Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 9-21
Stauffenburg Verlag Tübingen

Who Watches the Watchmen? – Datenschutzrechtliche Anforderungen an Überwachungssysteme

Maria Wilhelm, Leitung der Stabsstelle Europa beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Summary. Monitoring systems can be used by both private and public bodies. The European legislator created the legal basis and limits with the General Data Protection Regulation (GDPR; Regulation (EU) 2016/679) and the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Directive (EU) 2016/680). These also provide control and law enforcement possibilities for the data protection supervisory authorities. The granting of sufficient transparency is a central issue, especially in the area of video surveillance. Based on the discussion of the legal conformity of the data protection requirements themselves, the way in which information is provided is debated in this field. Here, the potential of data protection regulations remains largely unexploited.

Zusammenfassung. Überwachungssysteme können durch private und durch öffentliche Stellen eingesetzt werden. Rechtliche Grundlagen und Grenzen wurden durch den europäischen Gesetzgeber mit der Datenschutz-Grundverordnung (DS-GVO; Verordnung (EU) 2016/679) und der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (JI-RL; Richtlinie (EU) 2016/680) geschaffen. Diese sehen auch Kontroll- und Rechtdurchsetzungsmöglichkeiten für die Datenschutzaufsichtsbehörden vor. Die Gewährung von hinreichender Transparenz ist gerade im Bereich der Videoüberwachung eine zentrale Fragestellung. Ausgehend von der Diskussion der Rechtskonformität der datenschutzrechtlichen Vorgaben selbst wird in diesem Bereich die Art und Weise der Informationserteilung diskutiert. Hierbei bleiben Potenziale der datenschutzrechtlichen Vorgaben weitgehend ungenutzt.

1. Einleitung

Angesichts der Innovationen der letzten Jahre sieht der Mensch sich immer mehr Techniken der modernen Datenverarbeitung gegenüber, die neben anderen Verwendungszwecken auch für Überwachungsmaßnahmen eingesetzt werden können (vgl. etwa Weichert 2013: 251). Neben den Möglichkeiten der Auswertung von Kommunikationsverhalten im Online-Bereich und insbesondere innerhalb sozialer Netzwerke wurden aber auch auf eine längere historische Entwicklung zurückzuführende Beobachtungsmaßnahmen wie optische Überwachungsmittel revolutioniert. Mittels automatisierter Gesichtserkennung können Bewegungsprofile erstellt werden und sogar Gesten oder Körperbewegungen so genau abgeglichen werden, dass einzelne Personen identifiziert werden können (ausführlich Heldt 2019: 285). Die Bildung von Profilen ist Teil unseres Alltags geworden und im Bereich der interessensbasierten Werbung wie auch bei der Bildung unseres Bonitäts-Scorewertes durch Kreditauskunfteien ein zentrales Werkzeug (noch zur alten Rechtslage Arning und Moos 2014: 242; Schantz 2019b: Rn. 131). In Weiterentwicklung dieser Systeme ist China das erste Land, das ein umfangreiches staatliches Social Scoring System flächendeckend einführen will (Chinese State Council 2014: 1).

All diese Modelle bewegen sich nicht im rechtsfreien Raum, sondern tangieren Grundrechte und sehen sich den Regulierungsbemühungen des Gesetzgebers gegenüber. Dieser hat mit der Einrichtung unabhängiger Aufsichtsbehörden Kontrollorgane geschaffen, durch welche die Durchsetzung dieser Regelungen forciert und gewährleistet wird (Lewinski 2017: 1483). In materieller Hinsicht existieren Transparenzvorschriften, durch die Grundrechtseingriffe offen gelegt und Datenverarbeitungen nachvollziehbar gemacht werden. Hierdurch sollen die betroffenen Personen zu angemessenen eigenen Rechtsschutzmaßnahmen oder der Hinzuziehung der Kontrollorgane befähigt werden (Grittmann 2019: Art. 51, Rn. 9). Die Zurverfügungstellung von Informationen bedeutet aber nicht immer zugleich, dass bestimmte Vorgänge transparenter werden. Es kommt hier entscheidend darauf an, welche Informationen in welcher Art und Weise transportiert werden. Nur so kann effizient Transparenz von Datenverarbeitungsprozessen gewährleistet werden (vgl. die Kritik bei Wilhelm 2016: 903). Es bedarf also einer Rückbesinnung auf das eigentliche Schutzgut des Datenschutzes, um die gesetzlichen Vorschriften sinnvoll anwenden zu können.

