



TAGUNGSBAND HERBSTAKADEMIE 2016

herausgegeben von  
Univ.-Prof. Dr. Jürgen Taeger

Jürgen Taeger (Hrsg.)

## **Smart World - Smart Law?**

Weltweite Netze mit regionaler Regulierung

### **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.

Gedruckt auf alterungsbeständigem säurefreiem Papier.

Alle Rechte vorbehalten.

© OIWR Verlag

Oldenburger Verlag für Wirtschaft, Informatik und Recht  
Rudolf-Kinau-Str. 54, 26188 Edewecht  
[mail@olwir.de](mailto:mail@olwir.de)

Edewecht 2016

ISBN: 978-3-95599-036-7

# ZÄHMT SMART LAW ALLGEGENWÄRTIGE BILDERFASSUNG?

Dr. Edgar Rose

Carl von Ossietzky Universität Oldenburg  
Forschungsprojekt ChaRiSma<sup>1</sup>  
edgar.rose@uni-oldenburg.de

## Zusammenfassung

Smart Cams bieten vielfältige sinnvolle und legitime Anwendungsmöglichkeiten im öffentlichen Raum. Dabei werden in der Regel auch andere Personen bildlich erfasst. Digitale Fotos und Filme, die ohne Zustimmung und oft auch ohne Wissen der Erfassten hergestellt werden, stellen ein außergewöhnlich hohes Risiko für die Persönlichkeitsrechte der Betroffenen dar. Sie können analysiert, ins Netz gestellt, mit Personenbezug versehen und im ungünstigsten Fall mit zahlreichen anderen Bilddaten derselben Person zusammengeführt werden, so dass Persönlichkeitsprofile entstehen. Das geltende Recht untersagt zwar weitgehend schon die Bilderstellung. Es zeigt sich jedoch durchsetzungsschwach. Mit einer rechtlichen Verankerung des Konzepts Privacy by Design könnten technische Produktgestaltungen durchgesetzt werden, die bestimmte Anwendungen von Smart Cams erlauben, weil Rücksicht auf entgegenstehende Rechte genommen wird. Ob Art. 25 DSGVO hierfür eine geeignete Grundlage bietet, ist jedoch zweifelhaft.

## 1 Rechtliche Dämme digitaler Bilderflut

Im öffentlichen Raum der Städte verschmilzt der Einsatz verschiedener Techniken digitaler Bilderfassung zu einer nie gekannten Überwachungsichte. Die Flut an produziertem Bildmaterial, das Persönlichkeitsrechte berührt, weil es Personen erkennbar zeigt, wurde und wird durch mehrere Wellen technischer Innovation immer weiter in die Höhe getrieben.

In der ersten Welle, die ihren Scheitelpunkt noch nicht erreicht hat, sind stationäre Überwachungskameras – in großen Städten mehrere Tausend<sup>2</sup> – an öffentlichen Orten (an Straßen und Plätze, in Gebäuden und Verkehrsmitteln) installiert worden. Der betroffene Bürger verlässt sich darauf, dass das Material nur kurzzeitig gespeichert und eine Auswertung nur in begründeten Ausnahmefällen durchgeführt wird. Die zweite Welle ist schon nicht mehr an feste Orte und Speicherfristen gebunden. Haben

---

<sup>1</sup> Das Verbundprojekt ChaRiSma wird vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Förderung der „Innovations- und Technikanalyse (ITA)“ unter dem Förderkennzeichen 16/1664 gefördert.

<sup>2</sup> Am 23.1.2015 hat die Süddeutsche Zeitung berichtet, dass nach einer eigenen Umfrage 9200 Kameras, die von staatlichen Stellen und Verkehrsunternehmen betrieben werden, den öffentlichen Raum in München erfassen ([www.sueddeutsche.de/muenchen/videoueberwachung-in-muenchen-stadt-der-augen-1.2316618](http://www.sueddeutsche.de/muenchen/videoueberwachung-in-muenchen-stadt-der-augen-1.2316618)).

früher nur Touristen Fotos für ihr Fotoalbum gemacht, führen heute fast alle Passanten Mobiltelefone mit Kamerafunktion mit sich, deren Bilder umgehend ins Internet geladen werden können. Dass dies auch tatsächlich geschieht, belegen z.B. 2 Millionen Foto-Uploads auf der Online-Fotoplattform *flickr* pro Tag.<sup>3</sup> Das Teilen von Handyfotos aus dem individuellen Alltagsleben in sozialen Netzwerken ist ein zentraler Bestandteil aktueller Kommunikationskultur. Auch die dritte Welle rollt bereits, ohne dass ihre endgültige Wucht klar wäre. Hier sind es smarte Kamerasysteme, die per Dash Cam, Drohne, Datenbrille oder Body Cam zur digitalen Bilderflut beitragen. „Smart“ können diese Systeme unter verschiedenen Gesichtspunkten genannt werden. Sie arbeiten automatisch, sind sehr klein und verborgen oder können gar fliegen. Sie sind oft mit dem Internet verbunden und können – jedenfalls ist dies perspektivisch zu erwarten – erfasste Personen erkennen, womit sich die technische Möglichkeit eröffnen wird, mithilfe des Netzes die Bilddaten aus unterschiedlichen Quellen personenbezogen zusammenzuführen und vielfältig zu analysieren.

Die derzeit im öffentlichen Raum gelegentliche, kurzfristige und zufällige Erfassung einer Person durch Kameras im Einzelfall droht so in ihr Gegenteil zu kippen. Werden die Daten summiert, zeichnet sich ein System flächendeckender personenbezogener Überwachung ab, das zwar noch hier und da Lücken aufweist. Wegen der Unsichtbarkeit eines Teils der Kameras sind diese Lücken jedoch nicht bestimmbar; der Überwachungsdruck ist also trotzdem total.

