Oldenburger Forum der Rechtswissenschaften 7

Jürgen Taeger (Hrsg.)

Chancen und Risiken von Smart Cams im öffentlichen Raum

Nomos

Oldenburger Forum der Rechtswissenschaften

Schriftenreihe des Instituts für Rechtswissenschaften
der Carl von Ossietzky Universität

Herausgegeben von
Professor Dr. Dr. Volker Boehme-Neßler
Professor Dr. Christiane Brors
Professor Dr. Christine Godt
Professor Dr. Jürgen Taeger

Band 7

Jürgen Taeger (Hrsg.)

Chancen und Risiken von Smart Cams im öffentlichen Raum

Nomos

Das dieser Tagungsdokumentation zugrundeliegende Vorhaben „Smart Cams im öffentlichen Raum“ (ChaRiSma) wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16/1664 gefördert.

Bundesministerium
für Bildung
und Forschung

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

ISBN 978-3-8487-4271-4 (Print)
ISBN 978-3-8452-8534-4 (ePDF)

1. Auflage 2017
© Nomos Verlagsgesellschaft, Baden-Baden 2017. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der photomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Vorwort

Die Videoüberwachung hat in den letzten Jahren ohne Zweifel erheblich zugenommen. Die Anzahl der stationären Videoüberwachungsanlagen in Städten und Gemeinden ist genauso gewachsen wie die in Unternehmen und vor privaten Gebäuden. Daneben treten immer mehr neue Formen von sogenannten Smart Cams in Erscheinung. Dazu werden beispielsweise Datenbrillen, Videokameras an Drohnen, die Dashcams in Fahrzeugen oder auch Body Cams an Polizeiuniformen gezählt. Die Einsatzzwecke sind vielfältig. Smart Cams dienen privatem Freizeitvergnügen oder der Beweissicherung bei Verkehrsunfällen. Das Hauptargument für die stationären und mobilen Videoüberwachungsanlagen ist die Verbesserung der Sicherheitslage. Es werden der Videoüberwachung präventive Wirkungen zugesprochen und im Fall eines gefilmten Delikts bessere Aufklärungsmöglichkeiten und Beweiserleichterungen im Prozess. Die Gesellschaft scheint bei der Bewertung der Smart Cams gespalten zu sein. Einerseits wird der Zugewinn an Sicherheit begrüßt. Andererseits ist die Sorge spürbar, die Zunahme an Kameras könnte die Freiheitsrechte erheblich einschränken und Persönlichkeitsrechte verletzen.

Die Deutsche Bahn AG ist mit diesen Fragen unmittelbar konfrontiert. Sie betreibt in Kooperation mit der Bundespolizei an Bahnhöfen zahlreiche Videokameras. Auch in Bussen und Regionalzügen der Deutschen Bahn und anderer Verkehrsträgern werden Videokameras fast standardmäßig eingebaut. Die Aufsichtsbehörden sehen diese Entwicklung kritisch, erkennen aber an, dass Erfahrungen mit dem Einsatz von Body Cams bei der Bundespolizei und bei Sicherheitskräften der DB Security gesammelt werden müssen. Der *Datenschutzbeirat der Deutschen Bahn Konzern* befasst sich regelmäßig mit der Videoüberwachung an Bahnhöfen und in Verkehrsmitteln sowie mit den Body Cams der Sicherheitskräfte der Bahn und mit Videoüberwachung über Abstellgleisen, auf denen Sprayer erheblichen Schaden an Waggons anrichten können.

An der Carl von Ossietzky Universität Oldenburg werden die Fragen, die mit dem Einsatz von Smart Cams verbunden sind, in einem vom Bundesministerium für Bildung und Forschung geförderten Verbundprojekt mit dem Oldenburger Institut für Informatik (OFFIS) aus rechtlicher, technischer und sozialwissenschaftlicher Perspektive wissenschaftlich erforscht. Es lag daher nahe, die beide Seiten beschäftigenden Themen in einem gemeinsamen Workshop zu diskutieren.

Wir legen hiermit die Dokumentation dieses im Juni 2016 im Bahntower am Potsdamer Platz veranstalteten Workshops vor, wobei die vorbereiteten Referate als wissenschaftliche Beiträge aufgenommen wurden.

Hinzuweisen ist abschließend, dass § 6b Abs. 1 BDSG mit Wirkung zum 29. April 2017 ein Satz angefügt wurde (BGBl. I S. 968), der bei den Beiträgen in diesem Band noch nicht berücksichtigt wurde.

Berlin/Oldenburg, im Mai 2017

Klaus-Dieter Hommel

Vorsitzender des Datenschutzbeirats der Deutschen Bahn Konzern

Prof. Dr. Jürgen Taeger

Wissenschaftlicher Leiter des Projekts Chancen und Risiken von Smart Cams im öffentlichen Raum

Inhaltsverzeichnis

Erster Tag

Vorwort 5

Begrüßung
Jürgen Taeger / Peter Henke 13

Smartglasses im öffentlicher Raum –
Zwingender Fortschritt auf Kosten der Privatsphäre?
Thomas Schwenke 17

Videoüberwachung im ÖPNV
Alexander Bergfink 57

Drohnen: Chancen und Regulation
Claudia Bischof 75

Diskussion 101

Statement: Die Sicht der Konzernsicherheit
bei der Deutschen Bahn AG
Hans-Hilmar Rischke 111

Statement: Regelungsperspektiven für Smart Cams
im öffentlichen Raum
Bernd H. Harder 115

Statement: Bericht aus der Praxis
Jan-Keno Janssen 125

Statement: Die Sicht der Aufsichtsbehörde
Maja Smoltczyk 129

Statement: Die Sicht des Konzerndatenschutzes
der Deutschen Bahn AG
Chris Newiger 141

Diskussion 149

Zweiter Tag

Begrüßung
Jürgen Taeger 165

Statement: Die Sicht der Informatik zum „Life Logging"
Susanne Boll-Westermann 167

Statement: Die Sicht eines Bundestagsabgeordneten
der SPD-Fraktion
Dennis Rohde 177

Statement: Die Sicht eines Bundestagsabgeordneten
der Fraktion Bündnis 90/Die Grünen
Konstantin von Notz 183

Diskussion 187

Chancen und Risiken beim Einsatz von Dashcams
im öffentlichen Straßenverkehr
Jana Spilker 191

Diskussion 205

Einsatz von Body Cams bei privaten Sicherheitsdiensten
Morris Lee/Boris Reibach 209

Diskussion 227

Schattenseiten. Warum Smart Cams
im öffentlichen Raum ein Problem sind
Volker Boehme-Neßler 235

