Alexander Roßnagel, Monika Desoi, Gerrit Hornung

Gestufte Kontrolle bei Videoüberwachungsanlagen

Ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung

Moderne Videoüberwachungssysteme können über die Übertragung und Aufnahme von Videobildern hinaus diese auch auswerten. Sie können dadurch zum einen die Gefahrenabwehr verbessern, sie greifen dadurch zum anderen aber auch tiefer in die Grundrechte der Betroffenen ein. Um hier zu einem neuen, angemessenen Ausgleich zwischen Sicherheit und Freiheit zu gelangen, wird für Gestaltung und Einsatz der modernen Videoüberwachungssysteme (1.) ein Drei-Stufen-Modell vorgestellt (2.). Dieses wird sodann verfassungs- und datenschutzrechtlich hergeleitet (3.) und in seiner Ausgestaltung rechtlich begründet (4.). Schließlich wird erörtert, wie das Drei-Stufen-Modell im Rahmen von Erlaubnistatbeständen zur Anwendung gebracht werden kann (5.).*

Prof. Dr. Alexander Roßnagel

Universitätsprofessor für öffentliches Recht, Forschungszentrum für Informationstechnik-Gestaltung (ITeG) Vizepräsident der Universität Kassel
E-Mail: a.rossnagel@uni-kassel.de

Monika Desoi

Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und Wissenschaftliche Mitarbeiterin an der Universität Kassel
E-Mail: m.desoi@uni-kassel.de

Prof. Dr. Gerrit Hornung, LL.M.

Lehrstuhl für Öffentliches Recht, IT-Recht und Rechtsinformatik, Direktor am Institut für IT-Sicherheit und Sicherheitsrecht (ISL), Universität Passau
E-Mail: gerrit.hornung@uni-passau.de

1 Hintergrund

Der Einsatz von Videoüberwachungsanlagen an gefährlichen und gefährdeten Orten soll nach Absicht der Betreiber meist sowohl der Verhinderung von Straftaten als auch zu repressiven Zwecken dienen. Werden die Videodatenströme aufgezeichnet, können die Bilder als Beweismittel in einen Strafprozess eingeführt werden. Die Effektivität präventiver Videoüberwachung ist jedoch umstritten – sowohl hinsichtlich der Abschreckung als auch in Bezug auf die Verhinderung von Schäden.[1] Um in Zukunft Gefahren für Personen und Sachen bereits im Moment ihrer Entstehung effektiv verhindern zu können, wird in Forschungsprojekten an der Entwicklung „intelligenter" Videoüberwachungssysteme gearbeitet. Deren Software kann die von ihnen überwachten Personen automatisiert (wieder-) erkennen (Tracking), von ihnen Bewegungspfade (Trajektorien) erstellen, auch wenn sie sich im Erfassungsbereich unterschiedlicher Kameras bewegen, das Verhalten der überwachten Personen auf Abweichungen gegenüber dem „Normalverhalten" analysieren und schließlich das Überwachungspersonal am Monitor auf die erkannte Gefahr aufmerksam machen.[2]

Mit der Verwendung derartiger Tools sind einerseits große Hoffnungen für eine effektivere Kriminalitätsbekämpfung verbunden. Andererseits greift die „intelligente" Videoüberwachung stärker in das Recht auf informationelle Selbstbestimmung und gegebenenfalls weitere Grundrechte der Betroffenen ein, als dies bei der

* Der Text ist im Zusammenhang mit dem BMBF-geförderten Projekt „Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung Personen-induzierter Gefahrensituationen (CamInSens)", FKZ 13N10814, entstanden.

1 Siehe dazu ausführlich *Hempel*, in: Zurawski (Hrsg.), Surveillance Studies, 2007, 117 ff.; *Stutzer/Zehnder*, Vierteljahrshefte zur Wirtschaftsforschung 2009, 119 ff.; *Müller*, MschrKrim 2002, 33, 34, 38; *Steinbauer*, MschrKrim 2010, 214 ff.; *Hornung/Desoi*, K&R 2011, 153 ff. m.w.N.