Das BMBF-geförderte Forschungsprojekt ChaRiSma, das an der Universität Oldenburg in Kooperation mit OFFIS, Institut für Informatik, derzeit durchgeführt wird, soll Alternativen einer künftigen Regulierung des beschriebenen Konflikts zwischen Persönlichkeitsrechten der im öffentlichen Raum bildlich Erfassten und den unterschiedlichen Belangen der Anwender smarterer Kameras formulieren. Aus den Zwischenergebnissen des Projekts nach der halben Laufzeit berichtet der folgende Beitrag.

## 2 Chancen und Risiken von Smart Cams

### 2.1 Smart Cams im öffentlichen Raum

Das Projekt ChaRiSma befasst sich mit Smart Cams im öffentlichen Raum. Beide Begriffe sind eher als Sammelbegriffe und nicht als trennscharfe Kategorien zu verstehen.

Der Begriff Smart Cams fasst aktuelle technische Innovationen in Abgrenzung zu klassischen Foto- oder Videokameras zusammen. Es geht um

---

<sup>3</sup> Siehe eigene Angaben von *flickr* unter [www.flickr.com/photos/franckmichel/6855169886](http://www.flickr.com/photos/franckmichel/6855169886).

Kameras, bei denen die hergebrachte besondere Geste des Fotografierens bzw. Filmens entfällt, so dass der Erfasste im Unklaren bleibt, ob ein Bild von ihm entstanden ist. Am Körper getragene Kameras, die automatisch oder auf unsichtbaren Befehl des Trägers tätig werden (Body Cams, Datenbrillen), gehören ebenso hierzu wie Drohnen und Dash Cams. Smart sind solche Kameras insbesondere dann, wenn sie Bilder nicht nur machen, sondern auch direkt im Gerät oder weitergeleitet ins Netz personenbezogen analysieren können. Die Datenbrille steht in diesem Sinne im Brennpunkt des Interesses, da sie die ermittelten Informationen zum Abgebildeten dem Anwender über das Brillendisplay direkt zur Verfügung stellen kann, ohne dass dies für die Umwelt bemerkbar wäre. Geprägt ist das Problem aber nicht nur durch diese am weitesten fortgeschrittene Technik, sondern auch durch das mögliche Zusammenspiel einer Vielzahl unterschiedlicher Techniken.

Mit der Konzentration auf die Erfassung des öffentlichen Raums wird im Projekt eine forschungspragmatische Eingrenzung vorgenommen. Die zum Teil andersgearteten Probleme beim Einsatz von Smart Cams in privater Runde oder im Betrieb sollen nicht behandelt werden. Als öffentlicher Raum werden alle Orte verstanden, die für ein unbestimmtes Publikum ohne weiteres (eventuell unter Kauf eines Tickets) zugänglich sind, also auch z.B. Restaurants, Universitäten, Straßenbahnen oder Fußballstadien. Gemeinsam steht für diese Orte im Hintergrund die Frage, wieviel Privatheit soll ein Mensch beanspruchen können, der sich in den sozialen Raum einer unbestimmten Öffentlichkeit begibt.

## **2.2 Sinnvolle Anwendungen**

Smart Cams stoßen auf eine große Zahl unterschiedlicher Wünsche, die die Anwendung im öffentlichen Raum motivieren.

Body Cams können zu Dokumentations- und Ausbildungszwecken im Polizeieinsatz, bei Feuerwehr und Unfallrettung, bei Sicherheitsdiensten u. ä. eingesetzt werden. In etwas anderer Form spielen sie aber auch eine große Rolle für die individuelle Selbstverwirklichung von Sportlern oder Lifeloggern. Die gewonnenen Bilder können der Kontrolle des sportlichen Trainings, der eigenen Erinnerung und Selbstvergewisserung oder durch das Posten in der Peergroup auch zur Selbstdarstellung bzw. zur Herausbildung von Gruppenidentität dienen. Auch die Meinungsäußerung kann durch Fotodokumente unterstützt werden. Weiterhin sind künstlerische oder journalistische Zwecke vorstellbar.

Datenbrillen sind im Grunde spezielle Body Cams, bieten aber zusätzliche Möglichkeiten, die für einige Personengruppen von besonderem Interesse sind. Datenbrillen können mit einer Kopfbewegung ohne jede zusätzliche Geste auf ein bestimmtes Ziel gerichtet werden. Ausgabeeinhei-

ten können dem Träger in Bild oder Ton direkt und permanent mitteilen, was sich vor ihm befindet. Es gibt bereits Datenbrillen, die Sehbehinderten Texte vorlesen.<sup>4</sup> Weitere Informationen für diesen Personenkreis bis hin zur Personenerkennung sind denkbar. Auch andere Wahrnehmungseinschränkungen, wie sie etwa für Autisten typisch sind, könnten ebenfalls durch eine Datenbrille ausgeglichen werden, die dem Träger die Emotionen des Gegenübers deutet.<sup>5</sup> Menschen mit Orientierungsproblemen (Touristen, ältere Menschen) könnte die Datenbrille den Weg weisen: der grüne Pfeil im Display zeigt, wie das Museum gefunden werden kann.

Drohnen in der Gestalt fliegender Kameras, die auf dem Steuergerät das Life-Bild entweder nur zeigen oder auch speichern, üben offenbar einen hohen Spielanreiz aus. Gleichzeitig lassen sich damit Fotowünsche befriedigen, die eine besondere Perspektive erfordern, hochgelegene Objekte betreffen oder bei denen – z.B. bei Tieraufnahmen – die menschliche Anwesenheit stören würde. Denkbar sind u.a. journalistische, künstlerische oder auch touristische Zwecke. Angeboten wird auch die Drohne, die „ihrem Herrn“ folgt und dabei filmt. Dies mag für Zwecke des Lifelogging, für Trainingszwecke von Sportlern oder auch für Sicherheitsbedürfnisse interessant sein.