Statement: Regulierungsbedarf
aus der Sicht eines Wissenschaftsethikers
Oliver Bendel 269

Regelungsoptionen für Smart Cams
aus Sicht des Forschungsprojekts „ChaRiSma“
Edgar Rose 277

Schlusswort
Klaus-Dieter Hommel 293

Personenverzeichnis 295

Erster Tag

Begrüßung

Prof. Dr. Jürgen Taeger

Carl von Ossietzky Universität Oldenburg;
Wissenschaftlicher Leiter des Verbundprojekts „ChaRiSma“

Meine sehr geehrten Damen und Herren,

ich begrüße Sie alle sehr herzlich und möchte meiner Freude Ausdruck geben, dass Sie unserer Einladung zu diesem Workshop über Chancen und Risiken von Smart Cams im öffentlichen Raum gefolgt sind. Es freut mich außerordentlich, dass wir diesen Workshop gemeinsam mit dem ‚Datenschutz-Beirat Deutsche Bahn Konzern‘ organisieren durften. Deswegen begrüße ich Sie gemeinsam mit Herrn Peter Henke, dem Geschäftsführer des Datenschutzbeirats. Wir werden auch pünktlich beginnen können. Schließlich sind wir im BahnTower bei der Deutschen Bahn zu Gast, wofür ich dem Vorstand der Deutschen Bahn sehr dankbar bin.

Ich beginne mit mir selbst mit der Vorstellung. Mein Name ist Jürgen Taeger. Ich bin Rechtswissenschaftler an der Carl von Ossietzky Universität Oldenburg und leite zusammen mit unserer Verbundpartnerin, der Informatikerin Frau Prof. Susanne Boll-Westermann, das Forschungsprojekt „ChaRiSma“, in dem es um Chancen und Risiken smarter Videotechnik im öffentlichen Raum geht. Wir sollen mit diesem Projekt, das das Bundesministerium für Bildung und Forschung finanziert, denjenigen Fragen nachgehen, die sich daraus ergeben, dass immer mehr intelligente Kameratechnik im öffentlichen Raum genutzt wird – von hoheitlichen Stellen, von Unternehmen und von Bürgern. Es gibt die Videoüberwachung im öffentlichen Personennahverkehr, auf Bahnhöfen und in Zügen und Bussen. In Übereinstimmung mit den Anforderungen des Bundesdatenschutzgesetzes wird rechtskonform darauf hingewiesen, dass es solche Videoüberwachungen gibt. Darüber hinaus müssen wir auch sprechen über die sehr starke Zunahme von Smart Cams in Drohnen, auch über Dashcams in Fahrzeugen und die Kameras, die Live Logger mit sich tragen. Sicher wird es noch andere Anwendungen für Smart Cams geben – die Datenbrillen dürfen nicht vergessen werden –, mit denen wir uns bei dieser Veranstaltung befassen sollten. Viele weitere Techniken werden sich in den nächsten Jahren entwickeln, bei denen Smart Cams eine Rolle spielen werden. Wir wollen aus rechtlicher und sozialwissenschaftlicher Perspektive und

auch aus technischer Perspektive darauf vorbereitet sein, wollen uns diese Entwicklung ansehen. Wir wollen prüfen, ob die derzeitige Rechtslage ausreicht, um Persönlichkeitsrechte derjenigen, die von den Kameras erfasst werden, zu schützen oder ob es notwendig ist, Regulierungen vorzunehmen, die Stellschrauben nachzustellen und im einen oder anderen Fall Gesetze auf den Weg zu bringen und zu beschließen, die Persönlichkeitsrechte vor Beeinträchtigungen durch Smart Cams schützen sollen. Auf der anderen Seite ist es aber auch durchaus denkbar, dass sich in der Bevölkerung ein Wandel der Gefährdungseinschätzung dergestalt abzeichnet, dass die Notwendigkeit des Schutzes von Persönlichkeitsrechten nicht mehr gesehen wird. Die junge Generation lebt mit Technik, sie wächst mir ihr auf. Für sie liegt es außerhalb der Vorstellungswelt, dass Menschen früher ohne Smartphones kommunizieren konnten, sich analoge Informationen auf anderem Wege als über smart devices aus dem globalen Netz besorgen konnten. Sie wachsen mit sozialen Medien, mit Instagram und snapchat auf und verbreiten ohne jegliches Unrechtsbewusstsein Fotos, ohne die Abgebildeten um Zustimmung gebeten zu haben. Es ist also durchaus denkbar, dass die Gesellschaft sagt: Persönlichkeitsrechte in dem Maße wie bisher zu schützen, das ist nicht mehr zeitgemäß. Auch Fotos und Videos sollten nach dieser Auffassung frei erstellt und verbreitet werden dürfen.

Ob sich diese Ansicht durchzusetzen beginnt, wollen wir in unserem Forschungsprojekt mit Unterstützung von Sozialwissenschaftlern durch Befragungen herausfinden. In diesem Workshop wollen wir zunächst eine Bestandsaufnahme vornehmen und nach den Chancen des Einsatzes von Smart Cams fragen. Dann wenden wir uns möglichen Gefährdungen für die durch Verfassungsrecht und durch einfaches Recht – wie das Recht am eigenen Bild oder das Datenschutzrecht – geschützten Persönlichkeitsrechte zu.

Den ersten Vortrag wird Dr. Thomas Schwenke halten. Es freut mich sehr, dass er die Ergebnisse seiner Forschungsarbeit vorstellt. Soeben ist seine Dissertation über die private Nutzung von Smartglasses im öffentlichen Raum erschienen. In ihr findet sich nicht nur die juristische Analyse des Ist-Zustandes, sondern man erhält auch einen sozialwissenschaftlich untermauerten Ausblick auf die Zukunft dieser Datenbrillen. Die Arbeit empfehle ich Ihrer Aufmerksamkeit. Dann freue ich mich, dass aus dem Hause der Deutschen Bahn AG anschließend Herr Bergfink über Videoüberwachung im öffentlichen Personennahverkehr sprechen wird. Er ist Mitglied hier im Hause der Datenschutzorganisation und hat sich mit seinem Thema ebenfalls in einer Dissertation befasst. Es wird danach Frau

Rechtsanwältin Claudia Bischof, die auch Mitarbeiterin im Forschungsprojekt „ChaRiSma“ ist, einen Vortrag über die Drohnen halten.

