Verbreitung von polizeilichen Übergriffen durch die Bürger.[841] Im Ergebnis soll so durch Sousveillance eine Machtparität zwischen der auf visueller Überwachung beruhenden institutionellen Macht und der Macht der Bürger entstehen (Mann bezeichnet dieses Gleichgewicht als „Equiveillance").[842] Ohne diesen Ausgleich würde die Asymmetrie der Überwachung zwischen den staatlichen und den wirtschaftlichen Akteuren auf der einen und den Bürgern auf der anderen Seite weiterhin wachsen. Sich alleine auf die Wahrung der Überwachungsparität durch Machtinstanzen zu verlassen, ist laut Mann als Alternative nicht ausreichend, da der Überwachung immer ein Interessenkonflikt inhärent ist, z.B. die Gefahr, dass Polizisten Beweismaterial unterschlagen.[843]

Als allzeit präsente und schnell auslösbare Aufnahme- und Übertragungsgeräte sind Smartglasses prädestiniert, Menschen mit der Befähi-

---

[837] *Mann/Ferenbok*, Surveillance and Society 2013, Vol. 11, Nr. 1/2, p. 18; *Mann*, IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10 (12).

[838] Der Begriff "Sousveillance" leitet sich von dem französischen Begriff "veiller", d.h., "bewachen" ab, verbunden mit dem Vorsilbe "sous", französisch für "von unten" (im Kontrast zu der in dem Begriff "Surveillance" verwendeten Vorsilbe "sur", also "von oben"), *Mann*, IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10 (12).

[839] *Mann/Ferenbok*, Surveillance and Society 2013, Vol. 11, Nr. 1/2, p. 18 (19).

[840] Ebenda, 22 ff.

[841] Vgl. BVerfG, Beschl. v. 24.7.2015 (1 BvR 2501/13), ZUM 2015, 986 (987 f.); vgl. *Fuchs u.a.*, Introduction, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 1 (12); *Schaefer/Steinmetz*, Surveillance & Society 2014, Vol. 12, Nr. 4, p. 502 (502 ff.).

[842] *Mann/Ferenbok*, Surveillance and Society 2013, Vol. 11, Nr. 1/2, p. 18 (26).

[843] Ebenda, 20.

gung zur Sousveillance auszustatten. Zu fragen ist daher, wie die mit der Sousveillance zusammenhängenden Interessen der Nutzer von Smartglasses verfassungsrechtlich zu verorten sind. Da es bei Sousveillance zuerst um die Sammlung von Informationen durch Bürger geht, ist die Berufung auf die Informationsfreiheit gem. Art. 5 Abs. 1 Satz 1 HS. 1 GG die sachlich am nächsten liegende Wahl. Die weitere Verwendung der erworbenen Information wird wiederum den speziellen Grundrechten, wie z.B. der Meinungsfreiheit, zuzuordnen sein.

b) Negative Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 HS. 1 GG

Betrachtet aus der Sicht der Informationsflüsse, lässt sich die Privatsphäre in den Schutz des Informationsabflusses und den Schutz des Informationszuflusses unterteilen.[844] Dabei stellt die negative Informationsfreiheit ein Pendant zur negativen Meinungsfreiheit dar, welche ein negatives Recht enthält, eine Meinung nicht zu haben oder sich nicht zu äußern.[845] Zwar ist es im einzelnen umstritten, inwieweit ein Abblocken von Informationszuflüssen der negativen Informationsfreiheit oder dem Schutzbereich des Allgemeinen Persönlichkeitsrechts zuzuordnen ist.[846] Jedoch wird die negative Informationsfreiheit z.B. als einschlägig im Fall sog. „Adblock"-Filter betrachtet.[847] Bei „Adblock"-Filtern handelt es sich um Werbefilter für Internetbrowser, die Werbeanzeigen aus Internetseiten herausfiltern und entfernen.[848] Zumindest Smartglasses mit Mediated-Reality-Funktion können dazu beitragen, die Reizüberflutung durch Informationszuflüsse zu senken, indem sie visuelle Informationen ähnlich

---

[844] *Mann/Niedzviecki*, Cyborg, 2002, S. 147.

[845] Obiter dictum, in BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (40 f.); *Grabenwarter*, in: *Maunz/Dürig*, GG, Art.5, Rn. 95 f.

[846] Das BVerfG hat das Recht "in Ruhe gelassen zu werden" als Teil des privaten Lebensbereichs anerkannt, und vor dem Hintergrund des Schutzes vor Zwang zur politischer Teilnahme im Allgemeinen Persönlichkeitsrecht verortet, BVerfG, Beschl. v. 2.3.1977 (2 BvR 1319/76), BVerfGE 44, 197 (203); auch der Schutz vor Werbenachrichten wird dem Allgemeinen Persönlichkeitsrecht zugerechnet (bzw. dem insoweit vergleichbaren Recht aus eingerichtetem und ausgeübten Gewerbebetrieb), BGH, Beschl. v. 20.5.2009 (I ZR 218/07), GRUR 2009, 980 (981); BGH, Urt. v. 8.11.1989 (I ZR 55/88), NJW-RR 1990, 359 (359 f.); in der Literatur wird die dogmatische Konstruktion als negatives Recht zum Teil gänzlich angezweifelt, *Grabenwarter*, in: *Maunz/Dürig*, GG, Art.5, Rn. 98 f.; *Hellermann*, Die sogenannte negative Seite der Freiheitsrechte, 1993, S. 28 ff., 147 ff. ; *Hufen*, DÖV 1983, S. 353 (358); auf der anderen Seite wird der Informationsfreiheit als Abwehrrecht denknotwendig ein Recht zur Auswahl von Informationsquellen- und Möglichkeiten entnommen, *Fikentscher/Möllers*, NJW 1998, S. 1337 (1340); oder es wurd darauf verwiesen, dass negative Grundrechte generell anerkannt sind, *Herzog*, in: *Maunz/Dürig*, GG, Art.4, Rn. 78; ebenso für ein negatives Informationsrecht sprechend, *Jutzi*, NVwZ 2008, S. 603 (604); *Pieroth u.a.*, Grundrechte, 2014, Rn. 610.

[847] LG München I, Urt. v. 27.5.2015 (37 O 11673/14), MMR 2015, 660 (664)

[848] *Becker/Becker*, GRUR-Prax 2015, S. 245.

wie „Adblock"-Filter aus dem Sichtbereich ihrer Nutzer durch virtuelle Überlagerungen entfernen. Daher kann diese Filterfunktion der Smartglasses, ein durch die negative Informationsfreiheit oder bei alternativer Betrachtung durch das Allgemeine Persönlichkeitsrecht geschütztes Interesse an der Kontrolle von Informationszuflüssen begründen.[849]

c) Meinungs- und Medienfreiheiten

Während das Sammeln und Speichern von Informationen mittels Smartglasses der Informationsfreiheit unterfällt, kann die Veröffentlichung und Verbreitung von Informationen durch die Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 HS. 2 GG geschützt sein.[850] Je nach Umständen kann sogar ein Schutz durch die Presse- und Rundfunkfreiheit gem. Art. 5 Abs. 1 Satz 2 GG in Frage kommen, wenn die Nutzung von Smartglasses dem weiten Bereich des institutionellen Meinungs- und Medienschutzes unterfällt.[851] Die über die Informationserhebung hinausgehende Komponente der Kommunikationsfreiheit bringt jedoch keine für Smartglasses typischen Problemstellungen mit sich und wird daher im Rahmen dieser Untersuchung nicht vertieft.[852]

2. Kunstfreiheit aus Art. 5 Abs. 3 Satz 1 Var. 1 GG

Neben einer Meinungskundgabe könnten Smartglasses auch für Kunstzwecke eingesetzt werden. Neben klassischen Mitteln der Fotografie oder Videokunst sind auch neuartige Einsatzmöglichkeiten wie z.B. virtuelle Graffiti vorstellbar, die lediglich informatorisch als Augmented-Reality-Objekte in der physischen Welt verankert werden.[853] Im Rahmen solcher Anwendungsszenarien werden sich die Nutzer von Smartglasses auf die Kunstfreiheit berufen können. Die Kunstfreiheit ist nicht auf die traditionellen Werktypen und Ausdrucksformen beschränkt. Vielmehr liegt entsprechend dem offenen Kunstbegriff das kennzeichnende Merkmal einer künstlerischen Äußerung darin, „dass es wegen der Mannigfaltigkeit ihres Aussagegehalts möglich ist, der Darstellung im Wege einer fortgesetzten Interpretation immer weiterreichende Bedeutungen zu entnehmen, so dass sich eine praktisch unerschöpfliche, vielstufige Informationsvermitt-

---

[849] Vgl. B III. 5. c), S. 46.

[850] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (41); BVerfG, Beschl. v. 22.6.1982 (1 BvR 1376/79), BVerfGE 61, 1 (8); *Grimm*, NJW 1995, S. 1697 (1698); *Pieroth u.a.*, Grundrechte, 2014, Rn. 594.

[851] BVerfG, Urt. v. 5.8.1966 (1 BvR 586/62, 1 BvR 610/63 u. 1 BvR 512/64), BVerfGE 20, 162 (175); *Lent*, ZUM 2013, S. 914 ff.; *Pieroth u.a.*, Grundrechte, 2014, Rn. 615, 620 f.

[852] D.h. im Hinblick auf die getrennt von der Erhebung der Informationen für sich zu betrachtenden Veröffentlichungs- oder Verbreitungshandlungen könnten diese genauso gut auf Grundlage von Aufnahmen eines Smartphones erfolgen.

[853] Vgl. B IV. 3. f), S. 55.

lung ergibt".[854] Ebenfalls ist nicht nur das künstlerische Wirken selbst, sondern auch der Wirkbereich der Kunst vom Schutzbereich mit umfasst.[855] D.h., dass auch die Veröffentlichung und Verbreitung der mittels Smartglasses geschaffenen künstlerischen Kreationen oder Aktionen von der Kunstfreiheit mit umfasst wird.

3. Wissenschaftsfreiheit aus Art. 5 Abs. 3 Satz 1 Var. 2 GG

Gegenstand der Freiheit der Wissenschaft, Forschung und Lehre sind vor allem die auf wissenschaftlicher Eigengesetzlichkeit beruhenden Prozesse, Verhaltensweisen und Entscheidungen bei der Suche nach Erkenntnissen, ihrer Deutung und Weitergabe.[856] Der Begriff der Wissenschaft wird hierbei weit als alles, was nach Inhalt und Form als ernsthafter Versuch zur Ermittlung von Wahrheit anzusehen ist, bezeichnet.[857] Zum Schutzbereich der Wissenschaftsfreiheit gehört auch der Prozess der Gewinnung und Vermittlung von wissenschaftlichen Erkenntnissen.[858] Smartglasses sind somit durch die Möglichkeiten einer anschaulicheren und schnellen Vermittlung von Lehrinhalten, der Visualisierung und Simulation von technischen Vorgängen sowie kollaborativer Zusammenarbeit dafür prädestiniert, für Zwecke der Wissenschaft, Forschung und Lehre eingesetzt zu werden, sodass sich ihre Nutzer insoweit auf diese Interessen berufen können.[859]

4. Körperliche Unversehrtheit aus Art. 2 Abs. 2 GG

Auf den Schutz der körperlichen Unversehrtheit können sich die Nutzer von Smartglasses zum einen berufen, wenn sie die Geräte einsetzen, um ihre Gesundheit oder ihr Leben zu schützen, z.B. wie bei klassischer Videoüberwachung durch Abschreckung von Angreifern.[860]

Ein weiterer Fall des Art. 2 Abs. 2 GG, der mit fortschreitender Verbreitung von Smartglasses eintreten könnte, ist die Gewöhnung und Anpassung ihrer Nutzer an die Geräte. Bereits Smartphones sind für viele Menschen wie der Hausschlüssel und das Portemonnaie zu ihren täglichen

---

[854] BVerfG, Beschl. v. 17.7.1984 (1 BvR 816/82), BVerfGE 67, 213 (227).

[855] BVerfG, Beschl. v. 24.2.1971 (1 BvR 435/68), BVerfGE 30, 173 (189).

[856] BVerfG, Beschl. v. 13.4.1994 (1 BvR 23/94), BVerfGE 90, 1 (11 f.).

[857] BVerfG, BVerfGE 35, 79 v. 29.5.1973 (1 BvR 424/71 u. 325/72), BVerfGE 35, 1176 (113).

[858] BVerfG, Beschl. v. 13.4.1994 (1 BvR 23/94), BVerfGE 90, 1 (12).

[859] Vgl. BIV.3, S. 52.

[860] Vgl. B III. 1, S. 35.

Begleitern geworden.[861] Smartglasses könnten diesen Gewohnheitseffekt erheblich verstärken und als eine effiziente Schnittstelle für die virtuelle Welt ähnlich unentbehrlich werden wie eine Korrekturbrille.[862]

Daher erscheint auch eine Beeinträchtigung der körperlichen Integrität möglich, wenn Smartglasses als eine prothetische Erweiterung des Körpers und deren Verlust als ein körperlicher Schaden empfunden werden.[863] Das würde jedoch voraussetzen, dass Smartglasses für das Bestreiten des Alltags nach objektiven Maßstäben ähnlich essentiell wären wie eine Korrekturbrille. Eine solche Notwendigkeit ist derzeit zwar nicht ersichtlich, könnte sich jedoch ergeben, z.B. wenn die persönliche Sicherheit im Straßenverkehr von der Kommunikation zwischen Smartglasses und autonomen Fahrzeugen abhängen würde.[864]

Bereits heute könnten sich Nutzer von Smartglasses auf Art. 2 Abs. 2 GG berufen, wenn Smartglasses ihnen als Mittel dienen, um als Krankheit geltende körperliche Beeinträchtigungen, wie z.B. eine starke Sehbeeinträchtigung oder die Beeinträchtigung motorischer Fähigkeiten, auszugleichen.[865]

5. Sonstige Grundrechte

Die Nutzer von Smartglasses könnten sich ferner auf die Versammlungsfreiheit aus Art. 8 Abs. 1 GG berufen, wenn sie die Geräte einsetzen wür-

---

[861] Im Mai 2014 nutzen bereits 50% der Deutschen ein Smartphone, 63% davon nutzen es täglich, was eine Zunahme der täglichen Nutzung von 21% innerhalb eines Jahres bedeutet, Bundesverband Digitale Wirtschaft, Faszination Mobile Verbreitung, Nutzungsmuster und Trends, 2014, http://www.bvdw.org/mybvdw/media/view?media=5727 (7.1.2014), S. ; zu ähnlichen Ergebnissen kommt die Studie von ARD/ZDF, ard-zdf-onlinestudie.de, ARD-ZDF Onlinestudie: Mobile Nutzung, 2015, http://www.ard-zdf-onlinestudie.de/index.php?id=493 (22.8.2015); S. auch Auswertung von *Schart/Tschanz*, Augmented Reality, 2015, S. 59; laut einer Studie der University of Missouri soll sich die Abwesenheit von Smartphones sogar auf die kognitiven Fähigkeiten ihrer Nutzer auswirken, *Clayton/Leshner/Almond*, JCMC 2015, Vol. 20, Nr. 2, p. 119; vgl. *Leffler*, Cyber-Bullying, 2012, S. 125; *Menkens*, Wir sind Sklaven unserer Smartphones geworden, Welt Online, http://www.welt.de/debatte/kommentare/article108283729/Wir-sind-Sklaven-unserer-Smartphones-geworden.html (19.12.2014).

[862] *Mann*, IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10 (12).

[863] Mann iseht die von ihm getragenen Smartglasses als einen Teil seines Körpers an, *Mann/Niedzviecki*, Cyborg, 2002, S. 17.

[864] Vgl. B IV. 2, S. 51.

[865] Vgl. B IV. 3. d), S. 53; vgl. AG Köln, Urt. v. 20.12.1994 (208 C 57/94), NJW-RR 1995, 1226 (1227); *Brown/Harmon/Waelde*, IIC 2012, p. 901 (902 ff.); *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2 Abs.2 S.2, Rn. 56.

den, um z.B. tätliche Auseinandersetzungen und Übergriffe durch Gegendemonstranten oder Polizeibeamten zu dokumentieren.[866]

Des Weiteren können Smartglasses in vielfältiger Weise berufsmäßig i.S.d. Art. 12 Abs. 1 GG eingesetzt werden. Zu denken ist z.B. an den Einsatz bei Wachpersonal, das verdächtige Vorgänge aufzeichnen kann, über einen Techniker, der mittels Smartglasses effizienter Maschinen warten kann, oder Teilnehmer einer überörtlichen Besprechung, die ein mittels Augmented Reality dargestelltes Besprechungsobjekt vor sich sehen. Ferner kommt der Einsatz im Tourismus, Marketing oder Verkauf in Frage.[867] Da sich die Untersuchung jedoch primär der privaten Nutzung von Smartglasses widmet, werden diese Aspekte nicht weiter vertieft.

Smartglasses können ebenfalls zum Schutz des Eigentums eingesetzt werden, welches gem. Art. 14 Abs. 1 GG alle privatrechtlichen Vermögenswerte erfasst. Vorstellbar ist z.B. Objektsicherung oder Aufnahmen verdächtiger Personen in einer Menschenmenge, um diese im Fall eines Diebstahls von Eigentum verfolgen zu können.[868]

6. Allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG

Im Fall einer Nutzung von Smartglasses, die nicht durch die spezielleren Grundrechte erfasst wird, insbesondere einer Nutzung zwecks Bequemlichkeit, Unterhaltung, Erstellung von Erinnerungsbildern oder der Befriedigung von Neugierde, können sich die Nutzer von Smartglasses auf die subsidiär geltende und durch Art. 2 Abs. 1 GG geschützte allgemeine Handlungsfreiheit berufen.[869]

IV. Abwägung von Rechtsgütern

Nachdem die verfassungsrechtlich geschützten Interessen der Nutzer von Smartglasses herausgearbeitet wurden, müssen sie mit den beeinträchtigten Privatsphäreninteressen abgewogen werden. Das Ziel ist die Auflö-

---

[866] Zur Abbildung von Polizeibeamten bei Demonstrationen, vgl. BVerfG, Beschl. v. 24.7.2015 (1 BvR 2501/13), ZUM 2015, 986 (987 f.); von Gegendemonstranten, VGH München, Beschl. v. 16.10.2014 (10 ZB 13.2620), NVwZ-RR 2015, 104 (Rn. 8 ff.); *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 12.

[867] Vgl. B IV. 3, S. 52.

[868] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 84; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 193 f.

[869] Im Hinblick auf die Diskussion um ein "Grundrecht auf Sicherheit" und "Freisein von Furcht" ist Lang zuzustimmen, der ein solches Recht als gehaltlos betrachtet, da es lediglich eine Bündelung der Funktionen speziellerer Grundrechte darstellen würde, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 193; Ein "Grundrecht auf Sicherheit" verneinend, *Schellenberg*, ZRP 2014, S. 24 (25).

sung der Kollisionslage, die im Rahmen einer Gewichtung der einzelnen Interessen und deren Abwägung gegeneinander durchzuführen ist.[870]

Da die Schutzpositionen der Grundrechte gleichrangig nebeneinander stehen, ist eine abstrakte Präferenz der jeweiligen Interessen ausgeschlossen.[871] Die Gewichtung ist vielmehr im Rahmen der richterlichen Würdigung als auch bei der legislativ oder exekutiv ausgeübten Wahrnehmung staatlicher Schutzpflichten einzelfallbezogen im Wege einer praktischen Konkordanz herzustellen.[872] Dabei sind die Interessen der jeweiligen Parteien in ihrer Wechselwirkung zu sehen und so zu ordnen sowie zu begrenzen, „dass sie für alle Beteiligten möglichst weitgehend wirksam werden."[873] Erst wenn ein solcher Ausgleich nicht möglich ist, ist zu entscheiden, welches Grundrecht zurückzutreten hat.[874]

Das schwächere Grundrecht darf dabei unter Beachtung seines sachlichen Grundwertgehaltes nur so weit zurückgedrängt werden, wie dies logisch und systematisch zwingend erscheint.[875] Des Weiteren sind im Rahmen der Gewichtung der konkurrierenden Interessen auch die Grundsätze der Verhältnismäßigkeit zu berücksichtigen.[876]

Nachfolgend werden dementsprechend zuerst die Kriterien dargestellt, die zur Bemessung der Intensität der Privatsphärenbelastung maßgeblich sind. Anschließend werden sie mit den Interessen an der Nutzung von Smartglasses abgewogen.

---

[870] Vgl. E I, S. 89; vgl. *Gallwas*, NJW 1992, S. 2785 (2786).

[871] BVerfGE, Beschl. v. 19.10.1993 (1 BvR 567 u. 1044/89), BVerfGE 89, 214 (232); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 199 f.; *Schwenke*, Individualisierung und Datenschutz, 2006, S. 85.

[872] BVerfGE, Beschl. v. 19.10.1993 (1 BvR 567 u. 1044/89), BVerfGE 89, 214 (232); BVerfG, Beschl. v. 7.3.1990 (1 BvR 266/86 u. 1 BvR 913/87), BVerfGE 81, 278 (293); BVerfG, Beschl. v. 26.5.1970 (1 BvR 83/69, 1 BvR 244/69 u. 1 BvR 345/69), BVerfGE 28, 243 (261).

[873] BVerfGE, Beschl. v. 19.10.1993 (1 BvR 567 u. 1044/89), BVerfGE 89, 214 (232); BVerfG, Beschl. v. 8.2.1983 (1 BvL 20/81), BVerfGE 63, 131 (144); BVerfG, Beschl. v. 24.2.1971 (1 BvR 435/68), BVerfGE 30, 173 (195) ff.

[874] BVerfG, Beschl. v. 17.7.1984 (1 BvR 816/82), BVerfGE 67, 213 (228); BVerfG, Urt. v. 5.6.1973 (1 BvR 536/72), BVerfGE 35, 202 (255).

[875] BVerfG, Beschl. v. 26.5.1970 (1 BvR 83/69, 1 BvR 244/69 u. 1 BvR 345/69), BVerfGE 28, 243 (261).

[876] BVerfG, Beschl. v. 8.2.1983 (1 BvL 20/81), BVerfGE 63, 131 (144); zu berücksichtigen sind auch die im Rahmen von Maßnahmen der öffentlichen Gewalt entwickelten Grundsätze, BVerfG, Urt. v. 5.6.1973 (1 BvR 536/72), BVerfGE 35, 202 (221); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 200.

1. Gewichtung der Eingriffe in das Allgemeine Persönlichkeitsrecht

Da einfachgesetzliche Normen die Interessenlage modifizieren können, ist die konkrete Abwägung der Persönlichkeitsrechtsinteressen Betroffener und der Interessen an der Nutzung von Smartglasses im Einzelfall auf einfachgesetzlicher Ebene vorzunehmen.[877] Die Interessenabwägung auf verfassungsrechtlicher Ebene bleibt jedoch richtungsweisend und Maßstab sowie Ausgangspunkt für einfachgesetzliche Interpretationen von Normen und Generalklauseln sowie für Verhältnismäßigkeitsabwägungen.[878] Aus diesem Grund sollen an dieser Stelle bereits Abwägungskriterien berücksichtigt werden, die eng an die grundrechtlichen Positionen gekoppelt sind und für das einfachgesetzliche Abwägungsergebnis wesentlich prägend sein können.[879]

Um die Intensität der Beeinträchtigung der Privatsphäre zu bestimmen, müssen die Abwägungskriterien vor allem die Art, den Umfang und den Einsatz von Smartglasses berücksichtigen. Zu beachten ist jedoch, dass die Liste der Abwägungskriterien nicht erschöpfend ist und um weitere Kriterien ergänzt werden kann.

a) Schutzsphären des Allgemeinen Persönlichkeitsrechts

Als weitere Orientierungshilfe für die Bestimmung der Schutzhöhe des Allgemeinen Persönlichkeitsrechts im Rahmen von Abwägungen dienen sog. Schutzsphären, die jedoch im Einzelfall zu bestimmen sind.[880] Dabei wird der höchste Schutz der Intimsphäre zugestanden, die höchstpersönliche Lebensbereiche wie Sexualität oder Krankheiten umfasst.[881] Die Privatsphäre umfasst ferner Informationen, die sonst nachteilig für die Menschen werden und insbesondere zum Gefühl der Scham führen kön-

---

[877] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 85; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 201.

[878] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 201.

[879] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 85.

[880] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 158; *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 268 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 139; *Martin*, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, 2007, S. 255 f.; die Sphärentheorie wird als solche, d.h. als eine starre Konstruktion einzelner Sphären, durch das BVerfG nicht mehr angewendet, *Nebel*, ZD 2015, S. 517 (519); *Staudinger*, in: *Schulze*, BGB, § 823 BGB, Rn. 99; *Wanckel*, Persönlichkeitsschutz in der Informationsgesellschaft, 1999, S. 121.

[881] BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367 (374); BVerfG, Urt. v. 10.5.1957 (1 BvR 550/52), BVerfGE 6, 389 (433); *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 158; *Nebel*, ZD 2015, S. 517 (518); *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 40 ff.; *Staudinger*, in: *Schulze*, BGB, § 823 BGB, Rn. 99.

nen, welches als das Gefühl des Privaten schlechthin gilt.[882] Die Teilnahme des Menschen am gesellschaftlichen Leben wird dagegen als der Individualsphäre zugehörig weniger geschützt.[883] Den geringsten Schutz genießt die Öffentlichkeitssphäre, d.h., wenn eine Person sich bewusst der Öffentlichkeit zuwendet oder sich in der Öffentlichkeit äußert.[884] Zum Teil ist hier bereits die Eingriffsqualität fraglich.[885]

Je mehr die Nutzung von Smartglasses den höchstpersönlichen Bereich der Betroffenen berührt, desto intensiver ist die Verletzung ihrer Rechte. So wird die Intensität gering sein, wenn eine in der Öffentlichkeit sprechende Person auf einem belebten Platz aufgezeichnet wird.[886] Dagegen wird die Intimsphäre verletzt, wenn jemand mit aufgesetzten Smartglasses eine Umkleidekabine betritt, in der sich gerade eine Person entkleidet.[887]

b) Örtlicher und zeitlicher Umfang der Beeinträchtigung

Als Maßstab für die Intensität der Beeinträchtigung des Allgemeinen Persönlichkeitsrechts durch Überwachungsmaßnahmen werden vor allem deren örtliche Reichweite und ihre Dauer herbeigezogen. Je weniger sich die Personen der Überwachung räumlich und zeitlich entziehen können, desto höher ist die Eingriffswirkung.[888]

Die Grundsätze für diesen Maßstab wurden vor allem in Fällen der Überwachung von Arbeitnehmern und Nachbargrundstücken aufgestellt.[889] Im öffentlichen Raum ist es dagegen bisher grundsätzlich mög-

---

[882] Vgl. BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373; BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367; BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382); BGH, Urt. v. 28.10.2008 (VI ZR 307/07), BGHZ 178, 213; zum Schamgefühl S. *Sofsky*, Verteidigung des Privaten, 2007, S. 59.

[883] BVerfGE, Beschl. v. 11.4.1973 (2 BvR 701/72), BVerfGE 1973, 35 (39); BVerfG, Urt. v. 5.6.1973 (1 BvR 536/72), BVerfGE 35, 202 (220); *Die Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 160.

[884] BGH, Urt. v. 26.5.2009 (VI ZR 191/08), ZUM-RD 2009, 429 (433); BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (199).

[885] *Di Fabio*, in: *Maunz/Dürig*, GG, Art. 2, Rn. 161 Fn. 20.

[886] Vgl. E II. 2. a) dd), S. 110.

[887] BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545 (129); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 96.

[888] Vgl. BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 95.

[889] Vgl. BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437).

lich, sich der Videoüberwachung zu entziehen, indem z.B. ein videoüberwachter Ort gemieden wird.[890] Dennoch sind auch im öffentlichen Raum Zwangswirkungen zu erwarten, wenn z.B. ein Nachbar seine Smartglasses ständig trägt und dadurch die übrigen Anwohner der Straße jedes Mal, wenn sie ihr Haus verlassen, mit einer Erfassung rechnen müssen.[891] Ferner kann das zeitliche und räumliche Moment der Unausweichlichkeit auch bei räumlich und zeitlich beschränkter Beeinträchtigung der Privatsphäre vorliegen, wenn z.B. eine Person in einem Umkleidebereich der Erfassung mittels Smartglasses nicht ausweichen kann.[892] Umgekehrt wird im öffentlichen Raum die Zwangswirkung geringer sein, wenn die Überwachung nur temporär ist und Personen im Vorbeigehen oder während eines zeitlich beschränkten Aufenthaltes, z.B. in einem Ladenlokal, in den Erfassungsbereich von Smartglasses geraten.[893]

c) Art, Umfang und Sensibilität der erfassten Informationen

Für den Grad der Privatsphärenverletzung ist auch die Art der sie betreffenden Informationen maßgeblich. So wird eine Personenabbildung im Regelfall über eine höhere Eingriffswirkung verfügen als die Aufnahme einer Sache.[894] Ebenso wird bei Smartglasses, die im zwischenmenschlichen Bereich getragen werden, die Sensibilität von Aufnahmen höher sein als bei Videoüberwachungskameras. So können neben der ethnischen Herkunft z.B. Hautverhältnisse oder die Augen aus der Nähe abgebildet werden, wodurch die Erkennung von Krankheitssymptomen und damit sensibler Informationen möglich wird (vgl. § 3 Abs. 9 BDSG).[895] Durch die Beobachtung der Augenbewegungen oder Mikrobewegungen des Gesichts können auch innere Vorgänge der Person ausgewertet werden, wie z.B. die Wahrscheinlichkeit, dass sie lügt.[896] Neben der Erkennbarkeit psychischer Vorgänge wird eine hohe Eingriffsintensität bei der Freile-

---

[890] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 95.

[891] Vgl. BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 95.

[892] BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545 (129); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 96.

[893] Vgl. BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957).

[894] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 63, 240 f.

[895] Vgl. *Karg*, HFR 2012, S. 120 (123); *Opel/Körffer/Nouak*, DuD 2013, S. 347 (348); *Roßnagel/Hornung*, DuD 2005, S. 69 (70).

[896] Vgl. *Davison u.a.*, Micro-Facial Movements: An Investigation on Spatio-Temporal Descriptors, in: *Agapito/Bronstein/Rother*, Micro-Facial Movements, 2014, S. 111 (111 ff.); *Lim u.a.*, Proceedings of the 6th Workshop on Eye Gaze in Intelligent Human Machine Interaction 2013, p. 51 (51 ff.).

gung innerer körperlicher Vorgänge, z.B. mittels einer Thermalansicht, vorliegen.[897] Das gilt erst recht, wenn die Thermalabbildungen sehr detailreich sein sollten und anhand des Wärmebildes des Körpers z.B. der Grad sexueller Erregung einer Person erkannt werden könnte.[898] Hierdurch wird „das bewusst gesetzte optische Hindernis der Kleidung" überwunden, wobei bereits das Vordringen auf den Bereich der Körperoberfläche „von vielen Menschen als höchst intimer Eingriff empfunden wird."[899]

Nicht zuletzt kann sich auch der Umfang der erhobenen Informationen belastend auswirken, wenn z.B. das Missgeschick einer Person nicht nur in einer Fotografie, sondern als ein Video aufgenommen wird und zugleich Ort, Zeitpunkt oder gar der Name der Person mit der Aufnahme gespeichert werden.[900]

d) Kontext der erfassten Informationen

Auch der Kontext der Informationen kann für die Eingriffsintensität maßgeblich werden, da er zum einen überhaupt erst zur Herstellung eines Personenbezuges der durch Smartglasses erfassten Informationen führen und zum anderen die Intensität des Eingriffs erhöhen kann (z.B. wenn eine Person Freizeitaktivitäten nachgeht, während sie krankgeschrieben ist, und dabei in den Erfassungsbereich von Smartglasses gerät).[901]

e) Streubreite und Anlasslosigkeit der Erfassung

Erfassungsmaßnahmen, die über eine hohe Streubreite verfügen und hierdurch besonders viele Personen ohne deren Zutun beeinträchtigen,

---

[897] Vgl. E II. 2. b) aa), S. 113.

[898] *Kukkonen u.a.*, The Journal of Sexual Medicine 2007, Vol. 4, Nr. 1, p. 93; für die Smartglasses Moverio BT-200 wurde z.B. eine Venenerkennung durch Auswertung des Multispektrallichts entwickelt, *Maerian*, Smart glasses let nurses see veins through skin, Computerworld, http://www.computerworld.com/article/2486116/emerging-technology/smart-glasses-let-nurses-see-veins-through-skin.html (24.9.2015).

[899] Vor dem Hintergrund sog. "Nacktscanner" an Flughäfen, *Busche*, DÖV 2011, S. 225 (230).

[900] Vgl. OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087.

[901] Im konkreten Fall wurde das Schutzinteresse des durch einen Kollegen fotografierten Arbeitnehmers verneint, LAG Rheinland-Pfalz, Urt. v. 7.11.2013 (10 SaGa 3/13), ZD 2013, 631.

verfügen über eine besonders hohe Eingriffsintensität.[902] Mit hoher Streubreite und Anlasslosigkeit der Datenerfassung steigen die Gefahr des Missbrauchs der Daten und das Gefühl ständiger Überwachung für Menschen.[903] Als Folge steigt die Zahl der beeinträchtigten Individuen und damit die Gefährdung einer demokratischen Gesellschaft, die auf mündige und selbstbestimmte Individuen als Grundlage des Meinungspluralismus angewiesen ist.[904] Da Smartglasses zu omnipräsenten Begleitern der Menschen werden sollen, ist eine hohe Streubreite und Anlasslosigkeit der Datenerfassungen und damit eine hohe Gefährdung der Interessen von Individuen und damit einer demokratischen Gesellschaftsentwicklung zu befürchten.

f) Grad der hergestellten Öffentlichkeit

Für die Beurteilung der Eingriffsintensität von Smartglasses ist es ferner erheblich, in welchem Maß die durch Smartglasses erhobenen Daten der Öffentlichkeit zugänglich gemacht werden. Denn mit zunehmender Öffentlichkeit steigt die Gefahr, dass die erfassten Informationen zum Nachteil der Betroffenen verarbeitet werden können und diese daher bereits durch die Furcht vor negativen Konsequenzen in ihrer Autonomie beeinträchtigt werden.

Dabei liegt die geringste Eingriffsintensität vor, wenn die Erfassung nur für eigene Zwecke der Nutzer der Smartglasses, z.B. im Fall von Augmented-Reality-Funktionen, erfolgt. Die Intensität steigert sich mit der Zahl der Personen, die Zugang zu den Smartglasses erhalten. Die größte Öffentlichkeit ist hergestellt, wenn jedermann die Möglichkeit des Zu-

---

[902] BVerfG, Urt. v. 2.3.2010 (1 BvR 256/08, 1 BvR 263/08 u. 1 BvR 586/08), BVerfGE 125, 260 (318); BVerfG, Urt. v. 11.3.2008 (1 BvR 2074/05, 1 BvR 1254/07), BVerfGE 120, 378 (402); BVerfG, Beschl. v. 4.4.2006 (1 BvR 518/02), BVerfGE 115, 320 (354); BVerfG, Urt. v. 12.3.2003 (1 BvR 330/96 u. 1 BvR 348/99), BVerfGE 107, 299 (320 f.); BVerfG, Urt. v. 14.7.1999 (1 BvR 2226/94, 2420/95 u. 2437/95), BVerfGE 100, 313 (376, 392); LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (Rn. 17); AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (238); *Balzer/Nugel*, NJW 2014, S. 1622 (1624); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 90; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 31; *Weichert*, ZD 2012, S. 501 (503).

[903] BVerfG, Urt. v. 12.3.2003 (1 BvR 330/96 u. 1 BvR 348/99), BVerfGE 107, 299 (328).

[904] Vgl. D II. 2, S. 81.; vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 90.

gangs eröffnet wird, z.B. indem Inhalte im Internet ohne Zugangsschranken publiziert werden.[905]

g) Heimlichkeit der Erfassung

Die Beeinträchtigung der Autonomie durch Smartglasses steigt mit dem Grad der Heimlichkeit von Erfassungsvorgängen, die den Betroffenen die Möglichkeit passiver und aktiver Abwehrmaßnahmen nimmt und zugleich ein Gefühl permanenter Überwachung erzeugen kann.[906]

Das Bundesverfassungsgericht sah daher bereits durch die Verbreitung von Mobiltelefonen mit integrierten Kameras ein besonderes Risiko für die Betroffenen, „in praktisch jeder Situation unvorhergesehen und unbemerkt mit der Folge fotografiert zu werden, dass das Bildnis in Medien veröffentlicht wird."[907] Dabei betonte das Gericht die besondere Eingriffsintensität und damit eine höhere Schutzbedürftigkeit, die sich aus einem „heimlichen oder überrumpelnden Vorgehen" ergibt.[908] Die im Hinblick auf Mobiltelefone und übrige Kameratechnik getroffene Aussage trifft erst recht und in einem höheren Umfang auf Smartglasses zu.

aa) Transparenz der Erfassung als Mittel des Rechtsschutzes

Bei gegenwärtig verwendeten optischen Erfassungsgeräten wie Fotokameras oder Smartphones ist ein gewisser Schutz für die Betroffenen bereits in dem Aufnahmevorgang implementiert. Dieser Schutz äußert sich darin, dass die Geräte auf das Motiv gerichtet werden müssen, sodass der Erfassungsvorgang mit einer „Fotografiergeste" verbunden ist, die den Erfassungsvorgang für Dritte erkennbar macht.[909]

---

[905] Vgl zur Gefahren der Publikation im Internet LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002 (1003); VGH München, Beschl. v. 16.10.2014 (10 ZB 13.2620), NVwZ-RR 2015, 104 (105); *Golla/Herbort*, GRUR 2015, S. 648 (648) ff.; *Leffler*, Cyber-Bullying, 2012, S. 111 f.; *Payandeh*, NVwZ 2013, S. 1458 (1460); *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 4.

[906] Vgl. EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051 (1054 f.); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (384); *Gola/Schomerus*, BDSG, § 6b, Rn. 26 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 98; *Solmecke/Nowak*, MMR 2014, S. 431 (434).

[907] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (198).

[908] Ebenda.

[909] *Fuchs*, ZD 2015, S. 212 (216); *Schwenke*, K&R 2013, S. 685 (686).

Die Fotografiergeste erlaubt es den Betroffenen zudem, sich gegen die Erfassung sowohl passiv als auch aktiv zu wehren.[910] So ist z.B. häufig zu beobachten, wie sich Personen aus dem Aufnahmebereich einer Fotokamera wegducken oder wegbewegen. Neben dieser passiven Abwehr könnten Betroffene auch aktiv werden und z.B. einen Aufnahmevorgang unterbrechen oder sich gegen die Möglichkeit des Missbrauchs der Aufnahmen durch Verlangen der Auskunft und Löschung etwaiger Aufnahmen absichern.

bb) Intransparenz der Erfassung durch Smartglasses

Dadurch, dass Smartglasses auf dem Kopf getragen werden, folgen sie den Kopfbewegungen ihrer Nutzer und müssen nicht gesondert auf die Aufnahmeobjekte gerichtet werden. Zudem können die Aufnahmen unbemerkt per Sprachbefehle, Augenbewegungen oder sogar automatisch ausgelöst werden.[911] Dadurch ist es für Betroffene in dem Erfassungsbereich von Smartglasses kaum erkennbar, ob und in welchem Umfang sie aufgenommen werden.

Zwar kann die Fixierung des Blickes auf eine Person ein Hinweis auf die Aufnahme sein. Jedoch kann nicht von einer hinreichend erkennbaren Aufnahmegeste ausgegangen werden, wenn der Unterschied zwischen einer bloßen Beobachtung mit den Augen und einer Aufnahme in einem bloßen Zwinkern des Auges besteht.[912]

Die Erkennbarkeit der Aufnahme muss sich daher aus anderen Umständen ergeben. Im optimalen Fall kann die betroffene Person auf den Erfassungsvorgang ausdrücklich hingewiesen werden. Fehlt ein solcher Hinweis, kann z.B. ein Signallicht die Erfassung ähnlich einer „Achtung Aufnahme“-Lampe auf Videokameras kenntlich machen.[913] Ebenso könnten andere visuelle Signale, wie z.B. ein „On Air“-Aufsatz, auf eine Aufnahme

---

[910] "[…] after all, there are certain social norms that go with pulling out a camera, even a camera phone, and then framing a shot and snapping a picture. It's a clear, albeit sometimes nonverbal, process in which the subject of the photo is offered the opportunity to opt out of the photo.", *Fankhauser*, Tiny Camera Logs Your Life As Long as the Lighting Is Good, Mashable, http://mashable.com/2014/02/26/narrative-clip/(2.10.2015).

[911] Vgl. B II. 2. a), S. 30.

[912] Vgl. B II. 2. a), S. 30.

[913] Z.B. verfügt die Datenbrille über eine kleine Leuchtdiode, die angeht, wenn die Kamerafunktion aktiviert wird, "Moverio", Moverio BT-200: Das kann Epsons Computerbrille - SPIEGEL ONLINE, http://www.spiegel.de/netzwelt/gadgets/moverio-bt-200-das-kann-epsons-computerbrille-a-942149.html(8.1.2014);Moverio BT-200 Smart Glasses, Epson, http://www.epson.com/cgi-bin/Store/jsp/Product.do?sku=V11H560020 (6.9.2015).

hinweisen oder umgekehrt mechanische Kappen über der Kamera demonstrieren, dass keine Aufnahme stattfindet.[914]

Im Fall der Datenbrille „Glass“ ist zwar lt. Google das Aufleuchten des Bildschirms als ein Indiz für die Aufnahme zu verstehen, jedoch ist der Bildschirm zum einen sehr klein und leuchtet zum anderen auch in Situationen auf, in denen die Kamera nicht eingesetzt wird.[915] D.h., eine eindeutige Erkennung des Aufnahmevorgangs ist nicht möglich. Ferner müssten die Betroffenen sich mit den Eigenschaften der einzelnen Geräte auskennen, um derartige Signale deuten zu können. Zudem können Signalmöglichkeiten wie z.B. die kleine Leuchtdiode der Datenbrille Moverio BT-200 zugeklebt oder überstrichen werden.[916] Auch ein starkes Tageslicht oder die räumliche Distanz zwischen Betroffenen und den Smartglasses kann die Erkennbarkeit der schwachen visuellen Signale beeinträchtigen.

Wer in das Erfassungsfeld von Smartglasses gerät, wird folglich die Wahl haben, zu vertrauen, dass eine Erfassung nicht erfolgt, sich mit der Erfassung abzufinden oder das Risiko von Abwehrmaßnahmen aufgrund einer unbekannten Tatsachenlage einzugehen. Als möglich erscheint vor allem, dass Betroffene sich der Erfassung eher fügen, als dass sie die Gefahr eingehen, sich der Belustigung anderer auszusetzen, wenn sie permanent versuchen, aus dem Erfassungsbereich von Smartglasses zu flüchten. Sollten Smartglasses irgendwann überhaupt nicht mehr als solche zu erkennen sein, entfällt die Möglichkeit, aus dem Erfassungsbereich zu flüchten, gänzlich. Die gegenwärtigen Smartglasses sind noch anhand der Wülste, in denen sich die Bildprojektoren oder die Recheneinheiten befinden, als Smartglasses zu erkennen oder erwecken zumindest den Eindruck, keine gewöhnliche Brille zu sein. Ferner werden Smartglasses auch zunehmend zum Gegenstand medialer Berichterstattung, sodass immer mehr Menschen Smartglasses als solche erkennen können. Für die Zukunft ist jedoch damit zu rechnen, dass Smartglasses sich optisch immer

[914] Auf der Crowdfundingplattform "Kickstarter" wurden z.B. Plastikkappen für die die Datenbrille Google Glass mit Aufschriften, wie z.B. "On Air", vorgestellt, GlassKap, Kickstarter, http://www.kickstarter.com/projects/baltimore/glasskap-a-lens-cover-and-fun-accessories-for-goog (26.7.2013).

[915] Vgl. B II. 2. a), S. 30.

[916] Vgl. B II. 2. b), S. 32.

weiter gewöhnlichen Brillen nähern und so immer weniger als Smartglasses erkannt werden können.[917]

cc) Fortschritt der Miniaturisierung

Die mit Googles Datenbrille „Glass“ im Alltag gesammelten Erfahrungen zeigen, dass Dritte sich von der Präsenz des Gerätes bedroht fühlten, weil sie „Glass“ als eine auf sie gerichtete Kamera wahrnahmen.[918] Dagegen scheinen sich Menschen an der Präsenz nicht sichtbarer Videoüberwachungskameras, die sich z.B. in Wölbungen (sog. „Domes“) unter der Decke eines Raumes befinden, weniger zu stören.[919] Dies erlaubt den Rückschluss, dass weniger als Smartglasses erkennbare Geräte das Risiko negativen Reaktionen seitens Dritter senken würden. Dies wäre im Sinne der Nutzer von Smartglasses, die mehrheitlich ihre Geräte nutzen möchten, ohne dabei als potenzielle Aggressoren betrachtet zu werden.[920]

Der Logik einer an den Bedürfnissen des Marktes orientierten technischen Entwicklung folgend, ist daher damit zu rechnen, dass Hersteller von Smartglasses ihre Geräte entsprechend dem Kundenwunsch möglichst unauffällig gestalten.[921] Folglich ist eine Entwicklung zu erwarten, an deren Ende Smartglasses den heute als „Spionagebrillen“ bekannten Brillen mit nicht sichtbar eingebauten Kameras gleichen werden.[922]

Werden Smartglasses aufgrund ihrer Bauweise nicht mehr erkannt, fragt es sich jedoch umgekehrt, ob hierdurch überhaupt eine belastende Einschüchterungswirkung entstehen kann. Für die rechtliche Erheblichkeit einer Zwangswirkung ist es notwendig, dass objektive Faktoren vorliegen, die auf eine mögliche Überwachung schließen lassen, sodass bloße subjektive Befindlichkeiten nicht ausreichend sind.[923] Allerdings kann eine Überwachungswirkung trotz fehlender Erkennbarkeit aufgrund der Verbreitung von Smartglasses entstehen. Es ist nicht ausgeschlossen, dass der Grad der Furcht vor panoptischer Erfassung sich steigern würde,

---

[917] Google meldete im August 2014 ein Patent an (US Patent D710,928 S, eingetragen am 12.08.2014), das einer "Glass"-Brille ähnelt, die optisch kaum erkennbar in ein reguläres Brillengestell eingelassen ist, *Kooser*, Patent pictures hint at unobtrusive Google Glass design, CNET, http://www.cnet.com/news/patent-pictures-hint-at-unobtrusive-google-glass-design/(22.8.2014).

[918] Vgl. C II. 3, S. 68.

[919] Zum Begriff, AG Dinslaken, Urt. v. 5.3.2015 (34 C 47/14), ZD 2015, 531 (532); zu unterschiedlichen Reaktionen auf Smartglasses, *Mann/Niedzviecki*, Cyborg, 2002, S. 157.

[920] Vgl. C II. 3, S. 68.

[921] Vgl. zur Beeinflussung der Technikentwicklung durch Verbraucher, *Agar*, Constant Touch, 2004, S. 171 ff.; *Ellul*, The Technological Society, 1967, S. 112.

[922] Zum Begriff der "Spionage"-Geräte S. BT-DrS. 10/1618, S. 9.

[923] Vgl. E II. 2. b) gg) (3), S. 128.

wenn Smartglasses an jedem Ort und zu jeder Zeit unerkannt präsent sein könnten.[924] Ferner ist davon auszugehen, dass, wenn Smartglasses zu einem unsichtbaren Massenprodukt werden, sich ihr Einsatz kaum mehr kontrollieren lässt.[925]

dd) Senkung der Hemmschwelle

Die fehlende Erkennbarkeit der Erfassungsvorgänge als auch der Smartglasses als solche kann zudem die Hemmschwelle senken, die ein Mensch überwinden muss, bevor er die Persönlichkeitsrechte einer anderen Person durch eine Aufnahme beeinträchtigt.[926]

Wenn der Erfassungsvorgang aufgrund der „Fotografiergeste" durch die betroffene Person oder Dritte wahrgenommen werden kann, müssen mögliche negative Reaktionen der fotografierten Personen befürchtet werden. Hierzu können die Kundgebung des Missfallens (was im Beisein anderer Personen für den Aufnehmenden beschämend wirken kann), in extremeren Fällen tätliche Abwehr oder Hausverbote gehören.[927] Diese negativen Folgen stellen eine Hürde für die Aufnahme dar, da sie mit den sich aus der Aufnahme ergebenden Vorteilen abgewogen werden müssen. Eine solche Hemmschwelle sinkt erheblich, wenn die Aufnahme heimlich erfolgt und mit negativen Konsequenzen nicht gerechnet werden muss.[928]

Ferner kann die Hemmschwelle kaum in den Überlegungsprozess einfließen, wenn der Wunsch der Aufnahme mit dessen Durchführung praktisch zusammenfällt. Die technische Eigenart heutiger Aufnahmegeräte bietet ihren Nutzern eine gewisse Überlegungszeit zwischen dem Aufnahmewunsch und dem Auslösen der Aufnahme. Kameras oder Smartphones werden oft verstaut getragen und es erfordert einen gewissen Zeitaufwand und Mühe, sie hervorzuholen und auf das Motiv zu richten. D.h., bevor der Aufnahmevorgang durchgeführt wird, können die Vorteile der Aufnahme mit den persönlichen Mühen der Nutzer und möglichen negativen Reaktionen Dritter abgewogen werden. Diese Dauer kann zwar nur wenige Augenblick betragen, wird jedoch in der Relation viel länger sein als der Auslösevorgang von bereits auf das Motiv gerichteten Smartglasses. Das bedeutet, dass damit zu rechnen ist, dass Nutzer von Smartglasses häufiger unbedacht und impulsiv Aufnahmen erstellen werden.

---

924 Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 98.

925 *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 102.

926 Vgl. *Schwenke*, K&R 2013, S. 685 (686).

927 Vgl. C II. 3, S. 68.

928 *Beuth*, Google Glass, Die Zeit, http://www.zeit.de/digital/datenschutz/2013-03/stop-the-cyborgs-google-glass (7.9.2015).

h) Speicherort, Speicherdauer, Übermittlung und Zugriffsmöglichkeiten Dritter auf Daten

Die durch Smartglasses erfassten Informationen können auf dem Gerät selbst gespeichert werden, was eine geringere Beeinträchtigung mit sich bringt als die Speicherung der Daten auf Cloud-Servern. Der Nachteil von Cloud-Servern besteht darin, dass die Daten aus dem Verfügungsbereich der Nutzer gelangen und so dem Zugriff durch die Cloud-Anbieter oder sonstiger Dritter, insbesondere während der Datentransaktion zwischen dem Nutzer und dem Cloud-Anbieter, unterliegen.[929] Ferner hat der Ort der Speicherung des Cloud-Dienstes als auch der Sitz seines Anbieters eine Relevanz. So ist insbesondere die Auslagerung von Daten auf Cloud-Server außerhalb der Europäischen Union im Hinblick auf das Datenschutzniveau vor Ort umstritten.[930] Aber auch wenn sich die Daten physisch in einem Land mit sicherem Datenschutzniveau befinden, können rechtliche Pflichten am Sitz des Anbieters im Ausland eine Gefährdung für die Daten mit sich bringen, da räumliche und staatliche Grenzen häufig kaum Einfluss auf den Schutz von Daten zu haben scheinen.[931]

Aber auch die Speicherung von Daten auf dem eigenen Gerät kann zu einer Beeinträchtigung führen, wenn Dritte sich Zugang zu den Daten verschaffen können. Dies kann zum einen mit Einwilligung der Nutzer von Smartglasses geschehen. Ein befugter Zugang läge z.B. vor, wenn der Nutzer dem Anbieter einer biometrischen Applikation erlauben würde, auf die erfassten Informationen zuzugreifen. In diesen Fällen ist die Gefahr für personenbezogene Daten Dritter mit einer Speicherung dieser Daten in der Cloud zu vergleichen.

Ebenfalls als Maßstab für die Bemessung der Eingriffsintensität ist die Wahrscheinlichkeit eines unerlaubten Fremdzugriffs auf Smartglasses zu berücksichtigen.[932] Im Fall eines unbefugten Zugriffs besteht die besondere Gefahr, dass die unbefugte Person einen permanenten Zugriff auf das

---

[929] *Geis*, ZD 2013, S. 591 (592 f.); *Schulz*, MMR 2010, S. 75 (77 f.).

[930] EuGH, Urt. v. 6.10.2015 (C-362/14), MMR 2015, 753 (754 ff.); *Geis*, ZD 2013, S. 591 (592).

[931] Z.B. sollen US-Anbieter auch Daten, die auf deren Servern in Europa belegen sind, entsprechend der Sec. 215 des US-Patriot Act an US-Justizbehörden herausgeben, vgl. *Becker/Nikolaeva*, CR 2012, S. 170 (170 f.).

[932] Zu Schwierigkeiten des Schutzes von Informationstechnischen Systemen, zu denen auch Smartglasses gehören, vgl. BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274 (306); vgl. *Arthur*, Google Glass security failings may threaten owner's privacy, The Guardian, http://www.guardian.co.uk/technology/2013/may/01/google-glass-security-privacy-risk (9.7.2013); *Freeman*, Exploiting a Bug in Google's Glass, http://www.saurik.com/id/16 (1.12.2015); zu ähnlichen Befürchtungen vor dem Hintergrund der Nutzung von Drohnen, S. *Weichert*, ZD 2012, S. 501 (502).

Blickfeld des Trägers von Smartglasses erhalten kann.[933] Dadurch kann sie z.B. Aufnahmevorgänge ausführen, ohne dass der Träger von Smartglasses dies selbst mitbekommt. Diese Art von Missbrauch ist mit den Fällen vergleichbar, in denen Webcams „gekapert" wurden, bloß mit dem Unterschied, dass eine Webcam in den meisten Fällen stationär ist und der unberechtigte Zugriff nicht zugleich Dritte betrifft, sondern meistens nur die Inhaber der Webcam.[934]

Des Weiteren kann die Beeinträchtigung Dritter eine unterschiedlich starke Intensität erreichen, je nachdem, wie lange die mit Smartglasses erhobenen Daten gesichert werden. Z.B. können Aufnahmen als Schnappschüsse dauerhaft oder nur flüchtig und damit weniger beeinträchtigend für die Zwecke von Augmented Reality gespeichert werden.[935]

i) Möglichkeiten der Rechtsdurchsetzung für Betroffene

Wenn Smartglasses von einer Vielzahl von Menschen getragen werden sollten, wird die Rechtsdurchsetzung im Fall von Rechtsverstößen erheblich erschwert.[936] So konnten sich Betroffene z.B. im Fall von Googles umstrittenem „Street View"-Projekt direkt an das Unternehmen als unmittelbar verantwortliche Stelle richten.[937] Im Fall von Smartglasses sind dagegen zuerst die einzelnen Träger von Smartglasses verantwortlich. Diese müssten zunächst ausfindig gemacht werden, was bei den vielfältigen Möglichkeiten, z.B. kompromittierende Aufnahmen anonym herzustellen und ebenso zu verbreiten oder zu veröffentlichen, erheblich erschwert wird.[938]

Ferner könnte es nicht ausreichen, gegen den Nutzer von Smartglasses vorzugehen, wenn z.B. Aufnahmen einer Vielzahl von Menschen zugänglich gemacht wurden oder auf Plattformen und Servern weltweit verbreitet sind, deren Anbieter grundsätzlich nur mittelbar ab Kenntnis der

---

933 *Arthur*, Google Glass security failings may threaten owner's privacy, The Guardian, http://www.guardian.co.uk/technology/2013/may/01/google-glass-security-privacy-risk (9.7.2013); *Perlow*, Google Glass, ZDNet, http://www.zdnet.com/article/google-glass-let-the-evil-commence/(2.7.2013).

934 Vgl. *Meusers*, Hacker können Macbook-Webcams unbemerkt einschalten, Spiegel Online, http://www.spiegel.de/netzwelt/web/hacker-koennen-macbook-webcams-unbemerkt-einschalten-a-939998.html (23.1.2015).

935 Vgl. E II. 2. b) dd), S. 115.

936 Vgl. zu Datenschutzproblemen durch die Steigerung der Beteiligtenzahl, *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 7.

937 *Moos/Zeiter*, ZD 2013, S. 178.

938 Vgl. *Krohm/Müller-Peltzer*, ZD 2015, S. 409.

Rechtsverletzungen haften.[939] Dabei muss insbesondere bedacht werden, dass, auch wenn die Persönlichkeitsverletzungen durch Smartglasses in ihrer Summe als gesellschaftsschädlich eingestuft werden, die einzelnen Betroffenen selbst nur einen im Vergleich geringen Schaden erfahren könnten.[940] Angesichts des geringen Schadens kann eine prozessuale Durchsetzung der Ansprüche auch im Inland für Betroffene als im Vergleich zu den Prozessrisiken nicht lohnenswert erscheinen und sie von der Verfolgung ihrer Interessen abhalten.

j) Anonymisierungsverfahren

Sofern die Gefahr einer Verletzung des Rechts auf informationelle Selbstbestimmung aufgrund zugelassener oder unfreiwilliger Zugriffe auf die durch Smartglasses erfassten Daten droht, kann diese Gefahr durch die Verschlüsselung der Daten sowie ihrer Übermittlung gemindert werden.[941] Ferner könnten die erhobenen Informationen bereits vor dem Speichern anonymisiert werden, z.B. wenn Personen auf den Aufnahmen automatisch unkenntlich gemacht werden.[942] Eine solche Anonymisierungssoftware wird z.B. von dem Unternehmen Google für die Unkenntlichmachung von Personen auf Aufnahmen des Straßenpanoramadienstes „Street View“ oder innerhalb der Videoplattform „YouTube“ eingesetzt.[943]

---

[939] LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002 (1003); VGH München, Beschl. v. 16.10.2014 (10 ZB 13.2620), NVwZ-RR 2015, 104 (105); *Golla/Herbort*, GRUR 2015, S. 648 (650); *Leffler*, Cyber-Bullying, 2012, S. 111 f.; *Payandeh*, NVwZ 2013, S. 1458 (1460); *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 4; Hostprovidern steht z.B. in Europa ein Haftungsprivileg für nutzergenerierte, d.h. ihnen fremde Inhalte, zu, S. Art 14 der Richtlinie 2000/31/EG.

[940] Schrems meint, dass es "regelmäßig ein wirtschaftlicher Wahnsinn" ist, wenn sich Unternehmen angesichts der geringen Folgen von Datenschutzverstößen an Gesetze halten, *Schrems*, Kämpf um deine Daten, 2014, S. 216.

[941] Überwiegend wird in der Verschlüsselung von personenbezogenen Daten noch keine Anonymisierung gesehen, da eine Entschlüsselung in der Zukunft nicht ausgeschlossen werden kann, Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 01248/07/DE, 2007, S. 21 ff.; Düsseldorfer Kreis, Orientierungshilfe – Cloud Computing, Version 2.0, 2014, https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf (5.9.2015), S. 12 f.; m.w.N. *Spies*, Cloud Computing: Keine personenbezogenen Daten bei Verschlüsselung, MMR-Aktuell, 2011, Nr. 313727; *Heidrich/Wegener*, MMR 2015, S. 487 (492); *Pordesch/Steidle*, 2015, S. 536 (537 ff.).

[942] Vgl. Information and Privacy Commissioner of Ontario, Anonymous Video Analytics (AVA) technology and privacy, 2011, https://www.ipc.on.ca/images/Resources/AVAwhite6.pdf (2.9.2015), p. 4; *Ernst*, CR 2010, S. 178 (179); *Jahn/Striezel*, K&R 2009, S. 753 (758); *Moos/Zeiter*, ZD 2013, S. 178 (179); Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 01248/07/DE, 2007, S. 25.

[943] *Beuth*, Anonymität, Die Zeit, http://www.zeit.de/digital/internet/2012-07/youtube-gesichter-anonym (11.9.2015).

Im Fall von Google Street View wurde die Verwischung der Gesichter von Personen jedoch nicht als ausreichend für eine Anonymisierung erachtet.[944] Ebenso reicht es nicht aus, wenn lediglich die Gesichter auf den Aufnahmen einer Überwachungskamera verpixelt werden, wenn die Möglichkeit besteht, dass die Personen auf den Aufnahmen aufgrund ihrer Figur, Frisur und Kleidung von Freunden, Verwandten oder Nachbarn erkannt werden könnten.[945] Insbesondere die „smarten" Überwachungstechnologien können bestimmte Verhaltensmuster von Personen erkennen und diese so identifizieren.[946]

Des Weiteren muss auch beachtet werden, auf welcher Stufe des Datenumgangs die Verpixelung erfolgt. So ist eine Verpixelung, die nicht bereits bei der Erfassung, sondern z.B. im Fall der Übermittlung erfolgt, erst auf dieser Verarbeitungsstufe im Rahmen der Interessenabwägung zu berücksichtigen.[947]

k) Summierungseffekte

Im Rahmen der rechtlichen Beurteilung der Eingriffsintensität von Smartglasses dürfen diese nicht alleine für sich betrachtet werden. Sowohl bei der Frage der Möglichkeiten künftiger Verarbeitung von Daten als auch der verhaltensbeeinträchtigenden Überwachungsaspekte muss berücksichtigt werden, dass Smartglasses lediglich ein Teil eines umfassenden Geflechts von Überwachungs- und Datenverarbeitungstechnologien sind, das immer mehr zum Teil des Alltags von Menschen wird.[948]

Zu prüfen ist daher, in welchem Umfang sich Smartglasses im Zusammenwirken mit anderen Technologien auf die Privatsphäre auswirken können und inwieweit diese Gefährdungen der Smartglasses-Technologie zuzurechnen sind. D.h., es ist zu untersuchen, inwieweit die modernen Informationstechnologien die Persönlichkeitsentfaltung einzelner sowie

---

[944] *Caspar*, Gutachten zu Rechtsfragen betreffend den Internet-Dienst Google Street View, Schleswig-Holsteinischer Landtag Kiel/Wissenschaftlicher Dienst, 2009, S. 15 ff.; auf den Umstand der Erkennbarkeit vor dem Hintergrund des Rechts am eigenen Bild eingehend, *Ernst*, CR 2010, S. 178 (179); *Jahn/Striezel*, K&R 2009, S. 753 (758); zusammenfassend, *Moos/Zeiter*, ZD 2013, S. 178 (179); Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 25.

[945] Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 25; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 166.

[946] *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (239 f.); *Spiecker genannt Döhmann*, K&R 2014, S. 549 (551).

[947] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 166.

[948] *Allmer*, Critical Internet Surveillance Studies, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 124 (127); *Ketzer*, Securitas ex Machina, 2005, S. 4 ff.; *Mathiesen*, Preface, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. xv (xviii).

die Pluralität der Gesellschaft beeinträchtigen können. Daneben sind auch die von Smartglasses selbst ausgehenden Summierungseffekte zu berücksichtigen, wenn die Geräte Eingang in den Alltag finden und sich deren Zahl vervielfacht.

aa) Rechtliche Anerkennung von Summierungseffekten

Generell werden im Rahmen einer Interessenabwägung einzelne Maßnahmen für sich betrachtet. Jedoch kann sich erst aus der Zusammenwirkung mehrerer Maßnahmen, die für sich kaum belastend sind, kumulativ und additiv wirkend eine relevante Gesamtbelastung ergeben.[949] So erkannte das Bundesverfassungsgericht den Summierungseffekte unterschiedlicher Technologien bereits im Rahmen des Volkszählungsurteils und verwies darauf, dass personenbezogene Daten „vor allem beim Aufbau integrierter Informationssysteme […] mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden“ können.[950] Auch mit der Ausgestaltung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betonte das Bundesverfassungsgericht im Jahr 2008, dass die über einzelne Daten hinausgehenden Gefahren der Datensummierung insbesondere für die gegenwärtigen Technologien gelten.[951] Ebenso wurden Summierungseffekte bei der Addition von Ermittlungseffekten und bei Datensammlungen berücksichtigt.[952]

Die Relevanz von Summierungseffekten zeigt sich insbesondere in der Diskussion um den Einfluss des technischen Fortschritts auf das Kriterium der Bestimmbarkeit im Rahmen der Prüfung, ob ein Datum personenbezogen ist.[953] Dabei geht es im Wesentlichen um die Frage, ob und wie weit auch die Erkenntnisse Dritter und noch nicht konkretisierte Möglichkeiten der Datenverarbeitung einzubeziehen sind.[954] Nach der Ansicht der Vertreter eines absoluten bzw. objektiven Personenbezuges ist die rasant fortschreitende technologische Entwicklung zu berücksichtigen, die faktisch die Anzahl derjenigen Stellen schrumpfen lässt, die

---

[949] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 93; den Begriff "Überwachungsgesamtrechnung" im Hinblick auf die Maßnahmen der Vorratsdatenspeicherung verwendend, *Roßnagel*, NJW 2010, S. 1238 (1242).

[950] BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42).

[951] BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274 (302 ff.).

[952] Vorratsdatenspeicherung, BVerfG, Urt. v. 2.3.2010 (1 BvR 256/08, 1 BvR 263/08 u. 1 BvR 586/08), BVerfGE 125, 260 (324); Ermittlungsmaßnahmen, BVerfG, Urt. v. 12.4.2005 (2 BvR 581/01), BVerfGE 112, 304 (304 ff.); S. auch im Steuer- und Abgabenrecht, BVerfG, Beschl. v. 29.5.1990 (1 BvL 20, 26/84 u. 4/86), BVerfGE 82, 60 (84).

[953] Vgl. E II. 2. a) aa) (1), S. 98.

[954] *Heidrich/Wegener*, MMR 2015, S. 487 (488); *Brink/Eckhard*, ZD 2015, S. 205 (205 ff.).

tatsächlich nicht in der Lage sind, einen Bezug zwischen gespeicherten Angaben und bestimmten Personen herzustellen.[955] Die Vertreter des derzeit herrschenden relativen Personenbezuges konzentrieren sich dagegen auf den Vorgang der Datenverwendung und stellen für die Bestimmbarkeit der Person nur auf die Möglichkeiten und Fähigkeiten der speichernden und verarbeitenden Stelle ab.[956] D.h., auch wenn der Grad ihrer Relevanz umstritten ist, sind Summierungseffekte sowohl von der Rechtsprechung als auch von der Literatur grundsätzlich anerkannt.

bb) Doppelte Verhältnismäßigkeitsprüfung

Bei einer in Frage kommenden kumulativen Gesamtbelastung des Allgemeinen Persönlichkeitsrechts durch unterschiedliche Maßnahmen, sollte eine doppelte Verhältnismäßigkeitsprüfung vorgenommen werden. Hierbei werden auf der ersten Stufe einzelne grundrechtsbeeinträchtigende Maßnahmen für sich alleine gewürdigt und auf der zweiten Stufe wird deren Zusammenwirken in einem Kontext betrachtet.[957]

Problematisch ist jedoch die Bestimmung, welche Maßnahmen und Wirkungen zusammen zu addieren sind, d.h., wann die Voraussetzungen einer Summierung erfüllt sind und wann es sich bloß um ein Nebeneinander einzelner Maßnahmen handelt. Als Kriterien werden die Gleichzeitigkeit der Maßnahmen genannt sowie die Auswirkung auf den gleichen Adressaten und mit Blick auf die Belastung auf vergleichbare Gegenstände.[958] Ein Indiz ist ferner eine einheitliche Rechtsfolge der Maßnahmen.[959] Dagegen wird der Zweck der Maßnahmen als weniger relevant betrachtet, da es für die Betroffenen nicht relevant ist, aus welchen Gründen sie eine Belastung erfahren.[960] Diese Beurteilung ist vor dem Hintergrund der Normwirklichkeit durchzuführen. Das bedeutet, es ist nicht auf

---

[955] BGH, Beschl. v. 28.10.2014 (VI ZR 135/13), BeckRS 2014, 20158 (Rn. 28); *Bergt*, ZD 2015, S. 365 (368 ff.); *Karg*, MMR 2011, S. 341 (346); *Weichert*, DuD 2007, S. 17 (19).

[956] BGH, Urt. v. 12.5.2010 (I ZR 121/08), MMR 2010, 565 (567); OLG Hamburg, Beschl. v. 3.11.2010 (5 W 126/10), MMR 2011, 281; den Personebezug annehmend, aber ohne tiefere Begründung von den Verarbeitungsmöglichkeiten der jeweiligen Stelle ausgehend, BGH, Urt. v. 13.1.2011 (III ZR 146/10), MMR 2011, 341 (346); Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 01248/07/DE, 2007, S. 15; zwischen absoluten und relativen Ansichten vermittelnd, *Brink/Eckhard*, ZD 2015, S. 205 (210 ff.); *Buchner*, in: *Taeger/Gabel*, BDSG, § 3 BDSG Rn. 12; *Dammann*, in: *Simitis*, BDSG, § 3 Rn. 32; *Gola/Schomerus*, BDSG, § 3, Rn. 10; *Forgó/Krügel*, MMR 2010, S. 17 (19); *Krüger/Maucher*, MMR 2011, S. 433 (436); *Mayer-dierks*, MMR 2009, S. 8 (12); *Spiecker genannt Döhmann*, CR 2010, S. 311 (313).

[957] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 94.

[958] *Kirchhof*, NJW 2006, S. 732 (734).

[959] Ebenda.

[960] Ebenda; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 95.

die normativen Schutzbereiche der Grundrechte zu schauen, sondern auf deren praktische Auswirkungen.[961] So werden unterschiedliche Maßnahmen, die jedoch alle die Privatsphäre als Schutzgut beeinträchtigen, einer Normwirklichkeit zuzurechnen sein, und damit einen additionsfähigen Wirkungszusammenhang aufweisen. [962]

Neben der generellen Möglichkeit der Summierung stellt sich die Frage, ob diese auch im Rahmen der Prüfung von mittelbar zwischen Privaten wirkenden Grundrechte zu berücksichtigen ist. Da die Privatsphäre jedoch sowohl subjektive als auch gesellschaftliche Interessen schützt, erscheint es sachgerecht, die Gesamtbelastung der Privatsphäre auch im Rahmen der Rechtsbeziehungen zwischen Privatpersonen zu berücksichtigen.[963] Zudem müssen aus diesem Grund Überwachungsmaßnahmen Privater zusammen mit der Belastungswirkung staatlicher Maßnahmen betrachtet werden.[964]

cc) Zur Gesamtbelastung beitragende Überwachungsmaßnahmen

Nachfolgend werden Technologien und Verfahren vorgestellt, die kumulativ mit den Belastungen durch Smartglasses zur Belastung der Privatsphäre beitragen könnten. Zu beachten ist jedoch, dass es sich um keine empirische und erschöpfende Darstellung, sondern vielmehr um eine abstrakte Übersicht handelt. Um die Summierungswirkung tatsächlich bestimmen zu können, ist der Rückgriff auf interdisziplinäre Erhebungen und Studien erforderlich, um die von der Addition der Maßnahmen ausgehenden Einschüchterungseffekte sowie die Beeinträchtigung der Unbefangenheit von Menschen zu beurteilen.[965] D.h., die Summierungseffekte können allenfalls als Indizien aufgefasst werden und müssen anhand ihrer potenziellen Folgen im jeweiligen Einzelfall beurteilt werden.

(1) Summierungswirkung durch die Verbreitung von Smartglasses

Das Konzept einer „Ubiquitous Augmented Reality“ verfolgt das Ziel einer möglichst umfassenden virtuellen Abbildung der physischen Realität, weshalb damit zu rechnen ist, dass mit der Verbreitung von Smartglasses auch die Menge der durch sie erfassten Informationen aus dem

---

961 *Kirchhof*, NJW 2006, S. 732 (734 f.).

962 Vgl. Ebenda, 735; Lücke stellt auf die Betroffenheit desselben Grundrechtsguts ab, was hier durch die Betroffenheit des Allgemeinen Persönlichkeitsrechts zu bejahen wäre, *Lücke*, DVBl 2001, S. 1469 (1470).

963 Vgl. D II. 2, S. 81; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 96.

964 Ebenda.

965 Ebenda, 94 f.

öffentlichen Raum radikal zunehmen wird.[966] Ferner könnte ein gegenseitiges „Aufrüsten" mit Smartglasses ausgelöst werden.[967] Es wäre nicht fernliegend, dass Menschen, die das Gefühl haben, Opfer einseitiger Bildaufnahmen oder durch geminderte Teilhabe an einer virtuellen Realität benachteiligt zu werden, ebenfalls Smartglasses erwerben, um diese Nachteile auszugleichen.[968] Das Konzept der „Sousveillance" sieht eine solche Aufrüstung als Gegenpol zur institutionellen Überwachung sogar als unausweichlich und notwendig an.[969]

(2) Smarte und mobile Videoüberwachung

Neben Smartglasses ist der öffentliche Raum bereits gegenwärtig durch die Präsenz einer Vielzahl von Videokameras geprägt, und es gibt kaum einen Bereich, in denen die Videotechnik nicht zur Anwendung durch staatliche oder private Stellen, vor allem zu Zwecken der Prävention und Repression, gelangt.[970] Die Qualität und Quantität der Videoüberwachung wird sich zudem in der Zukunft vor allem durch „smarte" Geräte verändern, die Auswertungs- und Entscheidungskompetenzen von Menschen auf Computeralgorithmen übertragen sowie Daten aus anderen Sensoren herbeiziehen (z.B. akustische Daten oder RFID-Chips), wodurch die Ge-

---

[966] Vgl. B III. 5. d), S. 47; vgl. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 88 ff.

[967] Vgl. zur Gefahr einer standardmäßigen Ausstattung von Fahrzeugen mit "Dashcams", wenn diese als Beweismittel zugelassen werden würden, AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291.

[968] Vgl. C II. 3, S. 68.

[969] Vgl. E III. 1. a) dd), 142; vgl. LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (Rn. 17); AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291.

[970] Videotechnik wird durch staatliche Stellen zur Überwachung öffentlicher Plätze und Straßen eingesetzt, zur Beobachtung von Demonstrationen und Großveranstaltungen, zur Überführung von Straßenverkehrsverstößen sowie zur Objekt- Eigen- und Beweissicherung an Grenzübergängen, Schulgebäuden, Krankenhäusern, Schimmbädern oder Gerichten und durch private Stellen auf Privatgrundstücken, in Bahnhöfen, Hauseingängen oder in Ladenlokalen, *Ketzer*, Securitas ex Machina, 2005, S. 4; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 33 ff.; Überwachungskameras werden auch in Fahrzeugen, wie z.B. im öffentlichen Nahverkehr oder Taxen eingesetzt, *Bergfink*, DuD 2015, S. 145 (147); zu den Überwachungskameras kommen "Webcams", d.h. stationäre Kameras, die Livebilder zur Informations- und Unterhaltszwecken z.B. von Gemeindeplätzen dienen, vgl. Wie ist der Einsatz von Webcams durch Kommunen datenschutzrechtlich zu bewerten, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/video/Webcam_Kommunen.pdf (13 .8.2014); der Rheinland-Pfälzische Datenschutzbeauftragte geht davon aus, dass deutschlandweit ca. 100.000 Kameras durch Jäger in den Wäldern montiert worden sind, Wildkameras: Datenschützer gehen gegen Jäger vor, SPIEGEL ONLINE, http://www.spiegel.de/netzwelt/gadgets/wildkameras-datenschuetzer-gehen-gegen-jaeger-vora-967549.html (5.5.2014).

fahr der durchgehenden Überwachung und einer Profilierung der erfassten Personen steigt.[971]

Des Weiteren wird der öffentliche Raum mithilfe immer genauer werdender Luftbildaufnahmen[972] sowie Straßenpanoramadiensten wie „Google Street View“ oder Microsofts „Street Side“, die virtuelle Begehungen physischer Orte ermöglichen, abgebildet.[973] Zur Visualisierung des öffentlichen Raums tragen sowohl im Umfang als auch in der Qualität mobile Erfassungsmöglichkeiten via Smartphones oder sonstiger Minikameras bei.[974] Die mobilen Geräte können Bereiche des menschlichen Alltags einsehen, die fest montierten Kameras vorenthalten sind. Da die Geräte immer erschwinglicher werden, steigt ihre Nutzung vor allem bei Privatpersonen, von denen sie im großen Umfang eingesetzt werden, um Fotografien und Videofilme zu erstellen.[975] Auch Smartwatches können mit Kameras ausgestattet werden, die es erlauben, Aufnahmen „vom Handgelenk aus“ zu erstellen, ohne das Smartphone hervorholen zu müssen.[976]

Daneben gibt es spezielle Geräte, die für „Life Logging“ geeignet sind und z.B. um den Hals getragen und permanent oder in bestimmten Intervallen Aufnahmen auslösen, ohne dass sie direkt als Aufnahmegeräte für ein ungeübtes Auge erkennbar sind.[977] Ebenfalls im regulären Handel sind sog. „Minispione“ erhältlich, die kleine Kameras z.B. in Brillengestellen oder in Kugelschreibern enthalten und darauf angelegt sind, dass der

---

[971] *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (239 f.); *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (112 f.); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 15 f.; *Spiecker genannt Döhmann*, K&R 2014, S. 549 (550 f.); *Wrede*, ZD 2012, S. 321 (322).

[972] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 23 ff.

[973] *Ernst*, CR 2010, S. 178; *Forgó*, MMR 2010, S. 217; *Jahn/Striezel*, K&R 2009, S. 753; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 27 ff.; *Klar*, MMR 2012, S. 788 (789); *Lindner*, ZUM 2010, S. 292; *Moos/Zeiter*, ZD 2013, S. 178; *Spiecker genannt Döhmann*, CR 2010, S. 311; *Weber*, NJOZ 2011, S. 673.

[974] BT-DrS. 18/3202, S. 28; BT-DrS. 18/2601, S. 36; *Busch*, NJW 2015, S. 977; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 1 f.

[975] Alle Smartphone-Nutzer machen Fotos, BITKOM, http://www.bitkom.org/de/presse/8477_79882.aspx (11.8.2014); Bundesverband Digitale Wirtschaft, Faszination Mobile Verbreitung, Nutzungsmuster und Trends, 2014, http://www.bvdw.org/mybvdw/media/view?media=5727 (7.1.2014); Smartphones werden zur Urlaubskamera, BITKOM, http://www.bitkom-research.de/epages/63742557.sf/de_DE/?ObjectPath=/Shops/63742557/Categories/Presse/Pressearchiv_2013/Smartphones_werden_zur_Urlaubskamera (7.1.2014).

[976] Galaxy Gear: Samsung wird Uhrmacher, heise online, http://www.heise.de/newsticker/meldung/Galaxy-Gear-Samsung-wird-Uhrmacher-1947433.html (5.7.2014).

[977] *Fankhauser*, Tiny Camera Logs Your Life As Long as the Lighting Is Good, Mashable, http://mashable.com/2014/02/26/narrative-clip/(2.10.2015).

Aufnahmevorgang nicht bemerkt wird.[978] Daneben werden im Privatbereich sog. „Actioncams“ eingesetzt, die z.B. von Fahrradfahrern auf ihren Helmen montiert werden (daher auch als „Helmkameras“ bezeichnet), um ihre Fahrten zu Erinnerungs- oder Beweiszecken aufzuzeichnen.[979] Ebenso im Freizeitbereich werden vermehrt unbemannte Fluggeräte, sog. „Drohnen“, eingesetzt, die oft werkseitig mit Kameras ausgestattet werden und auch handflächentellergroß oder gar kleiner sein können.[980]

Mobile Aufzeichnungsgeräte finden auch in den Polizeidienst Eingang. Unter dem Begriff „Bodycams“ werden am Körper, z.B. auf der Schulter (in diesem Fall werden sie als „Schultercams“ bezeichnet) oder am Kopf, getragene Minikameras verstanden, die zur Deeskalation sowie dem Schutz der Polizeikräfte dienen sollen.[981]

Ein weiteres Einsatzfeld für mobile Kameras zu Überwachungszwecken bieten Kraftfahrzeuge. Als „Dashcams“ (das englische Wort „dashboard“ bedeutet Armaturenbrett) werden On-Board-Kameras bezeichnet, die in Kraftfahrzeugen angebracht werden und das Geschehen vor dem Fahrzeug

---

978 Vgl. BT-DrS. 10/1618, S. 9.

979 *Fuchs*, ZD 2015, S. 212 (212 f.); *Hilgefort/Labusga*, Action-Cams für Full-HD-Videos – wasserdicht, staubgeschützt, weitwinkelig, c't, http://www.heise.de/ct/ausgabe/2014-18-Test-Action-Cams-fuer-Full-HD-Videos-wasserdicht-staubgeschuetzt-weitwinkelig-2284622.html (5.9.2015); *Reibach*, DuD 2015, S. 157.

980 *Bumiller/Shanker*, Microdrones, Some as Small as Bugs, Are Poised to Alter War, http://www.nytimes.com/2011/06/20/world/20drones.html (3.7.2013); *Hofmann/Hödl*, DuD 2015, S. 167; *Regenfus*, NZM 2011, S. 799 (800); *Solmecke/Nowak*, MMR 2014, S. 431; *Weichert*, ZD 2012, S. 501.

981 In Deutschland werden Bodycams in Hamburg und Hessen, laut Behördenaussagen mit positiven Effekten, erprobt, Mini-Kamera soll Polizei schützen: „Body-Cam-Projekt“ wird auf Offenbach ausgeweitet, OP-Online, http://www.op-online.de/lokales/nachrichten/offenbach/mini-kamera-soll-polizei-schuetzen-offenbach-3515776.html (5.7.2014); Bodycams für Hamburgs Polizisten - Innenbehörde Hamburg - FHH, hamburg.de, http://www.hamburg.de/pressearchiv-fhh/4366188/2014-09-02-bis-pm-bodycam/ (2.10.2014); die Kameras werden nach Angaben des hessischen Innenministeriums an der Uniformschulter getragen, zeichnen nur Bilder ohne den Ton auf und dürfen nur punktuell bei Einsätzen im öffentlichen Raum, wie Kontrollen oder dem Schlichten von Streitigkeiten eingeschaltet werden und zudem müssen die Polizisten über den Einsatz der Kamera informieren sowie eine Aufschrift "Videoüberwachung" an deren Uniform tragen, Innenminister Boris Rhein: „Body-Cam“ verhindert Gewalt gegen Polizeibeamte, Hessisches Ministerium des Innern und für Sport, https://innen.hessen.de/presse/pressemitteilung/innenminister-boris-rhein-body-cam-verhindert-gewalt-gegen-polizeibeamte (5.7.2014).

aufzeichnen.[982] Sie dienen vor allem dazu, Beweise für den Fall von verkehrsbezogenen Geschehnissen, wie Unfällen, zu sammeln oder als Abschreckung gegen Diebstahl oder Vandalismus.[983] Dashcams werden auch in Deutschland zunehmend populär, nachdem sie in vielen ausländischen Staaten Verbreitung gefunden haben und dort insbesondere auch zum Schutz vor Gewalttätern und korrupten Polizisten eingesetzt werden.[984]

Auch Fahrzeughersteller bauen in die Fahrzeuge Systeme ein, die zur optischen Erkennung des Verkehrsgeschehens dienen. Hierbei ist zwischen Assistenzsystemen zu unterscheiden, die Aufnahmen lediglich zu technischen Zwecken verwenden, und damit Persönlichkeitsrechte Dritter kaum oder gar nicht beeinträchtigen.[985] Andere Systeme erlauben dagegen ähnlich wie bei Dashcams einen Zugriff auf die vom Fahrzeug erstellten Videoaufzeichnungen.[986]

Nicht zuletzt ist zu berücksichtigen, dass die visuelle Erfassung des öffentlichen Raums nicht nur aus Aufnahmen besteht, sondern diese häufig von Geo- und anderen Daten begleitet werden.[987]

(3) Potenzial von Big-Data-Analysen

Im Rahmen der Summierungseffekte muss neben der bloßen Abbildung des öffentlichen Raums in Form von Bildaufnahmen und sonstigen Daten auch ihre Verschneidung, vor allem das unter dem Begriff „Big Data Ana-

---

[982] LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (Rn. 17); AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (238); *Balzer/Nugel*, NJW 2014, S. 1622; *Knyrim/Trieb*, ZD 2014, S. 547; *Lachenmann/Schwiering*, NZV 2014, S. 291; *Terhaag*, K&R 2015, S. 556.

[983] *Balzer/Nugel*, NJW 2014, S. 1622; *Knyrim/Trieb*, ZD 2014, S. 547; *Lachenmann/Schwiering*, NZV 2014, S. 291.

[984] *Lachenmann/Schwiering*, NZV 2014, S. 291; im Jahr 2014, sollen rund 79.000 Dashcams in Deutschland verkauft worden sein, *Przybilla*, Frontscheibenkameras - Die Debatte um Dashcams, SZ, http://www.sueddeutsche.de/auto/frontscheibenkameras-ungetruebter-blick-nach-vorn-1.2603860 (15.8.2015); *Spoerr*, Warum Russen Armaturenbrett-Kameras haben, Welt Online, http://www.welt.de/vermischtes/article113661810/Warum-Russen-Armaturenbrett-Kameras-haben.html (3.7.2013).

[985] *Fuchs*, ZD 2015, S. 212 (213); *Grundhoff*, Verkehrszeichenerkennung, FOCUS Online, http://www.focus.de/auto/ratgeber/sicherheit/assistenzsysteme/verkehrszeichenerkennung-das-magische-auge_aid_346187.html (22.8.2014).

[986] *Harder*, Valet Mode in der Chevrolet Corvette, Spiegel Online, http://www.spiegel.de/auto/aktuell/valet-mode-in-der-chevrolet-corvette-big-brother-faehrt-mit-a-987189.html (22.8.2014).

[987] Vgl. Neue Foursquare-App trackt den Nutzer permanent, Mac & I, http://www.heise.de/mac-and-i/meldung/Neue-Foursquare-App-trackt-den-Nutzer-permanent-2289001.html (13.8.2014); *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 115; *Weichert*, SVR 2014, S. 201.

lytics“ diskutierte Potenzial ihrer Analyse, berücksichtigt werden.[988] Dazu gehört u.a. die Auswertung des Verhaltens von Menschen zu wirtschaftlichen Zwecken sowohl im virtuellen als auch im physischen Raum.[989] Ebenso werden unter dem Begriff der „Predictive Politics“ oder „Precrime“ Datenanalysen zur Verhinderung von Gefahren, aber auch der Einschätzung der Kriminalitätsneigung von Personen entwickelt.[990] Ebenso müssen die Begierden der geheimdienstlichen Überwachung in Erwägung gezogen werden.[991] Auch im privaten Bereich sollen digitale Assistenten den Menschen bei Alltagsaufgaben vorausschauend unterstützen, was wiederum die Analyse möglichst vieler Daten über Menschen und deren Gewohnheiten erfordert.[992] Bei der Addition dieser Möglichkeiten der Informationsgewinnung muss jedoch auch berücksichtigt werden, dass Daten häufig institutionell dezentral in unterschiedlichen Unternehmen und staatlichen Stellen gespeichert sowie verarbeitet werden, was deren Verschneidung erschweren kann.[993]

dd) Präzedenzlose Gefährdung der Privatsphäre

Die summarische Betrachtung der Nutzung von Smartglasses im öffentlichen Raum zeigt, dass die Wahrscheinlichkeit seiner Visualisierung und die Wahrscheinlichkeit, als Person im öffentlichen Raum von Kameras

---

[988] Vgl. A IV. 3, S. 10.

[989] Vgl. *Arning/Moos*, ZD 2014, S. 126; *Arning/Moos*, ZD 2014, S. 242; *Hammersen/Eisenried*, ZD 2014, S. 342 (343); *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 202; *Roßnagel*, NJW 2009, S. 2716.

[990] Precrime, heise online, http://www.heise.de/newsticker/meldung/Precrime-Bayerische-Polizei-setzt-Software-gegen-Einbrecher-ein-2287024.html (6.8.2014); *Goetz/Leyendecker /Obermaier*, Geheimdienst: BND will soziale Netzwerke ausforschen, Süddeutsche.de, http://www.sueddeutsche.de/digital/auslandsgeheimdienst-bnd-will-soziale-netzwerke-live-ausforschen-1.1979677 (15.6.2014); *Goode*, Sending the Police Before There’s a Crime, New York Times, http://www.nytimes.com/2011/08/16/us/16police.html (5.7.2014); *Kipker*, Precobs - Polizeiarbeit zwischen Fähnchenabstecken und Minority Report, EAID, http://www.eaid-berlin.de/?p=760 (11.9.2015); *Siegel*, Predictive Analytics, 2013, S. 51 ff.

[991] *Moglen*, Privacy under attack: the NSA files revealed new threats to democracy, The Guardian, http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy (10.6.2014).

[992] *Fabian/Hansen*, TAUCIS - Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, ULD und Institut für Wirtschaftsinformatik der HU Berlin, 2006, https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf (30.6.2014), S. 23; *Roßnagel*, Datenschutz bei Wearable Computing, 2012, S. 2 ff.; *Sheth*, Forget Apps, Now The Bots Take Over, TechCrunch, http://social.techcrunch.com/2015/09/29/forget-apps-now-the-bots-take-over/(3.10.2015); *Wortham*, Will Google’s Personal Assistant Be Creepy or Cool?, Bits Blog, http://bits.blogs.nytimes.com/2012/06/28/will-googles-personal-assistant-be-creepy-or-cool/(12.10.2013).

[993] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 33.

erfasst zu werden, mit der Verbreitung von Smartglasses im großen Umfang zunehmen werden. Des Weiteren ist zu berücksichtigen, dass eine strenge Regulierung des sonstigen Einsatzes von Videotechnik im öffentlichen Raum kaum gerechtfertigt werden könnte, wenn ohnehin jeder jeden heimlich überwachen kann. D.h., die Verbreitung von Smartglasses könnte eine Art Dammbruch bewirken, der Überwachungstechnologien im öffentlichen Raum omnipräsent machen würde. Dadurch steigt auch die Wahrscheinlichkeit, dass die bei audiovisueller Datenerhebung anfallenden Informationen wirtschaftlichen und staatlichen Zwecken oder zur moralischen Würdigung des Verhaltens von Betroffenen durch ihre Mitmenschen dienen werden. Zusammenfassend müssen Smartglasses, insbesondere in der Zusammenwirkung mit anderen informationellen Technologien, als eine der bisher größten technologischen Herausforderungen für die Privatsphäre angesehen werden.[994]

2. Gewichtung der Interessen an der Nutzung von Smartglasses

Da die Beeinträchtigung der Privatsphäre durch Smartglasses erheblich ist, müssen die Interessen der Nutzer von Smartglasses ebenfalls von hohem Gewicht sein, um sie zu rechtfertigen. Nachfolgend werden daher die typischerweise beim Einsatz von Smartglasses im öffentlichen Raum in Frage kommenden Interessen nach den Kriterien der Verhältnismäßigkeit beurteilt. Die Prüfung der Verhältnismäßigkeit beginnt zuerst mit der Prüfung, ob Smartglasses geeignet sind, um die verfassungsrechtlich geschützten Interessen zu verfolgen. Da für die Geeignetheit einer Maßnahme ausreichend ist, dass sie das angestrebte Ziel fördert, darf sie vorliegend im Rahmen der abstrakten verfassungsrechtlichen Prüfung unterstellt werden.[995] Ebenso wird unterstellt, dass Smartglasses für die geprüften Zwecke erforderlich, also das mildeste gleich geeignete Mittel sind, um diese Ziele zu erreichen.[996] Der Grund für die unterstellte Eignung und Erforderlichkeit liegt darin, dass im Rahmen dieser Untersuchung die besonderen Vorzüge von Smartglasses geprüft werden sollen, was die Annahme beinhaltet, dass es keine gleich geeigneten Mittel für die Verfolgung der konkreten Interessen gibt. Die Interessenabwägung soll daher auf der verfassungsrechtlichen Ebene nicht die Frage beantworten, ob Augmented Reality und ein schneller Informationszufluss in konkreter Situation hinreichend mit Smartphones oder anderer Technologie gewähr-

---

994 *Schwenke*, K&R 2013, S. 685.

995 Vgl. *Pieroth u.a.*, Grundrechte, 2014, Rn. 293 ff.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 46.

996 Vgl. *Pieroth u.a.*, Grundrechte, 2014, Rn. 295 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 296; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 87; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 48.

leistet werden können. Die zu beantwortende Frage ist vielmehr, ob die Inanspruchnahme von Augmented Reality, schnellere Informationsflüsse und andere Vorteile der Nutzung von Smartglasses, die Beeinträchtigung der Privatsphäre generell rechtfertigen können.

a) Bequemlichkeit, Effizienz und Gefahrenabwehr

Im Regelfall werden Smartglasses im öffentlichen Raum zu Zwecken der Bequemlichkeit oder Effizienzsteigerung genutzt.[997] Ebenso können sie Vorteile für eine demokratische Gesellschaft mit sich bringen, indem sich Bürger z.B. schneller informieren, sich einen Überblick über Tatsachen verschaffen und sich vernetzen können.[998] Das Interesse an der Verfolgung dieser Zwecke ist zwar verfassungsrechtlich geschützt, seine Bedeutung kann abstrakt jedoch nur schwer festgestellt werden. So ist dem Einsatz von Smartglasses zur Befriedigung persönlicher Neugier generell ein geringeres Gewicht beizumessen als z.B. dem Einsatz zur Kontrolle von Polizisten im Rahmen einer Demonstration.[999] In den meisten Fällen werden jedoch die Interessen an der Steigerung der effizienteren Anbindung von Menschen an die Informationsströme und deren Visualisierung nicht die Beeinträchtigungen der für den grundlegenden Schutz von Individuen und der demokratisch-freiheitlichen Gesellschaft erforderlichen Privatsphäre rechtfertigen. Dieser Zustand mag sich mit der steigenden Unvermeidlichkeit der Anbindung von Menschen an die virtuelle Realität ändern, ist derzeit jedoch noch nicht gegeben. D.h., solange Smartglasses die durch sie verursachten Nachteile nicht anderweitig ausgleichen können, ist deren Nutzung verfassungsrechtlich nicht gerechtfertigt.[1000]

---

997 Vgl. B III, S. 35.

998 Vgl. *Castells*, Communication Power, 2009, S. 421; *Koskela*, Surveillance & Society 2002, Vol. 2, Nr. 2/3, p. 199 (204); *Shirky*, The political power of social media: technology, the public sphere, and political change., Foreign Affairs, https://www.foreignaffairs.com/articles/2010-12-20/political-power-social-media (2.10.2015); *Webster*, Theories of the Information Society, 2014, S. 240 f.; eine Begrifflichkeit zur Umschreibung dieser Vorteile ist "participatory surveillance" (was in Deutsch ungefähr mit dem Begriff "partizipative Teilnahme an der Überwachung" übersetzt werden kann) und zum Ausdruck bringen soll, dass viele Typen der Überwachung auch sozial positive Effekte haben können, *Albrechtslund*, First Monday 2008, Vol. 13, Nr. 3, http://firstmonday.org/ojs/index.php/fm/article/view/2142 (30.9.2014); in diesem Zusammenhang wird auch von "Empowerment", d.h. stärkung der Entfaltungsmöglichkeiten der Menschen gesprochen, Art. 29-Datenschutzgruppe, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, 2013, S. 2.

999 Vgl. BVerfG, Beschl. v. 24.7.2015 (1 BvR 2501/13), ZUM 2015, 986 (987 f.); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (391); vgl. BVerfG, Urt. v. 14.2.1973 (1 BvR 112/65), BVerfGE 34, 269 (283).