2 Siehe Projekte z. B.: CamInSens, MuViT, APFel (BMBF, s. o.) und INDECT (http://www.indect-project.eu/); siehe zur Weiterentwicklung von Videoüberwachungssystemen auch *Schaup/Ott/Schallauer/ Winter/Thallinger*, Kriminalistik 2009, 635 ff.; *Coudert*, CLSR 2010, 377 ff.

herkömmlichen Videoüberwachung der Fall ist.[3] Um diesen Eingriff dennoch so gering wie möglich zu halten, wird für die Gestaltung und den Einsatz „intelligenter" Videoüberwachungssysteme ein Drei-Stufen-Modell vorgeschlagen. Es soll zum einen als Orientierung für technisch-organisatorische Absicherungen dienen, um eine grundrechtsschonende Videoüberwachung zu ermöglichen. Zum anderen soll es dem Überwachungspersonal am Monitor bei seinen Entscheidungen ein handhabbares Schema vorgeben, das im praktischen Einsatz die Unterscheidung zwischen rechtmäßigen und rechtswidrigen Eingriffen in das Recht auf informationelle Selbstbestimmung ermöglicht. Schließlich kann es auch zur Orientierung eines Gesetzgebers dienen, der neue und präzisere Regelungen für eine weiterreichende und eingriffsintensive Videoüberwachung erlassen will.

Die folgende Darstellung und Erläuterung des Drei-Stufen-Modells orientiert sich an dem Anwendungsbeispiel einer Videoüberwachung besonders gefahrenträchtiger oder gefährdeter öffentlich zugänglicher Einrichtungen durch Polizei oder private Sicherungskräfte, wie etwa Flughäfen, Bahnhöfe, Sportstadien oder Konzerthallen. Sie geht weiter davon aus, dass für die automatisierte Fahndung nach gesuchten Personen andere Systeme und nur unter engen Zulässigkeitsvoraussetzungen zum Einsatz kommen.[4] Datenabgleiche mit Fahndungsdateien sind zwar möglich,[5] Ermächtigungsgrundlagen für den massenhaften, vollautomatisierten Abgleich von Fahndungsfotos mit Gesichtsbildern aus Videoaufnahmen existieren jedoch nicht.[6]

2 Drei-Stufen-Modell

Im Drei-Stufen-Modell wird der Eingriff in das Grundrecht auf informationelle Selbstbestimmung abhängig vom Grad der Feststellung einer Gefahr auf jeder Stufe so gering wie möglich gehalten.

2.1 Erste Stufe: Allgemeine beobachtende Überwachung

In der ersten Stufe findet eine allgemeine Beobachtung aller Personen statt, die sich in gefährdeten oder gefahrgeneigten Teilen der Einrichtung aufhalten.[7] Ziel der Beobachtung ist es, möglichst frühzeitig auffällige Situationen oder Verhaltensweisen zu erkennen, die auf eine Gefahr hindeuten könnten. Das „intelligente" Kamerasystem beobachtet die Bewegungen der überwachten Personen und wertet sie darauf hin aus, ob sie von definierten Mustern abweichen oder bestimmte Muster erfüllen. Hierfür ist es nicht notwendig, dass die aufgenommenen Personen identifiziert oder individualisierbar dargestellt werden. Um dies zu vermeiden, können verschiedene Techniken der Anonymisierung und Pseudonymisierung verwendet werden.[8] Die Darstellung auf den Monitoren kann beispielsweise verpixelt sein, als reine Punktwolke erfolgen, stilisiert als Bewegung von Strichmännchen präsentiert werden oder als Überblicksaufnahme erfolgen. Zoommöglichkeiten sind in dieser Stufe ausgeschlossen. Je nach Einsatzbereich kann die Gesamtsituation durch den Beobachter an den Monitoren mit beobachtet oder vollautomatisch kontrolliert werden. In letzterem Fall können – vorausgesetzt die Analysetechnik garantiert, dass tatsächlich alle auffälligen Verhaltensweisen erkannt werden[9] – die Monitore sogar „schwarz" geschaltet sein und erst dann ein Bild zeigen, wenn die Softwareanalyse auffälliges Verhalten einer oder mehrerer Personen festgestellt hat und in die zweite Stufe schaltet. Für das nicht auffällige Verhalten ist es auch nicht notwendig, dass die Aufnahmen aufbewahrt werden. Sie sind umgehend zu löschen.