Nach der Pause hören wir dann Statements zu den Vorträgen. Herr Hans-Hilmar Rischke wird uns als Chief Security Officer der Deutschen Bahn AG seine Sicht auf die Videoüberwachung bei der Deutschen Bahn vorstellen. Herr Rechtsanwalt Bernd H. Harder ist Mitglied im Hauptvorstand des Bitkom und wird die positiven Aspekte hervorheben, die mit der Nutzung von Smart Cams verbunden sein können. Außerdem wird er, soviel darf ich vorab verraten, einen neuen Ansatz für eine Datenschutzregulierung in die Diskussion bringen. Von Herrn Jan-Keno Janssen, Redakteur der Zeitschrift c't, werden die meisten von Ihnen seine profunden Beiträge über Virtual Reality und ähnliche Themen kennen. Er kann uns von seinem Selbstversuch, sich mit einer Datenbrille in der Öffentlichkeit zu bewegen, und den Reaktionen der Menschen darauf berichten. Besonders gespannt bin ich auf die Einschätzungen der Berliner Beauftragte für den Datenschutz und Informationsfreiheit, Frau Maja Smoltczyk, und der Konzerndatenschutzbeauftragten der Deutschen Bahn AG, Frau Chris Newiger, die beide besonders mit der Videoüberwachung befasst sind.

Zunächst soll nach der Begrüßung durch Herrn Peter Henke für die Deutsche Bahn AG Herr Rechtsanwalt Dr. Thomas Schwenke mit seinem Vortrag über Datenbrillen das Wort erhalten.

Peter Henke

Syndikusrechtsanwalt Mitbestimmung,
Geschäftsführer des Datenschutz-Beirats DB Konzern

Ich freue mich, Sie heute im Namen des Datenschutzbeirats DB Konzern begrüßen zu dürfen. Ganz herzliche Grüße darf ich auch vom Vorsitzenden des Beirats, Herrn Klaus-Dieter Hommel, ausrichten. Er wird morgen an der Veranstaltung teilnehmen. Heute ist er wegen der zahlreichen Themen, die dieses Unternehmen bewegen und mit denen er als stellvertretender Vorsitzender der EVG, der Eisenbahn- und Verkehrsgewerkschaft, befasst ist, leider nicht dabei. Ich freue mich, dass es gelungen ist, so viele Stakeholder zu diesem Thema zusammenzubekommen. Gern unterstützen wir diese Veranstaltung, weil die Befassung mit diesem Thema auch hilfreich für unser Unternehmen ist. Auch die teilnehmenden Vertreter der Konzernsicherheit und gerade auch die der Datenschutzorganisation machen sich Gedanken zu dem Thema Smart Cams, zu den Möglichkeiten ihres Einsatzes, gleichfalls aber auch dazu, wie sich die Risiken bewältigen lassen.

Vielleicht noch ein Wort zum Datenschutzbeirat. Dieses Unternehmen hat das Gremium, das aus externen Stakeholdern, vor allem aus Experten zum Thema Datenschutz, zusammengesetzt ist, vor nunmehr fast sieben Jahren im Nachgang zu der damaligen „Daten-Havarie“ bei der Deutschen Bahn eingerichtet, um den Vorstand exklusiv zu Fragen des Datenschutzes vor allem auch strategisch zu beraten. Damit soll sichergestellt werden, dass wir einen möglichst vorbildlichen Datenschutz in diesem Konzern haben. Im Rahmen dieser Tätigkeit unterstützt der Beirat solche Veranstaltungen wie heute, weil sie einen wunderbaren Beitrag dazu leisten, dass die notwendige Awareness beim Thema Datenschutz möglich wird.

Vielen Dank und herzlich willkommen. Ich wünsche einen erfolgreichen Workshop.

Prof. Dr. Jürgen Taeger

Vielen Dank, Herr Henke, für den herzlichen Willkommensgruß. Ich darf nun Herrn Dr. Schwenke um seinen Vortrag bitten.

Smartglasses im öffentlichen Raum – Zwingender Fortschritt auf Kosten der Privatsphäre?

Dr. Thomas Schwenke

Rechtsanwalt

Zusammenfassung

Smartglasses stellen nach ihrer Konzeption effektive Schnittstellen zwischen Menschen und Computern dar und sollen ähnlich wie gegenwärtig Smartphones zu Alltagsbegleitern von Menschen werden. Ihre wesentlichen Vorteile beruhen auf einer Erweiterung der visuellen Wahrnehmung von Menschen. Der Nachteil ist jedoch, dass das menschliche Auge durch eine Kamera erweitert wird und das menschliche Gehirn durch ein computergestütztes Erinnerungsvermögen. Damit wird die, bis dato zumindest in dieser Hinsicht auf überwiegend menschliche Sinneswahrnehmung ausgerichtete Privatsphäre im öffentlichen Raum, in ihrem Bestand gefährdet. Ob und wie dieser Entwicklung zumindest aus rechtlicher Sicht zu begegnen ist, soll im Rahmen des folgenden Beitrags untersucht werden.

1 Einleitung

Bei Smartglasses handelt es sich um Geräte, die ähnlich einer Brille auf dem Kopf getragen werden (sog. „Head Mounted Displays“) und dazu dienen, Menschen im Alltag bei der Erfassung und Wiedergabe von Informationen zu unterstützen.[1] Smartglasses gehören der Kategorie der Wearables an,[2] also mobiler Computer, die ähnlich wie Kleidung oder Uhren unaufdringlich und flexibel den Menschen zur Verfügung stehen sollen.

Dass Smartglasses nicht nur Vorteile mit sich bringen, zeigten die negativen Reaktionen auf die vom Unternehmen Google vorgestellten Smartglasses mit der Bezeichnung „Glass“.[3] Das experimentelle Gerät polarisierte und Kritiker sahen darin vor allem das Potential zur Verletzung der Privatsphäre.[4] 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 und zu verbaler oder gar tätlicher Abwehr führte.[5] Diese Reaktion führten die Nutzer vor allem darauf zurück, dass Menschen sich durch die wahrnehm-

1 Der Begriff „Smartglasses“ wird im Rahmen dieser Untersuchung synonym mit dem im deutschen Sprachraum verbreiteten Begriff „Datenbrille“ verwendet.

2 Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, WP 223, 2014, p. 4; m. w. N. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 40 ff.; *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 Das Datum des letzten Abrufs von Onlinequellen wird nachfolgend in der Klammer an deren Ende angegeben; *von Gehlen*, Datenbrillen - Werkzeug des Bösen, SZ, http://www.sueddeutsche.de/digital/datenbrillen-werkzeug-des-boesen-1.1871620 (20.8.2016); *Schwenke*, K&R 2013, S. 685; *Thilo Weichert*, „Google Glass ist eine Waffe“, heise online, http://www.heise.de/newsticker/meldung/Thilo-Weichert-Google-Glass-ist-eine-Waffe-2176677.html (20.8.2016).