1000 Vgl. A III. 1, S. 6.

Eine Ausnahme wäre allenfalls dann zu machen, wenn Smartglasses eingesetzt würden, um präventiv der Abwehr und repressiv der Verfolgung von schweren Angriffen auf die Persönlichkeitsrechte, die körperliche Integrität, nicht nur unerhebliches Eigentum, oder die Existenz der Nutzer von Smartglasses zu sichern.[1001] Jedoch wären zumindest konkrete Anhaltspunkte für die Gefährdung dieser Rechtsgüter erforderlich und die Rechtfertigung würde punktuell auf die Gefährdungssituation beschränkt sein.[1002] Folglich würde lediglich ein abstraktes Gefährdungsgefühl nicht ausreichen, und damit wird die verhältnismäßige Nutzung von Smartglasses nur auf extreme Einzelfälle beschränkt sein.[1003] Als weiterer Sonderfall eines besonders hohen Interesses an der Nutzung von Smartglasses ist deren medizinische Indikation zu nennen, z.B. wenn körperliche Nachteile, insbesondere die Sehschwäche, ausgeglichen werden sollen.[1004]

b) Visuelle Informationskontrolle

Als eine die Privatsphäre möglicherweise rechtfertigende Nutzung soll deren Fähigkeit zur Kontrolle visueller Informationszuflüsse mittels Mediated Reality untersucht werden.[1005] Dem Konzept liegt der Gedanke zugrunde, dass Dritte aufgrund des Anstiegs von Überwachungsmaßnahmen zwar mehr über eine Person in Erfahrung bringen können, dieses Wissen jedoch im Gegenzug weniger zur Beeinflussung dieser Person einsetzen sollen.[1006] D.h., die Gefahr für die Selbstbestimmung der Person soll durch die Kontrolle des Informationszuflusses kompensiert werden. Es erscheint jedoch mehr als zweifelhaft, dass die Kontrolle des visuellen

---

[1001] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (50); BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238 (250); BGH, Urt. v. 27.1.1994 (I ZR 326/91), NJW 1994, 2289 (2292 f.); BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277 (278); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (287 f.); OLG Düsseldorf, Urt. v. 5.5.1997 (5 U 82/96), NJW-RR 1998, 241; BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); vgl. *Horst*, NZM 2000, S. 937 (942).

[1002] LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531); BAG, Urt. v. 21.6.2012 (2 AZR 153/11), NJW 2012, 3594 (3596 f.); BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 288 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 79 f.

[1003] OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545; AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 80.

[1004] Vgl. E III. 4, S. 146; da diese Untersuchung sich nicht speziell der Nutzung von Smartglasses durch körperlich beeinträchtigte Personen widmet, wird deren Nutzung nachfolgend nicht bei jeder Interessensabwägung gesondert berücksichtigt.

[1005] Vgl. E III. 1. b), S. 143.

[1006] Mann sieht darin einen "Trade off", also ein Tauschgeschäft zwischen Smartglasses und der Privatsphäre, *Mann/Niedzviecki*, Cyborg, 2002, S. 148.

Informationszuflusses das Recht auf Rückzug und Kontrolle der Informationsabflüsse ausgleichen kann.

Zum einen fehlt es bereits an einer nachvollziehbar dargelegten Wirksamkeit und Relevanz der visuellen Informationskontrolle als Schutz vor Konformität. Kommerzielle oder politische Werbung im öffentlichen Raum ist bereits heutzutage präsent,[1007] ohne jedoch im Regelfall einen Grad zu erreichen, der sie unausweichlich werden ließe und z.B. einen Unterlassungsanspruch gegenüber dem Werbenden begründen würde.[1008] Des Weiteren deutet nichts darauf hin, dass sich der Belästigungsgrad von beeinflussenden Informationszuflüssen in der rein physischen Realität dank Smartglasses wesentlich mindern wird. Vielmehr ist damit zu rechnen, dass die Informationszuflüsse zunehmend virtuell erfolgen und vor den Augen der Nutzer von Smartglasses eingeblendet werden (z.B. durch Einblendung virtueller Werbeobjekte, was verballhornend als „ADmented Reality", also um Werbung erweiterte Wirklichkeit, bezeichnet wird).[1009] Die Kontrolle einer virtuellen Informationsbelästigung durch Smartglasses kann an dieser Stelle jedoch nicht zu deren Gunsten berücksichtigt werden, da sie erst durch Smartglasses entsteht.

Im Ergebnis sind durch visuelle Informationskontrolle mit Mediated Reality nur relativ geringe Vorteile für die Privatsphäre zu erwarten, sodass sie keineswegs die Gefährdung der Privatsphäre durch Smartglasses zu rechtfertigen vermag.

c) Sousveillance und Transparenz

Als ein ebenfalls speziell mit Smartglasses verbundener Vorteil wird das Potenzial zur Umsetzung einer „Sousveillance", d.h. der Befähigung von Bürgern zur „Zurücküberwachung" von wirtschaftlichen oder staatlichen Instanzen, betrachtet.[1010] Das Konzept der Sousveillance entspricht insoweit der Vorstellung einer „transparenten Gesellschaft", deren Ziel die „Demokratisierung der Überwachung" ist, also Abschaffung einer auf einem Informationsgefälle beruhenden Asymmetrie der Macht dank der Transparenz aller Gesellschaftsakteure.[1011] Beide Transparenzkonzepte werden nachfolgend sowohl im Hinblick auf die Beeinträchtigung der Privatsphäre als auch deren Ausgleich gemeinsam gewürdigt.

1007 *Fikentscher/Möllers*, NJW 1998, S. 1337 (1338); *Pieroth u.a.*, Grundrechte, 2014, Rn. 610.

1008 *Fikentscher/Möllers*, NJW 1998, S. 1337 (1341); *Pieroth u.a.*, Grundrechte, 2014, Rn. 610.

1009 *Jonathan McIntosh*, ADmented Reality - Google Glasses Remixed with Google Ads, YouTube, https://www.youtube.com/watch?v=_mRF0rBXIeg (12.9.2015).

1010 Vgl. E III. 1. a) dd), 142.

1011 *Brin*, The Transparent Society, 1999, S. 14 ff.; ähnlich als Metapher des "kristallenen Herzens bereits vertreten von Rousseau, S. *Han*, Transparenzgesellschaft, 2012, S. 73; vgl. *Heller*, Post Privacy, 2011, S. 124 ff.

aa) Gefahr einer synoptischen Kontrollgesellschaft

Um die Eignung der vorgenannten Transparenz-Konzepte für die Stärkung der Bürgerrechte zu belegen, werden Beispiele aufgeführt, in denen (vor allem in den USA) das Fehlverhalten der Staatsgewalt mittels privater Videoaufnahmen überführt wurde.[1012] Jedoch ist zu bedenken, dass es sich i.d.R. um Situationen handelte, in denen eine konkrete Gefährdungslage gegeben war, die grundsätzlich die Berechtigung zum punktuellen Einsatz von Kameras mit sich bringen kann.[1013] Mit dem Konzept der Sousveillance soll dagegen der generelle Einsatz von Smartglasses gerechtfertigt werden, sodass deren Nutzung unabhängig von Gefahrensituationen erlaubt sein soll. Vom Standpunkt einer Gefährdung ihrer Nutzer sollen Smartglasses also bereits deren abstrakte Gefährdung durch institutionelle Kräfte abwehren. Diese Verteidigungsmaßnahme würde jedoch zugleich dazu führen, dass auch andere Menschen mit überwacht würden. Insoweit würden Smartglasses auf einen Generalverdacht hin gegenüber jedermann eingesetzt. Dies erscheint insoweit widersinnig, als gerade die Überwachung auf Grundlage eines Generalverdachts gegenüber den Menschen dem Staat vorgeworfen wird, wenn z.B. Daten der Bürger auf Vorrat wegen eines potenziellen Fehlverhaltens gespeichert werden sollen.[1014] Mit Sousveillance wäre ein solcher Generalverdacht zu einem Gesamtkonzept erhoben, dessen Vorteil für die Bürger und die Gesellschaft ebenfalls bezweifelt werden muss.

Mit der Omnipräsenz von Smartglasses würde die Focault'sche Idee einer panoptischen Disziplinargesellschaft zulasten der Individuen sowie der Meinungspluralität modifiziert.[1015] Die panoptische Disziplinierung ist auf eine zentrale Überwachung ausgerichtet, während mit Smartglasses

---

[1012] Vgl. Beispiele in *Fuchs u.a.*, Introduction, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 1 (12); *Mann/Ferenbok*, Surveillance and Society 2013, Vol. 11, Nr. 1/2, p. 18 (31).

[1013] Vgl. E IV. 2. a), S. 172; ebenso müssen z.B. die Aspekte einer herausfordernden Videoüberwachung durch Polizeibeamte bei der Beurteilung der Beeinträchtigungswirkung einer "Gegenüberwachung" berücksichtigt werden, wobei es jedoch lt. BVerfG keine "'Waffengleichheit" zwischen den Teilnehmern einer öffentlichen Versammlung und der Polizei geben kann, BVerfG, Beschl. v. 24.7.2015 (1 BvR 2501/13), ZUM 2015, 986 (987 f.).

[1014] EuGH, Urt. v. 8.4.2014 (C-293/12, C-594/12), NJW 2014, 2169 (2172); BVerfG, Urt. v. 2.3.2010 (1 BvR 256/08, 1 BvR 263/08 u. 1 BvR 586/08), BVerfGE 125, 260 (343 f.); *Beck*, Das Zeitalter der Nebenfolgen und die Politisierung der Moderne, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 19 (72); *Hotter*, Privatsphäre, 2011, S. 129; *Schaar*, Das Ende der Privatsphäre, 2007, S. 149 ff.

[1015] Vgl. D I. 5, S. 78; *Bauman*, Liquid Surveillance, 2012, S. 3 ff.; *Fuchs u.a.*, Introduction, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 1 (6 ff.); *Han*, Transparenzgesellschaft, 2012, S. 74 f.; *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (106); *Lyon*, Electronic Eye, 1994, S. 26, 67.

eine als „aperspektivisches Panoptikum“,[1016] „elektronisches Superpanoptikums“,[1017] „Post-Panoptikum“[1018] oder „Synoptikum“[1019] bezeichnete dezentralisierte, von räumlichen, territorialen und zeitlichen Beschränkungen gelöste Überwachung „von allen Seiten, von überall“, durch jede Institution und jedermann zu erwarten wäre.[1020]

Von den Vertretern einer transparenten Gesellschaft wird ein durch Smartglasses geschaffenes Synoptikum jedoch positiv betrachtet, da es sich um eine offene und nicht wie bisher verdeckte Videoüberwachung handelt.[1021] Nach deren Ansicht wird die auf der Unkenntnis einer zentralen Überwachung basierende Disziplinierung aufgehoben, wenn die Überwachung omnipräsent ist.[1022] Dahinter steht jedoch die Erwartung, dass Menschen sich an Smartglasses und damit eine ubiquitäre Überwachung freiwillig und selbstbestimmt gewöhnen werden. Doch die Gewöhnung an eine unausweichliche Überwachung kann zugleich eine kognitive Anpassung infolge der Aufgabe einer selbstbestimmten Persönlichkeitsentfaltung darstellen.[1023] Damit ist zu rechnen, wenn Menschen, deren Denken und Handeln dem öffentlichen Urteil unterstellt ist, sich daran werden gewöhnen müssen, nur ein gesellschaftlich akzeptiertes Verhalten an den Tag zu legen.[1024]

Es ist den Vertretern einer transparenten Gesellschaft insoweit zuzustimmen, als durch das Fehlen einer zentralen und heimlichen Überwachung das Konzept der Disziplinargesellschaft aufgegeben wird. Zu befürchten ist jedoch, dass die Disziplinargesellschaft durch ein nicht minder beeinträchtigendes Konzept einer „Kontrollgesellschaft“ abgelöst

---

1016 *Han*, Transparenzgesellschaft, 2012, S. 74 f.

1017 *Poster*, The Mode of Information, 1991, S. 93; von einem "elektronischen Panoptikon" sprechend, *Gordon*, Politics & Society 1987, Vol. 15, Nr. 4, p. 483.

1018 *Bauman*, Liquid Surveillance, 2012, S. 3 ff.

1019 *Hotter*, Privatsphäre, 2011, S. 92 f.; *Wall*, Surveillant Internet Technologies and the Growth in Information Capitalism, in: *Ericson/Haggerty*, The New Politics of Surveillance and Visibility, 2006, S. 340 (342 f.).

1020 Vgl. *Arthur*, Google Glass, The Guardian, http://www.guardian.co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy (2.7.2013); *Bauman*, Liquid Surveillance, 2012, S. 3 ff.; *Fuchs u.a.*, Introduction, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 1 (7); *Haggerty/Ericson*, The surveillant assemblage, in: *Hier*, The Surveillance Studies Reader, 2007, S. 104 (112); *Han*, Transparenzgesellschaft, 2012, S. 74 f.; *Poster*, The Mode of Information, 1991, S. 93.

1021 *Mann/Niedzviecki*, Cyborg, 2002, S. 143.

1022 Ebenda, 166.

1023 *Beck*, Das Zeitalter der Nebenfolgen und die Politisierung der Moderne, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 19 (74).

1024 *Han*, Transparenzgesellschaft, 2012, S. 78; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 100; *Sofsky*, Verteidigung des Privaten, 2007, S. 129 f.

wird.[1025] Eine Kontrollgesellschaft kann als eine Abwandlung der Disziplinargesellschaft betrachtet werden, in der Menschen in ein Überwachungssystem integriert sind und sich der Überwachung nicht aus äußerem Zwang, sondern aus einem „selbstgenerierten Bedürfnis" unterwerfen.[1026] Als Vorboten einer Kontrollgesellschaft werden z.B. soziale Netzwerke betrachtet, deren Nutzer sich freiwillig der Überwachung zu kommerziellen Zwecken im Tausch gegen die Vorzüge der Teilnahme an dem virtuellen gesellschaftlichen Leben aussetzen.[1027]

Mit der Verbreitung von Smartglasses als Schnittstellen zur virtuellen Realität ist durchaus damit zu rechnen, dass Menschen sich noch mehr in eine solche „digitale Einfriedung" (englisch: „Digital Enclosure") begeben könnten.[1028] Das bedeutet jedoch, dass Smartglasses es erlauben werden, nicht nur ihre Träger, sondern zugleich die von ihnen erfassten Dritten effektiver zu kontrollieren.[1029] Des Weiteren eröffnet sich durch das Potenzial der Einflussnahme auf die visuelle Realitätswahrnehmung von Datenbrillenträgern die Möglichkeit, deren Lebensalltag effektiver zu beeinflussen als z.B. mit Smartphones. Dystopisch betrachtet, könnten Menschen auf diese Art und Weise in kontrollierte Systeme integriert werden, in denen Smartglasses als Kontrollinstrumente für staatliche, wirtschaftliche oder moralische Interessen dienen.[1030] Als Folge einer derartigen Kontrolle von Menschen wird insbesondere deren soziale Benachteiligung durch die Möglichkeiten gesehen, Menschen effektiver nach Konformitäts-, Leistungs- und Relevanzkriterien sortieren zu können.[1031]

1025 *Deleuze*, Unterhandlungen, 1993, S. 250.

1026 *Han*, Transparenzgesellschaft, 2012, S. 76 f.

1027 *Fuchs*, Critique of the Political Economy of Web 2.0 Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 31 (53); *Gandy*, The Panoptic Sort, 1993, S. 15; *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (117); *Sandoval*, A Critical Empirical Case Study of Consumer Surveillance on Web 2.0, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 147 (163); *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (258).

1028 *Andrejevic*, iSpy, 2009, S. 257.

1029 Vgl. Ebenda, 3.

1030 Vgl. *Deleuze*, Unterhandlungen, 1993, S. 250; die durch die Vernetzung hergestellte Befähigung Einzelner zur sozialer Kommunikation und Erstellung von Inhalten verkomme lt. Fuchs zu einem asymetrischen Verwertungsprozess, *Fuchs*, Critique of the Political Economy of Web 2.0 Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 31 (53); vgl. *Han*, Transparenzgesellschaft, 2012, S. 58 f.; vgl. *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (109); vgl. *Ketzer*, Securitas ex Machina, 2005, S. 49; vgl. *Lindenberg/Schmidt-Semisch*, Kriminologisches Journal 1995, S. 2 (3); vgl. *Lyotard*, Das Postmoderne Wissen, 1986, S. 43 f.

1031 *Gandy*, The Panoptic Sort, 1993, S. 15.

bb) Risiken einer virtuellen Privatsphäre

Es ist zwar vorstellbar, dass auch innerhalb virtueller Systeme eine Privatsphäre geschaffen wird, in der Menschen, wie z.B. wie innerhalb von sozialen Netzwerken, mittels privaten Kommunikationskanälen oder Anonymisierungstechniken einen freien Meinungsaustausch pflegen, sich informieren und autonome Entscheidungen treffen könnten.[1032]

Virtuell geschaffene Freiheitsräume stellen jedoch grundsätzlich keinen negativen Schutzbereich i.S.d. modernen Privatsphärenkonzepts dar. In einer virtuellen Privatsphäre muss der Freiheitsraum erst als ein Bündel an Hardware- und Softwareeinstellungen hergestellt werden.[1033] D.h., es wird positiv ein Schutzbereich, der z.B. nur auf ein erwünschtes Verhalten beschränkt werden könnte, definiert.[1034] So behalten sich z.B. Anbieter wie Google vor, die Privatnachrichten ihrer Nutzer auf etwaige Rechtsverstöße zu überprüfen.[1035] Folglich birgt diese Art der Privatsphäre die Gefahr, nicht nur technisch, sondern auch im Hinblick auf ihre Schutzwirkung lediglich virtuell zu sein.[1036] Dementsprechend wird das Konzept einer technisch hergestellten Privatsphäre als deren „Simulacrum", d.h. eine Simulation der Privatsphäre, die lediglich das Gefühl der Freiheit vermittelt, kritisiert.[1037] Eine virtuelle Privatsphäre kann vor allem nach moralischen Vorstellungen derjenigen, die das ihr zugrunde liegende

---

[1032] Vgl. *Hotter*, Privatsphäre, 2011, S. 148.

[1033] Vgl. Ebenda, 121 ff.

[1034] *Bogard*, The Simulation of Surveillance, 1996, S. 126 ff.; *Lyon*, Surveillance Studies, 2007, S. 176.

[1035] Google scannt die E-Mails der Nutzer seines Dienstes "Google Mail", um sie zum einen für Werbezwecke auszuwerten oder nach verbotenen Inhalten wie Abbildungen missbrauchter Kinder zu durchsuchen, was im konkreten Fall moralische befürwortet werden kann, aber generell (neben fernmeldeschutzrechtlichen Bedenken) ein Gefährdungspotential mit sich trägt, wenn z.B. Scankriterien zu Lasten der Persönlichkeitsrechte geändert werden sollten, Debatte um Festnahme in den USA, Spiegel Online, http://www.spiegel.de/netzwelt/web/gmail-google-rechtfertigt-scan-von-e-mails-nach-kinderpornografie-a-984577.html (4.7.2015); *Hern*, Google stops scanning student emails after California lawsuit, the Guardian, http://www.theguardian.com/technology/2014/may/01/google-stops-scanning-student-emails-california-lawsuit (4.7.2015).

[1036] Castells spricht von Menschen als "Gefangenen der Netzwerkarchitektur", *Castells*, The Internet Galaxy, 2005, S. 184 ff.

[1037] Zum Begriff des virtuellen "Simulacrums" als Ausdruck der postmodernen Welt, S. *Baudrillard*, In the Shadow of the Silent Majorities, 2007, S. 121; *Webster*, Theories of the Information Society, 2014, S. 334; "Der virtuelle Raum ist keine Wohnung, in der man sich sicher wähnen darf, frei und unbeobachtet", so *Heckmann*, K&R 2011, S. 770 (773); unter Verweis auf BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120, 274.

System kontrollieren, modelliert und positiv gestaltet werden.[1038] Dabei ist zu befürchten, dass Menschen diesen Systemlenkern machtlos gegenüberstehen werden, da sie ohne eine negative Privatsphäre keinen Schutzraum haben werden, um eine Opposition gegen sie aufzubauen.[1039] Die virtuelle Privatsphäre stellt daher in ihrem derzeitigen Zustand und ausgehend von absehbarer gesellschaftlicher und technologischer Entwicklung keinen gleichwertigen Ausgleich für den Wegfall der Privatsphäre im öffentlichen Raum dar.

Diese Gefahren werden von Mann in seinem Konzept der Sousveillance zwar nicht verkannt.[1040] Jedoch hält er es für ausreichend, dass Menschen in räumlichen Privatbereichen eine Privatsphäre gewährt wird.[1041] Dabei übersieht Mann jedoch die Bedeutung der Privatsphäre im öffentlichen Raum als einem Ort, der vor allem für die politische Selbstentfaltung essentiell ist.[1042] Des Weiteren würde eine solche Ansicht dazu führen, dass die Privatsphäre auf den Schutz durch Privateigentum angewiesen wäre, was insbesondere sozial schwächer gestellte Personen benachteiligen würde.[1043]

cc) Keine Rechtfertigung durch Transparenzeffekte

Es kann an dieser Stelle dahingestellt bleiben, ob und in welchem Umfang die Utopie einer Transparenz-, als auch die Dystopie einer Kontrollgesellschaft zutreffend sind.[1044] In jedem Fall stehen sich die Utopie und die Dystopie mit zumindest gleicher Wahrscheinlichkeit gegenüber und daher heben sie sich in ihrer Bedeutung für diese Untersuchung auf. D.h., die erwarteten Vorteile der Sousveillance und einer transparenten Gesellschaft vermögen es nicht, die von Smartglasses für die Privatsphäre ausgehenden Nachteile aufzuwiegen.

1038 Vgl. D II. 3, S. 82; vgl. *Ericson/Haggerty*, The New Politics of Surveillance and Visibility, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 3 (29).

1039 Vgl. *Sofsky*, Verteidigung des Privaten, 2007, S. 18, 27 ff.

1040 Mann hält die Privatsphäre "wie wir sie kennen", generell für verloren, *Mann/Niedzviecki*, Cyborg, 2002, S. 146.

1041 Proposed law on sousveillance (MANN-WASSELL LAW), Verillance.me, http://veillance.me/blog/2012/11/20/proposed-law-on-sousveillance (23.6.2015).

1042 Vgl. BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 37.

1043 *Hotter*, Privatsphäre, 2011, S. 21 ff.

1044 Es werden auch Ansichten vertreten, die einen Anstieg der sozialen Verbundenheit und kollaborativer Wirtschaft erwarten, *Land/Kreutzer*, Dematerialisierung - Die Neuverteilung der Welt in Zeiten des digitalen Darwinismus, 2015, S. 124 ff.; *Mason*, The end of capitalism has begun, The Guardian, http://www.theguardian.com/books/2015/jul/17/postcapitalism-end-of-capitalism-begun (1.9.2015).

3. Keine Rechtfertigung der Eingriffe in das Allgemeine Persönlichkeitsrecht

Die Abwägung der sich gegenüberstehenden Interessen der Nutzer von Smartglasses mit den individuellen und gesamtgesellschaftlichen Interessen am Schutz der Privatsphäre fällt eindeutig aus. Es erscheint möglich, dass Smartglasses sich mit ihrer Zulassung ähnlich wie Smartphones verbreiten werden. Von Smartphones unterscheiden sich Smartglasses jedoch dadurch, dass sie anlasslos und im großen Umfang eine hohe Quantität an vielfach sensiblen Informationen erfassen können. Für die Betroffenen bleibt dabei intransparent, ob und in welchem Umfang Aufnahmen oder sonstige Daten erstellt werden, was dazu führt, dass sie jederzeit mit ihnen rechnen müssen. Hinzu kommt, dass mit der Verbreitung von Smartglasses ein Paradigmenwechsel auch im Hinblick auf die Verbreitung anderer Überwachungstechnologien und damit eine synoptische Überwachung sowie Kontrolle zu befürchten ist.

Eine synoptische Kontrollgesellschaft schafft jedoch nicht automatisch die Nachteile der panoptischen Überwachung ab.[1045] Beide Beobachtungssysteme können vielmehr miteinander interagieren, wodurch zwar eine synoptische Überwachung stattfindet, sie jedoch einer zentralen beobachtenden Stelle dienlich sein kann.[1046] In einer entsprechenden Abwandlung der Dystopie von George Orwell wäre daher weniger der Verlust der Privatsphäre aufgrund der Beobachtung durch einen „Big Brother" alleine, sondern vielmehr durch dessen Zusammenwirken mit vielen „little Brothers" zu befürchten.[1047]

Dieser Gefahr stehen Bequemlichkeits- und Effizienzinteressen der Nutzer von Smartglasses entgegen, die für sich gesehen durchaus ein relevantes Interesse an der Nutzung der Geräte begründen können. In der

---

[1045] Vgl. *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (46 f.); es könnte zudem sein, dass die Beobachtungsmöglichkeiten reiner Neugier dienen und nicht zur Förderung einer politischen Meinung führen werden, *Schaefer/Steinmetz*, Surveillance & Society 2014, Vol. 12, Nr. 4, p. 502 (505 ff.).

[1046] Ein Zusammenspiel zwischen synoptischer und panoptischer Überwachung hat sich seit dem 19ten Jahrhundert etabliert und trat z.B. im Form einer Gesellschaftskontrolle mit Hilfe von Spitzeln, wie in der DDR auf, vgl. *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (41); ähnliches (wenn auch die Folgen nicht vergleichbar sind) ist z.B. im Web 2.0 zu beobachten, in dem Nutzer einander beobachten und dadurch zugleich wirtschaftlich verwertbare Daten an die Betreiber sozialer Plattformen liefern, Ebenda; *Schaefer/Steinmetz*, Surveillance & Society 2014, Vol. 12, Nr. 4, p. 502 (512).

[1047] *Hotter*, Privatsphäre, 2011, S. 101; den Vorwurf einer dezentralen Überwachung stellt Mann bereits gegenüber traditionellen Überwachungskameras auf, *Mann/Niedzviecki*, Cyborg, 2002, S. 164.

Relation zu der von ihnen ausgehenden Gefahr für die Privatsphäre sind diese Interessen jedoch als geringer zu bewerten und können allenfalls bei medizinisch indizierter Nutzung sowie in extremen Gefahrensituationen ein höherwertiges Interesse an der Nutzung von Smartglasses begründen.

V. Unvereinbarkeit der Nutzung von Smartglasses mit der Menschenwürde

Nach dem bisherigen Ergebnis der verfassungsrechtlichen Prüfung von Smartglasses ist durch deren Einsatz im öffentlichen Raum die Verletzung des Allgemeinen Persönlichkeitsrechts Dritter als Regelfall zu erwarten. Es liegt also nahe, zu prüfen, ob nicht zugleich die Verletzung ihrer Menschenwürde zu befürchten ist. Das wäre der Fall, wenn durch die Beeinträchtigung der Privatsphäre mittels Smartglasses die Subjektsqualität der Menschen als autonome und mündige Individuen missachtet und generell in Frage gestellt würde.[1048]

Für eine derart intensive Beeinträchtigung der Betroffenen spricht, dass die zulasten von Smartglasses ausfallende Interessenabwägung nicht nur auf dem Umstand tatsächlicher und kontrollierbarer audiovisueller Aufnahmen oder sonstiger Datenerhebungen beruht. Mindestens ebenso relevant ist die Furcht der Betroffenen, dass sie jederzeit Opfer dieser Maßnahmen sein können. Zwar ist es möglich, dass bei ihnen Gewohnheitseffekte eintreten werden, jedoch ist zugleich zu befürchten, dass diese ein Ausdruck der Selbstaufgabe und Fügung in die Konformitätserwartungen der übrigen Gesellschaftsteilnehmer sein werden. Dabei kann auch die Idee der Sousveillance bzw. einer transparenten Gesellschaft keine überzeugende Rechtfertigung für den Verlust der Privatsphäre liefern. Ganz im Gegenteil birgt sie die Gefahr einer inhumanen Kontrollgesellschaft, in der Autonomie vernichtet und eine Gleichschaltung gefördert wird, in sich.[1049] Es ist eine als „flächendeckend", „lückenlos" oder „total" bezeichnete Überwachung im öffentlichen Raum zu befürchten, die mit biometrischer Identifizierung und der Erstellung lückenloser Persönlichkeits- und Bewegungsprofile einhergehen kann.[1050] Als Folge wäre

---

[1048] Vgl. E II. 1, S. 91.

[1049] *Han*, Transparenzgesellschaft, 2012, S. 77 f.

[1050] Vgl. BVerfG, Urt. v. 2.3.2010 (1 BvR 256/08, 1 BvR 263/08 u. 1 BvR 586/08), BVerfGE 125, 260 (324); BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (43); BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 33; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 410; *Schmidl*, in: *Hauschka*, Corporate Compliance, § 29 Rn. 302; *Weichert*, ZD 2012, S. 501 (503).

damit zu rechnen, dass Menschen eine selbstbestimmte Entfaltung ihrer Persönlichkeit im öffentlichen Raum praktisch unmöglich gemacht werden würde und damit ihre Qualität als entsprechend den freiheitlich-demokratischen Grundsätzen mündige Subjekte in Frage gestellt wäre.[1051]

Als Ergebnis der verfassungsrechtlichen Prüfung ist daher festzustellen, dass als Folge der Nutzung von Smartglasses im öffentlichen Raum Verletzungen der Menschenwürde Dritter im großen Umfang zu befürchten sind.

[1051] Vgl. E II. 1, S. 91; von der schwindenden Privatsphäre im öffentlichen Raum werden insbesondere sozial schwächer gestellte Personen betroffen, die nicht über einen Schutz des Eigentums als Ausgleich des Privatsphärenverlusts verfügen, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 109.

F EINFACHGESETZLICHE PRÜFUNG DER NUTZUNG VON SMARTGLASSES

Nach der verfassungsrechtlichen Untersuchung wird die Nutzung von Smartglasses im öffentlichen Raum auf einfachgesetzlicher Ebene geprüft. Die einfachgesetzliche Prüfung wird sowohl die zivilrechtlichen als auch die strafrechtlichen Vorschriften zum Schutz der Privatsphäre umfassen. Da diese Untersuchung sich ganz besonders der Auswirkung von Smartglasses auf zwischenmenschlicher Ebene widmet, wird sie ebenfalls die Möglichkeiten der Einwilligung in deren Nutzung als auch der Notwehr durch Betroffene berücksichtigen.

Die einfachgesetzliche Prüfung wird maßgeblich durch das verfassungsrechtliche Ergebnis geprägt, wonach die Nutzung von Smartglasses im öffentlichen Raum i.d.R. mit der Menschenwürde unvereinbar ist. Nur in extremen Gefahrensituationen oder bei medizinisch indizierter Nutzung muss das Privatsphäreninteresse der Betroffenen zurücktreten. Aufgrund dieser hohen Eingriffsintensität von Smartglasses stellt sich die Frage, ob nicht bereits der Besitz oder zumindest das Führen von Smartglasses im öffentlichen Raum untersagt sein könnte.

I. Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen gem. § 90 TKG

Der Besitz von Smartglasses könnte bereits als ein Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen gem. § 90 TKG verboten sein. Diese Vorschrift wurde als Reaktion auf die Miniaturisierung der Aufnahme- und Sendetechnik sowie das Aufkommen sog. „Minispione", d.h. sendefähiger Minikameras, geschaffen.[1052] Derartige Geräte machen es den Betroffenen schwer, etwaige Rechtsverstöße zu entdecken und nachzuweisen, dass sie stattfanden, in welchem Umfang sie stattfanden, als auch, wer für sie verantwortlich ist.[1053] Da sich jedoch Nachweisschwierigkeiten entsprechend dem verfassungsrechtlichen Grundsatz „in dubio pro reo" des Art. 103 Abs. 2 GG zugunsten der Angeklagten auswirken, wäre ein Persönlichkeitsschutz, der erst ab dem Versuchsstadium der Persönlichkeitsrechtsverletzung eingreift, im Hinblick auf Minispione

---

[1052] § 90 TKG 2004 wurde aus der Vorgängervorschrift des § 65 TKG 1996 übernommen, BT-DrS. 15/2316, S. 88; § 65 TKG-1996 basierte wiederum auf einer entsprechenden Vorschrift des ehemaligen Fernmeldeanlagengesetz (FAG), die 1986 aufgenommen wurde, BT-DrS. 10/1618, S. 7 ff.; *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 1; *Dierlamm*, in: *Scheurle/Mayen*, TKG, § 90, Rn.2.

[1053] *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 5.

ineffektiv.[1054] Mit dem § 90 TKG kommt der Staat also seinem Auftrag zum aktiven Schutz von Persönlichkeitsrechten seiner Bürger aus Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG nach.[1055]

§ 90 TKG richtet sich gegen die Vorfeldmaßnahme der Nutzung von Minispionen und verbietet deren Herstellung, Besitz, Vertrieb, Einfuhr oder Bewerbung. Auf Rechtsfolgenseite ist der vorsätzliche Verstoß gegen § 90 TKG gem. § 148 Abs. 1 Nr. 2 TKG mit einer Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bedroht. Die Herstellung, der Vertrieb, die Einfuhr und sonstiges Verbringen, also nicht der Besitz, werden auch beim fahrlässigen Handeln mit einer Freiheitsstrafe bis zu einem Jahr oder Geldstrafe geahndet.

1. Sende- oder sonstige Telekommunikationsanlagen

Die technischen Voraussetzungen des § 90 TKG verlangen zuerst das Vorliegen einer Sende- oder sonstigen Telekommunikationsanlage. Der Begriff der Sendeanlage ist zwar gesetzlich selbst nicht definiert, kann aber aus der alten Vorschrift des § 3 Nr. 4 TKG 1996 hergeleitet werden und umfasst „elektrische Sende- oder Empfangseinrichtungen, zwischen denen die Informationsübertragung ohne Verbindungsleitungen stattfinden kann“.[1056] Dabei kommt es vor allem auf die Fähigkeit, Signale zu senden, an, sodass z.B. Geräte, die Aufnahmen nur auf einer Speicherkarte sichern können, nicht hierunter fallen.[1057] Smartglasses können aber z.B. über WLAN oder drahtlose Netze elektronische Signale senden und stellen folglich Sendeanlagen dar.[1058] Daneben erfüllten Smartglasses auch die zweite Tatbestandsalternative, da es sich bei ihnen um Telekommunikationsanlagen, also „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden“, i.S.d. weit gefassten und technikoffenen Vorschrift des § 3 Nr. 23 TKG handelt.[1059]

2. Tarnung der Anlagen

§ 90 TKG umfasst nur Telekommunikationseinrichtungen, „die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegen-

---

[1054] Ebenda.

[1055] Vgl. BT-DrS. 15/2316, S. 88; BT-DrS. 10/1618, S. 9; *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 6; vgl. *Dierlamm*, in: *Scheurle/Mayen*, TKG, § 90, Rn. 1.

[1056] *Kalf/Papsthart*, in: *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, § 65 TKG, Rn. 4.

[1057] *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 8; *Ernst*, NJW 2004, S. 1277 (1278).

[1058] Zwar werden zum Teil auch "Fotohandies" nicht als Sendeanlagen verstanden, jedoch gilt dies nur für Geräte ohne Datensendefunktionen, also nicht für Smartphones, *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 8.

[1059] Ebenda, § 90, Rn. 7.

ständen des täglichen Gebrauchs verkleidet sind." Es genügt also nicht, dass ein Gerät aufgrund der kleinen Bauweise objektiv besonders gut und unauffällig versteckt ist und nur aus diesen Gründen für heimliche Bild- oder Wortaufnahmen verwendet werden kann.[1060] Das Gerät muss vielmehr besonders getarnt sein, also in seiner Form und Funktion darauf angelegt sein, unbefugt Abbildungen von Menschen oder deren Gespräche aufzunehmen.[1061] Erst so realisiert sich die Gefahr von Minispionen, die es den Betroffenen schwermachen, etwaige Rechtsverstöße zu entdecken und nachzuweisen.[1062] Folglich sind z.B. Minimikrofone, die in einem Lampenschirm eingebaut werden, tatbestandsmäßig,[1063] aber nicht wenn sie sichtbar am Revers getragen werden.[1064] Ebenso sind Richtmikrofone oder Super-Teleobjektive selbst nicht nach § 90 TKG verboten, da es an einer Tarnung ihrer Eigenschaften mangelt.[1065] Dementsprechend stellen auch Smartphones keine Minispione dar.[1066] Smartphones verfügen zwar über eine Sendefunktion mit Datenverbindung sowie mit der Kamera und dem Mikrofon über eine Aufnahmevorrichtung. Jedoch ist der Mehrheit der Menschen bekannt, dass Smartphones Aufnahmevorrichtungen besitzen, wodurch es an einer Tarnung und erst recht an einer bewussten Tarnung zwecks Umgehung der Arglosigkeit der Betroffenen mangelt.[1067]

Im Fall von Smartglasses kommt es auf ihre konkrete Bauweise und die Verwendung an, wobei an dieser Stelle auf die auf verfassungsrechtlicher Ebene getroffenen Überlegungen zum Kriterium der Heimlichkeit verwiesen werden kann.[1068] Gegenwärtig könnten Smartglasses zwar situationsbedingt für eine Korrekturbrille gehalten werden, z.B. bei einem flüchtigen Blick einer Person, die über keine Kenntnis über die Smartglasses-Technologie verfügt. Im Regelfall werden die aktuellen Smartglasses-Modelle jedoch aufgrund von Wülsten am Geräterahmen und an ihren Bildschirmen erkennbar und damit nicht i.S.d. § 90 TKG getarnt sein. Die

---

1060 Vgl. *Kalf/Papsthart*, in: *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, § 65 TKG, Rn. 6.

1061 *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 11.

1062 "[…] eine eindeutige Errichtungshandlung ist schwer feststellbar, weil das Gerät schon beim Kauf praktisch fertiggestellt ist; ferner ist ein solches Gerät regelmäßig nur kurze Zeit in Betrieb und läßt sich schnell verstecken", BT-DrS. 10/1618, S. 9; *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 5.

1063 *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 11; Spionagekamera im Prüfungsamt, Legal Tribune Online, http://www.lto.de/recht/studium-referendariat/s/pruefungsamt-kamera-spionage-referendar/(24.4.2014).

1064 Vgl. *Kalf/Papsthart*, in: *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, § 65 TKG, Rn. 6.

1065 *Ernst*, NJW 2004, S. 1277 (1278).

1066 Ebenda.

1067 *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn.11.

1068 Vgl. E IV. 1. g) bb), S. 155.

künftige Entwicklung kann in zwei unterschiedliche Richtungen verlaufen. Zum einen ist in der Zukunft mit Geräten zu rechnen, die sich nicht von Korrekturbrillen als „Gegenständen des täglichen Gebrauchs" unterscheiden und damit für sich betrachtet i.S.d. § 90 TKG getarnt sein werden.[1069] Umgekehrt kann deren Verbreitung, ähnlich wie im Fall von Smartphones, dazu führen, dass Smartglasses in jedem Brillengestell zu vermuten sein werden, wodurch der rechtlich sanktionierte Tarneffekt entfallen wird. Ob ein Tarneffekt vorliegt, könnte jedoch dahingestellt bleiben, wenn die Smartglasses ohnehin nicht zu schlechthin schädlichen Zwecken i.S.d. § 90 TKG bestimmt wären.

3. Keine Eignung und Bestimmung zum heimlichen Abhören und Aufnehmen von Bildern

Neben der technischen Komponente setzt § 90 TKG auch eine sanktionswürdige Zweckbestimmung der Sendeanlagen voraus. Das Bestimmungsmerkmal wurde im Jahr 2011 in den Tatbestand des § 90 Abs. 1 TKG aufgenommen, um dessen Ausuferung zu vermeiden.[1070] Die Verbotswirkung der Vorschrift sollte damit entsprechend der ursprünglichen Gesetzesbegründung auf Anlagen beschränkt werden, die „von vorneherein keinem anerkennenswerten Zweck" dienen, „sondern offensichtlich nur dem heimlichen Abhören von Gesprächen bzw. dem heimlichen Anfertigen von Bildaufnahmen eines anderen dienen sollen".[1071]

Smartglasses sind nicht primär dazu bestimmt, Menschen heimlich abzuhören oder abzubilden. Vielmehr bieten sie eine Vielzahl von nützlichen Funktionen, die der Verfolgung von verfassungsrechtlich anerkannten Interessen dienen.[1072] Das heimliche Aufnehmen und Abhören ist zwar möglich, stellt jedoch keine bestimmungsgemäße Funktion von Smartglasses, sondern vielmehr deren subjektive „Umwidmung", z.B. durch einen bewussten Erwerb oder Einsatz für voyeuristische Zwecke, dar. Dadurch werden Smartglasses jedoch nicht ihrer ursprünglichen Funktionen und des Nutzens für andere als die sanktionierten Zwecke beraubt. Das gilt insbesondere, weil der Gesetzgeber mit § 90 TKG eben nicht die konkrete Nutzung, sondern die objektive Schädlichkeit von Minispionen verhindern wollte.[1073]

[1069] Vgl. E IV. 1. g) bb), S. 155.

[1070] *Bock*, in: *Geppert/Schütz*, BeckOK TKG, § 90, Rn. 12.

[1071] BT-DrS. 10/1618, S. 1.

[1072] Vgl. E III, S. 136.

[1073] Vgl. BT-DrS. 10/1618, S. 1, 9.

4. Kein Verbot gem. § 90 TKG

Im Ergebnis ist daher festzustellen, dass nicht nur die Tarnung der Smartglasses als Gegenstände des täglichen Lebens zweifelhaft ist, sondern es ihnen vor allem an einer Bestimmung zum unbefugten Abhören oder Aufnehmen von Personen fehlt. Allein die objektive Eignung hierzu führt jedoch nicht zu einem grundsätzlichen Verbot von Smartglasses gem. § 90 TKG. Es wird also zu prüfen sein, inwieweit die konkrete Nutzung von Smartglasses sanktioniert sein kann.

II. Datenschutzvorschriften

Als Verbotsvorschriften für die Nutzung von Smartglasses kommen aufgrund ihrer datenbasierten Funktionsweise zuerst die Vorschriften des BDSG in Frage.

1. Videoüberwachung gem. § 6b BDSG

Den weitesten Schutz vor Smartglasses scheint die Vorschrift des § 6b BDSG zu bieten, da sie nicht lediglich konkrete Aufnahmen untersagt, sondern die ungerechtfertigte Videoüberwachung im öffentlichen Raum an sich. Nach dem Willen des Gesetzgebers sollte mit § 6b BDSG insgesamt eine „restriktivere Verwendungspraxis“ der Videoüberwachung herbeigeführt werden, ohne jedoch dabei die Interessen der Betreiber der Videoüberwachung zu missachten.[1074] Damit könnte gem. § 6b BDSG zwar nicht der Besitz von Smartglasses, aber wegen der hohen Beeinträchtigung des Rechts auf informationelle Selbstbestimmung praktisch deren Führung, also das bestimmungsgemäße Tragen im öffentlichen Raum, untersagt sein.

a) Optisch-elektronische Einrichtung

§ 6b BDSG ist nur bei Videoüberwachung mittels optisch-elektronischer Einrichtungen einschlägig. Die Voraussetzung einer „optisch-elektronischen“ Überwachung ist im Fall von Smartglasses erfüllt, da ihre typische Funktionsweise sowohl eine visuelle Erfassung als auch die Umwandlung der Lichtimpulse in elektronische Signale zur Weiterleitung oder Speicherung umfasst.[1075] Dagegen ist es nicht eindeutig, ob es sich bei Smartglasses um eine „Einrichtung“ i.S.d. Vorschrift handelt. Zwar enthalten weder der Gesetzeswortlaut noch die Gesetzesmaterialien technische Beschränkungen im Bezug auf Größe, Funktionalität, Bedienungs-

[1074] Begründung zum Regierungsentwurf, BT-DrS. 14/5793, S. 30, 38, 61; *Gola/Schomerus*, BDSG, § 6b, Rn. 1; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 3.

[1075] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 246; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 19.

art oder Ortsgebundenheit einer solchen Einrichtung.[1076] Jedoch unterscheiden sich Smartglasses von der klassischen Videoüberwachung insbesondere dadurch, dass sie nicht ortsgebunden sind und die Videokamera ohne größere Umstände jederzeit abgedeckt oder abgeschaltet werden kann. Daher ist zu prüfen, ob Smartglasses dem Begriff der Einrichtung i.S.d. § 6b BDSG unterfallen.

aa) Anwendbarkeit bei mobilen Geräten

Aus dem Begriff einer „Einrichtung" wird zum Teil abgeleitet, dass damit zumindest eine vorübergehende örtliche Fixierung der Überwachungskamera notwendig ist.[1077] Ebenso ausgehend vom Wortlaut wird vertreten, dass § 6b BDSG die Beobachtung von öffentlichen „Räumen" und nicht eine Beobachtung von Personen regeln soll.[1078] Da Menschen ihre Aufmerksamkeit jedoch typischerweise anderen Menschen zuwenden, würden die an deren Kopf getragenen Smartglasses eher der Personenbeobachtung dienen und nicht wie eine festmontierte Kamera „in den Raum blicken".[1079] Die Beschränkung des § 6b BDSG auf ortsgebundene Videoüberwachung wird ferner mit dem Argument gestützt, dass die Pflicht, eine Videoüberwachung gem. § 6b Abs. 2 BDSG zu kennzeichnen, bei mobilen Geräten faktisch kaum erfüllbar wäre.[1080]

Diese Ansichten überzeugen jedoch nicht. Zum einen umfasst die sprachliche Bedeutung einer Einrichtung „technische Vorrichtungen" aller Art, wobei mit der Begriffsteil „Richtung" weniger die Ortsgebundenheit, als dass „etwas für einen bestimmten Zweck, für eine bestimmte Funktion" hergestellt ist, zum Ausdruck gebracht wird.[1081] Ebenso bedeutet die Beschränkung des Regelungsbereiches auf den „öffentlichen Raum" nicht zwangsläufig, dass die Beobachtung von Personen im öffentlichen Raum ausgenommen sein soll.[1082] In vielen Fällen dienen die Überwachungskameras sogar gerade dazu, bestimmte Personen zu beobachten, die innerhalb eines Raums einen Schaden anrichten könnten.[1083] Würde zudem die Möglichkeit der Fixierung auf bestimmte Personen als Ausschlusskriteri-

---

[1076] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 244; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 36.

[1077] *Duhr u.a.*, DuD 2002, S. 1 (27).

[1078] AG Nürnberg, Urt. v. 8.5.2015 (18 C 8938/14), BeckRS 2015, 14846; vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 245.

[1079] *Schwenke*, K&R 2013, S. 685 (690).

[1080] AG Nienburg, Urt. v. 20.1.2015 (4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14)), BeckRS 2015, 07708.

[1081] Duden, 2013, Stichworte „Einrichtung" u. „Vorrichtung".

[1082] Vgl. *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 63.

[1083] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 245.

um für die Anwendbarkeit des § 6b BDSG dienen, müssten auch Videokameras mit Schwenk-, Neige- und Vergrößerungsfunktion aus dem Anwendungsbereich ausscheiden.[1084] Dass auch der Hinweis auf eine angeblich nicht umsetzbare Kennzeichnung mobiler Videoüberwachung nicht haltbar ist, zeigt das Beispiel von Polizeibeamten, die beim Einsatz von Bodycams Schutzwesten mit der Aufschrift „Videoüberwachung" tragen.[1085]

Des Weiteren muss bedacht werden, dass die Typisierung von Geräten als mobil oder immobil heutzutage kaum praktisch umsetzbar ist, da die heutigen Überwachungskameras klein, flexibel platzier- und mobil betreibbar sind.[1086] Abgrenzungen zwischen mobiler und immobiler Videoüberwachung wären so zwangsläufig kaum anhand objektiver Kriterien zu treffen und damit willkürlich. Z.B. ist eine in einem Kraftfahrzeug eingesetzte Dashcam für sich ein mobiles Gerät, das jedoch fest in einem Fahrzeug eingerichtet wird und der Beobachtung Dritter sowohl während dessen Mobilität als auch Immobilität des Fahrzeugs, z.B. wenn es auf einem Parkplatz über Nacht steht, dienen kann.[1087] Letztendlich würde es dem Zweck der umfassenden Regelung der Videoüberwachung mit § 6b BDSG widersprechen, wenn dessen Regelungsbereich durch eine lediglich vorübergehende statt dauerhafte Aufstellung von Kameras umgangen werden könnte.[1088] Auch der Schutz des Rechts auf informationelle Selbstbestimmung rechtfertigt die Einbeziehung mobiler Überwachung, da von ihr keine geringere Eingriffsintensität als von ortsgebundener Videoüberwachung zu erwarten ist.[1089] Ganz im Gegenteil können Nutzer mobiler Geräte spontan, kosten- und technisch umstandslos Videoauf-

---

[1084] *Hilpert*, RDV 2009, S. 160 (162); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 245; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 20.

[1085] Innenminister Boris Rhein: „Body-Cam" verhindert Gewalt gegen Polizeibeamte, Hessisches Ministerium des Innern und für Sport, https://innen.hessen.de/presse/pressemitteilung/innenminister-boris-rhein-body-cam-verhindert-gewalt-gegen-polizeibeamte (5.7.2014).

[1086] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 247 f.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, Gutachten für das Bundesministerium des Innern, 2001, S. 184 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 39.

[1087] Im Ergebnis §6b BDSG bei Dashcams annehmend, VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (237); ebenso *Gola/Schomerus*, BDSG, § 6b, Rn. 7b; a.A. AG Nürnberg, Urt. v. 8.5.2015 (18 C 8938/14), BeckRS 2015, 14846.

[1088] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 37.

[1089] *Brink*, in: *Wolff/Brink*, BeckOK BDSG, § 6b, Rn. 25; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 245; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 37, 39; *Solmecke/Nowak*, MMR 2014, S. 431 (433); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 19.

nahmen von jedem Ort ins Internet übertragen.[1090] Zusammenfassend stellen Smartglasses daher optisch-elektronische „Einrichtungen" i.S.d. § 6b Abs. 1 BDSG dar.

bb) Abgedeckte oder ausgeschaltete Kamera

Zur Minderung der von Smartglasses ausgehenden Gefahr einer heimlichen Erfassung werden mechanische Abdeckungen vorgeschlagen, die über der Kamera platziert werden (z.B. als „mechanical Blinds", also mechanische Fensterläden, bezeichnete Objektivabdeckungen und –kappen).[1091] Da derartig präparierte Smartglasses keine visuellen Informationen erfassen können, könnte auch deren Eigenschaft als eine optisch-elektronische Einrichtung entfallen. In diesem Fall würden Smartglasses allenfalls eine Abschreckungsfunktion, ähnlich wie Videokameraattrappen, entfalten.[1092] Attrappen sind jedoch nicht zu einer optisch-elektronischen Beobachtung fähig, sondern können nur durch eine psychologische Wirkung die persönliche Entfaltung der betroffenen Person beeinträchtigen.[1093] Diese Beeinträchtigung kann insbesondere auf zivilrechtlicher Ebene zur Verletzung des Allgemeinen Persönlichkeitsrechts führen.[1094] Sie führt jedoch nicht zu einer Videobeobachtung gem. § 6b BDSG.[1095]

Jedoch handelt es sich bei derartigen Abdeckungen der Kamera nur um temporäre Lösungen, bei denen die Smartglasses generell weiterhin zur

---

[1090] *Breithut*, Meerkat versus Periscope, Spiegel Online, http://www.spiegel.de/netzwelt/apps/meerkat-versus-periscope-livestreaming-apps-im-vergleich-a-1025738.html (2.7.2015); *Copperstein*, Periscope And Meerkat Up The Ante On User-Generated Content And Why That's A Good Thing, Forbes, http://www.forbes.com/sites/davidcooperstein/2015/05/06/periscope-and-meerkat-why-thats-a-good-thing/(2.7.2015); *Fuchs*, ZD 2015, S. 212; *Kwok*, Periscope und Meerkat sind eine Gefahr für unsere Privatsphäre, AndroidPIT, https://www.androidpit.de/periscope-meerkat-gefahr-fuer-die-privatsphaere (2.7.2015).

[1091] Vgl. *Bergfink*, DuD 2015, S. 145; *Hansen*, DuD 2015, S. 435 (437); *Schröder*, GlassKap, #WWSW, http://www.wewearsmartwear.de/2013/07/glasskap-accessoires-fur-google-glass-aus-dem-3d-drucker/(4.7.2015); *Schwenke*, K&R 2013, S. 685 (691).

[1092] LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1067 f.); AG Dinslaken, Urt. v. 5.3.2015 (34 C 47/14), ZD 2015, 531 (532); AG Frankfurt a.M., Urt. v. 14.1.2015 (33 C 3407/14 (93)), ZD 215, 280 (280 f.); AG Aachen, Urt. v. 11.11.2003 (10 C 386/03), NZM 2004, 339 (339 f.); BAG, Urt. v. 15.5.1991 (5 AZR 115/90), BAGE 68, 52 (56); *Fuchs*, ZD 2015, S. 212 (213); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 41.

[1093] *Gola/Schomerus*, BDSG, § 6b, Rn. 7; *Hilpert*, RDV 2009, S. 160 (162); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 41; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 19.

[1094] *Gola/Schomerus*, BDSG, § 6b, Rn. 7.

[1095] *Lang/Lachenmann*, NZA 2015, S. 591 (593); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 41; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 20.

Videoerfassung fähig bleiben.[1096] Mechanische Kappen oder Deckel können jederzeit abgenommen werden und sind damit praktisch mit einer Ein-/Aus-Funktion der Geräte vergleichbar. Würde man jedoch abgeschaltete Videokameras aus dem Tatbestand des § 6b BDSG herausnehmen, würde dies dazu führen, dass das Gesetz seine Schutzwirkung nicht entfalten könnte.[1097] Denn es wäre durch Betroffene oder Aufsichtsbehörden praktisch nicht erkennbar, ob gerade eine Videoüberwachung stattfindet. Daher reicht für das Vorliegen einer optisch-elektronischen Einrichtung aus, dass eine Kamera ohne erkennbare Maßnahmen zur Videoüberwachung potenziell eingesetzt werden kann.[1098] Die Fähigkeit zur Videoüberwachung und damit die Anwendbarkeit des § 6b BDSG entfällt daher erst dann, wenn es sich bei der Kamera um eine bloße Attrappe handelt, die über gar keine technischen Fähigkeiten zur Beobachtung oder Aufzeichnung verfügt.[1099]

Folglich stellen Smartglasses auch dann eine optisch-elektronische Einrichtung i.S.d. § 6b BDSG dar, wenn ihre Kamera vorübergehend abgedeckt oder abgeschaltet ist. Die Einschränkungen der Kamerafunktionen können daher allenfalls bei der Frage der Eingriffsintensität der Geräte im Rahmen einer Interessenabwägung zugunsten der Nutzer von Smartglasses berücksichtigt werden.

b) Einsatz im öffentlichen Raum

§ 6b BDSG regelt nur die Videoüberwachung im öffentlichen Raum, zu dessen Definition auf die Einleitung zu dieser Untersuchung verwiesen wird.[1100] Ein öffentlicher Raum ist demnach weit als ein räumlich-physischer Bereich zu verstehen, zu dem jedermann oder ein nur nach allgemeinen Merkmalen bestimmter Personenkreis Zugang hat.[1101] Daher gehören Parkplätze, Tankstellen, Haltestellen, Fußgängerzonen, öffentliche Straßen, Wege und Plätze, Bibliotheken, Bahnhöfe, öffentliche Verkehrsmittel, Schwimmbäder, Fußballstadien, Veranstaltungshallen, La-

---

[1096] Vgl. LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1068); AG Dinslaken, Urt. v. 5.3.2015 (34 C 47/14), ZD 2015, 531 (532).

[1097] OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827 (182); LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327 (328).

[1098] OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827 (182); LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327 (328); AG Dinslaken, Urt. v. 5.3.2015 (34 C 47/14), ZD 2015, 531 (532).

[1099] *Gola/Schomerus*, BDSG, § 6b, Rn. 7; *Hilpert*, RDV 2009, S. 160 (162); *Lang/Lachenmann*, NZA 2015, S. 591 (593); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 41; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 19 f.

[1100] Vgl. A IV. 9, S. 18.

[1101] Vgl. A IV. 9, S. 18.

dengalerien oder der Publikumsbereich von Geschäften zu öffentlichen Räumen.[1102] Nicht zum öffentlichen Raum gehören dagegen Wohnungen, Hausflure, Wohnanlagen, Vorgärten, Büros, Firmengelände, Werkhallen und sonstige nicht für den Publikumsverkehr vorgesehene Bereiche.[1103] Zu beachten ist jedoch, dass die Beobachtung des öffentlichen Raums auch vom nicht öffentlichen Raum aus erfolgen kann, z.B. vom eigenen Grundstück aus.[1104]

c) Begrenzung des Anwendungsbereichs im § 1 Abs. 2 Nr. 3 BDSG

Die Vorschriften des BDSG sind grundsätzlich auch für nicht öffentliche Stellen, zu denen ebenfalls Privatpersonen gehören, anwendbar.[1105] Dies gilt gem. § 1 Abs. 2 Nr. 3 BDSG aber nur, wenn die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien erfolgt. Die Anwendung des BDSG wird wiederum ausgeschlossen, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt (engl. „household exemption“).

Da § 6b BDSG nachträglich in das Gesetz eingefügt wurde und eine Ausnahmestellung neben der bisherigen Gesetzessystematik einnimmt, muss jedoch zuerst geprüft werden, inwieweit die Regelungen zur Videoüberwachung von den Voraussetzungen des § 1 Abs. 2 Nr. 3 BDSG abhängig sind.[1106]

aa) Datenverarbeitungsanlage und Datenbezug

Der Streit, ob die Videoüberwachung unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien erfolgen muss, wurde vor allem vor dem Hintergrund analoger Überwachungskameras geführt.[1107] Im Fall von Smartglasses hat diese Streitfrage jedoch keine Relevanz, da Smartglasses ohnehin Datenverarbeitungsanlagen

---

[1102] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 242.

[1103] OVG Lüneburg, Urt. v. 29.9.2014 (11 LC 114/13), NJW 2015, 502 (505); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 242.

[1104] BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955; OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827 (182).

[1105] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 34; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 14.

[1106] *Duhr u.a.*, DuD 2002, S. 1 (27); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 250 ff.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 52 ff.

[1107] Zur Diskussion, vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 252 ff.; ablehnend, *Lachenmann/Schwiering*, NZV 2014, S. 291 (292); m.w.N., *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 52 f.

darstellen oder zumindest Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben.[1108]

Eine Datenverarbeitungsanlage i.S.d. §§ 1 Abs. 2 Nr. 3, 3 Abs. 2 Satz 1 BDSG ist eine Maschine, die Daten automatisiert handhabt, sie also nicht lediglich transportiert oder kopiert, sondern nach ihrem Informationsgehalt unterscheiden und daher unterschiedlich behandeln kann.[1109] Zwar ist das bloße Aufzeichnen von Informationen, z.B. von Bildaufnahmen, noch keine automatisierte Datenverarbeitung, da es nicht auf Grundlage eines automatisierten Verarbeitungssystems erfolgt, das „zwischen den Daten verschiedener Personen unterscheiden und darauf aufbauend die Verarbeitung steuern kann."[1110] Smartglasses im Sinne dieser Untersuchung sind mehr als bloße Kameras, sondern darauf ausgelegt, die erfassten audiovisuellen Informationen sowie weitere Daten einer informatorischen Auswertung zuzuführen.[1111] Insbesondere dienen die Funktionen zur Objekterkennung für Zwecke der Augmented Reality einer Unterscheidung von visuellen Informationen nach ihrem Informationsgehalt.[1112]

Aber auch dann, wenn man Smartglasses nicht als Datenverarbeitungsanlagen betrachtet sollte, würden sie der Erzeugung von nicht automatisierten Dateien i.S.v. § 1 Abs. 2 Nr. 3 i.V.m. § 3 Abs. 2 Satz 2 BDSG dienen. Bei nicht automatisierten Dateien handelt es sich um eine Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten personenbezogenen Merkmalen zugänglich ist und ausgewertet werden kann.[1113] Diese Definition umfasst die von Smartglasses erzeugten Aufnahmen, die in einem gleichen Format gespeichert werden sowie inhaltlich indizierbar, sortierbar und z.B. mittels Bildalgorithmen personenbezogen auswertbar sind.[1114] Ferner können die Dateien mit zusätzlichen Daten, insbesondere den Standortdaten sowie dem Aufnahmezeitpunkt, versehen werden.[1115] Da die Aufnahmen entweder der Speicherung, Übermittlung oder sonstiger Verarbeitung oder Nutzung zugeführt

---

1108 Vgl. VG Schwerin, Beschl. v. 18.6.2015 (6 B 1637/15 SN), ZD 2015, 448 (449).

1109 *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 79.

1110 VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (236); *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 79.

1111 Vgl. BII., S. 26.

1112 Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 212 ff.

1113 Vgl. VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (236); *Buchner*, in: *Taeger/Gabel*, BDSG, § 3, Rn. 23; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 86 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 215 ff.

1114 Vgl. zur Bildauswertung BIII.4.b), S. 42.

1115 Vgl. VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (236).

werden sollen, werden sie auch für diese Zwecke gem. § 1 Abs. 2 Nr. 3 BDSG erhoben.

bb) Personenbezug von Daten

Bei der Nutzung von Smartglasses ist entsprechend der verfassungsrechtlichen Prüfung im Regelfall von einer Erhebung personenbezogener Daten i.S.d. § 3 Abs. 1 BDSG auszugehen.[1116] Es werden zwar nicht alle von ihnen erfassten Daten, z.B. Sachen ohne Beziehung zu Menschen, personenbezogen sein.[1117] Jedoch kommt es auf den Personenbezug im Rahmen des gesamten zu würdigenden Videoüberwachungsvorgangs an, also dass anhand der erfassten Daten überhaupt eine Person identifiziert werden kann.[1118] Da Smartglasses in räumlicher Nähe zu Menschen getragen werden, ist daher regelmäßig mit der Erfassung von personenbezogenen Daten zu rechnen.[1119]

cc) Nutzung von Smartglasses für ausschließlich persönliche oder familiäre Tätigkeiten

Gegenstand dieser Untersuchung ist der Einsatz von Smartglasses durch Privatpersonen, weshalb dem Ausschlusskriterium einer ausschließlich persönlichen und familiären Nutzung gem. § 1 Abs. 2 Nr. 3 BDSG eine besonders hohe Bedeutung zukommt.

(1) Anwendbarkeit im Fall der Videoüberwachung

Die Ausnahme einer ausschließlich persönlichen und familiären Nutzung im Fall der Videoüberwachung wird zum Teil mit Hinweis auf den Ausnahmecharakter des § 6b BDSG verneint.[1120] Zwar findet sich in der Gesetzesbegründung kein Ausschluss der Ausnahme für persönliche und familiäre Videoüberwachung.[1121] Jedoch wird darauf verwiesen, dass § 6b BDSG außerhalb der übrigen Anwendungssystematik des BDSG steht und seine Anwendbarkeit daher abschließend selbst regelt.[1122] Auf teleologischer Ebene wird diese Ansicht damit gestützt, dass die Videobeobach-

---

[1116] Vgl. E II. 2. a) aa) (1), S. 98.

[1117] Vgl. E II. 2. a) aa) (1) (b), S. 101.

[1118] OVG Lüneburg, Urt. v. 29.9.2014 (11 LC 114/13), NJW 2015, 502 (503); *Fuchs*, ZD 2015, S. 212 (213).

[1119] Da die Nutzer von Smartglasses sich zudem im Regelfall im Gehtempo bewegen werden, kann auf sie auch nicht die (zweifelhafte) Ansicht des AG Nürnberg zu Dashcams übertragen werden, wonach die Erfassung der Passanten während der Autofahrt eine anonyme "technikbedingte Miterfassung ohne Erkenntnisgewinn" darstellt, AG Nürnberg, Urt. v. 8.5.2015 (18 C 8938/14), BeckRS 2015, 14846.

[1120] *Duhr u.a.*, DuD 2002, S. 1 (27).

[1121] *Gola/Klug*, RDV 2004, S. 65 (67); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 256; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 54.

[1122] *Duhr u.a.*, DuD 2002, S. 1 (27).

tung sich wesentlich von einer menschlichen Beobachtung unterscheidet und ihr die Privilegierung persönlicher und familiärer Nutzung nicht zuteilwerden sollte.[1123]

Diese Ansicht muss jedoch vor dem Hintergrund des gegenwärtigen technologischen Entwicklungsstandes angezweifelt werden. Zum einen würde eine Reduktion der persönlichen und familiären Nutzung auf „menschlichen" Datenumgang den Anwendungsbereich der Vorschrift praktisch aushöhlen, da heutzutage bereits Vorgänge wie die E-Mail-Kommunikation von ihrer Reichweite, Geschwindigkeit und Möglichkeit, z.B. durch Massenmailings Rechte Dritter zu verletzen, sich wesentlich von rein menschlicher Kommunikation unterscheiden.[1124] Das bedeutet jedoch nicht, dass die technologische Entwicklung im persönlichen und familiären Bereich gar nicht zur Anwendung gelangen soll. Vielmehr ist sie im Rahmen der Voraussetzungen einer persönlichen und familiären Tätigkeit zu prüfen.[1125] Diese Meinung vertritt auch der EuGH, der im Fall privater Videoüberwachung, zumindest dann, wenn sie dem Schutz des Eigentums, der Gesundheit und des Lebens dient, die Anwendbarkeit einer ausschließlich persönlichen und familiären Nutzung prüft.[1126] Die Anwendbarkeit des § 6b BDSG könnte daher bei ausschließlich persönlicher oder familiärer Nutzung von Smartglasses ausgeschlossen sein.

(2) Ausschließlich persönliche und familiäre Tätigkeit

Bei der folgenden Prüfung der Kriterien einer persönlichen und familiären Tätigkeit ist vor allem zu berücksichtigen, dass der Zweck dieser Ausnahme nicht darin liegt, den Datenumgang durch Privatpersonen generell aus dem Regelungsbereich des BDSG auszunehmen.[1127] Die Ausnahme soll vielmehr die Ausuferungen des weit gefassten Schutzbereichs des BDSG verhindern.[1128] Daher wird bereits aufgrund der generellen Eingriffsintensität von Datenverarbeitungsmaßnahmen der Anwendungsausschluss streng restriktiv ausgelegt, wofür auch der Wortlaut einer „aus-

---

[1123] Ebenda.

[1124] Vgl. Art. 29-Datenschutzgruppe, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, 2013, S. 1 f.

[1125] Vgl. Ebenda; s. die Beispiele in *Dammann*, in: *Simitis*, BDSG, § 1, Rn. 151.

[1126] Auch wenn der persönliche und familiäre Charakter im Regelfall verneint wird, EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196).

[1127] *Dammann*, in: *Simitis*, BDSG, § 1, Rn. 147 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 257.

[1128] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 257.

schließlich“ persönlichen und familiären Tätigkeit sowie der Ausnahmecharakter dieses Kriteriums des § 1 Abs. 2 Nr. 3 BDSG spricht.[1129]

(a) Kriterien einer persönlichen und familiären Tätigkeit

Der Anwendungsausschluss für persönliche und familiäre Tätigkeiten findet seine Grundlage in der EG-DSRL.[1130] Dementsprechend ist er wie die Richtlinie auf Grundlage einer Lebenswirklichkeit Anfang der 1990er Jahre geschaffen worden, in der die Richtlinienverfasser als persönliche und familiäre Nutzung beispielhaft den persönlichen Schriftverkehr oder das Führen von Anschriftenverzeichnissen nannten.[1131] Diese Beispiele sind jedoch mit den gegenwärtigen technologischen Möglichkeiten des Datenumgangs durch Privatpersonen nicht zu vergleichen, was auch die Art. 29-Datenschutzgruppe feststellte.[1132] Das unabhängige Beratungsgremium der Europäischen Kommission befand, dass die gegenwärtigen digitalen Publikations- und Kollaborationsfähigkeiten der Privatpersonen nicht mehr der zugrunde gelegten Lebenswirklichkeit des Richtliniengesetzgebers entsprechen und daher neuer Beurteilungskriterien bedürfen.[1133]

Die Art. 29-Datenschutzgruppe wies jedoch zugleich darauf hin, dass die geänderten Umstände nicht per se dazu führen, dass die Ausnahme des persönlichen und familiären Datenumgangs daher im virtuellen Raum gar nicht mehr zur Anwendung kommt.[1134] Vielmehr brächten die neuen Entwicklungen zugleich Vorteile für die persönliche Entfaltung der Einzelnen, Meinungsfreiheit, sozialen und kulturellen Austausch mit sich.[1135] Die Beurteilung, ob eine Tätigkeit persönlich und familiär ist, müsse daher alle relevanten Vorteile und Nachteile der Datenverarbeitung bedenken.[1136] Ferner müsse berücksichtigt werden, dass die Einbeziehung jeglicher Handlungen von Privatpersonen in den Regelungsbereich der Datenschutzvorschriften zum einen die Datenschutzbehörden überfor-

---

[1129] EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196); *Dammann*, in: *Simitis*, BDSG, § 1, Rn. 148; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 257; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 55.

[1130] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[1131] Richtlinie 95/46/EG, 24.10.1995 S. Erwägungsgrund 12.

[1132] Art. 29-Datenschutzgruppe, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, 2013, S. 3 ff.

[1133] Ebenda, 1 f.

[1134] Ebenda, 9.

[1135] Ebenda, 2.

[1136] Ebenda.

dern würde.[1137] Des Weiteren sehen Datenschutzgesetze umfangreiche Offenlegungs- und behördliche Prüfungsmöglichkeiten vor, die wiederum die Privatsphäre der Privatpersonen gefährden würde, wenn diese Informationsflüsse aus ihrem Alltag offenlegen müssten.[1138]

Aus diesen Gründen schlägt die Art. 29-Datenschutzgruppe eine „sanfte" Herangehensweise vor, welche die Belange aller Beteiligten berücksichtigt.[1139] In diesem Zusammenhang zieht das Beratungsgremium eine Parallele zu dem datenschutzrechtlichen Medienprivileg, das in Deutschland im § 41 BDSG geregelt ist. Zwar sind durch digitale Medien in ihrer Entfaltung befähigte Privatpersonen nicht vollends mit Journalisten vergleichbar, jedoch ist der Umstand einer Datennutzung im Rahmen der Ausübung von Kommunikations- und politischen Freiheiten vergleichbar.[1140] Ebenso verweist die Art. 29-Datenschutzgruppe darauf, dass viele der zu erwartenden Verstöße bereits durch Vorschriften zum Schutz vor Nötigung, Bedrohung, Beleidigung, Diskriminierung etc. sanktioniert werden, deren Anwendung sachnäher sein kann.[1141]

Zur eigentlichen Bestimmung der Grenzen der persönlichen und familiären Tätigkeit schlägt die Art. 29-Datenschutzgruppe mehrere Faktoren vor, die nicht notwendigerweise jeweils für sich, sondern vielmehr im Rahmen einer Gesamtschau zu würdigen sind:[1142]

Werden die personenbezogenen Daten eher einer nicht bestimmbaren Zahl von Personen, als einer beschränkten Gemeinschaft von Freunden, Familienmitgliedern oder Bekannten zugänglich gemacht?

Betreffen die personenbezogenen Daten andere Personen, als solche, zu denen eine persönliche oder familiäre Beziehung besteht?

Lassen der Umfang und die Häufigkeit der Verarbeitung personenbezogener Daten eine professionelle oder eine Vollzeittätigkeit vermuten?

Liegen Anhaltspunkte dafür vor, dass eine Zahl von Personen in einem kollektiven und organisierten Verbund tätig ist?

Ist mit schädlichen Auswirkungen auf Individuen, zu denen Eingriffe in deren Privatsphäre gehören, zu rechnen?

1137 Ebenda, 7.

1138 Ebenda, 6 f.

1139 "[…] the application of the rules should be effective but relatively 'lite'", Ebenda, 5.

1140 Ebenda, 1 f.

1141 Die Art. 29-Datenschutzgruppe verweist darauf, dass die Datenschutzbehörden trotzdem darauf achten müssen, dass keine Schutzlücken entstehen, Ebenda, 6 f.

1142 Übersetzung aus dem Englischen, S. Ebenda, 4.

Die durch die Art. 29-Datenschutzgruppe aktualisierten Kriterien ausschließlich persönlicher und familiärer Nutzung entsprechen weitestgehend der bisherigen, im Rahmen persönlicher und familiärer Videoüberwachung am Schutzzweck des Rechts auf informationelle Selbstbestimmung orientierten Betrachtung. Ob eine ausschließlich persönliche oder familiäre Nutzung vorliegt, ist demnach ausgehend von der Verkehrsanschauung „anhand des äußeren Rahmens, der organisatorischen Anlagen und inhaltlicher Konzeption des Handelns" zu beurteilen.[1143] Vor allem ist ein möglicher Kontrollverlust der betroffenen Person über ihre Daten zu berücksichtigen, der bei Videoaufnahmen vor allem im Fall ihrer Verbreitung und Veröffentlichung droht.[1144] Es kommt also vor allem auf die Ausrichtung des Datenumgangs an.[1145] Eine ausschließlich persönliche und familiäre Nutzung soll vor allem dann entfallen, wenn der Verbleib von erfassten Vorgängen „in dem privaten Herrschaftsraum" der Privatpersonen nicht mehr gewährleistet, sondern ein Zugriff durch Dritte, sei es berechtigt oder unberechtigt, nicht ausgeschlossen ist.[1146]

Da die vorstehend dargelegten Kriterien eine Einzelfallprüfung voraussetzen und keine trennscharfen abstrakten Aussagen ermöglichen, werden die Grenzen des persönlichen und familiären Einsatzes von Smartglasses nachstehend anhand typisierender Fallgruppen der Nutzung beurteilt.[1147]

(b) Abgrenzung von geschäftlicher und beruflicher Nutzung

Eindeutig nicht persönlich-familiär ist die Nutzung von Smartglasses für kommerzielle oder berufliche Zwecke, d.h., wenn die Ergebnisse der Datenverarbeitung unmittelbar oder mittelbar einer geschäftlichen oder wirtschaftlichen Verwertung zugeführt werden sollen, z.B. beim Einsatz

---

[1143] *Dammann*, in: *Simitis*, BDSG, § 1, Rn. 151; *Fuchs*, ZD 2015, S. 212 (213); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 257; *Schmidt*, in: *Taeger/Gabel*, BDSG, § 1, Rn. 31.

[1144] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 258.

[1145] Lt. Piltz kann der Umfang des Datenumgangs allenfalls ein Indiz dafür sein, dass eine Tätigkeit nicht mehr persönlich und familiär ist, *Piltz*, Soziale Netzwerke im Internet, 2013, S. 94 f.

[1146] *Fuchs*, ZD 2015, S. 212 (213); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 258.

[1147] Zur Diskussion vgl. *Dammann*, in: *Simitis*, BDSG, § 1, Rn. 149; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 254 ff.; *Piltz*, Soziale Netzwerke im Internet, 2013, S. 93 ff.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 54 ff.

durch Fotografen.[1148] Die Abgrenzung zwischen privaten und geschäftlichen Zwecken fällt jedoch aufgrund der zunehmenden Verschmelzung zwischen privaten und geschäftlichen Lebensbereichen immer schwerer.[1149] Dies ist z.B. in sozialen Netzwerken zu beobachten, wo die private Kommunikation mit der geschäftlichen Kommunikation vermischt wird.[1150] In einem solchen Fall müsste eine Einzelfallbetrachtung stattfinden, wobei bereits eine nicht unwesentliche geschäftliche Vermischung gegen die Anwendung des § 1 Abs. 2 Nr. 3 BDSG sprechen würde, da eine persönliche und familiäre Nutzung ausschließlich vorliegen muss.

(c) Herstellung von Bild- und Tonbeweisen

Werden Aufnahmen, die zu möglichen Beweiszwecken in Zivil- oder Strafverfahren dienen sollen, erstellt, können sie nach überwiegender Meinung nicht mehr als persönlich betrachten werden, da von einer späteren Zugänglichmachung der Aufnahmen gegenüber Dritten im Gerichtsverfahren und dem Einsatz gegen die Betroffenen auszugehen ist.[1151] Dadurch erfolgt ein Eingriff in das Recht auf informationelle Selbstbestimmung, da die Betroffenen sich nicht sicher sein können, ob, wann und wie die sie betreffenden Informationen gegen sie verwendet werden könnten.

Nach einer einschränkenden Ansicht ist jedoch zwischen der Aufnahme und der späteren Verwendung der Aufnahmen als Beweismittel zu unterscheiden.[1152] Während bei der Verwendung der herrschenden Meinung zugestimmt wird, soll die Aufnahme dennoch ausschließlich persönlich

---

[1148] Zur mittelbaren Nutzung, z.B. durch Werbeschaltungen, S. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 258; vgl. *Schmundt/Krug/Sperber*, Fotobrille Google Glass: Star-Fotografen testen die Zukunft, Spiegel Online, http://www.spiegel.de/netzwelt/gadgets/google-glass-star-fotografen-elliott-erwitt-und-bruce-gilden-testen-a-1015979.html (3.7.2015); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 57; ferner soll laut Art. 29-Datenschutzgruppe für die Annahme einer geschäftlichen Tätigkeit nicht nur das kommerzielle Interesse maßgeblich sein, sondern auch eine andere über den persönlichen Rahmen hinausgehende Interessensverfolgung, wie z.B. bei einer wohltätigen Spendensammeltätigkeit, Art. 29-Datenschutzgruppe, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, 2013, S. 8.

[1149] Vgl. *Göpfert/Wilke*, NZA 2012, S. 765 (765 f.); *Piltz*, Soziale Netzwerke im Internet, 2013, S. 94.

[1150] Vgl. *Piltz*, Soziale Netzwerke im Internet, 2013, S. 94.

[1151] VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (237); *Balzer/Nugel*, NJW 2014, S. 1622 (1625); *Golla/Herbort*, GRUR 2015, S. 648 (649); *Lachenmann/Schwiering*, NZV 2014, S. 291 (292); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 261; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 58.

[1152] *Fuchs*, ZD 2015, S. 212 (2015).

und familiär sein können.[1153] So soll z.B. ein Autofahrer, der eine Dashcam zwar mitlaufen lässt, aber nur um Beweise über eigenes Verhalten zu sammeln (z.B. um sich beim Unfall vom Eigenverschulden zu entlasten) ausschließlich persönlich und familiär handeln, auch wenn Dritte miterfasst werden.[1154] Als Argument für diese vorstehende Ansicht wird darauf verwiesen, dass bei mobilen Geräten, anders als bei stationärer Videoüberwachung, die Überwachung lediglich der Wahrnehmung ihrer Nutzer entspricht und mit „privaten Fotoaufnahmen" vergleichbar ist.[1155] Dabei wird auch auf Smartglasses und den Umstand Bezug genommen und gesagt, dass die fehlende „Fotografiergeste" keine abweichende Betrachtung rechtfertigt, da § 1 Abs. 2 Nr. 3 BDSG nicht auf die Erkennbarkeit der Aufnahme abstellt.[1156] Ferner wird in derartig „privater" Videoüberwachung keine hohe Belastung gesehen, da sie nicht zu lückenloser Überwachung führe.[1157]

Die einschränkende Ansicht vermag vor dem Hintergrund der im Rahmen verfassungsrechtlicher Prüfung erzielten Ergebnisse nicht zu überzeugen.[1158] Zum einen können „private Fotoaufnahmen", womit gelegentliche Schnappschüsse gemeint sind, nicht mit der Intensität einer permanent auf Menschen ausgerichteten Videokamera verglichen werden.[1159] Auch ist die Erkennbarkeit der Beobachtungs- oder Aufnahmevorgänge von großer Relevanz für die Eingriffsintensität der Videoüberwachung, da die Intransparenz möglicher Aufnahmevorgänge eine panoptische Einschüchterungswirkung auf Betroffene ausüben kann.[1160] Auch das Argument, dass die Erkennbarkeit der Aufnahme nicht im § 1 Abs. 2 Nr. 3 BDSG wörtlich enthalten ist, schlägt fehl, da diese Voraussetzung ein Auslegungskriterium des unbestimmten Rechtsbegriffs einer „persönlichen und familiären Tätigkeit" darstellt und als solches nicht ausdrücklich im Wortlaut des Gesetzes auftauchen muss.[1161] Ebenso kann eine lückenlose Überwachung nicht mit dem Blick auf einzelne Videoüberwachungsmaßnahmen abgelehnt werden. Ganz im Gegenteil müssen auch

---

[1153] Lt. AG München sollte die Zulässigkeit der Aufnahme sogar ihre Verwertbarkeit implizieren, AG München, Urt. v. 6.6.2013 (343 C 4445/13), NJW-RR 2014, 413 (414); *Fuchs*, ZD 2015, S. 212 (2015 f.).

[1154] *Fuchs*, ZD 2015, S. 212 (2015).

[1155] Ebenda.

[1156] Ebenda, 2016; bezugnehmend auf *Schwenke*, K&R 2013, S. 685 (686).

[1157] *Fuchs*, ZD 2015, S. 212 (216).

[1158] Vgl. E V, S. 181.

[1159] Vgl. E V, S. 181.

[1160] Vgl. E II. 2. b) gg) (3), S. 128.

[1161] Vgl. zur mittelbaren Drittwirkung verfassungsrechtlicher Kriterien im einfachen Recht E I, S. 89.

die Summierungseffekte einzelner Maßnahmen bei deren Bewertung berücksichtigt werden.[1162]

Folglich ist entsprechend der herrschenden Ansicht jeder Einsatz von Smartglasses zur Sicherung von Beweismitteln nicht ausschließlich persönlich und familiär, auch wenn Dritte nur möglicherweise miterfasst werden.[1163]

(d) Einsatz zu präventiven Abschreckungszwecken

Ähnlich wie Bodycams von Polizeibeamten können Smartglasses zum Schutz der persönlichen Sicherheit und des Eigentums eingesetzt werden, z.B. beim Spaziergang in einer unsicheren Gegend.[1164] Dritte, die mit einer Aufzeichnung rechnen müssten, könnten so von etwaigen persönlichen Angriffen auf den Träger oder dessen Eigentum abgeschreckt werden.[1165] Eine derartige Nutzung wird im Regelfall mit der Absicht, Beweismittel zu sichern, verbunden und daher entsprechend den vorgehenden Ausführungen nicht mehr ausschließlich persönlicher und familiärer Natur sein.[1166]

Allerdings sind auch Situationen vorstellbar, in denen tatsächlich keine Aufnahmen beabsichtigt werden, z.B. bei einer Live-Übertragung des Geschehens oder bei abgeschalteten Smartglasses. Jedoch sollen Smartglasses auch in diesem Fall dazu eingesetzt werden, Dritte außerhalb des Bekannten-, Freundes- oder Familienkreises in ihrer Entschluss- und Handlungsfreiheit durch die Abschreckungswirkung der Geräte einzuschränken.[1167] D.h., der Zweck eines derartigen Einsatzes von Smartglasses liegt geradezu in der Beeinträchtigung der persönlichen Entfaltung Dritter im öffentlichen Raum, wodurch die Grenze persönlicher Nutzung überschritten wird.[1168] Dies gilt umso mehr, als Smartglasses diese Abschreckungswirkung permanent und anlasslos auf alle Personen in ihrem Erfassungsbereich ausüben können.[1169] Einer permanenten Überwachung kommt auch der Einsatz von Smartglasses gleich, wenn Passanten nur möglicherweise kurzfristig erfasst werden, da die Träger von Smartglasses

---

[1162] Vgl. E IV. 1. k) cc) (1), S. 165; LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233; AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291.

[1163] EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196).

[1164] Vgl. E III. 4, S. 146.

[1165] Vgl. B III. 1, S. 35.

[1166] Vgl. F II. 1. c) cc) (2) (c), S. 199.

[1167] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 60.

[1168] So im Ergebnis auch EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196); *Lachenmann/Schwiering*, NZV 2014, S. 291 (292); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 60.

[1169] Eine derartige Abschreckungswirkung wurde bereits im Fall einer Klingelschildkamera bejaht, KG Berlin, Beschl. v. 26.6.2002 (24 W 309/01), NJW 2002, 2798.

sich nach ihnen z.B. umdrehen und ihnen generell näher als Videoüberwachungskameras oder Dashcams kommen können.[1170]

(e) Alltägliche Nutzung und Augmented Reality

Es ist damit zu rechnen, dass Smartglasses im Regelfall nicht zu präventiven oder repressiven Zwecken eingesetzt werden.[1171] Vielmehr ist mit ihrer Nutzung zur Erstellung alltäglicher Schnappschüsse oder Videos wie bei Smartphones, um sich an Lebensmomente zu erinnern, andere zu informieren oder zu unterhalten, zu rechnen. Ebenfalls könnte, je nach Entwicklungsstufe, ein großer Teil der Nutzungszeit auf Augmented-Reality-Funktionen entfallen.

Derartige private Nutzungen sind nicht darauf gerichtet, andere Menschen zu einem Handeln oder Unterlassen zu bewegen. Sofern dies passiert, geschieht es nur als Nebenfolge. Dennoch kommt es nicht nur auf die subjektiven Vorstellungen der Nutzer von Smartglasses an, sondern auf den objektiven Schutz von Individuen und der Meinungspluralität.[1172] Denn anders als die Nutzer, können die Betroffenen den Zweck der Nutzung von Smartglasses nicht erkennen. Sie können daher berechtigterweise auch von Aufnahmen zur Beweissicherung, Voyeurismus oder, bei entsprechendem technischen Entwicklungsstand, von biometrischer Erkennung ausgehen.[1173] Ansonsten wären die Betroffenen eines Rechtsschutzes gegen die Verletzung ihrer Privatsphäre generell beraubt. Da die konkrete Nutzung der Smartglasses nicht nachweisbar ist, könnten deren Nutzer immer behaupten, die Geräte privat genutzt zu haben. Dann wäre auch eine geschäftliche, repressive oder präventive Nutzung von Smartglasses praktisch immer legitimiert.

Eine weitere Beeinträchtigung der Rechte Betroffener kann eintreten, wenn die mittels Smartglasses erstellten Aufnahmen oder sonst erhobenen Daten innerhalb von Cloud-Diensten gespeichert werden, deren Schutzniveaus einen unbefugten Datenzugriff befürchten lassen.[1174] Dasselbe gälte, wenn die Aufnahmen anderen Personen zugänglich gemacht werden würden. Hierbei ist zu bedenken, dass auch geschlossene „Freundeskreise“ oder vergleichbare Gruppen innerhalb sozialer Netzwerke eine hohe Gefahr des Kontrollverlusts über die Aufnahmen mit sich bringen,

---

[1170] Vgl. E IV. 1. c), S. 151; *Dammann*, in: *Simitis*, BDSG, § 1, Rn. 148.

[1171] Vgl. B IV. 3, S. 52.

[1172] Vgl. *Golla/Herbort*, GRUR 2015, S. 648 (650).

[1173] Vgl. E II. 2. b) gg) (3), S. 128.

[1174] Vgl. zu der Problematik, *Heckmann*, K&R 2011, S. 770 (773); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 259; *Piltz*, Soziale Netzwerke im Internet, 2013, S. 96.

da sie häufig über hohe mehrstellige Personenzahlen verfügen.[1175] In jedem Fall liegt keine ausschließlich persönliche und familiäre Nutzung vor, wenn die Aufnahmen einem unbeschränkten Personenkreis zugänglich gemacht werden.[1176]

(f) Persönliche und familiäre Nutzung von Smartglasses nur in Ausnahmefällen

Der von Smartglasses permanent ausgehende Überwachungs- und Anpassungsdruck sowie je nach Fall die Gefahr des Verfügungsverlusts über Aufnahmen und sonst erhobene Daten führen dazu, dass Smartglasses unabhängig von der Art ihrer Nutzung die Persönlichkeitsrechte Dritter erheblich gefährden. Ihr Einsatz im öffentlichen Raum kann daher nicht als ausschließlich persönlich und familiär betrachtet werden.[1177]

Eine Ausnahme wäre jedoch dann zu machen, wenn Smartglasses aus medizinischen Gründen eingesetzt werden würden, z.B. um körperliche Nachteile, insbesondere die Sehschwäche, auszugleichen.[1178] Die hierbei erfassten Informationen werden regelmäßig dem typischen persönlichen Zweck dienen und aufgrund der vergleichsweise geringen Fallzahl ist nicht mit einer Einschüchterung Dritter sowie einer unkontrollierbaren Verbreitung von Smartglasses zu rechnen.[1179]

Ein weiterer Ausnahmefall könnte allenfalls dann vorliegen, wenn Smartglasses in einem räumlichen Bereich genutzt werden würden, in dem mit der Beeinträchtigung anderer Menschen in keinem Fall zu rechnen wäre. Solche Fälle der Nutzung, z.B. in einem von Menschen nicht frequentierten Waldstück, stellen jedoch ebenfalls seltene Ausnahmen der

---

[1175] Nur wenn zwischen allen Personen einer geschlossenen Gruppe eine engere soziale Verbindung besteht und die Gruppe über eine geringe Personenzahl verfügt, kann laut der Literatur und Rechtsprechung noch von einem persönlich verbundenem Personenkreis gesprochen werden, vgl. VGH München, Beschl. v. 29.2.2012 (12 C 12.264), NZA-RR 2012, 302 (304); Art. 29-Datenschutzgruppe, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, 2013, S. 9; *Fuchs*, ZD 2015, S. 212; *Golla/Herbort*, GRUR 2015, S. 648 (649 f.); *Ohly*, AfP 2011, S. 428 (430); *Piltz*, Soziale Netzwerke im Internet, 2013, S. 194, 199 f.; *Schwenke*, K&R 2013, S. 685 (687).

[1176] EuGH, Urt. v. 6.11.2003 (C-101/01), MMR 2004, 95 (96); *Golla/Herbort*, GRUR 2015, S. 648 (649); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 260.

[1177] Vgl. E V, S. 181; der EuGH bezog sich mit demselben Ergebnis zwar nur auf Videoüberwachung zu präventiven und repressiven Zwecken, betonte jedoch ausdrücklich dass sie auf das absolut Notwendige beschränkt werden muss, EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196).

[1178] Vgl. E III. 4, S. 146.

[1179] Vgl. E IV. 3, S. 180.

alltäglichen Nutzung von Smartglasses dar, die von der, für diese Untersuchung vor allem maßgeblichen Alltagsnutzung, abweichen.

dd) Grundsätzliche Anwendbarkeit des § 6b BDSG bei der Nutzung von Smartglasses

Smartglasses stellen Datenverarbeitungsanlagen dar, die personenbezogene Daten im öffentlichen Raum generell nicht ausschließlich zu persönlichen oder familiären Zwecken erfassen. Die Frage, ob die Anwendbarkeitskriterien des § 1 Abs. 2 Nr. 3 BDSG auf § 6b BDSG anzuwenden sind, wirkt sich daher im Fall von Smartglasses insgesamt nicht aus, da alle ihre Anforderungen ohnehin erfüllt werden. D.h., § 6b BDSG ist bei der Nutzung von Smartglasses grundsätzlich anwendbar. Die Nutzer von Smartglasses sind ferner im Hinblick auf die Videoüberwachung als verantwortliche Stellen i.S.d. § 3 Abs. 7 BDSG zu betrachten, da sie personenbezogene Daten für sich selbst erheben, verarbeiten oder nutzen.

d) Zulässigkeit der Videoüberwachung mit Smartglasses

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen gem. § 6b Abs. 1 BDSG stellt zugleich den Anknüpfungspunkt für die gesamte Regelung des § 6b BDSG als auch einen ersten Zulässigkeitstatbestand der so legal definierten Videoüberwachung dar.[1180] Bevor die zulässigen Beobachtungszwecke geprüft werden, muss jedoch zuerst untersucht werden, welche Arten der Nutzung von Smartglasses eine „Beobachtung" darstellen, die dem Regelungsbereich dieser Vorschrift unterfällt.

aa) Beobachtung

Als Beobachtung i.S.d. § 6b Abs. 1 BDSG ist grundlegend eine visuelle Betrachtung zu verstehen, bei der Personen oder Geschehnisse optisch mittels einer technischen Einrichtung sichtbar gemacht werden.[1181] Diese Definition würde jedoch jede bloße visuelle Wahrnehmung umfassen, unabhängig von einer möglichen Beeinträchtigung der informationellen Selbstbestimmung. Z.B. würde auch der reflexartige Blick eine Beobachtung i.S.d. Gesetzes darstellen.[1182] Daher werden für die Beobachtung ein gewisses Zeitmoment und eine Systematik gefordert, die auf ein mehr oder weniger gezieltes Vorgehen hindeuten.[1183] Zu fragen ist jedoch, ob

---

[1180] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 268.

[1181] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 63 f.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 17.

[1182] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270.

[1183] *Gola/Schomerus*, BDSG, § 6b, Rn. 10; *Hilpert*, RDV 2009, S. 160 (161); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 64; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 21.

auch Smartglasses als mobile Geräte einer Beobachtung im Rahmen des § 6b Abs. 1 BDSG dienen können.

(1) Mobile Beobachtung

Die gesetzliche Konzeption des § 6b Abs. 1 BDSG orientiert sich zwar entsprechend der Gesetzesbegründung an bereits bestehender Videoüberwachung und ist bei historischer Betrachtung im Hinblick auf ortsgebundene Kameras entstanden.[1184] Doch bereits im Rahmen der Prüfung der Voraussetzungen einer optisch-elektronischen Einrichtung wurde festgestellt, dass auch mobile Geräte diese erfüllen.[1185] Die Grenzen zwischen mobilen und immobilen Kameras sind aufgrund von deren Miniaturisierung und Flexibilität kaum feststellbar und ein Festhalten an einer Standortfestigkeit würde dem gesetzlichen Vorhaben einer umfassenden und restriktiven Regelung der Videoüberwachung widersprechen.[1186]

Auch im Hinblick auf eine Beobachtung ist nicht einzusehen, warum eine zweckgerichtete, über ein gewisses zeitliches und systematisches Moment verfügende Betrachtung nicht auch mittels eines mobilen Gerätes erfolgen kann.[1187] Der vorgebrachte Einwand, dass die Beobachtung gem. § 6b BDSG auf eine Raumbeobachtung gerichtet sein soll, überzeugt auch an dieser Stelle nicht, da auch Räume mobil beobachtet werden können und auch Raumbeobachtung häufig auf die Beobachtung eines möglichen Verhaltens von Personen in dem Raum gerichtet ist.[1188] Mithin ist davon auszugehen, dass auch Smartglasses zur Videoüberwachung gem. § 6b Abs. 1 BDSG generell geeignet sind.

(2) Zeitliche und systematische Anforderungen der Beobachtung

Die Beobachtung setzt zwar ein gewisses Zeitmoment voraus, jedoch wird dessen Schwelle sehr niedrig angesetzt. So reicht z.B. der Zeitraum, den es erfordert, um die Einlasswürdigkeit einer an der Tür klingelnden Person durch eine Türklingelkamera einzuschätzen, für die Annahme einer Beobachtung aus.[1189]

Nicht notwendig ist zudem, dass der Beobachtung ein „festgelegtes und durchdachtes Vorgehen" zugrunde liegt.[1190] So kann auch eine zuerst unsystematische Betrachtung in eine zielgerichtete Beobachtung überge-

---

[1184] BT-DrS. 14/4329, S. 30, 38; *Gola/Schomerus*, BDSG, § 6b, Rn. 10.

[1185] Vgl. F II. 1. a) aa), S. 188.

[1186] Vgl. F II. 1. a) aa), S. 188.

[1187] So im Ergebnis *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 19.

[1188] Vgl. F II. 1. a) aa), S. 188.

[1189] *Klar*, MMR 2012, S. 788 (196).

[1190] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270.

hen (z.B. im Fall eines Voyeurs, der seinen Blick umherschweifen lässt, und anschließend gezielt die visuelle Verfolgung einer Person aufnimmt).[1191]

Dagegen ist es fraglich, ob auch einzelne Betrachtungen, z.B. wenn ein Träger von Smartglasses eine Szene als Standbild oder mittels einer Videoaufnahme zu Erinnerungszwecken festhält, bereits eine Beobachtung darstellen. Zum Teil wird zwischen einfachen Standbildern bzw. Fotografien unterschieden, wobei die ersteren keine Beobachtung darstellen sollen, da es ihnen an dem erforderlichen Zeitmoment mangelt, das bei einer Beobachtung vorausgesetzt wird.[1192] Nach anderer Ansicht ist der Begriff „Video" in Videoüberwachung entsprechend dem lateinischen Begriff „ich betrachte" zu verstehen, sodass er auch Einzel- und Bewegtbilder umfasst.[1193] Eine solche Generalisierung wäre jedoch genauso zu weitgehend, wie das Abstellen auf einzelne Aufnahmen zu eng wäre. Vielmehr ist zu prüfen, ob einzelne Betrachtungsvorgänge durch eine Systematik und ein gewisses Zeitmoment zusammengefasst werden und so auf eine Beobachtung hindeuten.[1194] So wird das einmalige Festhalten eines Geschehens als Fotografie oder auch als eine Videoaufnahme keine Beobachtung darstellen, wenn diese lediglich eine punktuelle Abbildung eines Geschehens darstellt, wie es typisch für Schnappschüsse ist.[1195]

Zum Teil wird für die Beobachtung ein auf Kontrolle, Sicherheit oder Ausspähung und Registrierung bestimmter Vorgänge gerichteter Zweck der visuellen Wahrnehmung gefordert.[1196] Diese Ansicht ist jedoch abzulehnen.[1197] Zum einen wird die Beobachtung öffentlicher Räume mittels

---

1191 Vgl. Ebenda, 270 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 63.

1192 *Hilpert*, RDV 2009, S. 160 (161); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 64.