Der Übergang in die zweite Stufe (gezielte Personenverfolgung) erfolgt automatisch, wenn eine auffällige Situation von der Software erkannt wurde, oder manuell, wenn der Beobachter eine solche Situation erkennt. Die Herausforderung liegt darin, für diesen Übergang bestimmte typische Schwellen zu definieren. Diese müssen typische Geschehensabläufe beschreiben, die aus kriminalistischer oder polizeilicher Erfahrung auf eine ausreichende Wahrscheinlichkeit hinweisen, dass Grenzen der jeweiligen Stufen überschritten werden. Für den Übergang in die zweite Stufe ist es erforderlich, aber auch ausreichend, wenn das Kamerasystem oder der Beobachter ein Verhalten feststellen, das hinreichende Anhaltspunkte enthält, um bei verständiger und besonnener Lagebeurteilung eine Situation anzunehmen, die erfahrungsgemäß eine Gefahr verursacht (Gefahrenverdacht).[10] Auf dieser Stufe wird noch nicht zwischen dem Einsatz zu präventiven und zu repressiven Zwecken unterschieden, weil die Vorbereitung einer Straftat oder das Ansetzen zu ihr zumindest auch einen Gefahrenverdacht begründen.

2.2 Zweite Stufe: Gezielte Personenüberwachung

In der zweiten Stufe werden Personen, deren Verhalten auffällig vom durchschnittlichen Verhalten am überwachten Ort abweicht, gezielt auf ihrem weiteren Weg überwacht. Spätestens jetzt wird der Beobachter durch das Überwachungssystem auf die Situation aufmerksam gemacht. Das „intelligente" Kamerasystem verfolgt die Bewegungspfade der markierten Person, wählt die Kameras mit der besten Blickrichtung aus und überprüft, ob das weitere Verhalten des Überwachten auf eine Situation schließen lässt, durch die ein Schaden für die Person selbst, andere Personen oder Sachen entstehen kann.

Auch innerhalb der zweiten Stufe soll der Eingriff in das Recht auf informationelle Selbstbestimmung so gering wie möglich gehalten werden. Zwar wird das Verhalten der überwachten Person aufgezeichnet, um nachträglich das Entstehen der Gefahr oder der Straftat nachverfolgen zu können. Auch muss der Beobachter im Kontrollraum das Verhalten realistisch wahrnehmen und daher manuell zoomen können. Das Kamerasystem vermeidet jedoch eine Aufnahme des Gesichts oder anderer biometrischer Merkmale und bietet noch keine Möglichkeiten, die Daten zu erfassen, um biometrische Templates für einen automatischen Vergleich zu erstellen. Die Identität der beobachteten Person wird nicht aufge-

3 Siehe *Hornung/Desoi*, K&R 2011, 155 f.

4 Siehe hierzu z.B. für Kfz-Kennzeichen-Scanning *BVerfGE* 120, 378 ff.; *Roßnagel*, NJW 2008, 2547.

5 Siehe z.B. § 25 HSOG; § 28 ASOG Bln.

6 Wie schon das Beispiel Kfz-Kennzeichen-Scanning zeigt, wären hierfür erst recht spezielle Erlaubnisregelungen erforderlich.

7 Siehe z.B. § 14 Abs. 4 HSOG; § 28 Abs. 1 ASOG Bln.; eine vollkommen anlasslose Überwachung an beliebigen Stellen ist ohnehin rechtswidrig – s. z.B. *BVerfGE* 120, 378 ff.

8 Zu den technischen Möglichkeiten siehe *v. Stechow*, Datenschutz durch Technik, 2005, 53 f.

9 Dies dürfte auf absehbare Zeit technisch nicht realisierbar sein.

10 Siehe z.B. *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 4. Aufl., 2007, E Rn. 46 ff.

deckt. Die Aufnahmen werden unmittelbar nach der Feststellung durch den Beobachter, dass weder eine Gefahr entstanden, noch eine Straftat begangen worden ist, gelöscht.

Der Übergang in die dritte Stufe (Personenerkennung) erfolgt automatisch, wenn eine gefährliche Situation von der Software erkannt wurde, oder manuell, wenn der Überwachende eine solche Situation erkennt. Für den Übergang in die dritte Stufe ist es erforderlich, aber auch ausreichend, wenn das Kamerasystem oder der Beobachter ein Verhalten feststellen, das bei verständiger und besonnener Lagebeurteilung eine konkrete unmittelbare Gefahr oder den konkreten Verdacht einer Straftat begründet. Eine Gefahr liegt vor, wenn eine Sachlage festgestellt wird, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen ein Schaden an Rechtsgütern verursacht wird.[11] Das Überschreiten der Schwelle zur dritten Stufe erfordert in der Regel auch das Einschreiten von Sicherungskräften.