Dash Cams werden teilweise auch als Unfallkameras bezeichnet, weil ein zentraler Zweck darin bestehen soll, für den Fall eines Unfalls beweiskräftiges Bildmaterial herzustellen. Aber auch Fehlverhalten im Verkehr, das nicht zu einem Unfall führt, wird dokumentiert und hat schon als Beweis vor Gericht in einem Bußgeldverfahren (Missachtung des Rotlichts) eine Rolle gespielt.<sup>6</sup> In einem anderen Verfahren ging es um ein parkendes Fahrzeug, dessen Dash Cam Bilder dokumentierte, die (vermeintlich) auf den Urheber von Sachbeschädigungen am Fahrzeug hinweisen sollten.<sup>7</sup> Ganz unabhängig von solchen Beweis Zwecken werden Dash Cams auch in der Funktion gesehen, persönliche Wünsche im Sinne des Lifelogging z.B. nach Dokumentation einer Reise zu unterstützen.<sup>8</sup>

Die Interessen hinter den Smart Cam Anwendungen können also sehr unterschiedliche rechtliche Relevanz besitzen. In eine Grundrechtsabwä-

---

<sup>4</sup> Apfel, FOCUS-Online, 22.1.2014, [www.focus.de/gesundheit/ratgeber/sehen/yonatan-wexler-macht-blinde-gluecklich-orcam-ist-besser-als-stock-und-blindenhund\\_id\\_3557875.html](http://www.focus.de/gesundheit/ratgeber/sehen/yonatan-wexler-macht-blinde-gluecklich-orcam-ist-besser-als-stock-und-blindenhund_id_3557875.html).

<sup>5</sup> Simon, Die Welt, 16.2.2015, [www.welt.de/gesundheit/psychologie/article137514796/Autisten-koennen-Gefuehle-mit-Datenbrille-entziffern.html](http://www.welt.de/gesundheit/psychologie/article137514796/Autisten-koennen-Gefuehle-mit-Datenbrille-entziffern.html).

<sup>6</sup> OLG Stuttgart BeckRS 2016, 09359.

<sup>7</sup> LG Memmingen CR 2016, 240.

<sup>8</sup> So Fuchs, ZD 2015, S. 212 (215).

gung mit den Belangen der bildlich Erfassten bringen sie zum Teil erhebliches Gewicht ein.

## 2.3 Risiken für die bildlich Erfassten

### 2.3.1 Besondere Eingriffstiefe von Bilddaten

Die Erstellung und Nutzung von Bildern, die Personen zeigen, können ungleich tiefer in deren Selbstbestimmungsrechte eingreifen als die Verwendung sonstiger personenbezogener Daten, die begrifflich oder in Zahlenwerten erfasst werden. Der Hauptgrund dürfte in der hohen und zugleich schwer kalkulierbaren Informationsfülle liegen, die das Bild eines Menschen und insbesondere seines Gesichts liefert.

Bilder wecken Aufmerksamkeit, sprechen Emotionen spontan an und graben sich tief in das Gedächtnis ein. Man spricht von der besonderen „Macht der Bilder“ im Vergleich zu Texten.<sup>9</sup> Besonders Gesichter ziehen das Interesse der Bildbetrachter auf sich. In einer Zehntelsekunde werden Alter, Geschlecht, emotionaler Zustand und zentrale Charaktereigenschaften eingeschätzt.<sup>10</sup> Zweifellos enthält das Gesicht einer Person zahlreiche Informationen. Deren Relevanz wird noch verstärkt durch die menschliche, in der Kindheit ausgiebig trainierte Fertigkeit, sich sozial durch das blitzschnelle Taxieren der Mitmenschen zu orientieren. Dieses Taxieren findet spontan ohne besonderen Grund automatisch statt.<sup>11</sup> Die Auswirkung auf das Verhalten der Beteiligten soll erheblich sein, obwohl sich in Studien herausgestellt hat, dass die Beurteilung derselben Person je nach Gestaltung vorgelegter Bilder stark variiert – also keineswegs zuverlässig ist.<sup>12</sup>

Die meisten Menschen wissen um die „Macht des ersten Eindrucks“, auch wenn die einzelnen Aspekte des Vorgangs keineswegs durchschaut werden. Um diesen dennoch zu steuern, kleiden sie sich gezielt, richten die Haare oder schminken sich. Soll ein Foto gemacht werden, wird eine spezielle Pose (Körperhaltung, Gesichtsausdruck) eingenommen. Umso verhasster ist es vielen, spontan oder gar unbemerkt aufgenommen zu werden, vor allem wenn dies durch Fremde geschieht. Denn das so entstandene Bild ist dem eigenen Einfluss entzogen. Es liefert möglicherweise Informationen, die den eigenen Selbstdarstellungswünschen widersprechen, und seine Verwendung ist unkontrollierbar. Es besteht dann eine belastende mehrfache Ungewissheit über den Bildinhalt, die Bildnut-

---

<sup>9</sup> Ausführlich *Boehme-Neßler*, BilderRecht, 2010, S. 55 ff.

<sup>10</sup> *Willis/Todorov*, Psychol Sci, 2006, p 592.

<sup>11</sup> *Vernon/Sutherland/Young/Hartley*, PNAS, 2014, p E 3353.

<sup>12</sup> *Todorov/Porter*, Psychol Sci, 2014, p 1404.



zung und die Erkenntnisse, die andere aus der Betrachtung ziehen können.