1193 *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 18.

1194 *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 63.

1195 *Hilpert*, RDV 2009, S. 160 (161); das gilt auch, wenn als Teil eines systematisch größeren Konzepts viele Einzelaufnahmen von Straßenpanoramen erstellt werden, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 64; denn in diesem Fall richtet sich die Systematik auf das Sammeln von einzelnen Aufnahmen, enthält jedoch keine Motivation die Aufmerksamkeit der Betrachtung über einen gewissen Zeitraum systematisch einem bestimmten räumlichen Bereich oder einem Objekt zu widmen, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 193; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 64; auf der anderen Seite kann auch ein Einzelbild zum Teil einer auf über gewissen Zeitraum erfolgenden systematischen Betrachtung sein, z.B. wenn jedes Fahrzeug, das die Schranke eines Parkhauses passiert, eine Fotografie auslöst, vgl. *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 18.

1196 *v. Zezschwitz*, in: Handbuch Datenschutzrecht, 2003, Kap. 9.3. Rn. 18.

1197 So im Ergebnis *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 194; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 268 f.

optisch-elektronischer Einrichtungen als Videoüberwachung definiert, was nicht notwendig wäre, wenn die Beobachtung bereits die Merkmale der Überwachung enthalten würde.[1198] So wird der Überwachungsbegriff, zumindest wie er im Rahmen dieser Untersuchung verstanden wird, durch eine Beobachtung definiert, die zusätzlich um eine Kontroll- bzw. eine Machtkomponente ergänzt wird, die folglich bei einer bloßen Beobachtung fehlen darf.[1199] Das kann z.B. der Fall sein, wenn die Beobachtung bloß aus Neugierde oder Langeweile erfolgt.[1200]

Die Beobachtung kann somit allenfalls als eine Form der Überwachung verstanden werden, die sich nicht zwangsläufig auf die Verfolgung der Handlungen anderer Menschen beschränken muss.[1201] Ebenso ist es nicht maßgeblich, ob die visuell verfolgte Person sich beobachtet fühlt. Ansonsten würde gerade die eingriffsintensivere heimliche Videoüberwachung aus dem Tatbestand des § 6b BDSG ausscheiden.[1202] Findet die Beobachtung jedoch nach objektiven Maßstäben statt, ist es ferner irrelevant, ob sie das primäre Interesse, die Motivation oder den eigentlichen Zweck der Nutzung von Smartglasses darstellt.[1203]

Fasst man die Anforderungen an eine Beobachtung zusammen, ist im Fall der typischen Nutzung von Smartglasses bei einer ganzheitlichen Betrachtung von einer Beobachtung i.S.d. § 6b Abs. 1 BDSG auszugehen.[1204] Der Grund liegt zum einen darin, dass Smartglasses jederzeit zu Aufnahmen oder Live-Übertragungen bereit und auf die möglichen Aufnahmeobjekte gerichtet sind.[1205] Nutzt z.B. ein Träger von Smartglasses auf dem Weg zur Arbeit die Datenbrille, um Aufzeichnungen möglicherweise in Gefahrensituationen, aus sonstigem persönlichen Interesse oder zu Zwecken von Augmented Reality vorzunehmen, dann stellt diese Nutzung der Smartglasses als Ganzes ein systematisches und durch eine zeitliche Nachhaltigkeit gekennzeichnetes Vorgehen, mithin eine Beobachtung dar.

Damit sind Smartglasses eher mit klassischer Videoüberwachung als mit Urlaubsschnappschüssen vergleichbar. Urlaubsschnappschüsse und sonstige einzelne Maßnahmen sind objektiv als solche erkennbar, weil die

---

1198 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 268 f.

1199 Vgl. A IV. 8, S. 17.

1200 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 269.

1201 Ebenda, 268 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 63.

1202 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270.

1203 Vgl. Ebenda, 271; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 63.

1204 Entsprechend der verfassungsrechtlichen Bewertung in E II. 2. b) gg) (1), S. 124.

1205 Vgl. F II. 1. a) bb), S. 190.

Kamera für diese Zwecke hervorgeholt und auf die Aufnahmeobjekte gerichtet wird. Bei Smartglasses fehlt diese „Fotografiergeste".[1206] Ganz im Gegenteil können sich Betroffene nicht sicher sein, ob und wann die Smartglasses auf sie gerichtet werden oder eine Aufnahme erfolgt, sodass diese objektiv betrachtet zu jeder Zeit stattfinden kann.[1207]

Folglich ist bei der Nutzung von Smartglasses zu jeder Zeit ein Beobachtungsvorgang gem. § 6b Abs. 1 BDSG anzunehmen, unabhängig davon, ob Personen tatsächlich länger fixiert werden oder nicht. Ausnahmen sind nur dann zu machen, wenn Smartglasses kurzfristig aufgesetzt werden, um Aufnahmen ähnlich wie mit einer Fotokamera zu erstellen. Dies wäre jedoch kein Fall typischer Nutzung von Smartglasses als alltägliche Begleiter von Menschen.

(3) Notwendigkeit der Erhebung personenbezogener Daten

Nach herrschender Ansicht wird für die Videoüberwachung die im § 1 Abs. 2 BDSG vorausgesetzte (bzw. als Teil des „Umgangs" gem. § 1 Abs. 1 BDSG verstandene) Erhebung von personenbezogenen Daten ebenfalls im § 6b BDSG verlangt.[1208] Die Erhebung ist gem. § 3 Abs. 3 BGB legal als eine objektive Beschaffung von Daten beim Betroffenen definiert, was nach überwiegender Meinung zugleich eine subjektive Aktivität voraussetzt, die der erhebenden Stelle die Verfügungsmacht oder zumindest die Kenntnis von Daten über die betroffene Person verschafft.[1209] Die objektive Erhebung personenbezogener Daten wurde bereits im Rahmen der Prüfung der Voraussetzungen des § 1 Abs. 2 Nr. 3 BDSG bejaht.[1210] Eine subjektive Erhebung dient der Abgrenzung von

---

[1206] Vgl. E IV. 1. g), S. 154.

[1207] Vgl. LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327 (328); LG Itzehoe, Urt. v. 11.9.1997 (7 (9) 0 51–96), NJW-RR 1999, 1394 (1395).

[1208] In der Rechtsprechung wird auf die Erhebung i.d.R. selten eingegangen, jedoch wird sie vorausgesetzt, wie z.B. die Nichtanwendung des § 6b BDSG bei Kameraattrappen zeigt, LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1067 f.); AG Aachen, Urt. v. 11.11.2003 (10 C 386/03), NZM 2004, 339 (339 f.); BAG, Urt. v. 15.5.1991 (5 AZR 115/90), BAGE 68, 52 (56); *Fuchs*, ZD 2015, S. 212 (213); die vor dem Hintergrund der Einbeziehung von Kameraattrappen in den Tatbestand des § 6b Abs. 1 BDSG geführte Diskussion, ist im Fall der funktionell zu Aufnahme einsatzfähigen Smartglasses nicht relevant, vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 197 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 272 ff.; *Scholz*, in: *Simitis*, BDSG, § 3, Rn. 166.

[1209] LAG Hamm, Beschl. v. 16.9.2011 (10 TaBV 17/11), ZD 2012, 183; *Buchner*, in: *Taeger/Gabel*, BDSG, § 3, Rn. 26; *Gola/Schomerus*, BDSG, § 3, Rn. 23 f.; m.w.N. *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 102; *Fuchs*, ZD 2015, S. 212 (213); *Gola/Schomerus*, BDSG, § 3, Rn. 24.

[1210] Vgl. F II. 1. c) bb), S. 193.

einer lediglich zufälligen oder aufgedrängten Datenerhebung.[1211] Sie liegt aber auch dann vor, wenn die objektive Erhebung personenbezogener Daten lediglich in Kauf genommen wird, z.B. wenn eine Kamera in Bereichen eingesetzt wird, in denen typischerweise Personen sich aufhalten könnten. In solchen Fällen kann nicht von zufälliger oder aufgedrängter Erhebung gesprochen werden.[1212] D.h., ähnlich wie schon bei der Frage der rein persönlichen oder familiären Nutzung, können Nutzer von Smartglasses allenfalls ausnahmsweise in räumlich entlegenen Bereichen, wie z.B. einem entlegenen Wald, davon ausgehen, keine personenbezogenen Daten zu erheben.[1213]

Der Anlass der Datenerhebung ist dagegen irrelevant.[1214] D.h., auch wenn ein Nutzer die Smartglasses z.B. nur zur Aufnahme einer Landschaft einsetzen wollte und dabei identifizierbare Personen erfasst, handelt es sich um eine Erhebung personenbezogener Daten. Ebenso ohne Bedeutung ist, ob die durch die Smartglasses erfassten Daten von ihrem Nutzer tatsächlich zur Kenntnis genommen werden.[1215] Z.B. könnte eine Aufzeichnung zur Objekterkennung zwecks Erzeugung einer Augmented Reality Personen erfassen, während der Nutzer der Smartglasses sich auf einen Punkt in seinem Sichtfeld konzentriert.

Es wird ferner diskutiert, ob es eine Voraussetzung des § 6b Abs. 1 BDSG ist, dass die erhobenen Daten anschließend verarbeitet, insbesondere gespeichert oder übermittelt bzw. genutzt werden müssen.[1216] Der Streit um die Erforderlichkeit der Verwendung der erhobenen Daten wurde jedoch vor dem Hintergrund einer als „verlängertes Auge" bezeichneten Videoüberwachung geführt, bei dem das Geschehen lediglich von Personen am Bildschirm beobachtet und daher nicht immer automatisch ausgewertet werden konnte.[1217] Smartglasses sind jedoch zur Aufzeichnung, Übermittlung und Verarbeitung der erhobenen Informationen fähig, sodass diese Problematik vorliegend keine Relevanz hat.

1211 *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 104; *Gola/Schomerus*, BDSG, § 3, Rn. 24.

1212 *Fuchs*, ZD 2015, S. 212 (214).

1213 Vgl. F II. 1. c) cc) (2) (e), S. 201; vgl. Ebenda.

1214 *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 105; *Fuchs*, ZD 2015, S. 212 (214).

1215 *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 105 f.

1216 Eine anschließende Verwendung der Daten ist nicht erforderlich lt. *Buchner*, in: *Taeger/Gabel*, BDSG, § 3, Rn. 25; *Dammann*, in: *Simitis*, BDSG, § 3, Rn. 106; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 277 f.; a.A. *Gola/Schomerus*, BDSG, § 3, Rn. 10; *Königshofen*, RDV 2001, S. 220 (221 f.).

1217 *Gola/Schomerus*, BDSG, § 3, Rn. 24; *Königshofen*, RDV 2001, S. 220 (221 f.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 272; *Taeger*, ZD 2013, S. 571 (574).

bb) Zulässigkeitstatbestände des § 6b Abs. 1 BDSG

§ 6b Abs. 1 BDSG enthält drei Zulässigkeitstatbestände der Videoüberwachung, von denen für Privatpersonen als nicht öffentliche Stellen die Wahrnehmung des Hausrechts (Nr. 2) und die Wahrnehmung berechtigter Interessen für konkrete Zwecke (Nr. 3) in Frage kommen, sofern keine Anhaltspunkte bestehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen.[1218]

(1) Wahrnehmung des Hausrechts

Das Hausrecht ist im BDSG selbst nicht definiert und bestimmt sich nach anderen Vorschriften, insbesondere dem Recht des Besitzers oder Eigentümers gem. §§ 859 ff., 904, 1004 BGB sowie § 123 StGB.[1219] Das Hausrecht gibt dem unmittelbaren Besitzer das Recht, die erforderlichen Maßnahmen zu treffen, um bestimmte Räume oder befriedetes Besitztum und die sich innerhalb dieser aufhaltenden Personen zu schützen, sowie zur Abwehr unbefugten Betretens.[1220] Anders als im Fall klassischer Videoüberwachung[1221] ist nicht damit zu rechnen, dass Smartglasses zur Wahrnehmung des Hausrechts im öffentlichen Raum eingesetzt werden. Allenfalls im geschäftlichen Bereich ist z.B. vorstellbar, dass das Sicherheitspersonal Smartglasses zu präventiven oder repressiven Zwecken einsetzt.[1222] Sofern Privatpersonen mit Smartglasses z.B. ihr Grundstück überwachen und dabei auch den öffentlichen Raum mit erfassen sollten (weil sie z.B. ihrer Kopfbewegung folgend den Straßenbereich miterfassen), wird es sich dabei insoweit nicht mehr nur um die Wahrnehmung des eigenen Hausrechts handeln.[1223]

(2) Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

Die Wahrnehmung berechtigter Zwecke gem. § 6b Abs. 1 Nr. 3 BDSG entspricht dem Zulässigkeitstatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, sodass die zu dieser Vorschrift entwickelten Grundsätze entspre-

---

[1218] Zwar ist das Hausrecht als ein eigener Tatbestand normiert, stellt aber zugleich auch eine Wahrnehmung des berechtigten Interesses der Gefahrenabwehr i.S.d. § 6b Abs. 1 Nr. 3 BDSG dar, weswegen die Zulässigkeit und Interessensabwägung der Videoüberwachung an dortiger Stelle einheitlich geprüft werden kann, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 285.

[1219] *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 34.

[1220] *Gola/Schomerus*, BDSG, § 6b, Rn. 16; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 73.

[1221] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 286; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 75; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 38.

[1222] Vgl. *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 61; *Weichert*, DuD 2000, S. 662 (667).

[1223] Vgl. BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); *Gola/Schomerus*, BDSG, § 6b, Rn. 16; so auch im Fall von "Dashcams" in Fahrzeugen, *Lachenmann/Schwiering*, NZV 2014, S. 291 (292); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 286; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 37.

chend herangezogen werden können.[1224] Etwaige verbleibende Zweifelsfälle und Unklarheiten sind hierbei im Hinblick auf die gem. § 6b BDSG restriktiv geregelte Videoüberwachung zulasten der Beobachtenden auszulegen.[1225]

(a) Arten berechtigter Interessen

Die Arten der berechtigten Interessen sind selbst nicht beschränkt und können z.B. rechtlicher, wirtschaftlicher oder ideeller Natur sein.[1226] Im Fall der Nutzung von Smartglasses kommen vor allem die im Rahmen verfassungsrechtlicher Prüfung festgestellten Interessen in Frage.[1227]

Zu den verfassungsrechtlich geschützten Interessen gehören vor allem die körperliche Unversehrtheit, das Eigentum, die Informations-, Kunst- und Wissenschaftsfreiheiten sowie die allgemeine Handlungsfreiheit.[1228] Jedoch enthält der restriktiv konzipierte Begriff der berechtigten Interessen i.S.d. § 6b Abs. 1 Nr. 3 BDSG bereits eine kodifizierte Interessenabwägung, welche Motive wie Neugierde, Bequemlichkeit oder Hobby im Hinblick auf das hohe Schutzgut des Rechts auf informationelle Selbstbestimmung generell als Rechtfertigung einer Videoüberwachung ablehnt.[1229] Das gilt erst recht für eine Motivation, die von vornherein darauf ausgerichtet ist, die Rechte der Betroffenen zu beeinträchtigen, wie z.B. Stalking oder Erpressung.[1230] Dagegen stellt die medizinisch indizierte Nutzung von Smartglasses ein berechtigtes Interesse dar.[1231] Die bloße Berufung auf die Informationsfreiheit als Grundlage der Meinungsbildung wird hingegen kein berechtigtes Interesse begründen können. Mit der Regelung des § 41 BDSG hat der Gesetzgeber eine gesetzliche Vorabwertung vorgenommen, die ein berechtigtes Interesse im Fall einer journalistisch-redaktionellen Tätigkeit sieht und diese bereits aus dem Anwen-

---

1224 *Bergfink*, DuD 2015, S. 145 (148); *Duhr u.a.*, DuD 2002, S. 1 (28); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 78; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 41.

1225 *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 77.

1226 *Duhr u.a.*, DuD 2002, S. 1 (28); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 78.

1227 Vgl. E III, S. 136.

1228 Vgl. E III, S. 136.

1229 Vgl. zur Einschränkung auf "das absolut Notwendige", EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196); ebenfalls sind Motive wie Kunst oder Wissenschaft prinzipiell geschützt, wobei ein berechtigtes Interesse regelmäßig ausscheidet, wenn die Videoüberwachung außerhalb eigener Geschäftsbereiche erfolgt, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 292 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 78; *v. Zezschwitz*, in: Handbuch Datenschutzrecht, 2003, Kap. 9.3. Rn. 102.

1230 *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 78; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 43.

1231 Vgl. E III. 4, S. 146.

dungsbereich des BDSG herausnimmt.[1232] Nur in Ausnahmefällen, z.B. im Fall eines überragenden öffentlichen Interesses, ist eine Ausnahme für nicht journalistische Informationsbeschaffung vorstellbar, die jedoch keinen Fall typischer Nutzung von Smartglasses darstellt.

Ein berechtigtes Interesse an der Nutzung von Smartglasses kommt vor allem bei Gefahrenabwehr oder Sicherung von Beweismitteln, z.B. Schutz vor Vandalismus, Raubüberfällen oder Diebstahl, in Frage.[1233] Erforderlich ist jedoch eine objektive Begründbarkeit der Gefährdungslage, die sich auf einzelfallbezogene Tatsachen stützen kann.[1234] Daneben ist auch die Berufung auf eine abstrakte Gefährdungslage ausreichend, wenn diese der Lebenserfahrung nach typischerweise gefährlich ist und dies substantiiert, z.B. unter Nennung konkreter Vorfälle, belegt werden kann.[1235] Auch der repressive Einsatz zur Sicherung von Beweismitteln in einem zivilrechtlichen Verfahren ist vom berechtigten Interesse umfasst.[1236] Jedoch ist zu beachten, dass ausgehend von der Rechtsprechung selbst mehrere Straftaten, die im öffentlichen Raum begangen wurden, zumindest in Fällen des Vandalismus nicht automatisch dessen Videoüberwachung rechtfertigen, sondern weiterer konkreter Anhaltspunkte der Wiederholung bedürfen.[1237] Ebenso sind lange zurückliegende Delikte, wie z.B. eine zweieinhalb Jahre zurückliegende Körperverletzung, nicht ausreichend, um eine hinreichende Gefahrenlage zu begründen.[1238] Eine abstrakte Gefahrenvorsorge, z.B. eine möglichen allgemeinen Gefahren vorbeugende Abschreckung, ist dagegen nicht ausreichend.[1239] Das gilt z.B., wenn Bildmaterial

---

[1232] Vgl. *Caspar*, NVwZ 2010, S. 1451 (1456); *Gola/Schomerus*, BDSG, § 41, Rn.4; *Westphal*, in: *Taeger/Gabel*, BDSG, § 41, Rn. 1; *Zscherpe*, in: Ebenda, § 6b, Rn. 43.

[1233] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 291 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 79.

[1234] BT-DrS. 14/5793, S. 61; AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; *Duhr u.a.*, DuD 2002, S. 1 (28); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 79.

[1235] BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531); BAG, Urt. v. 21.6.2012 (2 AZR 153/11), NJW 2012, 3594 (3596 f.); BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 288 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 79 f.

[1236] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 81.

[1237] OLG Düsseldorf, Beschl. v. 5.1.2007 (3 Wx 199/06), NJW 2007, 780 (781); KG Berlin, Beschl. v. 26.6.2002 (24 W 309/01), NJW 2002, 2798; OLG Karlsruhe, Urt. v. 8.11.2001 (12 U 180/01), NZM 2002, 703 (704); *Lachenmann/Schwiering*, NZV 2014, S. 291 (295).

[1238] OLG Düsseldorf, Beschl. v. 5.1.2007 (3 Wx 199/06), NJW 2007, 780 (781).

[1239] OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545; AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 80.

für künftige, nicht näher definierte Zwecke beschafft wird und dabei unbeteiligte Dritte erfasst werden.[1240] Umgekehrt ist aber auch kein konkreter Beleg für eine schwerwiegende Beeinträchtigung eines Schutzgutes erforderlich, da die Prüfung der Intensität des Eingriffs die Interessenabwägung vorwegnehmen und die Interessen des Schutzgutberechtigten verkürzen würde.[1241]

Aufgrund der hohen Anforderungen an das Vorliegen einer Gefahrenlage stellt die Nutzung von Smartglasses zur Stärkung des allgemeinen Sicherheitsgefühls kein berechtigtes Interesse i.S.d. § 6b Abs. 1 Nr. 3 BDSG dar.[1242] Auch die politisch motivierte Förderung eines „Sousveillance"-Konzeptes fußt auf keiner konkreten Gefahrenlage und scheidet als berechtigtes Interesse ebenfalls aus.[1243] Ein berechtigtes Interesse würde dagegen vorliegen, wenn der Nutzer von Smartglasses z.B. in eine akute Gefahrensituation gerät, in der er einen ihn oder sein Eigentum gefährdenden Angreifer wegen des erhöhten Risikos nachträglicher Überführung abschrecken und für den Fall des Angriffs Beweise erstellen möchte.[1244] Auch wenn z.B. ein Park durchquert werden soll, in dem mehrere, zeitlich nahe Übergriffe auf Personen verübt worden sind, wird eine hinreichende Gefahrenlage und damit ein berechtigtes Interesse an der Nutzung von Smartglasses gegeben sein.

Ferner ist zu berücksichtigen, dass es sich um berechtigte Interessen des Trägers von Smartglasses handeln muss. Interessen Dritter oder der Öffentlichkeit sind dagegen nicht nach § 6b Abs. 1 Nr. 3 BDSG gerechtfertigt.[1245] Jedoch kann die Wahrnehmung fremder Interessen eine eigene Aktivität darstellen, die insoweit schützenswert wäre.[1246] In Frage kommt z.B. eine Nothilfehandlung in konkreter Situation.[1247]

[1240] AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; *v. Zezschwitz*, in: Handbuch Datenschutzrecht, 2003, Kap. 9.3. Rn. 104.

[1241] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 288 f.

[1242] Vgl. B III. 1, S. 35; allgemeine Gefahren des Straßenverkehrs als berechtigtes Interesse am Einsatz der Videoüberwachung mittels von Dashcams, verneinente das AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; vgl. *Bergfink*, DuD 2015, S. 145 (149); *Horst*, NZM 2000, S. 937 (942); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 291.

[1243] Vgl. E III. 1. a) dd), 142.

[1244] Vgl. AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291; VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (238); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 72 ff.

[1245] LG Bonn, Urt. v. 7.1.2015 (5 S 47/14), ZD 2015, 434 (435); *Simitis*, in: *Simitis*, BDSG, § 28, Rn. 105.

[1246] Vgl. *Simitis*, in: *Simitis*, BDSG, § 28, Rn. 106.

[1247] Vgl. ebenda.

(b) Konkrete Festlegung des Zwecks

Die Zwecke der Videoüberwachung müssen vorab konkret festgelegt werden, wodurch die verantwortliche Stelle zu einer sorgfältigen Prüfung der Rechtmäßigkeit veranlasst wird.[1248] Der Zweck darf nicht allgemein, z.B. als „Gefahrenabwehr", beschrieben, sondern muss präzise benannt werden.[1249] Hiermit wird auch die Zweckbindung der Daten initiiert.[1250] Eine Schriftform ist zwar gem. § 6b BDSG nicht erforderlich, kann sich jedoch bei meldepflichtigen automatisierten Datenverarbeitungen aus der Notwendigkeit eines Verfahrensverzeichnisses gem. § 4g Abs. 2 i.V.m. § 4e Satz 1 Nr. 4 BDSG ergeben.[1251] Die Schriftform kann jedoch entbehrlich sein, wenn sich der Zweck der Videoüberwachung in einem einfachen Fall eindeutig ergibt, wie z.B. der Ausrichtung einer Kamera auf einen Kassenbereich, wenn nur der Eigentümer Zugang zu der Kamera hat.[1252]

Bei der Nutzung von Smartglasses durch Privatpersonen ist nicht damit zu rechnen, dass die Nutzer die Einsatzzwecke vorab fixieren werden. Im Fall medizinisch indizierter Nutzung werden sie sich jedoch im Regelfall aus den Umständen ergeben, ebenso wie beim Einsatz in konkreten Gefahrensituationen.[1253] Darüber hinaus wird ohnehin kein Fall eines berechtigten Zwecks i.S.d. § 6b Abs. 1 Nr. 3 BDSG vorliegen.

(c) Erforderlichkeit

Es ist anhand konkreter und objektiver Umstände im Einzelfall zu prüfen, ob die Videoüberwachung zu der Verfolgung des berechtigten Interesses erforderlich ist.[1254] Dazu ist entsprechend dem allgemeinen rechtlichen Verständnis im ersten Schritt zu untersuchen, ob die Maßnahme zur Verfolgung des berechtigten Zweckes geeignet ist, und anschließend im zweiten Schritt, ob dafür kein anderes, gleich wirksames, aber den Betroffenen weniger in seinen Rechten beeinträchtigendes Mittel zur Verfügung steht.[1255] Da neben dem speziellen Ausnahmefall medizinischer Nutzung der Einsatz von Smartglasses nur in Gefahrensituationen in

---

[1248] BT-DrS. 14/5793, S. 61; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 82.

[1249] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 82.

[1250] *v. Zezschwitz*, in: Handbuch Datenschutzrecht, 2003, Kap. 9.3. Rn. 79.

[1251] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 294; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 84 Fn. 217.

[1252] *Duhr u.a.*, DuD 2002, S. 1 (28).

[1253] Vgl. im Fall einer Dashcam, VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (237).

[1254] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 295; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 87.

[1255] *Gola/Schomerus*, BDSG, § 6b, Rn. 18a; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 86; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 45 ff.

Frage kommt, wird sich die nachfolgende Prüfung der Erforderlichkeit auf diese Interessen beschränken.[1256]

Im Rahmen der Prüfung der Geeignetheit ist zu untersuchen, ob die konkrete Maßnahme die Erreichung des angestrebten Zwecks zumindest maßgeblich unterstützt.[1257] Das ist nicht der Fall, wenn z.B. eine zur Gefahrenabwehr eingesetzte Videokamera für die abzuschreckenden Subjekte nicht sichtbar ist oder über tote Winkel verfügt, über die man die zu schützenden Bereiche unbesehen erreichen kann.[1258] Andererseits ist es für die Geeignetheit nicht erforderlich, dass ein umfassender Schutz gewährleistet wird.[1259] Es kann grundsätzlich davon ausgegangen werden, dass Smartglasses sich zur Abschreckung potenzieller Angreifer oder Sicherung von Beweismitteln eignen. Zwar wird deren Erkennbarkeit je nach Grad der Miniaturisierung der Technik zurückgehen können, jedoch werden ihre Träger z.B. verbal auf die Präsenz der Geräte hinweisen können.[1260] Ebenso könnten je nach Gerät die Signallampen einer aktiven Kamerafunktion in der Dunkelheit erkennbar sein. Ferner folgen Smartglasses den Kopfbewegungen ihrer Nutzer und können so auf die abzuschreckenden oder aufzunehmenden Subjekte bzw. Objekte gerichtet werden.[1261]

Bei der Prüfung der Erforderlichkeit geht es nicht darum, die „beste Lösung“ für die Betroffenen zu finden, sondern eine alternative Vorgehensweise, die zugleich möglich sowie zumutbar ist und den Eingriff in die Rechte der Betroffenen möglichst gering hält.[1262] Hierbei ist i.S.d.

1256 Soweit die Frage behandelt wird, inwieweit Aufnahmen von Smartglasses in einen Prozess als Beweise verwertbar sind, widmet sich die Untersuchung nur der Beweiswürdigung, wohingegen die spezielleren Probleme und Unterschiede zwischen Beweiserhebungs-, Beweisverwertungs- und Beweiswürdigungsverboten nicht Gegenstand der Untersuchung sind, vgl. dazu *Greger*, NZV 2015, S. 114 f.

1257 Vgl. E IV. 1, S. 149; BAG, Beschl. v. 14.12.2004 (1 ABR 34/03), NJOZ 2005, 2708 (2715); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 46.

1258 LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1068 f.); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 87; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 46.

1259 OVG Münster, Urt. v. 8.5.2009 (16 A 3375/07), RDV 2009, 232; *Gola/Schomerus*, BDSG, § 6b, Rn. 18a.

1260 Vgl. E IV. 1. g) cc), S. 157.

1261 Es wäre jedoch u.U. zu prüfen, z.B. bei schlechten Lichtverhältnissen, inwieweit die technische Qualität von Aufnahmen eine Nutzung zu Beweiszwecken erlaubt, vgl. OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545 (129); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 87; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 46.

1262 Im Fall klassischer Videoüberwachung werden an dieser Stelle z.B. alternative Schutzmaßnahmen wie die Einstellung von Sicherheitspersonal oder die Ausrichtung einer Überwachungskamera geprüft, vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 296; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 87 f.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 48.

Grundsätze der Datenvermeidung und Datensparsamkeit gem. § 3a BDSG sowohl zu prüfen, ob es erforderlich ist, Smartglasses in der konkreten Gefahrensituation einzusetzen, als auch ob der räumliche und zeitliche Umfang der Nutzung erforderlich ist.[1263] Bei der Nutzung von Smartglasses wird es sich ohnehin nur um zeitlich und räumlich begrenzte Situationen handeln, in denen überhaupt ein berechtigtes Interesse an deren Einsatz vorliegt.[1264] Ferner kann in solchen Situationen generell davon ausgegangen werden, dass die jederzeit aufnahmebereiten und permanent am Kopf getragenen Smartglasses eine höhere Abschreckungswirkung und Fähigkeit zur Sammlung von Bildbeweisen mit sich bringen als z.B. Smartphones, die auf einen Angreifer gerichtet werden müssten. Ferner stellen Foto- oder Videoaufnahmen gegenüber anderen Beweismitteln, z.B. dem Zeugenbeweis, ein offensichtlicheres und damit besser geeignetes Beweismittel dar.[1265] Ebenso ist das Gemeinwohlinteresse an einer funktionstüchtigen Rechtspflege zu beachten, welches die Gerichte anhält, grundsätzlich alle angebotenen Beweismittel zu beachten, um die Wahrheit zu ermitteln.[1266]

Die Erforderlichkeit des Einsatzes von Smartglasses kann entsprechend der verfassungsrechtlichen Prüfung grundsätzlich unterstellt werden.[1267] Allenfalls, wenn eine Gefahrensituation anderweitig und gleich wirksam abgewendet werden kann, z.B. weil Polizeibeamte vor Ort sind, wird der Einsatz von Smartglasses nicht erforderlich sein.[1268] Auch wenn die Gefahrensituation in einem Bereich stattfindet, der mit Videotechnik überwacht wird, und sichergestellt ist, dass die Überwachungskamera die Situation tatsächlich aufzeichnet, die gleiche Abschreckungswirkung ausübt bzw. die Identifizierung von erfassten Personen ermöglicht, könnte die Erforderlichkeit der Nutzung von Smartglasses abgelehnt werden. Ein solch verlässlicher Schutz wird jedoch im öffentlichen Raum nur in seltenen Ausnahmefällen vorliegen.

[1263] Vgl. LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067 (1069); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 89 ff.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 49 f.

[1264] Vgl. F II. 1. d) bb) (2) (a), S. 210.

[1265] KG, Urt. v. 5.7.1979 (12 U 1277/79), NJW 1980, 894; AG Nürnberg, Urt. v. 8.5.2015 (18 C 8938/14), BeckRS 2015, 14846; AG Nienburg, Urt. v. 20.1.2015 (4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14)), BeckRS 2015, 07708; *Balzer/Nugel*, NJW 2014, S. 1622 (1623); *Greger*, NZV 2015, S. 114 (116); *Hilpert*, RDV 2009, S. 160 (166).

[1266] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (49); *Greger*, NZV 2015, S. 114 (115).

[1267] Vgl. E IV. 2, S. 171.

[1268] Vgl. VGH München, Beschl. v. 16.10.2014 (10 ZB 13.2620), NVwZ-RR 2015, 104.

(d) Interessenabwägung

Der Spielraum für eine zulässige Videoüberwachung mithilfe von Smartglasses ist durch die strengen Anforderungen an die berechtigten Interessen bereits sehr eng gesetzt. Dennoch muss zusätzlich geprüft werden, ob keine Anhaltspunkte bestehen, die dafür sprechen, dass schutzwürdige Interessen der Betroffenen die berechtigten Interessen der Nutzer von Smartglasses überwiegen. Dabei ist es nicht notwendig, dass das Überwiegen der Interessen Betroffener positiv festgestellt wird. Vielmehr reicht bereits aus, dass Anhaltspunkte dafür, dass die Interessen Betroffener überwiegen, bei einer Betrachtung ex ante nicht ausgeräumt werden können.[1269]

Im Rahmen dieser Interessenabwägung ist zudem nicht nur das Recht der Betroffenen auf informationelle Selbstbestimmung zu berücksichtigen, sondern alle ihre Privatsphäre schützenden Ausprägungen des Allgemeinen Persönlichkeitsrechts.[1270] Die objektive Ausstrahlungswirkung des Allgemeinen Persönlichkeitsrechts, auf die sich Betroffene berufen können, fällt hierbei desto geringer aus, je eher die Belastung der Betroffenen eine Folge ihrer Entscheidungen ist, z.B. wenn sie sich als Angreifer in die Gefahrensituation begeben, und desto höher, je eher sie anlasslos zum Objekt der Beobachtung werden.[1271] Ferner sind der Ort und die Dauer des Einsatzes von Smartglasses zu berücksichtigen, sodass örtliche Rückzugsbereiche oder die Erfassung privater Informationen sich zulasten der Nutzer von Smartglasses auswirken.[1272] Ebenso wirken sich die Heimlichkeit, die Dauer der Beobachtung und die fehlende Möglichkeit, ihr auszuweichen, zulasten eines Trägers von Smartglasses aus.[1273]

Ein wesentliches Merkmal der Interessenabwägung sind die Schwere der drohenden Rechtsverletzung und die Wahrscheinlichkeit ihres Eintritts.[1274] Ausgehend von dem verfassungsrechtlichen Ergebnis, ist die

---

[1269] *Greger*, NZV 2015, S. 114 (117); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 82 f.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 52.

[1270] Vgl. E I, S. 89; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 94 f.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 51.

[1271] LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531); LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (Rn. 17); *Balzer/Nugel*, NJW 2014, S. 1622 (1624 ff.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 299; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 101.

[1272] BT-DrS. 14/5793, S. 62; *Hilpert*, RDV 2009, S. 160 (164); *Nguyen*, DuD 2011, S. 715 ff.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 99 ff.

[1273] Vgl. LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 95 ff.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 58.

[1274] Vgl. *Lackner*, in: *Lackner/Kühl*, StGB, § 32, Rn. 13 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 300.

Eingriffswirkung von Smartglasses derart hoch, dass nur schwere Angriffe und eine nicht anders abwendbare Gefährdung der Persönlichkeitsrechte, der körperlichen Integrität, nicht nur unerheblicher Eigentumswerte, oder der Existenzgrundlagen, deren Einsatz als Verteidigungsmittel rechtfertigen können.[1275] D.h., es wird sich um Situationen handeln müssen, die eine zivil- und strafrechtliche Notwehr- oder notwehrähnliche Lage bei erheblicher Eingriffsintensität, wie drohender Körperverletzung,[1276] erpresserischer Drohung, Ehrverletzungen oder Angriffen auf die berufliche Existenz begründen.[1277]

Zum selben Ergebnis gelangten Gerichte bei Dashcams, die im Hinblick auf den Aspekt der Mobilität mit Smartglasses vergleichbar sind. Dabei wurden vor allem Nachteile drohender Summierungs- und gegenseitiger Aufrüstungseffekte betont.[1278] So wurde die Verwertbarkeit von Aufnahmen aus Dashcams durch das LG Heilbronn und das AG München verneint, weil deren Anerkennung als Beweismittel zu einer Verbreitung von Überwachungskameras in Kraftfahrzeugen und damit zu einer jeder Kontrolle entzogenen privaten Überwachung oder sogar biometrischen Auswertung führen könnte.[1279] Damit würde die informationelle Selbstbestimmung praktisch aufgegeben werden.[1280] Das gelte auch für eine mittels Sensoren automatisch ausgelöste Beobachtung, die z.B. auf ein bestimmtes Verhalten reagiert, da Betroffene weder erkennen, wann die Aufnahme ausgelöst wird, noch wie sie sich verhalten müssen, um die

---

1275 Vgl. E IV. 2. a), S. 172; die Zulässigkeit der Überwachung eines Autostellplatzes wegen einer möglichen Sachbeschädigung am Fahrzeug trotz vorhergehenden Schadens im Wert von 5.400 Euro wurde abgelehnt, wenn damit zugleich die Nutzer anderer Stellflächen erfasst werden würden, OLG Düsseldorf, Beschl. v. 5.1.2007 (3 Wx 199/06), NJW 2007, 780 (781).

1276 OLG Düsseldorf, Urt. v. 5.5.1997 (5 U 82/96), NJW-RR 1998, 241.

1277 Vgl. die durch die Rechtsprechung aufgestellten Kriterien für die Verletzung von Persönlichkeitsrechten, BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (50); BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238 (250); BGH, Urt. v. 27.1.1994 (I ZR 326/91), NJW 1994, 2289 (2292 f.); BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277 (278); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (287 f.); OLG Düsseldorf, Urt. v. 5.5.1997 (5 U 82/96), NJW-RR 1998, 241; BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436 (3437); der Einsatz alleine zur Verfolgung von Ordnungswidrigkeiten, wird für eine Rechtfertigung der Videoüberwachung als nicht ausreichend erachtet, *Hilpert*, RDV 2009, S. 160 (165); vgl. *Horst*, NZM 2000, S. 937 (942); zum Begriff der "notwehrähnlichen Lage" vgl. *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 55 ff.

1278 Vgl. E IV. 1. k) cc) (1), S. 165.

1279 LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (233 f.); AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291.

1280 LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (234).

Auslösung nicht zu aktivieren, sodass sie sich ihr im Ergebnis nicht entziehen können.[1281]

Das AG Nienburg ließ dagegen die Aufnahme einer Dashcam als Beweismittel zu.[1282] Das Besondere an dem Fall war jedoch, dass der Autofahrer die Dashcam in einer Gefahrensituation punktuell einschaltete. Dabei verwies das Gericht darauf, dass die abstrakten Gefahren einer Veröffentlichung der Aufnahmen nicht berücksichtigt werden können, da sie bei gefertigten Beweismitteln immer bestehen.[1283] Ferner darf „die dem Einwand zugrundeliegende abstrakte Furcht vor allgegenwärtiger Datenerhebung und dem Übergang zum Orwell'schen Überwachungsstaat […] nicht dazu führen, dass den Bürgern sachgerechte technische Hilfsmittel zur effektiven Rechtsverfolgung und Rechtsverteidigung kategorisch vorenthalten werden."[1284] Ähnlich entschied das AG Nürnberg, welches in einer fragwürdigen Entscheidung auf die Einschüchterungswirkung der Dashcams gar nicht einging und beim Mitfilmen von Passanten nur eine anonyme „technikbedingte Miterfassung ohne Erkenntnisgewinn" als auch einen „Beweisnotstand" des Dashcam-Verwenders sah.[1285] Ebenso abzulehnen ist eine frühere Entscheidung des AG München, wonach eine mittels einer Helmkamera eines Radfahrers erstellte Videoaufnahme als Beweismittel verwertbar ist, da sie mit einer Urlaubsaufnahme, bei der Dritte nur zufällig ins Bild gerieten, vergleichbar sei.[1286] Die Entscheidung kann allenfalls mit dem Umstand erklärt werden, dass die Aufnahme sich letztendlich zulasten des beweisführenden Radfahrers auswirkte.

Zu bedenken ist jedoch, dass die auf Dashcams oder eine Helmkamera bezogenen Entscheidungen sich auf den Einsatz der Videoüberwachung im Straßenverkehr beziehen.[1287] Der Straßenverkehr ist jedoch typischerweise der Raum einer auf die Fortbewegung konzentrierten Handlungsweise und im Hinblick auf die freie individuelle Entfaltung von Individuen nicht mit dem öffentlichen Raum, den Träger von Smartglasses nutzen, vergleichbar. Ebenso ist durch die Fortbewegung und gewisse Fixierung

---

[1281] LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531); *Lachenmann/Schwiering*, NZV 2014, S. 291 (295).

[1282] AG Nienburg, Urt. v. 20.1.2015 (4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14)), BeckRS 2015, 07708.

[1283] Ebenda.

[1284] Ebenda.

[1285] AG Nürnberg, Urt. v. 8.5.2015 (18 C 8938/14), BeckRS 2015, 14846.

[1286] AG München, Urt. v. 6.6.2013 (343 C 4445/13), NJW-RR 2014, 413 (414 f.).

[1287] Vgl. AG Nienburg, Urt. v. 20.1.2015 (4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14)), BeckRS 2015, 07708.

auf den Straßenbereich vor den Fahrzeugen die Gefahr der längeren Ausrichtung auf bestimmte Personen geringer.[1288] D.h., die beeinträchtigende Wirkung durch Smartglasses in einer Fußgängerzone ist wesentlich höher zu werten als durch Dashcams oder Helmkameras im Straßenverkehr.[1289] Daher können die Entscheidungen des AG Nürnberg und des AG München sowie des AG Nienburg grundsätzlich nicht auf Smartglasses übertragen werden. Ebenso wäre eine punktuelle Zuschaltung der Smartglasses nur in Gefahrensituationen, anders als im Fall des AG Nienburg, wenig glaubhaft.[1290]

Zusammenfassend ist festzustellen, dass das Interesse der Nutzer von Smartglasses nur in extremen Gefahrensituationen deren Nutzung auf Grundlage des § 6b Abs. 1 Nr. 3 BDSG rechtfertigen wird. Die sich daraus ergebende Berechtigung, Smartglasses nur zeitlich und örtlich punktuell zu deren Abwehr im öffentlichen Raum aufsetzen zu dürfen, wird daher im Hinblick auf die Nutzung von Smartglasses als permanente technische Begleiter keine praktisch wesentliche Bedeutung haben.

cc) Kenntlichmachung der Beobachtung entsprechend § 6b Abs. 2 BDSG

Gemäß § 6b Abs. 2 BDSG hat die verantwortliche Stelle bestimmte Hinweispflichten zu erfüllen, wozu insbesondere die Kenntlichmachung der Videoüberwachung und die Unterrichtung über die Identität der erhebenden Stelle gehören. Als geeignete Hinweise gelten üblicherweise Piktogramme oder Hinweistafeln.[1291] Ferner kann sich die Überwachung auch aus den Umständen ergeben, z.B. wenn eine deutlich erkennbare Kamera im Kassenbereich eines Geschäfts eingesetzt wird.[1292] Bei mobiler Beobachtung könnten die Träger der Kameras, wie z.B. im Fall von Bo-

---

[1288] Vgl. BVerfG, Beschl. v. 20.5.2011 (2 BvR 2072/10), NJW 2011, 2783 (2785); VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (238); *Greger*, NZV 2015, S. 114 (115).

[1289] Vgl. AG Berlin-Mitte, Urt. v. 18.12.2003 (16 C 427/02), NZM 2004, 318 (319).

[1290] In dem Fall könnte dem Betreiber der Dashcam wohl deswegen Glauben geschenkt worden sein, weil er im Verfahren nicht als Partei, sondern als Zeuge auftrat, AG Nienburg, Urt. v. 20.1.2015 (4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14)), BeckRS 2015, 07708.

[1291] *Balzer/Nugel*, NJW 2014, S. 1622 (1627); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 312; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 105 f.; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 65 f.

[1292] Vgl. *Duhr u.a.*, DuD 2002, S. 1 (29); *Gola/Schomerus*, BDSG, § 6b, Rn. 23; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 109; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 65.

dycams der Polizei, Westen oder ähnliche Kleidungsstücke mit einer Aufschrift „Videoüberwachung“ anziehen.[1293]

Im Fall von privat genutzten Smartglasses ist nicht damit zu rechnen, dass deren Nutzer freiwillig derartige Hinweise tragen werden. Ganz im Gegenteil ist eher davon auszugehen, dass ihnen wegen des Argwohns Dritter daran gelegen ist, die Smartglasses möglichst unauffällig zu nutzen.[1294] Ebenso ist nicht anzunehmen, dass die Betroffenen Smartglasses anhand der Umstände erkennen werden, bevor sie in deren Erfassungsbereich geraten.[1295] Das gilt erst recht für die Identität ihrer Träger. Zu denken wäre allenfalls an eine Art elektronische Datenschutzerklärung, die mittels der Smartglasses automatisch an den Betroffenen mit Angaben zum Umfang der Beobachtung und Identität des Nutzers übermittelt werden würde.[1296] Hierfür müssten jedoch zuerst entsprechende Übermittlungsverfahren geschaffen und unter allen Betroffenen verbreitet sein.

Die fehlende Bereitschaft entsprechender Kennzeichnung dürfte auch durch den Mangel direkter Sanktionen bekräftigt werden, da § 6b Abs. 2 BDSG nach herrschender Meinung keine Zulässigkeitsvoraussetzung der Videoüberwachung darstellt.[1297] Ebenso wenig kann sie gem. §§ 43, 44 BDSG mit Bußgeldern bzw. Strafen sanktioniert werden.[1298] Auch eine Anordnung durch Datenschutzbehörden nach § 38 Abs. 5 Satz 1 BDSG scheidet aus, da die Kennzeichnungspflicht nicht im Katalog der Sicherungsmaßnahmen des § 9 BDSG aufgeführt ist.[1299] Ein fehlender Hinweis kann sich daher nur mittelbar auswirken, indem er die Beeinträchtigungswirkung der Smartglasses durch die Intransparenz ihrer Nutzung

---

[1293] Innenminister Boris Rhein: „Body-Cam“ verhindert Gewalt gegen Polizeibeamte, Hessisches Ministerium des Innern und für Sport, https://innen.hessen.de/presse/pressemitteilung/innenminister-boris-rhein-body-cam-verhindert-gewalt-gegen-polizeibeamte (5.7.2014); *Mann/Niedzviecki*, Cyborg, 2002, S. 115.

[1294] Vgl. C II. 3, S. 68.

[1295] Zum Erfordernis rechtzeitigen Vorabhinweises, *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 68.

[1296] *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 160 f.

[1297] BAG, Urt. v. 21.6.2012 (2 AZR 153/11), NJW 2012, 3594 (3597 f.); LAG Hamm, Urt. v. 15.7.2011 (10 Sa 1781/10), BeckRS 2011, 79152 (79152); LAG Köln, Urt. v. 18.11.2010 (6 Sa 817/10), NZA-RR 2011, 241 (243); m.w.N. *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 110; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 70; a.A. vertritt u.a. LG Detmold, wenn es die Erfüllung der Kennzeichnung als formelle Voraussetzung rechtmäßiger Videoüberwachung gem. § 6b BDSG bezeichnet, LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531).

[1298] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 311.

[1299] VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (238 f.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 314; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 110; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 70.

erhöht.[1300] Diese Folge dürfte für die Nutzer von Smartglasses jedoch geringer erscheinen, als sich offen dem Argwohn Dritter auszusetzen.[1301]

dd) Zulässigkeit der Verarbeitung und Nutzung von nach § 6b Abs. 1 BDSG erhobenen Daten

Die Zulässigkeit der Verarbeitung und Nutzung der nach § 6b Abs. 1 BDSG erhobenen Daten muss gem. § 6b Abs. 3 BDSG für sich gesondert geprüft werden.[1302] Da die weiteren Verwendungsphasen nur im Rahmen des ursprünglichen Zwecks erfolgen dürfen, müssen sie durch das für die Beobachtung festgelegte berechtigte Interesse gerechtfertigt werden.[1303] Die Änderung des Zwecks ist gem. § 6b Abs. 3 Satz 2 BDSG auf eine erforderliche Übermittlung der Daten an staatliche Stellen zu Zwecken der Gefahrenabwehr oder Strafverfolgung beschränkt.[1304]

Folglich muss gem. § 6b Abs. 3 Satz 1 BDSG wie im Fall der Erhebung nach Abs. 1 geprüft werden, ob die Verarbeitung und Nutzung der mittels Smartglasses erhobenen Daten erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.[1305] Als berechtigtes Interesse kommt an dieser Stelle praktisch nur die medizinisch indizierte Nutzung in Frage, die z.B. der Erkennung von Personen oder Objekten zur Unterstützung sehbeeinträchtigter Personen dient. Für die zulässige Abschreckung von potenziellen Angreifern ist im Regelfall keine weitere Verwendung von Daten erforderlich, es sei denn, die Situation rechtfertigt eine Übermittlung der Daten in einem Live-Stream an Dritte, die z.B. als Zeugen dienen sollen. Dasselbe gilt, wenn die Gefahrenabwehr oder Verfolgung von Rechtsverstößen eine Übermittlung von Aufnahmen an zuständige staatliche Stellen erforderlich macht.[1306]

Änderungen gegenüber einer zulässigen Erhebung von Daten können sich dann ergeben, wenn die Beeinträchtigung der Interessen Betroffener z.B. durch die Art und Dauer der Speicherung oder Verbreitung der erho-

---

[1300] Vgl. ausführlich zum Personenbezug von Daten unten, F II. 1. d) bb) (2) (c), S. 214; *Lachenmann/Schwiering*, NZV 2014, S. 291 (293); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 70.

[1301] Vgl. E IV. 1. g) cc), S. 157.

[1302] *Duhr u.a.*, DuD 2002, S. 1 (29); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 113; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 73.

[1303] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 115.

[1304] Ebenda, § 6b, Rn. 124.

[1305] *Duhr u.a.*, DuD 2002, S. 1 (29); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 116; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 77 f.

[1306] Die Übermittlung zu diesen Zwecken wäre ohnehin gem. § 6b Abs. 3 Satz 2 BDSG zulässig; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 322; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 124; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 74 f.

benen Daten steigt. Z.B. wäre eine Verbreitung oder Veröffentlichung von Aufnahmen für die Rechtsdurchsetzung grundsätzlich nicht erforderlich.[1307] Ebenso sind der Umfang und die Dauer der Speicherung der erhobenen Daten relevant, sodass z.B. situationsgebundene Auslösemechanismen mit einem Ringspeicher, bei dem die Sekunden vor dem Auslösevorgang (sog. „Voralarmbilder“) gespeichert werden, im Vergleich zu einer dauerhaft laufenden Aufnahme weniger beeinträchtigend sind.[1308]

ee) Löschung von Daten gem. § 6b Abs. 5 BDSG

Nach § 6b Abs. 5 BDSG sind die personenbezogenen Daten unverzüglich zu löschen, sobald sie zur Verfolgung der ursprünglichen Zwecke nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.[1309] Die Löschung erfordert also eine Prüfung des angefallenen Foto- oder Videomaterials, die einzelfallbedingt ist und je nach Ansicht innerhalb von 24 bis 48 Stunden verlangt oder gar erst nach zehn Tagen für praktikabel gehalten wird.[1310] Bei der berechtigten Erhebung der Daten als Beweismittel wird die Löschung zumindest so lange nicht erforderlich sein, wie die Aufnahmen für die Rechtsverfolgungszwecke benötigt werden.[1311]

Für den Löschungsvorgang bestehen keine gesetzliche Vorgaben, wobei jedoch beachtet werden muss, dass scheinbar gelöschte Daten in vielen Fällen aus Datenträgern wiedergewonnen werden können und eine wirksame Löschung generell das Überschreiben der alten Datenfragmente mit neuen Daten erforderlich macht.[1312] Ein solches Verfahren ist bei Smartglasses nicht zu erwarten, da diese wie grundsätzlich alle Computergeräte die Daten zuerst aus dem Systemindex entfernen und nach und nach mit anderen Daten überschreiben.[1313]

[1307] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 325 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 122.

[1308] Zu sog. "Black Box"-Systemen, LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233 (Rn. 17); *Balzer/Nugel*, NJW 2014, S. 1622 (1623 f.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 325 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 119.

[1309] Wurden die Daten unberechtigt erhoben, ergibt sich die Pflicht zu deren Löschung unmittelbar aus § 35 Abs. 2 Nr. 1 BDSG; *Golla/Herbort*, GRUR 2015, S. 648 (650).

[1310] OVG Lüneburg, Urt. v. 29.9.2014 (11 LC 114/13), NJW 2015, 502 (508); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 330; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 140 f.; zehn Tage lt. *Taeger*, ZD 2013, S. 571 (577); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 97.

[1311] *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 93.

[1312] BT-DrS. 14/5793, S. 63.

[1313] *Weichert*, in: *Kilian/Heussen*, Computerrecht, 1. Abschn., Teil 13, Mat.Allg.DatenschutzR, VIII. Rn. 103.

Neben einer unsicheren Löschung besteht für Betroffene die Gefahr, dass deren Daten bereits auf einen Cloud-Speicher transferiert worden sind. Aus diesem Grund muss der Nutzer von Smartglasses die wirksame Löschung der widerrechtlich erhobenen Daten schriftlich nachweisen.[1314]

ff) Hinweispflicht gem. § 6b Abs. 4 BDSG

§ 6b Abs. 4 BDSG bestimmt, dass die Betroffenen entsprechend §§ 19a, 33 BDSG über eine Datenverarbeitung oder Nutzung informiert werden müssen, sobald durch Videoüberwachung erhobene Daten ihnen zugeordnet werden. Die Zuordnung muss jedoch tatsächlich erfolgt und nicht nur möglich sein, da sich ansonsten eine Identifizierungspflicht ergeben würde.[1315] In diesem Fall muss die betroffene Person über die Speicherung oder Nutzung, die Art der Daten, den Zweck ihrer Erhebung, die Verarbeitung und die Nutzung sowie die Identität der verarbeitenden Stelle und etwaige Übermittlungen unterrichtet werden. Eine Mitteilungspflicht kann jedoch in den im § 33 Abs. 2 Satz 1 BDSG genannten Fällen ausgeschlossen sein. Bei der Nutzung von Smartglasses kommt insbesondere die Nr. 7 a) zum Tragen, die eine Benachrichtigung entfallen lässt, wenn die Daten aus allgemeinen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig wäre.

Über die Reichweite des Begriffs einer allgemeinen Quelle herrscht keine Einigkeit. Nach einer Ansicht ist die verfassungsrechtliche Bedeutung maßgeblich und umfasst solche Quellen, die nach ihrer technischen Ausgestaltung und Zielsetzung sich dazu eigenen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[1316] Dazu gehören insbesondere der öffentliche Raum und die Beobachtung von Personenmerkmalen, die „im sozialen Umgang typischerweise nicht verborgen werden und im Wege der menschlichen Wahrnehmung ohne weiteres zu verarbeiten sind".[1317] D.h., die der räumlichen Privatsphäre zugeordneten Bereiche oder private Informationen stellen grundsätzlich keine allgemein zugänglichen Quellen dar.[1318] Nach einer strengen Ansicht können Personen dagegen grundsätzlich keine allgemeine Informationsquelle sein und ihr Aufenthalt im öffentlichen Raum dient nicht dazu, einem nicht individuell bestimmten Personenkreis Informationen über sich zu vermitteln.[1319] Als vermittelnder Maßstab kommt die im § 23 Abs. 2 KUG kodi-

---

[1314] Vgl. OLG Frankfurt a.M., Beschl. v. 22.5.2006 (11 W 13/06), GRUR-RR 2007, 30 f.

[1315] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 316.

[1316] Vgl. E III. 1. a) bb), S. 139.

[1317] Vgl. E III. 1. a) bb), S. 139; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 318 ff.

[1318] Vgl. E III. 1. a) bb), S. 139; Ebenda ff.

[1319] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 136.

fizierte Wertung in Frage, wonach Menschen nur als Beiwerke oder im Zusammenhang mit Ereignissen der Zeitgeschichte sowie als Teil von Versammlungen, Aufzügen und ähnlichen Vorgängen abgebildet werden dürfen. Dagegen kann nicht angenommen werden, dass sich heutzutage jede Person im öffentlichen Raum mit der Erfassung durch Videokameras einverstanden erklärt.[1320]

Ferner ist die Ausnahme des § 33 Abs. 2 Satz 1 Nr. 7 a) BDSG ohnehin durch den Grundsatz eingeschränkt, dass die Benachrichtigung wegen der Vielzahl der Fälle unverhältnismäßig sein müsste. Eine Vielzahl der Fälle ist jedoch nicht zu erwarten, da die Zuordnung der Daten zu bestimmten Personen i.d.R. nicht häufig passieren bzw. in Gefahrensituationen für etwaige Angreifer erkennbar sein wird.[1321] Nur dann kann die Verletzung der Hinweispflicht gem. § 6b Abs. 4 BDSG mit einem Bußgeld gem. § 43 Abs. 1 Nr. 8 BDSG geahndet werden. Die fehlende Unterrichtung kann jedoch keinen Schadensersatzanspruch der Betroffenen begründen, da die Hinweispflicht keine Zulässigkeitsvoraussetzung für erlaubnispflichtige Maßnahmen ist.[1322]

e) Unzulässigkeit der Videoüberwachung mithilfe von Smartglasses

Die typische und alltägliche Nutzung von Smartglasses im öffentlichen Raum stellt im Ergebnis unabhängig von der konkreten Art der Nutzung eine Videoüberwachung i.S.d. § 6b Abs. 1 BDSG dar. Der Grund liegt darin, dass auf die objektive Wirkung der Smartglasses abzustellen ist, die aus der Sicht der Betroffenen jederzeit zu Zwecken der Aufzeichnung eingesetzt werden könnten. Zwar mögen die Nutzer von Smartglasses nur in Ausnahmefällen Aufzeichnungen von Menschen erstellen wollen. Jedoch werden sie praktisch jederzeit Aufnahmen erstellen oder das Geschehen mittels Live-Streamings übertragen können, was dazu führt, dass die Betroffenen sich ähnlich wie bei traditionellen Überwachungskameras der Entscheidungsgewalt der Nutzer von Smartglasses ausgeliefert fühlen dürften.

Eine derartige Videoüberwachung wird wegen ihrer durch Intransparenz, Streubreite, Anlasslosigkeit sowie Gefahr von Summierungseffekten begründeten Eingriffsintensität nur in äußersten Ausnahmefällen als letztes Mittel zur Abwehr von erheblichen Gefahren oder Verfolgung der sich aus ihnen ergebenden Rechtsverstöße in punktuellen Situationen zulässig sein. Als weitere Ausnahmen kommen eine ebenfalls nur in Aus-

---

[1320] A.A. im Hinblick auf den Straßenverkehr, AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291.

[1321] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 320.

[1322] Ebenda, 341 f.

nahmefällen denkbare medizinisch indizierte Nutzung oder der Einsatz an abgelegenen Orten, an denen mit der Erfassung von Menschen nicht zu rechnen ist, in Betracht. In diesen Fällen wird jedoch bereits eine rein persönliche und familiäre Nutzung anzunehmen sein, die gem. § 1 Abs. 2 Nr. 3 BDSG die Anwendbarkeit des § 6b BDSG entfallen lässt. Darüber hinaus wird dieser Anwendungsausschluss aufgrund der vorstehend geschilderten Einschüchterungswirkung von Smartglasses nicht einschlägig sein. Demzufolge wird die Nutzung von Smartglasses im öffentlichen Raum im Regelfall eine gem. § 6b BDSG unzulässige Videoüberwachung darstellen.

f) Verhältnis des § 6b Abs. 1 BDSG zu anderen Vorschriften

Aufgrund der Feststellung, dass die Nutzung von Smartglasses im öffentlichen Raum sowie die Verwendung der hierbei erhobenen personenbezogenen Daten praktisch immer dem Regelungsbereich des § 6b BDSG unterfallen wird, stellt sich die Frage, ob und in welchem Umfang andere Vorschriften daneben einschlägig sein können. Diese Frage lässt sich jedoch nicht einfach beantworten, da das Verhältnis des § 6b BDSG zu anderen in vergleichbaren Konstellationen in Frage kommenden Regelungen sehr komplex ist und einer sorgfältigen Einzelfallbetrachtung bedarf.[1323]

Innerhalb des Regelungsbereichs des BDSG ist der § 6b BDSG im Fall der Videoüberwachung im öffentlichen Raum spezieller gegenüber anderen Erlaubnisnormen der Datenverarbeitung durch nicht öffentliche Stellen gem. §§ 28 bis 32 BDSG.[1324] Im Verhältnis zu Regelungen außerhalb des BDSG ergibt sich aus § 1 Abs. 3 Satz 1 BDSG, dass diese § 6b BDSG verdrängen können, wenn sie in dem zu beurteilenden Fall als spezieller anzusehen sind.[1325] Da die Kriterien für einen derartigen Vorrang nicht vorgegeben sind, müssen sie, wie z.B. im Fall der Vorschriften der §§ 22 ff. KUG, anhand des Sinns und Zwecks einschlägiger Vorschriften beurteilt werden.[1326] So soll das KUG bei Verbreitung und Zurschaustellung von Personenabbildungen einschlägig sein, während die Herstellung

---

[1323] *Gola/Schomerus*, BDSG, § 6b, Rn. 4; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 5; auf der Ebene der Auslegung der Tatbestandsmerkmale einzelner Vorschriften besteht dagegen kein Konkurrenzverhältnis, so dass insbesondere die durch unterschiedlichen Gerichtsbarkeiten entwickelten Grenzen und Grundlagen der Videoüberwachung, generelle Geltung entfalten, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 343.

[1324] *Gola/Schomerus*, BDSG, § 6b, Rn. 4; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 332; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 64 f.

[1325] *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 5.

[1326] *Lachenmann/Schwiering*, NZV 2014, S. 291 (293); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 12.

und übrige Verwendung der Abbildungen (wozu z.B. eine Verarbeitung zur Erzeugung einer Augmented Reality zu zählen wäre) dem § 6b BDSG zugeordnet wird.[1327] Im Übrigen wird § 6b BDSG als eine neben anderen Bereichsvorschriften anzuwendende Komplementärvorschrift betrachtet, wenn es um die Geltendmachung von Rechten Betroffener im Rahmen einer Abwehr von Videoüberwachungsmaßnahmen geht.[1328]

2. Andere Erlaubnistatbestände des BDSG

Die Nutzung von Smartglasses durch Privatpersonen eröffnet zwar gem. § 27 Abs. 1 Nr. 1 BDSG die Anwendbarkeit der Erlaubnisvorschriften des § 28 Abs. 1 Satz 1 BDSG, jedoch werden diese im Regelfall von der spezielleren Regelung des vorliegend einschlägigen § 6b BDSG verdrängt.[1329] Damit scheidet eine Nutzung von Smartglasses auf Grundlage gesetzlicher Erlaubnistatbestände des BDSG im Regelfall aus, weswegen der verbleibenden Möglichkeit einer Einwilligung der Betroffenen gem. §§ 4 Abs. 1, 4a BDSG besondere Beachtung geschenkt werden muss.

a) Erlaubnistatbestände des § 28 Abs. 1 Satz 1 BDSG

Die Vorschriften des § 28 Abs. 1 Satz 1 BDSG können zur Anwendung gelangen, wenn die Nutzung von Smartglasses keine Beobachtung darstellt, z.B. weil diese ähnlich wie Smartphones oder Fotokameras lediglich punktuell eingesetzt würden.[1330] Hierbei würde es sich jedoch zum einen um keine typische Nutzung von Smartglasses handeln.[1331] Zum anderen würde es sich bei vereinzelten Schnappschüssen, sofern diese nicht als Beweismittel dienen sollen, um eine typische persönliche und familiäre Nutzung handeln, die aus dem Regelungsbereich des BDSG ohnehin gem. § 1 Abs. 2 Nr. 3 BDSG ausgenommen wäre.[1332]

An eine Heranziehung des § 28 Abs. 1 Satz 1 BDSG wäre allenfalls im Fall einer nicht optisch-elektronischen Erhebung personenbezogener Daten, z.B. bei rein akustischer Aufzeichnung, zu denken. Jedoch ist zu beachten, dass § 6b BDSG bei der Nutzung von Smartglasses vor allem aufgrund der objektiv gegebenen und unabhängig von einer tatsächlich stattfindenden Videoüberwachung einschlägig ist.[1333] D.h., auch wenn

---

[1327] Vgl. LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233; *Balzer/Nugel*, NJW 2014, S. 1622 (125); *Golla/Herbort*, GRUR 2015, S. 648 (651); *Lachenmann/Schwiering*, NZV 2014, S. 291 (293); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 12.

[1328] BT-DrS. 14/4329, S. 38; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 5.

[1329] Vgl. F II. 1. f), S. 225.

[1330] Vgl. F II. 1. d) aa) (2), S. 205.

[1331] Vgl. B III, S. 35.

[1332] Vgl. F II. 1. c) cc) (2) (e), S. 201.

[1333] Vgl. F II. 1. d) aa) (2), S. 205.

lediglich eine Audioaufzeichnung erstellt wird, wird sie als Bestandteil der Videoüberwachung nach den Maßstäben des § 6b BDSG zu beurteilen sein.[1334] Ansonsten könnte die Vorschrift des § 6b BDSG einfach umgangen werden, obwohl sich das Eingriffspotenzial der Videoüberwachung mit der zusätzlichen Informationsdichte aufgrund der Erhebung von akustischen, Standort- oder sonstigen Daten steigert.[1335]

Eine Anwendung des § 28 Abs. 1 Satz 1 BDSG käme ferner in Betracht, wenn die Voraussetzungen des § 6b BDSG als nicht erfüllt anzusehen wären. Z.B. wandte das AG Nienburg im Fall einer Aufzeichnung des Verkehrsgeschehens mittels einer Dashcam den § 28 Abs. 1 Satz 1 Nr. 1 BDSG an, da es den § 6b BDSG bei mobiler Videoüberwachung als nicht einschlägig ansah.[1336] Ein solcher Rückfall ist jedoch nicht notwendig, wenn wie im Rahmen dieser Untersuchung auch die mobile Videoüberwachung dem § 6b BDSG zugeordnet wird. Ferner stehen auch die bei der privaten Nutzung einschlägigen Zulässigkeitstatbestände des § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG unter dem Vorbehalt entgegenstehender schutzwürdiger Interesse des Betroffenen. D.h., die hohe Eingriffswirkung von Smartglasses wird entsprechend § 6b BDSG im Regelfall auch im Rahmen der Vorschriften des § 28 Abs. 1 BDSG der Zulässigkeit ihrer Nutzung entgegenstehen.

b) Einwilligung nach §§ 4 Abs. 1, 4a BDSG

Die Prüfung des § 6b BDSG zeigte, dass eine gesetzliche Erlaubnis der Nutzung von Smartglasses praktisch nicht möglich ist und es daher bei dem Verbot ihrer Nutzung im öffentlichen Raum gem. § 4 Abs. 1 BDSG bleibt. Vor diesem Hintergrund verbleibt lediglich die Möglichkeit, Smartglasses mit der Einwilligung von Betroffenen gem. §§ 4 Abs. 1, 4a BDSG zu nutzen. Der Einwilligungstatbestand des § 4a BDSG stellt eine Umsetzung des Art. 7 lit. a) der EG-DSRL dar, die laut Art. 2 lit. h) der EG-DSRL eine Einwilligung als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden“, definiert.

[1334] Vgl. *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 64 f.

[1335] Vgl. *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 17.

[1336] Das Gericht wandte § 28 Abs. 1 Satz 1 Nr. 1 BDSG an, da es in dem Festhalten einer verkehrsgefährlichen Lage eine Nutzung der Dashcam im Rahmen eines rechtsgeschäftlichen Verhältnisses, nämlich der Schadensminderung im Rahmen des Versicherungsverhältnisses, sah, AG Nienburg, Urt. v. 20.1.2015 (4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14)), BeckRS 2015, 07708.

aa) Freie Entscheidung der einwilligenden Person

Entsprechend dem Ergebnis der verfassungsrechtlichen Prüfung kommt eine Einwilligung nur dann in Frage, wenn die Betroffenen sich dabei nicht der durch die Menschenwürde gem. Art. 1 Abs. 1 GG geschützten Subjektsqualität begeben.[1337] Diese Vorgabe findet sich in der Voraussetzung einer gem. § 4a Abs. 1 Satz 1 BDSG auf freier Entscheidung beruhenden Einwilligung wieder.

(1) Kein unmittelbarer oder mittelbarer Zwang

Eine freiwillige Einwilligung setzt voraus, dass die Betroffenen eine echte Wahl treffen, d.h. im Zuge der Einholung der Einwilligung nicht vor vollendete Tatsachen gestellt werden und eine realistische Möglichkeit zur Verweigerung oder zum Widerruf der Einwilligung haben, ohne hierdurch Nachteile zu erleiden.[1338] Hiermit sind nicht nur Zwangssituationen gemeint, in denen Gewalt angedroht wird, sondern auch solche, in denen sich die Betroffenen in einer Situation befinden, die sie faktisch dazu zwingt, sich mit der Datenverarbeitung einverstanden zu erklären.[1339] Auch mittelbare Zwänge, z.B. ein sozialer Druck, dem sich eine Person nicht entziehen kann, können die Freiwilligkeit ausschließen.[1340] Ein solcher Zwang ist vor allem dann anzunehmen, wenn es der Person nicht zuzumuten ist, sich der Teilnahme am gesellschaftlichen Leben wegen mangelnder Einwilligung zu entziehen.[1341] Solche Fälle kommen jedoch weniger bei typischem privatem Einsatz von Smartglasses, sondern eher in besonderen Konstellationen, wie dem Arbeitsumfeld oder im Rahmen von Veranstaltungen, in Frage.

(2) Bewusstsein der Tragweite und Bestimmtheit der Einwilligung

Eine auf freier Entscheidung basierende Einwilligung setzt voraus, dass die einwilligende Person sich der vollen Tragweite der Einwilligung bewusst ist, also deren Umfang und deren Folgen abschätzen kann.[1342] Denn nur wenn ihr die Folgen ihres Verhaltens bekannt sind, kann ihre Entscheidung als autonom bezeichnet werden. Daher müssen der einwilli-

---

[1337] Vgl. E II. 2. d) aa), S. 134; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 5.

[1338] Art. 29-Datenschutzgruppe, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, 2093-01/05/DE, 2005, S. 13; *Gola/Schomerus*, BDSG, § 4a, Rn. 19.

[1339] *Gola/Schomerus*, BDSG, § 4a, Rn. 22; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 21, Fn. 62.

[1340] *Möncke*, DuD 2015, S. 617 (621); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 62 ff.; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 55.

[1341] Vgl. *Möncke*, DuD 2015, S. 617 (621); *Schmitt Glaeser*, ZRP 2000, S. 395 (399).

[1342] Vgl. E II. 2. d) bb), S. 135; *Gola/Schomerus*, BDSG, § 4a, Rn. 25; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 20.

genden Person z.B. auch die Risiken des Datenumgangs, in den sie einwilligt, bekannt sein.[1343]

Bereits dieser Punkt stellt die Einwilligung in die Erfassung durch Smartglasses vor erhebliche Probleme. Denn die Einwilligenden müssten die Art, den Umfang als auch den Zweck sowie mögliche Folgen der Beobachtung durch Smartglasses kennen und verstehen.[1344] Die erste Hürde würde bereits darin bestehen, dass die Einwilligenden die Smartglasses als solche sowie deren mögliche Funktionen erkennen müssten. Davon ist gegenwärtig nicht auszugehen, denn alleine, dass Smartglasses als neuartige und sich von einer typischen Korrekturbrille unterscheidende Vorrichtung erkannt werden, bedeutet nicht, dass auch deren technischer Hintergrund erfasst wird.

Die hohen Anforderungen an die Erkennbarkeit von Smartglasses werden zudem dadurch gesteigert, dass auch deren konkrete Nutzung für die Einwilligenden erkennbar sein muss.[1345] Ein diffuses Gefühl, dass eine Art der Erfassung stattfinden könnte, oder ein Schätzen „ins Blaue hinein" ist zu pauschal und nicht ausreichend.[1346] Es wird daher zu fragen sein, mit welcher Art der Nutzung der Smartglasses die Einwilligenden rechnen mussten. Z.B. könnten Betroffene bei hinreichender Verbreitung von Augmented-Reality-Funktionen davon ausgehen, dass sie für deren Zwecke als Objekte im physischen Raum registriert werden. Dagegen müssten sie nicht davon ausgehen, dass ihre Abbildung dauerhaft gespeichert, verbreitet, veröffentlicht, an Dritte live übertragen oder biometrisch ausgewertet werden.[1347]

Ferner müssen sich die Betroffenen auch der Risiken der Erfassung durch Smartglasses bewusst sein. Hierzu gehört, dass den Einwilligenden die Möglichkeit der informatorischen Auswertung ihrer Aufnahmen, z.B. einer biometrischen Erkennung, bekannt sein muss. Zu bedenken ist auch, dass die Übermittlung der erfassten Daten an Dritte, vor allem in Länder ohne ein entsprechendes datenschutzrechtliches Schutzniveau, und fehlende Kenntnis, wie diese Daten verarbeitet werden können, sowie

---

[1343] Art. 29-Datenschutzgruppe, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, 2093-01/05/DE, 2005, S. 14.

[1344] Vgl. *Gola/Schomerus*, BDSG, § 4a, Rn. 26 f.

[1345] Vgl. *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 21; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 30.

[1346] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 198.

[1347] Vgl. E II. 2. d) bb), S. 135.

die Unmöglichkeit, sich nachträglich dagegen zu wehren, eine Einwilligung zumindest nach mancher Ansicht, generell ausschließen könnte.[1348]

(3) Einwilligungsfähigkeit

Eine freie Entscheidung der Einwilligenden setzt voraus, dass diese über die notwendigen geistigen Fähigkeiten verfügen, um die Tragweite der Einwilligung überblicken zu können.[1349] Bei der Nutzung von Smartglasses im öffentlichen Raum ist davon auszugehen, dass häufig auch minderjährige Personen erfasst werden, denen nur eine durch den Grad ihrer geistigen Reife beschränkte Einwilligungsfähigkeit zugestanden wird.[1350] Unabhängig von der Frage, ab wann eine für die Einwilligungsfähigkeit nötige geistige Reife vorliegt, muss ohnehin davon ausgegangen werden, dass häufig auch Minderjährige unter den diskutierten Grenzen von 15 oder 16 Jahren erfasst werden.[1351] Vor dem Hintergrund der vorstehend geschilderten Risiken der Verbreitung und Veröffentlichung der durch Smartglasses erhobenen Daten werden zudem sehr hohe Anforderungen an die Einwilligungsfähigkeit der Minderjährigen zu fordern sein, die in Zweifelsfällen eher für deren Fehlen sprechen werden.[1352] Neben den Minderjährigen kann die Einwilligungsfähigkeit auch bei anderen Personen, wie z.B. stark Betrunkenen, fehlen.[1353]

[1348] Vgl. EuGH, Urt. v. 6.10.2015 (C-362/14), MMR 2015, 753; eine Einwilligungsmöglichkeit gem. § 4c Abs. 1 Nr. 1 BDSG vor dem Hintergrund des Urteils des EuGH zum Datentransfer in die USA verneinend, ULD, Positionspapier des ULD zum EuGH Urteil vom 6.10.2015, 2015, https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf (18.10.2015), S. 3; vgl. *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 15.

[1349] OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087; *Libertus*, ZUM 2007, S. 621 (624).

[1350] *Gola/Schomerus*, BDSG, § 4a, Rn. 2a; *Wintermeier*, ZD 2012, S. 210 (2012 ff.).

[1351] *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 29, Fn. 47; allenfalls als Orientierungspunkte und Mindestgrenzen dienen die Regelungen der § 36 SGB I (wonach sozialrechtliche Handlungsfähigkeit mit 15 Jahren festgelegt wird), § 40 Abs. 4 AMG (wonach Einwilligungen in Arzneimitteltests das Alter von 16 Jahren voraussetzen) und § 2229 BGB (der eine Eheschließung ab Vollendung des 16. Lebensjahres erlaubt), vgl. OLG Hamm, Urt. v. 20.9.2012 (4 U 85/12), K&R 2013, 53 (56); *Gola/Schomerus*, BDSG, § 4a, Rn. 25; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 29, Fn. 47.

[1352] Vgl. F II. 2. b) aa) (2), S. 229; zu beachten ist ferner, dass auch wenn die Einwilligung durch die Erziehungsberechtigten abgegeben wird, die Minderjährigen im Rahmen einer "Doppelzuständigkeit" ihr widersprechen können, *Libertus*, ZUM 2007, S. 621 (624); *von Zimmermann*, Die Einwilligung im Internet, 2014, S. 152, 170 f.

[1353] Vgl. E II. 2. d) bb), S. 135; OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087.

(4) Sensible Daten

Werden besondere Arten personenbezogener Daten i.S.v. § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt, muss ich die Einwilligung ausdrücklich auf diese Daten beziehen.[1354] Zu diesen Daten gehören insbesondere mit der rassischen und ethnischen Herkunft oder der Gesundheit Informationen, die durch Smartglasses erfasst werden können.[1355] Allerdings ergibt sich aus Art. 8 Abs. 2 lit. e) der EG-DSRL, dass Daten, die eine Person offenkundig öffentlich macht, nicht als besonders sensibel einzustufen sind. Folglich werden die Aufnahmen eines Gesichts im öffentlichen Raum keine besonders sensiblen Daten umfassen, sodass ein gesonderter Hinweis nicht notwendig ist.[1356] Das ist sachgerecht, denn wer z.B. damit einverstanden ist, von einer ca. einen Meter entfernten Kamera aufgenommen zu werden, wird im Regelfall erahnen, dass die Aufnahme z.B. Krankheitssymptome in seinem Gesicht oder seine Ethnie erfasst.

bb) Form der Einwilligung

Die Einwilligung bedarf gem. § 4a Abs. 1 Satz 3 BDSG i.V.m. §§ 125, 126 BGB grundsätzlich der Schriftform, um wirksam zu sein.[1357] Die Schriftform soll nicht nur dem Nachweis der Einwilligung dienen, sondern hat wegen der Warn- und Bedenkfunktion eine Schutzwirkung zugunsten der Einwilligenden.[1358]

(1) Mündliche Einwilligung

Bei der typischen alltäglichen Nutzung von Smartglasses wird eine schriftliche Einwilligung eher die Ausnahme darstellen, genauso wie z.B. Nutzer von Smartphones im Regelfall keine schriftliche Einwilligung einholen, wenn sie eine Person fotografieren. Dies führt nicht zwangsläufig zur Unwirksamkeit der Einwilligung, da die Schriftform aufgrund besonderer Umstände entfallen kann.[1359] Dementsprechend ist eine mündliche Einwilligungserklärung möglich, wobei jedoch zu bedenken ist, dass sie aufgrund ihres Ausnahmecharakters möglichst restriktiv auszulegen ist.[1360]

[1354] Vgl. *Gola/Schomerus*, BDSG, § 4a, Rn. 34.

[1355] Vgl. E IV. 1. c), S. 151.

[1356] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 108.

[1357] *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 26, 35; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 33.

[1358] *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 33; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 33.

[1359] *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 43.

[1360] Vgl. LG Darmstadt, Urt. v. 24.9.1998 (15 O 204/98), RDV 1999, 28; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 44 f.

Angesichts des zumindest gegenwärtig hohen Umfangs der für eine Einwilligung vorausgesetzten Aufklärung der Betroffenen über Zweck, Art und Umfang sowie Risiken ihrer Erfassung, erscheint es eher unwahrscheinlich, dass Nutzer von Smartglasses eine wirksame mündliche Einwilligung einholen und erst recht werden nachweisen können.

(2) Schlüssige Einwilligung

Neben einer mündlichen Einwilligung könnte auch eine konkludente Einwilligung eingeholt werden, z.B. wenn eine Person sich bewusst in den Erfassungsbereich einer Datenbrille hineinbegeben würde. Ob eine konkludente Einwilligung zulässig ist, ist aufgrund deren Ausnahmecharakters gem. § 4a Abs. 1 Satz 3 BDSG umstritten.[1361] Jedoch gibt Art. 7 lit. a der EG-DSRL keine Form vor, sodass eine konkludente Einwilligung aufgrund der richtlinienkonformen Auslegung der Vorschrift möglich ist, wenn sie ohne jeden Zweifel abgegeben wird.[1362] Konkludente Einwilligungen kommen nur bei Vorliegen spezieller Umstände in Frage, z.B. wenn es auch im Sinne der einwilligenden Personen ist, die Einwilligung möglichst schnell und zeitnah zu erklären.[1363] Erforderlich ist, dass ein bestimmtes Verhalten in einem solchen Maße üblich und geradezu selbstverständlich ist, dass entsprechend dem Grundgedanken der §§ 133, 157 BGB nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte vernünftigerweise nur von einer Einwilligung des Betroffenen ausgegangen werden kann.[1364] Insbesondere kann allein deshalb, weil ein Verhalten verbreitet ist, nicht auf eine schlüssige Einwilligung geschlossen werden, wenn nicht zugleich festgestellt wird, dass in den beteiligten Kreisen ein fehlender Widerspruch zugleich als eine Einwilligung gedeutet wird.[1365] Dementsprechend erscheint die Wahrscheinlichkeit einer schlüssig wirk-

---

[1361] Bejahend, OLG Frankfurt a.M., Urt. v. 13.12.2000 (13 U 204/98), CR 2001, 294 (296); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 333; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 41; verneinend, BVerfG, Beschl. v. 23.2.2007 (1 BvR 2368/06), NVwZ 2007, 688 (690); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 44.

[1362] Vgl. zur generellen Möglichkeit konkludenter Einwilligungen, BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (45); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 333; *Piltz*, Soziale Netzwerke im Internet, 2013, S. 133 ff.; so im Ergebnis *Vulin*, ZD 2012, S. 414 (417 f.); *von Zimmermann*, Die Einwilligung im Internet, 2014, S. 63 ff.

[1363] *Buschbaum/Rosak*, ZD 2015, S. 354 (356); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 44.

[1364] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (45 f.); mit Verweis auf BGH, Urt. v. 10.7.1991 (VIII ZR 296/90), BGHZ 115, 123 (126 ff.); und BGH, Urt. v. 20.5.1992 (VIII ZR 240/91), NJW 1992, 2348 (2349); *Gola/Schomerus*, BDSG, § 4a, Rn. 2; *Libertus*, ZUM 2007, S. 621.

[1365] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (45 f.); mit Verweis auf BGH, Urt. v. 8.6.1989 (I ZR 178/87), NJW 1989, 2820; und BGH, Urt. v. 4.12.1992 (6 U 32/92), NJW-RR 1993, 753.

sam erklärten und nachweisbaren Einwilligung noch geringer als bei deren mündlicher Erklärung.

(3) Mutmaßliche und stillschweigende Einwilligung

Der mögliche Verzicht auf die Schriftform bezieht sich nur auf die Form der Erklärung, jedoch nicht auf das Vorliegen einer Einwilligung an sich.[1366] Eine mutmaßliche Erklärung wird daher nicht als Rechtfertigungstatbestand herbeigezogen werden können, da es auf die tatsächliche Willensbildung bei der betroffenen Person ankommt.[1367] Ebenso wird eine stillschweigende Erklärung eines inneren Einverständnisses nicht genügen, da es ihr an einer Willenskundgebung nach außen hin mangelt.[1368]

Mutmaßliche und stillschweigende Einwilligungen sind jedoch von Fällen zu unterscheiden, in denen eine formgerechte Einwilligung im Hinblick auf einen konkreten Sachverhalt abgegeben wurde und dieser Sachverhalt unverändert fortdauert.[1369] In diesem Fall geht es jedoch weniger um die Frage der Form der Einwilligung als um ihre Reichweite oder Wiederholung in der Zukunft.[1370]

cc) Nutzung von Smartglasses bei Veranstaltungen

Aufgrund der strengen gesetzlichen Anforderungen und sozialen Vorbehalte ist damit zu rechnen, dass Smartglasses nur innerhalb beschränkter räumlicher Bereiche eingesetzt werden. Vorstellbar sind z.B. Veranstaltungen, innerhalb derer die Nutzung von Smartglasses ausdrücklich erlaubt wird. In Frage kommen z.B. Sportveranstaltungen, Konzerte, Messen, Museen, Geschäftsstätten, Büros oder Freizeitlokalitäten wie Bars oder Clubs, aber auch räumlich offene Bereiche, wie z.B. ein Strandabschnitt.[1371] Bei derartigen Veranstaltungen könnte z.B. ein Schild am Eingang aufgehängt werden, das darauf hinweist, dass innerhalb des Veranstaltungsbereichs Smartglasses verwendet werden dürfen und die sich innerhalb des Bereichs aufhaltenden Besucher sich mit dem Einsatz von

---

1366 *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 43.

1367 Vgl. *Libertus*, ZUM 2007, S. 621 (624); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 44; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 46; *von Zimmermann*, Die Einwilligung im Internet, 2014, S. 93 ff.

1368 *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 44.

1369 *Gola/Schomerus*, BDSG, § 4a, Rn. 29a.

1370 Vgl. F II. 2. b) dd), S. 236.

1371 Vgl. *Schleeh*, Mit Google Glass und iPad im Museum - Augmented Reality, Schleeh.de, http://schleeh.de/mit-google-glass-und-ipad-durch-das-museum-augmented-reality/ (18.10.2015).

Smartglasses für Aufnahmen, Augmented Reality oder gar biometrische Erfassung einverstanden erklären.[1372]

Derartige Einwilligungen müssen jedoch zum einen die vorgenannten Anforderungen an die Freiwilligkeit, Bestimmtheit und Form erfüllen.[1373] Das stellt die Veranstalter vor besondere Schwierigkeiten, da sie die Einwilligungen als Boten im Namen der sich vor Ort befindlichen Nutzer von Smartglasses einholen und daher deren mögliche Nutzungen der Smartglasses abdecken müssten.[1374] Die Wirksamkeit der Einwilligung würde zudem voraussetzen, dass die Nutzer von Smartglasses sich an ihren Umfang halten. Sind die Räumlichkeiten nicht bis zur Kopfhöhe der Menschen umzäunt, muss zudem beachtet werden, dass die Einwilligungen die Betroffenen außerhalb dieser Stätten und Räume umfassen könnten, z.B. wenn Träger von Smartglasses Menschen auf einem anderen Strandabschnitt oder auf der öffentlichen Straße beobachten. Eine derartige Erfassung wäre nicht durch die räumlich begrenzte Einwilligung gerechtfertigt.

Ferner ist zu fragen, ob allein das Betreten einer für die Nutzung von Smartglasses zugelassenen Räumlichkeit als eine Einwilligung zu verstehen ist. Nach Ansicht des Bundesverfassungsgerichts stellt das Betreten eines Teils des öffentlichen Raums trotz Hinweisen auf Videoüberwachungsmaßnahmen keine wirksame Einwilligung dar, da das Unterlassen eines Protests gegen die Maßnahme „nicht stets mit einer Einverständniserklärung gleichgesetzt werden kann".[1375] Eine konkludente Handlung soll dagegen zu einer Einwilligung führen können, wenn sie durch eine aktive Handlung hinreichend gekennzeichnet ist.[1376] So wird in Übereinstimmung mit der Entscheidung des Bundesverfassungsgerichts eine hinreichende schlüssige Erklärung der Einwilligung beim Betreten einer Räumlichkeit, wie z.B. einer Diskothek oder eines Taxis, zumindest dann angenommen, wenn zugleich deutlich gemacht wurde, dass das Betreten dieser Räume als eine Einwilligung in Videoüberwachung aufgefasst wird.[1377] Dabei ist die Einwilligung nicht in einem fehlenden Widerspruch gegen die Datenerfassung, sondern in der schlüssigen Handlung des Betretens der Räumlichkeit zu sehen.[1378] Allerdings ist der Vorgang so zu

---

[1372] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 334.

[1373] Vgl. BVerfG, Beschl. v. 23.2.2007 (1 BvR 2368/06), NVwZ 2007, 688 (690).

[1374] Vgl. *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 30 f.; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 18.

[1375] BVerfG, Beschl. v. 23.2.2007 (1 BvR 2368/06), NVwZ 2007, 688 (690).

[1376] *Piltz*, Soziale Netzwerke im Internet, 2013, S. 143 ff.

[1377] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 334.

[1378] *Gola/Schomerus*, BDSG, § 4a, Rn. 41.

gestalten, dass die Betroffenen ähnlich wie im Fall einer schriftlichen Einwilligung hinreichend Zeit haben, um die Tragweite ihrer Entscheidung zu würdigen, bevor sie den Bereich betreten.[1379] Dies wäre nicht der Fall, wenn die Personen z.B. in einer sich schnell bewegenden Menschenmenge an Schildern, die auf die Einwilligung in die Nutzung von Smartglasses hinweisen, „verbeigeschleust" werden würden.[1380]

Eine freie Entscheidung wäre ferner anzuzweifeln, wenn deren Erfordernis den Besuchern erst nach einer Anreise zu der Veranstaltung mitgeteilt werden würde. In diesem Fall wäre aufgrund der Vorbemühungen, wie des Erwerbs von Tickets, der Reservierung eines Termins und Anreise sowie ggf. Verabredung mit Freunden, eine soziale Zwangslage der Teilnehmer anzunehmen. In einer solchen Zwangslage wäre es nicht unüblich, wenn die Personen ohne Rücksicht auf die Risiken zur Erklärung einer Einwilligung bewegt werden würden.[1381] D.h., dass ein schlüssiges Handeln keine Einwilligung begründet, wenn die einwilligende Person faktisch keine Wahl hat, als den von der Einwilligung umfassten räumlichen Bereich aufzusuchen. Umgekehrt können länger vorab mitgeteilte Informationen einen ausreichenden Überlegungszeitraum bieten. Auf die Schriftform der Einwilligung kann dagegen generell verzichtet werden, da es unangemessen wäre, sie von jedem Gast zu fordern, bevor er eine Lokalität betritt.[1382] Ferner müssen die Grenzen der Einwilligungsfähigkeit für Minderjährige beachtet werden, als auch dass die Einwilligung freiwillig erfolgt.

D.h., auf eine Pflicht zur Einwilligung mit der Nutzung von Smartglasses durch Dritte müsste bereits im Rahmen der Ankündigung von Veranstaltungen oder Einladungen zur Örtlichkeiten deutlich hingewiesen werden, damit die Einwilligungen als freiwillig gelten und wirksam sind. Dabei würde ein Hinweis in den AGB nicht ausreichen, da solche Einwilligungen zumindest gegenwärtig nicht der Üblichkeit entsprechen und eine überraschende und unwirksame Klausel gem. § 305c Abs. 1 BGB darstellen würden; es sei denn eine derartige Einwilligungsklausel wäre aufgrund der Art der Veranstaltung zu erwarten (z.B. bei einer Technikmesse).

[1379] Vgl. F II. 2. b) bb), S. 231; *Buschbaum/Rosak*, ZD 2015, S. 354 (356).

[1380] Ebenda.

[1381] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 333; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 56.

[1382] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 334.

dd) Zeitliche Dauer der Einwilligung

Die Einwilligung muss entsprechend § 4a Abs. 1 BDSG i.V.m. § 183 BGB bereits vor dem Beginn der Datenerhebung oder -verwendung erklärt werden.[1383] Eine nachträgliche Genehmigung gem. § 184 BGB lässt einen datenschutzrechtlichen Verstoß nicht nachträglich entfallen.[1384] Sie kann jedoch auf die Rechtsfolgen Einfluss haben und lässt insbesondere in aller Regel mögliche Schadensersatzansprüche der Betroffenen entfallen.[1385]

Die Reichweite der Einwilligung bemisst sich daran, ob und inwieweit ein Sachverhalt, welcher der Einwilligung zugrunde gelegt wurde, unverändert fortdauert.[1386] Dabei wird ausgehend von dem der Einwilligung zugrunde gelegten Zweck, der Art und dem Umfang der Datenverarbeitung im Zeitpunkt der Abgabe der Einwilligung zu urteilen sein. Als Maßstab für die Auslegung der Einwilligung wird zu fragen sein, inwieweit die Abweichung des Sachverhalts einen Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen darstellt.[1387] Z.B. könnte sich eine Person (unter Annahme ihrer hinreichenden Aufklärung) damit einverstanden erklären, dass sie z.B. beim gemeinsamen Spaziergang mit einem Träger von Smartglasses von dessen Datenbrille visuell erfasst, aufgezeichnet und den Augmented-Reality-Funktionen zugeführt wird. Findet der Spaziergang erneut statt, kann davon ausgegangen werden, dass die Einwilligung aufgrund der Sachverhaltsähnlichkeit fortwirkt. Begegnet der Träger von Smartglasses der Person dagegen auf einer abendlichen Veranstaltung, dann wird ein anderer Sachverhalt vorliegen. Z.B. könnte eine Aufzeichnung im Zusammenhang mit Alkohol, Zigaretten oder beim Zusammentreffen mit bestimmten Personen sich negativ auf die soziale Wahrnehmung der Person auswirken. Das bedeutet, dass die Abweichung im Sachverhalt eine neue Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der betroffenen Person darstellt, die nicht mehr von deren Einwilligung gedeckt wird. Darüber hinaus gilt

---

1383 *Gola/Schomerus*, BDSG, § 4a, Rn. 2; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 27; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 32.

1384 OLG Köln, Urt. v. 12.6.1992 (19 U 154/91), NJW 1993, 793 (794); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 29.

1385 *Gola/Schomerus*, BDSG, § 4a, Rn. 32; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 29.

1386 *Gola/Schomerus*, BDSG, § 4a, Rn. 29a.

1387 Vgl. OLG Koblenz, Urt. v. 20.5.2014 (3 U 1288/13), ZUM 2015, 58 (61 f.).

eine einmal erteilte Einwilligung, sofern sie nicht ausnahmsweise befristet erteilt wird, bis zu ihrer Anfechtung oder einen Widerruf.[1388]

ee) Anfechtbarkeit der Einwilligung

Eine Einwilligung kann nachträglich aufgehoben werden, wenn die betroffene Person sich in einem Irrtum befand oder getäuscht wurde.[1389] In diesem Fall kann die Einwilligung auch wegen arglistiger Täuschung oder Irrtums gem. §§ 119, 123 BGB angefochten werden.[1390] Eine Anfechtung kommt immer dann in Frage, wenn der Wille und der Anschein der Erklärung auseinanderfallen.[1391] In diesem Fall wird die Einwilligung durch eine Erklärung der Anfechtung gem. § 142 Abs. 1 BGB ex tunc, also rückwirkend, entfallen.[1392] Als Folge wird der bis dahin erfolgte Umgang mit den maßgeblichen Daten als unzulässig gelten.[1393]

ff) Widerruf der Einwilligung

Neben der Anfechtung kann die Einwilligung nach herrschendem Verständnis durch einen Widerruf als „actus contrarius" ex nunc aufgehoben werden.[1394] Sofern der Widerruf im Hinblick auf eine künftige Datenerhebung erfolgt, ist mit keinen Schwierigkeiten zu rechnen.