2.3 Dritte Stufe: Personenerkennung

Die dritte Stufe dient der weiteren Beobachtung und eventuell der Einsatzleitung, vor allem aber der Beweissicherung. Zu diesem Zweck wird die Situation in einer Detailschärfe auf den Monitor übertragen, dass das Geschehen genau beobachtet werden kann und die Einsatzkräfte effektiv angewiesen werden können. Die Videobilder werden so aufgenommen und gespeichert, dass das Geschehen später zu Beweiszwecken nachvollzogen werden kann. Außerdem werden die biometrischen Merkmale der verdächtigen Person, insbesondere ihr Gesicht, so aufgenommen, dass eine Identifizierung möglich ist.

Aber auch in der dritten Stufe findet noch keine automatisierte Identifizierung der beobachteten Person durch Abgleiche mit (Fahndungs-)Datenbanken statt. Dies soll nur durch eine sich an die Beobachtung anschließende ausdrückliche Entscheidung eines verantwortlichen Experten erfolgen. Die Videoaufnahmen werden solange aufbewahrt, bis die Gefahrenabwehr oder die Strafverfolgung abgeschlossen sind, oder es sich herausstellt, dass trotz der eindeutigen Hinweise doch weder eine Gefahr vorlag, noch eine Straftat verübt wurde.

2.4 Gefahrenabwehr und Strafverfolgung

Mit Eintreten in die dritte Stufe können Maßnahmen der Gefahrenabwehr und der Strafverfolgung erforderlich sein. Für diese Maßnahmen können die Videoaufzeichnungen genutzt werden, die in der dritten Phase, aber auch in der zweiten Phase erstellt worden sind. Ob diese Maßnahmen, zu denen auch eine manuelle Identifizierung der aufgenommenen Personen oder gar ein Abgleich mit (Fahndungs-)Datenbanken gehört, zulässig sind, richtet sich nach den jeweiligen Ermächtigungsvorschriften im Strafprozessrecht oder im Polizeirecht.[12] In einem sich anschließenden Gerichtsprozess können die Videoaufzeichnungen nach den einschlägigen Vorschriften als Objekte des Augenscheins in das Beweisverfahren eingebracht werden.[13]

3 Rechtliche Begründung

Das Drei-Stufen-Modell berücksichtigt vor allem verfassungsrechtliche und datenschutzrechtliche Vorgaben. Sein Zweck ist es, die Intensität der Überwachung so gering wie möglich zu halten. Hierfür werden die Kamerasysteme so ausgestaltet, dass sie in der Grundeinstellung so wenige (Wieder-)Erkennungsmerkmale der überwachten Personen übertragen und aufnehmen wie möglich. Erst bei Vorliegen von Anhaltspunkten für Prognosen zu unterschiedlich wahrscheinlichen Gefahren werden schrittweise weitere Details der überwachten Situation erhoben und gespeichert.

3.1 Verfassungsrechtliche Anforderungen

Das Drei-Stufen-Modell dient dem Schutz des Rechts auf informationelle Selbstbestimmung. Dieses Recht stellt das für den Datenschutz wichtigste Grundrecht dar. Es verlangt, dass der Einzelne grundsätzlich selbst darüber entscheiden kann, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[14] Diese Befugnis ist nicht auf eine persönliche Privatsphäre beschränkt, sondern schließt auch personenbezogene Daten mit ein, die von einem Auftreten in der Öffentlichkeit gesammelt werden können. „Intelligente" Videoüberwachungsanlagen können nicht nur speichern, wer sich wann wo wie lange und mit wem aufgehalten hat, sie können auch das Verhalten der aufgenommenen Personen auf Abweichungen gegenüber einem definierten „Normalverhalten" analysieren.[15] Für die Betreiber der „intelligenten" Videoüberwachungsanlagen ist es daher möglich, auch sehr aussagekräftige personenbezogene Daten der Personen zu sammeln, die in das Blickfeld der Kameras geraten sind.

Um das Recht auf informationelle Selbstbestimmung effektiv zu schützen, haben Gesetzgebung, Rechtsprechung und Literatur eine Reihe von Anforderungen an die Erhebung und Verwendung von Daten abgeleitet, die das Schutzprogramm der informationellen Selbstbestimmung darstellen. Die Grundsätze der Interessenabwägung und der Verhältnismäßigkeit, der Zweckbindung und der Erforderlichkeit sowie der Datensparsamkeit stellen die verfassungsrechtlichen und datenschutzrechtlichen Vorgaben dar, die das Grundgerüst für das Drei-Stufen-Modell bilden.