Der Eingriff in die Persönlichkeitsrechte der Betroffenen kann sogar schon im Vorfeld tatsächlich aufgenommener Bilder erfolgen. Wenn die reine Möglichkeit, abgebildet zu werden, antizipiert wird, entsteht auch so bereits Verhaltensdruck. Der Weg durch die Fußgängerzone kann zur permanenten Pose werden, weil Fotoaufnahmen aus allen Richtungen drohen. Zutreffend wird darauf hingewiesen, dass dies nicht nur eine gravierende persönliche Beeinträchtigung darstellt, sondern in letzter Konsequenz auch das gesellschaftliche bzw. politische Leben durch Anpassungsdruck verarmt.<sup>13</sup>

### 2.3.2 Summierungseffekte

Es gibt keine andere Möglichkeit, so viele personenbezogene Daten über einen Menschen in so kurzer Zeit zu sammeln, wie durch das Erstellen einer Bildaufnahme. Mit einem Klick können Aufenthaltsort, Kleidungspräferenzen, Stimmung und – je nach Aufnahmeinhalt – vieles mehr erfasst worden sein. Es gibt auch keine andere Möglichkeit, so viele personenbezogene Daten über einen Menschen in so kurzer Zeit der weltweiten Nutzung zur Verfügung zu stellen wie durch einen Upload von Bildern bei einschlägigen Internetportalen. Dem Personenbezug von Bildern entgegen stehen derzeit vor allem Defizite der automatischen Erkennung und Identifizierung von Gesichtern. Sobald die Personenzuordnung anhand von biometrischen Bilddaten zuverlässig funktioniert, vervielfachen sich die Analysemöglichkeiten.

Durch die Verbreitung von Smart Cams wächst die Gefahr erheblich, dass Bilder einer Person, die sich z.B. in das Zentrum einer belebten Stadt begibt, in großer Zahl nicht nur entstehen, sondern die gewonnenen Bilddaten per Internetnutzung personenbezogen miteinander verknüpft und analysiert werden. Es können nicht nur personenbezogene Bewegungsprofile entstehen, sondern auch Handlungsprofile, Kontaktprofile, Konsumprofile, emotionale Profile – letztlich umfassende Persönlichkeitsprofile.<sup>14</sup>

Allerdings wächst diese Gefahr nicht zwangsläufig. Mehrere Voraussetzungen müssen erfüllt sein. Erstens müssen Bilder einer Person erstellt werden. Zweitens müssen die Daten online zur Verfügung gestellt werden. Drittens muss eine Personenidentifizierung stattfinden. Viertens

---

<sup>13</sup> Eingehend *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 35 ff.; *Schwenke*, Private Nutzung von Smartglases im öffentlichen Raum, 2016, S. 89 ff.

<sup>14</sup> Zur rechtlichen Beurteilung von Summierungseffekten *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 92 ff.

müssen dann auf dieser Grundlage Profile tatsächlich erstellt werden. Sinnvoll zu kontrollieren ist dieser Ablauf nur auf den ersten beiden Stufen. Wenn kein Bild erstellt wird, kann dies auch nicht zum Profiling herangezogen werden. Auch wenn das erstellte Bild dem Profiling nicht zur Verfügung steht, weil es z.B. ohne Weitergabe wieder gelöscht wird, ist der Ablauf unterbrochen. Bilder allerdings, die erstmal dem potenziellen Profiler zur Verfügung stehen, lassen sich nicht mehr zuverlässig zurückholen. Schutzkonzepte müssen also bei den ersten beiden Voraussetzungen ansetzen.

### 3 Smart Law

#### 3.1 Defizite gegenwärtigen Rechts

Bei der rechtlichen Auseinandersetzung mit verschiedenen Smart Cam-Varianten werden eine Vielzahl an Rechtsquellen auf vier Regulierungsebenen zugunsten eines Schutzes der bildlich Erfassten ins Feld geführt.<sup>15</sup> Auf der internationalen Ebene steht wegen der fortgesetzten Rechtsprechung des EGMR zum Recht am eigenen Bild Art. 8 Abs. 1 EMRK im Mittelpunkt, der die Achtung des Privat- und Familienlebens vorsieht. Auf EU-Ebene hat der EuGH die Datenschutzrichtlinie 95/46/EG bereits im Hinblick auf Maßnahmen der Videoüberwachung ausgelegt.<sup>16</sup> Auf Ebene des nationalen Verfassungsrechts werden aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG Persönlichkeitsrechte sowohl als Recht auf informationelle Selbstbestimmung als auch als Recht am eigenen Bild herangezogen, um die Zulässigkeit von Bilderstellung bzw. -veröffentlichung zu beurteilen. Aus dem nationalen einfachgesetzlichen Rechtsbestand schließlich werden Vorschriften des Bundesdatenschutzgesetzes und §§ 22, 23 Kunsturhebergesetz (Recht am eigenen Bild) geprüft. Hinzu kommt § 201a StGB, durch den u.a. die unbefugte Herstellung einer Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt und die damit den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt, unter Strafe gestellt wird.<sup>17</sup> Es ist hier nicht der Ort, die einschlägigen Vorschriften im Detail auszuleuchten. Es geht vielmehr darum, die Anwendungsdefizite herauszuarbeiten.

---

<sup>15</sup> Klar, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 47 ff.; Schwenke, Private Nutzung von Smartglasses im öffentlichen Raum, 2016, S. 93 ff.

<sup>16</sup> EuGH NJW 2015, 463.

<sup>17</sup> Eingehend Schwenke, Private Nutzung von Smartglasses im öffentlichen Raum, 2016, S. 258 ff.; Wieduwilt, K&R 2015, S. 83 (85).

Ein erstes Problem besteht darin, dass die genannten Vorschriften alle – begrenzte Ausnahme: § 201a StGB<sup>18</sup> – voraussetzen, dass sich die bildlich Erfassten zur Wehr setzen und Beseitigung und Unterlassen der Beeinträchtigung bzw. Ersatz des Persönlichkeitsschadens verlangen. Dazu müssen sie aber erst einmal wissen, dass sie fotografiert oder gefilmt worden sind, was bei den Smart Cam-Techniken gerade nicht gewährleistet ist, da die Geste des Fotografierens entfällt.