(1) Auswirkung auf gespeicherte Aufnahmen und übrige Daten

Schwierigkeiten könnten jedoch auftreten, wenn der Widerruf im Hinblick auf die bereits gespeicherten oder einer Verarbeitung zugeführten Daten erklärt wird und z.B. die Löschung von Bildaufnahmen verlangt wird. Problematisch wird der Widerruf vor allem in Fällen von Bildauf-

---

[1388] Allerdings soll eine Einwilligung nach Auffassung der Aufsichtsbehörden und der Rechtsprechung durch Zeitablauf ihre Wirkung verlieren, wenn ein Betroffener nicht mehr nachvollziehen kann, ob und wann er die Erklärung abgegeben hat, *Gola/Schomerus*, BDSG, § 4a, Rn. 32a; ein festgelegter Zeitraum für den Verfall existiert nicht und auch wenn er im Fall des Direktmarketings zumindest nach 17 Monaten angenommen wurde, wird er aufgrund der höheren Eingriffswirkung und Umfangs der zu erinnernden Umstände im Fall von Smartglasses nach einem weitaus kürzerem Zeitraum eintreten, vgl. LG München I, Urt. v. 8.4.2010 (17 HK O 138/10), CR 2011, 830; einen Zeitraum von zwei Jahren bei Einwilligung in E-Mailempfang als zu lang ansehend, LG Berlin, Urt. v. 2.7.2004 (15 O 653/03), MMR 2004, 688

[1389] Eine datenschutzrechtliche Einwilligung wird überwiegend als eine rechtsgeschäftliche Erklärung oder zumindest eine geschäftsähnliche Handlung betrachtet, auf die die Regelungen für Willenserklärungen entsprechend anwendbar sind, OLG Koblenz, Urt. v. 20.5.2014 (3 U 1288/13), ZUM 2015, 58 (61); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 20 m.w.N.; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 14.

[1390] *Gola/Schomerus*, BDSG, § 4a, Rn. 22; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 25.

[1391] *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 25.

[1392] *Gola/Schomerus*, BDSG, § 4a, Rn. 2; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 25.

[1393] *Gola/Schomerus*, BDSG, § 4a, Rn. 2; *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 25.

[1394] *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 102; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 81 f.

nahmen, da der datenschutzrechtliche Widerruf grundsätzlich jederzeit erklärt werden kann.[1395] Im Fall des § 22 KUG ist dagegen grundsätzlich zu fragen, ob sich die Umstände seit der Erteilung der Einwilligung so gravierend verändert haben, dass eine weitere Verbreitung oder Veröffentlichung der Aufnahme das Allgemeine Persönlichkeitsrecht des Betroffenen verletzen würde.[1396]

Bei einem Widerruf nach begonnener Datenverarbeitung wird die Abwägung der Interessen der Betroffenen und der Nutzer von Smartglasses ferner im Hinblick auf die Frage zu treffen sein, wie mit den erhobenen Daten zu verfahren ist, wobei diese im Regelfall gem. § 35 Abs. 2 Nr. 1 BDSG zu löschen sein werden.[1397] Wurden die Daten an Dritte übermittelt, sind die Dritten über den Widerruf zu informieren.[1398] Hat eine Löschung zu erfolgen, so wird der Nutzer von Smartglasses die Daten nicht nur unmittelbar von seinem Gerät, sondern auch von anderen Speicher- und Verarbeitungsorten löschen müssen, über die er mittelbar verfügen kann.[1399]

(2) Form des Widerrufs

Umstritten ist ebenfalls, ob eine besondere Form des Widerrufs notwendig ist, d.h. der Widerruf als Spiegelbild der Einwilligung ebenfalls im Regelfall schriftlich erklärt werden muss.[1400] Die strenge Formbindung

---

[1395] Vgl. OLG Düsseldorf, Urt. v. 12.7.1985 (15 U 240/84), ZIP 1985, 1319; *Golla/Herbort*, GRUR 2015, S. 648 (652); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 94 ff.

[1396] Der Widerruf darf nach manchen Ansichten nicht willkürlich erfolgen, sondern kann entsprechend den Grundsätzen von Treu und Glauben nur dann zurückgenommen werden, wenn die für die Erteilung der Einwilligung maßgebenden Gründe entfallen sind, sich wesentlich geändert oder die tatsächlichen Voraussetzungen für die Erteilung sich verändert haben, *Gola/Schomerus*, BDSG, § 4a, Rn. 38; es ist also vor dem Hintergrund der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung, den die Einwilligung rechtfertigt zu fragen, ob der betroffenen Person das Festhalten an der Einwilligung zumutbar ist (dabei wird z.T. § 42 Abs. 1 UrhG analog angewandt), OLG Koblenz, Urt. v. 20.5.2014 (3 U 1288/13), ZUM 2015, 58 (61); OLG München, Urt. v. 17.3.1989 (21 U 4729/88), NJW-RR 1990, 999 (1000); LG Oldenburg, Beschl. v. 21.4.1988 (5 S 1656/87), GRUR 1988, 694 (695); *Alexander*, ZUM 2011, S. 382 (388); *Frömming/Peters*, NJW 1996, S. 958 (959); *Golla/Herbort*, GRUR 2015, S. 648 (652); *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 99; nach anderer Ansicht sollen Einwilligungen, die gegen Entgelt erteilt wurden grundsätzlich nicht widerruflich sein, während gefälligkeitshalber erteilte Einwilligungen jederzeit widerruflich sein sollen, wodurch dem vermögensrechtlichen Umstand von bildrechtlichen Einwilligungen Rechnung getragen wird, *Ohly*, Volenti non fit iniuria, 2002, S. 353; vgl. E II. 2. a) bb) (2), S. 106.

[1397] *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 103; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 81.

[1398] *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 82.

[1399] Vgl. OLG Koblenz, Urt. v. 20.5.2014 (3 U 1288/13), ZUM 2015, 58 (60).

[1400] So, *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 96.

erscheint jedoch nicht interessengerecht, da die hohen Formanforderungen dem Schutz des Betroffenen dienen.[1401] Das bedeutet umgekehrt, dass ein Widerruf der Einwilligung vor keine derartigen Hürden gestellt werden darf, sofern er als Erklärung oder Handlung durch Nutzer von Smartglasses objektiv wahrnehmbar ist.[1402] Folglich muss auch ein mündlich oder schlüssig erklärter Widerruf, z.B. durch das Vorhalten der Hand vor die Kamera der Datenbrille oder das Sich-Abwenden einer Person, als ein Widerruf einer zuvor erteilten Einwilligung verstanden werden. Dabei müsste jedoch gem. §§ 133, 157 BGB ausgelegt werden, ob und inwieweit der Widerruf erfolgt und ob er z.B. auf eine konkrete räumlich, zeitlich oder sachlich abgrenzbare Situation beschränkt ist.[1403]

gg) Geringe Wahrscheinlichkeit einer wirksamen Einwilligung

Es erscheint zumindest gegenwärtig kaum vorstellbar, dass die Nutzung von Smartglasses im öffentlichen Raum auf Grundlage von Einwilligungen erlaubt sein wird. Auch wenn Einwilligende Smartglasses als solche erkennen, wird aus ihrem fehlenden Widerspruch mangels einer Willensbekundung nicht automatisch eine Einwilligung abgeleitet werden können. Doch auch wenn eine Person eine Einwilligung eindeutig zum Ausdruck bringt, z.B. weil von ihrer Kenntnis der Funktionen der Smartglasses auszugehen ist, wird zu fragen sein, wie weit ihre Einwilligung reicht.

Grundsätzlich kann allenfalls eine Einwilligung in die Präsenz der Smartglasses angenommen werden, also ein Einverständnis mit der von ihnen ausgehenden Überwachungswirkung. Je nachdem, wie verbreitet und bekannt der Einsatz von Augmented-Reality-Funktionen ist, kann sich die Einwilligung auch auf diese erstrecken. Dagegen werden Aufnahmen, Live-Übertragungen oder biometrische Erkennungsverfahren im Regelfall einer ausdrücklichen Einwilligung bedürfen. Dabei werden die Einwilligenden umfangreich aufgeklärt werden müssen, was innerhalb räumlich beschränkter Bereiche als möglich erscheint. Darüber hinaus, z.B. auf öffentlichen Straßen oder Plätzen, wird eine Einwilligung dagegen gegenwärtig kaum in Frage kommen, vor allem wenn Minderjährige erfasst werden. Im Ergebnis kommt auch die Einwilligung nur in Ausnahmefällen gem. §§ 4 Abs. 1, 4a BDSG als Grundlage für die zulässige Nutzung von Smartglasses im öffentlichen Raum in Frage.

[1401] Vgl. F II. 2. b) bb), S. 231.

[1402] So im Ergebnis *Gola/Schomerus*, BDSG, § 4a, Rn. 37.

[1403] Vgl. *Simitis*, in: *Simitis*, BDSG, § 4a, Rn. 97; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4a, Rn. 82.

3. Übrige Vorgaben des BDSG

Neben den Zulässigkeitstatbeständen müssen weitere Vorgaben des BDSG beachtet werden, die vor allem der Information der Betroffenen über den Umgang mit ihren Daten dienen. Wie bereits im Rahmen des § 6b Abs. 2 BDSG ist jedoch nicht davon auszugehen, dass die Nutzer der Smartglasses aufgrund der Befürchtung sozialer Nachteile die Betroffenen auf etwaige Datenerhebungen hinweisen werden.[1404] Ebenso wenig ist davon auszugehen, dass sie die folgenden Verfahrensvorgaben des BDSG beachten werden.

Nach § 4 Abs. 2 Satz 1 BDSG sind Daten grundsätzlich direkt bei Betroffenen zu erheben. Damit ist gemeint, dass die Betroffenen an der Erhebung mitwirken, was zumindest eine bewusste Duldung der Erhebung sowie Kenntnis der erhebenden Stelle und der Grundlage der Datenerhebung erfordert.[1405] Ausnahmsweise kann auf die Information der Betroffenen verzichtet werden, wenn dies einen unverhältnismäßigen Aufwand mit sich bringen würde und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Derartige Hinweise wären entsprechend den Ausführungen zur Kennzeichnungspflicht gem. § 6b Abs. 2 BDSG den Nutzern von Smartglasses jedoch möglich und auch zumutbar.[1406] Im Unterschied zu § 6b Abs. 2 BDSG ist § 43 Abs. 2 Nr. 1 BDSG mit einem Bußgeld bewehrt, wenn die Daten nicht allgemein zugänglich sind.[1407]

Die Videoüberwachung gem. § 6b BDSG löst eine Meldepflicht gem. § 4d Abs. 1 BDSG aus, die gem. Abs. 3 beim Vorliegen einer Einwilligung der Betroffenen entfällt. Da die Nutzung von Smartglasses eine hohe Beeinträchtigung für die Rechte Betroffener mit sich bringt, unterfällt sie zudem der Pflicht zur Vorabkontrolle nach § 4d Abs. 5 BDSG.[1408] Da Smartglasses ähnlich wie Smartphones höchstwahrscheinlich Daten an Cloud-Anbieter oder sonstige Dienstleister übermitteln werden, müssen im Hinblick auf die im Regelfall ohne entsprechende Einwilligung erhobene Daten die Vorgaben der Auftragsdatenverarbeitung gem. § 11 Abs. 2 BDSG bzw. §§ 4b, 4c BDSG beachtet werden.

[1404] Vgl. F II. 1. d) cc), S. 220.

[1405] *Scholz/Sokol*, in: *Simitis*, BDSG, § 4, Rn. 19 ff.; *Taeger*, in: *Taeger/Gabel*, BDSG, § 4, Rn. 59.

[1406] Vgl. F II. 1. d) cc), S. 220.

[1407] Vgl. zur allgemeinen Zugänglichkeit F II. 1. d) ff), S. 223.

[1408] BT-DrS. 14/5793, S. 62; vgl. *Balzer/Nugel*, NJW 2014, S. 1622 (1624); *Gola/Schomerus*, BDSG, § 6b, Rn. 32; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 339 f.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 149.

Ferner ist im Fall von Smartglasses, die anhand biometrischer Erkennung automatisch Entscheidungen treffen und z.B. die Betroffenen als nicht vertrauenswürdig kennzeichnen, an eine automatische Entscheidung i.S.d. § 6a BDSG zu denken. Die Vorschrift soll Menschen davor schützen, „zu Objekten von Computeroperationen" zu werden.[1409] Voraussetzung des § 6a BDSG ist, dass einzelne Persönlichkeitsmerkmale Betroffener bewertet werden und eine automatisierte Entscheidung auslösen, die erhebliche rechtliche Folgen, sowohl positiver als auch negativer Art, oder erhebliche Beeinträchtigungen für die betroffene Person zur Folge hat.[1410] Auch bei der Vertrauenswürdigkeit einer Person handelt es sich um die Bewertung eines persönlichen Merkmals und sie kann z.B. dazu führen, dass der Person ein Vertragsabschluss verweigert wird.[1411] Jedoch stellt die Kennzeichnung der jeweiligen Person selbst noch keine finale Entscheidung dar. Vielmehr liegt es grundsätzlich am Nutzer der Smartglasses, ob er z.B. mit der entsprechend gekennzeichneten Person einen Vertrag eingeht. Denn § 6a BDSG schützt nicht vor Erzeugung von Daten, die zu negativen Konsequenzen kausal führen, sondern vor fehlender Einbeziehung von Menschen in den Entscheidungsprozess.[1412] Dennoch erscheint es mit dem Fortschritt der Technik möglich, dass Entscheidungen auch ohne den Nutzer getroffen werden könnten, z.B. wenn die Entscheidung über einen elektronisch durchgeführten Vertragsschluss vollständig den Smartglasses übertragen wird.

4. Rechte der Betroffenen nach §§ 33 bis 35 BDSG

Sofern nicht bereits die Hinweis- und Löschungspflichten des § 6b BDSG einschlägig sind, können Betroffene gegenüber Nutzern von Smartglasses gem. § 35 Abs. 1 BDSG Berichtigungs- und gem. § 35 Abs. 2 bis Abs. 4 BDSG bei unzulässiger Speicherung oder Zweckentfremdung Löschungs- oder Sperrungsrechte geltend machen.[1413]

Nach § 34 BDSG können Betroffene ferner von den Nutzern der Smartglasses Auskunft über deren Identität sowie die Verwendung der erhobe-

---

[1409] *Gola/Schomerus*, BDSG, § 6a BDSG Rn. 11; *Mackenthun*, in: *Taeger/Gabel*, BDSG, § 6a, Rn. 1; *Scholz*, in: *Simitis*, BDSG, § 6a, Rn. 3.

[1410] *Gola/Schomerus*, BDSG, § 6a BDSG Rn. 2 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 227; *Mackenthun*, in: *Taeger/Gabel*, BDSG, § 6a, Rn. 7 ff.; *Möller/Florax*, MMR 2002, S. 806 (810); *Scholz*, in: *Simitis*, BDSG, § 6a, Rn. 13 ff.

[1411] Vgl. *Mackenthun*, in: *Taeger/Gabel*, BDSG, § 6a, Rn. 13; *Scholz*, in: *Simitis*, BDSG, § 6a, Rn. 21 ff.

[1412] Vgl. BT-DrS. 14/4329, S. 37; *Gola/Schomerus*, BDSG, § 6a BDSG Rn. 5 f.; *Mackenthun*, in: *Taeger/Gabel*, BDSG, § 6a, Rn. 17; *Möller/Florax*, NJW 2003, S. 2724 (2725 f.); *Scholz*, in: *Simitis*, BDSG, § 6a, Rn. 16.

[1413] Zur schriflichen Bestätigung der Löschung, vgl. F II. 1. d) ee), S. 222.

nen personenbezogenen Daten verlangen.[1414] Zwar wird eine Auskunftsanfrage „ins Blaue“ abgelehnt, jedoch setzt § 34 BDSG keine tatsächliche, sondern lediglich eine potenzielle Datenverarbeitungsmöglichkeit voraus.[1415] Diese wird bereits dann vorliegen, wenn die Betroffenen in den Erfassungsbereich der Smartglasses gelangt sind und so potenziell aufgenommen oder ihre Daten sonst erhoben und verwendet sein könnten. Wird die Auskunft bezweifelt, kann die betroffene Person bis zu einer sachgerechten Klärung die Herausgabe der Smartglasses an einen Gerichtsvollzieher als Sequester beantragen.[1416] Solche Zweifel sind anhand der Umstände zu bestimmen und können sich z.B. aufgrund des mangelnden Technikverständnisses Betroffener ergeben.

5. Rechtsfolgen der Verstöße gegen Datenschutzvorschriften

Da die Nutzung von Smartglasses im öffentlichen Raum im Regelfall entsprechend § 6b Abs. 1 BDSG datenschutzwidrig sein wird, ist zu prüfen, welche Rechtsfolgen die Verstöße auslösen können.

a) Ordnungswidrigkeit und Strafbarkeit gem. §§ 43, 44 BDSG

Der Katalog der Ordnungswidrigkeiten im Absatz 1 des § 43 BDSG umfasst nach Nummer 1 die fehlende Meldung gem. § 4d Abs. 1 BDSG als auch Mängel bei Erfüllung der Auskunftspflicht gem. § 34 BDSG. Die Verstöße gegen § 6b Abs. 1 bis 3 und 5 BDSG sind dagegen nicht im Katalog der Ordnungswidrigkeiten gem. § 43 BDSG enthalten. Jedoch kann die unbefugte Erhebung oder Verarbeitung (nicht die Nutzung) von nicht allgemein zugänglichen Daten eine Ordnungswidrigkeit gem. § 43 Abs. 2 Nr. 1 BDSG darstellen.[1417]

Die widerrechtliche Erhebung von nicht allgemein zugänglichen Daten kann ebenfalls eine Straftat darstellen, sofern der Nutzer der Smartglasses gem. § 44 Abs. 1 BDSG vorsätzlich gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern, d.h. zielgerichtet nach Entgelt strebend oder um einen anderen zu schädigen, handelt.[1418] Die Straftat wird auf Antrag verfolgt, wobei auch die Aufsichtsbehörden antragsberechtigt sind, und kann mit einer Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe geahndet werden.

[1414] *Dix*, in: *Simitis*, BDSG, § 34, Rn. 12.

[1415] Es muss eine zumindest örtliche und zeitliche Eingrenzung vorgenommen werden, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 341.

[1416] Vgl. OLG Celle, Urt. v. 8.8.1984 (13 U 44/84), afp 1984, 236 (236 ff.); vgl. *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 95.

[1417] Vgl. zur allgemeinen Zugänglichkeit F II. 1. d) ff), S. 223.

[1418] *Mackenthun*, in: *Taeger/Gabel*, BDSG, § 44, Rn. 3.

b) Maßnahmen der Aufsichtsbehörden gem. § 38 Abs. 5 BDSG

Nach § 38 Abs. 5 Satz 1 BDSG kann die zuständige Datenschutzbehörde Maßnahmen zur Beseitigung einer rechtswidrigen Videobeobachtung anordnen sowie bei schwerwiegenden Verstößen deren Untersagung verfügen.[1419] Hierzu muss die Datenschutzbehörde den Verhältnismäßigkeitsgrundsatz beachten und zuerst z.B. Teileinschränkungen anordnen.[1420] Fehlt die Zulässigkeitsgrundlage jedoch insgesamt, kann gem. § 38 Abs. 5 Satz 2 BDSG sofort die gesamte Videoüberwachung untersagt werden.[1421] Eine solche Situation wäre im Fall der Nutzung von Smartglasses im öffentlichen Raum anzunehmen. Andere Maßnahmen, die typischerweise bei Überwachungseinrichtungen angeordnet werden können, wie z.B. die Abdeckung eines Sichtbereichs oder die Beschränkung der Aufzeichnungsdauer, erscheinen bei Smartglasses als nicht praktikabel.[1422] Des Weiteren ist zu beachten, dass es sich bei § 38 Abs. 5 BDSG um eine Ermessensnorm handelt, die aufgrund der unterschiedlichen Intensitätsgrade möglicher Datenschutzverstöße keine Sollvorschrift darstellt, die ein Ermessen intendiert.[1423]

Im Hinblick auf die Bestimmtheit des Untersagungstenors forderte das VG Ansbach im Fall einer Dashcam-Nutzung die Angabe des konkreten Gerätes, z.B. mit dem Herstellernamen, dem Modell sowie der Fabrikationsnummer, da die Untersagung ansonsten nicht vollstreckbar wäre.[1424] Diese Einschränkung erscheint jedoch zumindest im Hinblick auf die hohe Beeinträchtigungswirkung von Smartglasses als zu restriktiv, da der Rechtsverstoß kerngleich mit anderen Geräten begangen werden könnte. Ferner ist eine Behörde nicht auf die Untersagung konkreter Geräte beschränkt, sondern kann auch rechtswidrige Datenverarbeitungsverfahren insgesamt untersagen, wozu die Nutzung von Smartglasses im öffentlichen Raum außerhalb von Gefahrensituationen, medizinischer Indikation oder Fällen der Einwilligung gehören kann.[1425]

Ebenfalls kann die Behörde als Beseitigungsmaßnahme gem. § 38 Abs. 5 Satz 1 die Löschung der mit den Smartglasses erhobenen personenbezogenen Daten anordnen und eine Löschungsbestätigung anfordern, wobei

---

[1419] *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 158.

[1420] *Grittmann*, in: Ebenda, § 38, Rn. 39.

[1421] *Gola/Schomerus*, BDSG, § 6b, Rn. 4; OLG Oldenburg, Urt. v. 12.3.2013 (1 A 3850/12), RDV 2013, 209 (210).

[1422] Vgl. OLG Oldenburg, Urt. v. 12.3.2013 (1 A 3850/12), RDV 2013, 209 (210); VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (237 f.).

[1423] VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (239 f.).

[1424] Ebenda, 239.

[1425] Vgl. *Petri*, in: *Simitis*, BDSG, § 38, Rn. 73.

auch in diesem Fall die zu löschenden Daten genau zu bezeichnen sind und der Entscheidung eine sachgerechte Ermessensausübung vorausgehen muss.[1426]

Wird eine Anordnung der Datenschutzbehörde nicht befolgt, so kann sie gem. § 38 Abs. 5 Satz 2 BDSG mithilfe von Zwangsgeld durchgesetzt werden. Das bedeutet zugleich, dass eine sofortige Durchsetzung der Anordnung grundsätzlich nicht vorgesehen ist.[1427] Jedoch kann die Durchsetzung sofort erfolgen, wenn die untersagte Maßnahme nicht nur nach einzelnen Gesichtspunkten, sondern insgesamt unzulässig ist.[1428] Dies ist im Regelfall auch bei der Nutzung von Smartglasses anzunehmen.

c) Schadensersatz nach § 7 BDSG

§ 7 BDSG gewährt den Betroffenen einen verschuldensabhängigen Anspruch auf den Ersatz des ihnen infolge unzulässiger oder unrichtiger Datenerhebung, Verarbeitung oder Nutzung entstandenen materiellen Schadens.[1429] Als solche Schäden kommen im Regelfall nur die Kosten der Rechtsverfolgung in Frage.[1430] Als Rechtsfolge des § 7 BDSG stehen den Betroffenen neben Zahlungsansprüchen auch Ansprüche auf Beseitigung oder Unterlassung bei Erstbegehungs- oder Wiederholungsgefahr zu, wenn rechtswidrige Zustände weiterhin fortdauern.[1431] Dies wäre z.B. ein Anspruch auf die Löschung der auf einer Datenbrille gespeicherten oder an Dritte übermittelten Daten.[1432] Zu beachten ist ferner die Schuldvermutung zulasten des Trägers von Smartglasses, der sich bei gleichzeitiger Beweislastumkehr zugunsten der Betroffenen exkulpieren muss.[1433]

Immaterielle Schäden werden gem. § 253 Abs. 1 BGB mangels ausdrücklicher Erwähnung nicht vom § 7 BDSG erfasst, weswegen dieser in der Praxis nur eine geringe Rolle spielt.[1434] Stattdessen werden immaterielle Schadensersatzansprüche über die deliktischen zivilrechtlichen Ansprüche wegen eines Eingriffs in das Allgemeine Persönlichkeitsrecht gem. §§ 1004 analog, 823 Abs. 1 BGB geltend gemacht.[1435] Ferner stellen

---

[1426] VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235 (240).

[1427] *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 6b, Rn. 5.

[1428] *Gola/Schomerus*, BDSG, § 6b, Rn. 26.

[1429] *Gabel*, in: *Taeger/Gabel*, BDSG, § 7, Rn. 1.

[1430] Ebenda, § 7, Rn. 9.

[1431] Ebenda, § 7, Rn. 17; *Simitis*, in: *Simitis*, BDSG, § 7, Rn. 21.

[1432] *Gabel*, in: *Taeger/Gabel*, BDSG, § 7, Rn. 17.

[1433] Vgl. ebenda, § 7, Rn. 12 u. 19; *Gola/Schomerus*, BDSG, § 7, Rn.9; *Simitis*, in: *Simitis*, BDSG, § 7, Rn. 21.

[1434] Vgl. *Gabel*, in: *Taeger/Gabel*, BDSG, § 7, Rn. 1.

[1435] Vgl. *e*benda, § 7, Rn. 10; *Gola/Schomerus*, BDSG, § 7, Rn.9; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 157 und § 7, Rn. 32 f.

die individuell schützenden Vorschriften des BDSG, insbesondere der § 6b BDSG, Schutzgesetze gem. § 823 Abs. 2 BDSG dar.[1436]

6. Ergebnis der datenschutzrechtlichen Prüfung

Die Führung von Smartglasses im öffentlichen Raum ist als eine Form der Videoüberwachung i.S.d. § 6b Abs. 1 BDSG, außer in Ausnahmefällen bei einer medizinischen Indikation, in extremen Notwehrsituationen oder Fällen der Einwilligung, verboten. Der Grund liegt in der von Smartglasses ausgehenden Einschüchterungswirkung, die Dritte erheblich in einer autonomen Entfaltung ihrer Individualität im öffentlichen Raum beeinträchtigt. Dadurch wird zugleich die objektive Funktion des öffentlichen Raums als Ort des Meinungsaustausches und -ausdrucks erheblich eingeschränkt. Aufgrund der objektiven Beeinträchtigung der Persönlichkeitsrechte Dritter können sich die Nutzer von Smartglasses zudem nicht darauf berufen, die Geräte ausschließlich für persönliche Zwecke zu nutzen und auf die Rechte Dritter Rücksicht nehmen zu wollen.

III. Strafgesetzlicher Schutz des Allgemeinen Persönlichkeitsrechts

Dem Gesetzgeber bleibt es vorbehalten, bestimmte Fälle besonders schwerwiegender Gefährdungen der Privatsphäre strafrechtlich zu sanktionieren. Einen solchen Fall stellen insbesondere die Verletzung der Vertraulichkeit des Wortes gem. § 201 StGB und die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen gem. § 201a StGB dar.[1437] Die Vorschriften sind insbesondere im Hinblick auf die technischen Gefahren der Persönlichkeitsrechtsverletzung konzipiert, mit deren Zunahme infolge der Verbreitung von Smartglasses und ihrer heimlichen Abhör- und Aufnahmemöglichkeiten zu rechnen ist.[1438]

1. Verletzung der Vertraulichkeit des Wortes gem. § 201 StGB

Die Vorschrift des § 201 StGB dient dem Schutz unbefangener menschlicher Kommunikation als einem Aspekt der Privatsphäre sowie des Rechts am nicht öffentlich gesprochenen Wort als Teil des Allgemeinen Persön-

[1436] AG Berlin-Mitte, Urt. v. 18.12.2003 (16 C 427/02), NZM 2004, 318 (319); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 157.

[1437] Daneben wird die Verletzung des Allgemeinen Persönlichkeitsrechts auch außerhalb des StGB, z.B. im § 44 BDSG und § 33 KUG strafrechtlich sanktioniert.

[1438] Vgl. zur Konzeption, BT-DrS. 15/1891, S. 6; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 1.

lichkeitsrechts.[1439] Gem. § 201 Abs. 4 wird auch den Versuch unter Strafe gestellt.

a) Aufnehmen, Gebrauchen und Zugänglichmachen gem. § 201 Abs. 1 StGB

§ 201 Abs. 1 Nr. 1 StGB verbietet die Aufnahme des nicht öffentlich gesprochenen Wortes einer Person auf einem Tonträger. Der Schutz entsteht entsprechend dem verfassungsrechtlichen Schutzbereich des nicht öffentlich gesprochenen Wortes unabhängig vom Inhalt des Gesprächs und ist auch bei einzelnen Worten einschlägig, sofern ihnen ein gedanklicher Inhalt zu entnehmen ist.[1440] Ebenso wie im Verfassungsrecht gilt ein gesprochenes Wort als nicht öffentlich, wenn es zum einem subjektiv nicht für einen nach Zahl und Individualität unbestimmten oder nicht durch persönliche Beziehungen verbundenen größeren Personenkreis bestimmt war und der Sprecher hierauf nach objektiven Gesichtspunkten vertrauen durfte.[1441] Hierbei ist es irrelevant, dass Smartglasses von den Sprechern als solche erkannt werden, solange diesen nicht bewusst ist, dass eine Aufzeichnung ihrer Worte erfolgt.[1442]

§ 201 StGB untersagt die Aufnahme nicht öffentlich gesprochener Worte auf einem Tonträger, worunter jegliche zur Wiedergabe von Tonfolgen bestimmte Vorrichtungen, also auch Smartglasses, verstanden werden.[1443] Der Zweck der Aufzeichnung ist hierbei irrelevant.[1444] Als weitere Voraussetzung verlangt die Vorschrift, dass die Aufnahme unbefugt war,

---

[1439] BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238 (245); *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 2 f.; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 1 f.; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 2.

[1440] Vgl. E II. 2. a) cc) (1), S. 107; BVerfG, Beschl. v. 10.12.2010 (1 BvR 1739/04), NJW 2011, 1859 (1862); OLG Karlsruhe, Urt. v. 9.11.1978 (2 Ss 241/78), NJW 1979, 1513 (1514 f.); *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 6 f.; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 2; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 5; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 82.

[1441] Vgl. E II. 2. a) cc) (2), S. 109; OLG Nürnberg, Beschl. v. 24.10.1994 (Ws 936/94), NJW 1995, 974 f.; OLG Frankfurt a.M., Urt. v. 28.3.1977 (2 Ss 2/77), NJW 1977, 1547; *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 8; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 2; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 6 ff.

[1442] Vgl. E II. 2. a) cc) (2), S. 109; so im Ergebnis auch, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 393.

[1443] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 10; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 3; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 11.

[1444] Vgl. BGH, Urt. v. 9.4.1986 (3 StR 551/85), BGHSt 34, 39 (43); *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 4.

also ohne Einwilligung des Sprechenden oder sonstige Rechtfertigung erfolgte.[1445]

Nach der Tatbestandsalternative des § 201 Abs. 1 Nr. 2 StGB ist auch das Gebrauchen, d.h. Kopieren oder Abspielen der unbefugten Aufnahme untersagt, auch wenn es nur durch den Aufnehmenden erfolgt.[1446] Ebenso untersagt ist es, die Aufnahmen Dritten zugänglich zu machen, also ihnen die Möglichkeit zu gewähren, sie zu hören oder über sie zu verfügen.[1447]

Smartglasses können ohne Weiteres zur Aufnahme nicht öffentlich gesprochener Worte eingesetzt werden, z.B. wenn im Rahmen einer audiovisuellen Aufzeichnung ein Gespräch ohne Einwilligung des Sprechers aufgezeichnet wird. Ebenfalls als tatbestandsmäßig sind flüchtige Aufnahmen zu werten, die entstehen, weil Smartglasses alles „Gehörte" aufzeichnen, um dadurch potenzielle Stimmbefehle ihrer Nutzer zu erkennen.[1448] Jedoch wird hierbei zu beachten sein, dass die Erkennung nur im Nahfeld erfolgt und ggf. eine Einwilligung des Sprechenden mit derart geringer Beeinträchtigung seiner Rechte durch diese zweckgebundene und flüchtige Datenverarbeitung vorliegt.[1449]

b) Abhören und Veröffentlichen gem. § 201 Abs. 2 StGB

§ 201 Abs. 2 StGB untersagt auch das bloße Abhören, ohne dass eine Aufzeichnung stattfindet, sofern hierzu ein Abhörgerät eingesetzt wird und das abgehörte Wort nicht zur Kenntnis des Täters bestimmt ist.[1450] Ein Abhören findet statt, wenn das durch das Abhörgerät vernommene Wort akustisch wahrgenommen wurde.[1451] Dabei muss der Täter im Gegensatz zum bloßen „Hören" ein aktives Verhalten entwickeln und z.B.

[1445] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 9; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 84.

[1446] OLG Düsseldorf, Beschl. v. 25.1.1995 (1 Ws 904, 969/94), NJW 1995, 975 (975 f.); *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 12 f.; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 4; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 85.

[1447] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 14; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 4.

[1448] Vgl. E II. 2. a) cc) (2), S. 109; *Venzke-Caprarese*, Internet der Dinge: Ist der Betrieb bestimmter Smart-TVs strafrechtlich relevant?, Datenschutz-Notizen, https://www.datenschutz-notizen.de/internet-der-dinge-ist-der-betrieb-bestimmter-smart-tvs-strafrechtlich-relevant-1010470/(22.10.2015).

[1449] Anders könnte es sein, wenn das Gesprochene an Dritte zur Stimmauswertung übermittelt wird, vgl. E II. 2. b) dd) (4), S. 119.

[1450] An wen ein Wort zur Kenntnis bestimmt wird, entscheidet die sprechende Person, *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 15; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 5.

[1451] *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 5.

„Horchen“ oder „Ausforschen“.[1452] Ein Abhörgerät ist eine technische Vorrichtung jeglicher Art, „die das gesprochene Wort über dessen normalen Klangbereich hinaus durch Verstärkung oder Übertragung unmittelbar wahrnehmbar macht“.[1453] Auch Smartglasses können als Abhörgeräte dienen, wenn sie z.B. zur Live-Übertragung eingesetzt werden. Hierbei ist es irrelevant, ob der Nutzer von Smartglasses oder nur der Empfänger das Gesprochene vernimmt.[1454] Jedoch werden die Worte bei einer Live-Übertragung ohnehin digital zwischengespeichert, also i.S.d. § 201 Abs. 1 Nr. 1 StGB aufgezeichnet, um sie beim Empfänger wiedergeben zu können. Folglich tritt § 201 Abs. 2 StGB neben § 201 Abs. 1 Nr. 1 StGB.

§ 201 Abs. 2 Satz 1 Nr. 2 StGB ist einschlägig, wenn das nach Abs. 1 Nr. 1 aufgenommene oder nach Abs. 2 Satz 1 Nr. 1 unbefugt abgehörte nicht öffentlich Gesprochene im Wortlaut oder seinem wesentlichen Inhalt nach veröffentlicht wird.[1455] Dabei reicht bereits die Möglichkeit der Wahrnehmung durch einen größeren, nach Zahl und Individualität unbestimmten und durch nähere Beziehungen nicht verbundenen Personenkreis aus.[1456] Das kann z.B. auch bei Zugänglichmachung von Aufnahmen innerhalb sozialer Netzwerke der Fall sein.[1457]

§ 201 Abs. 2 Satz 2 StGB enthält eine auf § 201 Abs. 2 Satz 1 Nr. 2 StGB beschränkte Bagatellklausel, nach der eine Veröffentlichung geeignet sein muss, berechtigte Interessen eines anderen zu beeinträchtigen. Hierunter fallen alle Arten von individuellen oder gemeinschaftlichen Interessen, sei es ideeller oder wirtschaftlicher Art, sofern sie nicht dem geltenden Recht zuwiderlaufen.[1458] D.h., die Veröffentlichung von inhaltlichen Banalitäten, wie z.B. Gesprächen über das Wetter, stellt keinen Verstoß dar.[1459] Ferner könnte im Fall des § 201 Abs. 2 Satz 1 Nr. 2 StGB die Bestrafung unter dem Gesichtspunkt der Sozialadäquanz entfallen.[1460] Es ist jedoch kaum

---

1452 *Kühl*, in: Ebenda; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 20.

1453 *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 17; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 5; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 19.

1454 Vgl. *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 16.

1455 Vgl. *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 88.

1456 OLG Stuttgart, Urt. v. 8.12.2003 (4 Ss 469/03), NJW 2004, 622 f.; *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 16; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 7; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 19.

1457 Vgl. F II. 1. c) cc) (2) (e), S. 201.

1458 *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 20; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 88.

1459 *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 20.

1460 Ablehnend, *Kargl*, in: Ebenda, § 201, Rn. 27; ebenfalls ablehnend, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 393; vgl. Übersicht in *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 14.

damit zu rechnen, dass das Abhören selbst gesellschaftlich akzeptiert wird.[1461]

c) Subjektiver Tatbestand und Rechtswidrigkeit

Der subjektive Tatbestand des § 201 Abs. 1 Nr. 1 StGB erfordert ein vorsätzliches Handeln, sodass zumindest ein Eventualvorsatz erforderlich ist.[1462] Im Fall des Gebrauchmachens, Zugänglichmachens gem. § 201 Abs. 1 Nr. 2 StGB und der Veröffentlichung gem. § 201 Abs. 2 Satz 1 Nr. 2 StGB muss der Täter auch davon ausgehen, dass die Aufnahme „unbefugt" war. [1463]

§ 201 Abs. 2 Satz 3 StGB enthält einen auf § 201 Abs. 2 Satz 1 Nr. 2 StGB beschränkten Rechtfertigungsgrund, falls der Täter in Wahrnehmung überragender öffentlichen Interessen handelt. Die Vorschrift kodifiziert vor allem die aus Art. 5 Abs. 1 GG abgeleitete Medienfreiheit, auch wenn sie für jedermann gilt.[1464] Ein überragendes öffentliches Interesse verlangt weder eine gegenwärtige Gefahr, noch dass die öffentliche Mitteilung zu deren Abwendung erforderlich ist.[1465] Im Vergleich mit § 34 StGB sind die Anforderungen insoweit zwar geringer, jedoch werden statt nur „berechtigter" Interessen „überragende" Interessen gefordert. Zu fordern ist also ein eindeutiges Interessenübergewicht, z.B. die Aufdeckung schwerwiegender Delikte gem. §§ 129a Abs. 1, 138 Abs. 1 StGB.[1466] Bei der typischen privaten Nutzung von Smartglasses ist jedoch nicht damit zu rechnen, dass diese Ausnahme einschlägig sein wird.

Als Rechtfertigungsgrund kommt vor allem eine Einwilligung in Betracht, jedoch ist hierzu nicht ausreichend, dass der sprechenden Person nur die Präsenz der Datenbrille bekannt ist.[1467] Vielmehr muss ihr auch das tatbestandsmäßige Handeln des § 201 StGB, d.h. insbesondere das Aufzeichnen, Gebrauchen, Zugänglichmachen oder Abhören, bewusst

---

[1461] Vgl. *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 89.

[1462] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 21.

[1463] Ebenda; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 16.

[1464] BT-DrS. 127/14, S. 4; BT-DrS. 11/7417, S. 4.

[1465] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 33; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 91.

[1466] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 33; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 15; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 91.

[1467] Der Streit, ob eine Einwilligung wegen des Begriffes "unbefugt" bereits tatbestandsausschließend wirkt oder erst auf der Rechtfertigungsebene zum Tragen kommt, kann i.R.d. Untersuchung dahingestellt bleiben, vgl. *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 9; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 13; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 84.

sein.[1468] Im Hinblick auf weitere Voraussetzungen kann auf die Ausführungen zur datenschutzrechtlichen Einwilligung verwiesen werden, wobei die strafrechtliche Einwilligung formfrei ist.[1469] Ferner kann sie auch mutmaßlich vorliegen, wenn eine ausdrückliche Einwilligung nicht rechtzeitig eingeholt werden konnte, was aufgrund räumlicher Nähe im Fall von Smartglasses jedoch generell möglich sein wird.[1470]

Neben der Einwilligung kann eine tatbestandsmäßige Begehung des § 201 StGB auch durch Notwehr gem. § 32 StGB und im Fall des rechtfertigenden Notstands nach § 34 StGB gerechtfertigt sein.[1471] Dabei wird es sich primär um Fälle der Aufnahme oder Übermittlung von Gesprächen zwecks Gefahrenabwehr oder Beweisführung handeln.[1472] Beide Interessen sind jedoch entsprechend den bisherigen Erkenntnissen dieser Untersuchung nur in extremen Ausnahmefällen, bei gewichtigen Straftaten wie Erpressung oder Feststellung der Identität bei einer Verleumdung, als Ultima Ratio zulässig.[1473] Dagegen reicht das Interesse an der Sicherung von Beweismitteln für zivilrechtliche Ansprüche generell nicht aus.[1474] Darüber hinaus wird ein Abhören „auf Verdacht“ im Rahmen privater

---

[1468] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 21; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 11.

[1469] Vgl. F II. 1. d) bb) (2), S. 210.

[1470] *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 30; vgl. *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 66.

[1471] Da § 201 StGB einen weiten Schutzbereich hat, der schon bei geringfügigen Eingriffen beeinträchtigt wird, kommt eine Rechtfertigung der Täter häufiger in Betracht, als z.B. im Fall des § 201a StGB, der den höchstpersönlichen Bereich schützt, *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 89 f.

[1472] Vgl. *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 31a f.

[1473] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (50); BGH, Urt. v. 27.1.1994 (I ZR 326/91), NJW 1994, 2289 (2292 f.); BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277; BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (289 f.); OLG Düsseldorf, Beschl. v. 23.11.1965 (1 Ws 754/65), NJW 1966, 214; *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 25 f.; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 11; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 31a.

[1474] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (50); BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277; BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (290); *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 27; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 31b; ferner kommt in solchen Konstellationen die Anwendung des § 127 Abs.1 StPO in Betracht wenn der Eingriff "auf frischer Tat" erfolgt und dazu dient, die Identität der Person, deren Stimme aufgezeichnet wird, zu klären, vgl. *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 31; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 68 f.

„Fahndungshilfe“ unzulässig sein, da hierzu nur die zuständigen Behörden in den Grenzen der §§ 100a ff. StPO befugt sind.[1475]

Die Strafbarkeit nach § 201 StGB entfällt ferner, wenn der Täter sich auf Entschuldigungsgründe berufen kann, die an dieser Stelle jedoch nicht vertieft werden.[1476]

2. Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB)

Die Vorschrift des § 201a StGB dient dem Schutz des höchstpersönlichen Lebensbereiches als einem besonders schützenswerten Bereich der Privatsphäre sowie des Rechts am eigenen Bild als Teil des Allgemeinen Persönlichkeitsrechts.[1477] Im Gegensatz zu § 201 StGB enthält die Vorschrift keine Versuchsstrafbarkeit.[1478]

a) Verschärfung des Gesetzes als Reaktion auf zunehmende Gefahren durch Mobil- und Informationstechnik

Mit dem Inkrafttreten des 49. Gesetz zur Änderung des Strafgesetzbuches mit der Umsetzung europäischer Vorgaben zum Sexualstrafrecht am 27.1.2015 ist der ursprünglich am 5.8.2004 in Kraft getretene § 201a StGB neu gefasst und erweitert worden.[1479] Mit der Neuaufnahme der § 201a Abs. 1 Nr. 3 und Abs. 2 StGB reagierte der Gesetzgeber auf die durch mobile Aufnahmegeräte steigende Anzahl von „entwürdigenden, bloßstellenden, gewalttätigen oder eine Person in hilfloser Lage zur Schau stellenden Bildaufnahmen“.[1480] Die Aufnahmen finden aufgrund der Anonymität im Internet ungehemmte Verbreitung und führen zu Nachteilen für Betroffene, wie etwa beim „Cyber-Mobbing“. [1481] Während die vorgenannte Verschärfung des § 201a StGB auch den von Smartglasses ausgehenden Gefahren begegnet, ist der auf die Eindämmung des kommerziellen Handels mit Bildaufnahmen von ganz oder teilweise unbekleideten Kindern und Jugendlichen gerichtete Abs. 3 für diese Untersuchung weniger relevant.[1482]

[1475] *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201, Rn. 31b.

[1476] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 22.

[1477] Ebenda, § 201a, Rn. 1; *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 1; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 1.

[1478] *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 1.

[1479] BT-DrS. 18/3202, S. 1; *Busch*, NJW 2015, S. 977.

[1480] BT-DrS. 18/3202, S. 28; BT-DrS. 18/2601, S. 36; *Busch*, NJW 2015, S. 977.

[1481] BT-DrS. 18/2601, S. 37; *Busch*, NJW 2015, S. 977.

[1482] Vgl. *Busch*, NJW 2015, S. 977.

Neben der Erweiterung der Tatbestände wurde die obere Grenze der Freiheitsstrafe von einem auf zwei Jahre angehoben.[1483] Ferner wurde § 201a Abs. 1 und 2 StGB in den Katalog der Privatklagedelikte gem. § 374 Abs. 1 Nr. 2a StPO aufgenommen.[1484] Ebenso stellt § 201a StGB gem. § 205 Abs. 1 Satz 2 StGB nunmehr nicht nur ein Antrags-, sondern auch ein Offizialdelikt dar.

b) Vorliegen einer Bildaufnahme

Als Bildaufnahme ist die Fixierung von Informationen über einen bestimmten Aufnahmegegenstand auf einem Bildträger zu verstehen, die es erlaubt, einen zumindest zweidimensionalen Sinneseindruck von dem Aufnahmegegenstand zu erhalten.[1485] Hierzu gehören auch digitale Speicher, wie im Fall von Smartglasses.[1486] Die Person auf dem Bild muss zwar nicht deutlich oder vollständig erkennbar sein, da der höchstpersönliche Bereich auch dann betroffen sein kann, wenn die Person nicht erkennbar ist.[1487] So stellt z.B. die Abbildung eines Geschlechtsteiles trotz fehlender Erkennbarkeit der Person einen Eingriff in die Intimsphäre dar.[1488] Allerdings ist es nicht ausreichend, wenn die Person gar nicht auf dem Bild zu erkennen ist, weil die Aufnahme z.B. verschwommen oder zu dunkel ist, da in diesem Fall das Recht am eigenen Bild nicht betroffen und eine Preisgabe höchstpersönlicher Informationen nicht zu befürchten ist.[1489]

c) Räumlich definierter Schutzbereich gem. § 201a Abs. 1 Nr. 1 StGB

§ 201a Abs. 1 Nr. 1 StGB verbietet im Kern die unbefugte Herstellung und Übertragung einer Bildaufnahme von einer Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum als „letzten Rückzugsbereich" befindet, wenn dabei der höchstpersönliche Lebensbereich der abgebildeten Person verletzt wird.[1490]

aa) Begriff der Wohnung und gegen Einblick besonders geschützter Räume

Die Wohnung setzt einen nach außen hin durch Wände und Decken umgrenzten Raum voraus, der dem ständigen Aufenthalt von Menschen dient. Sie umfasst auch die mit der Wohnung verbundenen Nebenräume,

---

1483 Ebenda.

1484 BT-DrS. 18/3202, S. 29.

1485 *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 33.

1486 Ebenda, 34.

1487 *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 4.

1488 BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1618).

1489 Vgl. *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 4.

1490 BT-DrS. 15/2466, S. 5; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 26.

wie Garagen oder den Keller.[1491] Ebenso werden Wohnwagen, Zelte oder Krankenhauszimmer vom Wohnungsbegriff umfasst.[1492] Die Wohnung ist als räumlicher Privatbereich absolut geschützt, unabhängig davon, ob sie sich im Eigentum oder Besitz der abgebildeten Person befindet.[1493] Der Begriff der Wohnung umfasst auch mit einer Wohnung vergleichbare Räumlichkeiten wie Hotel- und Gästezimmer, aber nicht einer (auch nur beschränkten) Öffentlichkeit zugängliche Geschäfts- und Diensträume.[1494]

Bei der Nutzung von Smartglasses im öffentlichen Raum sind Eingriffe in den Wohnungsraum zwar möglich, z.B. wenn ein Nutzer von Smartglasses durch ein Fenster in eine Wohnung hineinblickt. Im Regelfall wird jedoch die Alternative eines gegen Einblick besonders geschützten Raums einschlägig sein. Es kommt hierbei entsprechend dem Schutzzweck des Gesetzes auf den Schutz von räumlich geschützten Bereichen der höchstpersönlichen Sphäre an.[1495] Damit sind Räumlichkeiten gemeint, die dem Schutz der Menschenwürde besonders nahestehende Vorgänge schützen sollen, wie z.B. solche des inneren Familienlebens, des Gesundheitszustands, des Sexuallebens oder des Nacktseins.[1496] Der Gesetzgeber nennt als Beispiele Toiletten, Umkleidekabinen, ärztliche Behandlungszimmer als auch einen Garten, der mit einer hohen und undurchdringlichen Hecke bzw. einem dementsprechenden Zaun oder einer Mauer umgeben ist.[1497] Ebenso werden Solarien oder abgetrennte Duschkabinen zu besonders geschützten Räumen gerechnet.[1498] Da der Raum jedoch keiner, nicht einmal einer beschränkten Öffentlichkeit zugänglich sein darf, stellen öffentliche Saunen, Sammelumkleiden, das Wartezimmer einer Arztpraxis oder auch abgelegene FKK-Strände keine besonders geschützten Räume dar.[1499]

Es kommt zudem nicht auf die Umschlossenheit des Raums, sondern auf einen vorhandenen Sichtschutz, z.B. im Fall des durch einen hohen Zaun geschützten Gartens, an.[1500] Ebenso kann ein improvisierter Sicht-

---

[1491] BT-DrS. 15/2466, S. 5; *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 4; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 6; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 28.

[1492] *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 6.

[1493] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 4.

[1494] BT-DrS. 15/2466, S. 5.

[1495] Ebenda.

[1496] Ebenda.

[1497] Ebenda.

[1498] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 5.

[1499] Ebenda, § 201a, Rn. 12; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 7.

[1500] BT-DrS. 15/2466, S. 5.

schutz, z.B. aus Handtüchern am Strand, einen gegen Einblick besonders geschützten Raum darstellen.[1501] Im Hinblick auf die Funktion des Sichtschutzes wird zum Teil vertreten, dass der Sichtschutz mit besonderen Maßnahmen des Täters überwunden werden muss.[1502] Es muss daher ein über einen faktischen, über eine reine Umgrenzung hinausgehender, den Einblick erschwerender Sichtschutz vorhanden sein.[1503] Z.B. muss die Tür einer Umkleidekabine geschlossen oder ein Strandkorb durch eine Markise abgeschirmt werden.[1504] Entsprechend dieser Ansicht, aber ohne sich auf sie explizit zu beziehen, wurde auch der Schutz des § 201a Abs. 1 StGB im Fall eines hell erleuchteten und vorhanglosen Raumes einer Rechtskanzlei versagt.[1505] Auch das Fotografieren durch eine offene Tür oder nicht abgedunkelte Scheiben eines Kfz ist nicht tatbestandsmäßig.[1506] Die Aufnahmen müssen jedoch nicht von außen erfolgen, da auch eine Person, die befugt in einer Wohnung oder einem umschlossenen Raum verweilt, darin nach § 201a Abs. 1 StGB unbefugte Aufnahmen erstellen kann.[1507]

bb) Herstellung oder Übertragung der Bildaufnahme

Unter Herstellung einer Bildaufnahme versteht man ein gegenständliches Hervorbringen, das sämtliche Handlungen der Speicherung der Personenabbildung auf einem Bildträger umfasst.[1508] Der Begriff entspricht insoweit der Aufnahme gem. § 201 Abs. 1 Nr. 1 StGB.[1509] Er umfasst dementsprechend auch die digitale Speicherung in Smartglasses, sei es als Zwischenspeicherung zur weiteren Übertragung beim Live-Streaming bzw. Verarbeitung im Rahmen von Augmented-Reality-Funktionen oder zur Sicherung der Personenabbildung.[1510] Die Übertragung kann, z.B. im Fall des Live-Streamings, neben die erfolgte Aufnahme treten.[1511] Dies zeigt jedoch, dass eine dauerhafte Speicherung der Personenabbildungen nicht

---

1501 *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 5.

1502 *Rahmlow*, HRRS 2005, S. 84 (88).

1503 Ebenda.

1504 Ebenda.

1505 Vgl. OLG Karlsruhe, Urt. v. 7.4.2006 (14 U 134/05), NJW-RR 2006, 987 (988).

1506 *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 7.

1507 Ebenda, § 201a, Rn. 8.

1508 Vgl. *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 6; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 9; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 34.

1509 *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 4.

1510 Vgl. B III. 3, S. 38.

1511 Vgl. F III. 1. b), S. 247.

erforderlich ist.[1512] Einschlägig ist jedoch nur die erste Speicherung, alle weiteren Speicherungs- und Bearbeitungsvorgänge können allerdings von der Tathandlung des Gebrauchens nach § 201a Abs. 1 Nr. 3 StGB umfasst sein.[1513]

Die Herstellung oder Übertragung der Abbildung der Person muss nicht heimlich erfolgen.[1514] Damit wäre der Tatbestand des § 201a Abs. 1 Nr. 1 StGB nicht ausgeschlossen, wenn die aufgenommene Person z.B. anhand eines Aufnahmesignals den Aufnahmevorgang der Smartglasses erkennen würde.[1515] Sofern sie der Aufnahme jedoch trotz ihrer Kenntnis nicht widerspricht, muss das Vorliegen einer konkludenten oder mutmaßlichen Einwilligung geprüft werden.[1516]

d) Zurschaustellung der Hilflosigkeit von Personen gem. § 201a Abs. 1 Nr. 2 StGB

Die neue Regelung des § 201a Abs. 1 Nr. 2 StGB verbietet es, Bildaufnahmen, die die Hilflosigkeit einer anderen Person zur Schau stellen, unbefugt herzustellen oder zu übertragen und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person zu verletzen. Eine solche Gefahr droht bei Smartglasses insbesondere aufgrund der Möglichkeit spontaner Aufnahmen, die ohne weiteres Nachdenken z.B. mit dem Zwinkern des Auges oder einem kurzen Sprachbefehl ausgelöst werden können.[1517]

Laut gesetzlicher Begründung soll dieser Tatbestand Bildaufnahmen umfassen, die dem Ansehen der abgebildeten Person erheblich schaden können.[1518] Dies können z.B. Betrunkene auf dem Heimweg sein oder Opfer von Gewalttaten, die verletzt oder blutend auf dem Boden liegen.[1519] Jedoch muss ein Opfer, das z.B. unverschuldet in die Notlage geraten ist, nicht zwangsläufig einen Schaden im höchstpersönlichen Bereich durch die Abbildung davontragen.[1520] Darüber enthält die gesetz-

---

[1512] Vgl. *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 6a; *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 5.

[1513] *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 9; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 35.

[1514] *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 34.

[1515] Ebenda, 35.

[1516] Vgl. F III. 1. c), S. 249.

[1517] Vgl. E IV. 1. g), S. 154.

[1518] BT-DrS. 18/3202, S. 28.

[1519] Ebenda.

[1520] Ebenda.

liche Begründung keine weiteren Hinweise und überlässt es der Rechtsprechung, den unbestimmten Rechtsbegriff zu konturieren.[1521]

Die im § 221 Abs. 1 Nr. 1 und 2 sowie § 243 Abs. 1 Satz 2 Nr. 6 StGB verwendeten Begriffe der Hilflosigkeit können nicht unmittelbar auf den § 201a Abs. 1 Nr. 2 StGB übertragen werden, da sie jeweils eine abstrakte Gefahr des Todes oder schwerer Gesundheitsbeschädigung voraussetzen.[1522] § 201a Abs. 1 Nr. 2 StGB schützt dagegen nicht das Leben und die körperliche Integrität, sondern den höchstpersönlichen Lebensbereich als Teil des Persönlichkeitsrechts.[1523] Mithin ist der Begriff der Hilflosigkeit im § 201a Abs. 1 Nr. 2 StGB selbstständig zu definieren.[1524]

Den Schutzzweck ausklammernd, können die § 221 Abs. 1 Nr. 1 und 2 sowie § 243 Abs. 1 Satz 2 Nr. 6 StGB jedoch mittelbar zur Bestimmung der Hilflosigkeit im Rahmen des § 201a Abs. 1 Nr. 2 StGB herangezogen werden.[1525] Ausgehend vom Wortsinn ist unter Hilflosigkeit dementsprechend die Abwesenheit von eigener oder fremder Hilfe zu verstehen.[1526] Anknüpfungspunkt ist eine Situation, in der eine Person sowohl aufgrund psychischer oder körperlicher Konstitution als auch aufgrund äußerer Einflüsse nicht (mehr) in der Lage ist, einen eigenen Willen zu bilden, sich entsprechend einem gebildeten Willen zu verhalten oder sich ohne eigene oder fremde Hilfe dieser Situation zu entziehen.[1527]

e) Gebrauch der Bildaufnahme gem. § 201a Abs. 1 Nr. 3 StGB

Als Gebrauch der unbefugt hergestellten Bildaufnahme wird die Nutzung der Bildaufnahme z.B. durch Archivieren, Speichern oder Kopieren erfasst.[1528] Dabei wird sowohl der Gebrauch des Herstellers der Aufnahme als auch Dritter erfasst.[1529] Ausreichend ist damit auch, wenn ein Träger von Smartglasses die Aufnahme selbst betrachtet.[1530] Der Begriff des Zugänglichmachens entspricht § 201 StGB und liegt vor, wenn Dritten der

---

1521 *Busch*, NJW 2015, S. 977.

1522 Ebenda, 978; *Eser/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 221, Rn. 8; *Heger*, in: *Lackner/Kühl*, StGB, § 221, Rn. 2; *Neumann*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 221, Rn. 6.

1523 *Busch*, NJW 2015, S. 977 (978).

1524 Ebenda.

1525 Ebenda.

1526 Ebenda; *Eser/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 221, Rn. 4.

1527 *Busch*, NJW 2015, S. 977 (978); *Eser/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 221, Rn. 9; *Heger*, in: *Lackner/Kühl*, StGB, § 221, Rn. 2; *Neumann*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 221, Rn. 6 ff.

1528 BT-DrS. 15/2466, S. 5; *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 9.

1529 *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 6.

1530 Vgl. ebenda.

Zugriff auf die Bildaufnahmen z.B. durch Vorführung oder Übergabe der Daten verschafft wird.[1531]

f) Zugänglichmachen befugt hergestellter Bildaufnahmen gem. § 201a Abs. 1 Nr. 4 StGB

Nach § 201a Abs. 1 Nr. 4 StGB ist die wissentliche, d.h. nicht lediglich in Kauf genommene, Zugänglichmachung befugt hergestellter Aufnahmen unter Strafe gestellt, wodurch der Missbrauch persönlich entgegengebrachten Vertrauens unter Strafe gestellt wird.[1532] So sollte z.B. der Missbrauch von Bildern durch Ex-Partner sanktioniert werden.[1533] § 201a Abs. 3 StGB kann bei Aufnahmen, die mittels Smartglasses hergestellt worden sind, einschlägig sein, stellt jedoch keine den Smartglasses eigene Problematik dar.

g) Bildaufnahmen mit Schädigungsabsicht gem. § 201a Abs. 2 StGB

Nach dem ebenfalls neu eingeführten Abs. 2 des § 201a StGB werden diejenigen bestraft, die unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich machen. Die Vorschrift soll insbesondere Kinder und Jugendliche vor Nachteilen des Cyber-Mobbings schützen.[1534] Ebenso wie im § 201a Abs. 1 Nr. 2 StGB bestimmt das Gesetz nicht, wann eine solche Eignung vorliegen soll.

Laut der gesetzlichen Begründung sollen mit der Vorschrift Fälle erfasst werden, in denen mittels in Mobiltelefonen eingebauter Kameras hergestellte Bildaufnahmen von Personen in entwürdigenden, bloßstellenden Situationen, die nicht vom Täter herbeigeführt werden müssen, insbesondere über Telemedien, wie z.B. „Onlinechats oder -foren“, verbreitet werden.[1535] Es kann sich dabei insbesondere um Fälle handeln, in denen abgebildete Personen in einer peinlichen, ihre Würde verletzenden Situation dargestellt werden.[1536] Ebenso werden Aufnahmen umfasst, die eine Person in einem Zustand zeigen, bei dem angenommen werden kann, dass die Person üblicherweise ein Interesse daran hat, dass andere sie in diesem Zustand nicht sehen.[1537] Dabei sind solche Situationen und Zustände

---

[1531] Vgl. F III. 1. a), S. 246; *Kühl*, in: Ebenda; *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 9.

[1532] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 10; *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 8.

[1533] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 10.

[1534] BT-DrS. 18/2601, S. 36.

[1535] Ebenda, 37.

[1536] Ebenda.

[1537] Ebenda.

nicht auf geschützte Räumlichkeiten i.S.d. § 201a Abs. 1 Nr. 1 StGB beschränkt, sondern können auch im öffentlichen Raum vorliegen.[1538] Z.B. kann es sich um die Abbildung einer betrunkenen Person auf dem Heimweg handeln oder des Opfers einer Gewalttat, wobei der Gesetzeber keine Anhaltspunkte zur Abgrenzung zum § 201a Abs. 1 Nr. 2 StGB bietet, der solche Abbildungen, außer im Fall der Herstellung, ebenfalls umfassen kann.[1539]

Dem Begriff des „Bloßstellens" fehlt es an einer tatbestandlichen Eingrenzung und er könnte z.B. auch Fälle umfassen, in denen eine Aufnahme peinlich ist oder den Spott anderer Personen herausfordert.[1540] Hierdurch könnten aber auch Fälle, die nicht Ausgangspunkt der gesetzgeberischen Initiative waren, erfasst werden, wie z.B. das Bohren in der Nase, das unvorteilhafte Aussehen beim Essen in einem Restaurant, Menschen bei unvorteilhaften Bewegungen, z.B. sich „verrenkende Tänzer" oder „adipöse Personen" beim Hinaussteigen aus einem Swimmingpool.[1541] Ebenso wäre zu fragen, ob die Bloßstellung situationsbedingt erfolgen kann, wenn z.B. jemand während des außerehelichen Fremdgehens fotografiert wird.[1542] Zudem wird kritisiert, dass die Vorhersehbarkeit der Strafbarkeit abhängig von kulturellen und regionalen Anschauungen und Sitten sehr unterschiedlich ausfallen kann.[1543] Als Maßstab zur Bestimmung des Achtungsanspruchs wird daher die Orientierung an der Kasuistik zum strafrechtlichen Ehrschutz gem. § 185 ff StGB vorgeschlagen, also an der Frage, ob eine Aufnahme geeignet ist, eine Person „verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen".[1544] Allerdings fragt es sich in diesem Fall, warum der Gesetzgeber sich nicht selbst an dem Ehrbegriff orientiert hat. Diese Ansicht erscheint dennoch überzeugend, wobei eine vertiefte Erörterung dieser Auslegungsschwierigkeiten im Rahmen der Untersuchung nicht erfolgen soll, da es sich um keine spezielle Problematik der Nutzung von Smartglasses handelt.

h) Taterfolg der Verletzung des höchstpersönlichen Lebensbereichs

Der tatbestandsmäßige Erfolg der § 201a Abs. 1 Nr. 1 bis 4 StGB besteht in der Verletzung des höchstpersönlichen Lebensbereichs der abgebildeten Person. Mit der Voraussetzung eines Verletzungserfolges wird klarge-

---

1538 Ebenda, 36.

1539 Ebenda.

1540 *Wieduwilt*, K&R 2014, S. 627 (631).

1541 Ebenda.

1542 Ebenda.

1543 *Busch*, NJW 2015, S. 977 (978).

1544 Ebenda.

stellt, dass nicht jede Bildaufnahme im höchstpersönlichen räumlichen Bereich zu einer Tatbestandserfüllung führt.[1545] Es müssen höchstpersönliche, also besonders enge und private, Lebensbereiche sein und nicht Alltagssituationen.[1546] Als höchstpersönlich werden Abbildungen von Krankheitszuständen, dem engen Familienleben, sexuellen Tätigkeiten oder nackter Menschen angesehen.[1547] Problematisch wird die Abgrenzung im familiären Bereich, z.B. bei Handlungen wie dem Umgang mit Kindern, die im Einzelfall im Hinblick auf deren Zugehörigkeit zum höchstpersönlichen Bereich des Familienlebens bewertet werden müssen.[1548] Im Unterschied zu den Fällen des § 201a Abs. 1 wird der Taterfolg durch die Taten nach § 201a Abs. 2 und 3 StGB indiziert.[1549]

i) Subjektiver Tatbestand und Rechtswidrigkeit

Entsprechend § 201 StGB erfordert auch § 201a Abs. 1 StGB zumindest einen bedingten Vorsatz, der sich auch auf den geschützten räumlichen Bereich, die Hilflosigkeit einer Person sowie die Verletzung des höchstpersönlichen Lebensbereichs beziehen muss.[1550] Die irrige Bewertung, ein Lebensbereich sei nicht höchstpersönlich, stellt lediglich einen strafbaren Subsumtionsirrtum dar.[1551] § 201a Abs. 1 Nr. 4 StGB setzt ein absichtliches oder bewusstes Handeln voraus, d.h., der Eventualvorsatz ist nicht ausreichend.[1552] Im Fall des Abs. 2 muss sich der Vorsatz auch auf das Merkmal der fehlenden Befugnis beziehen.[1553]

Die Rechtfertigung der Wahrnehmung öffentlicher Interessen, die der „Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen“, wird bei einer typischen privaten Nutzung

---

[1545] *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 3.

[1546] *Leffler*, Cyber-Bullying, 2012, S. 293 f.

[1547] BT-DrS. 15/2466, S. 5; *Busch*, NJW 2015, S. 977 (979); *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 11 ff.; *Kühl*, in: *Lackner/Kühl*, StGB, § 201a, Rn. 3; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 10; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 40 ff.

[1548] Zur Bestimmung höchstpersönlicher Bereiche hat sich eine fallbezogene Kasuistik entwickelt, vgl. *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 11a; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 10.

[1549] *Busch*, NJW 2015, S. 977 (979).

[1550] Vgl. F III. 1. c), S. 249; *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 13; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 11.

[1551] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 13.

[1552] Ebenda, § 201a, Rn. 14.

[1553] Ebenda, § 201a, Rn. 13.

von Smartglasses selten einschlägig sein.[1554] Zudem ist diese Rechtsfolge gem. § 201a Abs. 4 StGB ohnehin nur für die Fälle des Gebrauchs unbefugter Bildaufnahmen nach § 201a Abs. 1 Nr. 3 StGB sowie der unbefugten Zugänglichmachung befugter Bildaufnahmen nach Abs. 1 Nr. 4 als auch nach den Absätzen 2 und 3 vorgesehen.

Darüber hinaus kommen in seltenen Ausnahmefällen zur Abwehr von Gefahren oder zu Beweiszwecken die Tatbestände der Notwehr gem. § 32 StGB oder des rechtfertigenden Notstands gem. § 34 StGB in Frage.[1555] Solche Situationen sind beim typischen Einsatz von Smartglasses jedoch praktisch nur in seltenen Fällen vorstellbar.[1556] Im Hinblick auf eine mögliche Einwilligung der Abgebildeten kann ferner für die Zwecke dieser Untersuchung auf die Prüfung i.R.d. § 201 StGB verwiesen werden.[1557]

Des Weiteren verbietet sich eine analoge Anwendung der Ausnahmen des § 23 KUG, da es bereits an einer vergleichbaren Sachlage fehlt, da § 201a StGB den höchstpersönlichen Lebensbereich und nicht nur das Recht am eigenen Bild schützt.[1558]

3. Rechtsfolgen der Verstöße gegen §§ 201, 201a StGB

Bei der Vorschrift des § 201 StGB handelt es sich gem. § 205 Abs. 1 Satz 1 StGB um ein absolutes Antragsdelikt. Ein Verstoß gegen § 201 StGB wird unter eine Freiheitsstrafe bis zu drei Jahren oder Geldstrafe gestellt.

Beim § 201a StGB handelt es sich gem. § 205 Abs. 1 Satz 2 StGB um ein Antrags- und ein Offizialdelikt. Die Begehung des § 201a StGB wird mit einer Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe geahndet. Die Tat steht ferner in Tatmehrheit zu § 33 KUG.[1559]

Die hergestellten Ton- oder Bildaufnahmen unterliegen ferner der Einziehung gem. § 74 StGB sowie gem. § 201a Abs. 5 StGB der erweiterten Einziehung des § 74a StGB.

Ferner können auch die Smartglasses als das zur Begehung der Straftaten unmittelbar verwendete Tatwerkzeug ebenfalls der Einziehung gem. § 74 Abs. 2 Nr. 1 sowie § 201a Abs. 5 i.V.m. § 74a StGB unterliegen.[1560]

[1554] Die Vorschrift lehnt sich laut gesetzlicher Begründung an § 86 Abs. 3 StGB an, BT-DrS. 18/3202, S. 29.

[1555] *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 13.

[1556] *Kargl*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201a, Rn. 17.

[1557] Vgl. F III. 1. c), S. 249; *Lenckner/Eisele*, in: *Schönke/Schröder*, StGB, § 201a, Rn. 11.

[1558] *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 69 f.

[1559] *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 11.

[1560] Vgl. *Eser*, in: *Schönke/Schröder*, StGB, § 74, Rn. 9a; *Heger*, in: *Lackner/Kühl*, StGB, § 74, Rn. 5; *Herzog/Saliger*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 74, Rn. 8 ff.

Die Vorschrift besitzt nach ihrer Rechtsnatur vornehmlich einen Strafcharakter und soll dem Gedanken des Unrechtsausgleichs Rechnung tragen.[1561] Unter Durchbrechung der grundgesetzlich gewährten Eigentumsgarantie sollen dabei dem Täter, der sein Eigentum rechts- und sozialwidrig verwendet, die Folgen seiner Tat fühlbar gemacht werden.[1562] Die Anordnung kann im Einzelfall aber auch aus general- und spezialpräventiven Gründen erfolgen.[1563] Die Einziehung darf jedoch nicht außer Verhältnis zur Schwere der Tat stehen.[1564] Dabei wird bei Zugrundelegung der Strafwirkung die Intensität des begangenen Rechtsverstoßes und im Hinblick auf die präventive Wirkung die Gefahr erneuter Begehung der Straftat zu berücksichtigen und mit dem wirtschaftlichen Wert der Datenbrille sowie deren Notwendigkeit für ihren Nutzer abzuwägen sein.[1565]

4. Ergebnis zum strafgesetzlichen Schutz des Allgemeinen Persönlichkeitsrechts

Smartglasses bringen eine erhöhte Gefahr für die Verletzung der nach §§ 201, 201a StGB geschützten Aspekte des Allgemeinen Persönlichkeitsrechts mit sich. Sie stellen geradezu ein Musterbeispiel für internetangebundene Mobilgeräte dar, derentwegen der § 201a StGB auch auf den Schutz hilfloser Personen erweitert worden ist. Da Smartglasses ihre Träger begleiten und deren Blick folgen, besteht eine hohe Gefahr, dass die objektiven Tatbestände des Abhörens oder der Verletzung des höchstpersönlichen Lebensbereichs mit ihrer Hilfe verwirklicht werden.

Es erscheint nicht unwahrscheinlich, dass die Heimlichkeit und die Einfachheit sowie Geschwindigkeit, mit der Aufnahmen ausgelöst werden können, gepaart mit menschlicher Neugier zur Senkung der Hemmschwelle vor der Verletzung der Persönlichkeitsrechte Dritter führen werden.[1566] Ebenso wahrscheinlich erscheint es, dass Menschen aufgrund ihres Sicherheitsbedürfnisses dieses Potenzial von Smartglasses zur Siche-

---

[1561] BGH, Beschl. v. 26.4.1983 (1 StR 28/83), NJW 1983, 2710 f.; BGH, Urt. v. 24.8.1972 (4 StR 308/72), BGHSt 25, 10 (12); OLG Karlsruhe, Beschl. v. 19.10.1973 (1 Ws 177/73), NJW 1974, 709 (711); *Eser*, in: *Schönke/Schröder*, StGB, § 74, Rn. 18; *Heger*, in: *Lackner/Kühl*, StGB, § 74, Rn. 1.

[1562] OLG Karlsruhe, Beschl. v. 19.10.1973 (1 Ws 177/73), NJW 1974, 709 (711); *Herzog/Saliger*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 74, Rn. 18.

[1563] OLG Karlsruhe, Beschl. v. 19.10.1973 (1 Ws 177/73), NJW 1974, 709 (711); *Heger*, in: *Lackner/Kühl*, StGB, § 74, Rn. 1.

[1564] *Herzog/Saliger*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 74, Rn. 39.

[1565] Vgl. *Eser*, in: *Schönke/Schröder*, StGB, § 74, Rn. 18; *Herzog/Saliger*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 74, Rn. 39.

[1566] So auch, *Weichert*, Google Glass, IT-Brillen und informationelle Selbstbestimmung, Virtuelles Datenschutzbüro - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutz.de/news/detail/?nid=5865 (7.4.2013).

rung von Beweismitteln, z.B. Stimmaufzeichnungen oder Bildaufnahmen, nutzen könnten.[1567]

Während die Fälle des Voyeurismus und der Beweissicherung ein vorsätzliches Vorgehen erfordern werden, wird es sonst möglicherweise an dem subjektiven Tatbestand mangeln, z.B. wenn ein Träger von Smartglasses mit aufnehmender oder übertragender Kamerafunktion zufällig eine Umkleidekabine, eine Toilette oder ein ärztliches Behandlungszimmer betritt. In solchen Fällen wird die Abgrenzung zwischen einem Eventualvorsatz und der nicht strafbaren groben Fahrlässigkeit schwerfallen. Es wird eine Tatfrage sein, ob der Träger von Smartglasses im Bewusstsein, dass das Gerät aktiv ist, diese Räumlichkeiten betreten und die Verletzung des höchstpersönlichen Bereiches in Kauf genommen oder eine hilflose Person abgelichtet hat. Ein weiteres Problem wird sich im Hinblick auf die Nachweisbarkeit der Rechtsverstöße stellen. Denn anders als bei einer Fotokamera oder einem Smartphone sind Smartglasses permanent auf das Geschehen vor dem Träger von Smartglasses gerichtet. D.h., wenn es an einer erkennbaren Aufnahmegeste fehlt, wird ein möglicher Aufnahmevorgang für die Opfer nicht erkennbar sein.[1568]

Der aus Art. 103 Abs. 2 GG abgeleitete Grundsatz in dubio pro reo verbietet es jedoch, alleine aus der Möglichkeit einer heimlichen Aufnahme auf deren Vorliegen zu schließen. Ansonsten würden die den Erfolg der Aufnahme, Übertragung, Zugänglichmachung oder des Gebrauchs nichtöffentlich gesprochenen Wortes, bzw. die Verletzung des höchstpersönlichen Bereichs voraussetzenden §§ 201 und 201a StGB zu Gefährdungsdelikten unqualifiziert.

IV. Zivilrechtlicher Schutz des Allgemeinen Persönlichkeitsrechts

Neben den Datenschutz- und den Strafvorschriften der §§ 201, 201a StGB wird das Allgemeine Persönlichkeitsrecht auch durch das Zivilrecht geschützt. Der Schutz hat zum Teil spezielle gesetzliche Normierungen erfahren, von denen im Rahmen dieser Untersuchung vor allem der Bildnisschutz gem. §§ 22 ff. KUG einschlägig ist.[1569] Daneben genießt das

[1567] Vgl. E IV. 1. k) cc) (1), S. 165.

[1568] Vgl. E IV. 1. g) bb), S. 155.

[1569] Vgl. *Mann*, in: *Spindler/Schuster*, Recht der elektronischen Medien, § 823 BGB, Rn. 6.

Allgemeine Persönlichkeitsrecht einen deliktischen Schutz als ein absolutes Recht i.S.d. § 823 Abs. 1 BGB.[1570]

Aufgrund des weiten Regelungsumfangs des § 6b BDSG, der die gesamte Nutzung von Smartglasses im öffentlichen Raum als eine Videoüberwachung versteht, stellt sich die Frage, inwieweit ein zusätzlicher zivilrechtlicher Schutz erforderlich ist. Dessen Bedürfnis ergibt sich jedoch bereits aus der Konzentration des Datenschutzes auf den Schutz des Rechts auf informationelle Selbstbestimmung. Im Unterschied dazu schützt das Zivilrecht das Allgemeine Persönlichkeitsrecht in allen seinen Ausprägungen. D.h., es umfasst u.U. auch das Recht am eigenen Bild, welches zum Teil andere Interessen schützt als der rein informationelle Datenschutz.[1571] Insoweit sind die Vorschriften des Zivilrechts neben § 6b BDSG anzuwenden.[1572]

1. Allgemeines Persönlichkeitsrecht als Auffangrecht

Zwar wurde das verfassungsrechtliche Allgemeine Persönlichkeitsrecht bereits untersucht, jedoch ist es mit seinem zivilrechtlichen Pendant strukturell nicht völlig deckungsgleich. Der Unterschied zeigt sich z.B. darin, dass das verfassungsrechtliche Allgemeine Persönlichkeitsrecht einen umfassenden Persönlichkeitsschutz bietet, der durch die Verfassung vorgegeben und damit der gesetzgeberischen Bestimmung im Wesentlichen entzogen ist.[1573] Dagegen ist die Gestaltung des einfachgesetzlichen Persönlichkeitsschutzes dem Willen des Gesetzgebers und seiner Einschätzungsprärogative unterstellt.[1574] Wegen der Unterschiede fragt es sich, ob verfassungsrechtliche Ergebnisse auf das zivilrechtliche Allgemeine Persönlichkeitsrecht übertragen werden können. Diese Frage ist jedoch zu bejahen, da etwaige einfachgesetzliche Schutzlücken (welche entstehen, wenn die einfachgesetzlichen Regelungen die verfassungsrechtlichen Mindeststandards unterschreiten) ohnehin durch das verfassungsrechtliche Allgemeine Persönlichkeitsrecht in einer zivilrechtlichen

---

[1570] BVerfG, Beschl. v. 14.2.1973 (1 BvR 112/65), BVerfGE 1973, 269 (281); BGH, Urt. v. 8.4.2011 (V ZR 210/10), NJW-RR 2011, 949 (950); BGH, Urt. v. 5.10.2004 (VI ZR 255/03), NJW 2005, 215 (216 ff.); BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1618); BGH, Urt. v. 14.2.1958 (I ZR 151/56), BGHZ 26, 349 (356 ff.); *Mann*, in: *Spindler/Schuster*, Recht der elektronischen Medien, § 823 BGB, Rn.2 ff.; *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823 BGB, Rn. 242.

[1571] Vgl. E II. 2. a) bb) (2), S. 106.

[1572] Vgl. F II. 1. f), S. 225.

[1573] Vgl. BVerfG, Beschl. v. 5.5.1987 (1 BvR 1113/85), BVerfGE 75, 318 (328); *Jarass*, NJW 1989, S. 857 (858).

[1574] Vgl. *Helle*, Persönlichkeitsrechte, 1969, S. 37 ff.; *Jarass*, NJW 1989, S. 857 (858); Nink in: *Spindler/Schuster*, Recht der elektronischen Medien, § 823, Rn. 6; *Schwerdtner*, JuS 1978, S. 289 (291).

Ausprägung als einem „Auffangrecht" ausgefüllt werden.[1575] Folglich spiegelt der einfachgesetzliche Persönlichkeitsschutz inhaltlich im Wesentlichen dessen verfassungsrechtliche Vorgaben wider, sodass insoweit ein einheitlicher Schutzumfang angenommen werden kann. Daher gelten die im Laufe dieser Untersuchung getroffenen Wertungen und erzielten Ergebnisse gleichermaßen für beide Ausprägungen des Persönlichkeitsschutzes.[1576]

2. Recht am eigenen Bild nach §§ 22 ff. KUG

Die Vorschriften der §§ 22 ff. KUG stellen die spezialgesetzliche Ausprägung des verfassungsrechtlich gewährleisteten Rechts am eigenen Bild dar.[1577] Jedoch regeln sie dessen Gewährleistungsgehalt nur beschränkt auf den Schutz vor Verfügungsverlust über Bildnisse in Fällen der Verbreitung und öffentlicher Zurschaustellung.[1578] Insbesondere wird die Herstellung von Bildnissen nicht erfasst.[1579] Da die Folgen der Verbreitung und Veröffentlichung von Bildnissen keine speziellen Probleme der Nutzung von Smartglasses darstellen, wird sich die nachfolgende Prüfung ihnen nur so weit widmen, wie sie für diese Untersuchung von Bedeutung sind.

a) Bildnis und Erkennbarkeit der Person

Das Schutzgut des § 22 BDSG ist das dem Recht am eigenen Bild entsprechende Bildnis, d.h. eine erkennbare Abbildung einer Person, als Ausdruck ihres Wesens und ihrer Persönlichkeit in einer dem Leben entsprechenden Erscheinung.[1580] Die Erkennbarkeit einer Person in dem Bildnis kann sich sowohl aus ihren Körpermerkmalen als auch aus zusätzlichen Informationen und den Umständen ergeben.[1581] Hierbei ist jedoch darauf zu achten, dass die Identifizierbarkeit einer Person nicht mit ihrer Er-

---

[1575] Vgl. BGH, Urt. v. 23.10.1979 (VI ZR 230/77), NJW 1980, 881 (882); BGH, Urt. v. 21.6.1966 (VI ZR 261/64), NJW 1966, 1617 (1619); *Schwerdtner*, JuS 1978, S. 289 (291); *Staudinger*, in: *Schulze*, BGB, § 823 BGB, Rn. 116; Wagner in: *Säcker/Rixecker*, MüKo BGB, § 823, Rn. 242.

[1576] So auch, *Jarass*, NJW 1989, S. 857 (858); *Piltz*, Soziale Netzwerke im Internet, 2013, S. 10; *Wieczorek*, Persönlichkeitsrecht und Meinungsfreiheit im Internet, 2013, S. 62.

[1577] Vgl. E II. 2. a) bb), S. 104; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 3.

[1578] Vgl. E II. 2. a) bb), S. 104.

[1579] OLG Frankfurt a.M., Urt. v. 15.6.2004 (11 U 5/04), ZUM-RD 2004, 576 (578); LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14),n.v.; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 11; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 9; *Golla/Herbort*, GRUR 2015, S. 648 (651).

[1580] Vgl. E II. 2. a) bb), S. 104; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 1; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 5.

[1581] Vgl. E II. 2. a) bb) (1), S. 105.

kennbarkeit gleichzusetzen ist.[1582] Da es nicht nur auf die Erkennbarkeit der Gesichtspartie ankommt, hebt ferner die Unkenntlichmachung eines Gesichts mittels Verpixelung oder schwarzer Balken die Erkennbarkeit nicht automatisch auf.[1583]

Von einer Erkennbarkeit ist auszugehen, wenn die abgebildete Person begründeten Anlass zu der Annahme hat, sie könnte möglicherweise von Dritten erkannt werden, auch wenn es nur Personen aus ihrem Bekanntenkreis sind.[1584] Nicht ausreichend ist dagegen, wenn die Person nur vom engsten Freundes- und Familienkreis erkannt wird, denn die Erkennbarkeit muss sich auf einen Personenkreis erstrecken, den die beeinträchtigte Person nicht selbst unterrichten oder überschauen kann.[1585]

Der Bildnisschutz erstreckt sich auf alle Arten der Darstellung, also auch auf Filme und Videos, die in Datenform gespeichert und ausschließlich mittels Technik menschlicher Sehwahrnehmung zugänglich gemacht werden können.[1586] Auch wenn die Abbildung erkennbarer Personen mithilfe von Smartglasses live übertragen wird, handelt es sich bei dem

---

[1582] Vgl. E II. 2. a) bb) (1), S. 105; wird eine Person auf ein Bildnis angesprochen, so wird darin die Bestätigung der Erkennbarkeit gesehen, LG Frankfurt a.M., Urt. v. 19.1.2006 (2/03 O 468/05), ZUM-RD 2006, 357 (358); *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 4; dies gilt jedoch nur, wenn die Ansprache eine direkte Folge der Erkennbarkeit der Person war und sie nicht aufgrund anderer Umstände, wie z.B. einer zulässigen Presseberichterstattung angesprochen wurde; AG Kerpen, Urt. v. 25.11. 2010 (102 C 108/10), BeckRS 2011, 10636.

[1583] Vgl. E IV. 1. j), S. 161; LG Düsseldorf, Urt. v. 16.11.2011 (12 O 438/10), ZUM-RD 2012, 407 (464); LG Hamburg, Urt. v. 27.2.2009 (324 O 703/08), BeckRS 2009, 18575; VGH Mannheim, Urt. v. 10.7.2000 (1 S 2239/99), NVwZ 2001, 1292 (1293); *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 3; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 20; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 7; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 116.

[1584] BGH, Urt. v. 26.6.1979 (VI ZR 108/78), GRUR 1979, 732 (733); BGH, Urt. v. 10.11.1961 (I ZR 78/60), GRUR 1962, 211; LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14), n.v.; AG Kerpen, Urt. v. 25.11.2010 (102 C 108/10), BeckRS 2011, 10636; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 4; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 7.

[1585] LG Köln, Urt. v. 3.11.2004 (28 O 731/03), ZUM-RD 2005, 351 (353); AG Kerpen, Urt. v. 25.11.2010 (102 C 108/10), BeckRS 2011, 10636.

[1586] BAG, Urt. v. 11.12.2014 (8 AZR 1010/13), ZUM 2015, 604 (606); OLG Frankfurt a.M., Urt. v. 15.6.2004 (11 U 5/04), ZUM-RD 2004, 576 (578); *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 1; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 20; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 5; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 349.

Inhalt der Übermittlung um ein Bildnis.[1587] Ebenso können biometrische Templates bei hinreichendem Erkennbarkeitsgrad Bildnisse darstellen.[1588]

aa) Öffentliche Zurschaustellung

Unter einer Zurschaustellung wird die unkörperliche Sichtbarmachung eines Bildnisses verstanden, bei der das Publikum keine Verfügungsgewalt über das Bildnis erhält.[1589] Der Begriff entspricht dem Verständnis der öffentlichen Wiederhabe gem. § 15 Abs. 3 UrhG oder der öffentlichen Zugänglichmachung gem. § 19a UrhG.[1590] Eine Zurschaustellung kann nicht nur durch Massenmedien wie Film und Fernsehen erfolgen, sondern vor allem auch durch das Internet.[1591]

bb) Verbreitung

Der ursprünglich körperlich verstandene Verbreitungsbegriff wird nunmehr auch bei unkörperlicher Verbreitung von Bildnissen in Datenform angewandt.[1592] Denn die durch § 22 KUG geregelte Gefahr des Verfügungsverlustes über ein Bildnis realisiert sich mit gleicher, wenn nicht mit höherer Wirkung bei Übertragung von Daten an Dritte.[1593] Für eine Verbreitung ist es jedoch nicht ausreichend, dass das Bildnis lediglich jemandem visuell vermittelt wird, z.B. durch das Vorzeigen eines Bildes oder Vorspielen eines Videos.[1594] Die Live-Übertragung der Abbildung einer Person an einen oder mehrere Empfänger stellt dagegen eine Verbreitung dar, da die Empfänger eine Bildschirmkopie erstellen und so das übertragene Bildnis fixieren können.[1595]

[1587] Vgl. E II. 2. b) cc), S. 114; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 348.

[1588] Vgl. E II. 2. b) dd) (2), S. 117.

[1589] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 10; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 54; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 7.

[1590] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 10.

[1591] Vgl. F II. 1. c) cc) (2) (e), S. 201; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 10; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 10.

[1592] OLG Frankfurt a.M., Urt. v. 15.6.2004 (11 U 5/04), ZUM-RD 2004, 576 (578); LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14), n.v.; LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 9; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 53; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 8; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 120 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 348 ff.

[1593] Vgl. E II. 2. b) bb), S. 114.

[1594] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 350.

[1595] Vgl. E II. 2. b) cc), S. 114.

Der Verfügungsverlust tritt grundsätzlich mit der Erweiterung des Zugriffskreises auf das Bildnis um eine Person ein.[1596] Damit ist auch die Weitergabe im privaten Kreis, z.B. in sozialen Netzwerken und zu gleich welchen Zwecken, z.B. als Beweismittel vor Gericht, als Verbreitung zu verstehen.[1597] Allenfalls die Zugänglichmachung der Bildaufnahme im ausschließlich persönlichen und familiären Kreis soll nach einer zum Teil vertretenen Ansicht keine Verbreitung darstellen.[1598] Diese mit der Ausnahme ausschließlich persönlicher und familiärer Tätigkeit im § 1 Abs. 2 Nr. 3 BDSG harmonierende Ansicht erscheint überzeugend, da der Zweck des § 22 KUG im Schutz vor Verfügungsverlust über Bildnisse besteht.[1599] Ob allerdings das Hochladen der Bildnisse auf Server von Drittanbietern (jedoch zugangsbeschränkt auf Freunde und Familie) noch von dieser Ausnahme erfasst ist, erscheint zweifelhaft und muss anhand der Sicherheitsstandards und der Gefahren dieser Datenübermittlung, z.B. durch missbräuchlichen Zugriff Dritter, beurteilt werden.[1600]

cc) Einwilligung

§ 22 Satz 1 KUG erlaubt es, ein Bild auf Grundlage einer Einwilligung zu verbreiten oder zu veröffentlichen. Insoweit kann an dieser Stelle auf die entsprechend anwendbaren Ausführungen zur datenschutzrechtlichen Einwilligung verwiesen werden.[1601]

b) Ausnahmen des § 23 KUG

Ohne eine Einwilligung ist die Verbreitung oder Veröffentlichung von Bildnissen nur in den Fällen des § 23 Abs. 1 KUG zulässig, die eine grundgesetzlich vorgegebene Interessenabwägung zwischen den Interes-

---

[1596] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 9; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 51 ff.; *Golla/Herbort*, GRUR 2015, S. 648; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 120 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 350.

[1597] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 9; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 52; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 9; a.A. jedoch ohne Argumente zu benennen, *Balzer/Nugel*, NJW 2014, S. 1622 (1625).

[1598] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 9; *Strobl-Albeg*, in: *Wenzel u.a.*, Recht der Wort- und Bildberichterstattung, 2003, S. Kap.7, Rn. 43.

[1599] Dabei spricht auch der Wortlaut für eine solche Auslegung, da eine "Verbreitung" sinngemäß erst dann vorliegt, wenn etwas "in einem weiten Umkreis bekannt wird", "in einen weiteren Umkreis gelangt" oder "sich ausbreitet", Duden, 2013, Stichwort „verbreiten“; ebenso erscheint eine fehlende explizite Ausnahme für den persönlichen Bereich angesichts der, zum Zeitpunkt des Inkrafttretens des § 22 KUG im Jahr 1907 nicht vorhandenen Gefahr privater Massenverbreitung von Bildnissen, als nachvollziehbar, vgl. *Leffler*, Cyber-Bullying, 2012, S. 56.

[1600] Vgl. F II. 1. c) cc) (2) (e), S. 201.

[1601] Vgl. F II. 2. b), S. 228.

sen der über das Bildnis Verfügenden und dem Persönlichkeitsrecht der Betroffenen konkretisieren.[1602]

aa) Öffentliches Ereignis

Nach § 23 Abs. 1 Nr. 1 KUG dürfen Personen im Rahmen von Bildnissen „aus dem Bereich der Zeitgeschichte" abgebildet werden.[1603] Der Bereich der Zeitgeschichte umfasst gleich welche Erscheinungen im Leben der Gegenwart, die von der Öffentlichkeit beachtet werden, bei ihr Aufmerksamkeit finden und „Gegenstand der Teilnahme oder Wissbegier weiter Kreise sind".[1604] Hierzu können auch Unfälle, Verbrechen oder Naturkatastrophen gehören sowie lediglich lokale Vorgänge, die kein dauerhaftes Interesse auslösen.[1605] Ebenso kann sich das öffentliche Ereignis auf andere Personen als diejenigen, die es auslösen, erstrecken.[1606]

Nicht ausreichend ist dagegen, wenn die Bildberichterstattung sich darauf beschränkt, irgendeinen Anlass für die Abbildung einer Person zu schaffen.[1607] Ferner ist die inhaltliche Seriosität oder Qualität von Berichten zwar nicht relevant, jedoch ist deren Beitrag zur öffentlichen Meinungsbildung ein Abwägungskriterium.[1608] Die Verbreitung von alltäglichen Schnappschüssen, auch wenn sie Neugierde wecken oder das Sensationsbedürfnis befriedigen würden, wird daher nicht der Ausnahme des

---

[1602] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 1.

[1603] Vgl. weiterführend die Rechtsprechung zu Bildnissen von Prominenten, EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051; BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180; BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 3.

[1604] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (203); BGH, Urt. v. 28.10.2008 (VI ZR 307/07), BGHZ 178, 213 (216); RG, Urt. v. 26.6.1929 (I 97/29), RGZ 125, 80 f.; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 3 f.

[1605] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 3.

[1606] Vgl. BGH, Urt. v. 21.4.2015 (VI ZR 245/14), BeckRS 2015, 10534 (Rn. 10 ff.); BGH, Urt. v. 11.11.2014 (VI ZR 9/14), ZUM 2015, 329 (329 f.); m.w.N., *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 23 KUG, Rn. 10.

[1607] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (206 f.).

[1608] BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1196); BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (205 f.); BGH, Urt. v. 19.6.2007 (VI ZR 12/06), GRUR 2007, 899 (901); BGH, Urt. v. 19.10.2004 (VI ZR 292/03), NJW 2005, 594 (595 f.); *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 11 f.

§ 23 Abs. 1 Nr. 1 KUG unterfallen.[1609] Auch wenn sich eine Person gegen Bildaufnahmen zu Wehr setzt, z.B. gegen einen Träger von Smartglasses vorgeht, würde diese Situation von sich aus im Regelfall noch kein öffentliches Ereignis i.S.d. 23 Abs. 1 Nr. 1 KUG darstellen.[1610]

bb) Unwesentliche Beiwerke

§ 23 Abs. 1 Nr. 2 KUG enthält eine Ausnahme für Aufnahmen, in denen die abgebildeten Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen.[1611] Es handelt sich jedoch nur um Fälle, in denen die Örtlichkeit im Vordergrund steht, die Personenabbildung ihr also so untergeordnet ist, dass sie ohne den Charakter des Bildes zu verändern, entfallen könnte.[1612] Vor allem wenn die Person aufgrund ihrer Merkmale, wie z.B. der Nacktheit oder einer Notlage,[1613] in das Zentrum der Aufmerksamkeit rückt, stellt sie kein Beiwerk mehr dar.[1614] Ebenso wird bei einer Erstellung von Aufnahmen zu Beweiszwecken davon auszugehen sein, dass die mit Absicht abgebildeten Personen nicht bloß als Beiwerk dienen, sondern geradezu aus der Anonymität gelöst werden sollen.[1615] Auch wenn Personen erst nachträglich „herausvergrößert, herausgeschnitten bzw. maskiert und alleingestellt“ werden, und so in den Vordergrund des Bildes rücken, stellen sie keine unwesentlichen Beiwer-

---

[1609] Vgl. EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051 (1053 f.); BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (190 ff.); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (395 f.); BGH, Urt. v. 18.10.2011 (VI ZR 5/10), ZUM 2012, 140 (141); BGH, Urt. v. 28.10.2008 (VI ZR 307/07), BGHZ 178, 213 (216); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 4.

[1610] Umkehrschluss aus dem vom KG Berlin entschiedenem Fall, in dem die Berechtigung zur Berichterstattung alleine aus der Prominenz der sich wehrenden Person bezogen wurde, KG, Urt. v. 2.3.2007 (9 U 212/06), ZUM 2007, 475 (476 ff.).

[1611] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 35; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 24.

[1612] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 35; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 24.

[1613] OLG Karlsruhe, Urt. v. 18.8.1989 (14 U 105/88), GRUR 1989, 823 (824); OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); OLG München, Urt. v. 13.11.1987 (21 U 2979/87), NJW 1988, 915 (916).

[1614] BGH, Urt. v. 26.6.1979 (VI ZR 108/78), GRUR 1979, 732 (734); OLG Karlsruhe, Urt. v. 18.8.1989 (14 U 105/88), GRUR 1989, 823 (824); OLG Düsseldorf, Urt. v. 30.9.1969 (20 U 80/69), GRUR 1970, 618 (619); LG Oldenburg, Beschl. v. 23.1.1986 (5 O 3667/85), GRUR 1986, 464 (465); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 24; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 124 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 353.