2. Gesetzliche Grundlagen

Im Rahmen der letzten europäischen Datenschutzreform wurden sowohl die allgemein automatisierte Datenverarbeitungen betreffende Datenschutz-Grundverordnung (DS-GVO, ABl. L 119/1 vom 04. Mai 2016) – gemäß Artikel 2 Absatz 1 DS-GVO unterfallen ihr alle automatisierten und teilwiese

auch die nicht automatisierten Verarbeitungen personenbezogener Daten, soweit diese in einem Dateisystem gespeichert sind – als auch die JI-RL für den Bereich der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie der Strafverfolgung (ABl. L 119/89 vom 04. Mai 2016) erlassen. Diese beiden sekundärrechtlichen Rechtsakte sind jeweils im Lichte des Datenschutzgrundrechts aus Artikel 8 Grundrechtecharta (GRCh) auszulegen (vgl. Sydow 2018: Rn. 7).

2.1 Datenschutzgrundrecht

Artikel 8 GRCh enthält das Datenschutzgrundrecht auf europäischer Ebene. Was genau der Inhalt dieser Rechtsposition ist, ist durch autonome Auslegung der europäischen Vorschrift zu ermitteln (vgl. Wegener 2016, Rn. 13 mit weiteren Nachweisen). Hierbei müssen die Rechtsauffassungen der europäischen Mitgliedstaaten berücksichtigt werden (Huber 2018: Rn. 14). Das herkömmliche deutsche Verständnis von einem aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz (GG) hergeleiteten Grundrecht auf informationelle Selbstbestimmung muss somit durch ein autonomes Verständnis des europäischen Datenschutzgrundrechts ersetzt werden (vgl. dazu Sydow 2018: Rn. 7ff.).

2.2 DS-GVO und flankierende Gesetze

Die DS-GVO gilt von ihrem sachlichen Anwendungsbereich in Artikel 2 Absatz 1 DS-GVO Verarbeitungen für personenbezogene Daten, die vollständig oder teilweise automatisiert sind und in Bezug auf die Speicherung in Dateisystemen auch für nichtautomatisierte Verarbeitungen personenbezogener Daten. Aus dem allgemeinen Grundsatz der Rechtsmäßigkeit der Verarbeitung personenbezogener Daten aus Artikel 5 Absatz 1 Buchstabe a) DS-GVO folgen die Vorschriften der Artikel 6 bis 10 DS-GVO, in denen zulässige Rechtsgrundlagen für die von der DS-GVO erfassten Datenverarbeitungen genannt werden. An gleicher prominenter Stelle in Artikel 5 Absatz 1 Buchstabe a) DS-GVO wird auch der Grundsatz der Transparenz genannt, sodass eine Datenverarbeitung nicht nur auf einer validen Rechtsgrundlage beruhen, sondern immer auch hinreichend transparent ausgestaltet sein muss (Schantz 2019a: Rn. 5, 6 und 11). Daneben finden sich mit dem Grundsatz der Datenverarbeitung nach Treu und Glauben, den Grundsätzen der Zweckbindung der Datenminimierung, der Datenrichtigkeit, der Speicherbegrenzung und der Integrität und Vertraulichkeit in Artikel 5 Absatz 1 DS-GVO weitere Grundsätze, die bei der Auslegung der gesamten Verordnung beachtet werden müssen. Der zuvor genannte Grundsatz der Transparenz wird daneben durch zahlreiche Einzelverbürgungen der Verordnung konkretisiert (Herbst 2018: Rn. 19), wobei die prominentesten die Informationspflichten aus Artikel 13 und 14 DS-

GVO sein dürften, aufgrund derer Datenschutzhinweise erstellt werden müssen (vgl. Franck 2018: Rn. 2).