Ein zweites Problem betrifft den Umstand, dass das Bestehen der Rechte oft erst in einer Interessenabwägung geklärt werden muss, deren Ausgang völlig offen ist. Besonders gutes Anschauungsmaterial bietet hierfür der seit 2014 andauernde Streit der Instanzen um die Zulässigkeit der Verwendung von Dash Cam-Aufnahmen als Beweismittel in Zivil- und Strafprozessen. Weil es um Verkehrsrechtsstreitigkeiten geht, die sehr häufig gerichtlich entschieden werden, hat sich in kurzer Zeit ein ebenso reiches wie gegensätzliches Meinungsspektrum zum Umgang der unteren Gerichte mit Persönlichkeitsrechtsverletzungen durch Dash Cams ergeben. Anfangs prägten Entscheidungen des Amtsgerichts München<sup>19</sup> und des Landgerichts Heilbronn<sup>20</sup> den Meinungsstand, die auf ein Beweisverwertungsverbot hinsichtlich Dash Cam-Aufnahmen wegen Persönlichkeitsrechtsverletzungen erkannten. Dann aber trat eine Reihe von gegenteiligen Entscheidungen ins Licht der Öffentlichkeit. Um nur die höheren Instanzen zu nennen, sei auf das Landgericht Landshut,<sup>21</sup> das Landgericht Frankenthal<sup>22</sup> und das Oberlandesgericht Stuttgart<sup>23</sup> verwiesen, die nach Abwägung Dash Cam-Aufnahmen als Beweismittel zugelassen haben. Zählt man nur die in der Fachliteratur veröffentlichten Verfahren, steht es inzwischen 6:4 gegen ein Beweisverwertungsverbot.

Mangels einer konkreten technikspezifischen Dash Cam-Gesetzgebung werden in allen Verfahren technikneutrale Rechtsgrundsätze, General Klauseln und z.T. § 6b BDSG angewendet, die alle in einer Interessenabwägung im Einzelfall münden. Bei dieser Interessenabwägung ist es den Gerichten dann leicht möglich, völlig gegensätzliche Standpunkte einzunehmen. In den Urteilsbegründungen contra Beweisverwertung wird betont, dass langandauernde Aufzeichnungen durch Dash Cams schwerwiegende Persönlichkeitsrechtsverletzungen zur Folge hatten, während in

---

<sup>18</sup> Hierbei handelt es sich gemäß § 205 Abs. 1 Satz 2 StGB um ein relatives Antragsdelikt. In der Regel muss also auch hier der Verletzte tätig werden und die Strafverfolgung beantragen.

<sup>19</sup> AG München ZD 2014, 530.

<sup>20</sup> LG Heilbronn ZD 2015, 233.

<sup>21</sup> LG Landshut ZD 2016, 187.

<sup>22</sup> LG Frankenthal BeckRS 2016, 09839.

<sup>23</sup> OLG Stuttgart BeckRS 2016, 09359.

den Begründungen pro Beweisverwertung darauf abgestellt wird, dass die Dash Cam nur kurz in Betrieb war („immer wenn ein anderer komisch fahre“).<sup>24</sup> Könnte es sein, dass sich hier ein Lernprozess der Rechtsberatung niederschlägt, so dass in jüngerer Zeit nur noch kurze Aufnahmesequenzen in das Verfahren eingebracht worden sind?

Für den vorliegenden Zusammenhang vorrangig interessant ist allerdings, dass Interessenabwägungen mit bedeutenden Rechtsgütern auf beiden Seiten zu keinen verlässlichen Ergebnissen in der Rechtsprechung führen. Die Nutzung neuer Technologie erzeugt große Rechtsunsicherheit. Es sei zugegeben, dass es auch weniger problematische Konstellation gibt, in denen die Abwägung wohl weniger Streitig zwischen den Gerichten wäre. So dürfte das Führen einer Drohne über einem fremden Grundstück mit Person auf der Sonnenliege, gegen das ein Unterlassungsanspruch vom Amtsgericht Potsdam anerkannt wurde,<sup>25</sup> wohl kaum von anderen Gerichten anders beurteilt werden. Der Grund ist hier, dass die Belange, die der Drohnenverwender anzuführen hat, rechtlich sehr schwach erscheinen. Sobald aber starke – das heißt vor allem von speziellen Grundrechten getragene – Gründe auf beiden Seiten stehen, ist der Ausgang der Interessenabwägung nicht vorhersagbar. Rechtsunsicherheit besteht und schreckt von Rechtsverfolgung ab.

Das dritte Problem resultiert aus der Schwerfälligkeit des Gesetzgebers. Die hohe Innovationsgeschwindigkeit in der Informationstechnologie führt dazu, dass der Gesetzgeber mit seinen politischen Hemmnissen und aufwändigen Verfahren der technologischen Entwicklung systematisch hinterherläuft.<sup>26</sup> Hinsichtlich der Dash Cams wird vom Deutschen Verkehrsgerichtstag 2016 bereits ein Eingreifen des Gesetzgebers mit einer klaren gesetzlichen Regelung gefordert.<sup>27</sup> Wegen des hohen Konfliktpotenzials könnte es hier ausnahmsweise einmal schnell gehen und schon in der nächsten Legislaturperiode eine gesetzliche Regelung erfolgen.