[1615] *Lachenmann/Schwiering*, NZV 2014, S. 291 (293).

ke mehr dar.[1616] Es ist auch bei den von Smartglasses erstellten Aufnahmen damit zu rechnen, dass eine Vielzahl von Personen als Beiwerk erfasst wird. Jedoch ist aufgrund der den Kopfbewegungen folgenden Smartglasses ebenso davon auszugehen, dass Personen häufig im Zentrum der Aufnahmen stehen und damit keine Beiwerke darstellen werden.

cc) Bilder von Versammlungen

Die Ausnahme des § 23 Abs. 1 Nr. 3 KUG bestimmt, dass Personen, die in der Öffentlichkeit an Veranstaltungen, Aufzügen und ähnlichen Vorgängen teilnehmen, damit rechnen müssen, in deren Zuge abgelichtet zu werden.[1617] Der Begriff der „Versammlungen, Aufzüge und ähnlichen Vorgänge" ist weit auszulegen und umfasst alle Zusammentreffen von Menschen, die den kollektiven Willen haben, etwas gemeinsam zu unternehmen und davon ausgehen müssen, von Dritten dabei als Teil einer solchen Gruppe wahrgenommen zu werden.[1618]

dd) Interessenabwägung gem. § 23 Abs. 2 KUG

Auch wenn die Ausnahmen des § 23 Abs. 1 KUG einschlägig sind, können im Einzelfall gem. § 23 Abs. 2 KUG berechtigte Interessen der Abgebildeten der Verbreitung und Zurschaustellung von Bildnissen entgegenstehen. Hierzu gehören insbesondere Fälle, in denen die Aufnahmen unter Verletzung der räumlichen Privatsphäre entstanden sind sowie private oder gar intime Vorgänge festhalten.[1619] Ein höheres Interesse der Abgebildeten wird regelmäßig dann bejaht, wenn diese unbekleidet oder teilbekleidet abgebildet wurden, da der nackte Körper zum intimsten Persön-

---

[1616] OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); OLG München, Urt. v. 13.11.1987 (21 U 2979/87), NJW 1988, 915 (916); *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 36.

[1617] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 38 f.; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 25.

[1618] OLG Celle, Urt. v. 25.8.2010 (31 Ss 30/10), ZUM 2011, 341 (344); OLG München, Urt. v. 13.11.1987 (21 U 2979/87), NJW 1988, 915 (916).

[1619] BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (215); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (395 f.); LG Berlin, Urt. v. 4.9.2007 (27 O 591/07), ZUM 2007, 866 (868); LG Hamburg, Urt. v. 8.5.1998 (324 O 736/97), ZUM 1998, 852 (859); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 30 f.

lichkeitsbereich eines jeden Menschen gehört.[1620] Dasselbe gilt auch für die Abbildung von Personen in einer durch eine Krankheit oder den Tod geprägten Situation.[1621] Ebenso ist es entscheidend, ob eine Person auf dem Bild kaum erkennbar ist oder umgekehrt deutlich zu erkennen ist.[1622] Ferner müssen eventuelle Gefahren für die abgebildete Person berücksichtigt werden, z.B. in Form von Racheakten Dritter.[1623] Auch heimliche oder überrumpelnde Aufnahmen bringen eine höhere Beeinträchtigung für Persönlichkeitsrechte mit sich.[1624]

c) Ausnahme des § 24 KUG

§ 24 KUG erlaubt es Behörden, Bildnisse für Zwecke der Rechtspflege und der öffentlichen Sicherheit ohne Einwilligung der abgebildeten Personen zu veröffentlichen. Diese Vorschrift ist jedoch nur auf behördliches Handeln beschränkt und privilegiert Privatpersonen nur dann, wenn diese mit behördlicher Erlaubnis handeln.[1625] Dagegen sind private Fahndungsaufrufe, wie z.B. Fahndungsbilder von Privatdetektiven, nicht privilegiert.[1626]

[1620] BGH, Urt. v. 21.4.2015 (VI ZR 245/14), BeckRS 2015, 10534 (Rn. 10 ff.); BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617; OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); OLG Stuttgart, Urt. v. 16.12.1981 (4 U 88/81), NJW 1982, 652 (653); LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319; LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (789); LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002; LG München I, Urt. v. 30.7.2003 (21 O 4369/03), NJW 2004, 617 (618); *Sofsky*, Verteidigung des Privaten, 2007, S. 59.

[1621] OLG Karlsruhe, Urt. v. 14.10.1998 (6 U 120–97), NJW-RR 1999, 169 (1700); OLG München, Urt. v. 13.11.1987 (21 U 2979/87), NJW 1988, 915 (916); OLG Hamburg, Urt. v. 7.7.1983 (3 U 7/83), AfP 1983, 466 (468); LG Essen, Urt. v. 10.7.2014 (4 O 157/14), BeckRS 2014, 17008; LG Frankfurt/Oder, Urt. v. 25.6.2013 (16 S 251/12), BeckRS 2013, 12059; LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (789); LG Köln, Urt. v. 29.6.1994 (28 S 3/94), NJW-RR 1995, 1175 (1176); AG Mannheim, Urt. v. 11.7.2008 (3 C 154/08), BeckRS 2008, 13697; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 39; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 34 f.

[1622] LG Köln, Urt. v. 29.6.1994 (28 S 3/94), NJW-RR 1995, 1175 (1176).

[1623] VGH Baden-Württemberg, Urt. v. 19.8.2010 (1 S 2266/09), ZUM-RD 2011, 126 (130 f.).

[1624] EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051 (1054 f.); BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (217); BGH, Urt. v. 6.3.2007 (VI ZR 51/06), GRUR 2007, 527 (528); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 36.

[1625] OLG München, Urt. v. 14.5.1970 (1 U 721/70), NJW 1970, 1745; LG Köln, Urt. v. 21.4.2004 (28 O 141/04), ZUM 2004, 495 (497); *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 6; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 3.

[1626] *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 23 KUG, Rn. 6; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 3.

Daher scheidet die Berufung auf § 24 KUG für Nutzer von Smartglasses im Regelfall aus.[1627]

d) Rechtsfolgen nach §§ 33 ff. KUG

Nach § 33 KUG droht Nutzern von Smartglasses bei Verstößen gegen § 22 KUG eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe, sofern der erforderliche Strafantrag gestellt wurde.

Gemäß § 37 KUG können sowohl die widerrechtlich hergestellten, verbreiteten, vorgeführten oder zur Schau gestellten Exemplare der Bildnisse als auch die zur widerrechtlichen Vervielfältigung, Vorführung oder Zurschaustellung ausschließlich bestimmten Vorrichtungen vernichtet werden. Dies gilt gem. § 50 KUG zumindest so lange, wie die Bildexemplare noch vorhanden sind. Gem. § 38 KUG kann statt der Vernichtung die Herausgabe der Bildexemplare und Vorrichtungen verlangt werden. Dieser Anspruch kam im Regelfall im Hinblick auf die Herausgabe analoger Bildnegative zur Geltung.[1628] Jedoch erscheint es sachgerecht, ihn auch im Hinblick auf die Herausgabe digitaler Aufnahmen anzuwenden, z.B. damit die betroffene Person mit ihnen unter Zuhilfenahme einer Bildähnlichkeitssuche überprüfen kann, ob die Aufnahmen bereits im Internet Verbreitung gefunden haben.[1629]

3. Andere Fallgruppen des Allgemeinen Persönlichkeitsrechts

Neben den §§ 22 ff. KUG wird das Allgemeine Persönlichkeitsrecht als ein absolutes „sonstiges Recht“ i.S.d. § 823 Abs. 1 BGB deliktisch geschützt.[1630] Um dessen Prüfung zu strukturieren, werden ähnlich seiner verfassungsrechtlichen Ausprägung einzelne Fallgruppen des zivilrechtli-

---

[1627] Allenfalls könnte sich ein Recht zur Veröffentlichung aus § 23 Abs. 1 Nr. 1 KUG ergeben, jedoch müsste sich die Straftat von der gewöhnlichen Kriminalität abheben, um als ein zeitgeschichtliches Ereignis gelten zu können, BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1196 f.); BVerfG, Beschl. v. 27.11.2008 (1 BvQ 46/08), NJW 2009, 350 (351); BVerfG, Urt. v. 5.6.1973 (1 BvR 536/72), BVerfGE 35, 202 (231 ff.); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 15.

[1628] Vgl. OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123; LG Oldenburg, Beschl. v. 21.4.1988 (5 S 1656/87), GRUR 1988, 694 (695).

[1629] Vgl. E II. 2. b) dd) (3), S. 118.

[1630] BGH, Urt. v. 19.5.1981 (VI ZR 273/79), BGHZ 80, 311 (319); OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123; LG Darmstadt, Urt. v. 17.3.1999 (8 O 42/99), NZM 2000, 360; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 3.

chen Allgemeinen Persönlichkeitsrechts gebildet, die ebenso weder trennscharf abgegrenzt noch abschließend sind. [1631]

Im Unterschied zu § 22 KUG setzt eine Verletzung des zivilrechtlichen Allgemeinen Persönlichkeitsrechts ebenso wie bei dessen verfassungsrechtlichem Pendant die Feststellung einer fehlenden Rechtfertigung durch entgegenstehende berechtigte Interessen voraus.[1632] Entsprechend dem Ergebnis der verfassungsrechtlichen Prüfung wird aufgrund einer gegen die Menschenwürde verstoßenden Eingriffsintensität von Smartglasses bei ihrer Nutzung im öffentlichen Raum auch im Zivilrecht regelmäßig eine Verletzung des Allgemeinen Persönlichkeitsrechts anzunehmen sein.[1633] Wie schon im Fall des § 22 KUG und des Datenschutzrechts kommt auch eine wirksame Einwilligung, eine Notwehr- bzw. notwehrähnliche Lage oder eine medizinischer Indikation als ein Rechtfertigungsgrund der Persönlichkeitsrechsverletzung in Frage.[1634] Jedoch wird es sich auch an dieser Stelle um seltene Ausnahmefälle handeln.[1635] D.h., die Nutzung von Smartglasses im öffentlichen Raum wird im Regelfall einen Verstoß gegen § 823 Abs. 1 BGB darstellen, sobald Personen in deren Erfassungsbereich geraten. Aufgrund dieser Vorprägung des Ergebnisses der Abwägung werden die Fallgruppen des zivilrechtlichen Allgemeinen Persönlichkeitsrechts nachfolgend nur übersichtsartig geprüft.

a) Herstellung von Bildnissen

Der Schutz vor Herstellung vor Bildnissen komplementiert den § 22 KUG um einen Schutz vor Gefahren, die sich bereits aus der Fixierung eines

---

[1631] Vgl. E II. 2. a), S. 94; BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180 (207); BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (41 f.); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (395 f.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 345, 366; *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823 BGB, Rn. 242.

[1632] St. Rspr., BGH, Urt. v. 21.6.2005 (VI ZR 122/04), GRUR 2005, 788 (790); BGH, Urt. v. 19.12.1978 (VI ZR 137/77), BGHZ 73, BGHZ 73 (124); BGH, Urt. v. 20.3.1968 (I ZR 44/66), BGHZ 50, 133 (143); BGH, Urt. v. 2.4.1957 (VI ZR 9/56), BGHZ 24, 72 (80); BGH, Urt. v. 25.5.1954 (I ZR 211/53), BGHZ 13, 334 (338); OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971; OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087 (1088); *Golla/Herbort*, GRUR 2015, S. 648 (651); *Kopke*, NZA 1999, S. 917 (918).

[1633] Vgl. E V, S. 181.

[1634] Vgl. E V, S. 181.

[1635] Vgl. F II. 1. d) bb) (2), S. 210.

Bildnisses ergeben.[1636] Diese Gefahren ergeben sich aus dem Umstand, dass Aufnahmen z.B. von dem Nutzer der Smartglasses heimlich verbreitet, veröffentlicht oder je nach Entwicklungsstand biometrisch ausgewertet werden könnten.[1637] Dementsprechend stellt die Herstellung von Bildnissen keine Gefahr dar, wenn entsprechend den §§ 22 ff. KUG bei der Herstellung ein Fall des § 23 KUG angenommen werden kann.[1638]

b) Abhören, Aufzeichnen oder Wiedergeben des nicht öffentlich gesprochenen Wortes

Auch das Zivilrecht schützt das Recht des Einzelnen, frei und unbefangen kommunizieren zu können, ohne den Argwohn hegen zu müssen, dass Dritte vertrauliche Gespräche abhören, aufzeichnen, veröffentlichen, verändern oder gegen den Betroffenen verwenden.[1639] Insbesondere darf jeder Mensch selbstbestimmt den Adressatenkreis der eigenen Worte bestimmen und entscheiden, ob diese nur bestimmten Personen oder der Öffentlichkeit zugänglich gemacht werden.[1640] Eine Beeinträchtigung dieses Rechts liegt schon dann vor, wenn einzelne Gesprächsfetzen unerlaubterweise aufgezeichnet werden, sofern sie für sich einen Sinn erge-

---

[1636] Vgl. BVerfG, Beschl. v. 24.7.2015 (1 BvR 2501/13), ZUM 2015, 986 (987 f.); BGH, Urt. v. 16.3.2010 (VI ZR 176/09), NJW 2010, 1533 (1534); BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955 (1957); BGH, Urt. v. 16.9.1966 (VI ZR 268/64), GRUR 1967, 205 (208); BGH, Urt. v. 10.5.1957 (I ZR 234/55), BGHZ 24, 200 (208); OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087 (1088); OLG Hamburg, Urt. v. 13.7.1989 (3 U 30/89), GRUR 1990, 35; OLG Frankfurt, Urt. v. 9.1.1958 (6 U 77/57), GRUR 1958, 508 (509); LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (788); LG Oldenburg, Beschl. v. 21.4.1988 (5 S 1656/87), GRUR 1988, 694 (695); VGH München, Beschl. v. 16.10.2014 (10 ZB 13.2620), NVwZ-RR 2015, 104 (1); *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 12; *Golla/Herbort*, GRUR 2015, S. 648 (650); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 9.

[1637] Vgl. E II. 2. b), S. 113; vgl. BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 354.

[1638] Vgl. F IV. 2. b), S. 268; OLG Brandenburg, Urt. v. 21.5.2012 (1 U 26/11), NJW-RR 2012, 1250 (1251); OLG Frankfurt a.M., Urt. v. 25.8.1994 (6 U 296/93), NJW 1995, 878 (880); KG, Urt. v. 5.7.1979 (12 U 1277/79), NJW 1980, 894; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 12 f.; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 9; *Golla/Herbort*, GRUR 2015, S. 648 (651).

[1639] Vgl. E II. 2. a) cc), S. 107; st. Rspr., BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (39); BVerfG, Beschl. v. 19.12.1991 (1 BvR 382/85), NJW 1992, 815; BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238; BGH, Urt. v. 10.3.1987 (VI ZR 244/85), NJW 1987, 2667; BGH, Urt. v. 16.3.1983 (2 StR 775/82), NJW 1983, 1569; BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277; BGH, Urt. v. 19.12.1978 (VI ZR 137/77), BGHZ 73, BGHZ 73 (123); BGH, Urt. v. 14.6.1960 (1 StR 683/59), NJW 1960, 1580; BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284; *Di Fabio*, in: *Maunz/Dürig*, GG, Art.2 GG, Rn. 196.

[1640] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 128.

ben.[1641] Die Gefahr besteht genauso wie im Fall der Bildherstellung, wenn Smartglasses im öffentlichen Raum z.B. Audiosignale alleine bzw. als Bestandteil von Videos aufnehmen oder die Gespräche in der Umgebung elektronisch analysieren.[1642]

Auch wenn die akustische Aufnahme dem Beweis dienen soll, werden entsprechend den Ausführungen zu § 201 StGB hohe Anforderungen an die Intensität der nachzuweisenden Rechtsverletzung erforderlich sein.[1643] Ein „schlichtes Beweisinteresse" alleine vermag einen Eingriff in das Persönlichkeitsrecht der Betroffenen nicht zu rechtfertigen.[1644] Das gilt ganz besonders, wenn die Aufnahme heimlich erfolgt oder ihr eine Überlistung des Betroffenen vorausgeht.[1645] Eine Rechtfertigung wird in der fachgerichtlichen Rechtsprechung angenommen, wenn sich der Beweisführer in einer Notwehrsituation oder einer notwehrähnlichen Lage befindet.[1646] Dabei wird im Rahmen der Erforderlichkeit der Aufnahme zu berücksichtigen sein, ob der Rückgriff auf andere, gleich wirksame Beweismittel nicht zumutbar war.[1647] Erst recht reicht ein Bequemlichkeitsinteresse, wie der Wunsch, eine Aufnahme als Gedächtnisstütze zu nutzen, zur Rechtfertigung des Abhörens nicht aus.[1648]

c) Verletzung der Privatsphäre

Wenn Smartglasses innerhalb von räumlichen Rückzugsbereichen getragen werden, verletzen sie das berechtigte Vertrauen der sich in den Bereichen aufhaltenden Personen auf den Schutz ihrer Privatsphäre.[1649] Die Verletzung der Privatsphäre kann vor allem im Rahmen der anderen Fallgruppen des Allgemeinen Persönlichkeitsrechts zur Begründung oder Intensivierung eines Eingriffs durch Smartglasses beitragen (z.B. wenn

---

[1641] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (41); vgl. BGH, Urt. v. 10.3.1987 (VI ZR 244/85), NJW 1987, 2667 (2668 ff.); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (286).

[1642] Vgl. E II. 2. b) dd) (4), S. 119.

[1643] Vgl. F III. 1. c), S. 249.

[1644] BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28 (50); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (290).

[1645] BGH, Urt. v. 3.6.1997 (VI ZR 133/96), NJW 1998, 155 (155); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (290).

[1646] BGH, Urt. v. 3.6.1997 (VI ZR 133/96), NJW 1998, 155 (155); BGH, Urt. v. 27.1.1994 (I ZR 326/91), NJW 1994, 2289 (2292 f.); BGH, Urt. v. 13.10.1987 (VI ZR 83/87), NJW 1988, 1016 (1017); BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277 (278); BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (289 f.).

[1647] BGH, Urt. v. 27.1.1994 (I ZR 326/91), NJW 1994, 2289 (2292 f.).

[1648] BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284 (290).

[1649] Vgl. E II. 2. a) dd) (1), S. 110.

Personenaufnahmen in einem privaten Bereich erstellt werden).[1650] Zu solchen Rückzugsräumen gehören z.B. Saunen, Duschen, Toiletten oder Umkleidebereiche.[1651] Ebenso zu einem räumlichen Privatbereich gehören ein unvollkommen beleuchtetes Gartenlokal[1652] wie auch ein nur vom Wasser aus zugänglicher Strand[1653] oder das Innere einer Kirche.[1654]

Das zivilrechtliche Allgemeine Persönlichkeitsrecht schützt Menschen auch vor Preisgabe von Informationen, deren Bekanntwerden sie in ihrer persönlichen Entfaltung, z.B. wegen eines moralischen Drucks seitens Mitmenschen, hemmen würde.[1655] Zu diesen Themenbereichen gehören typischerweise Informationen, die das Krankheitsleben, die Sexualsphäre, den (teil)nackten Körper,[1656] aber auch emotionale Ausnahmesituation, z.B. nach einem schweren Verkehrsunfall, betreffen.[1657] Anders als im Fall des Rechts am eigenen Bild muss die Person auf den Aufnahmen nicht

---

1650 EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051 (1052 ff.); BVerfG, Beschl. v. 2.5.2006 (1 BvR 507/01), NJW 2006, 2836 (2837); BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (384); BGH, Urt. v. 19.12.1995 (VI ZR 15/95), NJW 1996, 1128 (1129); Dreier/Schulze in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn.22 ff.

1651 BT-DrS. 14/5793, S. 62; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 23 KUG, Rn. 31 m.w.N.; vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 141; *Nguyen*, DuD 2011, S. 715 ff.; *Schmitz*, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, 2011, S. 40 ff.; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 99 ff.

1652 BGH, Urt. v. 19.12.1995 (VI ZR 15/95), NJW 1996, 1128 (1128 f.).

1653 LG Hamburg, Urt. v. 8.5.1998 (324 O 736/97), ZUM 1998, 852 (859).

1654 OLG Hamburg, Urt. v. 10.10.2000 (7 U 138/99), OLG Report 2001, 139 (140).

1655 Vgl. E II. 2. a) dd) (2), S. 112; vgl. BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361 (382); BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367 (373 ff.); BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373; BGH, Urt. v. 28.10.2008 (VI ZR 307/07), BGHZ 178, 213; *Horst*, NZM 2000, S. 937 (938 f.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 142.

1656 BGH, Urt. v. 21.4.2015 (VI ZR 245/14), BeckRS 2015, 10534 (Rn. 10 ff.); BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617; OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); OLG Stuttgart, Urt. v. 16.12.1981 (4 U 88/81), NJW 1982, 652 (653); LG Essen, Urt. v. 10.7.2014 (4 O 157/14), BeckRS 2014, 17008; LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319 (19319); LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (789); Ebenda; LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002; LG München I, Urt. v. 30.7.2003 (21 O 4369/03), NJW 2004, 617 (618); AG Mannheim, Urt. v. 11.7.2008 (3 C 154/08), BeckRS 2008, 13697; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 142 f.; *Sofsky*, Verteidigung des Privaten, 2007, S. 69 ff.

1657 OLG Köln, Urt. v. 26.3.2013 (15 U 149/12), ZUM 2013, 684 (687).

erkennbar sein, z.B. wenn diese einen Rückenakt, einen Torso oder ein Geschlechtsteil zeigen.[1658]

d) Erhebung und Verwendung personenbezogener Daten

Als Auffanggrundrecht umfasst das zivilrechtliche Allgemeine Persönlichkeitsrecht auch den Schutz des Rechts auf informationelle Selbstbestimmung.[1659] Da jedoch die Regelung des § 6b BDSG praktisch die gesamte Nutzung von Smartglasses im öffentlichen Raum umfasst, ergeben sich keine Schutzlücken, die zu füllen wären.[1660] Allenfalls wenn man im Gegensatz zum Ergebnis dieser Untersuchung eine persönlich-familiäre Nutzung von Smartglasses annehmen würde, müsste im Rahmen des § 823 Abs. 1 BGB die Rechtswidrigkeit privater Videoüberwachung geprüft werden.[1661]

e) Maßnahmen zur Erzeugung von Überwachungsdruck

Das Allgemeine Persönlichkeitsrecht schützt auch vor der von Smartglasses ausgehenden Einschüchterungswirkung, die zu autonomiebeeinträchtigenden Überwachungs- und Anpassungseffekten führen kann.[1662] Jedoch ist dieser Überwachungsdruck auch in dieser Konstellation vom Regelungsbereich des § 6b Abs. 1 BDSG umfasst, der bereits beim Vorliegen der technischen Möglichkeit einer Aufnahme unabhängig von ihrer tatsächlichen Durchführung einschlägig ist.[1663] D.h., der Schutz vor Erzeugung von Überwachungsdruck wird praktisch nur im Fall von Smartglasses ohne eine Kamera einschlägig sein, die jedoch nicht Gegenstand dieser Untersuchung sind.[1664] Im Übrigen steigern Überwachungs- und Anpas-

---

[1658] BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1618 f.); bereits der irrige Eindruck eine Person sei nackt, kann eine Verletzung der Privatsphäre darstellen, LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14), n.v.; LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319; *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 27.

[1659] Vgl. BGH, Urt. v. 22.5.1984 (VI ZR 105/82), BGHZ 91, 233 (237); BGH, Urt. v. 19.5.1981 (VI ZR 273/79), BGHZ 80, 311 (319); BGH, Urt. v. 23.10.1979 (VI ZR 230/77), NJW 1980, 881 (882); BGH, Urt. v. 21.6.1966 (VI ZR 261/64), NJW 1966, 1617 (1619); vgl. *Dix*, in: *Simitis*, BDSG, § 1, Rn. 186; *Schwerdtner*, JuS 1978, S. 289 (291); *Staudinger*, in: *Schulze*, BGB, § 823 BGB, Rn. 116; Wagner in: *Säcker/Rixecker*, MüKo BGB, § 823, Rn. 242.

[1660] Vgl. F II. 1. d) aa) (2), S. 205.

[1661] Vgl. F II. 1. c) cc) (2), S. 195.

[1662] Vgl. E II. 2. b) gg) (1), S. 124; vgl. BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1 (42 f.); vgl. LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531).

[1663] Vgl. F II. 1. d) aa) (2), S. 205.

[1664] Vgl. B II. 1, S. 27.

sungseffekte die Intensität von Eingriffen im Rahmen anderer Fallgruppen des Allgemeinen Persönlichkeitsrechts.[1665]

Nur wenn entgegen der im Rahmen dieser Untersuchung vertretenen Ansicht, die Anwendbarkeit des § 6b Abs. 1 BDSG abgelehnt werden sollte, wird der Schutz vor Erzeugung von Überwachungsdruck gem. § 823 Abs. 1 BDSG eine eigene Bedeutung erlangen. In diesem Fall können jedoch die im Rahmen des § 6b Abs. 1 BDSG gewonnenen Erkenntnisse, sowie das Ergebnis, d.h. insbesondere die Beschränkung der Zulässigkeit der Nutzung von Smartglasses auf Gefahrsituationen sowie bei medizinischer Indikation, übertragen werden.

4. Verletzung des Hausrechts

Das Hausrecht findet seine Grundlage im Eigentumsrecht, weshalb es systematisch nicht zur Prüfung des Allgemeinen Persönlichkeitsrechts gehört. Jedoch soll es an dieser Stelle im Rahmen eines Exkurses erwähnt werden, da das Hausrecht eine duale Schutzfunktion hat und neben dem Privateigentum auch die Privatsphäre schützt.[1666] Es gibt dem unmittelbaren Besitzer das Recht, die erforderlichen Maßnahmen zu treffen, um bestimmte Räume oder befriedetes Besitztum sowie die sich innerhalb dieser aufhaltenden Personen zu schützen und zu diesen Zwecken unbefugtes Betreten abwehren.[1667] Das Hausrecht schützt damit auch die Privatsphäre der sich innerhalb des Hausrechtsbereichs aufhaltenden Personen.[1668] So tauchten im Hinblick auf die Datenbrille „Google Glass" Berichte von Lokalitäten auf, in denen die Nutzung der Datenbrille untersagt wurde.[1669] Auch wenn die Möglichkeiten, Zutrittsverbote gegen einzelnen Personen bei sonst öffentlich zugänglichem Privateigentum auszusprechen, gem. § 242 BGB beschränkt sind (z.B. in Kaufhäusern oder im öffentlichen Personennahverkehr),[1670] wäre ein gegenüber Nutzern von Smartglasses ausgesprochenes Zutrittsverbot aus Rücksicht auf die Privatsphäre der sich darin aufhaltenden Personen gerechtfertigt.

[1665] LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530 (531); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 361.

[1666] Zur Unterscheidung und Zusammenwirken zwischen Privateigentum und Privatsphäre, vgl. *Hotter*, Privatsphäre, 2011, S. 23 ff.; *Sofsky*, Verteidigung des Privaten, 2007, S. 100.

[1667] *Gola/Schomerus*, BDSG, § 6b, Rn. 16; *Hotter*, Privatsphäre, 2011, S. 27; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 73.

[1668] Vgl. E II. 2. a) aa) (1) (b), 101.

[1669] *Beuth*, Google Glass, Die Zeit, http://www.zeit.de/digital/mobil/2013-05/google-glass-verboten (12.7.2013); *Schwenke*, K&R 2013, S. 685 (690, Fn. 87).

[1670] M.w.N., BGH, Urt. v. 3.11.1993 (VIII ZR 106/93), BGHZ 124, 39 (43); vgl. *Roth/Schubert*, in: *Säcker/Rixecker*, MüKo BGB, § 242 BGB, Rn. 56 ff.

Es bedarf jedoch keines expliziten Zutrittsverbotes oder besonderer Schilder, um Trägern von Smartglasses den Zugang zu privaten Räumlichkeiten und Örtlichkeiten zu untersagen. Wenn Smartglasses wegen ihres hohen Gefährdungspotenzials im öffentlichen Raum generell nicht eingesetzt werden dürfen, so wird nichts anderes innerhalb von öffentlichen Räumlichkeiten und Örtlichkeiten in Privathand (bzw. Fiskalhand) gelten. Denn sie werden der Öffentlichkeit nicht zur beliebigen Nutzung zur Verfügung gestellt, sondern nur entsprechend dem üblichen örtlichen Verhalten.[1671] Zu einem solchen Verhalten gehört es nicht, die Privatsphäre Dritter, z.B. von Kunden eines Kaufhauses, zu gefährden.[1672]

5. Zivilrechtliche Rechtsfolgen der Verletzungen des Allgemeinen Persönlichkeitsrechts

Als Rechtsfolge der rechtswidrigen Verletzung des Allgemeinen Persönlichkeitsrechts aus § 823 Abs. 1 BGB stehen den Betroffenen Abwehr-, Beseitigungs-, Unterlassungs-, Auskunfts- und Schadensersatzansprüche zu.[1673] Ferner können sie sich auf dieselben Ansprüche gem. § 823 Abs. 2 BGB berufen, da in der Regel Schutzgesetze i.S.d. Vorschrift verletzt sein werden. Zu solchen individualschützenden Vorschriften gehören die Regelungen der §§ 4 Abs. 1 und 6b BDSG[1674] als auch der §§ 22 ff. KUG[1675] sowie die Vorschriften der §§ 201 und 201a StGB.[1676]

Auf weitere Ansprüche, die einer Persönlichkeitsrechtsverletzung folgen können, wie z.B. Bereicherungsansprüche aus §§ 812 ff. BGB, solche aus Geschäftsführung ohne Auftrag §§ 687 Abs. 2, 681 Satz 2, 667 BGB, die Kreditgefährdung aus § 824 BGB sowie die sittenwidrige vorsätzliche

---

1671 BGH, Urt. v. 3.11.1993 (VIII ZR 106/93), BGHZ 124, 39 (43).

1672 Vgl. BGH, Urt. v. 25.1.2007 (I ZR 133/04), NJW-RR 2007, 1335 (1336); BGH, Urt. v. 25.4.1991 (I ZR 283/89), NJW-RR 1991, 1512.

1673 Zu speziellen medialen Ansprüchen, wie z.B. Richtigstellung oder Gegendarstellung, vgl. *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 16 ff.; auf weitere Ansprüche, die einer Persönlichkeitsrechtsverletzung folgen können, wie Bereicherungsansprüche aus §§ 812 ff. BGB, solche aus Geschäftsführung ohne Auftrag §§ 687 Abs. 2, 681 Satz 2, 667 BGB, die Kreditgefährdung aus § 824 BGB sowie die Sittenwidrige vorsätzliche Schädigung aus § 826 BGB wird mangels Relevanz für diese Untersuchung nicht näher eingegangen, vgl. ebenda, S. 78 ff.

1674 Vgl. F II, S. 187; AG Berlin-Mitte, Urt. v. 18.12.2003 (16 C 427/02), NZM 2004, 318 (319); *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 157.

1675 Vgl. F IV. 2, 264; BGH, Urt. v. 23.6.2009 (VI ZR 232/08), NJW 2009, 2823.

1676 *Staudinger*, in: *Schulze*, BGB, § 823 BGB, Rn. 90; *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823 BGB, Rn. 423.

Schädigung aus § 826 BGB wird mangels Relevanz für diese Untersuchung nicht näher eingegangen.[1677]

a) Beseitigungsanspruch

Wird das Allgemeine Persönlichkeitsrecht verletzt, steht den Betroffenen zunächst ein vom Verschulden des Täters unabhängiger Anspruch auf Beseitigung des Rechtsverstoßes gem. §§ 823 Abs. 1, 2 BGB in Verbindung mit § 1004 Abs. 1 Satz 1 BGB analog zu.[1678]

Der Beseitigungsanspruch setzt eine fortdauernde Beeinträchtigung des Allgemeinen Persönlichkeitsrechts voraus, die insbesondere dann vorliegt, wenn ein Nutzer von Smartglasses das Gerät auf eine Person im öffentlichen Raum richtet. In dieser Konstellation hat die Person einen Anspruch darauf, dass je nach Sachlage der Nutzer von Smartglasses diese absetzt oder sich so entfernt, dass die beeinträchtigte Person nicht mehr der Überwachungsgefahr ausgesetzt wird.[1679] Eine fortdauernde Beeinträchtigung kann sich ferner auch aus einer in der Vergangenheit abgeschlossenen Handlung ergeben.[1680] Das ist z.B. der Fall, wenn widerrechtlich hergestellte Aufnahmen oder biometrische Templates einer Person vom Nutzer der Smartglasses auf dem Gerät oder auf Cloud-Speichern gesichert wurden und daher die Gefahr einer ebenfalls rechtswidrigen Verbreitung, Verarbeitung oder Veröffentlichung besteht.[1681] Hierbei kann sich der Nutzer zudem nicht auf hypothetische Möglichkeiten einer in der Zukunft möglicherweise zulässigen Nutzung berufen.[1682] Ferner haben Betroffene wegen der Unsicherheit einer hinreichenden Löschung oder bereits erfolgter Verbreitung der Aufnahmen einen Anspruch auf eine schriftliche Bestätigung der Löschung.[1683]

Der zivilrechtliche Beseitigungsanspruch besteht generell neben den Löschungsansprüchen der § 6b Abs. 5 BDSG und § 35 Abs. 2 BDSG.[1684] Im Fall verbreiteter und veröffentlichter Aufnahmen ist die Spezialvorschrift

---

[1677] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 389; vgl. zum Bereicherungsanspruch *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 78 ff.

[1678] LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (788); *Golla/Herbort*, GRUR 2015, S. 648 (651).

[1679] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 386.

[1680] *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823 BGB, Rn. 17.

[1681] Vgl. OLG Koblenz, Urt. v. 20.5.2014 (3 U 1288/13), ZUM 2015, 58 (58); vgl. LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319; LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (788); *Golla/Herbort*, GRUR 2015, S. 648 (651).

[1682] OLG Hamburg, Urt. v. 22.7.2008 (7 U 21/0), NJW 2009, 784 (786).

[1683] Vgl. F II. 1. d) ee), S. 222.

[1684] Vgl. F II. 1. d) ee), S. 222; vgl. F II. 4, S. 241.

des § 37 KUG vorrangig.[1685] Sollen Aufnahmen als Alternative zur Löschung herausgegeben werden, kann der Anspruch auf § 38 KUG analog gestützt werden.[1686]

b) Unterlassungsanspruch bei Wiederholungs- und Erstbegehungsgefahr

Während der Beseitigungsanspruch auf gegenwärtige Rechtsverstöße zielt, sollen mit dem ebenfalls verschuldensunabhängigen Unterlassungsanspruch gem. §§ 823 Abs. 1, 2 BGB in Verbindung mit analoger Anwendung des § 1004 Abs. 1 Satz 2 BGB künftige Verletzungen des Allgemeinen Persönlichkeitsrechts verhindert werden.[1687] Hierzu muss entweder die Gefahr einer im Kern gleichen Wiederholung eines bereits begangenen Rechtsverstoßes oder die Erstbegehungsgefahr eines Rechtsverstoßes in der Zukunft vorliegen.[1688]

aa) Gefahr der Wiederholung

Die Wiederholungsgefahr wird im Fall einer bereits erfolgten Rechtsverletzung im Regelfall indiziert.[1689] Um die Wiederholungsgefahr entfallen zu lassen, ist von dem Nutzer der Smartglasses daher zu erwarten, dass er eine strafbewehrte Unterlassungserklärung abgibt.[1690] In der Unterlassungserklärung muss sich der Nutzer zur Zahlung einer Vertragsstrafe verpflichten, die so hoch sein muss, dass damit zu rechnen ist, dass sie

---

[1685] Vgl. F IV. 2. d), S. 272.

[1686] Vgl. F IV. 2. d), S. 272; vgl. OLG Hamburg, Urt. v. 25.6.1996 (7 U 177/95), ZUM-RD 1997, 1 (4 f.); LG Oldenburg, Beschl. v. 21.4.1988 (5 S 1656/87), GRUR 1988, 694 (696).

[1687] BGH, Urt. v. 21.4.2015 (VI ZR 245/14), BeckRS 2015, 10534 (Rn. 10 ff.); OLG Hamburg, Urt. v. 22.7.2008 (7 U 21/0), NJW 2009, 784 (784); KG, Urt. v. 2.3.2007 (9 U 212/06), ZUM 2007, 475 (476); OLG Frankfurt a.M., Urt. v. 20.2.2002 (23 U 212/01), NJW-RR 2003, 37 (37); LG München I, Urt. v. 10.7.1996 (21 O 23932/95), ZUM-RD 1998, 18 (19); AG Aachen, Urt. v. 11.11.2003 (10 C 386/03), NZM 2004, 339; AG Berlin-Mitte, Urt. v. 18.12.2003 (16 C 427/02), NZM 2004, 318 (319); BAG, Urt. v. 11.12.2014 (8 AZR 1010/13), ZUM 2015, 604 (605); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 4; *Lachenmann/Schwiering*, NZV 2014, S. 291 (295 f.).

[1688] Vgl. OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827 (182); LG München I, Urt. v. 10.7.1996 (21 O 23932/95), ZUM-RD 1998, 18 (19); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 4.

[1689] BGH, Urt. v. 12.7.1994 (VI ZR 1/94), GRUR 1994, 913 (915); BGH, Urt. v. 8.2.1994 (VI ZR 286/93), NJW 1994, 1281 (1283); OLG Hamburg, Urt. v. 22.7.2008 (7 U 21/0), NJW 2009, 784 (784); LG Essen, Urt. v. 10.7.2014 (4 O 157/14), BeckRS 2014, 17008; LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (788); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 24.

[1690] BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1198); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 97a UrhG, Rn. 35.

den Täter von der Wiederholung der Rechtsverletzung abhalten wird.[1691] Gibt der Täter eine entsprechende Erklärung nicht ab, wird der Anspruch gerichtlich im Rahmen einer Klage oder in dringenden Fällen im Rahmen eines einstweiligen Verfügungsverfahrens durchgesetzt werden können.[1692]

Bei der Tenorierung der Unterlassungsverpflichtung kann auf die Erkenntnisse zur datenschutzrechtlichen Untersagung der Nutzung von Smartglasses verwiesen werden.[1693] D.h., die Verpflichtung erstreckt sich generell auf die Unterlassung der von dem Nutzer der Smartglasses ausgehenden Beeinträchtigungshandlung, jedoch ohne Beschränkung auf das konkret eingesetzt Gerät.[1694] Im Unterschied zu einer Datenschutzbehörde können Betroffene jedoch nur die Verletzung ihrer individuellen Rechte geltend machen, d.h. kein generelles Verbot der Nutzung der Smartglasses durch den Unterlassungsgläubiger verlangen.

Ferner wird überwiegend gefordert, dass die objektive Gefahr einer Wiederholung des deliktischen Rechtsverstoßes im Rahmen einer sachgerechten Würdigung der Umstände des Einzelfalls sowie der Interessen Betroffener nicht widerlegt werden kann.[1695] Denn anders als im Wettbewerbsrecht, wo die Wiederholung aufgrund der wirtschaftlichen Motivation angenommen wird, könne eine solche Indikation bei deliktischer Haftung nicht automatisch angenommen werden.[1696] Daher muss jeder Fall einzeln gewürdigt werden, wobei als Faktoren insbesondere die Umstände der Verletzungshandlung, der Grad der Wahrscheinlichkeit ihrer Wiederholung sowie die Motivation des Verletzers zu berücksichtigen sind.[1697] Aufgrund der erheblichen Belastung der Rechte Betroffener durch den Einsatz von Smartglasses werden jedoch im Regelfall keine Umstände

---

1691 Vgl. BGH, Urt. v. 8.2.1994 (VI ZR 286/93), NJW 1994, 1281 (1283); *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 41.

1692 LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14), n.v.

1693 Vgl. F II. 5. b), S. 243.

1694 *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 24.

1695 Vgl. BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1198); BGH, Urt. v. 8.2.1994 (VI ZR 286/93), NJW 1994, 1281 (1283); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 24.

1696 BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1198); BGH, Urt. v. 8.2.1994 (VI ZR 286/93), NJW 1994, 1281 (1283); OLG Düsseldorf, Urt. v. 8.3.2010 (I-20 U 188/09), BeckRS 2010, 07686; OLG Köln, Urt. v. 16.6.1992 (15 U 47/92), BeckRS 1992, 05031 (05031); OLG München, Urt. v. 13.4.1956 (8 U 2024/55), NJW 1956, 1075; *Regenfus*, NZM 2011, S. 799 (802).

1697 BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1198); BGH, Urt. v. 8.2.1994 (VI ZR 286/93), NJW 1994, 1281 (1283); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 24.

vorliegen, die gegen eine Wiederholungsgefahr sprechen.[1698] Allenfalls in Ausnahmefällen kann eine Wiederholungsgefahr verneint werden. Ein solcher Ausnahmefall ist anzunehmen, wenn der Nutzer die Smartglasses ohne Willen und Kenntnis der Verletzung von Rechten Dritter sowie Herstellung rechtswidriger Aufnahmen trug und dabei eine Person, ohne in deren Privatsphäre einzudringen, z.B. im Vorbeigehen auf öffentlicher Straße, erfasst hat.[1699] Zeigt der Nutzer auf die Beschwerde der betroffenen Person freiwillig sowie glaubwürdig Einsicht und war sein Handeln alleine auf Grundlage des Irrglaubens zulässiger Nutzung der Smartglasses erfolgt, wird im Regelfall ebenfalls nicht mit einer Wiederholung zu rechnen sein.[1700]

bb) Gefahr der Erstbegehung

Dieselben Verfahrensmöglichkeiten wie im Fall der Gefahr einer Wiederholung können Betroffenen auch im Fall einer Erstbegehungsgefahr zustehen. Jedoch müssen im Fall einer vorbeugenden Unterlassung konkret greifbare Anhaltspunkte vorliegen, die darauf schließend lassen, dass der Rechtsverstoß in nicht allzu ferner Zukunft eintreten und zu einer ernsthaft drohenden Verletzung führen wird.[1701] Das ist z.B. anzunehmen, wenn der Täter nachweislich einen Entschluss zur Begehung einer Rechtsverletzung gefasst hat und es nur noch an ihm liegt, ob er diesen in die Tat umsetzen wird.[1702] Ausgehend von der bisherigen Rechtsprechung wird für eine solche Gefahr nicht ausreichen, dass aufgrund eines nachbarschaftlichen Konflikts die Gefahr besteht, dass einer der Nachbarn seine Smartglasses zur Beweissicherung einsetzt.[1703] Denn ebenso könnte er auch eine Fotokamera verwenden. Erforderlich wäre vielmehr eine

---

1698 Vgl. E V, S. 181.

1699 Vgl. E II. 2. a) dd), S. 110.

1700 Vgl. BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195 (1198).

1701 BGH, Urt. v. 25.2.1992 (X ZR 41/90), BGHZ 117, 264 (271); OLG Brandenburg, Urt. v. 21.5.2012 (1 U 26/11), NJW-RR 2012, 1250; OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827 (182); LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327 (328); OLG Nürnberg, Urt. v. 11.6.2002 (1 U 3939/01), NJW-RR 2002, 1471 (1472 f.); LG Itzehoe, Urt. v. 11.9.1997 (7 (9) 0 51–96), NJW-RR 1999, 1394 (1395); *Engels*, in: *Ahlberg/Götting*, BeckOK UrhR, § 22 KUG, Rn. 53; *Golla/Herbort*, GRUR 2015, S. 648 (650).

1702 Vgl. OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827 (182).

1703 Vgl. Ebenda; LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327 (328); LG Itzehoe, Urt. v. 11.9.1997 (7 (9) 0 51–96), NJW-RR 1999, 1394 (1395).

konkrete sprachliche Androhung des Einsatzes von Smartglasses zu diesen Zwecken.[1704]

Zu beachten ist ferner, dass der separate Anspruch auf eine verbeugende Unterlassung entfällt, wenn die zu unterlassende Handlung bereits kerngleich von einer Unterlassungserklärung für den Wiederholungsfall erfasst ist.[1705]

c) Materielle und immaterielle Schadensersatzansprüche

§ 823 BGB gewährt im Fall schuldhaften Handelns einen materiellen Schadensersatzanspruch, dessen Umfang sich nach §§ 249 ff. BGB bestimmt.[1706] Ein materieller Anspruch kann sich in erster Linie beim Ersatz der Kosten der Verfolgung der Persönlichkeitsrechtsverletzung, insbesondere der außergerichtlichen Rechtsanwaltsgebühren, ergeben.[1707] Daneben wird ein materieller Anspruch durch die Verletzung von Persönlichkeitsrechten nur selten in Frage kommen. Vorstellbar sind z.B. Fälle, in denen eine Bildaufnahme für kommerzielle Zwecke verwendet wird.[1708] Außer bei prominenten Personen wird ein solcher Schaden jedoch nur schwer nachzuweisen sein.[1709] Im Fall datenschutzrechtlicher Verstöße gewährt zudem § 7 BDSG einen neben dem zivilrechtlichen Anspruch bestehenden Schadensersatzanspruch, der zwar verschuldensunabhängig und mit Umkehr der Beweislast zulasten der verarbeitenden Stellen verbunden, aber nur auf materielle Ansprüche beschränkt ist.[1710]

Im Fall von zivilrechtlichen Persönlichkeitsrechtsverletzungen kommt jedoch dem Ersatz des immateriellen Schadens gem. § 823 BGB i.V.m.

[1704] Vgl. zur Androhung der Ausstrahlung einer Videoaufnahme, LG München I, Urt. v. 10.7.1996 (21 O 23932/95), ZUM-RD 1998, 18 (18 ff.); ebenso spricht (zumindest im Hinblick auf Aufnahmen von Polizeibeamten im Rahmen von Demonstrationen) gegen die Erstbegehungsgefahr, wenn eine "Gegenbeobachtung" ohne hinreichende Anhaltspunkte für eine Veröffentlichung von Aufnahmen, lediglich als Gegereaktion auf eine Videoüberwachung erfolgt, BVerfG, Beschl. v. 24.7.2015 (1 BvR 2501/13), ZUM 2015, 986 (987 f.).

[1705] BGH, Urt. v. 23.6.2009 (VI ZR 232/08), NJW 2009, 2823 (2824).

[1706] BGH, Urt. v. 26.6.1979 (VI ZR 108/78), GRUR 1979, 732 (734); BGH, Urt. v. 8.5.1956 (I ZR 62/54), BGHZ 20, 345 (352 f.); m.w.N., *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 28 ff.

[1707] LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14), n.v.; LG Düsseldorf, Urt. v. 16.11.2011 (12 O 438/10), ZUM-RD 2012, 407 (409); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 28.

[1708] Vgl. BGH, Urt. v. 26.6.1979 (VI ZR 108/78), GRUR 1979, 732 (733 ff.); BGH, Urt. v. 8.5.1956 (I ZR 62/54), BGHZ 20, 345 (352 f.); OLG Karlsruhe, Urt. v. 18.11.1988 (14 U 285/87), NJW 1989, 401 (402).

[1709] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 388.

[1710] Vgl. F II. 5. c), S. 244.

Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG eine weitaus höhere Relevanz zu, als materiellen Schadensersatzansprüchen.[1711] Die Zahlung eines Geldausgleichs wird von der Rechtsprechung jedoch davon abhängig gemacht, dass die Verletzung des Allgemeinen Persönlichkeitsrechts nicht bereits durch andere Rechtsfolgen, wie z.B. die Beseitigung und die Unterlassung, hinreichend ausgeglichen werden kann.[1712] Kein hinreichender Ausgleich liegt insbesondere dann vor, wenn der Rechtsverstoß in der Verbreitung oder Veröffentlichung einer Bildaufnahme liegt, da deren Auswirkungen nicht durch Beseitigung und Unterlassung rückgängig gemacht werden kann.[1713] Ebenso bleibt der betroffenen Person die Zahl der Personen, die Zugang zu der Aufnahme gehabt haben könnten, unbekannt.[1714] Das wird erst recht der Fall sein, wenn die Aufnahme im Internet verbreitet oder veröffentlicht wird, auch wenn dies nur für wenige Stunden erfolgt.[1715]

Des Weiteren muss es sich um eine schwere Persönlichkeitsrechtsbeeinträchtigung handeln, was anhand der konkreten Umstände des Einzelfalls zu beurteilen ist.[1716] Maßgeblich sind die Art, die Schwere sowie der

---

[1711] Zur Anspruchsgrundlage, BGH, Urt. v. 5.10.2004 (VI ZR 255/03), NJW 2005, 215 (216); *Polenz*, in: *Kilian/Heussen*, Computerrecht, 1. Abschn., Teil 13, Betr.Rechte, VII. Rn. 38; *Scholz*, in: *Simitis*, BDSG, § 6b, Rn. 157.

[1712] BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1619); BGH, Urt. v. 5.3.1963 (VI ZR 55/62), BGHZ 39, 124 (132 f.); BGH, Urt. v. 15.1.1965 (I b ZR 44/63), NJW 1965, 1374 (1375); OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087 (1088); OLG Karlsruhe, Urt. v. 18.11.1988 (14 U 285/87), NJW 1989, 401 (402); OLG Stuttgart, Urt. v. 16.12.1981 (4 U 88/81), NJW 1982, 652 (653); LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319 (19319); LG Düsseldorf, Urt. v. 16.11.2011 (12 O 438/10), ZUM-RD 2012, 407 (408); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 388.

[1713] BGH, Urt. v. 15.1.1965 (I b ZR 44/63), NJW 1965, 1374 (1375); OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); OLG Stuttgart, Urt. v. 16.12.1981 (4 U 88/81), NJW 1982, 652 (653); LG Düsseldorf, Urt. v. 16.11.2011 (12 O 438/10), ZUM-RD 2012, 407 (408); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 30.

[1714] OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002 (1004).

[1715] LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002 (1003).

[1716] BGH, Urt. v. 21.4.2015 (VI ZR 245/14), BeckRS 2015, 10534 (Rn. 33); BGH, Urt. v. 5.10.2004 (VI ZR 255/03), NJW 2005, 215 (216); BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1619); KG, Urt. v. 28.8.1998 (25 U 7198/97), ZUM-RD 1998, 554 (555); OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545; OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087 (1088); OLG Stuttgart, Urt. v. 16.12.1981 (4 U 88/81), NJW 1982, 652 (653); LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319; BAG, Urt. v. 11.12.2014 (8 AZR 1010/13), ZUM 2015, 604 (608); *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 30; *Polenz*, in: *Kilian/Heussen*, Computerrecht, 1. Abschn., Teil 13, Betr.Rechte, VII. Rn. 38; *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 69 ff.

Anlass der Beeinträchtigung als auch die Motivation und der Verschuldensgrad des Täters.[1717] Die Schwere der Rechtsverletzung bestimmt sich u.a. nach dem Ausmaß der Verbreitung und Veröffentlichung einer Aufnahme, der Schutzbedürftigkeit Betroffener (insbesondere bei Minderjährigen) als auch der Nachhaltigkeit und Fortdauer einer Interessen- oder Rufschädigung der verletzten Person.[1718]

Im Hinblick auf die Höhe der Schadensersatzforderung muss in erster Linie dem Umstand Rechnung getragen werden, dass ohne eine spürbare Entschädigung kein ausreichender Schutz gegen erhebliche Beeinträchtigungen des Persönlichkeitsrechts bestehen würde.[1719] Ferner muss auch dem Genugtuungsbedürfnis der Verletzten Rechnung getragen werden.[1720] Der Genugtuungsgedanke verbietet jedoch zugleich, dass die Geldforderung den Rahmen eines angemessenen Ausgleichs der Rechtsverletzung übersteigt.[1721] Dennoch muss die Geldentschädigung fühlbar sein und etwaige wirtschaftliche Vorteile ausgleichen.[1722] Wirtschaftliche Vorteile sind jedoch bei einer privaten Nutzung von Smartglasses eher nicht anzunehmen. Insbesondere können den Nutzern etwaige Vorteile von Onlineplattformen, auf denen z.B. persönlichkeitsbeeinträchtigende

---

[1717] BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1619); KG, Urt. v. 28.8.1998 (25 U 7198/97), ZUM-RD 1998, 554 (555); OLG Karlsruhe, Urt. v. 18.11.1988 (14 U 285/87), NJW 1989, 401 (402); OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087 (1088); OLG Stuttgart, Urt. v. 16.12.1981 (4 U 88/81), NJW 1982, 652 (653); BAG, Urt. v. 11.12.2014 (8 AZR 1010/13), ZUM 2015, 604 (608); AG Kerpen, Urt. v. 25.11.2010 (102 C 108/10), BeckRS 2011, 10636; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 31.

[1718] BGH, Urt. v. 5.10.2004 (VI ZR 255/03), NJW 2005, 215 (216); BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1619); OLG Karlsruhe, Urt. v. 18.11.1988 (14 U 285/87), NJW 1989, 401 (402); LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002 (1004).

[1719] BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1619); BGH, Urt. v. 26.1.1971 (VI ZR 95/70), NJW 1971, 698 (699); BGH, Urt. v. 15.1.1965 (I b ZR 44/63), NJW 1965, 1374 (1375); OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087 (1088); LG Düsseldorf, Urt. v. 16.11.2011 (12 O 438/10), ZUM-RD 2012, 407 (408); LAG Hessen, Urt. v. 25.10.2010 (7 Sa 1586/09), MMR 2011, 346 (347).

[1720] BVerfG, Urt. v. 14.2.1973 (1 BvR 112/65), BVerfGE 34, 269 (274); BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617 (1619); BGH, Urt. v. 19.9.1961 (VI ZR 259/60), BGHZ 35, 363 (366); LG Düsseldorf, Urt. v. 16.11.2011 (12 O 438/10), ZUM-RD 2012, 407 (408).

[1721] BGH, Urt. v. 15.1.1965 (I b ZR 44/63), NJW 1965, 1374 (1375); OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345).

[1722] BGH, Urt. v. 5.10.2004 (VI ZR 255/03), NJW 2005, 215 (218); BGH, Urt. v. 15.11.1994 (VI ZR 56/94), BGHZ 128, 1 (9 f.); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 389; *Tacke*, Medienpersönlichkeitsrecht, 2009, S. 63 f.

Aufnahmen veröffentlicht worden sind, nicht zugerechnet werden.[1723] Denn die wirtschaftliche Betrachtung dient der Zumessung des immateriellen Schadensersatzanspruchs, aber nicht einer umfassenden „Gewinnabschöpfung" durch Betroffene.[1724]

Die bisherige Rechtsprechung spricht den Betroffenen ein Schmerzensgeld vor allem in Fällen der Verbreitung und Veröffentlichung von Aufnahmen zu, die intensiv in den Privatbereich der Personen eingreifen.[1725] Es handelt sich eher um niedrige vierstellige Beträge, die erst im Fall erheblicher Beeinträchtigung der Intimsphäre höhere Summen begründen.[1726] Im Fall der Videoüberwachung stellten die Gerichte auf deren Dauer und Hartnäckigkeit trotz Widerspruchs Betroffener ab. Hierfür wurde im Fall einer einjährigen Beobachtung des Nachbargrundstücks ein Schadensersatz von 5.000 DM zugebilligt.[1727] Dagegen wurde eine schwerwiegende Persönlichkeitsbeeinträchtigung im Fall einer Videobeobachtung, die grundsätzlich den Schutz des eigenen Grundstücks verfolgte und sich nicht gezielt gegen das Persönlichkeitsrecht der Klägerin richtete, zumindest im Jahr 1998 verneint.[1728]

Im Hinblick auf die Nutzung von Smartglasses ist aus der Entscheidungspraxis zu folgern, dass deren typische Nutzung keinen immateriel-

---

[1723] Vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 389.

[1724] BGH, Urt. v. 15.11.1994 (VI ZR 56/94), BGHZ 128, 1 (16); häufig wird es sich zudem nur um geringe Beträge handeln, da der wirtschaftliche Vorteil solcher Plattformen sich aus der Menge der Nutzer und weniger dem einzelnen Nutzer und dessen Beträgen ergibt, vgl. *Berberich*, MMR 2010, S. 736 (739); *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 15; *Schwenke*, WRP 2012, S. 37.

[1725] Übersicht in *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 34 f.; S. auch Schmerzensgeldtabelle in Slizyk/IMMDAT Plus, „Persönlichkeitsrechtsverletzung Recht am eigenen Bild".

[1726] 4.000 Euro im Fall einer "oben ohne"-Aufnahme, in einer Zeitschrift, OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344 (345); 3.000 DM bei öffentlicher, aber örtlicher, Wiedergabe von Aufnahmen eines betrunkenen Bauarbeiters, OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087 (1087 f.); 25.000 Euro bei veröffentlichung intimer Aufnahmen aus dem Sexualbereich mit textlichen Zusätzen im Internet und folgenden sexuell motivierten Belästigungen durch Dritte, LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002 (1004).

[1727] OLG Köln, Urt. v. 13.10.1988 (18 U 37/88), NJW 1989, 720 (721); höhere Ansprüche können mitunter innerhalb besonderer Vertrauensverhältnisse entstehen (z.B. bei Videoüberwachung von Arbeitnehmern), die jedoch im Fall privater Nutzung von Smartglasses im Regelfall nicht vorliegen werden, LAG Hessen, Urt. v. 25.10.2010 (7 Sa 1586/09), MMR 2011, 346 (347 f.).

[1728] OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545.

len Schadensersatz auslösen wird.[1729] Erst eine Hartnäckigkeit, die einem Nachstellen gleichkommt oder eine Verbreitung und Veröffentlichung von erheblich in die Privatsphäre Dritter eingreifenden Aufnahmen, kann einen derartigen Anspruch begründen. Dieser Anspruch ist jedoch insoweit keine spezielle Gefahr der Nutzung von Smartglasses, sondern kann z.B. auch bei Aufnahmen entstehen, die mithilfe von Smartphones entstanden sind. Darüber hinaus werden die Interessen der Betroffenen durch die Beseitigungs- und Unterlassungsansprüche hinreichend befriedigt.

d) Auskunftsanspruch

Eine rechtswidrige Verletzung von Persönlichkeitsrechten begründet einen aus dem Grundsatz von Treu und Glauben gem. § 242 BGB auf Grundlage eines gesetzlichen Schuldverhältnisses aus der unerlaubten Handlung hergeleiteten Auskunftsanspruch.[1730] Ein solcher Anspruch ist anerkannt, wenn der Betroffene sich die zur Durchsetzung und Bezifferung seiner übrigen Ansprüche auf Beseitigung, Unterlassung oder Schadensersatz notwendigen Informationen nicht selbst beschaffen kann und dem Auskunftspflichtigen die Auskunft möglich und zumutbar ist.[1731] Ein Anspruch kann insbesondere im Hinblick auf die Frage bestehen, ob und welche Bildaufnahmen von der betroffenen Person erstellt worden sind und ob sie sich im Besitz des Auskunftsverpflichteten befinden.[1732] Der Anspruch besteht neben einem Anspruch aus § 34 BDSG und ist ebenfalls bereits infolge der konkreten Möglichkeit einer Erfassung durch Smartglasses vorhanden.[1733] Ebenso kann im Fall eines berechtigten Zweifels an der Auskunft, bis zur Klärung der verbleibenden Zweifel, die Herausgabe der Smartglasses an einen Gerichtsvollzieher als Sequester verlangt werden.[1734]

[1729] Wohl a.A., für die im Fall der einmaligen und zufälligen Videoüberwachung mittels einer "Dashcam", jedoch ohne nähere Konkretisierung, ein niedriger Betrag zumindest in Frage kommt, *Lachenmann/Schwiering*, NZV 2014, S. 291 (296).

[1730] BGH, Urt. v. 24.6.2008 (VI ZR 156/06), GRUR 2008, 1017 f.; BGH, Urt. v. 19.5.1981 (VI ZR 273/79), BGHZ 80, 311 (319); KG, Urt. v. 13.6.2006 (9 U 251/05), ZUM-RD 2006, 552 (554 f.); *Dix*, in: *Simitis*, BDSG, § 34, Rn. 91; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 39; *Meents/Hinzpeter*, in: *Taeger/Gabel*, BDSG, § 34, Rn. 8; *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823 BGB, Rn. 17.

[1731] BGH, Urt. v. 7.6.1971 (I ZR 32/70), BGHZ 56, 256 (262); BGH, Urt. v. 28.10.1953 (II ZR 149/52), BGHZ 10, 385 (387); LG München I, Urt. v. 11.9.2003 (7 O 20974/02), ZUM-RD 2003, 601 (606).

[1732] LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787 (788); *Lachenmann/Schwiering*, NZV 2014, S. 291 (296).

[1733] Vgl. F II. 4, S. 241; *Meents/Hinzpeter*, in: *Taeger/Gabel*, BDSG, § 34, Rn. 8.

[1734] Vgl. F II. 4, S. 241.

6. Zivilrechtliche Inanspruchnahme als Regelfall des Vorgehens gegen die Nutzer von Smartglasses

Es ist zwar nicht unwahrscheinlich, dass Maßnahmen gegen die Nutzer von Smartglasses auch durch Datenschutzbehörden erfolgen werden. Im Regelfall wird jedoch eher damit zu rechnen sein, dass Betroffene sich direkt gegen die Nutzer wenden werden. Dabei werden sie sich zum einen auf die Verletzung des Allgemeinen Persönlichkeitsrechts als Schutzgut des § 823 Abs. 1 BGB berufen können. Parallel dazu werden sie insbesondere auch die Verletzung des Verbotes von Videoüberwachung gem. § 6b BDSG sowie der Verbreitung und Zurschaustellung von Bildnissen gem. § 22 KUG als Schutzrechte i.S.d. § 823 Abs. 2 BGB geltend machen können. In allen Fällen werden ihnen bei analoger Anwendung des § 1004 Abs. 1 BGB Beseitigungs- und Unterlassungsansprüche gegenüber den Nutzern von Smartglasses zustehen. Da die Betroffenen nicht wissen werden, ob und im welchen Umfang Aufnahmen von ihnen erstellt worden sind, werden sie zur Begründung der Beseitigungs- und Löschungsansprüche Auskunftsrechte gegenüber den Nutzern von Smartglasses geltend machen können. Diese werden ihnen z.B. durch Vorzeigen der Geräte überzeugend nachweisen müssen, dass keine Aufnahmen erstellt worden sind. Diese vorgenannten Ansprüche werden im Regelfall die Rechtsschutzbedürfnisse der Betroffenen hinreichend befriedigen, sodass außer in Ausnahmefällen hartnäckiger, lang andauernder oder den Privat- und Intimbereich erheblich verletzender Eingriffe ihnen kein immaterieller Schadensausgleich zustehen wird.

Des Weiteren wird der zivilrechtliche Schutz für Betroffene besonders relevant, um Auskunft im Hinblick auf etwaige Verstöße gegen §§ 201, 201a StGB zu erhalten. Denn anders als im Fall der Ermittlung der Strafverfolgungsbehörden werden die Nutzer von Smartglasses so die Rechtsverfolgung selbst in der Hand behalten und ggf. zügiger durchsetzen können.

V. Sofortige Abwehrmaßnahmen der Betroffenen

Die bisherigen Ergebnisse der Untersuchung zeigen, dass die Nutzung von Smartglasses im öffentlichen Raum im Regelfall mit erheblichen Verletzungen der Persönlichkeitsrechte Dritter einhergehen wird. Auf der anderen Seite steht den Betroffenen mit zivilrechtlichen Ansprüchen und der Möglichkeit, sich an Datenschutz- sowie Strafverfolgungsbehörden zu wenden, ein umfassendes Abwehrinstrumentarium gegen die Rechtsverstöße zur Verfügung.

Jedoch sind diese rechtlichen Werkzeuge vor dem Hintergrund einer traditionellen Videoüberwachung, Fotokameras und Smartphones ge-

schaffen worden. Zu prüfen ist daher, ob sie auch einen effektiven Schutz vor den Gefahren, die von Smartglasses ausgehen, bieten. Denn die bisherigen Erfahrungen mit Smartglasses lassen vermuten, dass mit Fällen zu rechnen ist, in denen die Betroffenen sich nicht auf nachträgliche Rechtsdurchsetzung verlassen werden. Ganz im Gegenteil ist ein Wunsch nach sofortiger Rechtsdurchsetzung zu beobachten, der ein zwischenmenschliches Konfliktpotenzial mit sich bringt, das in tätliche Gewalt umschlagen kann.[1735]

Die nachfolgende Prüfung wird zuerst das Konfliktpotenzial der Smartglasses untersuchen. Anschließend werden einschlägige Rechtsverstöße betrachtet, die durch Betroffene im Rahmen ihrer Abwehrmaßnahmen erfüllt sein könnten. Den Kern der Prüfung bildet die Untersuchung, inwieweit die Abwehrmaßnahmen der Betroffenen durch den Tatbestand der Notwehr gerechtfertigt sein können.

1. Hohes zwischenmenschliches Konfliktpotenzial

Anders als die traditionelle Videoüberwachung sind Smartglasses vor allem mobil und nicht institutionalisiert. D.h., bei fest angebrachten Überwachungskameras können Betroffene i.d.R. die verantwortliche Stelle, sei sie staatlicher oder privater Natur, ausfindig machen. Auch bei mobiler Überwachung durch Polizeibeamte oder Dashcams in Fahrzeugen können die Verantwortlichen durch entsprechende Personen- oder Kraftfahrzeugkennzeichen ermittelt werden.[1736] Insoweit müssen die für die Überwachung verantwortlichen Stellen mit der jederzeitigen Auffindbarkeit und Überprüfung ihrer Überwachungsmaßnahmen rechnen. Es erscheint daher insoweit erklärbar, dass Betroffene dadurch die Sicherheit gewinnen, dass sie sich auch nachträglich gegen derartige Videoüberwachung wehren können.[1737] Ebenso könnten sie ein Vertrauen gewinnen, dass die Möglichkeit jederzeitiger staatlicher und privatrechtlicher Kontrollen die Überwachenden zur Beachtung der rechtlichen Vorgaben bewegt. All diese Vertrauensgrundlagen fehlen bei den Nutzern von Smartglasses, die den Betroffenen i.d.R. unbekannt sein werden. Ganz im Gegenteil können sich die Nutzer jederzeit entfernen und nicht nachträglich belangt werden, z.B. nachdem sie heimlich erstellte persönlichkeitsrechtsverletzende Aufnahmen veröffentlicht haben.[1738]

[1735] Vgl. C II. 3, S. 68.

[1736] Vgl. E II. 2. a) aa) (1) (b), S. 101.

[1737] Vgl. OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); vgl. *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36b; zur Akzeptanz der institutionellen Videoüberwachung, vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 89 ff.; *Mann/Niedzviecki*, Cyborg, 2002, S. 27.

[1738] Vgl. E IV. 1. i), S. 160.

Ein weiterer Unterschied besteht bei Smartglasses in deren räumlicher Nähe zu den Betroffenen. Standortgebundene Videoüberwachungskameras nehmen das Geschehen aus dem Hintergrund, oft montiert unter Decken und versteckt in undurchsichtigen halbrunden „Domes", auf.[1739] Auch Dashcams in Kraftfahrzeugen fallen hinter den Windschutzscheiben nicht direkt ins Auge. Smartglasses sind dagegen im räumlich-zwischenmenschlichen Bereich präsent. Hierdurch wird den Betroffenen die Gefahr heimlicher Aufnahmen, ihrer Verbreitung, Veröffentlichung oder biometrischer Auswertung zum einen wortwörtlich vor die Augen geführt. Zum anderen können sie sich direkt und unmittelbar, also ohne die Verantwortlichen einer Videoüberwachung ermitteln zu müssen, zur Wehr setzen.

Die von Smartglasses ausgehenden Gefahren unterscheiden sich ebenfalls von der typischen Gefahrenlage bei heimlichen Kamera- oder Smartphone-Aufnahmen. Die letzteren werden von einer besonderen Fotografiergeste begleitet, die etwaige Rechtsverstöße für Betroffene deutlicher erkennbar macht.[1740] Betroffene können auf dieser Tatsachengrundlage zum einen selbstbewusster gegen die Fotografierenden auftreten, da zumindest ein Ansetzen zur Aufnahme nicht bestritten werden kann. Zum anderen können sie ihr Vertrauen darauf stützen, dass die Erkennbarkeit einer Aufnahme zu einer Hemmschwelle führt, die als Hürde gegen persönlichkeitsrechtsverletzende Aufnahmen dient.[1741]

Stehen Betroffene dagegen Nutzern von Smartglasses gegenüber, werden sie sich der Gefahr für ihre Persönlichkeitsrechte gewahr, können jedoch kein Vertrauen in die Rechtmäßigkeit der Videoüberwachung, Erkennbarkeit von Aufnahmevorgängen, eine Hemmschwelle der Nutzer sowie Möglichkeiten einer nachträglichen Rechtsdurchsetzung bilden. Damit liegt eine Situation vor, die einen Wunsch von Betroffenen nach sofortiger Rechtsdurchsetzung nahelegt und aus deren Sicht als notwendig erscheinen lässt, bevor sich die unbekannten Nutzer von Smartglasses entfernen. Diese Situation birgt ein hohes Konfliktpotenzial, vor allem wenn die Nutzer von Smartglasses kein Verständnis für dieses Bedürfnis Betroffener zeigen und es dadurch zu zwischenmenschlichen Spannungen kommt.

[1739] Zur größerer Sorglosigkeit im Umgang mit Überwachungskameras, als mit Smatrtglasses, vgl. *Mann/Niedzviecki*, Cyborg, 2002, S. 27.

[1740] Vgl. E IV. 1. g) aa), S. 154.

[1741] Vgl. E IV. 1. g) dd), S. 158.

2. Konfliktmatrix

Die Spannungslage zwischen Betroffenen und Nutzern von Smartglasses kann zu einer Vielfalt unterschiedlicher Konfliktsituationen führen, die nicht alle im Rahmen dieser Untersuchung betrachtet werden können. Die nachfolgende Darstellung hat daher zum Ziel, eine Matrix mit Konstellationen und Reaktionen Beteiligter zu erstellen, die typischerweise bei der Nutzung von Smartglasses im öffentlichen Raum zu erwarten sein werden. Diese „Konfliktmatrix" wird der anschließenden rechtlichen Würdigung als Grundlage dienen.

Da im Rahmen dieser Untersuchung vor allem die alltägliche Nutzung von Smartglasses untersucht wird, ist davon auszugehen, dass deren Nutzer nicht zielgerichtet darauf handeln, die Rechte der Betroffenen, z.B. als Voyeure, zu verletzen. Ferner ist, vorbehaltlich anderweitiger Hinweise, davon auszugehen, dass die Beteiligten sich nicht kennen.

a) Örtlichkeiten und Situationen

In der ersten Konstellation bewegt sich A mit aufgesetzten Smartglasses auf einem öffentlichen Gehweg, wo ihm der Passant B entgegenkommt. In einer Abwandlung dieser Konstellation handelt es sich bei B um einen Nachbarn, dem A jeden Tag auf dem Weg zur Arbeit begegnet.

In der zweiten Konstellation sitzt A in einem Café, wo in seinem Blickfeld der B am Nachbartisch Platz genommen hat und in ein Gespräch mit einer dritten Person vertieft ist.

In der dritten Konstellation betritt A mit aufgesetzten Smartglasses die Umkleidekabine eines Kaufhauses, wo sein Blick durch den Spalt einer Umkleidetür auf den entkleideten B fällt.

b) Handlungen des Nutzers

Während A die Smartglasses aufgesetzt hat, wird das Gerät wie folgt eingesetzt:

A erstellt Foto- oder Videoaufnahmen, auf denen B zu erkennen ist.

A hat die Smartglasses ausgeschaltet, sodass keine Erfassungsvorgänge stattfinden.

c) Subjektive Vorstellung des Betroffenen

B geht subjektiv von folgenden Handlungen des A aus:

- B geht davon aus, dass A tatsächlich Foto- oder Videoaufnahmen erstellt.
- B geht davon aus, dass A die Smartglasses abgeschaltet hat.

d) Aufforderungen des Betroffenen

Nachdem B die Smartglasses bemerkt, stellt er zuerst die folgenden Forderungen, die A sofort erfüllen soll:

- B fordert A auf, die Smartglasses abzusetzen oder die Örtlichkeit zu verlassen.
- B fordert A auf, die Smartglasses nicht noch einmal in seiner Nähe zu tragen.
- B fordert A auf, ihm seine Identität sowie Adresse mitzuteilen und z.B. durch Vorlage eines Personalausweises nachzuweisen.
- B fordert A auf, ihm Auskunft darüber zu geben, ob und welche Aufnahmen erstellt wurden.

Wurden Aufnahmen erstellt, fordert B den A zu deren Löschung auf.

- B fordert A auf, ihm die Smartglasses zu zeigen bzw. zu übergeben, damit B sich davon überzeugen kann, dass keine Aufnahmen erstellt wurden bzw. dass sie gelöscht worden sind.

e) Sofortige Abwehrmaßnahmen des Betroffenen

A kommt den Forderungen des B nicht nach, weswegen B die folgenden Maßnahmen ergreift:

B droht A, dass er die Polizei rufen werde.

B droht A tätliche Gewalt an.

B hält A fest, damit dieser sich nicht entfernen kann, bevor die Polizei eintrifft.

B nimmt dem A die Smartglasses ohne Widerstand und alternativ unter Überwindung seines körperlichen Widerstandes ab.

B schlägt den A mit der Faust, um ihn dazu zu bewegen, seinen Forderungen nachzukommen. In einer Alternative führt B seinen Schlag direkt gegen die von A getragenen Smartglasses.

Nachdem B die Smartglasses des A erlangt hat, betrachtet er die auf diesen befindlichen Aufnahmen und, sofern er welche von sich findet, löscht er diese.

B zerstört die Smartglasses des A, z.B. durch einen Schlag oder indem er sie auf den Boden wirft.

In der Abwandlung ergreift B diese Maßnahmen, jedoch ohne dem A vorher seine Forderungen mitzuteilen und A zu deren Befolgung aufzufordern.

3. Durch den Betroffenen erfüllte Verletzungstatbestände

Die sofortigen Abwehrmaßnahmen des Betroffenen beeinträchtigen die Rechte der Nutzer von Smartglasses und können so rechtlich sanktionierte Tatbestände verwirklichen. Deren nachfolgende Darstellung soll nur schematisch erfolgen, da sie nicht den Schwerpunkt der Untersuchung bildet und im Einzelfall geprüft werden muss.

a) Nötigung und Freiheitsberaubung gem. §§ 239, 240 StGB

Die Nötigung setzt gem. § 240 Abs. 1, 2 StGB eine verwerfliche Anwendung von Gewalt oder die Drohung mit einem empfindlichen Übel voraus, um jemanden zu einer Handlung, Duldung oder Unterlassung zu bewegen. Die Androhung körperlicher Gewalt stellt ein empfindliches und verwerfliches Übel dar, mit dem B den A zur Befolgung seiner Forderungen bewegen und damit tatbestandlich nötigen möchte.[1742] Das gilt erst recht, wenn B die Gewalt tatsächlich anwendet.

Dagegen darf sich B auf ihm rechtmäßig zustehende und angesichts möglicher Rechtsverletzungen adäquate Rechtsmittel berufen.[1743] Daher darf er dem A drohen, die Polizei herbeizurufen, um die rechtswidrige Videoüberwachung zu beenden oder Auskunft über eventuell erstellte Maßnahmen zu erhalten. Insoweit handelt es sich zwar um ein Drohen mit einem empfindlichen Übel, jedoch muss A dieses Übel hinnehmen, sodass in diesem Fall keine Nötigung vorliegt.

Wird A von B festgehalten, kann es sich um eine Freiheitsberaubung gem. § 239 Abs. 1 StGB handeln.[1744] Ist das Festhalten jedoch nur kurzfristig, z.B. im Rahmen einer körperlichen Auseinandersetzung, wie sie vorliegend anzunehmen sein wird, handelt es sich lediglich um eine mittels Gewalt begangene Nötigung gem. § 240 Abs. 1 StGB.[1745]

b) Diebstahl gem. § 242 StGB

Nimmt B dem A die Smartglasses weg, könnte es sich um einen Fall der Wegnahme mit Zueignungsabsicht, mithin um einen Diebstahl i.S.d. § 242 Abs. 1 StGB handeln. Im Regelfall wird die Wegnahme jedoch nur vorübergehender Natur sein und der Einholung von Informationen über

---

[1742] Vgl. *Heger*, in: *Lackner/Kühl*, StGB, § 240, Rn. 12; *Toepel*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 104 ff.; *Valerius*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 240, Rn. 36 f.

[1743] Vgl. BGH, Urt. v. 19.11.1953 (3 StR 17/53), BGHSt 5, 254 (258 ff.); *Heger*, in: *Lackner/Kühl*, StGB, § 240, Rn. 24; *Toepel*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 201, Rn. 113 ff.

[1744] Vgl. OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123.

[1745] Vgl. *Toepel*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 239, Rn. 19; vgl. *Valerius*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 239, Rn. 13.

erstellte Aufnahmen oder deren Löschung, verbunden mit der Absicht anschließender Rückgabe der Smartglasses an A, dienen. Eine solche kurzfristige und in die Substanz der Sache selbst nicht eingreifende Wegnahme mit Rückgabeabsicht stellt jedoch im Regelfall keine Zueignung und damit keinen Diebstahl dar.[1746] Auch wenn die Wegnahme lediglich der Zerstörung der Smartglasses dient, kann mangels eines eigentümergleichen Verbrauchs oder Gebrauchs der Sache kein Diebstahl angenommen werden.[1747]

c) Sachbeschädigung gem. § 303 StGB und Datenveränderung gem. § 303a StGB

Nimmt B zumindest in Kauf, dass die Smartglasses des A beschädigt oder zerstört werden, z.B. wenn er versucht, das Gerät dem A zu entreißen oder es auf den Boden wirft, wird ein Fall der Sachbeschädigung gem. § 303 Abs. 1 StGB vorliegen. Löscht B lediglich die von A erstellten Aufnahmen, begeht er eine Datenveränderung gem. § 303a Abs. 1 StGB.[1748] Sofern die Löschung nicht endgültig ist, weil die Aufnahme von A wiederhergestellt werden kann, liegt zumindest eine versuchte Datenveränderung gem. § 303a Abs. 2 StGB vor.[1749]

d) Körperverletzung und gefährliche Körperverletzung gem. §§ 223, 224 Abs. 1 Nr. 2 Alt. 2 StGB

Wendet B als Mittel der Nötigung eine gegen den Körper des A gerichtete Gewalt an, z.B. indem er B schlägt, begeht er dadurch eine als körperliche Misshandlung zu qualifizierende üble und unangemessene Behandlung, die den Tatbestand einer Körperverletzung gem. § 223 Abs. 1 StGB erfüllt.[1750] Ein bloßes Festhalten, das zu keiner sonstigen Beeinträchtigung

---

[1746] BayObLG, Beschl. v. 12.12.1991 (RReg. 4 St 158/91), NJW 1992, 1777 (1778); *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 242, Rn. 90 ff.; *Kühl*, in: *Lackner/Kühl*, StGB, § 242, Rn. 24.

[1747] BGH, Urt. v. 10.5.1977 (1 StR 167/77), NJW 1977, 1460; BGH, Urt. v. 23.4.1953 (3 StR 219/52), BGSt 4, 236 (239); *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 242, Rn. 87 f.

[1748] Vgl. *Stree/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 303a, Rn. 4 ff.; *Zaczyk*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 303a, Rn. 7 ff.

[1749] Der Begriff des Löschens, entspricht datenschutzrechtlichem Verständnis, BT-DrS. 10/5058, S. 34; vgl. F II. 1. d) ee), S. 222.

[1750] Vgl. *Eser/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 232, Rn. 3; *Kühl*, in: *Lackner/Kühl*, StGB, § 223, Rn. 4.

des körperlichen Wohlbefindens führt, stellt dagegen noch keine Körperverletzung dar.[1751]

Der Schlag des B gegen die von A getragenen Smartglasses könnte ferner den Tatbestand einer gefährlichen Körperverletzung unter Zuhilfenahme eines gefährlichen Werkzeugs gem. § 224 Abs. 1 Nr. 2 Alt. 2 StGB darstellen.[1752] Eine gefährliche Körperverletzung setzt nach h.M. voraus, dass der verwendete Gegenstand nach der Art seiner Benutzung und des Körperteils, gegen den er gewendet wird, geeignet ist, erhebliche Körperverletzungen hervorzurufen.[1753]

Bei einer durch einen Schlag auf eine Fotokamera vermittelten Körperverletzung entschied das OLG Hamburg, dass es sich bei der Fotokamera nicht um ein gefährliches Werkzeug handelte.[1754] Das Gericht argumentierte, dass die Fotokamera nach objektiver Beschaffenheit und der Art ihrer Benutzung im Einzelfall nicht geeignet war, erhebliche Körperverletzungen hinzuzufügen.[1755] Der Wucht gegen die Kamera sei zudem vergleichsweise gering gewesen und habe sich in der Verletzungsfolge nicht von einem Schlag mit bloßer Hand unterschieden.[1756] Eine Kamera verfügt jedoch auf der zum Auge gerichteten Rückseite im Regelfall über eine Augenmuschel des Suchers oder zumindest ein flaches Display. Im Fall der Smartglasses kann sich jedoch vor dem Auge ein vergleichsweise kleines Display oder eine Kameravorrichtung befinden, die ins Auge eindringen und splittern können.[1757] Dies führt dazu, dass auch ein geringer Schlag gegen die Datenbrille zu erheblichen Augenverletzungen führen und die Körperverletzung als gefährlich qualifizieren kann.[1758] Ausnahmen können sich bedingt durch die Konstruktion der Smartglasses und die Art der Gewaltanwendung ergeben, z.B. wenn sich kein Display direkt vor dem Auge befindet oder der Schlag so angesetzt ist, dass die Datenbrille nicht gegen, sondern vom Kopf geschlagen wird.

1751 BGH, Urt. v. 15.9.2010 (2 StR 400/10), NStZ-RR 2010, 374 (374); OLG Köln, Beschl. v. 28.5.2013 (III-1 RVs 81/13), NStZ-RR 2013, 308; *Eser/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 232, Rn. 4a; *Kühl*, in: *Lackner/Kühl*, StGB, § 223, Rn. 4.

1752 Vgl. OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462.

1753 BGH, Urt. v. 6.6.1952 (1 StR 708/51), BGHSt 3, 105 (109); *Eschelbach*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 224, Rn. 28; *Kühl*, in: *Lackner/Kühl*, StGB, § 224, Rn. 5; *Paeffgen*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 224, Rn. 14; *Stree/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 224, Rn. 3a.

1754 OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (463).

1755 Ebenda.

1756 Ebenda.

1757 Vgl. B II. 2, S. 29.

1758 Vgl. *Paeffgen*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 224, Rn. 14a.

Zusätzlich zu dem objektiven Tatbestand der Gefährlichkeit muss diese zumindest vom Eventualvorsatz des Täters umfasst werden.[1759] Dies hängt davon ab, ob die Gefährlichkeit der Handlung für den Täter erkennbar war. Allerdings kann zumindest bei derzeitigen Smartglasses im Regelfall davon ausgegangen werden, dass auch ein Laie die Gefahr erkennen kann, dass die Geräte oder deren Teile durch einen Schlag ins Auge eindringen oder durch Splitter verletzen können.[1760]

e) Zivilrechtliche Deliktstatbestände des § 823 BGB

Die von B beeinträchtigte körperliche Integrität, die Freiheit und das Eigentum des A stellen zugleich zivilrechtlich geschützte Schutzgüter gem. § 823 Abs. 1 BGB dar. Ferner handelt es sich bei den vorgenannten Strafvorschriften um Schutzgesetze i.S.d. § 823 Abs. 2 BGB.[1761] D.h., A wird gegen B nicht nur einen Strafantrag stellen, sondern selbst zivilrechtlich vorgehen können. Ein Vorgehen gegen B wird jedoch nur dann erfolgreich sein, wenn B nicht gerechtfertigt gehandelt hat.[1762]

4. Rechtfertigungsgründe

Als Rechtfertigungsgrund kommt für Betroffene vor allem der Tatbestand der Notwehr gem. § 32 StGB, § 227 BGB in Frage. Daneben kann das Festhalten der Nutzer von Smartglasses als vorläufige Festnahme gem. § 127 ZPO und die Beschädigung der Smartglasses als Selbsthilfe gem. § 229 BGB gerechtfertigt sein.

a) Rechtfertigung durch Notwehr des Betroffenen

Als schneidigster Rechtfertigungsgrund kommt für den Betroffenen B die Notwehr gem. § 32 StGB bzw. im Fall zivilrechtlicher Tatbestände gem. § 227 BGB in Betracht.[1763] Voraussetzung ist, dass Abwehrmaßnahmen des B geboten waren, um eine aufgrund der Nutzung von Smartglasses durch A entstandene Notwehrlage zu beseitigen.

[1759] *Paeffgen*, in: Ebenda, § 224, Rn. 34; *Stree/Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, § 224, Rn. 13.

[1760] Vgl. *Paeffgen*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 224, Rn. 35.

[1761] *Wagner*, in: *Säcker/Rixecker*, MüKo BGB, § 823 BGB, Rn. 423.

[1762] Der Betroffene muss ebenfalls schuldfähig und nicht entschuldigt sein, was jedoch im Rahmen dieser Untersuchung nicht problematisiert wird.

[1763] Die Prüfung der Notwehr im Rahmen dieser Untersuchung orientiert sich am § 32 StGB, wobei die Ergebnisse entsprechend dem Grundsatz der Einheit der Rechtsordnung sowie der gesetzlichen Konzeption, ebenso auf die zivilrechtliche Notwehrvorschrift des § 227 BGB übertragen werden können, *Braun*, NJW 1998, S. 941 f.; *Dörner*, in: *Schulze*, BGB, § 227 BGB, Rn. 1 ff.; *Grothe*, in: *Säcker/Rixecker*, MüKo BGB, § 227 BGB, Rn. 1 ff.

aa) Notwehrlage

Damit eine Handlung als Notwehr qualifiziert werden kann, muss eine Notwehrlage vorliegen, d.h. ein gegenwärtiger, rechtswidriger Angriff auf ein Rechtsgut der sich wehrenden Person.[1764] Als Angriff wird die unmittelbare Bedrohung rechtlich geschützter Güter durch menschliches Verhalten betrachtet.[1765] Das Allgemeine Persönlichkeitsrecht stellt ein rechtlich geschütztes und damit notwehrfähiges Rechtsgut dar.[1766] Im Fall der Nutzung von Smartglasses im öffentlichen Raum wird das Allgemeine Persönlichkeitsrecht von Dritten, die in deren Erfassungsbereich geraten, entsprechend der bisherigen verfassungsrechtlichen und einfachgesetzlichen Prüfung verletzt. Die Verletzung des Allgemeinen Persönlichkeitsrechts erfolgt nicht nur, wenn tatsächlich audiovisuelle Aufnahmen erstellt und verwendet werden, sondern bereits aufgrund der von Smartglasses ausgehenden Überwachungs- und Anpassungseffekte.[1767] Folglich stellen die Abwehrmaßnahmen des Betroffenen B gegen den Träger von Smartglasses A eine Verteidigung gegen den von diesem ausgehenden rechtswidrigen Angriff dar.

Der Angriff muss ferner gegenwärtig sein, was vom Augenblick seines unmittelbaren Bevorstehens bis zu seinem vollständigen Abschluss angenommen wird.[1768] Der Angriff wirkt insbesondere so lange fort, wie er den bereits herbeigeführten Schaden vergrößert oder intensiviert.[1769] D.h., solange sich Betroffener B in dem Erfassungsbereich der Smartglasses von A befindet, dauert der Angriff auf seine Persönlichkeitsrechte aufgrund der fortwährenden Überwachungs- und Anpassungswirkung entsprechend § 6b BDSG an.[1770] Auch wenn alleine auf die rechtswidrige Erstellung von Aufnahmen abgestellt wird, ist deren Speicherung auf den Smartglasses ein fortdauernder rechtswidriger Zustand. Denn aufgrund

---

[1764] *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 2.

[1765] *Perron*, in: Ebenda, § 32, Rn. 3.

[1766] OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (463 f.); OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123; *Dreier/Specht*, in: *Dreier/Schulze*, UrhG, § 22 KUG, Rn. 14; *Fricke*, in: *Wandtke/Bullinger*, UrhG, § 22 KUG, Rn. 9; *Haberstroh*, JR 1983, S. 314; *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 3; *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 32, Rn. 19; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 5a.

[1767] Vgl. E II. 2. b) gg) (3), S. 128; vgl. F II. 1. e), S. 224;

[1768] *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 4; *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 32, Rn. 20; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 13.

[1769] BGH, Urt. v. 12.2.2003 (1 StR 403/02), NJW 2003, 1955 (1956); OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 53; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 15.

[1770] Vgl. F II. 1. e), S. 224.

der einfachen Möglichkeit ihrer Verbreitung und Veröffentlichung, kann sich die Persönlichkeitsrechtsverletzung jederzeit vertiefen.[1771]

bb) Notwehrhandlung

Die Notwehrhandlungen des Betroffenen sind nur dann gerechtfertigt, wenn sie als Verteidigungsmaßnahmen erforderlich, also geeignet und das mildeste Mittel der Verteidigung sind.[1772] Die Beurteilung der Erforderlichkeit ist ex ante zu treffen.[1773] Der Betroffene muss ferner mit einem Verteidigungswillen handeln, der jedoch bei Verteidigungsmaßnahmen gegen Smartglasses generell anzunehmen sein wird.[1774] Nur wenn B in der hypothetischen Konstellation davon ausgehen würde, dass A keine Aufnahmen erstellt und erstellen wird, wären seine Notwehrhandlungen nicht gerechtfertigt.

(1) Eignung von Abwehrmaßnahmen gegen Smartglasses

Eine Eignung der Notwehrhandlung zur Abwehr des Angriffs ist bereits dann anzunehmen, wenn der Angriff abgeschwächt oder erkennbar behindert wird.[1775] Lediglich Abwehrhandlungen, die gar keine Chance auf Abwehr des Angriffs bieten, sind nicht geeignet und damit keine erforderlichen Notwehrhandlungen.[1776] Dabei ist auf die subjektive Sicht des Betroffenen abzustellen.[1777] Die Abwehrmaßnahmen des B, welche in Drohungen, körperlichem Angriff, Wegnahme oder Beschädigung der Smartglasses sowie Löschung von Aufnahmen bestanden, können den von Smartglasses sowie den erstellten Aufnahmen ausgehenden Angriff auf Bs

---

[1771] Soweit die von Aufnahmen ausgehende Gegenwärtigkeit des Angriffs angezweifelt wurde, geschah dies vor allem vor dem Hintergrund einer fehelenden engen zeitlichen Verknüpfung zwischen Aufnahme und deren (befürchteter) Verbreitung in Zeiten analoger Aufnahmetechnik, *Haberstroh*, JR 1983, S. 314 (318).

[1772] OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 9; *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 32, Rn. 25; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 34.

[1773] BGH, Urt. v. 25.6.2009 (5 StR 141/09), NStZ 2009, 626 (627); BGH, Urt. v. 26.2.1969 (3 StR 322/68), NJW 1969, 802 (802); *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 10.

[1774] Vgl. BGH, Urt. v. 26.2.1969 (3 StR 322/68), NJW 1969, 802 (802); es ist unschädlich, wenn neben dem Verteidigungswillen weitere Motivation, wie z.B. Wut oder Rachegelüste hinzutreten, solange der Vereidigungswille nicht nur als nebensächlich zurück tritt, BGH, Urt. v. 1.7.1952 (1 StR 119/52), BGHSt 3, 194 (198); *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 34, Rn. 42.

[1775] *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 9; *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 32, Rn. 26; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 35.

[1776] *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 34, Rn. 26.

[1777] Denn ansonsten würden Täter belohnt, die möglichst aggressiv vorgehen und damit die objektive Möglichkeit der Notwehr schmälern würden, *Momsen*, in: Ebenda.

Rechtsgüter zumindest abschwächen, wenn nicht beseitigen und sind damit als Notwehrmaßnahmen geeignet.

(2) Erforderlichkeit von Abwehrmaßnahmen gegen Smartglasses

Stehen mehrere mögliche Abwehrmöglichkeiten zur Wahl, muss die Verteidigung nach Art und Maß das im Verhältnis mildeste Angriffsmittel sein.[1778] Ferner ist das Verteidigungsmittel so schonend wie möglich einzusetzen.[1779] Bei der Prüfung der Wirksamkeit von Verteidigungsmaßnahmen sind alle Umstände des Einzelfalles zu berücksichtigen und die Intensität der Rechtsgutbedrohung, mit deren Anstieg auch die Schärfe zulässiger Verteidigungsmittel zunimmt.[1780] So ist die kurzfristige Beeinträchtigung des B als Passant auf der Straße geringer, als wenn er über einen längeren Zeitraum in einem Café oder zwar kurzfristig, aber unbekleidet in einer Umkleidekabine von Smartglasses erfasst wird.

Der sich Wehrende muss auf die alternativen Verteidigungsmittel jedoch dann nicht ausweichen, wenn weniger gefährliche Verteidigungsmaßnahmen nicht die gleiche Wirksamkeit besitzen.[1781] D.h., er muss sich nicht auf einen unsicheren oder ungewissen Verteidigungserfolg einlassen.[1782] Im Zweifelsfall wird er damit das schärfere, aber eindeutig sicherere Verteidigungsmittel wählen dürfen.[1783] Sofern es den Verteidigungserfolg jedoch nicht gefährdet, muss der sich Wehrende abgestuft vorgehen und einschneidendere Verteidigungsmittel erst dann einsetzen, wenn die

---

1778 *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 90; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 9; *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 32, Rn. 27; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36.

1779 *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 93; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36b.

1780 BGH, Beschl. v. 16.4.1998 (4 StR 114/98), NStZ 1998, 508 (509); *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 32, Rn. 28; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 34.

1781 *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 90.

1782 BGH, Urt. v. 25.6.2009 (5 StR 141/09), NStZ 2009, 626 (627); BGH, Urt. v. 28.2.1989 (1 StR 741/88), NJW 1989, 3027; BayObLG, Beschl. v. 15.3.1988 (RReg. 1 St 49/88), NStZ 1988, 408 (409); *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 90; *Kühl*, in: *Lackner/Kühl*, StGB, § 201, Rn. 9; *Momsen*, in: *Heintschel-Heinegg*, BeckOK StrGB, § 32, Rn. 28; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36c.

1783 BGH, Urt. v. 25.11.1980 (1 StR 563/80), NStZ 1981, 138 (138); BGH, Urt. v. 24.7.1979 (1 StR 249/79), NJW 1980, 2263; BGH, Urt. v. 26.2.1969 (3 StR 322/68), NJW 1969, 802 (802); OLG Karlsruhe, Urt. v. 4.7.1985 (1 Ss 40/85), NJW 1986, 1358 (1359); *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 90; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36c.

milderen Mittel nicht zur Beendigung des Angriffs geführt haben.[1784] Daneben muss eine Auswahl der Mittel überhaupt möglich und zumutbar sein. So wird insbesondere jemandem, der durch einen Angriff überrascht wird, kaum Zeit für eine Abwägung der Mittel verbleiben.[1785]

(3) Prüfung einzelner Abwehrmaßnahmen

Nachfolgend werden die in Frage kommenden sofortigen Abwehrmaßnahmen des B auf ihre Eignung und Erforderlichkeit zur Abwehr der von den Smartglasses des A ausgehenden Gefahren untersucht.

(a) Bloßes Ausweichen

Bevor die von B ergriffenen Maßnahmen als mögliche Handlungsalternativen geprüft werden, stellt sich die Frage, ob es dem B nicht zugemutet werden könnte, der Erfassung durch die Smartglasses auszuweichen. Z.B. könnte B sein Gesicht abwenden, abdecken oder auf der Straße eine andere Richtung einschlagen. Hierbei würde es sich im Vergleich mit einem Eingriff in die Rechte des A um mildere Maßnahmen handeln.

Die Hinnahme des Ausweichens als Alternative würde jedoch verkennen, dass das Notwehrrecht anders als z.B. der Notstand nach § 34 StGB nicht nur dem Schutz des durch den Angriff betroffenen Rechtsguts, sondern entsprechend dem Grundsatz, dass „das Recht dem Unrecht nicht zu weichen braucht" dem Rechtsbewährungsprinzip dient.[1786] Die Pflicht zur Hinnahme des Angriffs auf geschützte Rechtsgüter würde daher zur Entwertung dieses Prinzips führen.[1787] Das bloße Ausweichen kann folglich nicht als eine Verteidigungsalternative des B berücksichtigt werden, da A

[1784] BGH, Beschl. v. 12.12.1975 (2 StR 451/75), BGHSt 26, 256 (257); BGH, Urt. v. 15.5.1975 (4 StR 71/75), BGHSt 26, 143 (145 f.); *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36a.