5 *Holly*, Ten months through Google Glass, Geek, http://mobile.geek.com/latest/216501-ten-months-through-google-glass-exploring-our-wearable-future (20.8.2016); *Honan*, I, Glasshole: My Year With Google Glass, WIRED, http://www.wired.com/gadgetlab/ 2013/12/glasshole (20.8.2016); *Janssen*, Warum Glass (noch) nicht funktioniert, c’t, http://www.heise.de/ct/artikel/Warum-Glass-noch-nicht-funktioniert-1897211.html (20.8.2016); *Nieva*, Lost Explorers, CNET, http://www.cnet.com/news/lost-explorers-the-unrealized-vision - of-google-glass/ (20.8.2016).

bare Kamera der Smartglasses eingeschüchtert fühlten und um ihre Privatsphäre Angst hatten.

Im Rahmen der folgenden Technikfolgenabschätzung sollen dementsprechend sowohl die Vorteile als auch die Nachteile von Smartglasses näher beleuchtet werden. Die Prüfung soll vor dem Hintergrund der Nutzung von Smartglasses durch Privatpersonen im öffentlichen Raum, der traditionell zwischenmenschlicher Begegnung, der Teilnahme am öffentlichen Leben und politischer Willensbildung dient, erfolgen. Als öffentlicher Raum ist der räumlich-physische Bereich zu verstehen, zu dem jedermann oder ein nur nach allgemeinen Merkmalen bestimmter Personenkreis bestimmungsgemäß Zugang hat.[6]

Die Betrachtung wird sich dabei zuerst der technischen Seite der Smartglasses-Technologie widmen, anschließend ihre gesellschaftlichen Auswirkungen beleuchten, um danach diese beiden Aspekte rechtlich zu würdigen. Die Ergebnisse dienen anschließend als Grundlage für Vorschläge zum rechtlichen und technischen Umgang mit Smartglasses.

2 Die Smartglasses-Technologie

In ihren grundsätzlichen technischen Eigenschaften entsprechen Smartglasses mit Sensoren wie Kamera, Mikrofon, einer Computer- und Speichereinheit sowie Netzwerkfähigkeiten den Smartphones. Die wesentlichen Unterschiede bestehen jedoch darin, dass die visuelle Informationsausgabe direkt im Blickfeld der Nutzer erfolgt und die Kamera Aufnahmen aus dem Blickwinkel der Betrachter erstellt.

Weil die Nutzer kein Smartphone herausholen und ihre Aufmerksamkeit dem Display widmen müssen, werden sowohl die visuelle Informationsaufnahme als auch -wiedergabe wesentlich schneller und effizienter. Hierdurch werden wahrnehmungssteigernde Technologiekonzepte, wie z. B. die „Augmented Memory“ oder „Augmented Reality“, im Alltag umsetzbar. Unter Augmented Memory wird die Erweiterung kognitiver Fähigkeiten verstanden, z. B. wenn Smartglasses Objekte im Blickfeld scannen und z. B. fremdsprachige Texte übersetzen oder Informationen zu

6 *Gola*/*Schomerus*, BDSG, 2015, § 6b, Rn. 8; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 14; *Zscherpe*, in: Taeger/Gabel, BDSG, 2013, § 6b, Rn. 23.

Personen im Blickfeld anzeigen.[7] Als „Augmented Reality“ wird im Zusammenhang mit Smartglasses eine Erweiterung der physischen, d. h. körperlichen Wirklichkeit um virtuelle Objekte bezeichnet, die sich im Blickfeld der Betrachter zu einer einheitlichen Realitätswahrnehmung vermischt.[8] Damit diese Verschmelzung der physischen und der virtuellen Realität optimal funktioniert, muss die Umwelt der Nutzer visuell kartiert werden, damit die virtuellen Objekte registriert, d. h. „an der richtige Stelle platziert“ werden.[9] Z. B. können so Navigationspfeile direkt auf dem richtigen Straßenabschnitt oder virtuelle Etiketten auf Produkten im Supermarkt erscheinen.

Zusammengefasst ist das Ziel von Smartglasses, als effiziente Mensch-Maschine-Schnittstellen, Menschen bei der Visualisierung komplexer Informationsstrukturen in praktisch allen Lebens- sowie Arbeitsbereichen zu unterstützen.[10] Smartglasses können im Berufsleben eingesetzt werden, z. B. wenn Kabelstränge von Maschinen im Blickfeld mit Wartungsinformationen versehen oder Planungen visualisiert werden.[11] Im Alltag können Menschen mit anderen Menschen oder Computern, wie z. B. autonomen

7 Vgl. *Mann*/*Niedzviecki*, Cyborg, 2002, S. 24 ff.; *Pedersen*, Ready to Wear, 2013, S. 101 f.

8 *Abawi*, Augmented Reality - die angereicherte Realität, 2008, S. 1; *Azuma*, Presence: Teleoperators and Virtual Environments 1997, Vol. 6, Nr. 4, p. 355 (356); Umschreibungskonzepte, *Broll*, Augmentierte Realität, in: *Dörner u. a.*, Virtual und Augmented Reality (VR/AR), 2013, S. 241 (245); *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 39 f.; *Schart*/*Tschanz*, Augmented Reality, 2015, S. 21 f.

9 *Klein*, Visual Tracking for Augmented Reality, 2009, S. 27 ff.; *Mehler-Bicher*/*Reiß*/*Steiger*, Augmented Reality, 2011, S. 37; *Schart*/*Tschanz*, Augmented Reality, 2015, S. 39 f.

10 *Dörner u. a.*, Interaktion in Virtuellen Welten, in: Dörner u. a., Virtual und Augmented Reality (VR/AR), 2013, S. 157 (158); *Mehler-Bicher*/*Reiß*/*Steiger*, Augmented Reality, 2011, S. 54 f.; *Negroponte*, Total digital, 1997, S. 115 ff.

11 *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.; *Schart*/*Tschanz*, Augmented Reality, 2015, S. 29.

Fahrzeugen, effizienter kommunizieren,[12] sich Zusatzinformationen zu Orten oder Personen anzeigen[13] und bei Sehbehinderungen unterstützen lassen,[14] als auch ähnlich einer Überwachungskamera in Gefahrenlagen Beweisaufnahmen fertigen und so zugleich potentielle Angreifer abschrecken.