### 3.2 Alternative Regulierung

Bevor alternative Regulierungskonzepte für die Nutzung von Dash Cams erörtert werden, sei kurz erwogen, ob die geschilderten Defizite nicht auch hinnehmbar sein könnten. Dass neue Technik erstmal gesellschaftlich erprobt und die unterschiedlichen Interessen – auch in gerichtlichen Auseinandersetzungen mit ungewissem Ausgang – ausgelotet und erörtert werden, bevor der Gesetzgeber eingreift, entspricht einer offenen

---

<sup>24</sup> LG Frankenthal BeckRS 2016, 09839.

<sup>25</sup> AG Potsdam ZD 2016, 236.

<sup>26</sup> Zum Umgang mit diesem Problem Sydow/Kring, ZD 2014, S. 271.

<sup>27</sup> Meldung in ZD-Aktuell 2016, 04973.

demokratischen Gesellschaft. Das gilt vor allem, wenn die gesellschaftlichen Normen im Fluss sind und die hergebrachten Grenzen zwischen Privatsphäre und Informationsfreiheit in Frage stehen und neu ausgehandelt werden müssen. Auch mag man es für ausreichend halten, dass der Einzelne sich aufgrund individueller Rechte wehren kann, wenn er sich durch den Eingriff des Fotografierens oder Filmens für erheblich belastet fühlt. Mindestvoraussetzung wäre aber auch bei einer solchen Beurteilung Transparenz. Der einzelne Abgebildete muss wenigstens wissen, dass Fotos oder Filme von ihm entstehen, sonst gehen individuelle Rechte völlig ins Leere. Es sind für ein solches Konzept technische Vorkehrungen erforderlich, die Transparenz herstellen. Diese müssten durch technische Vorschriften durchgesetzt werden.

Alternativ könnte erwogen werden, der Smart Cam-Technik weitgehende Freiräume zu gewähren, aber bestimmte konkrete Nutzungen rechtlich auszuschließen – z.B. heimliches Aufnehmen von Menschen. Da die Betroffenen in diesem Fall von einem Verstoß keine Kenntnis haben, müsste das Risiko der untersagten Handlung zwecks Abschreckung rechtlich z.B. durch Strafbarkeit in die Höhe getrieben werden.

Ein drittes Konzept setzt wiederum bei der Technik an, geht aber über Transparenz hinaus. Es wird seit Jahren unter dem Schlagwort „Privacy by Design“ erörtert.<sup>28</sup> Hard- und Software sollen von vornherein so konstruiert werden, dass der Schutz der Privatsphäre der Nutzer oder Dritter möglichst gewahrt wird. Es gibt viele Beispiele, wie dies möglich sein könnte. So ist die bereits erwähnte Datenbrille, die Emotionen für Autisten interpretiert, so konstruiert, dass die Daten das Gerät nicht verlassen und die Identität der erfassten Person nicht festgestellt wird. Bei Datenbrillen für Sehbehinderte könnte eine automatische Gesichtsidifizierung des Gegenübers erwünscht sein. Doch könnte diese auf einen selbst vom Träger eingegebenen Personenkreis beschränkt werden. Für Drohnen könnte eine Mindestgröße vorgeschrieben sein, damit sie sichtbar bleiben. Flugverbotszonen könnten programmiert werden.<sup>29</sup> Dash Cams könnten die Aufnahmen kurzfristig überschreiben und damit löschen.<sup>30</sup> Das ist sicher nur ein Einstieg in zahlreiche weitere Möglichkeiten, die zutage treten werden, wenn sich die Hard- und Softwareentwicklung erst einmal intensiv mit dem Thema befasst.

Das Problem besteht dann darin, was das Recht leisten kann, dass bestimmte die Privatsphäre schonenden Lösungen auch tatsächlich zur Anwendung kommen. Es müsste konkrete technische Regeln geben, mit de-

---

<sup>28</sup> *Boehme-Neßler*, ZG 2013, S. 242; *Hornung*, ZD 2011, S. 51.

<sup>29</sup> Stichwort „Geofencing“, siehe *Uschkereit/Zdanowiecki*, NJW 2016, S. 444 (445).

<sup>30</sup> *Knyrim/Trieb*, ZD 2014, S. 547 (551).

nen relativ kurzfristig technikspezifisch auf neue Entwicklungen reagiert wird. Sie sollten daher nicht vom Gesetzgeber selbst, sondern auf einer zweiten, schneller reagierenden Regulierungsebene formuliert werden. Der Gesetzgeber muss aber dafür sorgen, dass diese Regeln eine rechtliche Verbindlichkeit bekommen, die über bloße Empfehlungen deutlich hinausgeht.

### 3.3 Arbeitsschutz als Vorbild

Smart Cams stellen ein für den Menschen gefährliches technisches Produkt dar. Nicht Leben und Gesundheit sind gefährdet, sondern die persönliche Selbstbestimmung. Dennoch liegt es nah, in den Weiten des Technikrechts, dessen zentrales Ziel der Schutz von Leben und Gesundheit ist, nach erfolgreichen rechtliche Lösungen zu suchen, die auf den Schutz des Persönlichkeitsrechts übertragbar sind. Besonders intensiv wirkt das Technikrecht im Bereich des Arbeitsschutzes. Dort ist es gelungen, durch eine Modernisierung des Regulierungsregimes seit Mitte der 1990er Jahren den Schutz von Leben und Gesundheit der Beschäftigten dramatisch zu erhöhen. Die Zahl sowohl der tödlichen als auch insgesamt der meldepflichtigen Arbeitsunfälle konnte in den letzten 20 Jahren halbiert werden. Die Ursachen sind vielfältig, aber die grundlegende Neustrukturierung des Arbeitsschutzrechts dürfte einen wesentlichen Beitrag geleistet haben.