[1785] BGH, Urt. v. 24.7.1979 (1 StR 249/79), NJW 1980, 2263; *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 90; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36; ferner ist bei der Beurteilung der Erforderlichkeit der Verteidigungsmaßnahme auf die Notwendigkeit der Verteidigungshandlung und nicht auf die beim Angreifer eingetretene Rechtsgutverletzung abzustellen, BGH, Urt. v. 25.11.1980 (1 StR 563/80), NStZ 1981, 138; BGH, Urt. v. 21.12.1977 (2 StR 421/77), BGHSt 27, 313 (314); *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 91; es ist grundsätzlich unerheblich, wenn der Erfolg der Handlung größer ist, als von der sich verteidigenden Person beabsichtigt, ebenda.

[1786] Vgl. BGH, Urt. v. 12.2.2003 (1 StR 403/02), NJW 2003, 1955 (1957); *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 1; *Perron*, in: *Schönke/Schröder*, StGB, § 34, Rn. 1 f., 40.

[1787] OLG Karlsruhe, Urt. v. 4.7.1985 (1 Ss 40/85), NJW 1986, 1358 (1360); *Perron*, in: *Schönke/Schröder*, StGB, § 34, Rn. 40.

hierdurch in der rechtsverletzenden Nutzung der Smartglasses nicht eingeschränkt wäre.[1788]

Dementsprechend ist es den Betroffenen nicht zuzumuten, sich der Erfassung durch Smartglasses zu entziehen, indem sie eine andere Gehrichtung einschlagen. Erst recht ist auch das Verdecken des Gesichts keine Alternative zu einer Verteidigung gegen die Herstellung von Bildnissen.[1789] Dies gilt insbesondere, weil Betroffene auch anhand anderer Umstände als des Gesichts erkannt werden könnten und diese Art der Verteidigung daher nicht gleichermaßen wie schärfere Verteidigungsmittel geeignet ist.[1790]

(b) Hilfe durch die Polizei

Private Notwehr ist gegenüber staatlichem Schutz subsidiär, weswegen ihre Erforderlichkeit entfällt, wenn zuständige und zum Einschreiten bereite staatliche Organe, wie z.B. die Polizei, präsent sind oder ohne Weiteres herbeigerufen werden können.[1791]

Das Einschreiten der Polizei ist als Sofortmaßnahme zum Schutz der Rechte von Privatpersonen dann erlaubt, ermessensgerecht und sogar geboten, wenn eine akute Gefahrenlage vorliegt, die befürchten lässt, dass ein Zuwarten oder Verweis auf andere Verteidigungsmittel zu einem nicht abwendbaren Schaden führen kann.[1792] Eine solche Konstellation liegt, wie bereits festgestellt, im Fall von Smartglasses vor, da sich deren Nutzer unerkannt entfernen könnten.[1793] Das bedeutet, der Betroffene B kann grundsätzlich erwarten, dass die Polizei einschreiten wird, allerdings nur, wenn sie zugegen ist oder ohne Weiteres herbeigerufen werden kann, ohne dass der Verteidigungserfolg gefährdet wird.[1794] Ob das der Fall ist, wird anhand des Einzelfalles zu entscheiden sein. Es ist jedoch

---

[1788] Allenfalls in speziellen Situationen, z.B. wenn der Angriff von einem schuldunfähigen Kind begangen wurde oder von einer Person zu der er eine enge zwischenmenschliche Beziehung besteht, können sich Ausnahmen von diesem Prinzip ergeben und ein Ausweichen geboten machen, vgl. BGH, Urt. v. 26.2.1969 (3 StR 322/68), NJW 1969, 802 (802); BayObLG, Beschl. v. 28.2.1991 (RReg. 5 St 14/91), NJW 1991, 2031.

[1789] OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (464 f.).

[1790] Ebenda.

[1791] BGH, Urt. v. 3.2.1993 (3 StR 356/92), BGHSt 39, 133 (137); *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 95; *Perron*, in: *Schönke/Schröder*, StGB, § 34, Rn. 41.

[1792] *Gusy*, Polizei- und Ordnungsrecht, 2014, Rn. 90 ff.; *Pieroth u.a.*, Polizei- und Ordnungsrecht, 2014, § 5, Rn. 18 f., 24 ff.; *Schmidt*, Polizei- und Ordnungsrecht, 2015, Rn. 634 ff.

[1793] Vgl. F V. 1, S. 290.

[1794] Vgl. BGH, Urt. v. 3.2.1993 (3 StR 356/92), BGHSt 39, 133 (137); OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); *Perron*, in: *Schönke/Schröder*, StGB, § 34, Rn. 41.

damit zu rechnen, dass die Polizei sich im Regelfall nicht vor Ort befinden wird.

Ein weiteres Problem kann bei einer Teilkooperation des A entstehen, wenn dieser z.B. die Smartglasses nicht herausgeben will, aber zusichert, auf die Polizei zu warten (und mit dessen Flucht aufgrund der Umstände nicht zu rechnen ist, z.B. weil B dem A körperlich überlegen ist oder die Örtlichkeiten es nicht erlauben). In diesem Fall würde ein Abwarten der Polizei ein milderes Verteidigungsmittel darstellen. Es würde den Verteidigungserfolg jedoch nur dann nicht gefährden, wenn sichergestellt wäre, dass A die Smartglasses nicht weiter bedienen und z.B. Aufnahmen auf einen Cloud-Speicher transferieren kann.

(c) Verbale oder konkludente Aufforderung

Bevor Betroffener B die gegen Rechtsgüter des A gerichteten Maßnahmen ergriff, forderte er den A zur Erfüllung seiner Forderungen auf. In der Abwandlung der Situation verzichtete B auf eine derartige Aufforderung.[1795] Es fragt sich an dieser Stelle, ob eine verbale Forderung gegenüber den Trägern von Smartglasses nicht generell schärferen Maßnahmen vorgehen muss und B daher in der Abwandlung nicht auf sie verzichten durfte.

Die Aufforderung gegenüber einem Träger von Smartglasses, das Gerät abzunehmen, eine Örtlichkeit zu verlassen oder Auskunft über etwaige Ausnahmen zu geben, ist ein milderes Mittel gegenüber der Androhung oder Anwendung von Gewalt.[1796] Eine solche Aufforderung wird dem Betroffenen dann zuzumuten sein, wenn der Erfolg seiner Verteidigung nicht gefährdet wird.[1797] Um das zu prüfen, müssen jedoch Umstände im Einzelfall gewürdigt werden. Generell ist in einer Aufforderung kein Nachteil für die Verteidigung zu sehen. So wurde entschieden, dass z.B. in Fällen einer Persönlichkeitsverletzung durch verbale Ehrkränkung die sofortige tätliche Notwehr nur ausnahmsweise erforderlich ist.[1798] Auch im Fall von Smartglasses erscheint eine verbale Aufforderung im Regelfall gegenüber der Gewaltanwendung oder ihrer Androhung ein milderes und

---

[1795] Vgl. F V. 4. a) bb) (3) (c), S. 302.

[1796] In vergleichbaren Konstellationen, die gerichtlich entschieden wurden, war die Frage der Notwendigkeit einer Aufforderung nicht zu entscheiden, da die Betroffenen die Fotografen zuvor zur Einstellung der perönlichkeitsrechtsverletzenden Handlungen aufgefordert haben, OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (462 f.); OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971; OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123.

[1797] Vgl. OLG Karlsruhe, Urt. v. 4.7.1985 (1 Ss 40/85), NJW 1986, 1358 (1359 f.).

[1798] BGH, Urt. v. 14.2.1952 (5 StR 1/52), BGHSt 3, 217 (218); BayObLG, Beschl. v. 28.2.1991 (RReg. 5 St 14/91), NJW 1991, 2031.

zugleich genauso geeignetes Mittel zur Gefahrenabwehr zu sein. Denn zumindest die reine Überwachungsgefahr ist im Einzelfall eher mit einer Ehrkränkung als z.B. mit einer Gewaltanwendung zu vergleichen. Die Aufforderung wird dem Betroffenen jedoch spätestens im Fall einer erheblichen Rechtsgutbedrohung, insbesondere verbunden mit einem Überraschungsmoment, nicht zuzumuten sein.[1799] Wer durch einen Angriff überrascht wird, dem wird grundsätzlich keine Zeit für eine Abwägung der Mittel verbleiben.[1800] Ferner ist zu beachten, dass sich eine Aufforderung auch nonverbal aus den Umständen ergeben kann. So müssen z.B. eine vor das Gesicht gehaltene Hand, rüde Gesten oder Kraftausdrücke als hinreichende Aufforderung, die Smartglasses abzusetzen oder den Raum zu verlassen, verstanden werden.[1801]

Das bedeutet vorliegend, dass es dem B zuzumuten wäre, seine Forderungen gegenüber dem A zu äußern, wenn er von dessen Smartglasses auf der Straße oder in einem Café erfasst wird. Dagegen würde eine Erfassung in der Umkleidekabine erheblich in die Rechtsgüter des B eingreifen und mit einem Moment der Überraschung verbunden sein. In dieser Konstellation wird B schärfere Verteidigungsmittel ergreifen können, ohne den A vorher verbal auffordern zu müssen, sein Verhalten einzustellen.

(d) Androhung von Gewalt

Anders als die bloße Aufforderung zu einer Handlung oder Unterlassung, erfüllt die Drohung mit Gewalt den Tatbestand einer (zumindest gem. § 240 Abs. 3 StGB versuchten) Nötigung und stellt damit eine weniger milde Maßnahme dar. Jedoch ist die Nötigung wiederum ein gegenüber der tatsächlichen Gewaltanwendung milderes Verteidigungsmittel.[1802]

Allerdings dürfte auch die Gewaltandrohung den Erfolg der Notwehrhandlung nicht vereiteln. So könnte z.B. eine Androhung der Wegnahme der Smartglasses dazu führen, dass deren Träger ihre Wehrhaftigkeit verstärken oder weglaufen. Etwas anderes gilt nur dann, wenn die Dro-

---

[1799] BGH, Urt. v. 24.7.1979 (1 StR 249/79), NJW 1980, 2263; *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 90; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36.

[1800] BGH, Urt. v. 24.7.1979 (1 StR 249/79), NJW 1980, 2263; *Kindhäuser*, in: *Kindshäuser/Neumann/Paeffgen*, StGB, § 32, Rn. 90; *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36.

[1801] Vgl. die Situation in *Slocum*, Assaulted and Robbed at Molotov Bar on Haight St. for Wearing Google Glass, YouTube, https://www.youtube.com/watch?v=BvTrx-i_nB4 (7.9.2015); *Pachal*, Woman Robbed, Assaulted for Wearing Google Glass in a Bar, Mashable, http://mashable.com/2014/02/26/google-glass-assault/(7.9.2015).

[1802] BGH, Beschl. v. 21.3.2001 (1 StR 48/01), NJW, 2001, 3200 (3202); BGH, Beschl. v. 12.12.1975 (2 StR 451/75), BGHSt 26, 256 (257); *Perron*, in: *Schönke/Schröder*, StGB, § 32, Rn. 36a.

hung den Verteidigungserfolg wegen der körperlichen Überlegenheit der sich verteidigenden Person nicht gefährdet.[1803] Ebenfalls ist die vorhergehende Androhung des Einsatzes lebensgefährlicher Verteidigungsmaßnahmen, z.B. beim Einsatz von Messern oder Pistolen, als milderes Mittel grundsätzlich erforderlich.[1804] Eine ähnliche Gefahr kann auch bei einem Schlag gegen Smartglasses, der zu einer gefährliche Körperverletzung führen kann, vorliegen.[1805] D.h., zumindest bevor derart gefährliche Gewaltanwendung bezweckt wird und nicht bloß die Smartglasses weggenommen oder die Person festgehalten werden soll, ist eine Androhung der Gewalt als ein milderes Mittel gegenüber ihrer Anwendung vorzuziehen.

Ferner wird es wie im Fall der bloßen Aufforderung auf die Intensität der Rechtsgutverletzung und den Überraschungsmoment ankommen.[1806] So wird dem B nicht zuzumuten sein, A Gewalt anzudrohen, bevor er die Tür der Umkleide dem A „vors Gesicht schlägt".

(e) Wegnahme der Smartglasses

Es kann zwei Gründe geben, auf die sich Betroffene berufen können, um dem Nutzer die Smartglasses wegzunehmen. Zum einen kann dadurch die rechtswidrige Videoüberwachung beendet werden. Zum anderen kann sich der Betroffene so davon überzeugen, ob Aufnahmen auf dem Gerät vorhanden sind, und diese löschen.[1807] Die Wegnahme wird in beiden Fällen gegenüber der Anwendung von Personengewalt grundsätzlich ein milderes Mittel darstellen. Ist es dem Betroffenen möglich, sich die notwendige Auskunft einzuholen oder Aufnahmen zu löschen, muss er die Smartglasses an ihren Nutzer zurückgeben.[1808] Ist der Betroffene sich dagegen nicht sicher, wie die Smartglasses zu bedienen sind, oder kann er das Gerät wegen einer Zugangssperre nicht nutzen, ist er berechtigt, eine kompetente dritte Person hinzuzuziehen, schriftliche Bestätigung, dass

---

[1803] BGH, Beschl. v. 12.12.1975 (2 StR 451/75), BGHSt 26, 256 (257); OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (465); OLG Frankfurt a.M., Urt. v. 1.10.1993 (10 U 181/92), NJW 1994, 946 (947).

[1804] BGH, Beschl. v. 11.8.2010 (1 StR 351/10), NStZ-RR 2011, 238 (238); BGH, Urt. v. 12.2.2003 (1 StR 403/02), NJW 2003, 1955 (1957); BGH, Beschl. v. 21.3.2001 (1 StR 48/01), NJW, 2001, 3200 (3202); BGH, Urt. v. 15.5.1975 (4 StR 71/75), BGHSt 26, 143 (145); *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 9.

[1805] Vgl. F V. 3. d), S. 295.

[1806] Vgl. F V. 4. a) bb) (3) (c), S. 302.

[1807] Diese Maßnahme ist jedoch nur dann geeignet, wenn der Betroffene davon ausgehen konnte, über die nötigen technischen Fähigkeiten zur verfügen.

[1808] Vgl. OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123.

keine Aufnahmen erstellt wurden, zu verlangen, bzw. dass der Nutzers der Smartglasses sich ausweist.[1809]

(f) Datenveränderung

Die Löschung von Aufnahmen stellt trotz der Gefahr ihrer Wiederherstellung eine geeignete und die mildeste Maßnahme zur Durchsetzung der Löschungsansprüche des Betroffenen dar.

(g) Beschädigung oder Zerstörung der Smartglasses

Die vorsätzliche Beschädigung oder Zerstörung von Smartglasses ist zumindest dazu geeignet, die rechtswidrige Videoüberwachung zu beenden. Sie wird im Regelfall ein milderes Mittel der Gewaltanwendung darstellen als die Körperverletzung. Dies kann im Einzelfall anders zu beurteilen sein, z.B. wenn die Körperverletzung nur sehr geringer Natur wäre, der wirtschaftliche Schaden durch die Zerstörung der Smartglasses des Betroffenen dagegen sehr groß. Ebenso wird ein Festhalten des Betroffenen ein gegenüber der Zerstörung von Smartglasses milderes Mittel sein. Allerdings wird die Wegnahme nicht gleichermaßen tauglich sein, wenn Anhaltspunkte dafür bestehen, dass der Nutzer von Smartglasses sich wehren und so die Wegnahme verhindern könnte (z.B. wegen seiner körperlichen Überlegenheit).[1810] In diesem Fall wird die Zerstörung des Gerätes erforderlich sein.

Die Zerstörung der Smartglasses wird ebenfalls ein geeignetes Mittel zur Vernichtung von Aufnahmen darstellen. Jedoch wird die Möglichkeit bloßer Wegnahme oder mögliche Löschung der Aufnahmen ein milderes und gleich effektives Mittel darstellen, wodurch die Zerstörung nicht erforderlich wäre. Dies gilt jedoch nur, wenn der Betroffene nicht damit rechnen muss, dass der Nutzer der Smartglasses diese zurückzugewinnen versuchen und aufgrund seiner körperlichen Konstitution eine Chance hierzu haben wird.

(h) Festhalten des Nutzers von Smartglasses

Das vorübergehende Festhalten des Nutzers von Smartglasses ohne Körperverletzung bis Hilfe, z.B. durch die Polizei, eingetroffen ist, wird ein zur Beendigung der Videoüberwachung oder Durchsetzung des Auskunfts- und Löschungsverlangens geeignetes und erforderliches Mittel sein. Jedoch wird es auch an dieser Stelle auf die körperlichen Verhältnisse der Beteiligten und die Intensität der Rechtsgutverletzungen ankommen.[1811] D.h., wenn keine Fluchtgefahr besteht, ist ein Festhalten nicht

---

[1809] In Frage kommt auch eine Hinterlegung bei einem Sequester, vgl. F IV. 5. d), S. 288.

[1810] vgl. OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (465).

[1811] Vgl. F V. 4. a) bb) (2), S. 299.

erforderlich. Andererseits kann die Erheblichkeit der Rechtsgutverletzung ein Festhalten gebieten, wie z.B. wenn A die Umkleide des B betritt. Ferner ist ein Festhalten kein im Vergleich mit der Wegnahme von Smartglasses gleich wirksames Verteidigungsmittel, wenn A währenddessen die Smartglasses z.B. mit Stimmbefehlen steuern und Aufnahmen verbreiten oder andernorts sichern könnte.

(i) Körperverletzung

Die direkte Anwendung von Gewalt gegen den Körper des Trägers von Smartglasses gehört zu den schärfsten Notwehrmitteln und ist grundsätzlich als letzte Maßnahme in Betracht zu ziehen. Muss der Betroffene jedoch befürchten, aufgrund körperlicher Unterlegenheit mit anderen Maßnahmen, wie z.B. Wegnahme der Smartglasses, keinen Verteidigungserfolg erzielen zu können, wird er Gewalt anwenden dürfen. Das gilt ebenfalls bei einer hohen Intensität der Rechtsgutverletzung und Vorliegen eines Überraschungsmoments.[1812]

cc) Irrtum über die tatsächlichen Umstände

Betroffene könnten sich über die tatsächlichen Umstände der Nutzung von Smartglasses irren. Es kann insbesondere häufig vorkommen, dass ein Dritter davon ausgeht, dass von ihm Aufnahmen erstellt wurden, obwohl dies tatsächlich nicht der Fall war. Allerdings wird kein Fall eines Irrtums vorliegen, wenn der Dritte die Notwehrmittel zugleich ergreift, um überhaupt eine Auskunft über das Vorliegen von potentiellen Aufnahmen zu erhalten, wie es im Regelfall anzunehmen sein wird. Denn ein Auskunftsverlangen besteht unabhängig vom Vorliegen tatsächlicher Aufnahmen.

Irrtümer können auch im Hinblick auf übrige Umstände, wie der Beurteilung der Eignung oder Erforderlichkeit einer Notwehrmaßnahme, vorliegen. Z.B. könnten Betroffene die körperliche Kraft des Nutzers von Smartglasses falsch einschätzen und körperliche Gewalt anwenden, obwohl es einfacher gewesen wäre, dem Nutzer die Smartglasses wegzunehmen.[1813] Ebenso könnte die Zerstörung von Smartglasses zum Zwecke der Vernichtung von Aufnahmen entgegen der Vorstellung der sich Wehrenden ungeeignet sein, wenn die Aufnahmen bereits auf einen externen Cloud-Speicher transferiert worden sind.

Im Fall derartiger Erlaubnistatbestandsirrtümer wäre die subjektiv vorgestellte Notwehr nicht erforderlich und es läge ein Erlaubnistatbestandsirrtum gem. § 16 Abs. 1 Satz 1 StGB vor, der zum Ausschluss einer

---

[1812] Vgl. F V. 4. a) bb) (2), S. 299.

[1813] Vgl. BGH, Urt. v. 9.5.2001 (3 StR 542/00), NStZ 2001, 530 (530); *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 19.

strafbaren Tat führen würde.[1814] Nach § 16 Abs. 1 Satz 2 StGB wäre jedoch die Begehung einer fahrlässigen Tat weiterhin möglich, was im Fall der fahrlässigen Körperverletzung gem. § 229 StGB in Frage käme. Wäre der Irrtum jedoch gem. § 17 Abs. 1 Satz 1 StGB unvermeidbar, dann hätte der Betroffene schuldlos gehandelt und wäre nicht strafbar.[1815]

Ein Irrtum gilt als vermeidbar, wenn der Täter „die gehörige Anspannung seines Gewissens unterlassen und dadurch versäumt hat, das Unrechtmäßige seines Handelns zu erkennen".[1816] D.h., die Annahme der Unermeidbarkeit setzt voraus, dass der Täter „alle seine geistigen Erkenntniskräfte eingesetzt und aufgetretene Zweifel durch Nachdenken und erforderlichenfalls durch Einholung von Rat bei einer sachkundigen und vertrauenswürdigen Stelle oder Person beseitigt hat."[1817] Im Hinblick auf die Vermeidbarkeit von Erlaubnistatbestandsirrtümern im Zusammenhang mit der Annahme von Persönlichkeitsrechtsverletzungen durch Herstellung von Fotografien hat sich die bisherige Rechtsprechung, zumindest in Augenblickssituationen und ganz besonders wenn der Betroffene überrascht worden ist oder in seine Persönlichkeitssphäre erheblich eingegriffen worden ist, zugunsten des Betroffenen ausgesprochen.[1818] Sollte der Irrtum dennoch vermeidbar gewesen sein, ist zumindest an eine mögliche Strafmilderung gem. § 17 Satz 2 StGB zu denken.[1819]

[1814] BGH, Beschl. v. 11.8.2010 (1 StR 351/10), NStZ-RR 2011, 238 (238); BayObLG, Beschl. v. 28.2.1991 (RReg. 5 St 14/91), NJW 1991, 2031 (2032); OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (465); OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123; OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); *Kühl*, in: *Lackner/Kühl*, StGB, § 32, Rn. 19.

[1815] BayObLG, Beschl. v. 28.2.1991 (RReg. 5 St 14/91), NJW 1991, 2031 (2032); OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (465); OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123; OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971 (1972); ebenso wäre keine Fahrlässigkeit gem. § 276 BGB im Hinblick auf zivilrechtliche Rechtsgutverletzungen anzunehmen.

[1816] BGH, Urt. v. 26.6.1962 (5 StR 180/62), NJW 1962, 1831 (1832); BGH, Urt. v. 23.4.1953 (3 StR 219/52), BGHSt 4, 236 (243); BGH, Urt. v. 19.12.1952 (1 StR 2/52), BGHSt 3, 357 (366); *Kühl*, in: *Lackner/Kühl*, StGB, § 17, Rn. 7; *Sternberg-Lieben/Schuster*, in: *Schönke/Schröder*, StGB, § 17, Rn. 14.

[1817] BGH, Urt. v. 21.6.1990 (1 StR 477/89), BGHSt 37, 55 (67); BGH, Urt. v. 8.11.1965 (8 StE 1/65), BGHSt 20, 342 (372); BGH, Urt. v. 23.4.1953 (3 StR 219/52), BGHSt 4, 236 (243); BGH, Urt. v. 19.12.1952 (1 StR 2/52), BGHSt 3, 357 (366); OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (465); *Kühl*, in: *Lackner/Kühl*, StGB, § 17, Rn. 7; *Sternberg-Lieben/Schuster*, in: *Schönke/Schröder*, StGB, § 17, Rn. 18.

[1818] OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (465); OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123; OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971.

[1819] OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462 (465).

Im Ergebnis ist festzuhalten, dass die Intransparenz der Nutzung von Smartglasses sich in einem sehr umfangreichen und starken Notwehrrecht der Betroffenen widerspiegelt, was sich auch im Fall eines Irrtums über tatsächlich vorliegende Aufnahmen auswirkt.

b) Vorläufige Festnahme gem. § 127 StPO

§ 127 Abs. 1 Satz 1 StPO gewährt jedermann das Recht zur vorläufigen Festnahme einer Person, wenn diese auf frischer Tat betroffen oder verfolgt wird sowie der Flucht verdächtig ist oder ihre Identität nicht sofort festgestellt werden kann. Eine Tat in diesem Sinne ist eine rechtswidrige, schuldhaft begangene Tat, die den Tatbestand eines Strafgesetzes verwirklicht.[1820] Folglich kann sich ein Betroffener dann auf § 127 StPO berufen, wenn der Träger von Smartglasses wegen der Begehung einer Tat gem. § 33 KUG, § 44 BDSG oder §§ 201, 201a StGB strafbar wäre. Da die Festnahme nach § 127 Abs. 1 Satz 1 StPO jedoch nur der Sicherung der Strafverfolgung dient, kann sie nicht als Grundlage für eine präventive Verhinderung weiterer Straftaten herangezogen werden.[1821]

Der Tatverdacht ist dringend, wenn die äußeren Umstände es nahelegen, wobei maßgeblich ist, wie sich die Situation für den Festnehmenden ex ante darstellt.[1822] Auf frischer Tat betroffen ist derjenige, der bei der Begehung einer rechtswidrigen Tat oder unmittelbar danach am Tatort oder in dessen unmittelbarer Nähe gestellt wird.[1823] Eine Verfolgung auf frischer Tat liegt vor, wenn sie unmittelbar aufgenommen wird, nachdem die kurz zuvor begangene Tat entdeckt wurde.[1824] Im Fall der Nutzung von Smartglasses im öffentlichen Raum kommen insbesondere Situationen der Verletzung höchstpersönlicher Bereiche gem. § 201a StGB oder der Verletzung der Vertraulichkeit des Wortes gem. § 201 StGB als zur Festnahme berechtigende Taten in Frage. Z.B. dürfte der Betroffene B von

---

[1820] *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 2; *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 7.

[1821] *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 10.

[1822] BGH, Urt. v. 18.11.1980 (VI ZR 151/78), NJW 1981, 745 (745); OLG Hamm, Beschl. v. 8.1.1998 (2 Ss 1526/97), NStZ 1998, 370 (370); BayObLG, Urt. v. 30.5.1986 (RReg. 5 St 43/86), BayObLGSt 1986, 52 (53 f.); m.w.N., auch im Hinblick auf eine einschränkende Minderansicht, die darauf abstellt, dass die Tat wirklich begangen sein muss, *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 3; *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 9.

[1823] *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 4; *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 10 f.

[1824] *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 5; *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 12.

einer Tat gem. § 201a Abs. 1 Nr. 1 StGB ausgehen, wenn A mit aufgesetzten Smartglasses in seine Umkleidekabine hineinblickt.[1825]

Die vorläufige Festnahme setzt ferner voraus, dass der Nutzer von Smartglasses der Flucht verdächtig ist oder seine Identität nicht sofort festgestellt werden kann. Der Fluchtverdacht ist gegeben, wenn der Betroffene nach dem erkennbaren Verhalten des Nutzers von Smartglasses vernünftigerweise davon ausgehen muss, dieser werde sich dem Strafverfahren durch Flucht entziehen, wenn er nicht alsbald festgenommen wird.[1826] Hierfür müssen Anhaltspunkte im Einzelfall vorliegen, die auf eine Fluchtbereitschaft des Trägers von Smartglasses hinweisen.[1827]

Die Identität eines Täters kann nicht sofort festgestellt werden, wenn ernstliche Zweifel bestehen, dass er ohne Vernehmung oder weitere Nachforschungen identifiziert werden kann.[1828] Identitätszweifel bestehen dann, wenn der Täter Angaben zur Person verweigert oder keine gültigen Ausweispapiere mit sich führt.[1829] Dabei reichen Namensangaben nicht aus, wenn sie an Ort und Stelle nicht überprüft werden können.[1830] Nur wenn die Person bekannt ist, z.B. wenn es sich bei dem Träger von Smartglasses um einen Nachbarn des Betroffenen handeln würde, wäre ihre Identität hinreichend festgestellt.[1831]

Die Festnahme selbst ist zwar an keine bestimmte Form gebunden, erlaubt jedoch grundsätzlich keine Gewalt, die über das Festhalten der Person oder Wegnahme bzw. Zerstörung oder Beschädigung von Sachen hinausgeht.[1832] Jegliche physische Gewaltanwendung darf nur unter Beachtung des Verhältnismäßigkeitsgrundsatzes erfolgen.[1833] Die Gewaltanwendung darf als „natürliche Folge“ der Verwirklichung des Festnahmerechts ein nach Lage der Sache erforderliches festes Anfassen oder Anpa-

---

[1825] Vgl. F III. 2. c), S. 253.

[1826] BGH, Urt. v. 11.6.1991 (1 StR 242/91), BeckRS 1991, 31085305 (31085305); *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 6; *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 16.

[1827] Vgl. BayObLG, Beschl. v. 25.7.2002 (5 StR RR 209/2002), NStZ-RR 2002, 336.

[1828] *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 7; *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 17 f.

[1829] *Paeffgen*, in: *Wolter*, SK-StPO, § 127, Rn. 16.

[1830] RG, Urt. v. 2.5.1895 (1164/95), RGSt 27, 198 (199).

[1831] RG, Urt. v. 13.11.1933 (II 579/33), RGSt 67, 351 (353).

[1832] *Krauß*, in: *Graf*, BeckOK StPO, § 127 StPO, Rn. 11; *Paeffgen*, in: *Wolter*, SK-StPO, § 127, Rn. 19.

[1833] BGH, Urt. v. 10.2.2000 (4 StR 558/99), BGHSt 45, 378 (381); OLG Stuttgart, Beschl. v. 2.3.1984 (3 Ss (14) 75/84), NJW 1984, 1694 (1695); *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 19.

cken zur Verhinderung der Flucht umfassen.[1834] Eine ernsthafte Beschädigung der Gesundheit der festgehaltenen Person, z.B. durch einen Schlag auf die Smartglasses oder gar lebensgefährdende Handlungen, sind dagegen nicht erlaubt.[1835] Allerdings ist das Festnahmerecht nur bei einem offensichtlichen Missverhältnis ausgeschlossen, da dem Festnehmenden nur begrenzte Beurteilungsmöglichkeiten bei der „Augenblicksentscheidung" zur Verfügung stehen.[1836] Das bedeutet, dass bei der Entscheidung über das zulässige Maß des Festhaltens der Grad der Verletzung der Persönlichkeitsrechte des Betroffenen und ein vorliegendes Überraschungsmoment maßgeblich werden.[1837]

Zusammenfassend wird der § 127 StPO neben dem in der Augenblickssituation i.d.R. ohnehin vorliegenden Notwehrrecht der Betroffenen eher eine untergeordnete Rolle spielen, zumal er nur repressives Einschreiten und eine von der Intensität her geringere Einwirkung auf den Träger von Smartglasses erlaubt.

c) Selbsthilfe gem. § 229 BGB

§ 229 BGB erlaubt es, Sachen zum Zweck der Selbsthilfe wegzunehmen, zu zerstören oder zu beschädigen als auch Verdächtige, die der Flucht verdächtig sind, festzunehmen oder Widerstand gegen eine Handlung, die sie zu dulden verpflichtet sind, zu beseitigen. Insbesondere können Betroffene auf Grundlage des § 229 BGB ihre zivilrechtlichen Ansprüche gem. §§ 823, 1004, 242 BGB auf Beseitigung, Unterlassung oder Auskunft im Rahmen der Selbsthilfe durchsetzen.[1838] Allerdings ist auch dieser Rechtfertigungsgrund nur dann einschlägig, wenn obrigkeitliche Hilfe nicht rechtzeitig zu erlangen ist und ohne sofortiges Eingreifen die Gefahr besteht, dass die Verwirklichung des Anspruchs vereitelt oder wesentlich erschwert wird.[1839] Dies wird, wie bereits im Rahmen der Notwehr, aufgrund der Schwierigkeit nachträglicher Geltendmachung der Ansprüche im Regelfall gegeben sein.[1840] Die Selbsthilfe muss gem. § 230 Abs. 1 BGB erforderlich sein. Die Erforderlichkeit entspricht der gleichen Vorausset-

---

[1834] OLG Stuttgart, Beschl. v. 2.3.1984 (3 Ss (14) 75/84), NJW 1984, 1694 (1695).

[1835] Vgl. BGH, Urt. v. 10.2.2000 (4 StR 558/99), BGHSt 45, 378 (381).

[1836] BayObLG, Urt. v. 30.5.1986 (RReg. 5 St 43/86), BayObLGSt 1986, 52 (53 f.); *Schultheis*, in: *Hannich*, KK-StPO, § 127 StPO, Rn. 19.

[1837] Vgl. F V. 4. a) bb) (2), S. 299.

[1838] Vgl. F IV. 5, S. 279; vgl. *Dennhardt*, in: *Bamberger/Roth*, BeckOK BGB, § 229, Rn. 3 f.; *Grothe*, in: *Säcker/Rixecker*, MüKo BGB, § 229 BGB, Rn. 3.

[1839] Vgl. OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123; *Dennhardt*, in: *Bamberger/Roth*, BeckOK BGB, § 229, Rn. 5; *Grothe*, in: *Säcker/Rixecker*, MüKo BGB, § 229 BGB, Rn. 4 f.

[1840] Vgl. F V. 4. a) bb) (3) (b), S. 301.

zung im Rahmen der Notwehr, sodass auf die dortige Interessenabwägung verwiesen werden kann.[1841] Im Fall eines Irrtums über die tatbestandlichen oder rechtlichen Voraussetzungen der Selbsthilfe gem. §§ 229, 230 BGB wäre der Betroffene dem Träger von Smartglasses gem. § 231 BGB auch dann zum Schadensersatz verpflichtet, wenn er nicht gem. § 276 BGB fahrlässig gehandelt hätte. Allerdings wird das Verschulden im Fall eines unvermeidbaren Verbotsirrtums entsprechend den Voraussetzungen der Notwehr ausscheiden.[1842]

5. Ergebnis zu sofortigen Abwehrmaßnahmen

Anders als bei traditioneller Videoüberwachung oder Fotografie ist im Fall von Smartglasses damit zu rechnen, dass Betroffene ihre Rechte unmittelbar gegenüber den Nutzern von Smartglasses geltend machen werden. Sie werden sich hierbei vor allem auf das Recht der Notwehr gem. § 32 StGB, § 227 BGB berufen können. Die rechtswidrige Videoüberwachung und die Gefahr, dass Nutzer von Smartglasses sich werden entfernen können, begründet eine Notwehrlage, die Betroffene grundsätzlich zum sofortigen Eingreifen berechtigt.

Jedoch wird die Gebotenheit der Maßnahmen Betroffener von den konkreten Umständen abhängen. Grundsätzlich müssen Betroffene aus den ihnen zur Verfügung stehenden Maßnahmen die mildesten wählen, es sei denn, sie gefährden damit den Verteidigungserfolg. Im Regelfall wird ihnen zuzumuten sein, die Nutzer von Smartglasses zuerst aufzufordern, die Smartglasses abzusetzen sowie Auskunft über etwaige Aufnahmen zu geben als auch diese zu löschen. Erst dann werden sie Gewalt androhen und diese durch Wegnahme von Smartglasses, deren Zerstörung sowie Festhalten oder Schlagen ihrer Nutzer anwenden dürfen. Abweichungen können sich jedoch ergeben, wenn der Angriff besonders intensiv in die Rechte Betroffener eingreift oder von einem Überraschungsmoment begleitet wird. Bei der Anwendung der körperlichen Gewalt werden Betroffene zudem berücksichtigen müssen, dass ein Schlag gegen die vor dem Auge der Träger von Smartglasses befindlichen Smartglasses je nach Art des Schlags und Konstruktion der Datenbrille zu schweren Verletzungen führen kann und die Datenbrille insoweit als ein gefährliches Werkzeug gem. § 224 Abs. 1 Nr. 2 Alt. 2 StGB zu betrachten wäre.

In den als Beispiele angenommenen Konfliktsituationen zwischen dem Nutzer von Smartglasses A und dem Betroffenen B bedeutet dies, dass B

[1841] Vgl. F V. 4. a) bb), S. 298; *Dennhardt*, in: *Bamberger/Roth*, BeckOK BGB, § 230, Rn. 1 ff.; *Grothe*, in: *Säcker/Rixecker*, MüKo BGB, § 230 BGB, Rn. 1.

[1842] *Grothe*, in: *Säcker/Rixecker*, MüKo BGB, § 231 BGB, Rn. 1 i.V.m. § 227 BGB, Rn. 26; vgl. F V. 4. a) cc), S. 306.

sich gegen A ohne Vorwarnung mit Gewalt wehren darf, wenn A mit aufgesetzten Smartglasses in dessen Umkleidekabine blickt. Gerät B dagegen auf der Straße oder in einem Café in den Erfassungsbereich der Smartglasses, wird er A zuerst auffordern müssen, die Smartglasses abzusetzen oder den Ort zu verlassen. Sollte B in Befürchtung rechtswidriger Aufnahmen den A zur Auskunft und Löschung auffordern, der A jedoch Anstalten machen sich entfernen zu wollen, wird B ihm mit Gewalt oder Wegnahme der Smartglasses drohen müssen. Dies gilt jedoch nur dann, wenn keine Gefahr besteht, dass A als Folge der Drohung seine Abwehr stärkt und z.B. aufgrund körperlicher Überlegenheit die Durchsetzung der angedrohten Gewalt oder Wegnahme der Smartglasses verhindern kann.

Ob A tatsächlich Aufnahmen erstellt hat oder nicht, wird in den meisten Fällen irrelevant sein. Zum einem ist B zur Abwehr der rechtswidrigen Videoüberwachung berechtigt und zum anderen zur Durchsetzung seines Auskunftsanspruchs im Hinblick auf die Frage, ob überhaupt Aufnahmen erstellt worden sind. Im Übrigen werden Tatbestandsirrtümer des B in einer derartigen Lage im Regelfall unvermeidbar sein, da die Aufnahmevorgänge der Smartglasses intransparent sind.

Zusätzlich zur Notwehr stehen Betroffenen Ansprüche aus § 127 Abs. 1 StPO zu, die zum Festhalten des Nutzers der Smartglasses berechtigen, wenn zu befürchten ist, dass dieser eine Straftat begangen hat. Ferner wird neben der Notwehr im Regelfall auch der Tatbestand einer rechtfertigenden Selbsthilfe gem. § 229 BGB erfüllt sein.

Zusammenfassend zeigt die Prüfung der sofortigen Abwehrmaßnahmen, dass die von Smartglasses ausgehende hohe Gefahr für das Allgemeine Persönlichkeitsrecht sich in dem starken und umfassenden Notwehrrecht widerspiegelt. Nutzer von Smartglasses müssen sich möglichst kooperativ verhalten und den Forderungen Betroffener Folge leisten. Weigern sie sich, müssen sie die Wegnahme oder Zerstörung der Smartglasses sowie körperliche Gewalt als auch etwaige Irrtümer der Betroffenen erdulden.

VI. Ergebnis der einfachgesetzlichen Prüfung

Da Smartglasses nicht schlechthin heimlichen Aufnahmen und dem Abhören von Menschen dienen, ist ihr Besitz zwar nicht generell gem. § 90 TKG verboten. Allerdings stellt ihre Nutzung im öffentlichen Raum eine Videoüberwachung i.S.d. § 6b BDSG dar, unabhängig davon, ob ihre Nutzer tatsächlich Aufnahmen Dritter erstellen. Aus diesem Grund ist die Nutzung von Smartglasses im öffentlichen Raum praktisch untersagt, außer in seltenen Ausnahmesituationen der Notwehr, bei medizinischer Indikation oder vorliegender Einwilligung Dritter. Werden mittels Smart-

glasses tatsächlich audiovisuelle Aufnahmen erstellt, können sie zudem bei Verletzung des höchstpersönlichen Lebensbereiches oder des nicht öffentlich gesprochenen Wortes die Straftatbestände der §§ 201, 201a StGB erfüllen. Im Fall der Verbreitung oder Zurschaustellung von Aufnahmen ohne Einwilligung Betroffener, wird wiederum der Straftatbestand der §§ 33, 22 KUG einschlägig. Neben den speziellen Regelungen wird das Allgemeine Persönlichkeitsrecht Betroffener zusätzlich als absolutes Recht gem. § 823 Abs. 1 BGB geschützt, welches vor der Herstellung von Aufnahmen, der Verletzung der Privatsphäre sowie der von Smartglasses ausgehenden Einschüchterungswirkung schützt.

Als Folge der Rechtsverstöße stehen Betroffenen Beseitigungs-, Unterlassungs- u.U. Schadensersatzansprüche sowie Herausgabe-, Vernichtungs- und Auskunftsansprüche zu, die sich auf zivilrechtliche Vorschriften der § 823 Abs. 1, 2 i.V.m. § 1004 BGB analog sowie §§ 242, 249 BGB und Schutzgesetzen der §§ 4 Abs. 1, 6b BDSG, 22 KUG, 201, 201a StGB, als auch speziellen Vorschriften des Datenschutzrechts (§§ 7, 6b Abs. 5, 34, 35 BDSG), des KUG (§§ 37 ff. KUG) sowie des Strafrechts stützen können (§§ 201a Abs. 5, 74 Abs. 2, 74a StGB). Da die Nutzung der Smartglasses für Betroffene intransparent ist und die Nutzer im Regelfall unbekannt, werden Betroffene ihre Ansprüche unmittelbar geltend machen und im Wege der Notwehr sofort durchsetzen dürfen. Nach § 38 Abs. 5 BDSG können zudem behördliche Maßnahmen und Untersagungsverbote sowie gem. § 43 Abs. 2, Abs. 3 BDSG Bußgelder in Höhe von bis zu 300.000 Euro verhängt werden. Ferner können Betroffene die Hilfe der Polizei zum Schutz ihrer Rechte in Anspruch nehmen.

Als Folge ist das Führen von Smartglasses im öffentlichen Raum praktisch unmöglich, ohne dabei Rechtsverstöße zu begehen oder sich den Ansprüchen Dritter ausgeliefert zu sehen. Alleine aufgrund der Auskunftsansprüche der Betroffenen gem. §§ 823, 242 BGB, 34 BDSG könnte die Nutzung von Smartglasses zu einem Spießrutenlauf werden, wenn jedermann im Erfassungsbereich der Smartglasses erfahren will, ob von ihm Aufnahmen erstellt worden sind.

Insgesamt ist als Ergebnis der einfachgesetzlichen Prüfung festzuhalten, dass der als Verletzung der Menschenwürde klassifizierte Einsatz von Smartglasses im öffentlichen Raum sich in einem umfassenden einfachgesetzlichen Verbot ihrer Nutzung widerspiegelt.

G INTERNATIONALER RECHTSRAHMEN

Der Schutz der Privatsphäre wird als ein elementares Menschenrecht verstanden, das Teil eines Wertsystems ist, welches die Würde und Gleichheit der Menschen sowie die Unverzichtbarkeit auf diese Rechte schützt.[1843] Ferner erstreckt sich der Schutz der Privatsphäre auch auf internationaler Ebene nicht nur auf den Schutz gegenüber dem Staat, sondern wirkt als eine negative und klassische Funktion der Menschenrechte, auch im Verhältnis zwischen Privatpersonen.[1844] Dementsprechend wurden auch im Rahmen dieser Untersuchung die maßgeblichen internationalen Regelungen berücksichtigt, soweit sie eine Auswirkung auf die nationale Rechtsordnung haben konnten.[1845] Die Übersicht der internationalen Rahmenbedingungen in diesem Kapitel dient vor allem als Grundlage für die Einschätzung, inwieweit die EU-Datenschutzgrundverordnung Einfluss auf das Ergebnis dieser Untersuchung haben wird.

I. Europäische Menschenrechtskonvention

Nach Art. 8 Abs. 1 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) hat jedermann ein Recht auf Achtung des Privat- und Familienlebens. Aus dieser Vorgabe werden insbesondere der Schutz von personenbezogenen Daten und der Schutz des Rechts am eigenen Bild sowohl in Fällen der Fotografie, als auch der Videoüberwachung abgeleitet.[1846] Insoweit steht dem auf Ebene eines einfachen Rechts stehenden Art. 8 Abs. 1 EMRK zwar eine weitreichende Schutzfunktion zu.[1847] Soweit es jedoch um den Schutz vor Überwachungs- und Anpassungseffekten videoüberwachter Personen geht, enthält die EMRK keine expliziten Vorgaben. Vielmehr lässt die bisherige Rechtsprechung des EGMR darauf schließen, dass die bloßen Einschüch-

---

[1843] *Hotter*, Privatsphäre, 2011, S. 155 ff.; *Weber*, How Does Privacy Change in the Age of the Internet, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 273 (277).

[1844] *Weber*, How Does Privacy Change in the Age of the Internet, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 273 (278).

[1845] Zum Anwendungsvorrang unionsrechtlicher Regelungen, *Lewinski*, DuD 2012, S. 564 (564 ff.).

[1846] EGMR, Urt. v. 12.7.2013 (63737/00), Reports 2003-IX Nr. 38http://hudoc.echr.coe.int/eng?i=001-61228 (7.11.2015); EGMR, Urt. v. 20.12.2005 (71611/01),http://hudoc.echr.coe.int/fre?i=001-71735 (7.11.2015); EGMR, Urt. v. 28.1.2003 (44647/98 Nr. 62), Slg. 03-Ihttp://hudoc.echr.coe.int/eng?i=001-60898 (7.11.2015); EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051; zur mittelbaren Drittwirkung, *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 203 ff.; *Nebel*, ZD 2015, S. 517 (520 f.).

[1847] Vgl. BVerfG, Beschl. v. 14.10.2004 (2 BvR 1481/04), BVerfGE 111, 307 (316 f.); BVerfG, Beschl. v. 26.3.1987 (2 BvR 589/79 u.a.), BVerfGE 74, 358 (370).

terungseffekte einer Videobeobachtung nicht zur Verletzung des Art. 8 Abs. 1 EMRK führen und lediglich eine durch systematische oder dauerhafte Videoaufzeichnung gekennzeichnete Videoüberwachung einen Eingriff in die Privatsphäre darstellt.[1848] Soweit die Nutzer von Smartglasses tatsächlich Aufzeichnungen vornehmen, die als Beobachtung zu qualifizieren sind, wird Art. 8 Abs. 1 EMRK einschlägig sein.[1849] Unklar ist jedoch, ob der im Rahmen dieser Untersuchung weit verstandene Begriff der Beobachtung ebenso dem Art. 8 Abs. 1 EMRK zugrunde gelegt wird oder in der potentiellen Möglichkeit mithilfe von Smartglasses jederzeit Dritte aufnehmen zu können, noch nicht als ein Eingriff betrachtet wird. Im Ergebnis wird Art. 8 Abs. 1 EMRK den Betroffenen daher einen mit nationalem Recht vergleichbaren, unter Umständen geringeren, aber keinen weiteren Schutz vor Smartglasses als das nationale Recht bieten.[1850]

II. Charta der Grundrechte der Europäischen Union

Die primärrechtliche Charta der Grundrechte der Europäischen Union (GRCh) enthält mit Art. 8 einen speziellen Schutz personenbezogener Daten (auch als "Datenschutzgrundrecht" bezeichnet).[1851] Darüber hinaus wird im Art. 7 GRCh die "Achtung des Privat- und Familienlebens" in einer dem Art. 8 Abs. 1 EMRK entsprechenden Formulierung geschützt, welche schon bereits zuvor dem EuGH als Quelle der Rechtserkenntnis diente.[1852] D.h. das Recht auf Privatsphäre ähnelt den, aus dem deutschen Kontext bekannten Fallgruppen des Allgemeinen Persönlichkeitsrechts in Form der Privatsphäre als räumlich und inhaltlich bestimmten Rückzugs-

---

[1848] EGMR, Urt. v. 12.7.2013 (63737/00), Reports 2003-IX Nr. 38http://hudoc.echr.coe.int/eng?i=001-61228 (7.11.2015); EGMR, Beschl. v. 27.11.1996 (28122/95),http://hudoc.echr.coe.int/eng?i=001-3402 (7.11.2015); EGMR, Beschl. v. 14.1.1998 (32200/96, 32201/96), http://hudoc.echr.coe.int/eng?i =001-88070 (7.11.2015).

[1849] EGMR, Urt. v. 28.1.2003 (44647/98 Nr. 62), Slg. 03-I http://hudoc.echr.coe.int/eng?i=001-60898 (7.11.2015).

[1850] So auch *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 103.

[1851] EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196); EuGH, Urt. v. 13.5.2014 (C-131/12), NJW 2014, 2257 (2258 ff.); EuGH, Urt. v. 8.4.2014 (C-293/12, C-594/12), NJW 2014, 2169 (2169 ff.); vgl. *Augsberg*, in: *Groeben/Schwarze/Hatje*, EU-Recht, Art. 8 GRC, Rn. 3 ff.; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 105 f.; *Nebel*, ZD 2015, S. 517 (521).

[1852] EuGH, Urt. v. 6.10.2015 (C-362/14), MMR 2015, 753 (754 ff.); EuGH, Urt. v. 29.1.2008 (C-275/06), EuZW 2008, 113 (116); EuGH, Urt. v. 6.11.2003 (C-101/01), EuR 2004, 291 (295 ff.); EuGH, Urt. v. 20.5.2003 (RS. C-465/00, C-138/01 u. C-139/01), EuR 2004, 276 (278 ff.); *Augsberg*, in: *Groeben/Schwarze/Hatje*, EU-Recht, Art. 7 GRC, Rn. 5; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 101.

bereichs, des Rechts am nichtöffentlich gesprochenen Wort und des Rechts am eigenen Bild.[1853]

Jedoch ist es wie bereits im Fall des Art. 8 Abs. 1 EMRK zumindest nicht eindeutig, ob den Art. 7 und 8 GRCh ein Schutz vor Überwachungs- und Anpassungseffekten unabhängig vom tatsächlich stattfindender Verarbeitung personenbezogener Daten zu entnehmen ist. Eine Datenverarbeitung kann z.B. fehlen, wenn Smartglasses lediglich getragen werden, um Informationen aus dem Internet abzurufen oder gelegentlich Schnappschüsse zu erstellen.[1854] Jedoch ist davon auszugehen, dass auch Einschüchterungseffekte durch die Charta der Grundrechte der Europäischen Union berücksichtigt werden müssen, wenn sie die selbstbestimmte Entfaltung Dritter im öffentlichen Raum gefährden. Dafür spricht, dass Art. 1 GRCh die Unantastbarkeit der Menschenwürde zumindest vom Wortlaut her, entsprechend der Formulierung des Art. 1 Abs. 1 GG, gewährleistet.[1855]

Allerdings ist Art. 1 GRCh nicht am Art. 1 Abs. 1 GG zu messen, sondern muss eine eigenständige Beurteilung erfahren, da insoweit die unionsrechtlichen Regelungen Vorrang vor dem nationalen Recht haben.[1856] Jedoch sind die von Smartglasses ausgehenden Überwachungseffekte entsprechend dem Untersuchungsergebnis in Quantität, Lückenlosigkeit und Invasivität derart hoch, dass sie eine große Gefahr für die Entfaltung der eigenen Individualität einzelner Menschen und den Fortbestand der demokratischen Meinungspluralität darstellen.[1857] Sowohl bei der Individualität, wie auch der Meinungspluralität handelt es sich entsprechend der Präambel der Charta der Grundrechte der Europäischen Union um unverzichtbare europäische Grundwerte.[1858]

Folglich würde die Nutzung von Smartglasses im öffentlichen Raum nicht nur im Fall der Verarbeitung personenbezogener Daten einen Verstoß gem. Art. 8 GrCh darstellen, sondern auch durch die Einschüchte-

---

[1853] *Augsberg*, in: *Groeben/Schwarze/Hatje*, EU-Recht, Art. 7 GRC, Rn. 5.

[1854] Vgl. B III. 6, S. 49.

[1855] Vgl. E II. 2. b) gg) (1), S. 124.

[1856] Mit der Solange II-Entscheidung erklärte das BVerfG, dass der Wesensgehalt des europäischen Grundschutzschutzes mit dem des GG vergleichbar ist und insoweit ein Rückgriff auf das GG nicht erforderlich ist, BVerfG, Beschl. v. 29.5.1974 (2 BvL 52/71), BVerfGE 37, 371 (278 ff.); damit wich das BVerfG von seiner in der Solange I-Entscheidung vertretenen Ansicht ab, vgl. BVerfG, Beschl. v. 22.10.1986 (2 BvR 197/83), BVerfGE 73, 339 (367 ff.); zum Rückgriff auf die Dogmatik des deutschen Verfassungsrechts, vgl. *Augsberg*, in: *Groeben/Schwarze/Hatje*, EU-Recht, Art. 1 GRC, Rn. 4; sowie *Lewinski*, DuD 2012, S. 564 (568).

[1857] Vgl. E V, S. 181.

[1858] *Augsberg*, in: *Groeben/Schwarze/Hatje*, EU-Recht, GRC Präambel, Rn. 6 f.

rungswirkung eine Verletzung des Art. 7 i.V.m. Art. 1 GRCh mit sich bringen. Zusammengefasst steht die Charta der Grundrechte der Europäischen Union ebenfalls der Nutzung von Smartglasses im öffentlichen Raum entgegen, wobei die Schutzwirkung mit dem nationalen verfassungsrechtlichen Schutz vergleichbar ist.

III. EU-Datenschutzrichtlinie 95/46/EG

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, kurz Datenschutzrichtlinie (EG-DSRL) dient auf sekundärrechtlicher Ebene der Herstellung eines einheitlichen unionsrechtlichen Datenschutzes durch Harmonisierung nationalrechtlicher Vorschriften.[1859] Die Vorgaben der EG-DSRL wurden während dieser Untersuchung beachtet und im Hinblick auf die Beurteilung einer ausschließlich persönlich-familiären Nutzung vertieft gewürdigt.[1860] Da die EG-DSRL den Umgang mit personenbezogenen Daten regelt, ist für die Nutzung von Smartglasses zumindest insoweit einschlägig, als personenbezogene Daten, insbesondere auch biometrischer Natur,[1861] tatsächlich verarbeitet werden.[1862] Dagegen werden Überwachungs- und Anpassungseffekte, die alleine aufgrund der Einschüchterungswirkung der Smartglasses entstehen, von der EG-DSRL nicht geregelt.[1863] Dementsprechend erreicht das normative deutsche Datenschutzniveau nicht nur die Vorgaben der EG-DSRL,[1864] sondern geht mit dem Tatbestand der Beobachtung im § 6b Abs. 1 BDSG über sie hinaus.[1865]

[1859] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 203 ff.; *Taeger/Schmidt*, in: *Taeger/Gabel*, BDSG, Einführung, Rn. 51 f.

[1860] Vgl. F II. 1. c) cc) (2), S. 195; zur Maßgeblichkeit der EG-DSRL für die Videoüberwachung, vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 205 ff.

[1861] Art. 29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP193, 00720/12/DE, 2012, S. 4.

[1862] Art. 29-Datenschutzgruppe, Working Document on the Processing of Personal Data by means of Video Surveillance, WP67, 11750/02/EN, 2002, S. 1 ff.; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 106 ff.

[1863] Vgl. *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 107.

[1864] Die EG-DSRL gebietet eine Vollharmonisierung, vgl. EuGH, Urt. v. 24.11.2011 (C-468/10 u. C-469/10), NZA 2011, 1409 (1410 f.); EuGH, Urt. v. 6.11.2003 (C-101/01), EuR 2004, 291 (303 f.).

[1865] *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 107.

IV. EU-Datenschutzgrundverordnung

Mit der "Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr", kurz Datenschutz-Grundverordnung (EU-DSGVO) als Sekundärrecht, soll gem. Art. 1 Abs. 1 EU-DSGVO eine einheitliche Gesetzesgrundlage für die Verarbeitung personenbezogener Daten in der Union geschaffen werden.

1. Umfang der Regelung der Videoüberwachung in der EU-DSGVO

Der Vorteil der Regelung der Videoüberwachung im § 6b BDSG bestand im Hinblick auf Smartglasses insoweit, als der Begriff der "Beobachtung" die gesamte Nutzung der jederzeit zur visuellen Aufzeichnung einsatzbereiten Smartglasses umfasste.[1866] Es fragt sich, ob die Datenverarbeitung als Anwendungsvoraussetzung i.S.d. des Art. 1 Abs. 1 EU-DSGVO, ebenso weit verstanden werden kann, ohne explizit den Tatbestand der Beobachtung zu erwähnen. D.h. es ist z.B. zu fragen, ob Smartglasses, die lediglich dazu getragen werden, um Informationen aus dem Internet zu beziehen oder gelegentlich Schnappschüsse zu erstellen, in den Anwendungsbereich der EU-Datenschutzgrundverordnung fallen würden, wie sie dem § 6b Abs. 1 BDSG, zumindest nach der im Rahmen dieser Untersuchung vertretenen Ansicht, unterfallen.[1867]

Dafür könnte zunächst sprechen, dass die Videoüberwachung in den Erwägungsgründen zur EU-Datenschutzgrundverordnung Anklang findet. Nach Erwägungsgrund 91 der EU-DSGVO bedarf die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, einer Datenschutz-Folgenabschätzung. Diese Regelung ähnelt, bis auf die Voraussetzung des großen Umfangs der Überwachung, der Legaldefinition der Videoüberwachung gem. § 6b Abs. 1 BDSG.[1868] Allerdings kann eine derart definierte weiträumige Überwachung auch nur die Fälle tatsächlicher Datenverarbeitung betreffen und muss nicht zwangsläufig bloße Einschüchterungseffekte umfassen. Dafür spricht auch, dass Art. 1 Abs. 1 EU-DSGVO nur "Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezoge-

---

1866 Vgl. F II. 1. d) aa), S. 204.

1867 Vgl. F II. 1. d) aa) (2), S. 205.

1868 Im Vorschlag der Europäischen Kommission vom 25. Januar 2012 (KOM(2012)0011) fand sich im 33 Nr. 2c EU-DSGVO-E zudem ein, dem § 6b Abs.1 BDSG entsprechender Klammerzusatz "(Videoüberwachung)", d.h. eine Legaldefinition der Videoüberwachung, Council of the European Union, Synopse zum Stand des Gesetzgebungsverfahrens der EU-DSGVO, 2012/0011 (COD), 2015, http://statewatch.org/news/2015/jul/eu-council-dp-reg-trilogue-10391-15.pdf (2.9.2015).

ner Daten" enthält und damit im Hinblick auf den Anwendungsbereich konzeptionelle Ähnlichkeit mit Art. 1 Abs. 1 der EG-DSRL aufweist. Dementsprechend finden sich in den Grundsätzen gem. Art. 5 EU-DSGVO und den Zulässigkeitstatbeständen gem. Art. 6 EU-DSGVO nur Regelungen mit eindeutigem Bezug zu personenbezogenen Daten.

Ausgehend von dieser Begrenzung ihres Anwendungsbereichs, würde die EU-Datenschutzgrundverordnung die Nutzung von Smartglasses entsprechend der EG-DSRL insoweit regeln, als eine Verarbeitung personenbezogener Daten tatsächlich stattfindet. Dagegen findet sich keine ausdrückliche Aufnahme einer Videoüberwachung i.S.d. § 6b Abs. 1 BDSG in die Anwendungs- oder Erlaubnistatbestände, d.h. auch keine ausdrückliche Berücksichtigung von Überwachungs- und Anpassungseffekten in dem Gesetzesvorschlag. Zudem ist angesichts des Umstandes, dass die Videoüberwachung nicht nur im deutschen § 6b BDSG, sondern auch in den Rechtsordnungen anderer Mitgliedsländern besonders geregelt wird,[1869] nicht davon auszugehen, dass der EU-Gesetzgeber sie unbeabsichtigt nicht in die EU-Datenschutzgrundverordnung aufgenommen hat. Folglich wird nur die Nutzung von Smartglasses erfasst, sofern sie tatsächlich mit der Erhebung von personenbezogenen Daten verbunden ist.[1870] D.h., sofern Smartglasses nur dazu verwendet werden, um Informationen zu empfangen oder gelegentlich Schnappschüsse zu erstellen, wird ihre Nutzung eher nicht von Regelungsbereich der EU-Datenschutzgrundverordnung erfasst.[1871] Allerdings ist zu bedenken, dass Smartglasses, zumindest entsprechend ihrer Bestimmung als eine Assistenztechnologie, die im Rahmen ihrer Unterstützungshandlungen die Umwelt des Nutzers visuell erfasst, im Regelfall personenbezogene Daten erheben sowie verarbeiten und somit sehr häufig dem Anwendungsbereich der DSGVO unterfallen werden.

2. Zulässigkeit der Videoüberwachung nach der EU-DSGVO

Soweit bei der Nutzung von Smartglasses Daten verarbeitet werden, wird entsprechend dem § 1 Abs. 2 Nr. 3 BDSG gem. Art. 2 Abs. 2 lit. c EU-DSGVO zu prüfen sein, ob die Nutzung zu persönlichen und familiären Zwecken erfolgt. Zwar enthält zumindest der Gesetzesentwurf des Rates der EU nicht mehr die Einschränkung einer "ausschließlichen" persönlichen und familiären Nutzung, jedoch kann diese Anwendungsvoraussetzung vor dem Hintergrund der Intensität der menschenunwürdi-

[1869] Art. 29-Datenschutzgruppe, Working Document on the Processing of Personal Data by means of Video Surveillance, WP67, 11750/02/EN, 2002, S. 8 ff.

[1870] Vgl. *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (241).

[1871] Vgl. F II. 1. d) aa) (2), S. 205.

gen Beeinträchtigung der Privatsphäre Dritter durch Smartglasses nicht anders, als im Rahmen dieser Untersuchung ausgelegt werden.[1872] Dementsprechend wird nicht nur die Nutzung von Smartglasses zu präventiven sowie repressiven Zwecken,[1873] sondern auch aus Gründen der Effizienz, Bequemlichkeit oder sonstigen privaten Vergnügens, aufgrund der Einschüchterungswirkung und damit einer menschenunwürdigen Überwachungswirkung, keine ausschließlich persönlichen und familiären Nutzung i.S.d. EU-Datenschutzgrundverordnung darstellen.

Auch im Hinblick auf die Zulässigkeitstatbestände ist keine Abweichung von dem Ergebnis dieser Untersuchung zu erwarten.[1874] Entsprechend dem Grundsatz des Verbots der Datenverarbeitung mit Erlaubnisvorbehalt,[1875] ist die Verarbeitung personenbezogener Daten gem. Art. 6 Abs. 1 lit. a EU-DSGVO nur mit einer unmissverständlichen Einwilligung gem. Art. 7 EU-DSGVO erlaubt oder zum Schutz lebensnotwendiger Interessen gem. Art. 6 Abs. 1 lit. d EU-DSGVO oder berechtigter Interessen gem. Art. 6 Abs. 1 lit. f EU-DSGVO, die jedoch die Grundrechte Betroffener überwiegen müssen, welche sich nach den Art. 1, 7 und 8 GRCh bestimmen werden.[1876] Folglich wird nur Nutzung von Smartglasses im öffentlichen Raum, wie auch i.R.d. § 6b BDSG, nur in seltenen und punktuellen Ausnahmefällen zulässig sein, wie z.B. zu medizinischen Zwecken oder in einer Notwehr-, bzw. notwehrähnliche Lage.[1877]

Des Weiteren bringt auch die EU-Datenschutzgrundverordnung dem BDSG entsprechende Transparenz-, Auskunfts- und Löschungspflichten (Art. 5 Abs. 1 lit. a, 12, 14, 15, 17) mit sich, die Betroffene den Nutzern von Smartglasses entgegenhalten und so das Tragen von Smartglasses im Alltag praktisch unmöglich machen könnten.[1878] Eine gesondert geregelte Kennzeichnungspflicht für Videoüberwachung im Sinne des § 6b Abs. 2 BDSG, ist in der EU-Datenschutzgrundverordnung jedoch nicht verankert.[1879]

[1872] Vgl. F II. 1. c) cc) (2), S. 195; so zumindest im Hinblick auf Videoüberwachung zu präventiven und repressiven Zwecken durch Privatspersonen, EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195 (196).

[1873] Ebenda.

[1874] Vgl. *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (242).

[1875] *Taeger/Schmidt*, in: *Taeger/Gabel*, BDSG, Einführung, Rn. 62.

[1876] Vgl. G II, S. 316.

[1877] Vgl. F II. 6, S. 245.

[1878] Vgl. F VI, S. 313

[1879] Die Vorgaben des § 6b Abs. 2 auf die Transparenzvorgaben der DSGVO übertragend, *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (243).

3. Kein Regelungsdefizit durch Aufhebung des § 6b BDSG

Da die EU-Datenschutzgrundverordnung die von Smartglasses ausgehende Einschüchterungswirkung in Fällen fehlenden Datenbezugs nicht regelt, stellt sich die Frage, ob hierdurch das gesetzliche Schutzniveau gesenkt wird oder gar eine Schutzlücke für Betroffene entsteht.

Zuerst ist jedoch zu beachten, dass eine derartige Schutzlücke nur entstünde, wenn § 6b Abs. 1 BDSG explizit aufgehoben werden würde. Ansonsten würde die Vorschrift von der EU-Datenschutzgrundverordnung insoweit nicht verdrängt werden, als sie Fälle der Videoüberwachung regelt, in denen keine personenbezogenen Daten i.S.d. EU-Datenschutzgrundverordnung verarbeitet werden.[1880]

Würde der § 6b Abs. 1 BDSG aufgehoben werden, müsste entsprechend den Ausführungen zur mittelbaren Schutzwirkung der Grundrechte beachtet werden, dass der Staat zur Schaffung eines rechtlichen Schutzniveaus verpflichtet ist, das den Grundrechtsschutz Betroffener gewährleistet.[1881] Hier hat der Staat insbesondere ein Untermaßverbot zu beachten, gegen das er verstoßen würde, wenn das Allgemeine Persönlichkeitsrecht Dritter vor den Nutzern von Smartglasses nicht hinreichend geschützt wäre. Zwar ist auch ein Übermaßverbot zu Gunsten der Nutzer von Smartglasses zu beachten, jedoch zeigten die bisherigen Ergebnisse der Untersuchung, dass § 6b Abs. 1 BDSG der verfassungsrechtlichen Gewichtung der widerstreitenden Interessen der Nutzer und der Betroffenen entspricht und die Nutzer von Smartglasses nicht unangemessen benachteiligt werden.[1882]

Aber auch im Hinblick auf den Schutz der Betroffenen wäre trotz der Aufhebung des § 6b Abs. 1 BDSG nicht davon auszugehen, dass der Staat dadurch seine primären Schutzpflichten unterschreiten würde. Die Prüfung des zivilrechtlichen Schutzes der Betroffenen zeigte vielmehr, dass diese sich auf § 823 Abs. 1 BGB berufen können, in dessen Rahmen das Allgemeine Persönlichkeitsrecht umfassend und lückenschließend geschützt wird.[1883] Insbesondere werden Betroffene auch vor der Einschüchterungswirkung von Smartglasses und den sich hieraus ergebenden Überwachungs- und Anpassungseffekten geschützt.[1884] Ihre Ansprüche auf Unterlassung und Beseitigung der Persönlichkeitsrechtsverstöße sowie Erteilung einer Auskunft über etwaige Datenerfassung, können die

---

[1880] Vgl. G IV. 1, S. 319; *Taeger/Schmidt*, in: *Taeger/Gabel*, BDSG, Einführung, Rn. 59.

[1881] Vgl. E I, S. 89.

[1882] Vgl. F II. 1, S. 187.

[1883] Vgl. F IV. 1, S. 264.

[1884] Vgl. F IV. 3. e), S. 277.

Betroffenen ferner unmittelbar selbst im Rahmen der Notwehr oder mit Hilfe von Gerichten durchsetzen.[1885] Durch die umfassende Judikatur kann auch von einer hinreichenden Bestimmtheit des Rechtsschutzes über § 823 Abs. 1 GG ausgegangen werden.[1886]

Im Ergebnis sind durch den Wegfall des § 6b BDSG keine Schutzlücken für Persönlichkeitsrechte der Betroffenen zu befürchten. Zwar läge eine ausdrückliche Regelung der Videoüberwachung außerhalb der Fälle der tatsächlichen Verarbeitung personenbezogener Daten innerhalb des gesetzgeberischen Spielraums. Jedoch wäre eine derartige Regelung nicht zwingend erforderlich. An dieser Stelle kann auf die bereits zur Einführung des § 6b BDSG kritisch geführte Diskussion zum Nutzen und Notwendigkeit der Regelung verwiesen werden.[1887] Im Ergebnis wurden der Vorschrift vielfach im Wesentlichen nur Vorteile einer regulatorischen Konzentration zugemessen, die jedoch lediglich bereits bestehende Regelungen wiederholte.[1888]

Ein praktischer Nachteil einer zergliederten Regelung der Videoüberwachung könnte sich ferner insoweit ergeben, als es je nach Fall unklar sein könnte, ob personenbezogene Daten erhoben wurden und die EU-Datenschutzgrundverordnung einschlägig ist oder mangels Datenbezug § 823 Abs. 1 BGB zur Anwendung kommt. Ein diesbezüglicher Nachteil wurde bisher mit dem Hinweis darauf abgelehnt, dass sowohl die Anwendung des § 6b BDSG, wie auch des § 823 Abs. 1 BGB im Fall der Videoüberwachung auf denselben, dem Allgemeinen Persönlichkeitsrecht entstammenden Grundsätzen fußen.[1889] Dies könnte sich jedoch mit der Geltung der EU-Datenschutzgrundverordnung ändern, die nach Maßgabe der Charta der Grundrechte der Europäischen Union anzuwenden ist, während für § 823 Abs. 1 BGB das GG maßgeblich bleibt. Doch erst die Zukunft wird zeigen, inwieweit die langjährige Rechtsprechung des Bundesverfassungsgerichts zur Privatsphäre und Persönlichkeitsrechten auch im Rahmen der Charta der Grundrechte der Europäischen Union einen Wi-

---

[1885] Vgl. F VI, S. 313; so auch im Hinblick auf Videoüberwachung *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 423 ff.

[1886] Ebenda, 443 f.

[1887] Vgl. hierzu die erschöpfende Darstellung ebenda, 449 ff.; resümierend vom Versagen im Hinblick auf die Zielrichtung der Eindämmung von Videoüberwachung sprechend, *Scholz*, in: *Simitis*, BDSG, § 6b Rn. 6.

[1888] Als Vorteil des § 6b BDSG, wird die Erschwerung der Zweckänderung i.R.d. Verarbeitung und Nutzung der durch Videoüberwachung erhobenen personenebezogenen Daten betrachtet, vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 481.

[1889] Ebenda, 483.

derhall findet.[1890] Ferner ist zu bemängeln, dass anders als im Rahmen der Verfassungsbeschwerde auf nationaler Ebene, nach der Erschöpfung des unionsrechtlichen Rechtsweges, kein direkter Rechtsbehelf wegen der Verletzung von Grundrechten aus der Charta der Grundrechte der Europäischen Union gegeben ist.[1891]

4. (Keine) Änderungen des Untersuchungsergebnisses durch den internationalen Rechtsrahmen

Die Übersicht internationaler Vorschriften zeigt, dass sie weder gegenwärtig noch in der Zukunft einen wesentlichen Einfluss auf die Ergebnisse dieser Untersuchung haben werden. Auch wenn die EU-Datenschutzgrundverordnung den Einsatz von Smartglasses nur dann regeln wird, wenn sie zur Verarbeitung personenbezogener Daten eingesetzt werden (was jedoch sehr häufig der Fall sein wird), werden für sich stehende Einschüchterungseffekte durch den Schutz des Allgemeinen Persönlichkeitsrechts im Rahmen des § 823 Abs. 1 BGB aufgefangen. Ferner wird die Nutzung von Smartglasses sowohl auf europäischer, wie auf nationaler Ebene solange untersagt bleiben, wie davon auszugehen ist, dass die von ihnen ausgehenden Überwachungs- und Anpassungseffekte die Selbstentfaltung Dritter sowie den Fortbestand der Meinungspluralität gefährden und damit einen Verstoß gegen die Menschenwürde aus Art. 1 GRCh und Art. 1 Abs. 1 GG darstellen.

[1890] Vgl. *Hornung*, ZD 2012, S. 99 (100); *Masing*, Ein Abschied von den Grundrechten, SZ, 2011, S. 10.

[1891] *Hornung*, ZD 2012, S. 99 (100); *Masing*, Ein Abschied von den Grundrechten, SZ, 2011, S. 10.

H ZUKUNFTSPROGNOSEN UND HANDLUNGSVORSCHLÄGE

Als Ergebnis der verfassungsrechtlichen, einfachgesetzlichen und unionsrechtlichen Untersuchung wurde festgestellt, dass der Einsatz von Smartglasses im öffentlichen Raum rechtlich unzulässig und damit praktisch unmöglich ist. Deren Nutzung stellt im Regelfall, und auch ohne dass tatsächliche Aufnahmen erstellt werden, eine nicht gerechtfertigte Videoüberwachung gem. § 6b BDSG und einen Verstoß gegen das Allgemeine Persönlichkeitsrecht gem. § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG dar.[1892] Der Grund liegt vor allem in der panoptischen Wirkung der Smartglasses, die aufgrund der Möglichkeit heimlicher audiovisueller Aufnahmen, sonstiger Datenerfassungen oder biometrischer Auswertungen auf Dritte einschüchternd wirken und deren autonome Selbstentfaltung verhindern können. Der Einsatz von Smartglasses kann so zu einem Verlust der Privatsphäre im öffentlichen Raum führen, wodurch die auf einer autonomen Selbstentfaltung basierende Menschenwürde und damit die Meinungspluralität als Grundlage einer demokratischen Gesellschaft gefährdet wären.[1893]

Allerdings kann die Untersuchung an dieser Stelle noch nicht beendet werden. Da ihr Ziel in der Erkennung, Bewertung und Beeinflussung der Veränderungskraft technischer Entwicklungen von Smartglasses liegt, müssen auch mögliche Entwicklungen in der Zukunft berücksichtigt werden.[1894] Dabei muss insbesondere die Kraft einer Entwicklung eingeschätzt werden, die eine Verbreitung von Smartglasses fordert und fördert. Anschließend muss beurteilt werden, inwieweit die bisherige Rechtslage fähig ist, dieser Entwicklung Stand zu halten und ob die Aufrechterhaltung des gegenwärtigen Privatsphärenkonzepts möglich und empfehlenswert ist. Erst auf Grundlage der Ergebnisse dieser Prüfung können Empfehlungen für rechtliche oder technische Maßnahmen zur Steuerung der Entwicklung der Smartglasses-Technologie abgegeben werden.

I. Prognose der technischen und gesellschaftlichen Entwicklung

Die weitere Entwicklung der Smartglasses-Technologie ist vor allem von den technischen und gesellschaftlichen Gegebenheiten abhängig. Gemeint

---

[1892] Vgl. F VI, S. 313.

[1893] Vgl. E V, S. 181.

[1894] Vgl. A III. 1, S. 6.

ist damit, dass ein Bedürfnis nach Smartglasses sich aus den Bedürfnissen des übrigen technischen Fortschritts als auch den Bedürfnissen der Menschen ergeben kann.[1895] Eine genaue Trennung dieser beiden Kräfte ist nicht möglich, da sie sich beide gegenseitig beeinflussen können.[1896] So können Technologien die Gesellschaft und herrschende Moral beeinflussen.[1897] Z.B. führte die Erfindung des Buchdrucks zu einem Anstieg der Aufklärung und das Aufkommen der Eisenbahn zu einer Lösung der Menschen aus örtlich-räumlichen Beschränkungen.[1898] Beide Technologien trugen ferner wesentlich dazu bei, dass der Mensch sich zunehmend als ein Individuum definierte.[1899]

Umgekehrt können die Bedürfnisse der Menschen wiederum die technische Entwicklung prägen.[1900] Oft sind Zwecke der Technik bei deren Entstehung nicht bekannt.[1901] Das Telefon wurde z.B. anfangs wie eine Art Radio benutzt und diente eher als Statussymbol.[1902] Es war nicht vorhersehbar, dass es ein Massenkommunikationsmittel wird.[1903] Ebenso wurde das Potenzial der Computertechnik in den 1970er Jahren noch nicht gesehen, und so ging man davon aus, dass Computer nur als zentrale Großrechner dienen werden.[1904] Auch beim Internet wusste man nicht, wie sich diese Technik entwickeln würde, und es scheint, als ob das Ende dieser Entwicklung immer noch nicht abzusehen ist.[1905] Das bedeutet, dass der technologische Fortschritt trotz Steuerungsmöglichkeiten kaum vorherzusehen ist.[1906] Das technische Gerät ist daher eher als eine Handlungsmöglichkeit zu verstehen und sein Zweck ist durch die Konstruktion eher negativ als positiv vorgegeben.[1907]

1895 *Agar*, Constant Touch, 2004, S. 171 ff.

1896 Ebenda; *Ellul*, The Technological Society, 1967, S. 112.

1897 *Mutschler*, Die Gottmaschine, 1998, S. 18 ff.

1898 Vgl. *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 215 f.; *Mutschler*, Die Gottmaschine, 1998, S. 183; *Radkau*, Technik in Deutschland, 2008, S. 347 f.; *Seemann*, Das neue Spiel, 2014, S. 17.

1899 Vgl. *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 215 f.; *Mutschler*, Die Gottmaschine, 1998, S. 183; vgl. D I, S: 73.

1900 Vgl. *Radkau*, Technik in Deutschland, 2008, S. 68

1901 *Mutschler*, Die Gottmaschine, 1998, S. 17.

1902 *Radkau*, Technik in Deutschland, 2008, S. 407.

1903 *Mutschler*, Die Gottmaschine, 1998, S. 19.

1904 *Radkau*, Technik in Deutschland, 2008, S. 406.

1905 Tim Berners-Lee ist der Ansicht, dass alleine die menschliche Vorstellungskraft die Grenzen des Internets bestimmt, *Ghos*, Warning sounded on web's future, BBC, http://news.bbc.co.uk/2/hi/technology/7613201.stm (13.2.2015).

1906 *Mutschler*, Die Gottmaschine, 1998, S. 20.

1907 Ebenda, 161.

1. Eigendynamik des technischen Fortschritts

Um die Dynamik der Smartglasses-Technologie beurteilen zu können, muss die gesamte technologische Entwicklung betrachtet werden. Denn Smartglasses sind lediglich eine Begleiterscheinung des gegenwärtigen technologischen Fortschritts.[1908] Diesem Fortschritt wird eine Eigenbewegung, mit dem Ziel, die Vollkommenheit zu erreichen und jede schwächere Kraft auf dem Weg dorthin zu verdrängen, zugerechnet.[1909] Generell werden Technologien nach verbreiteter Sichtweise als Kräfte betrachtet, die von der Natur aus darauf bedacht sind, sich beständig expansiv sowie invasiv auszuweiten.[1910] Diese Ausbreitung der Technik ist also nicht nur durch ihre Weite oder Tiefe, sondern auch durch ihre Dichte in der Gesellschaft gekennzeichnet, wodurch die Technologie zunehmend zu einem Teil der menschlichen Umwelt wird.[1911]

Technologie ist zudem konvergent (bzw. katalytisch), was bedeutet, dass Technologien weitere technische Innovationen hervorbringen, die zur Kombination vorhandener Technologien oder neuen Anwendungsbereichen für vorhandene Technologien führen.[1912] Ein Beispiel hierfür ist die Ausbreitung der Computertechnologie, welche anfangs in Form zentraler Rechner existierte und nunmehr praktisch jeden Bereich des Alltags- und Berufslebens von Menschen durchdringt.[1913] Mit dem Voranschreiten des Konzepts eines Ubiquitous Computing, das sich bereits heute mit der Omnipräsenz von Smartphones, Vernetzung von Menschen in sozialen Netzwerken und einem „Internet der Dinge“ ausdrückt, etabliert sich eine Kette von gegenseitigen technologischen Abhängigkeiten, die den Bestand der Informationstechnologien sichert.[1914]

Jedoch sichert der technologische Fortschritt nicht lediglich dessen status quo, sondern sorgt für seine weitere Entwicklung. Mit neuen Technologien entsteht ein „technologisches Dequilibrium“, womit ein systemati-

---

1908 Vgl. A IV. 1, S. 9.; vgl. B IV. 2, S. 51.

1909 *Ellul*, The Technological Society, 1967, S. 85.

1910 *Allmer*, Critical Internet Surveillance Studies, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 124 (127); "Technological development proceeds steadily from what it has already transformed and used up toward that which is still untouched", *Winner*, The Whale and the Reactor, 1989, S. 174.

1911 "[…] a generalized environment for human existence", *Winner*, Autonomous Technology, 1978, S. 210.

1912 *Hill*, Not So Fast: Thinking Twice About Technology, 2013, Chap. 7, Nr. 2; *Radkau*, Technik in Deutschland, 2008, S. 150.

1913 Vgl. *Radkau*, Technik in Deutschland, 2008, S. 350.

1914 *Hill*, Not So Fast: Thinking Twice About Technology, 2013, Chap. 7, Nr. 2; "[…] one must provide not only the means, but also the entire set of means to the means", *Winner*, Autonomous Technology, 1978, S. 100 f.

sches Ungleichgewicht im technischen, wirtschaftlichen und sozialen Bereich gemeint ist, das den Bedarf nach weiteren Technologien schafft.[1915] So sind viele technische Entwicklungen für sich unvollkommen und bedürfen weiterer Nachfolgetechnologien, um ihr volles Potenzial zu entfalten. Z.B. wurde das Telegraphennetz parallel zur Entwicklung der Eisenbahn entwickelt, um den Schienenverkehr zu kontrollieren und Unfälle auf eingleisigen Strecken zu vermeiden.[1916] Ebenso setzte sich die Kraftfahrzeugtechnik erst mit der erforderlichen Entwicklung von Straßen, Kraftstoffversorgung und Straßenverkehrsregelungen durch.[1917] Auch das Konzept der Augmented Reality existiert seit über 50 Jahren und wird erst mit der Entwicklung von Smartglasses in großem Umfang einsetzbar.[1918] D.h., die Technik vermag es selbst, den Bedarf nach weiterer Technik zu schaffen.[1919]

Statt einer Stagnation der technischen Entwicklung ist daher vielmehr eine Beschleunigung ihres Fortschritts zu erwarten.[1920] Als deren Treibmittel wird insbesondere ein durch rapide Zunahme der Qualität und der Quantität von Daten ausgelöster Anstieg des theoretischen Wissens gesehen.[1921] Damit ist gemeint, dass die Bandbreite an einzelnen Informationen, welche die Grundlage weiterer Überlegungen, Überzeugungen und Innovationen jeglicher Art theoretisch bilden können, zunimmt.[1922] Während frühere Innovationen auf Zufällen und Ausprobieren basierten, werden sie zunehmend durch gezielte Entwicklungen abgelöst, die in theoretischen Prozessen auf Tauglichkeit überprüft werden, bevor sie den Weg in die praktische Umsetzung finden.[1923] Zusätzlich können heutzutage theoretisch alle Menschen auf eine weite Bandbreite von generellem und universell in allen Berufs- und Lebenslagen anwendbarem Einzelwissen aus allen Disziplinen zugreifen, das früher nur den Experten oder be-

---

1915 *Ellul*, The Technological Society, 1967, S. 112.

1916 *Radkau*, Technik in Deutschland, 2008, S. 154.

1917 *Hill*, Not So Fast: Thinking Twice About Technology, 2013, Chap. 7, Nr. 3.

1918 Vgl. B, S. 23.

1919 *Radkau*, Technik in Deutschland, 2008, S. 150.

1920 *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 26 ff.

1921 *Bell*, The Coming of Post-Industrial Society, 1976, S. xxxix f.; *Mathiesen*, Preface, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. xv (xvi); *Webster*, Theories of the Information Society, 2014, S. 34 f.

1922 *Bell*, The Coming of Post-Industrial Society, 1976, S. 212 f.; auf dieser Grundlage wird als Bezeichnung der heutigen Gesellschaft der Begriff einer "Wissensgesellschaft" vorgeschlagen, *Stehr/Böhme*, The Knowledge Society, 1986, S. 7 ff.; *Webster*, Theories of the Information Society, 2014, S. 34 f.

1923 *Webster*, Theories of the Information Society, 2014, S. 62 f.

stimmten Menschen zugänglich war.[1924] Diese Entwicklung ist reziprok, was bedeutet, dass mit der Zunahme einer informationellen Ordnung, also strukturierten Vielfalt des Wissens, das theoretische Wissen selbst exponentiell ansteigt.[1925]

Infolge der technologischen Eigendynamik verändert sich die Beziehung des Menschen zu technischen Entwicklungen.[1926] In der Vergangenheit konnten technische Artefakte vorwiegend als Werkzeuge, also externe Hilfsmittel, betrachtet werden.[1927] Die ubiquitäre Verbreitung der Informations- und Telekommunikationstechnologien kann jedoch zunehmend als ein homogenes System betrachtet werden, in dem Menschen als Systemkomponenten existieren.[1928] Eine Trennung zwischen einer „echten Realität" in einer physischen Welt und der künstlich erzeugten „virtuellen Realität" kann immer weniger aufrechterhalten werden. Es handelt sich vielmehr um verschiedene Dimensionen einer einheitlichen Realität der Menschen.

Ein alltäglicher Ausdruck dieser Entwicklung sind z.B. Geschäftslokale, die neben der physischen auch über eine virtuelle Präsenz verfügen.[1929] Es handelt sich hierbei um Ansammlungen von ortsbezogenen Informationen, wie z.B. Abbildungen von Produkten oder Angeboten auf Unternehmenswebsites, Erfahrungsberichten von Kunden auf Bewertungsplattfor-

---

1924 *Bell*, The Coming of Post-Industrial Society, 1976, S. xxxix f.; *Webster*, Theories of the Information Society, 2014, S. 35.

1925 *Kurzweil*, Homo Sapiens, 2000, S. 57 f.; *Stonier*, Information und die innere Struktur des Universums, 1991, S. 25; der Gedanke beruht auf der Theorie von Norbert Wiener, der den den Grad der Ordnung eines [Wissens]Systems als Maßstab seines Informationsgehaltes ansieht (und die Entropie als das Gegenteil des Informationsgehaltes), *Wiener*, Kybernetik, 1963, S. 38.

1926 *Mutschler*, Die Gottmaschine, 1998, S. 17 ff.

1927 Doch bereits die früheren Technologien werden (zumindest entsprechend der Vorstellung vom Menschen als "Mängelwesen"), als "Organersatz, Organentlastung oder Organüberbietung" betrachtet, vgl. *Gehlen*, Die Seele im technischen Zeitalter, 2004, S. 151; *Gehlen*, Anthropologische Forschung, 1984, S. 93; *Mutschler*, Die Gottmaschine, 1998, S. 12.

1928 "As I see it, technology has built the house in which we all live. The house is continually being extended and remodelled. More and more of human life takes place within its walls, so that today there is hardly any human activity that does not occur within this house. All are affected by the design of the house, by the division of its space, by the location of its doors and walls. Compared to people in earlier times, we rarely have a chance to live outside this house", *Franklin*, The Real World of Technology, 1999, S. 1 f.

1929 *Albrechtslund*, Socializing the City, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 187 (194 f.); von einem "Outernet" sprechend, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 1 f.;*Schwenke*, DuD 2015, S. 161 (162).

men.[1930] Vor Ort können Besucher das physische Betreten der Ortes zugleich physisch durch sog. „Check-ins" auf virtuellen Plattformen abbilden.[1931] Sie können unter Zuhilfenahme von ortspräsenten Beacon-Technologien mit dem Ort zugleich physisch wie psychisch interagieren, zu gesuchten Produkten gelotst werden und dank den „Augmented Reality"-Anwendungen ihres Mobiltelefons virtuelle Einblendungen zu ihnen erhalten.[1932] Die so um virtuelle „Bedeutungsebenen" erweiterten und rekonfigurierten Orte werden als „Mixed Places", bzw. „Augmented Locations" bezeichnet.[1933] Die koexistierenden physischen und virtuellen Realitäten eines Ortes werden jedoch erst mithilfe der Augmented-Reality-Funktionen von Smartglasses zu einer einheitlich wahrnehmbaren und effektiv nutzbaren Realität verschmolzen werden können.[1934]

Abschließend betrachtet ist daher damit zu rechnen, dass die technologische Entwicklung einen zunehmenden Bedarf nach der Nutzung von Smartglasses schaffen wird. Um sich in ein virtuell geprägtes Realitätssystem integrieren zu können, werden Menschen auf eine maschinelle Kommunikation angewiesen sein. Die maschinelle Kommunikation unterscheidet sich wiederum insoweit von der menschlichen Sensorik und Sprache, als Erkenntnisse und Informationen entsprechend dem technologischen Gedanken der Effektivität maschinell kodifiziert werden müssen, um effizient verbreitet und verwendet werden zu können.[1935] Insoweit kann im Kontrast zu einer Augmented Reality (also einer erweiterten Realitätswahrnehmung) davon gesprochen werden, dass Menschen ohne Smartglasses nur über eine beschränkte Realitätswahrnehmung verfügen werden.

1930 *Albrechtslund*, Socializing the City, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 187 (194 f.).

1931 *Reißmann*, App-Umbau, Spiegel Online, http://www.spiegel.de/netzwelt/apps/app-umbau-foursquare-ist-jetzt-wie-yelp-a-982653.html (5.1.2015).

1932 *Levine*, Move over, iBeacons -- here come mesh beacons, VentureBeat, http://ven turebeat.com/2014/12/06/move-over-ibeacons-here-come-mesh-beacons/ (13.1.2015); *Reißmann*, App-Umbau, Spiegel Online, http://www.spiegel.de/netzwelt/a pps/app-umbau-foursquare-ist-jetzt-wie-yelp-a-982653.html (5.1.2015); *Schart/Tschanz*, Augmented Reality, 2015, S. 113 f.; *Venzke-Caprarese*, DuD 2014, S. 839.

1933 *Albrechtslund*, Socializing the City, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 187 (194).

1934 Vgl. B III. 5, S. 42; vgl. *Schwenke*, DuD 2015, S. 161 (162).

1935 *Bell*, The Coming of Post-Industrial Society, 1976, S. xxxix; *Webster*, Theories of the Information Society, 2014, S. 60 ff.

2. Smartglasses als effiziente Mittel der Selbstbehauptung in der Informationsgesellschaft

Die technologische Entwicklung spiegelt sich in dem gesellschaftlichen Wandel der Informationsgesellschaft wider, welcher als ein Übergang von einer modernen zu einer postmodernen Gesellschaft definiert wird.[1936] Es ist damit zu rechnen, dass die soziale und wirtschaftliche Bedeutung von Informationen zu radikalen gesellschaftlichen Änderungen führen wird, welche die durch das industrielle Zeitalter geprägte moderne Gesellschaft reformieren werden.[1937]

Bereits die Entwicklung der Moderne zeichnete sich durch eine Herauslösung von Menschen aus örtlich-sozialen Strukturen heraus, band sie jedoch weiterhin an kulturell und naturell vorgegebene und oft als Wahrheitsmonopole institutionalisierte Strukturen wie Nationalstaaten, Klassen oder Männer- und Frauenrollen.[1938] Die weltweite Vernetzung von Menschen und die Zunahme an Wissen transformieren diese Gesellschaftsformen und führen zur Entstehung andersartiger „Identitäten, Akteure, Politikstile, Beziehungsmuster und Verantwortungsformen."[1939] Das Leben der Menschen kann immer freier gestaltet werden, soziale Arrangements werden nicht vorgegeben oder können hinterfragt und nach Bedarf aus einer Vielzahl zur Wahl stehender Optionen konstruiert werden.[1940] Wirtschaftlich betrachtet wirken sich Informationen strukturell durch steigende Anforderungen an wettbewerbsrelevante Flexibilität und Anpassungsfähigkeit von Marktteilnehmern aus.[1941] Der wirtschaftliche Wettbewerb in einer Informationsgesellschaft ist globaler, allumfassender, interdependenter, d.h. wesentlich komplizierter zu handhaben.[1942]

Der Preis der postmodernen Flexibilisierung und Herauslösung aus vorgegebenen Strukturen ist eine zunehmende Unsicherheit, was die Wahl der richtigen Lebensoptionen und der Selbstbehauptung ohne vorgegebe-

---

[1936] M.w.N. *Ketzer*, Securitas ex Machina, 2005, S. 11 ff.; m.w.N. *Webster*, Theories of the Information Society, 2014, S. 366 ff.; vgl. A IV. 1, S. 9.

[1937] *Beck/Giddens/Lash*, Vorwort, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. (9 ff.); *Giddens*, Leben in einer posttraditionellen Gesellschaft, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 113 (114 ff.); *Webster*, Theories of the Information Society, 2014, S. 277.

[1938] *Beck*, Das Zeitalter der Nebenfolgen und die Politisierung der Moderne, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 19 (22).

[1939] Ebenda, 23.

[1940] Ebenda, 142; *Ketzer*, Securitas ex Machina, 2005, S. 11.

[1941] Vor dem Hintergrund unternehmerischen Wirkens, *Castells*, Contemporary Sociology 2000, Vol. 29, Nr. 5, p. 693 (695).

[1942] *Giddens*, Leben in einer posttraditionellen Gesellschaft, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 113 (176).

ne Lebensstrukturen angeht.[1943] Das Bedürfnis, die richtigen Entscheidungen zu treffen, führt zum einen zu dem Paradoxon, dass obwohl Menschen ihr Leben mehr bestimmen können als je zuvor, sie unsicher und mit Ängsten behaftet sind, ob ihre Entscheidungen richtig waren.[1944] Dazu gesellt sich eine Auflösung von Wahrheitsmonopolen durch offene und kontroverse Diskussionen, die Menschen ferner das Vertrauen in Expertenwissen nimmt.[1945] Hinzu kommt, dass die meisten Risiken menschengemacht sind und nicht mehr der Natur oder transzendentalen Mächten zugeschrieben werden können.[1946] Ferner führt die Zunahme an Umfang und Geschwindigkeit der Informationsflüsse dazu, dass Menschen örtlich weit entfernte Gefahren und Risiken unmittelbar auf sich beziehen.[1947] Die Folge all dieser Informationalisierung ist, dass Menschen sich aufgrund der Informationszunahme einem „askriptiven Gefährdungsschicksal“ ausgesetzt fühlen, d.h., ihre Risikowahrnehmung oft höher ist als tatsächlich bestehende Gefahren.[1948]

Um die Loslösung aus traditionellen Strukturen zu kompensieren, suchen Menschen Schutz in „abstrakten Systemen“, denen sie vertrauen und ihnen die Bestimmung ihres Alltags überlassen können.[1949] Abstrakte Systeme sind z.B. staatliche, wirtschaftliche und soziale Institutionen, aber auch virtuelle Netzwerke im Internet, die das Gefühl einer sozialen Sicherheit bieten.[1950] Innerhalb einer immer komplexer werdenden Gesellschaft bieten solche sich teils überlappenden abstrakten Systeme eine künstlich erzeugte Ordnung, die relativ „autark, funktional und rational zu durchschauen“ ist.[1951] Diese „Realitätsinseln“ üben auf Menschen eine psychische Sogwirkung aus, da in ihnen Durchschaubarkeit statt Chaos

---

1943 Beck fasst diese gesellschaftliche Entwicklung unter dem Begriff einer "Risikogesellschaft" zusammen, *Beck*, Risikogesellschaft. Auf dem Weg in eine andere Moderne, 1986, S. 61 f.

1944 *Webster*, Theories of the Information Society, 2014, S. 281

1945 Z.B. wenn es um globale Erwärmung geht, *Beck*, Risikogesellschaft. Auf dem Weg in eine andere Moderne, 1986, S. 256 ff.

1946 Ebenda, 300.

1947 Ebenda, 61 f.

1948 Ebenda, 8.

1949 *Giddens*, Leben in einer posttraditionellen Gesellschaft, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 113 (165 f.).

1950 Ebenda, 166 f.; nach Ansicht des Philosophen Han, verändert sich das Internet vor allem wegen der sozialen Netzwerke zu einer unkritischen "Wohlfühlzone", in der ein absoluter Nahraum zwischen den Mitgliedern herrscht und ein Außen eliminiert wird, so dass die Mitglieder nur Ausschnitte einer Welt präsentiert erhalten, die ihnen gefällt und zugleich ein öffentliches sowie kritisches Bewusstsein eliminiert, S. *Han*, Transparenzgesellschaft, 2012, S. 58 f.