Laut Prognosen soll es noch ca. 10 Jahre dauern, bevor Smartglasses an die Schwelle der Massenmarkttauglichkeit gelangen.[15] Die gegenwärtig vorhandenen Geräte, wie z. B. Googles „Glass" sind technisch noch nicht ausgereift.[16] Noch weiter im experimentellen Stadium befinden sich Geräte wie das „EyeTap" des Smartglassespioniers Steve Mann, bei denen sich die Kamera direkt vor dem Auge des Trägers befindet und die visuellen Informationen in Gänze durch den Computer bearbeitet werden können, bevor sie mit Hilfe von Laserstrahlen auf der Netzhaut ausgegeben werden.[17] Eine weitere Steigerung dieser Entwicklung stellen smarte Kontaktlinsen mit Kamera- und Display-Technik sowie Implantate im Augapfel dar.[18] Spätestens zu diesem Zeitpunkt sollte der Umgang mit Smartglasses rechtlich geklärt sein, wenn Smartglasses von außen nicht mehr erkennbar und zum integralen Teil des menschlichen Körpers werden.[19]

---

12 Vgl. *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/ (20.8.2016); *Kipper*/*Rampolla*, Augmented Reality, 2012, S. 65 ff.; *Tonnis*, Augmented Reality, 2010, S. 148 ff.

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

14 *Heinrich*, Retina-Implantate für Blinde, Spiegel Online, http://www.spiegel.de/gesundheit/diagnose/retina-implantate-lassen-blinde-wieder-sehen-a-1042526.html (20.8.2016); *Passary*, Precious Moment, Tech Times, http://www.techtimes.com/articles/28512/20150124/precious-moment-legally-blind-mom-sees-her-son-for-th e-very-first-time-video .htm (20.8.2016); *Schwan*, Brille liest für Sehbehinderte, Technology Review, http://www.heise.de/tr/artikel/Brille-liest-fuer-Sehbehinderte-1916999.html (20.8.2016); *Wenleder*, Technik, SZ, http://www.sueddeutsche.de/wissen/technik-sehen-dank-datenbrille-1.2114402 (20.8.2016).

15 Gartner's 2015 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business, Gartner, http://www.gartner.com/newsroom/id/3114217 (20.8.2016); *Kipper*/*Rampolla*, Augmented Reality, 2012, S. 8; *Preuß*, Augmented Reality, 2014, S. 13.

16 *Schwenke*, DuD 2015, S. 161 (163).

17 Ebenda.

18 *Kipper*/*Rampolla*, Augmented Reality, 2012, S. 138 f.

19 Mann sieht die von ihm getragenen Smartglasses als einen Teil seines Körpers an, *Mann*/*Niedzviecki*, Cyborg, 2002, S. 17.

3 Verletzung des Allgemeinen Persönlichkeitsrechts

Auch wenn die Konflikte zwischen Privatrechtssubjekten auf der Ebene der einfachen Gesetze ausgetragen werden, ist das Verfassungsrecht als objektiver Maßstab bei der Auslegung unbestimmter Rechtsbegriffe und Abwägung von Interessen der Beteiligten mittelbar maßgeblich (sog. „mittelbare Drittwirkung von Grundrechten").[20]

Angesichts der Berufung der Kritiker von Smartglasses auf die Privatsphäre, erscheint vor allem eine Verletzung des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1, 1 Abs. 1 GG naheliegend. Es handelt sich um ein Kombinationsgrundrecht, dessen Schutzbereich im Schnittbereich zwischen der allgemeinen Handlungsfreiheit gem. Art. 2 Abs. 1 GG und der Menschenwürde gem. Art. 1 Abs. 1 GG liegt.[21] Es handelt sich um ein dynamisches „Rahmenrecht", was bedeutet, dass dessen Schutzbereich und die Rechtswidrigkeit seiner Verletzung in einer einzelfallbezogenen Güter- und Interessenabwägung anhand der Umstände, wie des wissenschaftlich-technischen Fortschritts sowie gewandelter Lebensverhältnisse, zu bestimmen sind.[22]

Das flexible Konzept des Allgemeinen Persönlichkeitsrechts entspricht dabei dem modernen verfassungsrechtlichen Verständnis der Privatsphäre. Dieses wird definiert als ein individueller und wertneutraler Freiraum persönlicher Integrität, der das Individuum vor äußeren Einflüssen bewahrt, indem es ihm innerhalb dieses Bereichs Kontrolle über die eigene Selbstdarstellung bietet, d. h. freie Wahl, welche ihn betreffenden Informationen veröffentlicht werden und welche nicht.[23]

Die Privatsphäre soll Menschen in einer durch äußere Zwänge geprägten Umwelt, in der sie sich oft in sozialen Situationen selektiv darstellen

20 St. Rspr., BVerfGE, Beschl. v. 19.10.1993 – 1 BvR 567 u. 1044/89, BVerfGE 89, 214 (229 f.); BVerfG, Urt. v. 15.1.1958 – 1 BvR 400/57, BVerfGE 7, 198 (206 f.); *Herdegen*, in: Maunz/Dürig, GG, 2015, Art. 1 Abs. 3, Rn. 65; *Murswiek*, Technische Risiken, in: Westphalen, Technikfolgenabschätzung, 1997, S. 238 (240); *Pieroth u. a.*, Grundrechte, 2014, Rn. 195 ff.

21 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); *Martin*, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, 2007, S. 236.

22 St. Rspr., BVerfG, Urt. v. 15.12.1999 – 1 BvR 653/96, BVerfGE 101, 361 (380); *Wagner*, in: Säcker/Rixecker, MüKo BGB, 2013, § 823, Rn. 242.

23 *Hotter*, Privatsphäre, 2011, S. 43.

müssen,[24] geistige Entspannung und Freiheit bieten,[25] um die innere Balance und damit psychische sowie physische Stabilität wahren zu können.[26] Nur so können Menschen „zu sich finden", 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.[27]

Die Privatsphäre dient jedoch nicht nur dem Individuum, sondern auch der Sicherung einer meinungsoffenen demokratischen Gesellschaft. Denn erst die Privatsphäre schafft einen Freiraum, in dem sich auch abwegige sowie mit den Mehrheitsmeinungen kollidierende Ansichten entwickeln und in einen demokratischen Prozess eingebracht werden können.[28] Ohne diese geistigen Freiräume wäre eine erzwungene Konformität zu befürchten.[29]

Da die Privatsphäre damit selbst ein Schutzgut mit Verfassungsrang ist, bedarf sie selbst keiner Rechtfertigung.[30] Ganz im Gegenteil gilt der Grundsatz „in dubio pro libertate", wonach der Beweis der Rechtmäßigkeit demjenigen obliegt, der in das Freiheitsrecht eingreift.[31] Nur wenn die Privatsphäre dazu missbraucht werden sollte, um schützenswerte Freiheitswerte Dritter zu verletzen oder das liberale Systeme an sich anzugreifen, ist es geboten, die Privatsphäre einzuschränken.[32]

Dieser abstrakt gehaltene Schutz des Individuums und der Meinungspluralität findet sich in diversen Fallgruppen des Allgemeinen Persönlichkeitsrechts wieder, welche jedoch nicht abschließend sind und nur der Konturierung dieses Grundrechts dienen.[33] Zu den beim Einsatz von

---

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

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

26 *Westin*, Privacy And Freedom, 1968, S. 41 f.