Die DS-GVO gilt nach Artikel 288 Absatz 1 des Vertrages über die Arbeitsweise in der europäischen Union (AEUV) unmittelbar in allen europäischen Mitgliedstaaten und bedarf keiner Umsetzung in nationales Recht (Vedder 2018: Rn. 18). Die Verordnung enthält zu einzelnen inhaltlichen Fragestellungen aber Öffnungsklauseln, mithilfe derer der europäische Gesetzgeber den Mitgliedstaaten wieder Regelungsspielräume überlässt (kritisch dazu Laue 2016: 463, 464 und 467). Zur Ausfüllung dieser Regelungsspielräume hat der deutsche Bundesgesetzgeber das Bundesdatenschutzgesetz (BDSG vom 30. Juni 2017 (BGBl. I S. 2097)) für Datenverarbeitungen durch private Stellen und öffentliche Stellen des Bundes und zahlreiche fachspezifische Normen erlassen (vgl. dazu den Gesetzesentwurf der Bundesregierung 1-212). Bezüglich der öffentlichen Stellen der Länder finden sich die DS-GVO flankierenden Gesetze in den Landesdatenschutzgesetzen (vgl. etwa das Landesdatenschutzgesetz Baden-Württemberg vom 12. Juni 2018 (GBl. S. 173)).

Die DS-GVO gilt auch für Straftaten und Ordnungswidrigkeiten verfolgende Behörden, soweit diese unter anderem übliche Verwaltungstätigkeiten wahrnehmen, Öffentlichkeitsarbeit leisten, Beschaffungsgeschäfte durchführen oder politisch tätig werden (vgl. Hornung und Spiecker gen. Döhmann 2019: Rn. 215). Für den verfolgenden Bereich wurden in Form der JI-Richtlinie jedoch Spezialvorschriften geschaffen.

2.3 JI-RL und Umsetzungsrechtsakte

Werden Behörden zum Zwecke der „Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung“ tätig, so finden sich spezielle europarechtliche Vorgaben in der JI-RL. Im strafverfolgenden Bereich gelten hierbei andere Maßstäbe an Transparenzvorschriften, da ansonsten die Effektivität der Strafverfolgung beeinträchtigt würde (vgl. Artikel 13 Absatz 3 JI-RL). Die JI-RL ist gemäß Artikel 288 Absatz 3 AEUV nur hinsichtlich ihrer Zielvorgaben verbindlich für die Mitgliedstaaten und muss von diesen in nationales Recht umgesetzt werden (vgl. Vedder 2018: Rn. 23 und 24). Eine hohe Anzahl an Umsetzungsmaßnahmen wird in den Polizeigesetzen des Bundes und der Länder zu finden sein, sofern sie bereits an die neue Richtlinie angepasst wurden (zum Stand der Anpassung der Bundesgesetze BfDI: 1).

2.4 Befugnisse der Aufsichtsbehörden

Artikel 8 Absatz 3 GRCh ordnet auf der höchsten Ebene der Normenhierarchie an, dass die Einhaltung der datenschutzrechtlichen Grundsätze aus Artikel 8 GRCh durch unabhängige Stellen überwacht wird. In diesem Sinne

sieht Artikel 51 Absatz 1 DS-GVO die Einrichtung von unabhängigen Datenschutzaufsichtsbehörden vor, die in Artikel 57 und 58 DS-GVO mit Aufgaben und Befugnissen ausgestattet werden (vertiefend Nguyen 2015: 265). Ähnliche Anforderungen an die Errichtung von unabhängigen Aufsichtsbehörden finden sich in Artikel 41 JI-RL, wobei Aufgaben und Befugnisse in Artikel 46 und 47 JI-RL geregelt werden.

3. Transparenz als Grundsatz des Datenschutzrechts am Beispiel der DS-GVO

Die DS-GVO beinhaltet eine Vielzahl an Transparenzvorschriften von denen neben dem Grundsatz der Transparenz aus Artikel 5 Absatz 1 Buchstabe a) DS-GVO die umfangreichste Verpflichtung in Form einer allgemeinen Rechenschaftspflicht in Artikel 5 Absatz 2 DS-GVO enthalten ist (vgl. dazu die Anforderungen bei Roßnagel 2019: Rn. 181, 182 und 183).