Der Gesetzgeber hat auch im Arbeitsschutzrecht mit dem Problem zu kämpfen, dass eine schnelle technische Entwicklung immer wieder neue Gefahren aufwirft, auf die kurzfristig reagiert werden muss. Es ist hier jedoch nicht der Rechtsprechung überlassen, die Generalklauseln des Gesetzes auf die konkreten Anforderungen einzelner Technikgestaltungen zu konkretisieren. Vielmehr dient hierzu ein System aus Verordnungen und Technischen Regeln.<sup>31</sup> In diesen häufig aktualisierten Regeln wird sehr praxisnah und anschaulich beschrieben, durch welche organisatorischen und technischen Maßnahmen die allgemeinen Anforderungen der Arbeitsschutzverordnungen erfüllt werden können.

Wichtig ist dabei, dass die Technischen Regeln keine bloßen Empfehlungen sind, sondern durch die Einbindung in die Verordnungswerke hohe Verbindlichkeit erlangen. Ähnlich formulierte Vorschriften in den verschiedenen Arbeitsschutzverordnungen ordnen an, dass der Arbeitgeber den Stand der Technik und insbesondere die vom Bundesministerium für Arbeit und Soziales bekannt gemachten Regeln und Erkenntnisse zu berücksichtigen habe. Bei Einhaltung der genannten Regeln und Erkennt-

---

<sup>31</sup> Zur Funktion und Problematik technischer Regelsetzung *Kloepfer*, Instrumente des Technikrechts, in: Schulte/Schröder, Handbuch des Technikrechts, 2011, S. 151 (178 ff.).

nisse sei davon auszugehen, dass die in der Verordnung gestellten Anforderungen erfüllt seien. Wende der Arbeitgeber die Regeln und Erkenntnisse nicht an, müsse er durch andere Maßnahmen die gleiche Sicherheit und den gleichen Gesundheitsschutz der Beschäftigten erreichen.<sup>32</sup>

Für die hohe Funktionstüchtigkeit dieser konkreten technikspezifischen Regulierungsebene sorgen fünf Ausschüsse beim BMAS mit jeweils mehreren Arbeitsgruppen unter Mitarbeit von Ingenieuren, Chemikern, Medizinern usw., die das Regelwerk regelmäßig überarbeiten und ergänzen. Das Vertrauen der Praxis wird durch Mitarbeiter der verschiedenen Interessengruppen gestärkt.

Vorbildlich für künftige Regelungen des Daten- und Persönlichkeitsschutzes nicht nur gegenüber Smart Cams könnten also erstens der hohe Konkretisierungs- und Verbindlichkeitsgrad der Technischen Regeln im Arbeitsschutz sowie zweitens die effektive Besetzung der die Regeln schaffenden Arbeitsschutzausschüsse sein.

## 4 Konsequenzen der DSGVO

### 4.1 Privacy by Design in der DSGVO

In der EU-Datenschutzgrundverordnung wird in Art. 25 unter dem Titel „Datenschutz durch Technikgestaltung“ das Konzept Privacy by Design erstmals europarechtlich formuliert. Danach hat der Verantwortliche (unter Beachtung einer Reihe von Kriterien) geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

*Hornung* hat schon 2011 zutreffend darauf hingewiesen, dass das Konzept eines Datenschutzes durch Technik zwei Adressaten haben muss: Hersteller für die faktische Verfügbarkeit der Technik und Anwender für den tatsächlichen Einsatz.<sup>33</sup> Hersteller sind in Art. 25 DSGVO nicht angesprochen.<sup>34</sup> Sie gehören nicht zum Adressatenkreis der Grundverordnung. Angesprochen sind allein die Verantwortlichen. Das sind jene Personen, die laut Art. 4 Ziff. 7 DSGVO über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden – also auf Seiten der Technikanwender. Dass die Hersteller von Drohnen, Dash Cams und

---

<sup>32</sup> Nach § 3a Abs. 1 Satz 2-4 ArbStättV, ähnlich § 7 Abs. 2 Satz 2-4 GefStoffV und § 4 Abs. 3 Satz 1-3 BetrSichV.

<sup>33</sup> *Hornung*, ZD 2011, S. 51 (52).

<sup>34</sup> *Schantz*, NJW 2016, S. 1841 (1846).

Datenbrillen in der DSGVO nicht adressiert werden, wird vollständig klar durch Erwägungsgrund 78. Denn hier heißt es, dass die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden sollen, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Die Hersteller werden also lediglich ermutigt, die Verantwortlichen und Verarbeiter hingegen werden durch die Normen der Verordnung verpflichtet.

Wenn also die Herstellung von Smart Cam-Technik nicht in den Anwendungsbereich der DSGVO fällt, heißt das vor allem, dass auch kein Anwendungsvorrang für die Regelungen der DSGVO in diesem Bereich zu beachten ist. Der nationale Gesetzgeber ist also frei, unabhängig von der DSGVO eigene technische Regelungen an die Adresse der Hersteller zu formulieren. *Hornung* und *Hartl*<sup>35</sup> befürchten, dass die absichtliche Nichtregelung der Materie produktbezogener Prüfsiegel in der DSGVO auch nationale Produktzertifizierungen sperren könnte. Der Produkthersteller fällt jedoch insgesamt aus dem Regelungsbereich der DSGVO heraus. Die Nichtregelung der Produktzertifizierung ist daher konsequent und heißt nichts weiter, als dass dieses Feld anderen Regelungswerken auf europäischer oder auch nationaler Ebene überlassen wird.

Gleichzeitig ist aber Art. 25 DSGVO damit für das vorliegende Thema nicht wirkungslos. Es verpflichtet den Verantwortlichen auf der Anwenderseite, die Technik auszuwählen, die dafür ausgelegt ist, die Rechte der Betroffenen zu schützen. Also muss etwa der Anwender einer Datenbrille für Sehbehinderte jenes Modell auswählen, das keine personenbezogenen Daten ins Internet überträgt und nur vorgegebene Personen erkennt. Indirekt kann damit auch das Herstellerangebot beeinflusst werden.