27 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 9 ff.; *Hotter*, Privatsphäre, 2011, S. 31 f.; *Westin*, Privacy And Freedom, 1968, S. 36 f.

28 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.

29 *Hotter*, Privatsphäre, 2011, S. 29 ff.

30 Ebenda, 33 f.

31 *Hotter*, Privatsphäre, 2011, S. 34.

32 *Westin*, Privacy And Freedom, 1968, S. 21 ff.

33 *Di Fabio*, in: Maunz/Dürig, GG, 2015, 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.

Smartglasses einschlägigen Fallgruppen gehört u.a. der Schutz der Selbstbewahrung in der Ausformung von räumlichen und thematischen Rückzugsbereichen.[34] Des Weiteren wird mit der Fallgruppe der Selbstdarstellung die Verfügungsgewalt Einzelner an nicht öffentlich gesprochenen Worten, am eigenen Bild sowie als Recht auf informationelle Selbstbestimmung an personenbezogenen Daten umfasst.[35]

Wenn Personen sich mit Smartglasses im öffentlichen Raum bewegen werden, ist von der Beeinträchtigung all dieser Schutzrechte auszugehen. Eine effektive Nutzung von Augmented Memory und Augmented Reality setzt funktionsbedingt die visuelle Erfassung und Verarbeitung der Umwelt im Blickfeld ihrer Nutzer voraus. Die so erfassten Aufnahmen von Menschen beeinträchtigen nicht nur deren Bildnisschutz, sondern stellen im Regelfall zugleich personenbezogene Daten dar. Dabei können höchstpersönliche und thematische Rückzugsbereiche verletzt werden. Beides wäre z. B. der Fall, wenn ein Träger von Smartglasses einen Umkleideraum oder einen Saunabereich betritt. Zusätzlich kann das Recht am nichtöffentlich gesprochenen Wort verletzt werden, wenn die Geräte z. B. alles Gesprochene in Hörweite aufnehmen, um z. B. etwaige Funktionsbefehle der Nutzer zu erkennen.

Doch nicht nur die tatsächliche Erfassung, sondern auch die Befürchtung überwacht zu werden, stellt eine Gefahr für die Autonomie einer Person dar. Man spricht hierbei entsprechend einem metaphorischen Vergleich zu einer jederzeit möglichen und verdeckten Überwachung von Menschen aus einem Gebäude von einer panoptischen Überwachung.[36]

Wer jedoch aufgrund objektiver Anhaltspunkte jederzeit mit einer Überwachung rechnen muss, der passt sein Verhalten unabhängig davon an, ob die Überwachung stattfindet.[37] Diese Reduktion der inneren Diskrepanz, der sog. „kognitiven Dissonanz“, durch Selbstdisziplinierung ist

34 BVerfG, Urt. v. 15.12.1999 – 1 BvR 653/96, BVerfGE 101, 361 (382); *Pieroth u. a.*, Grundrechte, 2014, Rn. 394 ff.

35 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); *Pieroth u. a.*, Grundrechte, 2014, Rn. 394 ff.

36 *Bentham*, Das Panoptikum, 2013, passim.; *Foucault*, Überwachen und Strafen, 1994, S. 263 ff.

37 *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.).

die Anerkennung des erwarteten Verhaltens als eigenen Wertemaßstab.[38] Als Folge droht eine Beeinträchtigung der Meinungskonformität und damit der Gefährdung einer freiheitlich-demokratischen Gesellschaft mit sich.[39] Derartige Furcht vor möglicher Überwachung ist auch im Fall von Smartglasses zu erwarten, bei denen es an einer für Betroffene erkennbaren Fotografiergeste, wie z. B. bei Smartphones oder Fotokameras, fehlt.[40] Dadurch ist eine heimliche Aufnahme jederzeit möglich.

Es ist wahrscheinlich, dass Smartglasses den Kundenwünschen folgen und kleiner, unauffälliger werden. Ob Menschen dadurch Smartglasses, wie heutzutage häufig Überwachungskameras, nicht wahrnehmen, aber trotzdem ihr Verhalten unbewusst anpassen, ist wahrscheinlich, aber empirisch noch nicht bestätigt.

Zu der Intransparenz kommen auch die große Streuweite und Anlasslosigkeit der (möglichen) Erfassung von Menschen in deren Blickfeld.[41] Zumal damit zu rechnen ist, dass Smartglasses sich schnell verbreiten würden, wenn deren Nutzung Vorteile wie Bequemlichkeit und Sicherheit im Alltag mit sich bringt. Diese Summierungseffekte werden verstärkt,[42] wenn die Omnipräsenz von Smartglasses zugleich eine strenge Regulierung privater und staatlicher Videoüberwachung nicht mehr rechtfertigen würde. Mit dieser Entwicklung steigt entsprechend die Gefahr, dass Aufnahmen Dritter unkontrolliert verbreitet und veröffentlicht werden, wie dies in sozialen Netzwerken bereits heutzutage häufig geschieht.[43] Ebenso ist der Einsatz biometrischer Gesichtserkennungstechnologien naheliegend, um z. B. angenehme Erinnerungen zu Personen zu speichern oder

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

39 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 13; *Hotter*, Privatsphäre, 2011, S. 79 f.; vgl. *Nagel*, Concealment and Exposure, 2004, S. 21.

40 *Fuchs*, ZD 2015, S. 212 (216); *Schwenke*, K&R 2013, S. 685 (686).

41 Vgl. zur Beeinträchtigung durch breit gefächerte und anlasslose Überwachung, BVerfG, Urt. v. 12.3.2003 – 1 BvR 330/96 u. 1 BvR 348/99, BVerfGE 107, 299 (328).

42 Vgl. zu Summierungseffekten, *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 93; *Roßnagel*, NJW 2010, S. 1238 (1242).