3.1. Der Grundsatz der Rechenschaftspflicht in Artikel 5 Absatz 2 DS-GVO

Der Grundsatz der Rechenschaftspflicht aus Artikel 5 Absatz 2 DS-GVO stellt Anforderungen an die Transparenzanforderungen von Datenverarbeitungen. Gemäß der Norm ist der Verantwortliche für die Einhaltung der oben dargestellten Grundsätze der DS-GVO verantwortlich. Hierauf bezogen stellt die Norm eine Nachweispflicht auf, die den Verantwortlichen zu hinreichenden organisatorischen Maßnahmen und Dokumentationen bringen soll, um die Rechtmäßigkeit des eigenen Handeln nachweisen zu können (Roßnagel 2019: Rn. 181, 183). Durch diese Verteilung der Nachweislast werden durch die Datenverarbeitungen betroffenen Personen entlastet und ihre Rechtsschutzmöglichkeiten vergrößert (vgl. Voigt 2019: Rn. 40). Wird eine für die Verarbeitung von personenbezogenen Daten verantwortliche Stelle von der zuständigen Aufsichtsbehörde kontrolliert, so muss die verantwortliche Stelle nachweisen können, dass sie die personenbezogenen Daten rechtskonform verarbeitet (Roßnagel 2019: Rn. 186).

In erster Linie werden aus der Grundnorm des Artikels 5 Absatz 2 DS-GVO direkt interne Dokumentationspflichten wie Mitarbeiterrichtlinien und Dokumentationen im Rahmen der internen Datenverarbeitungsprozesse abgeleitet (vgl. Pötters 2018: Rn. 33). Aber auch alle anderen Transparenzvorschriften der DS-GVO können als Konkretisierung dieser generellen Nachweispflicht gesehen werden (in Bezug auf Art. 30 DS-GVO bejahend Roßnagel 2019: Rn. 183 und 184).

3.2 Datenschutzhinweise als Transparenzmaßnahmen der DS-GVO

Artikel 13 und 14 DS-GVO sehen bestimmte Vorschriften vor, nach denen betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten informiert werden müssen. Artikel 13 DS-GVO gilt für die Direkterhebung von Daten bei der betroffenen Person und Art. 14 DS-GVO für die Erhebung von anderer Stelle. Artikel 13 Absatz 1 und Artikel 14 Absatz 1 DS-GVO haben gemein, dass über Namen und Kontaktdaten der verantwortlichen Stelle, gegebenenfalls über die Kontaktdaten des Datenschutzbeauftragten, die Zwecke und die Rechtsgrundlage der Verarbeitung, Empfänger oder Kategorien von Empfängern und – falls vorhanden – die Absicht eines Drittlandtransfers informiert werden muss. Hinzu kommen die in Artikel 13 Absatz 2 und 14 Absatz 2 DS-GVO geforderten zusätzlichen Informationen, um „eine faire und transparente Verarbeitung zu gewährleisten". In der Praxis werden die beschriebenen Informationen in der Regel in der Form von Datenschutzerklärungen und Datenschutzhinweisen zur Verfügung gestellt (vgl. für Webseiten Stiemerling und Lachenmann 2014: 133).

Gemäß Artikel Absatz 12 Satz 1 DS-GVO sind diese Hinweise in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu übermitteln. Dies stellt für die Verarbeitung verantwortliche Stellen üblicherweise vor Herausforderungen. So nehmen die zur Verfügung zu stellenden Informationen einiges an Raum ein (vgl. auf Webseiten bezogen Stiemerling und Lachenmann 2014: 134). Auf europäischer Ebene hat der Europäische Datenschutzausschuss daher die Guidelines der Arikel-29-Datenschutzgruppe bestätigt, nach denen diese Hinweise gestuft zur Verfügung gestellt werden können (Artikel-29-Datenschutzgruppe, S. 23–24). Ausführliche Informationen können verlinkt oder mittels QR-Code eingebunden werden und nur die wesentlichen Informationen müssen auf der obersten Informationsebene enthalten sein (mit weiteren Beispielen Artikel-29-Datenschutzgruppe, S. 26).

Auch in sprachlicher Hinsicht sind die Erklärungen verständlich zu fassen. Wird beispielsweise ein konkretes Angebot vorwiegend den Einwohnern eines bestimmten Mitgliedstaates zur Verfügung gestellt, so müssen die Datenschutzhinweise auch in der Sprache dieses Staates zur Verfügung gestellt werden (Paal und Hennemann 2018: Rn. 35).