1951 *Mutschler*, Die Gottmaschine, 1998, S. 14 f.

herrschen, Eindeutigkeit statt Mehrdeutigkeit, Funktionalität statt Dysfunktionalität und Berechnung statt Unvorhersehbarkeit.[1952]

Die abstrakten Systeme sind jedoch häufig durch wirtschaftliche und staatliche Interessen geprägt, welche die Entwicklung zu einer postmodernen „Risikogesellschaft" fördern.[1953] Das Bedürfnis nach Risikovermeidung ist wirtschaftlich verwertbar, z.B. durch Sicherheitsdienstleistungen und -produkte (zu welchen Smartglasses in dieser Hinsicht gerechnet werden können).[1954] Angst ist zudem beeinflussbar und, anders als z.B. der Hunger potentieller Konsumenten, unlimitiert befriedigbar, wodurch sie entsprechend der kapitalistischen Logik zu einer unerschöpflichen wirtschaftlichen Ressource wird.[1955] Eine von Angst angetriebene Gesellschaft ist ferner ein Ausdruck des „leviathanischen" Machtstrebens des Staates.[1956] Auch der Staat formiert die Gesellschaft zunehmend nicht durch Ordnung und Vertrauen, sondern durch Schaffung von Angst und Misstrauen.[1957] Ein Anzeichen hierfür ist der Generalverdacht, der durch die Überwachungsmaßnahmen in der Gesellschaft implementiert wird.[1958] Die Folge ist ein Auseinandertreiben der Individuen und damit eine Stärkung der Herrschaft des Staates.[1959] D.h., eine Angstgesellschaft, die sich ihrer Privatsphäre begibt, liegt im Interesse des staatlichen Machtanspruchs.[1960]

Zusammenfassend setzen die postmodernen gesellschaftlichen Systeme also einen höheren Grad an Reflexion und Wissen voraus, damit Menschen aus der Vielzahl der ihnen zur Verfügung stehenden Optionen die für sie passenden wählen und damit das gefühlte Lebensrisiko minimieren können.[1961] Zudem wird die Fähigkeit zum Umgang mit Informationen in einer durch Informationen als Wirtschaftsfaktoren geprägten Gesellschaft zu einem wesentlichen Kriterium, das über das wirtschaftliche Fortkom-

---

1952 Ebenda, 15.

1953 *Beck*, Risikogesellschaft. Auf dem Weg in eine andere Moderne, 1986, S. 61 f.

1954 Laut Beck ist für die Bedürfnisschaffung eine "Risikokosmetik" wesentlich, bei der Risiken "symptomhaft und symbolisch" durch Folgenbeseitigung, statt präventiv durch Beseitigung von Risikoquellen bewältigt werden, Ebenda, 74 f.

1955 Beck spricht von einem "Faß ohne Boden", Ebenda, 30.

1956 *Sofsky*, Verteidigung des Privaten, 2007, S. 23 ff.

1957 Vgl. *Ketzer*, Securitas ex Machina, 2005, S. 176; *Sofsky*, Verteidigung des Privaten, 2007, S. 27.

1958 *Fuchs u.a.*, Introduction, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 1 (10 f.); *Klein*, The Shock Doctrine, 2008, S. 302; *Sofsky*, Verteidigung des Privaten, 2007, S. 27.

1959 *Sofsky*, Verteidigung des Privaten, 2007, S. 27.

1960 Ebenda, 28.

1961 *Giddens*, Modernity and Self-Identity, 1991, S. 18 ff.

men der Gesellschaftsmitglieder entscheidet.[1962] Der Sicherheitsbedarf von Menschen wird also durch eine auf Informationen basierende tatsächliche Risikokontrolle oder zumindest das Gefühl der Kontrolle gemindert.[1963] Das bedeutet wiederum, dass bei Gesellschaftsmitgliedern das individuelle Bedürfnis nach möglichst umfassender Informationsbasis mit der Komplexität der sozial-wirtschaftlichen Zusammenhänge steigt.[1964] Folglich steigt bei Menschen das Bedürfnis, das ihnen zur Verfügung stehende Informationspotenzial effektiv zu nutzen, um z.B. persönliche Risiken zu vermieden oder wirtschaftliche Gelegenheiten zu schaffen, indem das unzuverlässige, aber sehr wichtige Element des Vertrauens durch objektive Erkenntnisse ersetzt wird.[1965] Damit wird das Bedürfnis von Menschen nach Beständigkeit und innerer Ausgeglichenheit in einer zunehmend komplexer werdenden Welt befriedigt.[1966] Die Schwierigkeit besteht jedoch in der geistigen Limitierung der Menschen, deren Aufmerksamkeitskapazitäten nur eine beschränkte Verarbeitung von Informationen erlauben.[1967] Es wird daher immer wichtiger, der „Explosion von Informationen" durch eine maschinell unterstützte Kontextualisierung und Relevanzbestimmung, in Echtzeit Herr werden zu können. [1968]

Im Ergebnis zeichnet auch die Prognose der gesellschaftlichen Entwicklung das Bild einer „realen Virtualität", d.h. der physischen Existenz von

---

[1962] *Arning/Moos*, ZD 2014, S. 242; *Becker/Becker*, MMR 2012, S. 351 (351 f.); *Bell*, Post-Industrial Society, in: *Webster/Blom*, The Information Society Reader, 2004, S. 86 (87); *Fuchs u.a.*, Introduction, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 1 (1 ff.); *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 141 ff.; *Webster*, Theories of the Information Society, 2014, S. 122, 176 f.

[1963] *Legnaro*, Leviathan 1997, S. 271; *Lindenberg/Schmidt-Semisch*, Kriminologisches Journal 1995, S. 2 (3); *Hotter*, Privatsphäre, 2011, S. 88 f.; vgl. die Definition von Macht in A IV. 7, S. 16.

[1964] *Hotter*, Privatsphäre, 2011, S. 89.

[1965] *Hill*, 2014, Vol. DÖV, S. 213 (213 f.); *Han*, Transparenzgesellschaft, 2012, S. 78 f.; bei Vertrauen handelt es sich um eine subjektive Überzeugung vom Eintritt bestimmter Ereignisse in der Zukunft, die sich durch einen Zustand zwischen Wissen und Nichtwissen definiert, vgl. *Luhmann*, Vertrauen, 2000, S. 12.

[1966] Vgl. *Langheinrich*, Personal Privacy in Ubiquitous Computing, 2005, S. 55 ff.; *Sofsky*, Verteidigung des Privaten, 2007, S. 107 ff.

[1967] *Simon*, Designing Organizations for an Information-Rich World, in: *Greenberger/University/Institution*, Computers, communications, and the public interest, 1971, S. 37 (40).

[1968] *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 39 f.; *Schart/Tschanz*, Augmented Reality, 2015, S. 63 f.; *Schiller*, Columbia Journal of World Business 1983, Vol. 18, Nr. 1, p. 86 (88); *Simon*, Designing Organizations for an Information-Rich World, in: *Greenberger/University/Institution*, Computers, communications, and the public interest, 1971, S. 37 (40); *Sofsky*, Verteidigung des Privaten, 2007, S. 15; *Webster*, Theories of the Information Society, 2014, S. 149; vgl. BIV.1, S. 50.

Menschen innerhalb virtueller Netzwerke, die selbst von den Beschränkungen der physischen Welt und traditionellen örtlich-sozialen Strukturen unabhängig sind.[1969] Der Preis der Netzwerkzugehörigkeit besteht u.a. darin, sich deren Logik, Sprache und Schnittstellen, also der virtuellen Kommunikationsstruktur, anzupassen.[1970] Folglich zeigt neben der technischen Prognose auch der gesellschaftliche Blick in die Zukunft, dass Smartglasses als effiziente Schnittstellen zur Kommunikation innerhalb einer durch virtuelle Dimensionen bestimmten Realität ihren Nutzern immense Vorteile zur Selbstbehauptung in einer Informationsgesellschaft verschaffen werden.

3. Anstieg der Lust an Selbstdarstellung und Beobachtung Dritter

Ein weiteres Argument für den gesellschaftlichen Bedarf nach der Nutzung von Smartglasses kann in der Zunahme der Lust an der Information über andere Menschen, als auch an der Selbstdarstellung gesehen werden. Betrachtet man die mit der technologischen Entwicklung einhergehenden Veränderungen im Umgang mit Bildrechten Dritter, wird deutlich, dass die Zahl unerlaubter Veröffentlichung und Verbreitung von Bildnissen zugenommen hat.[1971] Neben der Präsenz der Smartphones und mobilem Internet trägt auch die im Internet herrschende Ökonomie der Aufmerksamkeit zur Zunahme der Bildpublikationen bei. Der Begriff der Aufmerksamkeitsökonomie beschreibt zugleich den Drang der Menschen nach medialer Wahrnehmung, als auch dessen wirtschaftliches Potenzi-

---

1969 Castells definiert diese neue gesellschaftliche Lebensumgebung als einen "Raum der Ströme" (englisch "Space of Flows"), der einen "Raum der Orte" ablöst und in dem die Ströme ein Ausdruck von Prozessen sind, die das wirtschaftliche, politische und soziale Leben beherrschen, *Castells*, Das Informationszeitalter, Bd.1, 2001, S. 374, 431 ff.; *Castells*, Contemporary Sociology 2000, Vol. 29, Nr. 5, p. 693 (695 f.); *Giddens*, Leben in einer posttraditionellen Gesellschaft, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 113 (166 f.); *Giddens*, Modernity and Self-Identity, 1991, S. 16 ff.; *Sofsky*, Verteidigung des Privaten, 2007, S. 20.

1970 *Castells*, Das Informationszeitalter, Bd.1, 2001, S. 374.

1971 Mit Hinweis auf "ubiquitäre Verbreitungsmöglichkeiten", *Golla/Herbort*, GRUR 2015, S. 648; Heckmann spricht von Rücksichtslosigkeit beim Umgang mit Daten Dritter, *Heckmann*, K&R 2011, S. 770 ff.; *Hotter*, Privatsphäre, 2011, S. 117 f.; *Kister*, Die Epoche der Augenzeugen, SZ, http://www.sueddeutsche.de/digital/internet-und-gesellschaft-epoche-der-augenzeugen-1.2274559 (26.7.2015); *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (40); *Leffler*, Cyber-Bullying, 2012, S. 26; *Moglen*, Privacy under attack: the NSA files revealed new threats to democracy, The Guardian, http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threats-democracy (10.6.2014).

al.[1972] Dieses Potenzial machen sich z.B. Anbieter sozialer Plattformen zunutze, indem sie Nutzer animieren, Inhalte zu publizieren, die wiederum andere Nutzer zum Besuch der Plattform anregen, und aus dem Besucheranstieg wirtschaftliche Vorteile ziehen können.[1973] Da Bilder den Menschen eine weitaus höhere Aufmerksamkeit gewährleisten als bloße Texte, helfen sie dabei, die eigene Sichtbarkeit in sozialen Netzwerken zu stärken.[1974]

In derartigem Wissensbedürfnis der Menschen wird zum Teil eine als „regelrechte Sensationsgier" bezeichnete Paarung aus Voyeurismus und Exhibitionismus, die einen Schlüsselpunkt der gegenwärtigen Gesellschaft darstellt, gesehen.[1975] Diese Zunahme der „individualisierten Öffentlichkeit" durch die Sorglosigkeit im Umgang mit eigenen Daten im Internet als auch die Rücksichtslosigkeit im Umgang mit den Daten Dritter[1976] führen nach vielen Ansichten zu einer Enttabuisierung und Potenzierung des exhibitionistischen und voyeuristischen Verhaltens.[1977] Als Folge lässt diese Beobachtungskultur die Überwachung anderer Menschen als eine kulturell akzeptable Art der sozialen Ordnung, Verwaltung und Kontrolle

---

1972 Vgl. *Beller*, The Cinematic Mode of Production: Attention Economy and the Society of the Spectacle, 2012, S. 4 ff.; *Goldhaber*, Die Aufmerksamkeits-Ökonomie und das Netz, Telepolis, http://www.heise.de/tp/artikel/6/6195/1.html (28.7.2015); *Hickethier*, Medien - Aufmerksamkeit, in: *Hickethier/Bleicher*, Aufmerksamkeit, Medien und Ökonomie, 2002, S. 5 (xi ff.); *Lanham*, The Economics of Attention, 2006, S. xi ff.; *Sofsky*, Verteidigung des Privaten, 2007, S. 15 f.

1973 *Andrejevic*, Exploitation in the Data Mine, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 71 (74 ff.); *Fuchs*, Critique of the Political Economy of Web 2.0 Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 31 (52 ff.); *Zwick/Bonsu/Darmody*, Journal of Consumer Culture 2008, Vol. 8, Nr. 2, p. 163 (186).

1974 Da Fotografien eine höhere Interaktionsrate (z.B. durch Kommentare anderer Nutzer) erreichen, werden deren Urheber von dem Algorithmus des Netzwerks als für andere Nutzer relevanter und interessanter eingestuft, was sie wiederum dazu bewegen kann, häufiger Fotografien zu veröffentlichen, Photos Cluttering Your Facebook Feed?, e-Marketer, http://www.emarketer.com/Article/Photos-Cluttering-Your-Facebook-Feed-Herersquos-Why/1010777 (26.7.2015).

1975 *Hotter*, Privatsphäre, 2011, S. 117 ff.; "[…] mediated watching has become a key fea ture of contemporary societies, sometimes to an obsessive degree", *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (40).

1976 Vgl. *Golla/Herbort*, GRUR 2015, S. 648; *Heckmann*, K&R 2011, S. 770 (773).

1977 *Hotter*, Privatsphäre, 2011, S. 117; als Bezeichnung für diese Art. virtuellen Voyeurismus und Exhibitionismus wird auch der sonst im sexuellen Bereich verortete und von Sigmund Freud eingeführte Begriff "Scopophilia" ("Schaulust") verwendet, d.h. die Lust am Sehen, Zusehen, aber auch beobachtet werden, *Kosut*, Encyclopedia of Gender in Media, 2012, S. 321.

erscheinen.[1978] Hieraus ergebe sich eine sich selbst verstärkende Feedbackschleife, denn die Zunahme von Möglichkeiten der Informationswahrnehmung wird parallel von dem Wunsch, diese Möglichkeiten in Anspruch zu nehmen, begleitet.[1979]

4. Zweifel an der Privatsphäre als Hemmnis des technologischen Fortschritts

Die Voraussage einer technologischen und gesellschaftlichen Fortschrittsdynamik, welche die Verbreitung von Smartglasses unterstützen wird, scheint in einem diametralen Gegensatz zum Privatsphärenbedürfnis der Menschen zu stehen. Daher ist zu fragen, ob die geschilderten Entwicklungen realistisch sind oder doch an Grenzen der gesellschaftlichen Akzeptanz stoßen werden.

Die bisherigen Erkenntnisse zu gesellschaftlichen Vorbehalten gegenüber privatsphärenbeeinträchtigenden Technologien lassen zwar zuerst eine Skepsis gegenüber Smartglasses erwarten, sprechen jedoch eher dafür, dass Smartglasses sich trotz der Angst vor Verlust der Privatsphäre durchsetzen werden. Ein derart widersprüchliches Verhalten, das als „Privacy Paradoxon" bezeichnet wird, wurde bereits anhand des Nutzungsverhaltens von Internetdiensten beobachtet.[1980] Obwohl sich Menschen wegen Datenschutzskandalen oder Berichten über Zugriffe auf ihre Daten durch Geheimdienste sorgen, schränken sie die Nutzung der Internetdienste nicht ein.

Die Ursache für das „Privacy Paradoxon" wird vor allem darin vermutet, dass Menschen es nicht vermögen, die Tragweite ihrer Entscheidungen zu überblicken.[1981] Hierzu trägt im Wesentlichen der Unterschied zwischen der Unmittelbarkeit der Wahrnehmung und Auswirkung von Vorteilen gegenüber den Nachteilen bei.[1982] Die Vorteile der Informationstechnolo-

---

[1978] *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (49).

[1979] "The more that can be seen, the more we want to see. If the techniques are available, the will is there for deeper mining of the data", Ebenda; *Sofsky*, Verteidigung des Privaten, 2007, S. 15 f.

[1980] *Barnes*, First Monday 2006, Vol. 11, Nr. 9, http://firstmonday.org/article/view/1394/1312 (3.10.2014); vgl. *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (41); *Seemann*, Die Privatsphären-Falle, ZEIT ONLINE, http://www.zeit.de/digital/datenschutz/2013-10/privatsphaere-ueberwachung-nsa-seemann (3.11.2015); *Tufekci*, Bulletin of Science, Technology & Society 2008, Vol. 28, Nr. 1, p. 20.

[1981] Vgl. *Taddicken*, Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 255 (258).

[1982] *Lyon*, 9/11, Synopticon, and Scopophilia, in: *Ericson/Haggerty/Wall*, The New Politics of Surveillance and Visibility, 2006, S. 35 (41).

gien, wie die ortsunabhängige Kommunikation mit anderen Menschen und die Bequemlichkeit, werden sofort und unmittelbar wahrgenommen, während die Nachteile der Privatsphärenverluste abstrakt und fernliegend erscheinen.[1983]

Ob das Privacy Paradoxon sich gleichermaßen bei Smartglasses auswirken wird, kann mangels empirischer Erkenntnisse allenfalls gemutmaßt werden. Dagegen spricht, dass Smartglasses anders als die Überwachung im Internet oder mittels traditioneller Videoüberwachung nicht aus dem Hintergrund agieren, sondern direkt präsent sind und ein Unwohlsein verbreiten (sog „function creep“).[1984] Aber auch die Nutzer der Smartglasses könnten um die eigene Privatsphäre fürchten, wenn Dritte auf ihren „Blick auf die Welt“ und damit intimste Bereiche ihres Lebens zugreifen könnten.[1985]

Auf der anderen Seite muss in Betracht gezogen werden, dass sich das Privacy Paradoxon durch eine schleichende Entwicklung kennzeichnet. D.h., Menschen haben sich langsam an die neuen Technologien sowie deren Vorteile gewöhnt und daher den Verlust ihrer Privatsphäre nicht wahrgenommen.[1986] Auch bei Smartglasses ist eine ähnliche Entwicklung zu vermuten. Nach den in sozialer Hinsicht negativen Erfahrungen mit Google Glass[1987] ist zunächst nur mit deren Einsatz im nicht öffentlichen Privat- und Berufsbereich zu rechnen.[1988] Allerdings werden Smartglasses so zunehmend Eingang in den Alltag von Menschen finden können, der oft keine scharfen Grenzen zwischen öffentlichen und nicht öffentlichen Bereichen aufweist. Z.B. kann von einem privaten Garten aus der öffentliche Raum einer vorbeiführenden Straße mittels Smartglasses beobachtet werden. Auch wird mit wenig Verständnis bei einem Träger von Smart-

---

1983 Ebenda; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 15, 25; *Sofsky*, Verteidigung des Privaten, 2007, S. 13 f.

1984 Vgl. F V. 1, S. 290; *Hotter*, Privatsphäre, 2011, S. 132.

1985 *Schwenke*, K&R 2013, S. 685 (691).

1986 Diese Entwicklung wird häufig mit der Metapher eines Frosches versinnbildlicht, der zwar aus einem kochenden Wasser springen, wenn man ihn hineinwerfen würde, es aber nicht merkt, wenn er langsam gekocht wird und so das Schicksal erduldet, vgl. *Schaar*, Das Ende der Privatsphäre, 2007, S. 15.

1987 Vgl. C II. 3, S. 68.

1988 So zielen aktuelle Modellentwicklungen auf diese Bereiche ab, vgl. Google Glass „Enterprise Edition“ is foldable, more water resistant, rugged for the workplace, 9to5Google, http://9to5google.com/2015/07/21/google-glass-enterprise-edition-is-foldable-water-resistant-rugged-for-the-workplace/(14.9.2015); Windows 10 und «HoloLens», sueddeutsche.de, http://www.sueddeutsche.de/news/wirtschaft/computer-windows-10-und-hololens-microsoft-will-wieder-cool-werden-dpa.urn-newsml-dpa-com-20090101-150122-99-04014 (14.2.2015); Not quite Google Glass, Engadget, http://www.engadget.com/2014/10/04/epson-moverio-bt-200/(19.12.2014).

glasses zu rechnen sein, der das Gerät beim Verlassen des Büros absetzen muss, obwohl er sich mitten in einer via Smartglasses geführten Konversation befindet. Es ist also nicht fernliegend, dass diese Inselnutzungen von Smartglasses immer weiter zusammenwachsen werden, bis Smartglasses ähnlich wie Smartphones zu einem Alltagsutensil werden.[1989] Zudem haben bereits Mobiltelefone und das Internet gezeigt, wie eine Technologie das Leben der Menschen so durchdringen kann, dass sie nicht beliebig und ohne Weiteres „abgeschaltet" werden kann. Das gilt erst recht für Smartglasses, deren Ziel die nahtlose Eingliederung in den Alltag von Menschen ist.[1990]

Ferner ist bei den künftigen Modellen von Smartglasses mit einer fortschreitenden Miniaturisierung und Unauffälligkeit bis hin zu einer möglichen Unterbringung in Kontaktlinsen oder retinalen Implantaten zu rechnen.[1991] Als Folge könnte die Angst Dritter vor Smartglasses ebenso zu einem abstrakten und hinnehmbaren Gefühl werden, wie die Angst vor der Videoüberwachung oder bei der Nutzung von Internetdiensten.[1992]

5. Prognose einer unaufhaltbaren Verbreitung von Smartglasses

Die Einschätzungen zur Entwicklung und Verbreitung von Smartglasses sind insoweit mit Vorsicht zu betrachten, als sie auf gegenwärtigem Kenntnisstand basieren sowie aus Erkenntnissen zu anderen Technologien interpoliert werden. Von diesem Standpunkt aus lassen jedoch sowohl der technologische Expansionsdrang als auch die Bedürfnisse der Mitglieder einer Informationsgesellschaft auf einen hohen Bedarf nach Smartglasses als effiziente Zugangspunkte zur virtuellen Dimension der menschlichen Existenz schließen.[1993]

Dabei darf nicht vergessen werden, dass auch die Vorteile des Internets angesichts der Nachteile zuerst skeptisch beäugt wurden, bevor sie zu einem essentiellen Bestandteil in fast allen menschlichen Lebensbereichen wurden. Vor allem das Marktpotenzial von Smartglasses könnte ihnen

---

1989 Vgl. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 23 ff.

1990 Vgl. B I, S. 24.

1991 Vgl. B II. 1, S. 27.

1992 Vgl. E IV. 1. g) bb), S. 155.

1993 38 Prozent der Deutschen können sich vorstellen, Datenbrillen zu nutzen (Umfrage von 1014 Bundesbürgerm ab 14 Jahren), Großes Interesse an den Funktionen von Smart Glasses, BITKOM, https://www.bitkom.org/Presse/Presseinformation/Grosses-Interesse-an-den-Funktionen-von-Smart-Glasses.html (14.11.2015); *Hofer*, Zukunft der IT, http://www.handelsblatt.com/unternehmen/it-medien/zukunft-der-it-das-ende-der-smartphones-naht/12370284.html (14.11.2015).

eine ähnlich rasante Verbreitung bescheren, mit deren Beginn laut den gegenwärtigen Prognosen in den Jahren 2020 bis 2025 zu rechnen ist.[1994]

II. Normative und technische Handlungsvorschläge

Das Ergebnis der bisherigen Untersuchung führt zu einem scheinbar unauflöslichen Dilemma. Auf der einen Seite wurde festgestellt, dass die Verbreitung von Smartglasses im öffentlichen Raum mit hoher Wahrscheinlichkeit zu einem "Verlust der Privatsphäre" führen wird. Auf der anderen Seite deuten die technologischen und gesellschaftlichen Prognosen auf eine unaufhaltbare Expansion von Smartglasses hin.

1. Wandel zu einer durch Zufriedenheit und Sicherheit definierten Gesellschaft

Eine Lösung dieses Spannungsverhältnisses zwischen dem Schutz der gesellschaftlichen Grundwerte und dem Fortschrittsdrang wäre eine „Flucht nach vorne“, die in der Aufgabe des Konzeptes der negativen Privatsphäre zugunsten einer transparenten Gesellschaft läge. Doch wie bereits im Rahmen der verfassungsrechtlichen Prüfung untersucht, bietet das Konzept einer transparenten Gesellschaft keine hinreichende Sicherheit für den Schutz der Individualität der Gesellschaftsmitglieder sowie der Meinungspluralität.[1995] Ebenso reicht der Schutz einer virtuell, d.h. positiv erzeugten, Privatsphäre, nicht an das Schutzniveau einer negativen Privatsphäre heran.[1996]

Mitunter wird auch diskutiert, ob in der Postmoderne eine Werteverschiebung zugunsten einer utilitaristischen Gesellschaft stattfinden wird, in der Menschen innerhalb vordefinierter Rahmenparameter unter optimalem Ausschluss der Risikofaktoren ein geordnetes, sicheres und produktives Leben führen könnten.[1997] Dies würde eine Ablösung der frei-

---

[1994] Gartner’s 2015 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business, Gartner, http://www.gartner.com/newsroom/id/3114217 (18.8.2015); *Mehler-Bicher/Reiß/Steiger*, Augmented Reality, 2011, S. 5, 126 f.; ähnliche Entwicklung sieht auch der Gründer von Facebook, Marc Zuckerberg, voraus, *Ferenstein*, Zuckerberg’s 3 predictions for what social networks will look like in 10 years, VentureBeat, http://venturebeat.com/2015/01/14/zuckerbergs-3-predictions-for-what-social-networks-will-look-like-in-10-years/(22.8.2015); *Müller-Jung*, Virtuelle Realität - ein Selbstversuch Die Maske, die die Welt bedeutet, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/feuilleton/oculus-rift-verschmelzen-mit-der-virtuellen-welt-13096319.html (14.8.2014); *Preuß*, Augmented Reality, 2014, S. 1; *Tonnis*, Augmented Reality, 2010, S. 168.

[1995] Vgl. E IV. 2. c) aa), S. 175.

[1996] Vgl. E IV. 2. c) bb), S. 178.

[1997] *Dienel*, Geleitwort zur deutschen Ausgabe, in: *Erving*, Verhalten in sozialen Situationen, 1971, S. 7 (8 f.); *Hotter*, Privatsphäre, 2011, S. 94.

heitlichen Werte durch die Vorzüge der Sicherheit und des Wohlstands bedeuten. Dabei gälte die Grundformel des Utilitarismus, nach der diejenige Handlung bzw. Handlungsregel im sittlichen bzw. moralischen Sinne gut bzw. richtig ist, deren Folgen für das Wohlergehen aller von der Handlung Betroffenen optimal sind.[1998] D.h., die Handlung wird ethisch nach dem Nützlichkeitsprinzip bewertet.[1999] Es wird also weniger die Freiheit als die Zufriedenheit in den Vordergrund der Lebensmaxime gestellt.[2000]

Dieses gesellschaftliche Paradigma der Nützlichkeit entspricht damit der kapitalistischen Logik, welche aus virtuell gelebten Gesellschaftsformen sowie den mit diesen verbundenen Gütern und Leistungen Gewinne ziehen kann, wie bereits heutzutage Konzerne wie Google, Facebook oder Amazon zeigen.[2001] In einer solchen Gesellschaft wird die Entwicklung des Menschen zu einem „homo oeconomicus", also zu wirtschaftlicher Effizienz, prädestiniert.[2002] Dazu soll vor allem die Eingliederung des Menschen in funktionelle und formalisierte Maschinenkommunikation dienen.[2003]

Die Maxime der Nützlichkeit fügt sich jedoch auch in die prognostizierte synoptische Gesellschaft, in der Menschen unter ständiger Überwachung anderer Menschen sowie staatlicher oder wirtschaftlicher Institutionen stehen und so im Hinblick auf die Wirtschaftlichkeit und Sicherheit optimiert werden.[2004] Als Ausgleich erhält das Individuum gesellschaftliche Anerkennung als Genugtuung, die es die eigene Unfreiheit vergessen lässt.[2005] Die Bedürfnisse nach Zufriedenheit und Glücksgefühl, wie sie durch autonome Lebensgestaltung entstehen, werden nach diesen Vorstellungen durch künstlich geschaffene Wahlmöglichkeiten und virtuelle

---

1998 *Kley*, Teleologische und deontologische Ethik, in: *Mastronardi*, Das Recht im Spannungsfeld utilitaristischer und deontologischer Ethik, 2004, S. 55; *Mill*, Utilitarismus, 2009, S. 12.

1999 Die Kriterien der Nützlichkeit sind je nach Betrachtung sehr unterschiedlich, sollen jedoch nicht Gegenstand dieser Untersuchung sein, vgl. *Honecker*, Einführung in die theologische Ethik, 2002, S. 185.

2000 Vgl. *Webster*, Theories of the Information Society, 2014, S. 318.

2001 Vgl. *Hotter*, Privatsphäre, 2011, S. 129 f.; *Schiller*, Columbia Journal of World Business 1983, Vol. 18, Nr. 1, p. 86 (88); *Webster*, Theories of the Information Society, 2014, S. 183.

2002 *Hotter*, Privatsphäre, 2011, S. 145; dabei wird durchaus eine Zunahme des Wohlstands beobachtet, der wiederum neue Bedürfnisse weckt, die zur Bildung neuer Beschäftigungsfelder im Dienstleistungssektor führen, *Bell*, The Coming of Post-Industrial Society, 1976, S. XV ff.

2003 *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (109).

2004 Vgl. E IV. 2. c) aa), S. 175.

2005 *Hotter*, Privatsphäre, 2011, S. 94.

Simulationen befriedigt.[2006] Zu diesen gehören z.B. die individuellen Konsummöglichkeiten, wie sie in der Produktindividualisierung liegen können.[2007]

In einer derartigen Gesellschaft scheint das orwellsche Konzept eines großen Bruders überholt, da es von einer zentralen panoptischen Überwachung ausgeht, jedoch die komplexen synoptischen Überwachungsstrukturen sowie die Diversität der teilnehmenden Akteure, insbesondere der Wirtschaft, außer Acht lässt.[2008] Passender erscheint die Dystopie von Aldous Huxleys „Schöne neue Welt", in der ein aus Arbeit und Konsum bestehendes System seinen Teilnehmern mit einer Droge ein dauerhaftes Glücksgefühl vermittelt.[2009] Dies scheint eher der modernen Gesellschaft zu entsprechen, deren Teilnehmer in routinierte Alltagsprozesse eingegliedert werden, deren Handlungsabläufe den einzelnen Individuen zunehmend weniger zur Disposition stehen.[2010] Dabei besteht ferner die Gefahr, dass die Persönlichkeit der durch äußere Reize überfluteten Menschen durch die äußere Einwirkung deformiert wird und sich vom Idealbild ihrer autonomen Prägung entfernt.[2011]

Es kann an dieser Stelle nicht abschließend beantwortet werden, ob dieses nur interdisziplinär erfassbare gesellschaftliche Konzept der regulierten Zufriedenheit und Sicherheit erstrebenswert ist. Die bisherigen Erkenntnisse dieser Untersuchung zeigen jedoch, dass eine synoptische Lebenswelt, in der Menschen lediglich eine virtuell vorgegebene Privatsphäre zugestanden wird, abzulehnen ist.[2012] In deren Folge passt sich das Individuum sonst den mehrheitlichen, innerhalb der jeweiligen Systeme existierenden, Ansichten an und verinnerlicht die kollektive Meinung als Maßstab des eignen zweckorientierten Handelns, ohne dies zugleich als Zwang oder Beengung der Identität zu empfinden.[2013] Denn ein Konformist zeichnet sich durch einen starren Gedankenrahmen aus, der ihn daran hindert, die Beschädigung seiner Denkfähigkeit zu bemer-

---

2006 *Andrejevic*, Exploitation in the Data Mine, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 71 (75); *Hotter*, Privatsphäre, 2011, S. 94, 128.

2007 Vgl. *Hotter*, Privatsphäre, 2011, S. 148 ff.; *Webster*, Theories of the Information Society, 2014, S. 103, 190.

2008 *Hotter*, Privatsphäre, 2011, S. 101.

2009 Ebenda; Thomas Petri, zitiert in: *Büschemann*, Datenschutz, SZ, http://www.sueddeutsche.de/digital/datenschutz-digitaler-sisyphos-1.2653568 (19.9.2015).

2010 *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (111).

2011 *Sofsky*, Verteidigung des Privaten, 2007, S. 126.

2012 Vgl. E IV. 2. c) aa), S. 175.

2013 *Dienel*, Geleitwort zur deutschen Ausgabe, in: *Erving*, Verhalten in sozialen Situationen, 1971, S. 7 (8 f.); *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 100.

ken.[2014] Diese Entwicklung wird durch die Schaffung von Konsumbedürfnissen unterstützt, die eine Sucht hervorrufen, welche Menschen die Möglichkeit nimmt, „über sich selbst Regie" zu führen.[2015] Etwaige psychische Spannungen, die aus der Abweichung der individuellen Bedürfnisse und Vorstellungen entstehen, werden dafür verdrängt.[2016] D.h., auch wenn Menschen sich scheinbar den neuen Gegebenheiten anpassen, ist es wahrscheinlich, dass es sich hierbei nicht um einen autonomen Vorgang, sondern um eine erzwungene Anpassung zur Beseitigung kognitiver Dissonanzen handelt.[2017] Die Anpassung wird hierbei nicht als Zwang oder Beengung empfunden, sondern schafft im Gegenteil ein Gefühl der Sicherheit, eines Lebenssinnes und einer inneren Balance in der schnelllebigen Risikogesellschaft.[2018]

Jedoch vermag eine Gesellschaft, die nicht auf autonomen Entscheidungen ihrer Mitglieder fußt, etwaige Kurswechsel oder Fehler ihrer Entwicklung nicht zu korrigieren.[2019] In der Quintessenz ist das Ziel der Privatsphäre, den gesellschaftlichen Fortschritt zu sichern und Sackgassen der menschlichen Entwicklung zu verhindern. Die menschliche Entwicklung soll sich auch in Richtungen entwickeln können, die nicht vorgegeben sind, und Zielen folgen, die vielleicht noch gefunden werden müssen.[2020] Aus diesem Grund ist es weiterhin zu empfehlen, an dem Konzept einer negativen Privatsphäre festzuhalten, zumindest solange keine nachweislich adäquaten Mittel zum Schutz der Autonomie einzelner Mitglieder der Gesellschaft zur Verfügung stehen.

Folglich ist die Aufgabe des Konzepts einer negativen Privatsphäre zugunsten einer alleine auf regulierte Zufriedenheit und Sicherheit bedachten Gesellschaft keine empfehlenswerte Lösung.

2014 *Sofsky*, Verteidigung des Privaten, 2007, S. 129 f.

2015 Ebenda, 130; vgl. *Rihaczek*, DuD 2015, S. 141; vgl. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 23.

2016 *Dienel*, Geleitwort zur deutschen Ausgabe, in: *Erving*, Verhalten in sozialen Situationen, 1971, S. 7 (9).

2017 Vgl. zu kognitiver Anpassung E IV. 2. c) aa), S. 175; *Beck*, Das Zeitalter der Nebenfolgen und die Politisierung der Moderne, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 19 (74); *Dienel*, Geleitwort zur deutschen Ausgabe, in: *Erving*, Verhalten in sozialen Situationen, 1971, S. 7 (9).

2018 *Dienel*, Geleitwort zur deutschen Ausgabe, in: *Erving*, Verhalten in sozialen Situationen, 1971, S. 7 (9).

2019 Vgl. DII.2, S. 81.

2020 Vgl. *Giddens*, Leben in einer posttraditionellen Gesellschaft, in: *Beck/Giddens/Lash*, Reflexive Modernisierung: Eine Kontroverse, 1996, S. 113 (143 f.); *Hill*, Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 106 (111); *Hotter*, Privatsphäre, 2011, S. 147.

2. Normative Maßnahmen

Eine für sich stehende normative Herangehensweise zur Auflösung des Spannungsverhältnisses zwischen der Notwendigkeit einer Privatsphäre und der Nutzung von Smartglasses im öffentlichen Raum verspricht wenig Aussicht auf Erfolg. Zum einen machen bereits die bestehenden Gesetze das Tragen von Smartglasses im öffentlichen Raum bis auf wenige Fälle der Einwilligung, medizinischen Indikation oder in Notwehr- bzw. notwehrähnlicher Lage praktisch unmöglich.[2021] D.h., eine Verschärfung des gesetzlichen Schutzstandards ist nicht erforderlich. Ein Verbot von Smartglasses im Generellen ist jedoch ebenfalls abzulehnen, da die Geräte aufgrund ihrer Nützlichkeit und der Möglichkeit rechtskonformer Nutzung, z.B. im räumlich-privaten Bereich, nicht schlechthin schädlich sind.[2022] Allenfalls wäre an die Beachtung der staatlichen Pflicht zur Durchsetzung der persönlichkeitsschützenden Gesetze zu denken, wenn Behörden z.B. Anzeigen der Bürger nicht beachten oder Polizeibeamte keine Soforthilfe gegen Nutzer von Smartglasses leisten würden.[2023]

Auf der anderen Seite ist eine Einschränkung des bisherigen gesetzlichen Rahmens nicht zu empfehlen, da hierdurch der Schutz der Privatsphäre nicht gewährleistet wäre. Eine derartige Einschränkung ist aber auch nicht notwendig, da die Ausnahme rein privat-familiärer Nutzung gem. § 1 Abs. 2 Nr. 3 BDSG aus dem Regelungsbereich des BDSG bereits einen Raum für eine zulässige private Nutzung von Smartglasses lässt. Ebenso kann im Rahmen des Allgemeinen Persönlichkeitsrechts die Interessenabwägung ergeben, dass Smartglasses nicht die Interessen am Schutz der Privatsphäre beeinträchtigen. Beide Fälle setzen jedoch vor allem voraus, dass Smartglasses ihre Einschüchterungswirkung verlieren und Dritte nicht zur Anpassung ihres Verhaltens aufgrund der Befürchtung möglicher Aufnahmen bewegen.

Es wird also darauf ankommen, dass Menschen in den Schutz ihrer Privatsphäre trotz der Präsenz von Smartglasses im öffentlichen Raum vertrauen können. Ein solcher Schutz kann jedoch aufgrund der beschränkten Kontroll- und Durchsetzungsmöglichkeiten gesetzlicher Verbote nicht alleine mit normativen Mitteln geschaffen werden. So zeigen andere als nützlich und zugleich als gefährlich eingestufte Werkzeuge, dass eine Gefahr gezügelt werden kann, was jedoch häufig ein Zusammenspiel zwischen den technischen und den normativen Mitteln erfordert. Ein Beispiel hierfür sind z.B. Kraftfahrzeuge, deren Gefährdungspotenzial durch ein breites Spektrum an technischen und rechtlichen Maßnahmen

[2021] Vgl. F VI, S. 313.

[2022] Vgl. F I. 3, S. 186.

[2023] Vgl. F V. 4. a) bb) (3) (b), S. 301.

gebannt wird, und die verbleibenden Risiken angesichts ihrer Nützlichkeit hingenommen werden.[2024]

3. Technische Maßnahmen

Gerade Smartglasses machen es deutlich, dass Persönlichkeitsrechte vor allem durch die sie bedrohende Technologie geschützt werden müssen, da das Gesetz zu reaktiv ist, um den rasanten technischen Innovationen beizukommen.[2025] Die Lösung ist daher in einer präventiven System- und Gerätegestaltung zu suchen, die den Persönlichkeitsrechtsschutz bereits im Vorfeld etwaiger Verstöße gewährleistet.[2026] Diese Herangehensweise ist gesetzlich in dem Prinzip der Datenvermeidung und Datensparsamkeit verankert, das sich im § 3a BDSG wiederfindet,[2027] im Erforderlichkeitsprinzip des Art. 6 Abs. 1 lit. c der EG-DSRL gesehen werden kann[2028] und sich ebenfalls in dem Art. 5 (c) der EU-Datenschutzgrundverordnung-E wiederfindet.[2029]

Der Gedanke des Persönlichkeitsschutzes durch Technik findet sich ferner in mehreren, sich teilweise überschneidenden Konzepten, wie der „Privacy Enhancing Technology", „Privacy by Design" und „Privacy by Default", wieder. Der Begriff der „Privacy Enhancing Technology" bezeichnet technische und organisatorische Konzepte, deren Zweck darin

---

2024 *Mutschler*, Die Gottmaschine, 1998, S. 211.

2025 *Bennett/Raab*, The Governance of Privacy, 2006, S. 146 f.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 491; *Piltz*, Soziale Netzwerke im Internet, 2013, S. 281; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 158; *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 11 ff.; *Schulz*, CR 2012, S. 204.

2026 Das präventive Gestaltungsprinzip wird zwar i.d.R. im Zusammenhang mit dem Datenschutz diskutiert, ist jedoch generell auf den Schutz der Persönlichkeitsrechte, z.B. den Schutz vor Herstellung von Aufnahmen, übertragbar; *Cavoukian*, Privacy by Design - Die 7 Grundprinzipien, Privacy by Design, 2011, https://www.privacybydesign.ca/index.php/paper/privacy-by-design/(2.9.2015), S. 1; *Hornung*, ZD 2011, S. 51 (51 f.); *Piltz*, Soziale Netzwerke im Internet, 2013, S. 292; vgl. zur ähnlichen Herangehensweise bei Dashcams, *Knyrim/Trieb*, ZD 2014, S. 547 (548); *Kipker*, DuD 2015, S. 410; *Krombholz u.a.*, Ok Glass, Leave Me Alone, in: *Brenner u.a.*, Financial Cryptography and Data Security, 2015, S. 247 (247); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 491 f.; *Saeltzer*, DuD 2015, S. 103; *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 3 ff.; *Schulz*, CR 2012, S. 204; einen Datenschutz der Technik hat bereits Weiser in seiner Konzeption von Ubiquitous Computing vorgeschlagen, *Weiser*, Scientific American 1991, Vol. 265, Nr. 3, p. 94 (104); *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 3a, Rn. 4 f.

2027 *Hornung*, ZD 2011, S. 51 (53); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 491; *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 3; BT-DrS. 14/4329, S. 30, 33; *Zscherpe*, in: *Taeger/Gabel*, BDSG, § 3a, Rn. 4 f.

2028 *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 17.

2029 Council of the European Union, Synopse zum Stand des Gesetzgebungsverfahrens der EU-DSGVO, 2012/0011 (COD), 2015, http://statewatch.org/news/2015/jul/eu-council-dp-reg-trilogue-10391-15.pdf (2.9.2015), S. 252.

besteht, die Privatsphäre zu schützen.[2030] Privacy Enhancing Technologies können unterschiedliche Schutzwirkungen haben und z.B. Subjekte vor deren Identifizierung oder im Fall der Identifizierung die identifizierenden Daten als Objekte schützen, genauso wie Datentransaktionen oder zwischenmenschliche Interaktionsräume.[2031]

Das Konzept des „Privacy by Design" inkorporiert die Idee der Privacy Enhancing Technologies in ein weitreichenderes Schutzkonzept, dessen Ziel eine „Win-Win-Situation" ist, in der Interessen der Technologie durch ihre Privatsphärenfreundlichkeit gefördert werden (z.B. indem ein höheres Vertrauen in die Technologie entsteht und rechtliche Verantwortung gemindert werden).[2032] D.h., Privacy by Design soll den Grundsatz der Erforderlichkeit durch einen optimalen Interessenausgleich im Wege praktischer Konkordanz fördern.[2033] Ferner kann durch den technischen Grundschutz ein global gleich bleibender Schutzstandard gewahrt werden.[2034]

Privacy by Design ist als ein fundamentales Datenschutzprinzip anerkannt.[2035] Es findet sich im BDSG zumindest indirekt in der Pflicht zur Befolgung erforderlicher technischer und organisatorischer Maßnahmen gem. § 9 BDSG und der Möglichkeit der Auditierung von Datenschutz-

---

2030 *Agre/Burkert*, Privacy-enhancing Technologies, in: *Rotenberg*, Technology and Privacy: The New Landscape, 1997, S. 125 (125); *Krombholz u.a.*, Ok Glass, Leave Me Alone, in: *Brenner u.a.*, Financial Cryptography and Data Security, 2015, S. 247 (247); *Langheinrich*, Personal Privacy in Ubiquitous Computing, 2005, S. 84 ff.; *Weber*, How Does Privacy Change in the Age of the Internet, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 273 (276).

2031 *Hahn/Johannes/Lange*, DuD 2015, S. 71 (74 ff.); Übersicht von technischen Maßnahmen zum Schutz vor Smartglasses, S. *Krombholz u.a.*, Ok Glass, Leave Me Alone, in: *Brenner u.a.*, Financial Cryptography and Data Security, 2015, S. 247 (248 ff.); *Weber*, How Does Privacy Change in the Age of the Internet, in: *Fuchs u.a.*, Internet and Surveillance, 2012, S. 273 (276).

2032 *Cavoukian*, Privacy by Design, Privacy by Design, 2009, https://www.privacybydesign.ca/index.php/paper/privacy-by-design/(2.9.2015), p. 1 ff.; *Bock/Rost*, DuD 2011, S. 30; *Hornung*, ZD 2011, S. 51 (54 f.); *Schulz*, CR 2012, S. 204 (207).

2033 Vgl. E IV, S. 148.

2034 *Scholz*, in: *Simitis*, BDSG, § 3a, Rn. 15 f.

2035 European Union Agency for Network and Information Security, Privacy and Data Protection by Design – from policy to engineering, 2014, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design (9.3.2015); Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, WP 223, 2014, p. 19; *Cavoukian*, Privacy by Design – Primer, Privacy by Design, 2013, https://www.privacybydesign.ca/index.php/paper/privacy-by-design/(9.1.2015), p. 1 f.; das Prinzip wurde von der Datenschutzbeauftragten in Ontario (Kanada), Ann Cavoukian Ende der 1990er Jahre entwickelt, *Cavoukian*, Privacy by Design, Privacy by Design, 2009, https://www.privacybydesign.ca/index.php/paper/privacy-by-design/(2.9.2015), p. 1.

konzepten sowie technischen Einrichtungen nach § 9a BDSG wieder.[2036] Der Entwurf der EU-Datenschutzgrundverordnung enthält im Art. 23 sogar eine explizite gesetzliche Förderung von „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen".[2037]

Das Herausstellungsmerkmal von Privacy by Design sind sieben Grundprinzipien des technischen und organisatorischen Schutzes.[2038] Zu ihnen gehören insbesondere die Prinzipien eines systemimmanenten vorbeugenden Privatsphärenschutzes als Standardeinstellung (sog. „Privacy by Default"), der Transparenz und Kontrollmöglichkeiten Betroffener sowie einer möglichst umfangreichen Beibehaltung der Funktionalität maßgeblicher Technologien.

Entsprechend der Idee von Privacy by Design werden nachfolgend mögliche technische Maßnahmen untersucht, die dazu beitragen könnten, dass Smartglasses ihre einschüchternde Wirkung verlieren und die Autonomie Dritter nicht beeinträchtigen. Die Maßnahmen müssen entsprechend dem Grundsatz der Verhältnismäßigkeit für den Schutz der Privatsphäre Betroffener geeignet und erforderlich sein, d.h. sowohl die Interessen der Träger von Smartglasses als auch der Betroffenen möglichst optimal fördern.

a) Störsender und Schutzkleidung

Im Hinblick auf den Schutz der Privatsphäre durch technische Mittel werden u.a. auf Radiowellen (bezeichnet als „Jammer") oder optischer Blendung (z.B. durch Infrarotstrahlen) basierende Störgeräte besprochen.[2039] Ähnliche Funktion erfüllt spezielle Kleidung, die z.B. Gesichtser-

---

[2036] *Kipker*, DuD 2015, S. 410; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 491.

[2037] Council of the European Union, Synopse zum Stand des Gesetzgebungsverfahrens der EU-DSGVO, 2012/0011 (COD), 2015, http://statewatch.org/news/2015/jul/eu-council-dp-reg-trilogue-10391-15.pdf (2.9.2015), S. 350 f.; *Hornung*, ZD 2012, S. 99 (103 ff.); *Schulz*, CR 2012, S. 204 (206).

[2038] *Cavoukian*, Privacy by Design, Privacy by Design, 2009, https://www.privacybydesign.ca/index.php/paper/privacy-by-design/(2.9.2015), p. 1; deutsche Übersetzung, *Cavoukian*, Privacy by Design - Die 7 Grundprinzipien, Privacy by Design, 2011, https://www.privacybydesign.ca/index.php/paper/privacy-by-design/(2.9.2015), S. 2; *Bock/Rost*, DuD 2011, S. 30 (31); *Schulz*, CR 2012, S. 204 (204 f.).

[2039] *Bekman u.a.*, SPIE Proceedings 2004, Vol. 5615, p. 27; *Krombholz u.a.*, Ok Glass, Leave Me Alone, in: *Brenner u.a.*, Financial Cryptography and Data Security, 2015, S. 247 (249); *Titterton*, Development of Infrared Countermeasure Technology and Systems, in: *Krier*, Mid-infrared Semiconductor Optoelectronics, 2006, S. 635; *Swetak/Summet/Truong*, BlindSpot: Creating Capture-Resistant Spaces, in: *Senior*, Protecting Privacy in Video Surveillance, 2009, S. 185 (185 ff.);*Yamada/Gohshi/Echizen*, Proceedings of the 20th ACM International Conference on Multimedia 2012, p. 1315.

kennungssoftware verwirren soll (sog. „Stealth Wear“).[2040] Derartige Maßnahmen stellen jedoch keinen adäquaten Schutz der Privatsphäre, sondern Abwehr- bzw. Widerspruchsmaßnahmen Betroffener dar. Sie sind also vielmehr die Folge der Gefährdung ihrer Privatsphäre und keine Maßnahme zu deren Schutz.[2041] Ferner ist zu bedenken, dass die Privatsphäre nicht nur eine individualschützende Funktion ausübt, sondern in ihrer objektiven Wirkung dazu dient, die demokratischen Strukturen zu schützen.[2042] Folglich kann sie nicht alleine zur Disposition der Betroffenen, die über den Einsatz der Schutzmaßnahmen entscheiden, gestellt werden.[2043]

b) Abdeckung der Kamera

Eine mechanische Abdeckung der Kamera kann von den Nutzern der Smartglasses ebenso jederzeit abgenommen werden. Ferner ist sie nicht für jedermann transparent und wird mit zunehmender Miniaturisierung von Smartglasses technisch kaum umsetzbar sein. Mechanische Abdeckungen sind mit der Ein- und Ausschaltfunktion vergleichbar und bieten daher außerhalb bestimmter Situationen, in denen sie deutlich zu erkennen und kontrollierbar sind, keinen adäquaten Schutz.[2044]

c) Aufnahmesignale

Die Aktivität der Kamera der Smartglasses kann mit Signalen, wie z.B. leuchtenden oder blinkenden Leuchtdioden, angezeigt werden. Vorstellbar sind auch unterschiedlich farbige Signale, je nachdem, ob Aufnahmen lediglich den Augmented-Reality-Funktionen dienen oder dauerhaft aufgezeichnet werden. Daneben könnten auch Signale wie z.B. ein Kamerageräusch auf die Kameraaktivität hinweisen. Derartige Signale müssten jedoch deutlich wahrnehmbar sein.[2045]

[2040] AVG Reveals Invisibility Glasses at Pepcom Barcelona, AVG, http://now.avg.com/avg-reveals-invisibility-glasses-at-pepcom-barcelona/(11.9.2015); *Franceschi-Bicchierai*, Do Not Track, Mashable, http://mashable.com/2013/09/17/stealthwear-protects-privacy/ (27.8.2015); *Maly*, Anti-Drone Camouflage, WIRED, http://www.wired.com/2013/01/anti-drone-camouflage-apparel/(27.8.2015); *Shandrow*, Protect Your Privacy With These Strange Anti-Surveillance Frocks and Fashions, Entrepreneur, http://www.entrepren eur.com/article/237467 (27.8.2015); ähnliches Ziel verfolgen besondere Haarschnitte und Makeups, Camouflage from face detection, CV Dazzle, http://cvdaz zle.com/ (8.11.2015).

[2041] Auch an dieser Stelle ist das Prinzip, dass Recht dem Unrecht nicht zu weichen braucht, zu beachten, vgl. F V. 4. a) bb) (3) (a), S. 300.

[2042] Vgl. E II. 2. d) aa), S. 134.

[2043] *Simitis*, in: *Simitis*, BDSG, Einleitung, Rn. 114.

[2044] Vgl. F II. 1. a) bb), S. 190.

[2045] Vgl. F II. 1. a) bb), S. 190.

Die Entwicklungsprognose zeigt jedoch, dass eher mit Smartglasses zu rechnen ist, die möglichst unaufdringlich sein sollen.[2046] Auch wenn die Aufnahmesignale in Smartglasses integriert sein sollten, wäre damit zu rechnen, dass Nutzer versuchen würden, sie auszuschalten oder abzudecken.[2047] Folglich bieten Aufnahmesignale zwar einen Schutz, jedoch ist nicht davon auszugehen, dass sie den Betroffenen die Angst vor intransparenter Erfassung durch Smartglasses nehmen werden.

d) Automatische Anonymisierungsverfahren

Es wurde bereits im Rahmen dieser Untersuchung angesprochen, dass die Belastung der Privatsphäre Dritte erheblich sinken würde, wenn Smartglasses Personen bereits im Rahmen der Aufzeichnung im ersten Schritt anonymisieren würden.[2048] Derartige Anonymisierung bietet die als „Anonymous Video Analytics" bezeichnete Technologie, bei der es sich um ein Verfahren handelt, das die Privatsphäre durch Bilderkennungsalgorithmen schützt.[2049] Zu diesem Zweck erkennt die Software die Gesichter oder ganze Menschen als solche, jedoch führt sie keine weitergehende Individualisierung durch, wie sie z.B. im Rahmen biometrischer Funktionen erfolgt.[2050] Das einzige Ziel der „Anonymous Video Analytics"-Technologie besteht darin, die erkannten Gesichter i.S.d. § 3 Abs. 6 BDSG zu anonymisieren, z.B. durch Verpixelungs- oder Verwischungstechniken.[2051] Aufgrund der Möglichkeit, Personen anhand ihrer Kleidung, Geodaten oder ihres Verhaltens zu identifizieren, müsste jedoch nicht nur deren Gesicht, sondern die gesamten Person dementsprechend anonymisiert werden.[2052] Die „Anonymous Video Analytics"-Technologie ist damit eine „smarte" Version von „Privacy Filtern", wie sie z.B. bei Überwa-

---

2046 Vgl. E IV. 1. g) cc), S. 157.

2047 Vgl. E IV. 1. g) bb), S. 155; vgl. *Ozawa*, Disabling camera shutter sound makes smartphones stealthy, Asiaone, http://news.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20111214-316106.html (7.11.2015).

2048 Vgl. E IV. 1. j), S. 161.

2049 Information and Privacy Commissioner of Ontario, Anonymous Video Analytics (AVA) technology and privacy, 2011, https://www.ipc.on.ca/images/Resources/AVAwhite6.pdf (2.9.2015), p. 4; vgl. *Bretthauer/Krempel/Birnstill*, CR 2015, S. 239 (243); Anonymisierungstechnologien werden z.B. durch den Anbieter Google bereits eingesetzt, *Beuth*, Anonymität, Die Zeit, http://www.zeit.de/digital/internet/2012-07/youtube-gesichter-anonym (11.9.2015); *Gross u.a.*, Face De-identification, in: *Senior*, Protecting Privacy in Video Surveillance, 2009, S. 129 (129 ff.).

2050 Information and Privacy Commissioner of Ontario, Anonymous Video Analytics (AVA) technology and privacy, 2011, https://www.ipc.on.ca/images/Resources/AVAwhite6.pdf (2.9.2015), p. 4.; vgl. zur biometrischer Individualisierung, E II. 2. b) dd) (3), S. 118.

2051 Vgl. Ebenda; *Zscherpe*, DuD 2015, S. 172 (173); vgl. B III. 5. c), S. 46.

2052 Vgl. E IV. 1. k) aa), S. 162; vgl. E IV. 1. j), S. 161.

chungskameras eingesetzt werden, um deren Beobachtungsbereiche einzuschränken.[2053]

Um die Privatsphäre effektiv schützen zu können, dürfte diese Anonymisierungs-Technologie jedoch nicht zur Disposition der Nutzer von Smartglasses stehen. Vielmehr müsste sie derart in Smartglasses verankert werden, dass sie nicht abgeschaltet werden kann. Dies würde umgekehrt Einschränkungen für die Nutzer von Smartglasses mit sich bringen, z.B. weil Schnappschüsse von Personen oder der Einsatz innerhalb privater Räumlichkeiten nicht möglich wären. Ebenso würden z.B. Personenabbildungen, wie etwa auf Plakatwänden, auf Gemälden oder als Statuen, sehr wahrscheinlich ebenfalls automatisch unkenntlich gemacht. Auch wäre z.B. die Nutzung von Smartglasses zu Zwecken der Gefahrenabwehr und Beweisführung oder im Rahmen zulässiger Aufnahmen entsprechend § 23 KUG ausgeschlossen. Augmented-Reality-Funktionen wären insoweit eingeschränkt, da sie nur Menschen als solche, aber nicht biometrisch erkennen könnten. Ferner wäre eine vollständig durch Smartglasses vermittelte Mediated Reality praktisch kaum umsetzbar, wenn Menschen für den Träger nur anonymisiert erscheinen würden. D.h., dass ein Schutz Betroffener durch „Anonymous Video Analytics"-Technologie, die Nutzbarkeit von Smartglasses im Hinblick auf Foto- und Videoaufnahmen sowie Augmented-Reality-Funktionen, erheblich einschränken würde.

e) Elektronische Datenschutzerklärung, Einwilligungs- und Widerspruchslösungen

Neben der Anonymisierungstechnologie könnte ein Ausgleich zwischen den Interessen von Nutzern der Smartglasses und den Interessen der von ihnen erfassten Personen durch elektronische Informations- und Zustimmungsprozesse gefördert werden.[2054] Z.B. könnten Smartglasses im Wege der Nahfeldkommunikation Informationen zur Identität ihrer Nutzer oder zu gerade stattfindenden Aufnahmevorgängen i.S.d. § 6b Abs. 2 BGB liefern. Diese Informationen könnten wiederum mittels anderer Smartglasses oder Geräte, wie z.B. Smartphones, abgerufen werden.

Des Weiteren könnten auf diesem Wege elektronische Einwilligungen der Betroffenen entsprechend § 13 Abs. 2 TMG erteilt oder von Nutzern der Smartglasses angefragt werden.[2055] Betroffene könnten z.B. durch Smartglasses abrufbare Einwilligungseinstellungen festlegen, mit denen

---

[2053] *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 492; sie entspricht auch dem Konzept der "differential privacy", bei der die Daten absichtlich so unscharf gemacht werden, so dass sie keine exakten, sondern nur Näherungswerte liefern, *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 220.

[2054] Vgl. *Langheinrich*, Personal Privacy in Ubiquitous Computing, 2005, S. 118 ff.

[2055] *Sassenberg/Berger*, K&R 2007, S. 499.

sie z.B. die Aufhebung der automatischen Anonymisierung oder biometrische Erkennungsverfahren generell, nur gegenüber bestimmten Personen, zeitlich und örtlich unbeschränkt oder temporär und lokal begrenzt, also fein granuliert, erlauben könnten.[2056] Derartige Informationen könnten ferner mittels optisch lesbarer und normierter 2D-Codes, die z.B. an der Kleidung getragen werden (z.B. als ein QR-Code), oder elektronisch mithilfe von „Privacy Beacons" (d.h. elektronischer Geräte, die dem Senden und Empfangen von privatsphärenrelevanten Informationen dienen) als auch mit speziellen Gesten vermittelt werden.[2057] Dennoch müsste auch in solchen Fällen geprüft werden, inwieweit derartige Einwilligungen auf freien Entscheidungen basieren und ob es hinreichend sicher ist, dass die Nutzer der Smartglasses die Grenzen der erteilten Einwilligungen nicht überschreiten werden.[2058]

Auf derselben technischen Grundlage wie die Einwilligung können auch Widerspruchssysteme umgesetzt werden, welche z.B. aufgrund von 2D-Codes, Gesten oder elektronischen Signalen den Einsatz von Smartglasses oder Teilen ihrer Funktionen unterbinden.[2059] So könnten z.B. die Nutzer von Smartglasses ein Kaufhaus betreten, während über spezielle Privacy Beacons gesendete Signale die Aufnahmefunktionen der Geräte abschalten würden.[2060] Ein derartiges Verfahren ist in der Zielsetzung mit dem als „PlaceAvoider" bezeichneten Verfahren vergleichbar, in dessen Rahmen eine Lokalität visuell durch Smartglasses gespeichert werden

---

[2056] *Omoronyia u.a.*, 2013 35th International Conference on Software Engineering (ICSE) 2013, p. 632 (632 ff.); *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 162.

[2057] TagMeNot privacy: no face recognition, don't tag, blur my face., http://tagmenot.info/(1.6.2014); ein ähnliches Konzept stellen "Sticky Policies" dar, d.h. Einwilligungen und Beschränkungend es Datenumgangs, die unmittelbar den Daten anhaften, Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, WP 223, 2014, p. 21, Fn. 29; *Hansen*, DuD 2015, S. 435 (438); *Langheinrich*, Personal Privacy in Ubiquitous Computing, 2005, S. 115 ff.; *Pallas u.a.*, CHI '14 Extended Abstracts on Human Factors in Computing Systems 2014, p. 2179; ein in diesem Zusammenhang verwendeter Begriff sind "Respectful Cameras", sinngem. rücksichtsvolle Kameras, *Schiff u.a.*, Respectful cameras, in: *Senior*, Protecting Privacy in Video Surveillance, 2009, S. 65 (65 ff.); *Yus u.a.*, Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services 2014, S. 366.

[2058] *Hansen*, DuD 2015, S. 435 (438 f.).

[2059] *Dabrowski/Weippl/Echizen*, SMC '13 Proceedings of the 2013 IEEE International Conference on Systems, Man, and Cybernetics 2013, S. 455 (455 ff.); *Pallas u.a.*, CHI '14 Extended Abstracts on Human Factors in Computing Systems 2014, p. 2179; *Yus u.a.*, Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services 2014, S. 366.

[2060] *Hansen*, DuD 2015, S. 435 (438); zu Beacons S., *Venzke-Caprarese*, DuD 2014, S. 839.

könnte, um die Verbreitung von Bildern dieser Lokalität auf Grundlage eines Bildabgleichs zu unterbinden.[2061] Ein ähnliches Verfahren wird auch unter dem Begriff „Geofencing" im Zusammenhang mit Drohnen diskutiert, die automatisch in ihren Funktionen eingeschränkt werden, sobald sie in bestimmten, in einer zentralen Datenbank gespeicherten Ortsbereichen eingesetzt werden.[2062] Ein „Geofencing"- oder ein „PlaceAvoider"-Verfahren würde jedoch eine vorherige Einspeisung von Daten über die jeweilige Lokalität in den Smartglasses voraussetzen, bietet im öffentlichen Raum also einen geringeren Schutz als Widerspruchssignale.

f) Unwägbarkeiten und adaptive Systeme

Die vorgestellten Schutzmaßnahmen sind weder abschließend noch kann derzeit gesagt werden, in welchem Umfang sie zur Anwendung gelangen müssen um Smartglasses ihre einschüchternde Wirkung zu nehmen. Vorstellbar ist vor allem eine Kombination der Technologien, die abhängig vom Grad der Gefährdung oder Kontext der Nutzung von Smartglasses als adaptive Schutzverfahren zur Anwendung kommen (bezeichnet als „Privacy Awareness System" oder „Adaptive Privacy").[2063] Z.B. wäre eine Lösung vorstellbar, bei der die Anonymisierung nur im Rahmen der Augmented Reality erfolgen würde und eine biometrische Identifizierung von Personen insgesamt technisch nicht möglich wäre. Personenabbildungen im Rahmen von Foto- und Videoaufnahmen wären dagegen möglich, müssten jedoch von optischen und/oder akustischen Signalen begleitet werden.

Darüber hinaus existieren zum derzeitigen Zeitpunkt keine als ausgereift zu bezeichnenden Schutzsysteme oder Verfahren für Smartglasses. Ebenso wie die Technologie von Smartglasses befinden sich auch die Schutzsysteme in einem Entwicklungsprozess, in dessen Rahmen technische, soziale und rechtliche Standards evaluiert sowie erst festgelegt werden müssen.[2064]

g) Vertragliche Bindung und Tethered Appliances

Es ist damit zu rechnen, dass die Einschränkungen durch die Implementierung einer „Anonymous Video Analytics"-Technologie, die Einschrän-

---

[2061] *Templeman u.a.*, Proceedings of The 21st Annual Network & Distributed System Security Symposium 2014, p. 23.

[2062] *Jurran*, Drohnen: DJI führt Geofencing-System für temporäre Flugverbotszonen ein, heise online, http://www.heise.de/newsticker/meldung/Drohnen-DJI-fuehrt-Geofencing-System-fuer-temporaere-Flugverbotszonen-ein-2923850.html (18.11.2015).

[2063] "Privacy Awareness System", *Langheinrich*, Personal Privacy in Ubiquitous Computing, 2005, S. 115 ff.; "Adaptive Privacy", *Omoronyia u.a.*, 2013 35th International Conference on Software Engineering (ICSE) 2013, p. 632 (632 ff.).

[2064] Vgl. Darstellung von *Hansen*, DuD 2015, S. 435 (438 f.).

kung biometrischer Funktionen sowie der Einsatz von Aufnahmesignalen von Nutzern der Smartglasses als eine große Bürde und Einschränkung ihrer Freiheit empfunden werden.[2065] Daher wäre damit zu rechnen, dass die Nutzer versuchen würden, derart einschränkende Funktionen zu umgehen.[2066] Damit würden die technischen Schutzmaßnahmen jedoch ihre vertrauensbildende Wirkung verlieren. Folglich ist es notwendig, dass deren Umgehung verhindert wird.

Eine Möglichkeit, die Umgehung zu verhindern, kann in der Technologie selbst liegen, wobei Smartglasses ähnlich den gegenwärtigen Smartphones durch die Nutzer mit neuer Software unter Umgehung der Herstellerbeschränkungen ausgestattet werden könnten (bei Smartphones je nach Betriebssystem als „Jailbreaking" oder „Rooting" bezeichnet).[2067]

Ein zusätzlicher Umgehungsschutz kann durch vertragliche Vorgaben der Geräteanbieter geschaffen werden, mit denen sich Nutzer der Smartglasses als auch Softwareprogrammierer einverstanden erklären müssten. Ein Beispiel sind die AGB von Google Glass, die den Einsatz zu Zwecken der Gesichtserkennung untersagten.[2068] Jedoch zeigte sich, dass Programmierer dadurch nicht davon abgehalten wurden, Gesichtserkennungsapplikationen zu entwickeln, auch wenn diese nicht über offizielle Vertriebswege bezogen werden konnten.[2069] Dennoch könnten auch die vertraglichen Beziehungen durch die Geräteanbieter forciert werden, z.B. indem sie sich Rechte zur Deaktivierung oder Einschränkung der Geräte-

---

2065 Vgl. *Krombholz u.a.*, Ok Glass, Leave Me Alone, in: *Brenner u.a.*, Financial Cryptography and Data Security, 2015, S. 247 (248).

2066 Z.B. müssen mittels von Smartphones erstellte Schnappschüsse von einem lauten Kamerageräusch begleitet werden, wogegen spezielle Umgehungssoftware Abhilfe schaffen soll, *Bruce*, Secretly Take Pictures On Your Android or iPhone Without Being Seen, MakeUseOf, http://www.makeuseof.com/tag/secretly-take-pictures-android-iphone/(7.11.2015); *Ozawa*, Disabling camera shutter sound makes smartphones stealthy, Asiaone, http://news.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20111214-316106.html (7.11.2015).

2067 Vgl. AG Göttingen, Urt. v. 4.5.2011 (62 Ds 51 Js 9946/10 (106/11)), MMR 2011, 626 (628); vgl. MMR-Aktuell, Apple: Patent gegen unautorisierte Nutzung, 2010, Nr. 307665; *Firstenberg/Salas*, Designing and Developing for Google Glass, 2014, S. 352 f.; *Olanoff*, Here Are The Commands You Need To Gain Root Access To Your Google Glass, TechCrunch, http://techcrunch.com/2013/05/16/here-are-the-commands-you-need-to-gain-root-access-to-your-google-glass/(8.6.2014).

2068 *Schwenke*, K&R 2013, S. 685 (686).

2069 *Koetsier*, NameTag releases first face recognition app for Google Glass, recognizes 450K sex offenders, VentureBeat, http://venturebeat.com/2013/12/19/nametag-releases-first-face-recognition-app-for-google-glass-recognizes-450k-sex-offenders/(7.11.2015); *Singer*, When No One Is Just a Face in the Crowd, The New York Times, http://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html (8.6.2014).

funktionen im Fall des Vertragsverstoßes durch technische Eingriffe in die Smartglasses vorbehalten (derart an Hersteller gebundene Geräte werden als „Tethered Appliances“ bezeichnet).[2070] So wurde Google Glass an Testnutzer mit derartigen Einschränkungen ausgeliefert, die den Weiterverkauf der Geräte verhindern sollten.[2071] Dennoch ist zu bedenken, dass je nach technischer Ausstattung auch eine solche Ankopplung der Geräte umgangen werden könnte.

Des Weiteren dürfen die Maßnahmen zur Verhinderung der Umgehung der technischen Schutzmaßnahmen nicht zugleich zu einem Verlust der Privatsphäre aufseiten der Nutzer von Smartglasses führen. Da die Privatsphäre auch dem Schutz der Meinungspluralität und damit der Allgemeinheit dient, dürfen die Träger von Smartglasses nicht freiwillig ihre Privatsphäre aufgeben, nur um die Geräte nutzen zu dürfen. Hier besteht eine besonders hohe Gefahr, da der Wille der Träger von Smartglasses zur Nutzung der Geräte im öffentlichen Raum, kombiniert mit dem ökonomischen Interesse der Anbieter an den Daten der Nutzer sowie des Staates an der Kontrolle seiner Bürger, dennoch zu einer Privatsphärenerosion führen könnte. Ein solcher Schutz würde keinen wirksamen technischen Schutz i.S.d. „Privacy by Design“-Konzeptes darstellen, sondern lediglich den Schwerpunkt der Beeinträchtigung der Privatsphäre verlagern. Zwar würden die Betroffenen geschützt, die Privatsphäre als ein die Allgemeinheit schützendes Konzept würde jedoch parallel zur Verbreitung der Smartglasses und damit der Überwachung ihrer Träge, gefährdet.

Daneben könnten die Privatbedenken der Nutzer zum Marktvorteil der Anbieter mit geringeren Beschränkungen der Persönlichkeitsrechte Dritter führen, was wiederum die technischen Schutzmaßnahmen zu Gunsten Betroffener entwerten könnte.[2072]

h) Gesetzliche Absicherung

Da die technischen und vertraglichen Maßnahmen für den Schutz der Privatsphäre Dritter alleine als nicht hinreichend verlässlich erscheinen,

---

[2070] *Soebbing*, InTeR 2013, S. 77 (77 f.); *Zittrain*, The Future of the Internet - And How to Stop It, 2008, S. 101 ff.

[2071] Die Androhung soll durch Google in einem Fall des unerlaubten Verkaufs von Google Glass vollzogen worden sein, *Harding*, Google Glass Kill Switch, iDigitalTimes.com, http://www.idigitaltimes.com/google-glass-kill-switch-search-company-can-remotely-deactivate-your-1500-device-report-354497 (27.8.2015).

[2072] Zur Bedenken gegen "Tethered Appliances", S. *Soebbing*, InTeR 2013, S. 77 (79 ff.); *Stöcker*, Blackberry, iPhone, Kindle und Co., Spiegel Online, http://www.spiegel.de/netzwelt/gadgets/blackberry-iphone-kindle-und-co-wie-uns-gadgets-an-konzerne-fesseln-a-637388.html (17.9.2013); *Zittrain*, The Future of the Internet - And How to Stop It, 2008, S. 101 ff.

müssen sie durch gesetzliche Maßnahmen gestützt werden. Hierbei erscheinen insbesondere Anreize für die Nutzung von persönlichkeitsrechtsschonenden Smartglasses als besonders aussichtsreich. Z.B. könnte eine normierte Sicherheitsüberprüfung und Zertifizierung für Smartglasses angeboten werden, die Grundlage für gesetzliche Ausnahmen wäre, die das Tragen von Smartglasses im öffentlichen Raum erlauben würden.[2073]

Ferner könnte auch an eine Registrierung von Smartglasses, ähnlich wie Kraftfahrzeuge, gedacht werden.[2074] Ein solches Verfahren erscheint jedoch angesichts der Zahl von Smartglasses, deren häufigen Austauschs (wie heutzutage Smartphones häufig durch neue Modelle ersetzt werden) sowie des damit verbundenen Verwaltungs- und Prüfungsaufwands als wenig praktikabel.

III. Faktischer Zwang zur privatsphärengerechten Integration von Smartglasses in den Alltag als Ergebnis der Zukunftsprognosen

Ausgehend vom heuten Stand des technischen und gesellschaftlichen Fortschritts ist damit zu rechnen, dass ein hoher Bedarf nach der Nutzung von Smartglasses bestehen wird und die Geräte mit großer faktischer Kraft auf den Markt drängen werden. Dabei werden ihre Nutzer zwangsläufig mit den Persönlichkeitsrechtsinteressen Dritter kollidieren, welche jedoch zum Schutz der Individuen sowie der Meinungspluralität nicht aufgegeben werden dürfen. Jedoch besteht die Möglichkeit, mit abgestimmten technischen, vertraglichen und rechtlichen Mitten die Privatsphäre Dritte zu schützen und vor allem den Überwachungs- und Anpassungseffekten Einhalt zu gebieten, indem die von Smartglasses ausgehende Einschüchterungswirkung gemindert wird. Voraussetzung hierfür sind vertrauensbildende Maßnahmen, wie z.B. automatische Anonymisierung von Personen, audiovisuelle Aufnahmehinweise, elektronisch abrufbare Informationen der Träger von Smartglasses sowie ebenfalls elektronische Einwilligungen Betroffener. Die Einhaltung dieser Vorgaben und ein Schutz vor deren Umgehung können wiederum selbst mit technischen

---

[2073] Vgl. *Hornung*, ZD 2011, S. 51 (52 ff.); *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 194 f.

[2074] Ein solches Registrierungsverfahren wird zumindest für manche Arten von Drohnen erwogen, Verkehrsministerium Regierung plant Führerschein und Kennzeichenpflicht für Drohnen, Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/politik/inland/verkehrsministerium-regierung-plant-fuehrerschein-und-kennzeichenpflicht-fuer-drohnen-13900555.html (17.11.2015).

Mitteln, vertraglichen Pflichten der Geräteanbieter sowie gesetzlichen Prüf- und Zertifizierungsverfahren gesichert werden.

Diese technischen Schutzmaßnahmen bringen zwar erhebliche Einschränkungen bei der Nutzung von Smartglasses mit sich, jedoch erscheint es sachgerecht, dass die Nutzer von Smartglasses diese Nachteile als Alternative zu einem völligen Verbot der Nutzung der Geräte im öffentlichen Raum hinnehmen müssen. Darüber hinaus kann an dieser Stelle keine abschließende Antwort gegeben werden, ob und inwieweit die vorgeschlagenen Maßnahmen zu einer Steigerung des Vertrauens in die persönlichkeitsrechtsschonende Nutzung von Smartglasses beitragen werden. Hierzu werden interdisziplinäre Untersuchungen und fortwährende Evaluierungen notwendig sein. Ferner können Smartglasses nicht für sich beurteilt werden, da sie lediglich ein Teil des Fortschrittsprozesses sind und daher in dem Gesamtzusammenhang betrachtet werden müssen. Es ist z.B. vorstellbar, dass sich das politische Leben von Menschen zunehmend in den virtuellen Raum verlagert und Privatsphärenkonzepte wie die Kryptographie, einen weitaus höheren Stellenwert als ein unbeobachteter öffentlicher Raum erhalten werden. Umgekehrt könnte die Einschränkung des Privatsphärenschutzes im virtuellen Raum dazu führen, dass der Schutz vor Überwachung im physisch-öffentlichen Raum umso bedeutender wird.[2075] D.h. im Ergebnis, dass wirtschaftliche, staatliche und moralisch motivierte Maßnahmen anderer Gesellschaftsmitglieder, die den Privatsphärenschutz angreifen, zugleich auch die Möglichkeiten zu einer persönlichkeitsschutzgerechten Nutzung von Smartglasses mindern.

[2075] Die bisherigen Erfahrungen zeigen, dass insbesondere staatliche Stellen die Kryptographiemöglichkeiten der Bürger einschränken möchten, vgl. *Geminn*, DuD 2015, S. 546 (546 f.); *Hornung*, MMR 2015, S. 145 (145 f.); *McCullagh*, Feds put heat on Web firms for master encryption keys, CNET, http://www.cnet.com/news/feds-put-heat-on-web-firms-for-master-encryption-keys/(2.9.2015); *Stöcker*, NSA-Attacke auf Internetverbindungen, Spiegel Online, http://www.spiegel.de/netzwelt/netzpolitik/nsa-und-fbi-verschluesselung-ist-notwehr-a-913083.html (2.9.2015).

I ERGEBNIS DER UNTERSUCHUNG

Zum Schluss der Untersuchung werden die zu Anfang aufgestellten Thesen auf Grundlage der gewonnenen Erkenntnisse verifiziert. Hierbei muss berücksichtigt werden, dass das Ergebnis auf derzeitigen Erkenntnissen basiert und daher mit fortschreitender technologischer und gesellschaftlicher Entwicklung einer erneuten Evaluation bedarf.

These 1: Smartglasses verfügen über das Potenzial, sich zu integralen Teilen des menschlichen Alltags zu entwickeln, da sie mit ihren Funktionen die Bedürfnisse der Informationsgesellschaft nach Effizienz, Sicherheit und Bequemlichkeit befriedigen.

Diese These wurde im Rahmen der Untersuchung bestätigt. Der menschliche Alltag in einer Informationsgesellschaft wird zunehmend durch die Allgegenwart von Computern und Verlagerung der alltäglichen beruflichen oder sozialen Vorgänge in einen virtuellen Raum (auch bezeichnet als Cyberspace) definiert. Auch der physische Raum wird immer stärker mit dem virtuellen Raum verwoben, wodurch die physische Realität mit der virtuellen Realität zu einer einheitlichen Realität verschmilzt. Jedoch ist diese Realität durch die rein körperlichen Funktionen des Menschen nicht erfassbar und bedarf zu ihrer Wahrnehmung und Beeinflussung mobiler Hilfswerkzeuge, wie z.B. der Smartphones. Smartglasses stellen jedoch eine radikale Verbesserung gegenüber den Smartphones dar, da sie nicht nur mobil sind, sondern vor den Augen der Nutzer permanent platziert werden können. Hierdurch können Menschen zum einen schneller Informationen erheben und abrufen (Augmented Memory) und zum anderen stehen ihre Hände für andere Aufgaben frei zur Verfügung. Der wesentliche Vorteil von Smartglasses ist jedoch die Erweiterung der bisher auf den physischen Raum beschränkten visuellen Wahrnehmung der Realität um virtuelle Objekte (Augmented Reality). In einer durch die Fähigkeit zur Informationskontrolle als Grundlage gesellschaftlicher Selbstbehauptung definierten postmodernen Lebenswelt werden sich Menschen dank Augmented Memory und Augmented Reality sowohl im Beruf als auch im Privatleben Vorteile gegenüber anderen Gesellschaftsmitgliedern verschaffen können.

These 2: Smartglasses bergen aufgrund fehlender Transparenz der Informationserfassung sowie mangelnder Kontrolle anschließender Informationsverarbeitung eine erhebliche Gefahr der Beeinträchtigung der Privatsphäre und damit rechtlich verbürgter Persönlichkeitsrechte der von ihnen erfassten Personen. Die Gefahren gehen weit über die bisher verwendeten Arten der optischen, akustischen und elektronischen Informati-

onserfassung, z.B. durch Videoüberwachung oder Smartphones mit Kameras, hinaus.

Auch die zweite These konnte bestätigt werden. Aufgrund der Intransparenz der Erfassungsvorgänge können Dritte im Erfassungsbereich von Smartglasses nicht wissen, ob und in welchem Umfang sie zu Objekten von Aufnahmen ihrer Verbreitung und Veröffentlichung, biometrischer Erkennungsmaßnahmen sowie sonstiger Verwendung der erfassten Informationen werden. Aufgrund der Vorteile, die Smartglasses für Menschen mit sich bringen, ist zudem mit ihrer rapiden Verbreitung zu rechnen, die in Kombination mit anderen Arten der Videoüberwachung sowie Datenverarbeitung zu einer synoptischen, d.h. permanenten und flächendeckenden Überwachung kumuliert. Hierdurch kann der öffentliche Raum seinen Charakter als ein Ort der autonomen Selbstentfaltung und politischen Teilnahme verlieren, da Menschen sich einer permanenten Überwachung und Kontrolle ausgesetzt sehen werden. Um kognitive Dissonanzen mit übrigen Gesellschaftsteilnehmern zu vermeiden, ist damit zu rechnen, dass Menschen aufgrund der Überwachung ihr Verhalten an die gesellschaftlichen Erwartungen anpassen werden. Hierdurch werden sie jedoch ihre Fähigkeit zur autonomen Meinungsbildung verlieren, wodurch nicht nur ihre subjektive Individualität, sondern auch die objektive Meinungspluralität als Grundlage einer freiheitlich-demokratischen Gesellschaft bedroht wäre.

Aufgrund dieser Gefahren stellt der Einsatz von Smartglasses im öffentlichen Raum einen Verstoß gegen das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG sowie gegen die Menschenwürde aus Art. 1 Abs. 1 GG und Art. 1 GRCh dar. Dieses verfassungsrechtliche Ergebnis wirkt sich auf einfachgesetzlicher Ebene aus, wo auch die private Nutzung von Smartglasses eine unerlaubte Videoüberwachung gem. § 6b BDSG sowie eine Verletzung des Allgemeinen Persönlichkeitsrechts als Schutzgut des § 823 Abs. 1 BGB darstellt. An diesem Ergebnis wird sich auch nichts mit dem Inkrafttreten der geplanten DS-GVO ändern. Daneben wird sich mit dem Einsatz von Smartglasses die Wahrscheinlichkeit von Verstößen gegen den strafrechtlich sanktionierten Schutz vor unbefugtem Abhören nicht öffentlich des gesprochenen Wortes gem. § 201 StGB sowie der Verletzung des höchstpersönlichen Schutzbereiches durch Personenbildnisse gem. § 201a StGB als auch der Verbreitung und Zurschaustellung von Bildnissen gem. §§ 22, 33 KUG steigern. Ausnahmen wie der Einsatz von Smartglasses in einer Notwehr- oder notwehrähnlichen Lage, bei medizinischer Indikation oder im Rahmen einer Einwilligung, werden dagegen praktisch kaum eine Rolle spielen. Auch die Ausnahme der Nutzung von Smartglasses an abgelegenen Orten, die nicht

von Menschen frequentiert werden ist zu vernachlässigen, da sie keine typische Nutzung von Smartglasses in Alltagssituationen darstellt.

These 3: Aufgrund der wahrnehmbaren Auswirkungen auf die Privatsphäre wird der Einsatz von Smartglasses im öffentlichen Raum zu Konflikten zwischen ihren Nutzern und den betroffenen Personen führen, die einen Bedarf nach unmittelbaren und sofortigen Schutzmöglichkeiten der Betroffenen mit sich bringen werden.

Anders als im Fall der traditionellen Videoüberwachung, die im Hintergrund erfolgt und deren Verantwortliche im Regelfall ermittelbar sind, ist eine nachträgliche Identifizierung der Nutzer von Smartglasses und damit ein effektiver Rechtsschutz der Betroffenen erheblich eingeschränkt. Aus diesem Grund ist damit zu rechnen, dass die Betroffenen bei der Nutzung von Smartglasses ihre Rechte unmittelbar und sofort geltend machen werden. Neben dem Recht auf Unterlassung und Beseitigung durch Löschung von Aufnahmen gem. §§ 823 Abs. 1 u. 2, 1004 Abs. 1 analog BGB sowie § 6b Abs. 5 BDSG und § 35 Abs. 2 BDSG bzw. analog § 38 KUG, werden Betroffene insbesondere ein Recht auf Auskunft über mögliche Erfassung durch Smartglasses gem. § 34 BDSG, § 823 Abs. 1 i.V.m. § 242 BGB jederzeit geltend machen können. Sollten die Nutzer von Smartglasses die Ansprüche der Betroffenen zurückweisen, werden die Betroffenen sie im Rahmen der Notwehr durch Wegnahme oder Zerstörung der Smartglasses bis zum körperlichen Angriff durchsetzen dürfen. Mithin kann auch die dritte These bestätigt werden.

These 4: Smartglasses sind lediglich der Bestandteil einer viel umfassenderen technologischen und sozialen Veränderung, die nicht aufgehalten werden kann. Ein langfristiges Verbot von Smartglasses ist aufgrund ihres Nutzens in einer zunehmend verdateten Gesellschaft nicht durchführbar.

Die Prognose einer technologischen und gesellschaftlichen Entwicklung bestätigte, dass sich das im Rahmen der ersten These festgestellte Potenzial von Smartglasses in der Zukunft realisieren wird. Smartglasses werden notwendig, damit Menschen mit übrigen technologischen Entwicklungen Schritt halten und sich somit im Wettbewerb mit anderen Menschen behaupten können. Zuerst in Inselbereichen, wie dem privaten Wohnbereich oder dem Arbeitsplatz eingesetzt, ist damit zu rechnen, dass Smartglasses zu unverzichtbaren Alltagsbegleitern werden, die ähnlich wie Smartphones oder das Internet trotz der Gefahren für die Privatsphäre Anwendung finden. Die vierte These konnte daher ebenfalls verifiziert werden.

These 5: Die gegenwärtige Privatsphäre im öffentlichen Raum wird zwar zugunsten von Smartglasses Einschränkungen hinnehmen müssen, darf

jedoch nicht aufgegeben werden. Es wird ein Miteinander des Rechts und der Technik erforderlich, um die Nutzung von Smartglasses im öffentlichen Raum zu ermöglichen.

Auch die letzte These fand im Rahmen der Untersuchung eine Bestätigung. Die Präsenz von Smartglasses wird die Privatsphäre erheblich transformieren, darf jedoch nicht dazu führen, dass diese aufgegeben und dadurch die Individualität und Autonomie von Menschen sowie die Meinungspluralität gefährdet werden. Aus diesem Grund bedarf es Schutzmaßnahmen, die einer möglichst persönlichkeitsrechtsschonenden Integration von Smartglasses in den Alltag von Menschen dienen. Hierzu sind technische Maßnahmen zu empfehlen, wie eine automatische Anonymisierung von Personenabbildungen, audiovisuelle Aufnahmesignale sowie elektronische Informations- und Einwilligungsverfahren. Damit diese Maßnahmen nicht umgangen werden können, müssen sie wiederum mit technischen, vertraglichen sowie rechtlichen Mitteln flankiert werden. Das Ziel ist der Aufbau des Vertrauens in Smartglasses, das Dritten die Angst vor ihnen nehmen soll. Als Ergebnis sollen sich Menschen trotz der Präsenz von Smartglasses in ihrem Verhalten als auch dem Ausdruck ihrer Meinung nicht eingeschränkt fühlen.

Es ist nicht damit zu rechnen, dass trotz der technischen Schutzmaßnahmen der Status quo des gegenwärtigen Privatsphärenkonzeptes aufrechterhalten wird. Ganz im Gegenteil forciert der technologisch-gesellschaftliche Fortschritt eine Vertiefung der Symbiose zwischen Menschen und Maschinen, die mit Smartglasses und ihren Nachfolgern in Form von „smarten“ Kontaktlinsen oder retinalen Implantaten auf eine neue Ebene gehoben werden könnte. Ob dieser große Schritt in Richtung einer Existenz als Cyborgs, d.h. Mensch-Maschine-Hybride, moralisch, biologisch oder existentiell empfehlenswert ist, kann dagegen nicht alleine im Rahmen einer rechtlichen Untersuchung beantwortet werden. Eine Antwort auf diese Frage, wird vielmehr nur unter Einbeziehung aller wissenschaftlichen Disziplinen gefunden werden können.

Als Teil eines kybernetischen Systems werden Menschen jedenfalls zwangsläufig zum Objekt einer durch Informationsrückkopplung bestimmten Lebensumgebung, die in eine auf Überwachung basierende Gesellschaft führt. Es handelt sich jedoch um eine menschengemachte Entwicklung, die so lange von Menschen beeinflusst werden kann, wie diese auf die, den Fortschritt antreibenden Technologien Einfluss nehmen können und wollen. So könnten Smartglasses ebenso zur Fremdbestimmung, wie auch zur Selbstbefähigung von Menschen eingesetzt werden. Die Smartglasses-Technologie kann daher je nach Anwendung und Motivation in eine Dystopie oder eine Utopie führen. Doch auch die Bestimmung was davon was ist, hängt von dem moralischen Standpunkt im

Zeitpunkt der Einschätzung ab. Vom derzeitigen Ideal einer freien und offenen gesellschaftlichen Entwicklung aus gesehen ist es jedenfalls wichtig, dass der moralische Standpunkt auf der Suche nach dessen optimaler Position überhaupt verschoben werden kann. Das setzt wiederum die Erhaltung der Privatsphäre als einen wertneutralen, negativen Schutzraum der autonomen Meinungsbildung voraus. Dies darf trotz utopischer Zukunftsvorstellungen und Technikbegeisterung nicht außer Acht gelassen werden, denn häufig ist der „romantische Geist" der Technik ein „Anästhetikum der Moral".[2076]

[2076] *Mutschler*, Die Gottmaschine, 1998, S. 59.

LITERATUR

Abawi, Daniel F., Augmented Reality - die angereicherte Realität: Ein autorenorientierter Prozess zur authentischen Integration von virtuellen Objekten in Augmented Reality-Anwendungen, Saarbrücken 2008.

Adams, Douglas/Schwarz, Benjamin, Lachs im Zweifel, München 2003.

Agar, Jon, Constant Touch: A Global History of the Mobile Phone, Cambridge 2004.

Agre, Philip E./Burkert, Herbert: Privacy-enhancing Technologies, in: *Marc Rotenberg* (Hrsg.): Technology and Privacy: The New Landscape, 22. Aufl., Cambridge, Mass. 1997, S. 125-142.

Ahlberg, Hartwig/Götting, Horst-Peter (Hrsg.): Beck'scher Onlinekommentar Urheberrecht, 8. Aufl., München 2015.

Albrechtslund, Anders: Socializing the City, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 187-197.

Alexander, Christian: Urheber- und persönlichkeitsrechtliche Fragen eines Rechts auf Rückzug aus der Öffentlichkeit, ZUM 2011, S. 382-389.

Allmer, Thomas: Critical Internet Surveillance Studies and Economic Surveillance, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 124-143.

Altman, Irwin, The environment and social behavior: privacy, personal space, territory, crowding, Monterey, CA 1975.

Andrejevic, Mark: Exploitation in the Data Mine, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 71-88.

Andrejevic, Mark, iSpy: Surveillance and Power in the Interactive Era, Lawrence, Kan. 2009.

Ariès, Philippe: Einleitung, in: *Philippe Ariès/Georges Duby/Roger Chartier* (Hrsg.): Geschichte des privaten Lebens, Bd. 3, Von der Renaissance zur Aufklärung, 3. Aufl., Frankfurt a.M. 1991, S. 7-20.

Arning, Marian/Moos, Flemming: Big Data bei verhaltensbezogener Online-Werbung, ZD 2014, S. 242-248.

Arning, Marian/Moos, Flemming: Location Based Advertising, ZD 2014, S. 126-133.

Assmann, Jan: Der Begriff des kulturellen Gedächtnisses, in: *Thomas Dreier* (Hrsg.): Kulturelles Gedächtnis im 21. Jahrhundert: Tagungsband des internationalen Symposiums, 23. April 2005, Karlsruhe, 2005, S. 21-32.

Azuma, Ronald T.: A Survey of Augmented Reality, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355-385.

Balzer, Timo/Nugel, Michael: Minikameras im Straßenverkehr – Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen, NJW 2014, S. 1622-1628.

Bamberger, Heinz Georg/Roth, Herbert (Hrsg.): Beck'scher Online-Kommentar BGB, 35. Aufl., München 2015.

Barnes, Susan B.: A privacy paradox: Social networking in the United States, First Monday 2006, Vol. 11, Nr. 9, Abrufbar unter: http://firstmonday.org/article/view/1394/1312 (3.10.2014).

Baudrillard, Jean, In the Shadow of the Silent Majorities, Los Angeles; Cambridge, Mass. 2007.

Bauman, Zygmunt, Liquid Surveillance: A Conversation, Cambridge, UK; Malden, Mass. 2012.

Becker, Maximilian/Becker, Felix: Die neue Google-Datenschutzerklärung und das Nutzer-Metaprofil - Vereinbarkeit mit nationalen und gemeinschaftsrechtlichen Vorgaben, MMR 2012, S. 351-355.

Becker, Maximilian/Becker, Felix: Zur rechtlichen Zulässigkeit von AdBlockern, GRUR-Prax 2015, S. 245-249.

Becker, Philipp/Nikolaeva, Julia: Das Dilemma der Cloud-Anbieter zwischen US Patriot Act und BDSG, CR 2012, S. 170-176.

Beck, Ulrich: Das Zeitalter der Nebenfolgen und die Politisierung der Moderne, in: *Ulrich Beck/Anthony Giddens/Scott Lash* (Hrsg.): Reflexive Modernisierung: Eine Kontroverse, 6. Aufl., Frankfurt a.M. 1996, S. 19-112.

Beck, Ulrich, Risikogesellschaft. Auf dem Weg in eine andere Moderne, Frankfurt a.M. 1986.

Beck, Ulrich/Giddens, Anthony/Lash, Scott: Vorwort, in: *Ulrich Beck/Anthony Giddens/Scott Lash* (Hrsg.): Reflexive Modernisierung: Eine Kontroverse, 6. Aufl., Frankfurt a.M. 1996.

Bekman, Herman/van den Heuvel, Johan/van Putten, Frank/Schleijpen, Ric: Development of a mid-infrared laser for study of infrared countermeasures techniques, SPIE Proceedings 2004, Vol. 5615, p. 27-38.

Bell, Daniel: Post-Industrial Society, in: *Frank Webster/Raimo Blom* (Hrsg.): The Information Society Reader, 2004, S. 86-102.

Bell, Daniel, The Coming of Post-Industrial Society: A Venture in Social Forecasting, New York 1976.

Beller, Jonathan, The Cinematic Mode of Production: Attention Economy and the Society of the Spectacle, Lebanon/USA 2012.

Bennett, Colin J./Raab, Charles D., The Governance of Privacy: Policy Instruments in Global Perspective, Cambridge, Mass. 2006.

Bentham, Jeremy, Das Panoptikum, Berlin 2013.

Berberich, Matthias: Der Content „gehört" nicht Facebook! AGB-Kontrolle der Rechteeinräumung an nutzergenerierten Inhalten, MMR 2010, S. 736-741.

Berg, Christian, Smartphones und Tablets. Ihre Auswirkungen auf den privaten Alltag, 2013.

Bergfink, Alexander: Videoüberwachung in Fahrzeugen des öffentlichen Personennahverkehrs, DuD 2015, S. 145-150.

Bergt, Matthias: Die Bestimmbarkeit als Grundprolem des Datenschutzrechts, ZD 2015, S. 365-371.

Bizer, Johann: Das Recht auf Anonymität in der Zange gesetzlicher Identifizierungspflichten, in: *Helmut Bäumler/Albert von Mutius* (Hrsg.): Anonymität im Internet: Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Braunschweig; Wiesbaden 2003, S. 78-94.

Bliem, Daniela, Wearable Computing: Benutzerschnittstellen zum Anziehen, München u.a. 2007.

Bockholt, Ulrich/Wuest, Harald/Wientapper, Folker/Engelke, Timo/Webel, Sabine: Augmented Reality Assistenzsysteme für Wartung und Service in Industrie, Bau und Gebäudemanagement, in: *Michael Schenk* (Hrsg.): 16. IFF-Wissenschaftstage 2013. Tagungsband: Digitales Engineering zum Planen, Testen und Betreiben technischer Systeme, Magdeburg 2013, S. 195-200.