Das Verhältnismäßigkeitsprinzip verlangt, dass die „intelligente" Videoüberwachung einen legitimen Zweck verfolgt, für die Zweckerreichung keine milderen, gleich effektiven Mittel zur Verfügung stehen und die Gefahren für das Recht auf informationelle Selbstbestimmung nicht außer Verhältnis zu dem angestrebten Zweck stehen.[16] Hierfür sind Sicherheits- und Freiheitsinteressen gegeneinander abzuwägen. Dabei ist nach Lösungen zu suchen, die im Weg des gegenseitigen Nachgebens ermöglichen, beide gegenläufigen Interessen jeweils möglichst weitgehend zu realisieren. Aus der Abwägung im Rahmen der Angemessenheit folgt, dass Überwachungsmaßnahmen, die ohne Anlass durchgeführt werden, grundsätzlich nicht in Grundrechte eingreifen dürfen. Umge-

11 Siehe z.B. *Denninger* (Fn. 10), Rn. 39f.; *Pieroth/Schlink/Kneisel*, Polizei- und Ordnungsrecht, 6. Aufl. 2010, § 4 Rn. 2, 9; *Gusy*, Polizei- und Ordnungsrecht, 7. Aufl. 2009, Rn. 108; *BVerfGE* 120, 274 (328f.) und 125, 260, Rn. 231 ergänzt die Definition um „verursacht durch bestimmte Personen"; kritisch *Darnstädt*, DVBl. 2011, 263 ff.

12 Siehe z.B. §§ 98c, 98a, oder 163d StPO oder § 25 HSOG; § 28 ASOG Bln.

13 Siehe § 371 ff. ZPO; §§ 86. StPO.

14 BVerfGE 65, 1 (42f.).

15 Zu den rechtlichen Implikationen siehe *Hornung/Desoi*, K&R 2011, 155 f.

16 Siehe zum Verhältnismäßigkeitsprinzip im Datenschutzrecht BVerfGE 65, 1, (54, 44 ff.).

kehrt sind abhängig vom Rang des betroffenen Rechtsguts und der Intensität der drohenden Gefahr auch eingriffsintensivere Maßnahmen zulässig. Dabei sind kontrollierende Instanzen aber dazu verpflichtet, auf starke Grundrechtseingriffe zu verzichten, solange keine konkreten Anhaltspunkte für Gefahren ausgemacht werden können, nur eine allgemeine Bedrohungslage besteht und keine hochrangigen Rechtsgüter betroffen sind. Der Abwägungsprozess kann mit Hilfe des Drei-Stufen-Modells vereinfacht durchgeführt werden, indem das Überwachungspersonal bei Erreichen festgelegter Gefahren- oder Verdachtsschwellen in die nächste Stufe übergehen kann. Für die Beobachter in Kontrollräumen, die zum großen Teil aus juristischen Laien bestehen, ist es ohne eine derartige Typisierung schwierig, in jedem Einzelfall aus diesen eher allgemeinen Prinzipien die konkret zulässige Art und den Umfang der Datenerhebung und -verwendung abzuleiten. Der Grund hierfür ist, dass Grundrechte, Eingriffstiefen und legitime Zwecke je nach Situation unterschiedlich gewichtet werden und daneben weitere Faktoren, wie beispielsweise der Einsatzort zusätzlich in die Gewichtung mit einfließen müssen. Für den praktischen Einsatz ist es daher notwendig, den Informationseingriff in der Grundeinstellung der Kameras so gering wie möglich zu halten und nur bei Erreichen von fest definierten Schwellen stufenweise zu erhöhen.

Aus der Beschränkung der Videoüberwachung auf bestimmte legitime Zwecke folgt überdies, dass die zu diesem Zweck erhobenen personenbezogenen Daten an den festgelegten Zweck gebunden sind und nicht später zu beliebigen anderen Zwecken weiterverwendet werden dürfen (Prinzip der Zweckbindung).[17] Um eine Weiterverwertbarkeit der erhobenen Daten zu begrenzen, muss die „intelligente" Videoüberwachung daher so ausgestaltet werden, dass die Daten zunächst pseudonymisiert erhoben werden und die Pseudonymisierung erst zum spätmöglichsten Zeitpunkt aufgehoben werden darf.