43 Vgl. *Golla*/*Herbort*, GRUR 2015, S. 648; *Heckmann*, K&R 2011, S. 770 ff.; *Kister*, Die Epoche der Augenzeugen, SZ, http://www.sueddeutsche.de/digital/internet-und-gesellschaft-epoche-der-augenzeugen-1.2274559 (20.8.2016); *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.

potentiell gefährliche Menschen anhand von Fahndungslisten zu erkennen.[44]

Die Folge könnte eine als „elektronisches Superpanoptikum“,[45] „Post-Panoptikum“[46] oder „Synoptikum“[47] bezeichnete, dezentralisierte, von räumlichen, territorialen und zeitlichen Beschränkungen gelöste Überwachung „von allen Seiten, von überall“, durch jede Institution und jedermann sein.[48] Daher bringen Smartglasses eine immense Gefahr für die Privatsphäre und damit eine Verletzung des Allgemeinen Persönlichkeitsrechts Betroffener mit sich. Der öffentliche Raum wird seinen Charakter als ein Ort der autonomen Selbstentfaltung und politischer Teilhabe verlieren, wenn Menschen sich einer permanenten Überwachung ausgesetzt sehen werden.

Eine derart weitreichende Einschränkung der Privatsphäre gefährdet die Subjektivität von Menschen, d. h. greift in den Schutzbereich der Menschenwürde ein. Eine Beeinträchtigung der Menschenwürde als eines absoluten Rechts kann auch nicht durch die Interessen der Nutzer von Smartglasses gerechtfertigt werden. Deren Einsatz wird allenfalls in punktuellen und seltenen Situationen zulässig sein. In Frage kommen z. B. Notwehr- oder notwehrähnliche Situationen, in denen Smartglasses der Beweissicherung dienen und damit auch Angriffen auf geschützte Interessen wie die körperliche Unversehrtheit gem. Art. 2 Abs. 2 GG oder Eigen-

44 *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/ (20.8.2016); *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-fac e-in-the-crowd.ht ml (20.8.2016).

45 *Poster*, The Mode of Information, 1991, S. 93; von einem „elektronischen Panoptikon” sprechend, *Gordon*, Politics & Society 1987, Vol. 15, Nr. 4, p. 483.

46 *Bauman*, Liquid Surveillance, 2012, S. 3 ff.

47 *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.).

48 Vgl. *Arthur*, Google Glass, The Guardian, http://www.guardian.co.uk/tech nology/2013/mar/06/google-glass-threat-to-our-privacy (20.8.2016); *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.

tum gem. Art. 14 GG vorbeugen können.[49] Eine weitere Möglichkeit wäre die medizinische Indikation, z. B. bei Sehbehinderungen.[50]

Dagegen werden allgemeine Informations-, Nützlichkeits- oder Bequemlichkeitsinteressen gem. Art. 5 Abs. 1 Satz 1 HS. 1, 2 Abs. 1 GG grundsätzlich nicht zur Rechtfertigung ausreichen.[51]

4 Einfachgesetzliche Nutzungsverbote

Das Ergebnis der verfassungsrechtlichen Prüfung ist eindeutig und lässt die Nutzung von Smartglasses nur in Sonderfällen zu. Damit wird maßgeblich das Ergebnis der einfachgesetzlichen Prüfung vorgegeben. Die nachfolgende Darstellung der einfachgesetzlichen Normen erfolgt daher übersichtsartig.

4.1 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen gem. § 90 TKG

Aufgrund der Eingriffsintensität liegt die Annahme eines Generalverbotes gem. 90 TKG nahe. Diese Vorschrift wurde als Reaktion auf die Miniaturisierung der Aufnahme- und Sendetechnik sowie das Aufkommen sog. „Minispione", d. h. sendefähiger und getarnter Minikameras, geschaffen.[52]

Zwar sind Smartglasses wegen einer möglichen Verwechslung mit regulären Korrekturbrillen insoweit durchaus tatbestandsmäßig. Um die Ausuferung des Tatbestandes des § 90 Abs. 1 TKG zu verhindern, ist die-

49 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); *Hilpert*, RDV 2009, S. 160 (165); vgl. *Horst*, NZM 2000, S. 937 (942); vgl. *Kindhäuser*, in: Kindshäuser/Neumann/Paeffgen, StGB, 2013, § 32, Rn. 55 ff.

50 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, 2015, Art. 2 Abs. 2 S. 2, Rn. 56.

51 Vgl. zur Einschränkung auf „das absolut Notwendige", EuGH, Urt. v. 11.12.2014 - C 212/13, DuD 2015, 195 (196); *Scholz*, in: Simitis, BDSG, 2014, § 6b, Rn. 78; *v. Zezschwitz*, in: Handbuch Datenschutzrecht, 2003, Kap. 9.3. Rn. 102.

52 *Bock*, in: Geppert/Schütz, BeckOK TKG, 2013, § 90, Rn. 1; *Dierlamm*, in: Scheurle/Mayen, TKG, 2008, § 90, Rn.2.

ser jedoch auf Anlagen beschränkt, 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“.[53] Smartglasses sind jedoch nicht schlechthin zu diesen Zwecken bestimmt, sondern sollen viele nützliche Funktionen erfüllen und sind damit nicht vom § 90 TKG erfasst. Ein etwaiger Missbrauch ist hierbei nicht relevant, da § 90 TKG nicht die konkrete Nutzung, sondern die objektive Schädlichkeit von Minispionen verhindern soll.[54]

4.2 Videoüberwachung gem. § 6b BDSG

Auch wenn der Besitz von Smartglasses nicht verboten ist, so wird deren Nutzung im Regelfall gem. § 6b BDSG untersagt sein.

Bei Smartglasses handelt es sich um „optisch-elektronische“ Einrichtung im Sinne des Gesetzes. Sie werden auch zur Beobachtung eingesetzt, die zwar eine gewisse Systematik und ein Zeitmoment erfordert, daran aber keine hohen Anforderungen stellt.[55] Es ist nicht ungewöhnlich, dass Menschen mit ihrem Blick andere Personen, sei es aus Neugierde oder aus Angst fixieren. Dabei gehen sie von der reinen Betrachtung zu einer systematisch auf eine Person gerichteten und eine gewisse Dauer dauernden Beobachtung über.