3.3 Verhaltenssteuerung durch Transparenzmaßnahmen

„Tools shape us as much as we shape them" (CNIL 2019: 6). Dieser Satz ist in einer Publikation der französischen Datenschutzaufsichtsbehörde zu lesen. Grafische Oberflächen und Transparenzwerkzeuge können uns genauso beeinflussen, wie wir sie beeinflussen (vgl. CNIL 2019: 6). Im Zuge der wachsenden Anzahl an wissenschaftlichen Arbeiten, Studien

und anderen Publikationen in diesem Feld (vgl. CNIL 2019: 45) wurden in diesem Bereich einige Hauptmethoden der Verhaltenssteuerung herausgearbeitet: So können die von der Verarbeitung personenbezogener Daten betroffenen Personen durch Nudging beeinflusst werden, wenn Ihnen durch kurzfristige Belohnungen Anreize und somit eine subjektive Tendenz für eine bestimmte Entscheidung mitgegeben werden (vgl. grundlegend Thaler und Sunstein 2008: 6; vgl. auch Forbrukerrådet 2018: 6–7). Diese Maßnahmen können von Framing und Priming durch fortgehende Betonung der positiven Aspekte der Datenverarbeitung (vgl. Forbrukerrådet 2018: 22–25) flankiert werden. Durch all diese Maßnahmen werden die Entscheidungen betroffener Personen oft in Richtung der Bejahung einer automatisierten Datenverarbeitung beeinflusst (vgl. CNIL 2019: 10).

3.4 Bildsymbole und andere Lösungen

Nach Artikel 12 Absatz 7 DS-GVO besteht die Möglichkeit, Datenschutzhinweise und -erklärungen mit standardisierten Bildsymbolen zu versehen. Gemäß Artikel 12 Absatz 8 DS-GVO ist die europäische Kommission im Zuge der Rechtssicherheit dazu berechtigt, in diesem Bereich einen delegierten Rechtsakt zu erlassen. Ein erster Entwurf derartiger Bildsymbole im Anhang der „Legislativen Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))“ des Europäischen Parlaments konnte sich innerhalb des Gesetzgebungsverfahrens zur DS-GVO leider nicht durchsetzen. Dies liegt vermutlich daran, dass die in den Datenschutzhinweisen beschriebenen Prozesse derart komplex sind, dass Grafiken sich nicht aus sich selbst heraus erklären und vom Betrachter nicht direkt gedeutet werden können. Erst wenn hier Standards gesetzt werden und allgemein geltende Symbole zentral bekannt gemacht werden, können betroffene Personen sich beim Betrachten erschließen, was die Bildsymbole bedeuten.

In der Zukunft sind besonders in diesem Bereich vereinfachende Innovationen gefragt, um die Selbstbestimmung der betroffenen Personen zu stärken (vgl. CNIL 2019: 44).

Es werden nicht mehr personenbezogene Daten erhoben, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.

Es werden nicht mehr personenbezogene Daten gespeichert, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.

Personenbezogene Daten werden nicht zu anderen als den Zwecken verarbeitet, für die sie erhoben werden.

Es werden keine personenbezogenen Daten an gewerbliche Dritte weitergegeben.

Es werden keine personenbezogenen Daten **verkauft oder verpachtet**.

Abb. 1: Quelle: Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)): (2017/C 378/55).

4. Transparenz und Videoüberwachung

Im Bereich der Verarbeitung personenbezogener Daten zur Videoüberwachung sieht sich die Umsetzung von Transparenzvorschriften gleich mehreren Schwierigkeiten gegenüber. Zum einen wird die Europarechtskonformität der deutschen gesetzlichen Vorschriften diskutiert (vgl. Brink und Wilhelm 2019: Rn. 18), zum anderen müssen die konkreten Transparenzmaßnahmen aber auch für alle Menschen erfassbar gestaltet werden.

4.1 Gesetzgeberische Regelungen

Neben den durch die DS-GVO vorgegebenen Vorschriften der Art. 13 und 14 DS-GVO sieht § 4 Abs. 2 BDSG vor, dass der „Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen […] durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen" sind. Diese Spezialregelung für den Bereich der Videoüberwachung stellt sicher, dass bei Hinweisschildern zu Videoüberwachungsanlagen kein erheblicher Suchaufwand für betroffene Personen besteht (Brink und Wilhelm 2019: Rn. 38). Werden Daten einer bestimmten Person zugeordnet, verweist § 4 Absatz 4 BDSG auf die Artikel 13 und 14 DS-GVO. Da bei Videoüberwachungsanlagen grundsätzlich eine dahingehende Gefährdungslage anzunehmen ist, werden in der Regel daher nur die allgemeinen Artikel 13 und 14 DS-GVO anwendbar sein (Brink und Wilhelm 2019: Rn. 39).