Bock, Kirsten/Rost, Martin: Privacy By Design und die Neuen Schutzziele, DuD 2011, S. 30-35.

Bogard, William, The Simulation of Surveillance: Hypercontrol in Telematic Societies, Cambridge; New York 1996.

Bohne, Michael: Die Informationsfreiheit und der Anspruch von Datenbankbetreibern auf Zugang zu Gerichtsentscheidungen, NVwZ 2007, S. 656-660.

Bökel, Rainer: Das Recht auf Anonymität in der Diskussion, in: *Helmut Bäumler/Albert von Mutius* (Hrsg.): Anonymität im Internet: Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Braunschweig; Wiesbaden 2003, S. 191-197.

Botella, Cristina/Bretón-López, Juani/Quero, Soledad/Baños, Rosa/García-Palacios, Azucena: Treating Cockroach Phobia With Augmented Reality, Behavior Therapy 2010, Vol. 41, Nr. 3, p. 401-413.

Boyd, Danah M./Ellison, Nicole B.: Social Network Sites: Definition, History, and Scholarship, JCMC 2007, Vol. 13, Nr. 1, p. 210-230.

Braun, Johann: Subjektive Rechtfertigungselemente im Zivilrecht?, NJW 1998, S. 941-944.

Bräutigam, Peter/Klindt, Thomas: Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, S. 1137-1142.

Bretthauer, Sebastian/Krempel, Erik/Birnstill, Pascal: Intelligente Videoüberwachung in Kranken- und Pflegeeinrichtungen von morgen, CR 2015, S. 239.

Brin, The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?, Reading, Mass 1999.

Brink, Stefan/Eckhard, Jens: Wann ist ein Datum ein personenbezogenes Datum, ZD 2015, S. 205-212.

Britz, Gabriele, Freie Entfaltung durch Selbstdarstellung: Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, Tübingen 2007.

Broll, Wolfgang: Augmentierte Realität, in: *Ralf Dörner/Wolfgang Broll/Paul Grimm/Bernhard Jung* (Hrsg.): Virtual und Augmented Reality (VR/AR), Berlin; Heidelberg 2013, S. 241-294.

Brown, Abbe/Harmon, Shawn/Waelde, Charlotte: Do You See What I See? Disability, Technology, Law and the Experience of Culture, IIC 2012, p. 901-930.

Bruns, Axel, Blogs, Wikipedia, Second Life, and Beyond, New York 2008.

Büllesfeld, Dirk, Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsvorsorge, Stuttgart 2002.

Buschbaum, Jörg/Rosak, Philip: Kfz-Kennzeichenerfassung in Parkhäusern, ZD 2015, S. 354-358.

Busch, Christian: Was meinen wir mit Biometrie?, DuD 2013, S. 386-386.

Busche, Katalin: Der Einsatz von Körperscannern auf deutschen Flughäfen: Eine verfassungsrechtliche Bewertung, DÖV 2011, S. 225-233.

Busch, Ralf: Strafrechtlicher Schutz gegen Kinderpornographie und Missbrauch, NJW 2015, S. 977-981.

Canton, Erik J.F./Groot, Henri L.F./Nahuis, Richard: Vested Interests and Resistance to Technology Adoption, CentER Discussion Paper, Tilburg University, Centre for Economic Research 1999, Vol. 106, p. 1-39.

Caspar, Johannes: Datenschutz im Verlagswesen: Zwischen Kommunikationsfreiheit und informationeller Selbstbestimmung, NVwZ 2010, S. 1451-1457.

Castells, Manuel, Communication Power, Oxford; New York 2009.

Castells, Manuel, Das Informationszeitalter Wirtschaft. Gesellschaft. Kultur. Bd. 1: Der Aufstieg der Netzwerkgesellschaft, Opladen 2001.

Castells, Manuel, Die Internet-Galaxie, Wiesbaden 2005.

Castells, Manuel: Toward a Sociology of the Network Society, Contemporary Sociology 2000, Vol. 29, Nr. 5, p. 693-699.

Clayton, Russell B./Leshner, Glenn/Almond, Anthony: The Extended iSelf: The Impact of iPhone Separation on Cognition, Emotion, and Physiology, JCMC 2015, Vol. 20, Nr. 2, p. 119-135.

Clynes, Manfred E./Kline, Nathan S.: Cyborgs and space, Astronautics 1960, Nr. 9, p. 26-76.

Coleridge, Samuel Taylor, Biographia Literaria, London 1965.

Dabrowski, Adrian/Weippl, Edgar R./Echizen, Isao: Framework Based on Privacy Policy Hiding for Preventing Unauthorized Face Image Processing, SMC '13 Proceedings of the 2013 IEEE International Conference on Systems, Man, and Cybernetics 2013, S. 455-461.

Davison, Adrian K./Yap, Moi Hoon/Costen, Nicholas/Tan, Kevin/Lansley, Cliff/Leightley, Daniel: Micro-Facial Movements: An Investigation on Spatio-Temporal Descriptors, in: *Lourdes Agapito/Michael M. Bronstein/Carsten Rother* (Hrsg.): Computer Vision - ECCV 2014 Workshops, 2014, S. 111-123.

DeCarlo, Douglas/Metaxas, Dimitris: Optical Flow Constraints on Deformable Models with Applications to Face Tracking, International Journal of Computer Vision 2000, Vol. 38, Nr. 2, p. 99-127.

Deleuze, Gilles, Unterhandlungen: 1972-1990, 5. Aufl., Frankfurt a.M. 1993.

Dienel, Peter C.: Geleitwort zur deutschen Ausgabe, in: *Goffman Erving* (Hrsg.): Verhalten in sozialen Situationen: Strukturen und Regeln der Interaktion im öffentlichen Raum., Gütersloh 1971, S. 7-12.

Dieterich, Thomas/Hanau, Peter/Schaub, Günter/Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid (Hrsg.): Erfurter Kommentar zum Arbeitsrecht, 15. Aufl., München 2015.

Dörner, Paul/Geiger, Christian/Oppermann, Leif/Paelke, Volker: Interaktion in Virtuellen Welten, in: *Ralf Dörner/Wolfgang Broll/Paul Grimm/Bernhard Jung* (Hrsg.): Virtual und Augmented Reality (VR/AR), Berlin; Heidelberg 2013, S. 157-194.

Dörner, Ralf u.a.: Fallbeispiele für VR/AR, in: *Ralf Dörner/Wolfgang Broll/Paul Grimm/Bernhard Jung* (Hrsg.): Virtual und Augmented Reality (VR/AR), Berlin; Heidelberg 2013, S. 295-326.

Dörner, Ralf/Broll, Wolfgang/Grimm, Paul/Jung, Bernhard/Göbel, Martin: Einleitung, in: *Ralf Dörner/Wolfgang Broll/Paul Grimm/Bernhard Jung* (Hrsg.): Virtual und Augmented Reality (VR/AR), Berlin; Heidelberg 2013, S. 1-32.

Dreier, Thomas/Schulze, Gernot (Hrsg.): Urheberrechtsgesetz, 5. Aufl., München 2015.

Duhr, Elisabeth/Naujok, Helga/Peter, Martina/Seiffert, Evelyn: Neues Datenschutzrecht für die Wirtschaft, DuD 2002, S. 1-36.

Dürig, Günter: Der Grundrechtssatz von der Menschenwürde, AöR 1956, S. 117-157.

Ehmann, Horst: Zur Struktur des Allgemeinen Persönlichkeitsrechts, JuS 1997, S. 193-203.

Ellul, Jacques, The Technological Society, New York 1967.

Ensthaler, Jürgen: Streaming und Urheberrechtsverletzung, NJW 2014, S. 1553-1558.

Erbs, Georg/Kohlhaas, Max (Hrsg.): Strafrechtliche Nebengesetze, 195. EL, München 2013.

Erd, Rainer: Datenschutzrechtliche Probleme sozialer Netzwerke, NVwZ 2011, S. 19-22.

Ericson, Richard V./Haggerty, Kevin D.: The New Politics of Surveillance and Visibility, in: *Richard V. Ericson/Kevin D. Haggerty/David Wall* (Hrsg.): The New Politics of Surveillance and Visibility, Toronto 2006, S. 3-25.

Ernst, Stefan: Gleichklang des Persönlichkeitsschutzes im Bild- und Tonbereich?, NJW 2004, S. 1277-1279.

Ernst, Stefan: Google StreetView: Urheber- und persönlichkeitsrechtliche Fragen zum Straßenpanorama, CR 2010, S. 178-184.

Etzioni, Amitai, Die Entdeckung des Gemeinwesens: Ansprüche, Verantwortlichkeiten und das Programm des Kommunitarismus, Frankfurt a.M. 1998.

Färber, Berthold: Kommunikationsprobleme zwischen autonomen Fahrzeugen und menschlichen Fahrern, in: *Markus Maurer/J. Christian Gerdes/Barbara Lenz/Hermann Winner* (Hrsg.): Autonomes Fahren, Berlin; Heidelberg 2015, S. 127-146.

Federrath, Hannes: Technik der Cloud, ZUM 2014, S. 1-3.

Fetscher, Iring, Karl Marx und der Marxismus, München 1967.

Fetscher, Iring, Rousseaus politische Philosophie: zur Geschichte des demokratischen Freiheitsbegriffs, Frankfurt a.M. 1993.

Fikentscher, Wolfgang/Möllers, Thomas: Die (negative) Informationsfreiheit als Grenze von Werbung und Kunstdarbietung, NJW 1998, S. 1337-1344.

Firstenberg, Allen/Salas, Jason, Designing and Developing for Google Glass: Thinking Differently for a New Platform, Sebastopol, CA 2014.

Fischer, Lorenz/Wiswede, Günter, Grundlagen der Sozialpsychologie, 3. Aufl., München u.a. 2009.

Floridi, Luciano, The Ethics of Information, Oxford 2013.

Forgó, Nikolaus: Google StreetView – Nur ein Spannungsverhältnis zwischen Privatsphäre und öffentlichem Raum?, MMR 2010, S. 217-218.

Forgó, Nikolaus/Krügel, Tina: Der Personenbezug von Geodaten - Cui bono, wenn alles bestimmbar ist?, MMR 2010, S. 17-23.

Foucault, Michel, Überwachen und Strafen: die Geburt des Gefängnisses, Frankfurt a.M. 1994.

Franklin, Ursula M., The Real World of Technology (CBC Massey Lectures series), 2. Aufl., Toronto, Ont.; Berkeley, CA 1999.

Friedrich, Marion, Die künstliche Evolution der Cyborgs. Erkenntnistheoretische Aspekte der Bioinformatik, Marburg 2003.

Frömming, Jens/Peters, Butz: Die Einwilligung im Medienrecht, NJW 1996, S. 958-962.

Fuchs, Christian: Critique of the Political Economy of Web 2.0 Surveillance, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 31-70.

Fuchs, Christian: studiVZ: social networking in the surveillance society, Ethics and Information Technology 2010, Vol. 12, Nr. 2, S. 171-185.

Fuchs, Christian/Boersma, Kees/Albrechtslund, Anders/Sandoval, Marisol: Introduction, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 1-30.

Fuchs, Daniel: Verwendung privater Kameras im öffentlichen Raum, ZD 2015, S. 212-217.

Gallwas, Hans-Ulrich: Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit, NJW 1992, S. 2785-2790.

Gandy, Oscar H. Jr., The Panoptic Sort: A Political Economy of Personal Information, Boulder, Col. 1993.

Gates, Kelly, Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance, New York u. London 2011.

Gehlen, Arnold, Anthropologische Forschung. Zur Selbstbegegnung und Selbstentdeckung des Menschen., Reinbek bei Hamburg 1984.

Gehlen, Arnold, Die Seele im technischen Zeitalter und andere sozialpsychologische, soziologische und kulturanalytische Schriften, Frankfurt a.M. 2004.

Geiger, Andreas: Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung, NVwZ 1989, S. 35-38.

Geiger, Andreas, Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie bei der Straftatbekämpfung., Berlin 1994.

Geis, Ivo: Unternehmen in der Flut elektronischer Kommunikation, ZD 2013, S. 591-594.

Geminn, Christian L.: Crypto Wars Reloaded, DuD 2015, S. 546-547.

Geppert, Martin/Schütz, Raimund (Hrsg.): Beck'scher TKG-Kommentar, 4. Aufl., München 2013.

Giddens, Anthony, Interpretative Soziologie: Einführung und Kritik, Frankfurt 1984.

Giddens, Anthony, Konsequenzen der Moderne, Frankfurt a.M. 1996.

Giddens, Anthony: Leben in einer posttraditionellen Gesellschaft, in: *Ulrich Beck/Anthony Giddens/Scott Lash* (Hrsg.): Reflexive Modernisierung: Eine Kontroverse, 6. Aufl., Frankfurt a.M. 1996, S. 113-194.

Giddens, Anthony, Modernity and Self-Identity: Self and Society in the Late Modern Age, Stanford, California 1991.

Giger, Roman, Street View mit Infrarotkamera, Rapperswil 2012.

Goffman, Erving, Verhalten in sozialen Situationen : Strukturen und Regeln der Interaktion im öffentlichen Raum, Gütersloh 1971.

Goffman, Erving, Wir alle spielen Theater, München u.a. 2003.

Gola, Peter: Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer – Zulässigkeit und Transparenz, NZA 2007, S. 1139-1144.

Gola, Peter/Klug, Christoph: Videoüberwachung gemäß § 6b BDSG - Anmerkungen zu einer verunglückten Gesetzeslage, RDV 2004, S. 65-74.

Gola, Peter/Schomerus, Rudolf (Begr.): Bundesdatenschutzgesetz, 12. Aufl., München 2015.

Golla, Sebastian J./Herbort, Nina Elisabeth: Zivilrechtlicher Bildnisschutz im Vorfeld von Weitergabe und Veröffentlichung - Wann müssen digitale Abzüge gelöscht werden?, GRUR 2015, S. 648-655.

González, Jennifer: Envisioning Cyborg Bodies: Notes form Current Research, in: *Chris Hables-Gray* (Hrsg.): The Cyborg Handbook, New York 1995, S. 267-280.

Göpfert, Burkard/Wilke, Elena: Nutzung privater Smartphones für dienstliche Zwecke, NZA 2012, S. 765-771.

Gordon, Diana R.: The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System, Politics & Society 1987, Vol. 15, Nr. 4, p. 483-511.

Graf, Jürgen-Peter (Hrsg.): Beck'scher Online-Kommentar Strafprozessordnung mit RiStBV und MiStra, 21. Aufl., München 2015.

Green, Lawrence R./Grotz, Janis: Conceptualization and Measurement of Reported Self-Fiscovery, Human Communication Research 1976, Vol. 2, Nr. 4, p. 338-346.

Greger, Reinhard: Kamera on board – Zur Zulässigkeit des Video-Beweises im Verkehrsunfallprozess, NZV 2015, S. 114-118.

Griffiths, Devin C., Virtual Ascendance: Video Games and the Remaking of Reality, 2013.

Grimm, Dieter: Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts, NJW 1995, S. 1697-1705.

Grimm, Paul/Herold, Ringo/Hummel, Johannes/Broll, Wolfgang: VR-Eingabegeräte, in: *Ralf Dörner/Wolfgang Broll/Paul Grimm/Bernhard Jung* (Hrsg.): Virtual und Augmented Reality (VR/AR), Berlin; Heidelberg 2013, S. 97-126.

Groeben, Hans von der/Schwarze, Jürgen/Hatje, Armin (Hrsg.): Europäisches Unionsrecht, 7. Aufl., Baden-Baden 2015.

Gross, Ralph/Sweeney, Latanaya/Cohn, Jeffrey/de la Torre, Fernando/Baker, Simon: Face De-identification, in: *Andrew Senior* (Hrsg.): Protecting Privacy in Video Surveillance, London 2009, S. 129-146.

Grötker, Ralf: Informationelle Selbstbestimmung - ein zeitgemäßes Leitprinzip? Für eine normative Konkretisierung informationsethischer Belange, in: *Bettina Sokol* (Hrsg.): Total transparent - Zukunft der informationellen Selbstbestimmung?, Düsseldorf 2006, S. 48-64.

Grünwald, Andreas/Nüßing, Christoph: Machine To Machine (M2M)-Kommunikation Regulatorische Fragen bei der Kommunikation im Internet der Dinge, MMR 2015, S. 378-383.

Gumm, Heinz-Peter/Sommer, Manfred, Einführung in die Informatik, 10. Aufl., München 2012.

Gusy, Christoph, Polizei- und Ordnungsrecht, 9. Aufl., Tübingen 2014.

Habermas, Jürgen, Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft, 17. Aufl., Darmstadt u.a. 1987.

Haberstroh, Dieter: Notwehr gegen unbefugte Bildaufnahmen - Angst als Rechtfertigungsgrund?, JR 1983, S. 314-318.

Hafner, V.V./Bachmann, F.: Human-Humanoid walking gait recognition, 8th IEEE-RAS International Conference on Humanoid Robots - Conference Paper 2008, p. 598-602.

Haggerty, Kevin/Ericson, Richard: The surveillant assemblage, in: *Sean Hier* (Hrsg.): The Surveillance Studies Reader, Maidenhead 2007, S. 104.

Hahn, Tobias/Johannes, Paul C./Lange, Benjamin: Schutzschilde gegen die NSA, DuD 2015, S. 71-77.

Hammersen, Jens/Eisenried, Ukrich: Ist „Redlining" in Deutschland erlaubt?, ZD 2014, S. 342-345.

Han, Byung-Chul, Transparenzgesellschaft, Berlin 2012.

Hannich, Rolf (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung: mit GVG, EGGVG, EMRK, 7. Aufl., München 2013.

Hansen, Marit: Zukunft von Datenschutz und Privatsphäre in einer mobilen Welt, DuD 2015, S. 435-439.

Härting, Niko: Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, S. 2065-2072.

Hauschka, Christoph E. (Hrsg.): Corporate Compliance, 2. Aufl., München 2010.

Hayles, N. Katherine: The Life Cycle of Cyborgs: Writing the Posthuman, in: *Chris Hables-Gray* (Hrsg.): The Cyborg Handbook, New York 1995, S. 321-340.

Heckmann, Dirk: Öffentliche Privatheit - Der Schutz der Schwächeren im Internet, K&R 2011, S. 770-777.

Heidrich, Joerg/Wegener, Christoph: Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten - Problemfall Logging, MMR 2015, S. 487-493.

Heinrich, Thorsten: Google Glass und der Datenschutz – alles glasklar?, AnwZert ITR 2014, 10/2014,. Anm. 2.

Heintschel-Heinegg, Bernd (Hrsg.): Beck'scher Online-Kommentar Strafrecht, 27. Aufl., München 2015.

Helle, Ernst, Der Schutz der Persönlichkeit der Ehre und des wirtschaftlichen Rufes im Privatrecht, 2. Aufl., Tübingen 1969.

Heller, Christian, Post Privacy: prima leben ohne Privatsphäre, München 2011.

Hellermann, Johannes, Die sogenannte negative Seite der Freiheitsrechte, Berlin 1993.

Hermes, Georg: Grundrechtsschutz durch Privatrecht auf neuer Grundlage ? Das BVerfG zu Schutzpflicht und mittelbarer Drittwirkung der Berufsfreiheit, NJW 1990, S. 1764-1768.

Hesse, Konrad, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Aufl., Heidelberg 1995.

Hickethier, Knut: Medien - Aufmerksamkeit, in: *Knut Hickethier/Joan Kristin Bleicher* (Hrsg.): Aufmerksamkeit, Medien und Ökonomie, Münster 2002, S. 5-13.

Hilgert, Peter/Hilgert, Sebastian: Nutzung von Streaming-Portalen Urheberrechtliche Fragen am Beispiel von Redtube, MMR 2014, S. 85-88.

Hill, David W.: Jean-François Lyotard and the Inhumanity of Internet Surveillance, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 106-123.

Hill, Doug, Not So Fast: Thinking Twice About Technology, 2013.

Hill, Hermann: Aus Daten Sinn machen: Analyse- und Deutungskompetenzen in der Datenflut, 2014, Vol. DÖV, S. 213-222.

Hilpert, Thomas: Zulässigkeit der Videoüberwachung nach § 6b BDSG, RDV 2009, S. 160-167.

Hobbes, Thomas, Leviathan, Hamburg 2005.

Hoeren, Thomas: Anonymität im Web – Grundfragen und aktuelle Entwicklungen, ZRP 2010, S. 251-253.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht, 41. EL, München 2015.

Hoffmann, Christian: Die Verletzung der Vertraulichkeit informationstechnischer Systeme durch Google Street View, CR 2010, S. 514-518.

Hofmann, Christina/Hödl, Elisabeth: Drohnen und Drohnenjournalismus, DuD 2015, S. 167-171.

Hofmann, Hasso: Die versprochene Menschenwürde, AöR 1993, S. 353-377.

Honecker, Martin, Einführung in die theologische Ethik: Grundlagen und Grundbegriffe, Berlin; New York 2002.

Hornung, Gerrit: Datenschutz durch Technik in Europa, ZD 2011, S. 51-56.

Hornung, Gerrit: Der Personenbezug biometrischer Daten, DuD 2004, S. 429-431.

Hornung, Gerrit: Die Krypto-Debatte: Wiederkehr einer Untoten, MMR 2015, S. 145-146.

Hornung, Gerrit: Eine DatenschutzGrundverordnung für Europa?, ZD 2012, S. 99-106.

Horst, Reinhold: Der Nachbar als „Big Brother" - Grenzen zulässiger Videoüberwachung, NZM 2000, S. 937-945.

Hotter, Maximilian, Privatsphäre: der Wandel eines liberalen Rechts im Zeitalter des Internets, Frankfurt a.M. u.a. 2011.

Hubmann, Heinrich, Das Persönlichkeitsrecht, 2. Aufl., Köln/Gratz 1967.

Hufen, Friedhelm: Zur rechtlichen Regelung der Straßenkunst - kommunikativer Gemeingebrauch oder Verbot mit Erlaubnisvorbehalt?, DÖV 1983, S. 353-362.

Humble, Jez/Farley, David, Continuous Delivery: Reliable Software Releases Through Build, Test, and Deployment Automation, Upper Saddle River, NJ 2010.

Jahn, David/Striezel, Julia: Google Street View is watching you, K&R 2009, S. 753-758.

Jarass, Hans: Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, S. 857-862.

Juan, M. Carmen/Alcaniz, Mariano/Monserrat, Carlos/Botella, Cristina/Banos, Rosa M./Guerrero, Belen: Using Augmented Reality to Treat Phobias, IEEE Comput. Graph. Appl. 2005, Vol. 25, Nr. 6, p. 31-37.

Jutzi, Siegfried: Informationsfreiheit und Rundfunkgebührenpflicht, NVwZ 2008, S. 603-608.

Kang, Jerry: Information Privacy in Cyberspace Transactions, Stanford Law Review 1998, Vol. 50, Nr. 4, S. 1193-1294.

Kant, Immanuel, Grundlegung zur Metaphysik der Sitten, Riga 1786.

Kant, Immanuel, Werkausgabe Band 11, 16. Aufl., Frankfurt a.M. 1977.

Karg, Moritz: BGH: Speicherung dynamischer IP-Adressen, MMR 2011, S. 341-346.

Karg, Moritz: Biometrische Verfahren zur Gesichtserkennung und Datenschutz in Sozialen Netzwerken, HFR 2012, S. 120-134.

Ketzer, Christine, Securitas ex Machina. Von der Bedeutung technischer Kontroll- und Überwachungssysteme für Gesellschaft und Pädagogik, Köln 2005.

Kilian, Wolfgang/Heussen, Benno (Hrsg.): Computerrechts- Handbuch, 32. EL, München 2013.

Kindshäuser, Urs/Neumann, Ulfried/Paeffgen, Hans-Ulrich (Hrsg.): Strafgesetzbuch, 4. Aufl., Baden Baden 2013.

Kipker, Dennis-Kenji: Privacy by Default und Privacy by Design, DuD 2015, S. 410-410.

Kipper, Greg/Rampolla, Joseph, Augmented Reality: An Emerging Technologies Guide to AR, Amsterdam u.a. 2012.

Kirchhof, Gregor: Kumulative Belastung durch unterschiedliche staatliche Maßnahmen, NJW 2006, S. 732-736.

Klar, Manuel, Datenschutzrecht und die Visualisierung des öffentlichen Raums, Berlin 2012.

Klar, Manuel: Der Rechtsrahmen des Datenschutzrechts für Visualisierungen des öffentlichen Raums. Ein taugliches Konzept zum Schutz der Betroffeneninteressen?, MMR 2012, S. 788-795.

Klaus, Haffner, Der „große Bruder", Chancen und Gefahren für eine informierte Gesellschaft, Düsseldorf 1980.

Klein, Georg, Visual Tracking for Augmented Reality: Edge-based tracking techniques for AR applications, Saarbrücken 2009.

Klein, Naomi, The Shock Doctrine: The Rise of Disaster Capitalism, London 2008.

Kley, Andreas: Teleologische und deontologische Ethik: Utilitarismus und Menschenrechte, in: *Philippe Mastronardi* (Hrsg.): Das Recht im Spannungsfeld utilitaristischer und deontologischer Ethik: Vorträge der Tagung der Schweizer Sektion der internationalen Vereinigung für Rechts- und Sozialphilosophie (SVRSP) vom 15. und 16. November 2002 in Luzern, Stuttgart 2004, S. 55-70.

Kloepfer, Michael/Breitkreutz, Katharina: Videoaufnahmen und Videoaufzeichnungen als Rechtsproblem, DVBl 1998, S. 1149-1157.

Knyrim, Rainer/Trieb, Gerald: Videokameras in Autos – vom Teufelszeug zum Beweismittel - Vereinbarkeit von Dash-Cams mit datenschutzrechtlichen Grundsätzen, ZD 2014, S. 547-552.

Königshofen, Thomas: Neue datenschutzrechtliche Regelungen zur Videoüberwachung, RDV 2001, S. 220-223.

Kopke, Wolfgang: Heimliches Mithörenlassen eines Telefongesprächs, NZA 1999, S. 917-921.

Köppen, Oliver M., Das Grundrecht der Informationsfreiheit unter besonderer Berücksichtigung der neuen Medien, Lohmar 2004.

Koskela, Hille: Webcams, TV Shows and Mobile phones: Empowering Exhibitionism, Surveillance & Society 2002, Vol. 2, Nr. 2/3, p. 199-215.

Kosut, Mary, Encyclopedia of Gender in Media, Thousand Oaks, CA 2012.

Krohm, Niclas/Müller-Peltzer, Philipp: Wunsch nach Identifizierung anonymer Internetnutzer - Spannungsverhältnis von Kommunikationsfreiheit und Persönlichkeitsrechten, ZD 2015, S. 409-415.

Krombholz, Katharina/Dabrowski, Adrian/Smith, Matthew/Weippl, Edgar: Ok Glass, Leave Me Alone: Towards a Systematization of Privacy Enhancing Technologies for Wearable Computing, in: *Michael Brenner/Nicolas Christin/Benjamin Johnson/Kurt Rohloff* (Hrsg.): Financial Cryptography and Data Security, Berlin; Heidelberg 2015, S. 247-280.

Krüger, Stefan/Maucher, Svenja-Ariane: Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, S. 433-439.

Kuhns, William, The Post-industrial Prophets: Interpretations of Technology, New York 1971.

Kukkonen, Tuuli M./Binik, Yitzchak M./Amsel, Rhonda/Carrier, Serge: Thermography as a physiological measure of sexual arousal in both men and women, The Journal of Sexual Medicine 2007, Vol. 4, Nr. 1, p. 93-105.

Kurzweil, Ray, Homo Sapiens: Leben im 21. Jahrhundert - Was bleibt vom Menschen?, München 2000.

Kymlicka, Will, Theorie und Gesellschaft Band 35: Politische Philosophie heute. Eine Einführung, Frankfurt a.M.; New York 1997.

Lachenmann, Matthias/Schwiering, Sebastian: Betrieb von Videokameras in PKW Datenschutzrechtliche (Un-)Zulässigkeit des Betriebs von On-Board-Kameras in PKWs, NZV 2014, S. 291-298.

Lackner, Karl/Kühl, Kristian (Hrsg.): Strafgesetzbuch, 28. Aufl., München 2014.

Land, Karl-Heinz/Kreutzer, Ralf T., Dematerialisierung - Die Neuverteilung der Welt in Zeiten des digitalen Darwinismus, Köln 2015.

Langheinrich, Marc, Personal Privacy in Ubiquitous Computing - Tools and System Support, Zürich 2005.

Lang, Markus, Private Videoüberwachung im öffentlichen Raum: eine Untersuchung der Zulässigkeit des privaten Einsatzes von Videotechnik und der Notwendigkeit von 6 b BDSG als spezielle rechtliche Regelung, Hamburg 2008.

Lang, Markus/Lachenmann, Matthias: Kein Mitbestimmungsrecht bei Videokamera-Attrappen, NZA 2015, S. 591-595.

Lanham, Richard A., The Economics of Attention: Style and Substance in the Age of Information, Chicago 2006.

Leffler, Ricarda, Der strafrechtliche Schutz des Rechts am eigenen Bild vor dem neuen Phänomen des Cyber-Bullying, Frankfurt a.M. u.a. 2012.

Legnaro, Aldo: Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze, Leviathan 1997, S. 271-284.

Lent, Wolfgang: Elektronische Presse zwischen E-Zines, Blogs und Wikis, ZUM 2013, S. 914-920.

Lessig, Lawrence, Code: And Other Laws of Cyberspace, Version 2.0, 2. Aufl., New York 2006.

Lewinski, Kai von: Europäisierung des Datenschutzrechts, DuD 2012, S. 564-570.

Libertus, Michael: Die Einwilligung als Voraussetzung für die Zulässigkeit von Bildnisaufnahmen und deren Verbreitung, ZUM 2007, S. 621-628.

Lim, Kai Keat/Friedrich, Max/Radun, Jenni/Jokinen, Kristiina: Lying Through the Eyes: Detecting Lies Through Eye Movements, Proceedings of the 6th Workshop on Eye Gaze in Intelligent Human Machine Interaction 2013, p. 51-56.

Lim, Mei Yii/Aylett, R.: MY virtual graffiti system, 2004 IEEE International Conference on Multimedia and Expo, 2004. ICME '04 2004, Vol. 2, p. 847-850.

Lindenberg, Michael/Schmidt-Semisch, Henning: Sanktionsverzicht statt Herrschaftsverlust: Vom Übergang in die Kontrollgesellschaft, Kriminologisches Journal 1995, S. 2-17.

Lindner, Christian: Persönlichkeitsrecht und Geo-Dienste im Internet – z.B. Google Street View/Google Earth, ZUM 2010, S. 292-301.

Locke, John/Ebbinghaus, Julius, Ein Brief über Toleranz, Hamburg 1996.

Lücke, Jörg: Der additive Grundrechtseingriff sowie das Verbot der übermäßigen Gesamtbelastung des Bürgers, DVBl 2001, S. 1469-1478.

Lüdemann, Volker: Connected Cars, ZD 2015, S. 247-254.

Luhmann, Niklas, Grundrechte als Institution - Ein Beitrag zur politischen Soziologie, Berlin 1965.

Luhmann, Niklas, Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, 5. Aufl., Stuttgart 2000.

Lützeler, Martin/Bissels, Alexander: Social Media-Leitfaden für Arbeitgeber: Rechte und Pflichten im Arbeitsverhältnis, ArbRAktuell 2011, S. 499-502.

Lyon, David: 9/11, Synopticon, and Scopophilia: Watching and Being Watched, in: *Richard V. Ericson/Kevin D. Haggerty/David Wall* (Hrsg.): The New Politics of Surveillance and Visibility, Toronto 2006, S. 35-54.

Lyon, David, Electronic Eye: The Rise of Surveillance Society, Minneapolis 1994.

Lyon, David, Surveillance Society: Monitoring Everyday Life, Buckingham, England; Philadelphia 2001.

Lyon, David, Surveillance Studies: An Overview, Malden (USA) 2007.

Lyotard, Jean-François, Das Postmoderne Wissen: Ein Bericht, Wien 1986.

MacKinnon, Catharine A., Toward a Feminist Theory of the State, 1989.

MacWilliams, Asa, A Decentralized Adaptive Architecture for Ubiquitous Augmented Reality Systems, 2005.

Mann, Steve: Through the Glass, Lightly, IEEE Technology and Society Magazine 2012, Vol. 31, Nr. 3, p. 10-14.

Mann, Steve/Ferenbok, Joseph: New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World, Surveillance and Society 2013, Vol. 11, Nr. 1/2, p. 18-34.

Mann, Steve/Niedzviecki, Hal, Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer, Toronto 2002.

Martin, Klaus, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, Hamburg 2007.

Marx, Karl, Das Kapital: Kritik der politischen Oekonomie, Hamburg 1872.

Mathiesen, Thomas: Preface, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. xv-xvii.

Mattern, Friedmann/Flörkemeier, Christian: Vom Internet der Computer zum Internet der Dinge, Informatik-Spektrum 2010, Vol. 33, Nr. 2, S. 107-121.

Maunz, Thodor/Dürig, Günter (Hrsg.): Grundgesetz, 74. EL., München 2015.

Mayerdierks, Per: Sind IP-Adressen personenbezogene Daten?, MMR 2009, S. 8-13.

Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data: Die Revolution, die unser Leben verändern wird, München 2013.

Mehler-Bicher, Anett/Reiß, Michael/Steiger, Lothar, Augmented Reality: Theorie und Praxis, München 2011.

Merten, Detlef: Nichtigkeit vereinbarter Freizügigkeitsbeschränkung geschiedener Eheleute, NJW 1972, S. 1799-1799.

Milgram, Paul/Takemura, Haruo/Utsumi, Akira/Kishino, Fumio: Augmented Reality: A Class of Displays on the Reality-Virtuality Continuum, SPIE 1994, Vol. 2351, p. 282-292.

Mill, John S., Über die Freiheit, Stuttgart 1986.

Mill, John S., Utilitarismus, Hamburg 2009.

Möller, Jan/Florax, Björn-Christoph: Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken?, NJW 2003, S. 2724-2726.

Möller, Jan/Florax, Björn-Christoph: Kreditwirtschaftliche Scoring-Verfahren Verbot automatisierter Einzelentscheidungen gem. § 6a BDSG, MMR 2002, S. 806-810.

Möncke, Ulrich: Cloudbasierte Werkzeuge in der Hochschullehre, DuD 2015, S. 617-621.

Moore, Gordon E.: Cramming More Components Onto Integrated Circuits, Proceedings of the IEEE 1998, Vol. 86, Nr. 1, p. 82-85.

Moos, Flemming/Zeiter, Anna: Vorabwiderspruch bei Geodatendiensten – Gesetz oder Geste? Zwischenbilanz anhand erster Gerichtsentscheidungen zu Google Street View, ZD 2013, S. 178-182.

Murswiek, Dietrich: Technische Risiken als verfassungsrechtliches Problem, in: *Raban Graf von Westphalen* (Hrsg.): Technikfolgenabschätzung als politische Aufgabe, 3. Aufl., München 1997, S. 238-265.

Mutschler, Hans-Dieter, Die Gottmaschine, Augsburg 1998.

Nagel, Thomas: Concealment and Exposure, Philosophy & Public Affairs 1998, Vol. 27, Nr. 1, p. 3-30.

Nagel, Thomas, Concealment and Exposure: And Other Essays, New York; Oxford 2004.

Nebel, Maxi: Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung?, Zeitschrift für Datenschutz, ZD 2015, S. 517.

Negroponte, Nicholas, Total digital. Die Welt zwischen 0 und 1 oder Die Zukunft der Kommunikation, München 1997.

Nguyen, Alexander: Videoüberwachung in sensitiven Bereichen, DuD 2011, S. 715-717.

Oberwetter, Christian: Soziale Netzwerke im Fadenkreuz des Arbeitsrechts, NJW 2011, S. 417-421.

Ohly, Ansgar: Verändert das Internet unsere Vorstellung von Persönlichkeit und Persönlichkeitsrecht?, AfP 2011, S. 428-438.

Ohly, Ansgar, „Volenti non fit iniuria“: die Einwilligung im Privatrecht, Tübingen 2002.

Omoronyia, I./Cavallaro, L./Salehie, M./Pasquale, L./Nuseibeh, B.: Engineering adaptive privacy: On the role of privacy awareness requirements, 2013 35th International Conference on Software Engineering (ICSE) 2013, p. 632-641.

Opel, Alexander/Körffer, Barbara/Nouak, Alexander: Datenschutz bei der Erhebung biometrischer Testdaten, DuD 2013, S. 347-351.

Orwell, George, 1984, Boston; New York 1983.

Palanker, Daniel/Vankov, Alexander/Huie, Phil/Baccus, Stephen: Design of a high-resolution optoelectronic retinal prosthesis, Journal of Neural Engineering 2005, Vol. 2, Nr. 1, p. 105-120.

Pallas, Frank/Ulbricht, Max-Robert/Jaume-Palasi, Lorena/Höppner, Ulrike: Offlinetags: A novel privacy approach to online photo sharing, CHI '14 Extended Abstracts on Human Factors in Computing Systems 2014, p. 2179-2184.

Payandeh, Mehrdad: Gefahrenabwehr gegen Bildaufnahmen von Polizeikräften, NVwZ 2013, S. 1458-1462.

Pedersen, Isabel, Ready to Wear: A Rhetoric of Wearable Computers and Reality-Shifting Media, Anderson, SC 2013.

Pieroth, Bodo/Schlink, Bernhard/Kingreen, Thorsten/Poscher, Ralf, Grundrechte - Staatsrecht II, 30. Aufl., Heidelberg 2014.

Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael/Kingreen, Thorsten/Poscher, Ralf, Polizei- und Ordnungsrecht: mit Versammlungsrecht, 8. Aufl., München 2014.

Piltz, Carlo, Soziale Netzwerke im Internet - eine Gefahr für das Persönlichkeitsrecht?, Frankfurt a.M. u.a. 2013.

Pöhl, Veronika, Der Cyborg als Medium des Körpers, Konstanz 2010.

Pordesch, Ulrich/Steidle, Roland: Entfernen des Personenbezugs mittels Verschlüsselung durch Cloudnutzer, 2015, S. 536-541.

Poster, Mark, The Mode of Information: Poststructuralism and Social Contexts, Cambridge 1991.

Pratsch, Daniel, Auswirkungen einer Aero-Cave Umgebung auf die Orientierung innerhalb einer virtuellen 3D-Umgebung, Bremen 2005.

Preuß, Simon, Augmented Reality: Hype oder zukunftsweisende Technik?, Nordestedt 2014.

Radkau, Joachim, Technik in Deutschland: Vom 18. Jahrhundert bis heute, Frankfurt a.M.; New York 2008.

Rahmlow, Matthias: Einzelne Probleme des Straftatbestands der „Verletzung des höchstpersönlichen Lebensbereiches durch Bildaufnahmen" (§ 201 a StGB), HRRS 2005, S. 84-93.

Regenfus, Thomas: Zivilrechtliche Abwehransprüche gegen Überflüge und Bildaufnahmen von Drohnen, NZM 2011, S. 799-803.

Reibach, Boris: Private Dashcams & Co. - Household Exemption ade?, DuD 2015, S. 157-160.

Richter, Kai, Methoden zur Unterstützung bei der Entwicklung plattformübergreifender Benutzerschnittstellen, Darmstadt 2007.

Rihaczek, Karl: Vordemokratisch, DuD 2015, S. 141-141.

Röger, Ralf/Stephan, Alexander: Die Videoüberwachung, NWVBl 2001, S. 243-248.

Roggan, Fredrik: Die Videoüberwachung von öffentlichen Plätzen, NVwZ 2001, S. 134-141.

Rosenbaum, Birgit/Tölle, Dennis: Aktuelle rechtliche Probleme im Bereich Social Media - Überblick über die Entscheidungen der Jahre 2011 und 2012, MMR 2013, S. 209-212.

Roßnagel, Alexander, Datenschutz bei Wearable Computing - Eine juristische Analyse am Beispiel von Schutzanzügen, Wiesbaden 2012.

Roßnagel, Alexander, Datenschutz in einem informatisierten Alltag, Berlin 2007.

Roßnagel, Alexander: Die Novellen zum Datenschutzrecht – Scoring und Adresshandel, NJW 2009, S. 2716-2722.

Roßnagel, Alexander: Die Rolle des Rechts im Prozeß der Technikfolgenabschätzung, in: *Raban Graf von Westphalen* (Hrsg.): Technikfolgenabschätzung als politische Aufgabe, 3. Aufl., München 1997, S. 222-237.

Roßnagel, Alexander: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, S. 1238-1242.

Handbuch Datenschutzrecht: die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

Roßnagel, Alexander: Konflikte zwischen Informationsfreiheit und Datenschutz?, MMR 2007, S. 16-21.

Roßnagel, Alexander/Hornung, Gerrit: Biometrische Daten in Ausweisen, DuD 2005, S. 69-73.

Russakovsky, Olga u.a.: ImageNet Large Scale Visual Recognition Challenge, Cornell University, n.n.v. Studienarbeit 2014, p. 1-43.

Säcker, Franz Jürgen/Rixecker, Roland (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 2: §§ 241-432, 6. Aufl., München 2012.

Säcker, Franz Jürgen/Rixecker, Roland (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 5: §§ 705-853, 6. Aufl., München 2013.

Saeltzer, Gerhard: Schaffen wir das vertrauenswürdigste, menschenfreundlichste, sicherste und beste Internet der Welt!, DuD 2015, S. 103-107.

Sandoval, Marisol: A Critical Empirical Case Study of Consumer Surveillance on Web 2.0, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 147-169.

Sassenberg, Thomas/Berger, Ernst Georg: Rechtliche Zulässigkeit von Werbung via Bluetooth, K&R 2007, S. 499-503.

Scellato, Salvatore/Mascolo, Cecilia/Musolesi, Mirco/Latora, Vito: Distance Matters: Geo-social Metrics for Online Social Networks, Proceedings of the 3rd Wonference on Online Social Networks 2010, p. 8-8.

Schaar, Peter, Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft, München 2007.

Schaefer, Brian P./Steinmetz, Kevin F.: Watching the Watchers and McLuhan's Tetrad: The Limits of Video-Activism in the Internet Age, Surveillance & Society 2014, Vol. 12, Nr. 4, p. 502-515.

Schart, Dirk/Tschanz, Nathaly, Praxishandbuch Augmented Reality für Marketing, Medien und Public Relations, Konstanz 2015.

Schellenberg, Ulrich: Wie die bürgerliche Freiheit im digitalen Fegefeuer verbrennen könnte, ZRP 2014, S. 24-26.

Scheurle, Klaus-Dieter/Mayen, Thomas (Hrsg.): Telekommunikationsgesetz, 2. Aufl., München 2008.

Schiff, J./Meingast, M./Mulligan, D.K./Sastry, S./Goldberg, K.: Respectful cameras: detecting visual markers in real-time to address privacy concerns, in: *Andrew Senior* (Hrsg.): Protecting Privacy in Video Surveillance, London 2009, S. 65-89.

Schiller, Herbert: The World Crisis and the New Information Technologies, Columbia Journal of World Business 1983, Vol. 18, Nr. 1, p. 86-90.

Schleeh, Hannes/Sohn, Gunnar, Live Streaming mit Hangout On Air: Techniken, Inhalte & Perspektiven für kreatives Web TV, München 2014.

Schmidt, Rolf, Polizei- und Ordnungsrecht: sowie Grundzüge des Versammlungsrechts und des Verwaltungsvollstreckungsrechts, 17. Aufl., Grasberg bei Bremen 2015.

Schmitt Glaeser, Walter: Big Brother is watching you - Menschenwürde bei RTL 2, ZRP 2000, S. 395-402.

Schmitz, Albert, Strafrechtlicher Schutz vor Bild- und Wortaufnahmen, Hamburg 2011.

Schnabel, Christoph: Das Recht am eigenen Bild und der Datenschutz, ZUM 2008, S. 657-662.

Schönke, Adolf/Schröder, Horst (Hrsg.): Strafgesetzbuch, 29. Aufl., München 2014.

Schrems, Max, Kämpf um deine Daten, Wien 2014.

Schultze-Melling, Jyn: Informationelle Selbstverwertung - die Hoffnung stirbt zuletzt, ZD 2013, S. 570-571.

Schulze, Reiner (Hrsg.): Bürgerliches Gesetzbuch: Handkommentar, 8. Aufl., Baden-Baden 2014.

Schulz, Sebastian: Privacy by Design - Datenschutz durch Technikgestaltung im nationalen und europäischen Kontext, CR 2012, S. 204-208.

Schulz, Sönke E.: Cloud Computing in der öffentlichen Verwaltung Chancen – Risiken – Modelle, MMR 2010, S. 75-80.

Schwenke, Matthias Christoph, Individualisierung und Datenschutz: Rechtskonformer Umgang mit personenbezogenen Daten Im Kontext der Individualisierung, Wiesbaden 2006.

Schwenke, Thomas: Google Glass – Eine Herausforderung für das Recht, K&R 2013, S. 685-691.

Schwenke, Thomas: Nutzungsbedingungen sozialer Netzwerke und Onlineplattformen, WRP 2012, S. 37-41.

Schwenke, Thomas: Schnittstellen zum „Cyborgspace“ — Erkenntnisse zu Datenbrillen nach Ende des „Google Glass“-Experiments, DuD 2015, S. 161-166.

Schwerdtner, Peter: Der zivilrechtliche Persönlichkeitsschutz, JuS 1978, S. 289-299.

Schwind, Hans-Dieter, Kriminologie: eine praxisorientierte Einführung mit Beispielen, 2011.

Seemann, Michael, Das neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust, Freiburg im Breisgau 2014.

Sennett, Richard, Verfall und Ende des öffentlichen Lebens: Die Tyrannei der Intimität, 14. Aufl., Frankfurt a.M. 2004.

Sieber, Bayreuth: Informationsrecht und Recht der Informationstechnik - Die Konstituierung eines Rechtsgebietes in Gegenstand, Grundfragen und Zielen, NJW 1989, S. 2569-2580.

Siegel, Eric, Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, Hoboken, N.J 2013.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014.

Simmel, Georg: Die Großstädte und das Geistesleben, in: *Theodor Petermann* (Hrsg.): Die Großstadt. Vorträge und Aufsätze zur Städteausstellung, Dresden 1903, S. 1985.

Simmel, Georg, Individualismus der modernen Zeit: und andere soziologische Abhandlungen, Frankfurt a.M. 2008.

Simmel, Georg, Philosophie des Geldes, Leipzig 1900.

Simmel, Georg, Soziologie: Untersuchungen über die Formen der Vergesellschaftung., 6. Aufl., Berlin 1983.

Simmel, Georg, Über soziale Differenzierung. Soziologische und psychologische Untersuchungen, Leipzig 1890.

Simon, Herbert A.: Designing Organizations for an Information-Rich World, in: *Martin Greenberger/Johns Hopkins University/Brookings Institution* (Hrsg.): Computers, communications, and the public interest, Baltimore 1971, S. 37-72.

Slizyk, Andreas, (Hrsg.): Beck'sche Schmerzensgeld-Tabelle IMMDAT Plus, 11. Aufl., München 2015.

Soebbing, Thomas: Googles Glass - Rechtliche Grenzen der Nutzung und Vermarktung von angebundenen Geräten (Tethered Appliances), InTeR 2013, S. 77-82.

Sofsky, Wolfgang, Verteidigung des Privaten: Eine Streitschrift, München 2007.

Solmecke, Christian/Kocatepe, Sibel: Google Glass – Der Gläserne Mensch 2.0, Die neueste technische Errungenschaft – ein Fluch oder eine Herausforderung?, ZD 2014, S. 22-27.

Solmecke, Christian/Nowak, Fabian: Zivile Drohnen – Probleme ihrer Nutzung. Rechtliche Bewertung eines künftigen Millardenmarkts, MMR 2014, S. 431-435.

Spiecker genannt Döhmann, Indra: Big Data intelligent genutzt: Rechtskonforme Videoüberwachung im öffentlichen Raum, K&R 2014, S. 549-556.

Spiecker genannt Döhmann, Indra: Datenschutzrechtliche Fragen und Antworten in Bezug auf Panorama - Abbildungen im Internet, CR 2010, S. 311-318.

Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 3. Aufl., München 2015.

Spreen, Dierk: Der Cyborg: Diskurse zwischen Körper und Technik, in: *Eva Eßlinger/Tobias Schlechtriemen/Doris Schweitzer/Alexander Zons* (Hrsg.): Die Figur des Dritten: Ein kulturwissenschaftliches Paradigma, Berlin 2010, S. 166-179.

Stehr, Nico/Böhme, Stehr, The Knowledge Society: The Growing Impact of Scientific Knowledge on Social Relations, Dordrecht ; Boston : Norwell, MA, U.S.A 1986.

Steinbuch, Karl: Über den Wert von Informationen, GRUR 1987, S. 579-584.

Steinmüller, Wilhelm, Informationstechnologie und Gesellschaft. Einführung in die Angewandte Informatik., Darmstadt 1993.

Stonier, Tom, Information und die innere Struktur des Universums, Berlin u.a. 1991.

Störmer, Andre, Blickrichtungsunabhängige Erkennung von Personen in Bild- und Tiefendaten, Ilmenau 2009.

Suthau, Tim, Positionsgenaue Einblendung räumlicher Informationen in einem See Through Head Mounted Display für die Medizin am Beispiel der Leberchirurgie, Berlin 2006.

Sutherland, Ivan E.: A Head-Mounted Three-Dimensional Display, Proceedings of AFIPS 1968, p. 506-508.

Swetak, N. Patel/Summet, Jay W./Truong, Jeffrey: BlindSpot: Creating Capture-Resistant Spaces, in: *Andrew Senior* (Hrsg.): Protecting Privacy in Video Surveillance, London 2009, S. 185-201.

Tacke, Sarah C., Medienpersönlichkeitsrecht: Das System der Rechtsfolgen von Persönlichkeitsrechtsverletzungen durch Massenmedien, Berlin; Münster 2009.

Taddicken, Monika: Privacy, Surveillance, and Self-Disclosure in the Social Web, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 255-273.

Taeger, Jürgen: Videoüberwachung von Bürohäusern, ZD 2013, S. 571-577.

Taeger, Jürgen/Gabel, Detlev (Hrsg.): BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl., Frankfurt am Main 2013.

Taigman, Yaniv/Yang, Ming/Ranzato, Marc'Aurelio/Wolf, Lior: DeepFace: Closing the Gap to Human-Level Performance in Face Verification, IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2014, p. 1701-1708.

Templeman, Robert/Korayem, Mohammed/Crandall, David/Kapadia, Apu: PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces, Proceedings of The 21st Annual Network & Distributed System Security Symposium 2014, p. 23-26.

Terhaag, Michael: Filmen während der Fahrt - der rechtliche Umgang mit Dashcams, K&R 2015, S. 556-559.

Titterton, D. H.: Development of Infrared Countermeasure Technology and Systems, in: *Anthony Krier* (Hrsg.): Mid-infrared Semiconductor Optoelectronics, 2006, S. 635-671.

Toffler, Alvin, Die dritte Welle, München 1980.

Tonnis, Marcus, Augmented Reality: Einblicke in die Erweiterte Realität, Berlin; Heidelberg 2010.

Tufekci, Zeynep: Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites, Bulletin of Science, Technology & Society 2008, Vol. 28, Nr. 1, p. 20-36.

Uckelmann, Dieter/Harrison, Marc/Michahelles, Florian, Architecting the Internet of Things, New York 2011.

Venzke-Caprarese, Sven: Standortlokalisierung und personalisierte Nutzeransprache mittels Bluetooth Low Energy Beacons, DuD 2014, S. 839-844.

Vulin, Danica: lst das deutsche datenschutzrechtliche Schriftformerfordernis zu viel des Guten?, ZD 2012, S. 414-418.

Wagner, Thomas, Robokratie: Google, das Silicon Valley und der Mensch als Auslaufmodell, Köln 2015.

Wall, David S.: Surveillant Internet Technologies and the Growth in Information Capitalism: Spams and Public Trust in the Information Society, in: *Richard V. Ericson/Kevin D. Haggerty* (Hrsg.): The New Politics of Surveillance and Visibility, Toronto 2006, S. 340-362.

Wanckel, Endress, Persönlichkeitsschutz in der Informationsgesellschaft: Zugleich ein Beitrag zum Entwicklungsstand des allgemeinen Persönlichkeitsrechts, Frankfurt a.M.; New York 1999.

Wandtke, Artur-Axel/Bullinger, Winfried (Hrsg.): Praxiskommentar zum Urheberrecht, 4. Aufl., München 2014.

Warren, Samuel D./Brandeis, Louis D.: The Right to Privacy, Harvard Law Review 1890, Vol. 4, Nr. 5, p. 193-220.

Weber, Jörg-Andreas: Google „Street View" und ähnliche Geo-Datendienste im Internet aus zivilrechtlicher Sicht, NJOZ 2011, S. 673-676.

Weber, Karsten: Surveillance, Sousveillance, Equiveillance: Google Glasses, SSRN Electronic Journal 2012, Nr. 6, p. 1-3.

Weber, Rolf H.: How Does Privacy Change in the Age of the Internet, in: *Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval* (Hrsg.): Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York 2012, S. 273-293.

Webster, Frank, Theories of the Information Society, 4. Aufl., Abingdon, Oxon 2014.

Weichert, Thilo: Big Data und Datenschutz, ZD 2013, S. 251-259.

Weichert, Thilo: Datenschutz im Auto – Teil 1, SVR 2014, S. 201-207.

Weichert, Thilo: Der Bodyscanner und die menschliche Scham, RDV 2009, S. 154-159.

Weichert, Thilo: Der Personenbezug von Geodaten, DuD 2007, S. 17-23.

Weichert, Thilo: Drohnen und Datenschutz, ZD 2012, S. 501-504.

Weichert, Thilo: Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, DuD 2009, S. 347-352.

Weichert, Thilo: Rechtsfragen der Videoüberwachung, DuD 2000, S. 662-669.

Weiser, Mark: The computer for the 21st Century, Scientific American 1991, Vol. 265, Nr. 3, p. 94-104.

Wenzel, Karl E./Burkhardt, Emanuel H./Gamer, Waldemar/Strobl-Albeg, Joachim von, Das Recht der Wort- und Bildberichterstattung: Handbuch des Äußerungsrechts, 5. Aufl., Köln 2003.

Westin, Alan F., Privacy And Freedom, New York 1968.

Westphalen, Raban Graf von: Einführung in die Technikfolgenabschätzung, in: *Raban Graf von Westphalen* (Hrsg.): Technikfolgenabschätzung als politische Aufgabe, 3. Aufl., München 1997, S. 9-14.

Wicklund, Robert/Frey, Dieter: Die Theorie der objektiven Selbstaufmerksamkeit, in: *Dieter Frey/Martin Irle* (Hrsg.): Theorien der Sozialpsychologie, Bd.1, Kognitive Theorien, 2. Aufl., Bern u.a. 1993, S. 155-174.

Wieczorek, Mirko Andreas, Persönlichkeitsrecht und Meinungsfreiheit im Internet: Kollision und Abwägung bei Internetangeboten - eine verfassungsrechtliche Analyse, Frankfurt a.M. 2013.

Wieduwilt, Hendrik: Verbot „bloßstellender Bilder" - das Ende der Straßenfotografie?, K&R 2014, S. 627-632.

Wiener, Norbert, Kybernetik. Regelung und Nachrichtenübertragung im Lebewesen und in der Maschine, Düsseldorf u.a. 1963.

Winner, Langdon, Autonomous Technology: Technics-out-of-control as a Theme for Political Thought, 1978.

Winner, Langdon, The Whale and the Reactor: A Search for Limits in an Age of High Technology (Paperback) - Common, Chicago 1989.

Wintermeier, Martin: lnanspruchnahme sozialer Netzwerke durch Minderiährige, ZD 2012, S. 210-214.

Wiskott, Jens/Fellous, Jean-Marc/Krüger, Norbert/Malsburg, von der, Christoph: Face Recognition by Elastic Bunch Graph Matching, in: *Lakhmi C. Jain/Ugur Halici/Isao Hayashi/S. B. Lee/Shigeyoshi Tsutsui* (Hrsg.): Intelligent Biometric Techniques in Fingerprint and Face Recognition, Boca Raton 1999, S. 355.

Wolff, Heinrich A./Brink, Stefan (Hrsg.): Beck'scher Online-Kommentar Datenschutzrecht, 12. Aufl., München 2015.

Wolter, Jürgen (Hrsg.): SK-StPO Systematischer Kommentar zur Strafprozessordnung, Band II: §§ 94-136a StPO, 4. Aufl., Köln 2010.

Wrede, Ann-Karina: Spannungsverhältnis zwischen Datenschutz und Ethik - Am Beispiel der „smarten" Videoüberwachung, ZD 2012, S. 321-324.

Yamada, Takayuki/Gohshi, Seiichi/Echizen, Isao: Use of Invisible Noise Signals to Prevent Privacy Invasion Through Face Recognition from Camera

Images, Proceedings of the 20th ACM International Conference on Multimedia 2012, p. 1315-1316.

Yus, Roberto/Pappachan, Primal/Das, Prajit Kumar/Mena, Eduardo/Joshi, Anupam/Finin, Tim: Demo: FaceBlock: Privacy-aware Pictures for Google Glass, Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services 2014, S. 366-366.

von Zimmermann, Georg, Die Einwilligung im Internet, Berlin 2014.

Zittrain, Jonathan, The Future of the Internet - And How to Stop It, New Haven; London 2008.

Zscherpe, Kerstin A.: Videoüberwachung in Bürogebäuden, DuD 2015, S. 172-175.

Zwick, Detlev/Bonsu, Samuel K./Darmody, Aron: Putting Consumers to Work „Co-creation" and new marketing govern-mentality, Journal of Consumer Culture 2008, Vol. 8, Nr. 2, p. 163-196.

GERICHTSENTSCHEIDUNGEN

Reichsgericht

RG, Urt. v. 13.11.1933 (II 579/33), RGSt 67, 351

RG, Urt. v. 29.4.1930 (II 355/29), RGZ 128, 330

RG, Urt. v. 26.6.1929 (I 97/29), RGZ 125, 80

RG, Urt. v. 28.10.1910 (II 688/09), RGZ 74, 308

RG, Urt. v. 28.12.1899 (VI. 259/99), RGZ 45, 170

RG, Urt. v. 2.5.1895 (1164/95), RGSt 27, 198

Europäischer Gerichtshof für Menschenrechte

EGMR, Urt. v. 12.7.2013 (63737/00), Reports 2003-IX Nr. 38, http://hudoc.echr.coe.int/eng?i=001-61228 (7.11.2015)

EGMR, Urt. v. 7.2.2012 (40660/08 u. 60641/08), ZUM 2012, 551

EGMR, Urt. v. 20.12.2005 (71611/01), http://hudoc.echr.coe.int/fre?i=001 -71735 (7.11.2015)

EGMR, Urt. v. 24.6.2004 (59320/00), GRUR 2004, 1051

EGMR, Urt. v. 28.1.2003 (44647/98), http://hudoc.echr.coe.int/eng?i=001-60898 (7.11.2015)

EGMR, Beschl. v. 14.1.1998 (32200/96, 32201/96), http://hudoc.echr.coe.int/eng?i=001-88070 (7.11.2015)

EGMR, Beschl. v. 27.11.1996 (28122/95), http://hudoc.echr.coe.int/eng?i=001-3402 (7.11.2015)

Europäischer Gerichtshof

EuGH, Urt. v. 6.10.2015 (C-362/14), MMR 2015, 753

EuGH, Urt. v. 11.12.2014 (C 212/13), DuD 2015, 195

EuGH, Urt. v. 13.5.2014 (C-131/12), NJW 2014, 2257

EuGH, Urt. v. 8.4.2014 (C-293/12, C-594/12), NJW 2014, 2169

EuGH, Urt. v. 24.11.2011 (C-468/10 u. C-469/10), NZA 2011, 1409

EuGH, Urt. v. 29.1.2008 (C-275/06), EuZW 2008, 113

EuGH, Urt. v. 6.11.2003 (C-101/01), MMR 2004, 95

EuGH, Urt. v. 6.11.2003 (C-101/01), EuR 2004, 291

EuGH, Urt. v. 20.5.2003 (Rs. C-465/00, C-138/01 u. C-139/01), EuR 2004, 276

Bundesverfassungsgericht

BVerfG, Beschl. v. 24.7.2015 (1 BvR 2501/13), ZUM 2015, 986

BVerfG, Beschl. v. 20.5.2011 (2 BvR 2072/10), NJW 2011, 2783

BVerfG, Beschl. v. 10.12.2010 (1 BvR 1739/04), NJW 2011, 1859

BVerfG, Beschl. v. 9.3.2010 (1 BvR 1891/05), NJW-RR 2010, 1195

BVerfG, Urt. v. 2.3.2010 (1 BvR 256/08, 1 BvR 263/08 u. 1 BvR 586/08), BVerfGE 125, 260

BVerfG, Beschl. v. 27.11.2008 (1 BvQ 46/08), NJW 2009, 350

BVerfG, Urt. v. 11.3.2008 (1 BvR 2074/05, 1 BvR 1254/07), BVerfGE 120 , 378

BVerfG, Urt. v. 27.2.2008 (1 BvR 370/07, 1 BvR 595/07), BVerfGE 120 , 274

BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07 u. 1 BvR 1606/07), BVerfGE 120, 180

BVerfG, Beschl. v. 26.2.2008 (1 BvR 1602/07, 1606/07 u. 1626/07), BVerfGE 120, 180

BVerfG, Beschl. v. 16.6.2007 (1 BvR 1550/03), BVerfGE 118, 168

BVerfG, Beschl. v. 13.6.2007 (1 BvR 1550/03), BVerfGE 118, 168

BVerfG, Beschl. v. 23.2.2007 (1 BvR 2368/06), NVwZ 2007, 688

BVerfG, Beschl. v. 21.1.2007 (1 BvR 382/05), NVwZ 2007, 805

BVerfG, Beschl. v. 2.5.2006 (1 BvR 507/01), NJW 2006, 2836

BVerfG, Beschl. v. 4.4.2006 (1 BvR 518/02), BVerfGE 115, 320

BVerfG, Urt. v. 15.2.2006 (1 BvR 357/05), BVerfGE 115, 751

BVerfG, Urt. v. 27.7.2005 (1 BvR 668/04), BVerfGE 113, 348

BVerfG, Beschl. v. 12.4.2005 (2 BvR 1027/02), BVerfGE 113, 29

BVerfG, Urt. v. 12.4.2005 (2 BvR 581/01), BVerfGE 112, 304

BVerfG, Beschl. v. 14.2.2005 (1 BvR 240/04), NJW 2005, 3271

BVerfG, Beschl. v. 14.10.2004 (2 BvR 1481/04), BVerfGE 111, 307

BVerfG, Beschl. v. 14.7.2004 (1 BvR 263/03), NJW 2004, 3619

BVerfG, Urt. v. 17.3.2004 (1 BvR 1266/00), BVerfGE 110, 177

BVerfG, Urt. v. 3.3.2004 (1 BvR 2378/98 u. 1 BvR 1084/99), BVerfGE 109, 279

BVerfG, Urt. v. 3.3.2004 (1 BvF 3/92), BVerfGE 110, 33

BVerfG, Urt. v. 5.2.2004 (2 BvR 2029/01), BVerfGE 108, 133

BVerfG, Urt. v. 12.3.2003 (1 BvR 330/96 u. 1 BvR 348/99), BVerfGE 107, 299

BVerfG, Beschl. v. 11.3.2003 (1 BvR 426/02), BVerfGE 107, 275

BVerfG, Urt. v. 9.10.2002 (1 BvR 330/96 u. 1 BvR 348/9), BVerfGE 106, 28

BVerfG, Beschl. v. 24.1.2001 (1 BvR 2623/95 u. 1 BvR 622/99), BVerfGE 103, 44

BVerfG, Beschl. v. 14.12.2000 (2 BvR 1741/99, 2 BvR 276/00 u. 2 BvR 2061/00), BVerfGE 103, 29

BVerfG, Beschl. v. 25.8.2000 (1 BvR 2707/95), ZUM 2001, 232

BVerfG, Urt. v. 15.12.1999 (1 BvR 653/96), BVerfGE 101, 361

BVerfG, Urt. v. 14.7.1999 (1 BvR 2226/94, 2420/95 u. 2437/95), BVerfGE 100, 313

BVerfG, Beschl. v. 29.11.1995 (1 BvR 2203/95), NJW 1996, 651

BVerfG, Beschl. v. 10.10.1995 (1 BvR 1476/91), BVerfGE 93, 266

BVerfG, Beschl. v. 14.7.1994 (1 BvR 1595/92 u. 1606/92), BVerfGE 91, 125

BVerfG, Beschl. v. 13.4.1994 (1 BvR 23/94), BVerfGE 90, 1

BVerfG, Beschl. v. 9.2.1994 (1 BvR 1687/92), BVerfGE 90, 27

BVerfGE, Beschl. v. 19.10.1993 (1 BvR 567 u. 1044/89), BVerfGE 89, 214

BVerfG, Beschl. v. 20.10.1992 (1 BvR 698/89), BVerfGE 87, 209

BVerfG, Beschl. v. 25.3.1992 (1 BvR 1430/88), BVerfGE 85, 386

BVerfG, Beschl. v. 19.12.1991 (1 BvR 382/85), NJW 1992, 815

BVerfG, Beschl. v. 11.6.1991 (1 BvR 239/90), BVerfGE 84, 192

BVerfG, Beschl. v. 24.7.1990 (1 BvR 1244/87), MMR 1990, 1162

BVerfG, Beschl. v. 29.5.1990 (1 BvL 20, 26/84 u. 4/86), BVerfGE 82, 60

BVerfG, Beschl. v. 7.3.1990 (1 BvR 266/86 u. 1 BvR 913/87), BVerfGE 81, 278

BVerfG, Beschl. v. 7.2.1990 (1 BvR 26/84), BVerfGE 81, 242

BVerfG, Beschl. v. 14.9.1989 (2 BvR 1062/87), BVerfGE 80, 367

BVerfGE, Beschl. v. 3.6.1987 (1 BvR 313/85), BVerfGE 75, 369

BVerfG, Beschl. v. 5.5.1987 (1 BvR 1113/85), BVerfGE 75, 318

BVerfG, Beschl. v. 26.3.1987 (2 BvR 589/79 u.a.), BVerfGE 74, 358

BVerfG, Beschl. v. 22.10.1986 (2 BvR 197/83), BVerfGE 73, 339

BVerfG, Beschl. v. 24.4.1986 (2 BvR 1146/85), BVerfGE 72, 105

BVerfG, Beschl. v. 23.4.1986 (2 BvR 487/80), BVerfGE 73, 261

BVerfG, Beschl. v. 17.7.1984 (1 BvR 816/82), BVerfGE 67, 213

BVerfG, Urt. v. 15.12.1983 (1 BvR 209/83), BVerfGE 65, 1

BVerfG, Beschl. v. 8.2.1983 (1 BvL 20/81), BVerfGE 63, 131

BVerfG, Beschl. v. 22.6.1982 (1 BvR 1376/79), BVerfGE 61, 1

BVerfG, Beschl. v. 18.8.1981 (2 BvR 166/81), NJW 1982, 375

BVerfG, Beschl. v. 5.2.1981 (2 BvR 646/80), BVerfGE 57, 170

BVerfG, Beschl. v. 14.1.1981 (1 BvR 612/72), BVerfGE 56, 54

BVerfG, Beschl. v. 3.6.1980 (1 BvR 185/77), BVerfGE 54, 148

BVerfG, Beschl. v. 23.5.1980 (2 BvR 854/79), BVerfGE 54, 143

BVerfG, Beschl. v. 3.10.1979 (1 BvR 726/78), BVerfGE 52, 203

BVerfG, Beschl. v. 25.7.1979 (2 BvR 878/74), BVerfGE 52, 131

BVerfG, Beschl. v. 11.10.1978 (1 BvR 16/72), BVerfGE 49, 286

BVerfG, Urt. v. 8.8.1978 (2 BvL 8/77), BVerfGE 49, 89

BVerfG, Beschl. v. 21.12.1977 (1 BvL 1/75), BVerfGE 47, 46

BVerfG, Urt. v. 21.6.1977 (1 BvL 14/76), BVerfGE 45, 187

BVerfG, Beschl. v. 24.5.1977 (2 BvR 988/75), BVerfGE 44, 353

BVerfG, Beschl. v. 2.3.1977 (2 BvR 1319/76), BVerfGE 44, 197

BVerfG, Urt. v. 25.2.1975 (1 BvF 1 - 6/74), BVerfGE 39, 1

BVerfG, Beschl. v. 29.5.1974 (2 BvL 52/71), BVerfGE 37, 371

BVerfG, Urt. v. 5.6.1973 (1 BvR 536/72), BVerfGE 35, 202

BVerfG BVerfGE 35, 79 v. 29.5.1973 (1 BvR 424/71 u. 325/72), BVerfGE 35, 1176

BVerfGE, Beschl. v. 11.4.1973 (2 BvR 701/72), BVerfGE 1973, 35

BVerfG, Beschl. v. 27.3.1973 (2 BvR 684/72), BVerfGE 35, 307

BVerfG, Urt. v. 14.2.1973 (1 BvR 112/65), BVerfGE 34, 269

BVerfG, Beschl. v. 14.2.1973 (1 BvR 112/65), BVerfGE 1973, 269

BVerfG, Beschl. v. 31.1.1973 (2 BvR 454/71), BVerfGE 34, 238

BVerfG, Beschl. v. 8.3.1972 (2 BvR 28/71), BVerfGE 32, 373

BVerfG, Beschl. v. 24.2.1971 (1 BvR 435/68), BVerfGE 30, 173

BVerfG, Urt. v. 15.12.1970 (2 BvF 1/69), BVerfGE 30, 1

BVerfG, Beschl. v. 26.5.1970 (1 BvR 83/69, 1 BvR 244/69 u. 1 BvR 345/69), BVerfGE 28, 243

BVerfG, Beschl. v. 15.1.1970 (1 BvR 13/68), BVerfGE 27, 344

BVerfG, Beschl. v. 3.10.1969 (1 BvR 46/65), BVerfGE 27, 71

BVerfG, Beschl. v. 16.7.1969 (1 BvL 19/63), BVerfGE 27, 1

BVerfG, Urt. v. 5.8.1966 (1 BvR 586/62, 1 BvR 610/63 u. 1 BvR 512/64), BVerfGE 20, 162

BVerfG, Urt. v. 15.1.1958 (1 BvR 400/57), BVerfGE 7, 198

BVerfG, Urt. v. 10.5.1957 (1 BvR 550/52), BVerfGE 6, 389

BVerfG, Urt. v. 16.1.1957 (1 BvR 253/56), BVerfGE 6, 32

BVerfG, Urt. v. 13.6.1952 (1 BvR 137/52), BVerfGE 1, 332

Verwaltungsgerichte

BVerwG, Urt. v. 22.10.2014 (6 C 7/13), NVwZ 2015, 906

BVerwG, Urt. v. 15.6.1999 (2 WD 34/98), BVerwGE 113, 340

BVerwG, Urt. v. 31.8.1988 (6 P 35.85), BVerwGE 80, 143

BVerwG, Urt. v. 29.4.1988 (7 C 33/87), NJW 1988, 2396

BVerwG, Urt. v. 27.5.1983 (4 C 40, 44 u. 45/81), BVerwGE 67, 206

BVerwG, Urt. v. 15.12.1981 (1 C 232/79), BVerwGE 64, 274

BVerwG, Urt. v. 16.9.1980 (1 C 52/75), BVerwGE 61, 15

BVerwG, Urt. v. 3.12.1974 (I C 30.71), BVerwGE 47, 247

OVG Lüneburg, Urt. v. 29.9.2014 (11 LC 114/13), NJW 2015, 502

VGH München, Beschl. v. 16.10.2014 (10 ZB 13.2620), NVwZ-RR 2015, 104

VGH München, Beschl. v. 29.2.2012 (12 C 12.264), NZA-RR 2012, 302

VGH Baden-Württemberg, Urt. v. 19.8.2010 (1 S 2266/09), ZUM-RD 2011, 126

OVG Münster, Urt. v. 8.5.2009 (16 A 3375/07), RDV 2009, 232

VGH Mannheim, Urt. v. 10.7.2000 (1 S 2239/99), NVwZ 2001, 1292

VG Schwerin, Beschl. v. 18.6.2015 (6 B 1637/15 SN), ZD 2015, 448

VG Ansbach, Urt. v. 12.8.2014 (AN 4 K 13.01634), SVR 2015, 235

Arbeitsgerichte

BAG, Urt. v. 11.12.2014 (8 AZR 1010/13), ZUM 2015, 604

BAG, Urt. v. 21.6.2012 (2 AZR 153/11), NJW 2012, 3594

BAG, Beschl. v. 14.12.2004 (1 ABR 34/03), NJOZ 2005, 2708

BAG, Urt. v. 27.3.2003 (2 AZR 51/02), NJW 2003, 3436

BAG, Urt. v. 15.5.1991 (5 AZR 115/90), BAGE 68, 52

LAG Rheinland-Pfalz, Urt. v. 7.11.2013 (10 SaGa 3/13), ZD 2013, 631

LAG Hamm, Urt. v. 11.7.2013 (11 Sa 312/13), ZD 2014, 204

LAG Hamm, Beschl. v. 16.9.2011 (10 TaBV 17/11), ZD 2012, 183

LAG Hamm, Urt. v. 15.7.2011 (10 Sa 1781/10), BeckRS 2011, 79152

LAG Köln, Urt. v. 18.11.2010 (6 Sa 817/10), NZA-RR 2011, 241

LAG Hessen, Urt. v. 25.10.2010 (7 Sa 1586/09), MMR 2011, 346

Zivilgerichte

BGH, Urt. v. 21.4.2015 (VI ZR 245/14), BeckRS 2015, 10534

BGH, Urt. v. 11.11.2014 (VI ZR 9/14), ZUM 2015, 329

BGH, Beschl. v. 28.10.2014 (VI ZR 135/13), BeckRS 2014, 20158

BGH, Urt. v. 30.9.2014 (VI ZR 490/12), ZD 2015, 227

BGH, Urt. v. 18.10.2011 (VI ZR 5/10), ZUM 2012, 140

BGH, Urt. v. 8.4.2011 (V ZR 210/10), NJW-RR 2011, 949

BGH, Urt. v. 13.1.2011 (III ZR 146/10), MMR 2011, 341

BGH, Urt. v. 17.12.2010 (V ZR 45/10), GRUR 2011, 323

BGH, Urt. v. 15.9.2010 (2 StR 400/10), NStZ-RR 2010, 374

BGH, Beschl. v. 11.8.2010 (1 StR 351/10), NStZ-RR 2011, 238

BGH, Urt. v. 12.5.2010 (I ZR 121/08), MMR 2010, 565

BGH, Urt. v. 16.3.2010 (VI ZR 176/09), NJW 2010, 1533

BGH, Urt. v. 29.10.2009 (I ZR 65/07), NJW-RR 2010, 855

BGH, Urt. v. 25.6.2009 (5 StR 141/09), NStZ 2009, 626

BGH, Urt. v. 23.6.2009 (VI ZR 196/08), BGHZ 181, 328

BGH, Urt. v. 23.6.2009 (VI ZR 196/08), MMR 2009, 608

BGH, Urt. v. 23.6.2009 (VI ZR 232/08), NJW 2009, 2823

BGH, Urt. v. 26.5.2009 (VI ZR 191/08), ZUM-RD 2009, 429
BGH, Beschl. v. 20.5.2009 (I ZR 218/07), GRUR 2009, 980
BGH, Urt. v. 28.10.2008 (VI ZR 307/07), BGHZ 178, 213
BGH, Urt. v. 24.6.2008 (VI ZR 156/06), GRUR 2008, 1017
BGH, Urt. v. 19.6.2007 (VI ZR 12/06), GRUR 2007, 899
BGH, Urt. v. 6.3.2007 (VI ZR 51/06), GRUR 2007, 527
BGH, Urt. v. 25.1.2007 (I ZR 133/04), NJW-RR 2007, 1335
BGH, Urt. v. 21.6.2005 (VI ZR 122/04), GRUR 2005, 788
BGH, Urt. v. 19.10.2004 (VI ZR 292/03), NJW 2005, 594
BGH, Urt. v. 5.10.2004 (VI ZR 255/03), NJW 2005, 215
BGH, Urt. v. 9.12.2003 (VI ZR 373/02), GRUR 2004, 438
BGH, Urt. v. 12.2.2003 (1 StR 403/02), NJW 2003, 1955
BGH, Urt. v. 9.5.2001 (3 StR 542/00), NStZ 2001, 530
BGH, Urt. v. 10.2.2000 (4 StR 558/99), BGHSt 45, 378
BGH, Urt. v. 1.12.1999 (I ZR 49/97), BGHZ 143, 214
BGH, Beschl. v. 16.4.1998 (4 StR 114/98), NStZ 1998, 508
BGH, Urt. v. 3.6.1997 (VI ZR 133/96), NJW 1998, 155
BGH, Urt. v. 19.12.1995 (VI ZR 15/95), NJW 1996, 1128
BGH, Urt. v. 25.4.1995 (VI ZR 272/94), NJW 1995, 1955
BGH, Urt. v. 15.11.1994 (VI ZR 56/94), BGHZ 128, 1
BGH, Urt. v. 12.7.1994 (VI ZR 1/94), GRUR 1994, 913
BGH, Urt. v. 8.2.1994 (VI ZR 286/93), NJW 1994, 1281
BGH, Urt. v. 27.1.1994 (I ZR 326/91), NJW 1994, 2289
BGH, Urt. v. 3.11.1993 (VIII ZR 106/93), BGHZ 124, 39
BGH, Urt. v. 3.2.1993 (3 StR 356/92), BGHSt 39, 133
BGH, Urt. v. 4.12.1992 (6 U 32/92), NJW-RR 1993, 753
BGH, Urt. v. 20.5.1992 (VIII ZR 240/91), NJW 1992, 2348
BGH, Urt. v. 25.2.1992 (X ZR 41/90), BGHZ 117, 264
BGH, Urt. v. 10.7.1991 (VIII ZR 296/90), BGHZ 115, 123
BGH, Urt. v. 11.6.1991 (1 StR 242/91), BeckRS 1991, 31085305
BGH, Urt. v. 14.5.1991 (1 StR 699/90), NJW 1991, 2651

BGH, Urt. v. 25.4.1991 (I ZR 283/89), NJW-RR 1991, 1512
BGH, Urt. v. 21.6.1990 (1 StR 477/89), BGHSt 37, 55
BGH, Urt. v. 8.11.1989 (I ZR 55/88), NJW-RR 1990, 359
BGH, Urt. v. 8.6.1989 (I ZR 178/87), NJW 1989, 2820
BGH, Urt. v. 9.3.1989 (I ZR 54/87), NJW 1989, 2251
BGH, Urt. v. 28.2.1989 (1 StR 741/88), NJW 1989, 3027
BGH, Urt. v. 13.10.1987 (VI ZR 83/87), NJW 1988, 1016
BGH, Urt. v. 10.3.1987 (VI ZR 244/85), NJW 1987, 2667
BGH, Urt. v. 9.4.1986 (3 StR 551/85), BGHSt 34, 39
BGH, Urt. v. 22.1.1985 (VI ZR 28/83), NJW 1985, 1617
BGH, Urt. v. 22.5.1984 (VI ZR 105/82), BGHZ 91, 233
BGH, Beschl. v. 26.4.1983 (1 StR 28/83), NJW 1983, 2710
BGH, Urt. v. 16.3.1983 (2 StR 775/82), NJW 1983, 1569
BGH, Urt. v. 17.2.1982 (VIII ZR 29/81), NJW 1982, 1397
BGH, Urt. v. 24.11.1981 (VI ZR 164/79), NJW 1982, 277
BGH, Urt. v. 19.5.1981 (VI ZR 273/79), BGHZ 80, 311
BGH, Urt. v. 25.11.1980 (1 StR 563/80), NStZ 1981, 138
BGH, Urt. v. 18.11.1980 (VI ZR 151/78), NJW 1981, 745
BGH, Urt. v. 23.10.1979 (VI ZR 230/77), NJW 1980, 881
BGH, Urt. v. 24.7.1979 (1 StR 249/79), NJW 1980, 2263
BGH, Urt. v. 26.6.1979 (VI ZR 108/78), GRUR 1979, 732
BGH, Urt. v. 19.12.1978 (VI ZR 137/77), BGHZ 73, BGHZ 73
BGH, Urt. v. 21.12.1977 (2 StR 421/77), BGHSt 27, 313
BGH, Urt. v. 10.5.1977 (1 StR 167/77), NJW 1977, 1460
BGH, Beschl. v. 12.12.1975 (2 StR 451/75), BGHSt 26, 256
BGH, Urt. v. 15.5.1975 (4 StR 71/75), BGHSt 26, 143
BGH, Urt. v. 24.8.1972 (4 StR 308/72), BGHSt 25, 10
BGH, Urt. v. 7.6.1971 (I ZR 32/70), BGHZ 56, 256
BGH, Urt. v. 26.1.1971 (VI ZR 95/70), NJW 1971, 698
BGH, Urt. v. 26.2.1969 (3 StR 322/68), NJW 1969, 802
BGH, Urt. v. 20.3.1968 (I ZR 44/66), BGHZ 50, 133

BGH, Urt. v. 16.9.1966 (VI ZR 268/64), GRUR 1967, 205
BGH, Urt. v. 21.6.1966 (VI ZR 261/64), NJW 1966, 1617
BGH, Urt. v. 8.11.1965 (8 StE 1/65), BGHSt 20, 342
BGH, Urt. v. 15.1.1965 (I b ZR 44/63), NJW 1965, 1374
BGH, Urt. v. 21.10.1963 (AnwSt (R) 2/63), NJW 1964, 165
BGH, Urt. v. 5.3.1963 (VI ZR 55/62), BGHZ 39, 124
BGH, Urt. v. 26.6.1962 (5 StR 180/62), NJW 1962, 1831
BGH, Urt. v. 10.11.1961 (I ZR 78/60), GRUR 1962, 211
BGH, Urt. v. 19.9.1961 (VI ZR 259/60), BGHZ 35, 363
BGH, Urt. v. 14.6.1960 (1 StR 683/59), NJW 1960, 1580
BGH, Urt. v. 5.12.1958 (IV ZR 95/58), BGHZ 29, 33
BGH, Urt. v. 20.5.1958 (VI ZR 104/57), BGHZ 27, 284
BGH, Urt. v. 14.2.1958 (I ZR 151/56), BGHZ 26, 349
BGH, Urt. v. 10.5.1957 (I ZR 234/55), BGHZ 24, 200
BGH, Urt. v. 2.4.1957 (VI ZR 9/56), BGHZ 24, 72
BGH, Urt. v. 8.5.1956 (I ZR 62/54), BGHZ 20, 345
BGH, Urt. v. 26.11.1954 (I ZR 266/52), BGHZ 15, 249
BGH, Urt. v. 25.5.1954 (I ZR 211/53), BGHZ 13, 334
BGH, Urt. v. 19.11.1953 (3 StR 17/53), BGHSt 5, 254
BGH, Urt. v. 28.10.1953 (II ZR 149/52), BGHZ 10, 385
BGH, Urt. v. 23.4.1953 (3 StR 219/52), BGSt 4, 236
BGH, Urt. v. 23.4.1953 (3 StR 219/52), BGHSt 4, 236
BGH, Urt. v. 19.12.1952 (1 StR 2/52), BGHSt 3, 357
BGH, Urt. v. 1.7.1952 (1 StR 119/52), BGHSt 3, 194
BGH, Urt. v. 6.6.1952 (1 StR 708/51), BGHSt 3, 105
BGH, Urt. v. 14.2.1952 (5 StR 1/52), BGHSt 3, 217
OLG Koblenz, Urt. v. 20.5.2014 (3 U 1288/13), ZUM 2015, 58
OLG Köln, Beschl. v. 28.5.2013 (III-1 RVs 81/13), NStZ-RR 2013, 308
OLG Köln, Urt. v. 26.3.2013 (15 U 149/12), ZUM 2013, 684
OLG Oldenburg, Urt. v. 12.3.2013 (1 A 3850/12), RDV 2013, 209
OLG Hamm, Urt. v. 20.9.2012 (4 U 85/12), K&R 2013, 53

OLG Brandenburg, Urt. v. 21.5.2012 (1 U 26/11), NJW-RR 2012, 1250
OLG Hamburg, Beschl. v. 5.4.2012 (3-14/12), ZUM-RD 2012, 462
OLG Hamburg, Urt. v. 18.1.2012 (5 U 51/11), MMR 2012, 605
OLG Hamburg, Beschl. v. 3.11.2010 (5 W 126/10), MMR 2011, 281
OLG Celle, Urt. v. 25.8.2010 (31 Ss 30/10), ZUM 2011, 341
OLG Düsseldorf, Urt. v. 8.3.2010 (I-20 U 188/09), BeckRS 2010, 07686
OLG Köln, Urt. v. 9.2.2010 (15 U 107/09), ZUM 2010, 706
OLG Köln, Beschl. v. 30.10.2008 (21 U 22/08), NJW 2009, 1827
OLG Hamburg, Urt. v. 22.7.2008 (7 U 21/0), NJW 2009, 784
KG, Urt. v. 2.3.2007 (9 U 212/06), ZUM 2007, 475
OLG Düsseldorf, Beschl. v. 5.1.2007 (3 Wx 199/06), NJW 2007, 780
KG, Urt. v. 13.6.2006 (9 U 251/05), ZUM-RD 2006, 552
OLG Frankfurt a.M., Beschl. v. 22.5.2006 (11 W 13/06), GRUR-RR 2007, 30
OLG Karlsruhe, Urt. v. 7.4.2006 (14 U 134/05), NJW-RR 2006, 987
OLG Frankfurt a.M., Urt. v. 15.6.2004 (11 U 5/04), ZUM-RD 2004, 576
OLG Hamburg, Urt. v. 13.1.2004 (7 U 41/03), ZUM 2004, 309
OLG Stuttgart, Urt. v. 8.12.2003 (4 Ss 469/03), NJW 2004, 622
BayObLG, Beschl. v. 25.7.2002 (5 StR RR 209/2002), NStZ-RR 2002, 336
KG Berlin, Beschl. v. 26.6.2002 (24 W 309/01), NJW 2002, 2798
OLG Nürnberg, Urt. v. 11.6.2002 (1 U 3939/01), NJW-RR 2002, 1471
OLG Frankfurt a.M., Urt. v. 20.2.2002 (23 U 212/01), NJW-RR 2003, 37
OLG Karlsruhe, Urt. v. 8.11.2001 (12 U 180/01), NZM 2002, 703
OLG Frankfurt a.M., Urt. v. 13.12.2000 (13 U 204/98), CR 2001, 294
OLG Hamburg, Urt. v. 10.10.2000 (7 U 138/99), OLG Report 2001, 139
OLG Karlsruhe, Urt. v. 8.12.1998 (6 U 64/97), BeckRS 1998, 30996545
OLG Karlsruhe, Urt. v. 14.10.1998 (6 U 120–97), NJW-RR 1999, 169
KG, Urt. v. 28.8.1998 (25 U 7198/97), ZUM-RD 1998, 554
OLG Hamm, Beschl. v. 8.1.1998 (2 Ss 1526/97), NStZ 1998, 370
OLG Düsseldorf, Urt. v. 5.5.1997 (5 U 82/96), NJW-RR 1998, 241
OLG Hamburg, Urt. v. 25.6.1996 (7 U 177/95), ZUM-RD 1997, 1

OLG Düsseldorf, Beschl. v. 25.1.1995 (1 Ws 904, 969/94), NJW 1995, 975

OLG Nürnberg, Beschl. v. 24.10.1994 (Ws 936/94), NJW 1995, 974

OLG Frankfurt a.M., Urt. v. 25.8.1994 (6 U 296/93), NJW 1995, 878

OLG Düsseldorf, Beschl. v. 15.10.1993 (2 Ss 175/93), NJW 1994, 1971

OLG Frankfurt a.M., Urt. v. 1.10.1993 (10 U 181/92), NJW 1994, 946

OLG Köln, Urt. v. 16.6.1992 (15 U 47/92), BeckRS 1992, 05031

OLG Köln, Urt. v. 12.6.1992 (19 U 154/91), NJW 1993, 793

BayObLG, Beschl. v. 12.12.1991 (RReg. 4 St 158/91), NJW 1992, 1777

BayObLG, Beschl. v. 28.2.1991 (RReg. 5 St 14/91), NJW 1991, 2031

OLG Karlsruhe, Urt. v. 18.8.1989 (14 U 105/88), GRUR 1989, 823

OLG Hamburg, Urt. v. 13.7.1989 (3 U 30/89), GRUR 1990, 35

OLG München, Urt. v. 17.3.1989 (21 U 4729/88), NJW-RR 1990, 999

OLG Karlsruhe, Urt. v. 18.11.1988 (14 U 285/87), NJW 1989, 401

OLG Oldenburg, Urt. v. 14.11.1988 (13 U 72/88), GRUR 1989, 344

OLG Köln, Urt. v. 13.10.1988 (18 U 37/88), NJW 1989, 720

BayObLG, Beschl. v. 15.3.1988 (RReg. 1 St 49/88), NStZ 1988, 408

OLG München, Urt. v. 13.11.1987 (21 U 2979/87), NJW 1988, 915

OLG Frankfurt a.M., Urt. v. 21.1.1987 (21 U 164/86), NJW 1987, 1087

BayObLG, Urt. v. 30.5.1986 (RReg. 5 St 43/86), BayObLGSt 1986, 52

OLG Düsseldorf, Urt. v. 12.7.1985 (15 U 240/84), ZIP 1985, 1319

OLG Karlsruhe, Urt. v. 4.7.1985 (1 Ss 40/85), NJW 1986, 1358

OLG Celle, Urt. v. 8.8.1984 (13 U 44/84), afp 1984, 236

OLG Stuttgart, Beschl. v. 2.3.1984 (3 Ss (14) 75/84), NJW 1984, 1694

OLG Hamburg, Urt. v. 7.7.1983 (3 U 7/83), AfP 1983, 466

OLG Stuttgart, Urt. v. 16.12.1981 (4 U 88/81), NJW 1982, 652

OLG Karlsruhe, Urt. v. 1.10.1981 (1 Ss 200/81), NStZ 1982, 123

KG, Urt. v. 5.7.1979 (12 U 1277/79), NJW 1980, 894

OLG Karlsruhe, Urt. v. 9.11.1978 (2 Ss 241/78), NJW 1979, 1513

OLG Frankfurt a.M., Urt. v. 28.3.1977 (2 Ss 2/77), NJW 1977, 1547

OLG Karlsruhe, Beschl. v. 19.10.1973 (1 Ws 177/73), NJW 1974, 709

OLG Nürnberg, Urt. v. 26.10.1971 (3 U 68/71), GRUR 1973, 40

OLG München, Urt. v. 14.5.1970 (1 U 721/70), NJW 1970, 1745

OLG Düsseldorf, Urt. v. 30.9.1969 (20 U 80/69), GRUR 1970, 618

OLG Düsseldorf, Beschl. v. 23.11.1965 (1 Ws 754/65), NJW 1966, 214

OLG Frankfurt, Urt. v. 9.1.1958 (6 U 77/57), GRUR 1958, 508

OLG München, Urt. v. 13.4.1956 (8 U 2024/55), NJW 1956, 1075

LG Detmold, Urt. v. 8.7.2015 (10 S 52/15), ZD 2015, 530

LG München I, Urt. v. 27.5.2015 (37 O 11673/14), MMR 2015, 660

LG Heilbronn, Urt. v. 17.2.2015 (I 3 S 19/14), ZD 2015, 233

LG Bonn, Urt. v. 7.1.2015 (5 S 47/14), ZD 2015, 434

LG Frankfurt a.M., Beschl. v. 30.9.2014 (2-03 O 378/14), n.v.

LG Essen, Urt. v. 10.7.2014 (4 O 157/14), BeckRS 2014, 17008

LG Frankfurt a.M., Urt. v. 20.5.2014 (2-03 O 189/13), BecksRS 2014, 19319

LG Frankfurt/Oder, Urt. v. 25.6.2013 (16 S 251/12), BeckRS 2013, 12059

LG Düsseldorf, Urt. v. 16.11.2011 (12 O 438/10), ZUM-RD 2012, 407

LG Aschaffenburg, Urt. v. 31.10.2011 (14 O 21/11), NJW 2012, 787

LG Hamburg, Urt. v. 20.9.2010 (325 O 111/10), MMR 2011, 488

LG Hamburg, Urt. v. 16.6.2010 (325 O 448/09), ZUM-RD 2010, 623

LG München I, Urt. v. 8.4.2010 (17 HK O 138/10), CR 2011, 830

LG Hamburg, Urt. v. 27.2.2009 (324 O 703/08), BeckRS 2009, 18575

LG Berlin, Urt. v. 4.9.2007 (27 O 591/07), ZUM 2007, 866

LG Bielefeld, Urt. v. 17.4.2007 (20 S 123/06), NJW-RR 2008, 327

LG Kiel, Urt. v. 27.4.2006 (4 O 251/05), NJW 2007, 1002

LG Frankfurt a.M., Urt. v. 19.1.2006 (2/03 O 468/05), ZUM-RD 2006, 357

LG Bonn, Urt. v. 16.11.2004 (8 S 139/04), NJW-RR 2005, 1067

LG Köln, Urt. v. 3.11.2004 (28 O 731/03), ZUM-RD 2005, 351

LG Berlin, Urt. v. 2.7.2004 (15 O 653/03), MMR 2004, 688

LG Köln, Urt. v. 21.4.2004 (28 O 141/04), ZUM 2004, 495

LG München I, Urt. v. 11.9.2003 (7 O 20974/02), ZUM-RD 2003, 601

LG München I, Urt. v. 30.7.2003 (21 O 4369/03), NJW 2004, 617

LG Darmstadt, Urt. v. 17.3.1999 (8 O 42/99), NZM 2000, 360

LG Darmstadt, Urt. v. 24.9.1998 (15 O 204/98), RDV 1999, 28

LG Hamburg, Urt. v. 8.5.1998 (324 O 736/97), ZUM 1998, 852

LG Itzehoe, Urt. v. 11.9.1997 (7 (9) 0 51–96), NJW-RR 1999, 1394

LG München I, Urt. v. 10.7.1996 (21 O 23932/95), ZUM-RD 1998, 18

LG Köln, Urt. v. 29.6.1994 (28 S 3/94), NJW-RR 1995, 1175

LG Oldenburg, Beschl. v. 21.4.1988 (5 S 1656/87), GRUR 1988, 694

LG Oldenburg, Beschl. v. 23.1.1986 (5 O 3667/85), GRUR 1986, 464

LG Göttingen, Urt. v. 16.11.1978 (2 O 152/78), NJW 1979, 601

AG Nürnberg, Urt. v. 8.5.2015 (18 C 8938/14), BeckRS 2015, 14846

AG Dinslaken, Urt. v. 5.3.2015 (34 C 47/14), ZD 2015, 531

AG Nienburg, Urt. v. 20.1.2015 (4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14)), BeckRS 2015, 07708

AG München, Beschl. v. 13.8.2014 (345 C 5551/14), BeckRS 2014, 16291

AG München, Urt. v. 6.6.2013 (343 C 4445/13), NJW-RR 2014, 413

AG Göttingen, Urt. v. 4.5.2011 (62 Ds 51 Js 9946/10 (106/11)), MMR 2011, 626

AG Kerpen, Urt. v. 25.11.2010 (102 C 108/10), BeckRS 2011, 10636

AG Mannheim, Urt. v. 11.7.2008 (3 C 154/08), BeckRS 2008, 13697

AG Berlin-Mitte, Urt. v. 18.12.2003 (16 C 427/02), NZM 2004, 318

AG Aachen, Urt. v. 11.11.2003 (10 C 386/03), NZM 2004, 339

AG Köln, Urt. v. 20.12.1994 (208 C 57/94), NJW-RR 1995, 1226

Ausländische Gerichte

Kyllo v. United States, 533 U.S. 27 (2001)