§ 6b BDSG ist entgegen mancher Ansicht der Rechtsprechung auch bei mobiler Videoüberwachung einschlägig.[56] Das Argument, dass mobile Videoüberwachung nicht gem. § 6b Abs. 2 BDSG gekennzeichnet werden kann und damit generell nicht vom Tatbestand des § 6b BDSG mitumfasst wird,[57] überzeugt bereits aufgrund der beim Einsatz von sog. „Body

53 BT-Drs. 10/1618, S. 1.
54 Vgl. BT-Drs. 10/1618, S. 1, 9.
55 *Gola*/*Schomerus*, BDSG, 2015, § 6b, Rn. 10; *Hilpert*, RDV 2009, S. 160 (161); *Klar*, MMR 2012, S. 788 (196); *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 270; *Scholz*, in: Simitis, BDSG, 2014, § 6b, Rn. 63 f.; *Zscherpe*, in: Taeger/Gabel, BDSG, 2013, § 6b, Rn. 21.
56 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 246; *Zscherpe*, in: Taeger/Gabel, BDSG, 2013, § 6b, Rn. 19.
57 AG Nienburg, Urt. v. 20.1.2015 – 4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14), BeckRS 2015, 7708.

Cams“ mit Warnwesten und Aufschrift „Videoüberwachung“ ausgestatteten Polizisten nicht.[58]

Die Zulässigkeitstatbestände der Videoüberwachung gem. § 6b Abs. 1 BDSG kommen nur in Frage, sofern keine Anhaltspunkte bestehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen. Im Fall von Smartglasses ist jedoch ausgehend vom verfassungsrechtlichen Ergebnis von der Beeinträchtigung schutzwürdiger Interessen der Betroffenen, außer in seltenen Ausnahmefällen wie einer Notwehrlage oder medizinischer Indikation, auszugehen.

Eine freiwillige und bewusste Einwilligung gem. §§ 4 Abs. 1, 4a BDSG als mögliche Rechtfertigung erscheint im öffentlichen Raum aufgrund des hohen Aufklärungsumfangs über Umfang, Risiken und Folgen der Erfassung gegenüber einer Vielzahl von Betroffenen und häufigen Fällen fehlender Einwilligungsfähigkeit Minderjähriger[59] kaum möglich.[60] Ausnahmen können z. B. bei örtlich beschränkten Einwilligungen, z. B. in Museen oder bei Veranstaltungen in Frage kommen.

Die hohe Beeinträchtigungswirkung und Einflussnahme auf das Verhalten Dritter durch das von Smartglasses erzeugte Gefühl, man werde überwacht, führt auch dazu, dass die alltägliche Nutzung von Smartglasses, z. B. für persönliche Schnappschüsse oder Augmented Reality und erst Recht zur Beweiszwecken,[61] nicht als ausschließlich persönlich und familiär gem. § 1 Abs. 2 Nr. 3 BDSG betrachtet werden kann. Diese Vorschrift ist eng auszulegen und soll nur die Ausuferung des BDSG verhindern,

---

58 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 (20.8.2016); ebenso bedeutet der Begriff „Einrichtung“ allgemeinsprachlich keine Ortsfixierung, sondern die Ausrichtung auf einen konkreten Zweck, Duden, 2013, Begriff. „Einrichtung“, „Vorrichtung“; vgl. *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 245.

59 *Gola*/*Schomerus*, BDSG, 2015, § 4a, Rn. 2a; *Taeger*, in: Taeger/Gabel, BDSG, 2013, § 4a, Rn. 29, Fn. 47; *Wintermeier*, ZD 2012, S. 210 (2012 ff.).

60 Vgl. zu Anforderungen, Art. 29-Datenschutzgruppe, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Abs. 1 der Richtlinie 95/46/EG v. 24. Oktober 1995, WP 114, 2093-01/05/DE, 2005, S. 14; *Gola*/*Schomerus*, BDSG, 2015, § 4a, Rn. 25; *Simitis*, in: Simitis, 2014, BDSG, § 4a, Rn. 20.

61 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, 2014, § 6b, Rn. 58.

aber auch Privatpersonen einschließen, wenn deren Handlungen die informationelle Selbstbestimmung Dritter verletzen.[62]

Im Rahmen der privaten Nutzung von Smartglasses ist es auch kaum zu erwarten, dass Nutzer die Kennzeichnungspflichten gem. § 6b Abs. 2 BDSG, Hinweispflichten gem. § 6b Abs. 4 BDSG, Einschränkungen weiterer Verwendung der erhobenen Daten gem. § 6b Abs. 3 BDSG, Löschungspflichten gem. § 6b Abs. 5 BDSG sowie Rechte der Betroffenen gem. §§ 33 ff. BDSG beachten werden.

Als Folge können neben zivilrechtlichen Ansprüchen der Betroffenen gem. §§ 7 BDSG, 823 Abs. 2 BGB i. V. m. § 6b BDSG[63] auch die Datenschutzbehörden sowohl Bußgelder wegen Ordnungswidrigkeiten gem. § 43 Abs. 2 Nr. 1 BDSG gegen die Nutzer verhängen als auch die Nutzung von Smartglasses gem. § 38 Abs. 5 Satz 1 BDSG untersagen.[64]

4.3 Strafgesetzlicher Schutz des Allgemeinen Persönlichkeitsrechts

Der Gesetzgeber hat mit dem Schutz der Verletzung der Vertraulichkeit des Wortes gem. § 201 StGB und die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen gem. § 201a StGB besonders hohe Gefahren für die Persönlichkeitsrechte strafrechtlich sanktioniert.[65] Beide Vorschriften sind insbesondere im Hinblick auf die Verbreitung von technischen Möglichkeiten zum heimlichen Abhören und Aufnehmen konzipiert und schützen die Vertraulichkeit der Kommunikation und den höchstpersönlichen Lebensbereich in Wohnungen, gegen Einblick in besonders geschützte Räume, in hilflosen Situationen oder solchen, die dem Ansehen der abgebildeten Person erheblich schaden könnten.

Ferner schützen die §§ 22, 33 KUG den Gewährleistungsgehalt des Rechts am eigenen Bild vor Verfügungsverlust über Bildnisse in Fällen

62 EuGH, Urt. v. 11.12.2014 – C 212/13, DuD 2015, 195 (196); *Dammann*, in: Simitis, BDSG, 2014, § 1, Rn. 147; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, S. 257.

63 AG Berlin-Mitte, Urt. v. 18.12.2003 – 16 C 427/02, NZM 2004, 318 (319); *Scholz*, in: Simitis, BDSG, 2014, § 6b, Rn. 157.

64 *Scholz*, in: Simitis, BDSG, 2014, § 6b, Rn. 158.

65 Daneben wird die Verletzung des Allgemeinen Persönlichkeitsrechts auch außerhalb des StGB, z. B. im § 44 BDSG und § 33 KUG strafrechtlich sanktioniert.