Die Vorschrift des § 4 BDSG wird jedoch bezüglich ihres Geltungsanspruches für die Rechtmäßigkeiten der Datenverarbeitungen im nichtöffentlichen Bereich kritisiert, da der europäische Gesetzgeber gerade hier keine Öffnungsklausel für Regelungen des nationalen Gesetzgebers belassen hat (vgl. unter anderem DSK 2018: 1). Insoweit sind auch nach der Rechtsprechung des Bundesverwaltungsgerichtes die vorrangig geltenden Regelungen des Artikels 6 Absatz 1 Satz 1 Buchstabe f) DS-GVO heranzuziehen (BVerwG, Urt. v. 27.3.2019 – 6 C 2/18).

4.2 Praktische Umsetzung

Auch bezüglich der praktischen Implementierung wirft die Umsetzung der Transparenzvorschriften im Bereich der Videoüberwachung noch Fragen auf. Zwar ist die Videoüberwachung einer der wenigen Bereiche, in denen die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein gemeinsames Musterhinweisschild entwickelt haben. Dieses kann ausgefüllt werden und bietet insofern eine Vereinfachung im Rahmen der Handhabung der DS-GVO.

Im täglichen Gebrauch bestehen aber gerade im Bereich der Videoüberwachung erschwerende praktische Probleme. So können beispielsweise Sehgeschädigte nicht inkludiert werden, solange nur mit Hinweisschildern

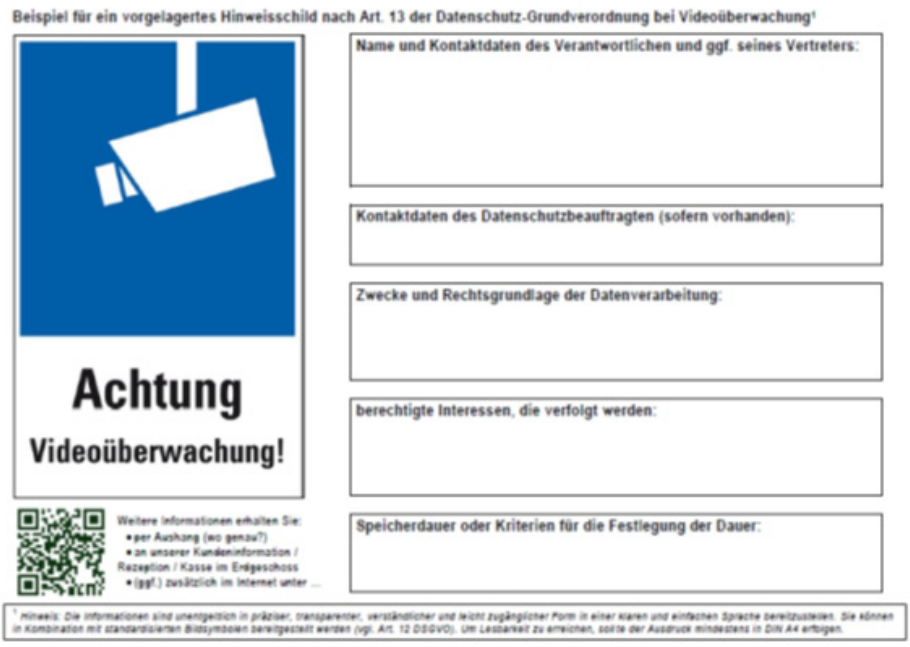

Abb. 2: Von den deutschen Datenschutzaufsichtsbehörden erarbeitete Vorlage für Datenschutzhinweise beim Betrieb einer Videoüberwachungsanlage; bereit gestellt von der LfD Niedersachsen.

gearbeitet wird. Automatisierte Lösungen führen oft zu weiteren Datenerhebungen, die theoretisch wiederum Targeting oder Profiling ermöglichen könnten und entsprechen somit oftmals nicht dem Grundsatz der Datenminimierung. Auch die Abgrenzung durch spezielle Bodenbeläge, durch die man den Beginn des videoüberwachten Bereichs mit Hilfsmitteln ertasten kann, sind aufgrund der hohen Präsenz von Videoüberwachungsanlagen im öffentlichen Raum schwer umzusetzen. Gerade in diesem Bereich sind jedoch Innovationen gefragt, da ansonsten die Verwirklichung der eigenen Rechte für im hohen Maße schutzbedürftige Personen am schwersten ist.