#### 4.2 Durchsetzung durch Zertifikate

In Art. 25 Abs. 3 DSGVO ist vorgesehen, dass die Verantwortlichen im Rahmen eines genehmigten Zertifizierungsverfahrens nachweisen, dass sie die Anforderungen des Datenschutzes durch Technikgestaltung bzw. durch datenschutzfreundliche Voreinstellungen erfüllen. Auch dies richtet sich an die Anwenderseite. Zertifikate für technische Produkte sind hier nicht gemeint.

Allerdings ist im Rahmen der Zertifizierung nach Art. 42 Abs. 1 DSGVO nicht völlig auszuschließen, dass auch für technische Produkte ein Daten-

---

<sup>35</sup> *Hornung/Hartl*, ZD 2014, S. 219 (224).



schutzsiegel vergeben werden kann, um dadurch die Verantwortlichen bei der Auswahl der datenschutzkonformen Technik zu unterstützen.

Auf jeden Fall könnte die Kommission im Rahmen von Art. 43 Abs. 8 DSGVO auch produktbezogene Anforderungen an die Zertifizierung von Verantwortlichen formulieren. Die Zertifizierung eines Verantwortlichen könnte davon abhängig gemacht werden, dass er nur Technik verwendet, die Privacy by Design-Kriterien entspricht. Nun erfolgt der Einsatz von Smart Cams vielfach von privaten Einzelpersonen, für die eine Zertifizierung z.B. ihrer Dash Cam-Nutzung ganz abwegig wäre. Aber auch Unternehmen setzen Smart Cams ein, so dass im Hinblick auf ein Zertifikat nach Art. 42 DSGVO der Einsatz datenschutzfreundlicherameratechnik, für die konkrete technische Anforderungen gemäß Art. 43 Abs. 8 DSGVO formuliert werden, sinnvoll zur Voraussetzung gemacht werden könnte.

## 5 Perspektiven des Projekts ChaRiSma

Im kommenden zweiten Projektjahr wird das Forschungsprojekt ChaRiSma verschiedene Regelungsalternativen für Smart Cams im öffentlichen Raum entwerfen und auf Vor- und Nachteile durchleuchten. Viele der hier eher thesenhaft angerissenen Punkte werden noch näher zu untersuchen sein: Welche Belange von Smart Cam-Nutzern sind so gewichtig, dass sie auch Eingriffe in Persönlichkeitsrechte von bildlich Erfassten rechtfertigen? Welche technischen Lösungen gibt es, die ausreichend Rücksicht auf Persönlichkeitsrechte nehmen, und wie können diese mit hoher Zuverlässigkeit implementiert werden? Sind nationale Lösungen z.B. der Zertifizierung technischer Produkte anzustreben oder kann eine solche auch auf die DSGVO gestützt werden? Ist das europäische Recht in diesem Sinne zu ergänzen? Ergebnisse der Überlegungen zu diesen und weiteren Fragen werden zu gegebener Zeit zur Diskussion gestellt werden.

## Literatur

*Boehme-Neßler, Volker*: BilderRecht: Die Macht der Bilder und die Ohnmacht des Rechts, Berlin/Heidelberg 2010.

*Boehme-Neßler, Volker*: Privacy by Design – Der EU-Datenschutz als Modell moderner Gesetzgebung, ZG 2013, S. 242-249.

*Fuchs, Daniel*: Verwendung privater Kameras im öffentlichen Raum – Datenschutz bei Dash-Cams, Helm-, Wildkameras & Co., ZD 2015, S. 212-217.

- Hornung, Gerrit*: Datenschutz durch Technik in Europa. Die Reform der Richtlinie als Chance für ein modernes Datenschutzrecht, ZD 2011, S. 51-56.
- Hornung, Gerrit/Hartl, Korbinian*: Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit, ZD 2014, S. 219-225.
- Klar, Manuel*: Datenschutzrecht und die Visualisierung des öffentlichen Raums, Berlin 2012.
- Kloepfer, Michael*: Instrumente des Technikrechts, in: Martin Schulte/Rainer Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl., Berlin/Heidelberg 2011, S. 151-199.
- Knyrim, Rainer/Trieb, Gerald*: Videokameras in Autos – vom Teufelszeug zum Beweismittel. Vereinbarkeit von Dash-Cams mit datenschutzrechtlichen Grundsätzen, ZD 2014, S. 547-552.
- Schantz, Peter*: Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841-1847.
- Schwenke, Thomas*: Private Nutzung von Smartglasses im öffentlichen Raum, Edeweicht 2016.
- Sydow, Gernot/Kring, Markus*: Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug. Konkurrierende Leitbilder für den europäischen Rechtsrahmen, ZD 2014, S. 271-276.
- Todorov, Alexander/Porter, Jenny M.*: Misleading First Impressions: Different for Different Facial Images of the Same Person, Psychological Science, vol. 25 no. 7, July 2014, pp. 1404–1417.
- Uschkereit, Tim/Zdanowiecki, Konrad*: Rechtsrahmen für den Betrieb ziviler Drohnen, NJW 2016, S. 444-449.
- Vernon, Richard J. W./Sutherland, Clare A. M./Young, Andrew W./Hartley, Tom*: Modeling first impressions from highly variable facial images, Proceedings of the National Academy of Sciences of the United States of America (PNAS), vol. 111 no. 32, August 2014, E3353-E3361.
- Wieduwilt, Hendrik*: Neues Fotorecht im öffentlichen Raum, K&R 2015, S. 83-85.
- Willis, Janine/Todorov, Alexander*: First Impressions. Making up your Mind after a 100-Ms Exposure to a Face, Psychological Science, vol. 17 no. 7, July 2006, pp. 592–598.