5. Ausblick

DS-GVO und JI-RL bilden zusammen mit den nationalen Vorschriften der Mitgliedstaaten einen neuen Rechtsrahmen für staatliche und private Überwachungsmaßnahmen, der auch eine unabhängige Kontrolle durch Aufsichtsbehörden ermöglicht. Neben dem Bestehen einer Rechtsgrundlage ist für den Schutz der betroffenen Personen aber auch die Transparenz der Maßnahmen entscheidend, da sie ansonsten keinen Rechtsschutz suchen können. Die immer komplexer und leistungsfähiger werdenden technischen Überwachungsanlagen fordern ein erhöhtes Maß an Transparenz, um die Selbstbestimmung betroffener Personen zu schützen. Hierbei gilt es, gra-

fische und technische Lösungen zu finden, die nicht anfällig für versteckte verhaltenssteuernde Maßnahmen sind. Die Entwicklung vereinfachter grafischer Darstellungen muss ebenso vorangetrieben werden und es müssen Lösungen gefunden werden, die alle Menschen inkludieren. Insoweit gilt es, Datenschutzhinweise in Zukunft nicht nur an den rechtlichen Voraussetzungen auszurichten, sondern auch die Erkenntnisse aus anderen Fachdisziplinen miteinzubinden.

Literatur

Arning, Marian und Flemming Moos (2014). Big Data bei verhaltensbezogener Online-Werbung. Programmatic Buying und Real Time Advertising. *Zeitschrift für Datenschutz* 4, 5, 242–248.

Artikel-29-Datenschutzgruppe. Leitlinien für Transparenz gemäß der Verordnung 2016/679. Angenommen am 29. November 2017. Zuletzt überarbeitet und angenommen am 11. April 2018. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 [Letzter Zugriff am 04.10.2019].

Brink, Stefan und Maria Wilhelm (2019). BDSG § 4. In: Heinrich Amadeus Wolff und Stefan Brink (eds.). *BeckOK Datenschutzrecht.* München: C.H. Beck, Rn. 1–84.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Umsetzung der JI-Richtlinie in Deutschland. URL: https://www.bfdi.bund.de/DE/Datenschutz/Themen/Sicherheit_Polizei_Nachrichtendienste/SicherheitArtikel/JI-Richtlinie.html [Letzter Zugriff am 04.10.2019].

Bundesregierung, Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU). URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/dsanpug.html [Letzter Zugriff am 04.10.2019].

Chinese State Council, Planning Outline for the Construction of a Social Credit System (2014–2020). 14. Juni 2014. URL: https://chinacopyrightandmedia.wordpress.com/2014/06/14/ [Letzter Zugriff am 02.10.2019].

Commission Nationale de l'Informatique et des Libertés (2019). Shaping Choices in the Digital World. From. *IP Reports* N°06. URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf [Letzter Zugriff am 04.10.2019].

Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)(2018). *Kurzpapier Nr. 15.* Videoüberwachung nach der Datenschutz-Grundverordnung URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf [Letzter Zugriff am 04.10.2019].

Europäisches Parlament. Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE#title2 [Letzter Zugriff am 04.10.2019].

Forbrukerrådet (2018). Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy. URL: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [Letzter Zugriff am 04.10.2019].

Franck, Lorenz (2018). Art. 13 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten bei der betroffenen Person. In: Peter Gola (ed.). *DS-GVO*. München: C.H. Beck, Rn. 1–59.

Grittmann, Joachim (2019). Art. 51. In: Jürgen Taeger, Detlev Gabel und Joachim Grittmann (eds.). *DS-GVO*. Frankfurt am Main: Fachmedien Recht und Wirtschaft / dfv Mediengruppe.

Heldt, Amélie P. (2019). Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raum. *MultiMedia und Recht* 22, 5, 285–289.

Herbst, Tobias (2018). Art. 5. Grundsätze für die Verarbeitung personenbezogener Daten. In: Jürgen Kühling und Benedikt Buchner (eds.). *DS-GVO*. München: C.H. Beck, 210–232.

Hornung, Gerrit und Indra Spiecker gen. Döhmann (2019). Einleitung. In: Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann (eds.). *Datenschutzrecht.* Baden-Baden: Nomos, 158–240.

Huber, Peter M. (2018). Art. 19. In: Rudolf Streinz (ed.). *EUV/AEUV*. München: C.H. Beck.

Laue, Philip (2016). Öffnungsklauseln in der DS-GVO – Öffnung wohin? Geltungsbereich einzelstaatlicher (Sonder-)Regelungen. *Zeitschrift für Datenschutz* 6, 10, 463–467.

Lewinski, Kai von (2017). Datenschutzaufsicht in Europa als Netzwerk. *Neue Zeitschrift für Verwaltungsrecht* 36, 20, 1483–1490.

Nguyen, Alexander (2015). Die zukünftige Datenschutzaufsicht in Europa. *Zeitschrift für Datenschutz* 5, 6, 265–270.

Paal, Boris P. und Moritz Hennemann (2018). Art. 12. In: Boris P. Paal und Daniel A. Pauly (eds.). *DS-GVO*. München: C. H. Beck, Rn. 33–35.

Pötters, Stephan (2018). Art. 5. Grundsätze für die Verarbeitung personenbezogener Daten. In: Peter Gola (ed.). *DS-GVO*. München: C.H. Beck, 216–223.

Roßnagel, Alexander (2019). Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten. In: Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann (eds.). *Datenschutzrecht.* Baden-Baden: Nomos, 363–398.

Schantz, Peter (2019a). Art. 5. In: Heinrich Amadeus Wolff und Stefan Brink (eds.). *BeckOK Datenschutzrecht*. München: C.H. Beck.

Schantz, Peter (2019b). Art. 6 Abs. 1 Rechtmäßigkeit der Verarbeitung. In: Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann (eds.). *Datenschutzrecht*. Baden-Baden: Nomos, Rn. 133–139.

Stiemerling, Oliver und Matthias Lachenmann (2014). Erhebung personenbezogener Daten beim Aufruf von Webseiten – Notwendige Informationen in Datenschutzerklärungen. *Zeitschrift für Datenschutz* 4, 3, 133–136.

Sydow, Gernot (2018). Einleitung. In: Gernot Sydow (ed.). *Europäische Datenschutzgrundverordnung.* Baden-Baden: Nomos, 245–304.

Thaler, Richard H. und Cass R. Sunstein (2008). *Nudge, Improving Decisions About Health, Wealth and Happiness.* New York: Penguin.

Vedder, Christoph (2018). Art. 288. In: Christoph Vedder und Wolff Heintschel von Heinegg (eds.). *Europäisches Unionsrecht.* Baden-Baden: Nomos.

Voigt, Paul (2019). Art. 5. In: Jürgen Taeger, Detlev Gabel und Paul Voigt (eds.). *DSGVO/BDSG*. Frankfurt am Main: Fachmedien Recht und Wirtschaft / dfv Mediengruppe.

Wegener, Bernhard W. (2016). Art. 18. In: Calliess/Ruffert (eds.). *EUV/AEUV*. München: C.H. Beck.

Weichert, Thilo (2013). Big Data und Datenschutz Chancen und Risiken einer neuen Form der Datenanalyse. *Zeitschrift für Datenschutz* 3, 6, 251–259.

Wilhelm, Maria (2016). Auskunftsansprüche in der Informationsgesellschaft. *Die öffentliche Verwaltung* 21, 899–905.

Bildquellen

Abb 1: Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)): (2017/C 378/55).

Abb.2: URL: https://lfd.niedersachsen.de/startseite/themen/videouberwachung/transparenzanforderungen_bei_einer_videouberwachung_nach_der_ds_gvo/transparenzanforderungen-und-hinweisbeschilderung-bei-einer-videoueberwachung-nach-der-ds-gvo-158959.html [Letzter Zugriff am 15.09.2019]

Maria Wilhelm
Leitung der Stabsstelle Europa beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Königstraße 10a
D-70173 Stuttgart
E-Mail: poststelle@lfdi.bwl.de