Schließlich dürfen nach dem Prinzip der Erforderlichkeit stets nur die personenbezogenen Daten erhoben und verwendet werden, die für das Erreichen dieses Zwecks erforderlich sind.[18] Sind hierfür keine personenbezogenen Daten, sondern nur allgemeine Informationen oder aggregierte Daten erforderlich, darf kein Personenbezug hergestellt werden. Ist der Zweck erreicht, sind die Daten zu löschen oder zu anonymisieren. Aus dem Prinzip der Erforderlichkeit folgt als Gestaltungsanforderung an das Drei-Stufen-Modell, dass ein Personenbezug der Videodaten erst dann hergestellt werden darf, wenn dies für die Gefahrenabwehr oder Strafverfolgung notwendig ist.

Zur Umsetzung des Vorsorgeprinzips im Schutz der informationellen Selbstbestimmung muss darüber hinaus das Erforderlichkeitsprinzips um den Grundsatz der Datenvermeidung und Datensparsamkeit ergänzt werden.[19] Während sich das Erforderlichkeitsprinzip auf einen vom Datenverarbeiter vorgegebenen Zweck,

17 *Albers*, Informationelle Selbstbestimmung, 2005, 166; *von Zezschwitz*, Konzepte der normativen Zweckbegrenzung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 219 ff.

18 *BVerfGE* 65, 1, 46.

19 Siehe zu diesem Grundsatz ausführlich *Roßnagel*, Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes?, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation, Recht und öffentliche Kommunikation, Berlin 2011, 41 ff.

ein von ihm ausgesuchtes technisches System und einen von ihm definierten Datenverarbeitungsprozess bezieht, fordert das Prinzip der Datenvermeidung von der verantwortlichen Stelle, ihre technisch-organisatorischen Verfahren vorsorgend so zu gestalten, dass sie möglichst keine oder so wenig personenbezogene Daten wie möglich verarbeiten.[20] Es fordert von der verantwortlichen Stelle zu prüfen, ob die gegebenen oder geplanten Umstände der Datenverarbeitung so verändert werden können, dass keine personenbezogenen Daten erforderlich sind. Kann im Prinzip auf den Personenbezug verzichtet werden, entsteht daraus eine Rechtspflicht, die Verfahren und Systeme so zu gestalten, dass ein Personenbezug vermieden wird, soweit dies technisch möglich und verhältnismäßig ist. Der Grundsatz der Datenvermeidung und Datensparsamkeit führt dazu, dass das Drei-Stufen-Modell eine Perspektive zur Gestaltung des „intelligenten" Kamerasystems und zur Organisation seines Einsatzes beinhaltet.

3.2 Datenschutzrechtliche Anforderungen

Die aus der Verfassung abgeleiteten Anforderungen zum Schutz des Rechts auf informationelle Selbstbestimmung wurden im Bundes- und in den Landesdatenschutzgesetzen normiert. Insbesondere in § 6b BDSG und vergleichbaren Regelungen der Landesdatenschutzgesetze[21] wurden Anforderungen an die Beobachtung „öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung)" formuliert.[22] Sie fordern, wie § 6b Abs. 1 BDSG, u.a. eine Abwägung zwischen den schutzwürdigen Interessen der Betroffenen und den berechtigten Interessen der Betreiber der Videosysteme.[23] Nach § 6b Abs. 3 BDSG ist für die Verarbeitung und Nutzung der gewonnenen Daten eine ebensolche Abwägung erforderlich. „Intelligente" Videoüberwachung, die durch den Einsatz von Software die aufgenommenen Personen automatisiert (wieder-)erkennen, über den Aufnahmebereich mehrerer Kameras hinweg verfolgen und deren Verhalten analysieren kann, findet weder im Gesetzeswortlaut noch in der Gesetzesbegründung[24] Erwähnung – mutmaßlich, weil im Jahr 2001 der praktische Einsatz einer solchen Technik noch nicht vorhersehbar war. „Intelligente" Videoanalysen lassen sich aber unter § 6b Abs. 3 BDSG subsumieren.[25] Bei ihrer Anwendung müssen daher beide von § 6b Abs. 1 und 3 BDSG geforderten Abwägungen zwischen den Interessen der Betroffenen und denen der Betreiber durchgeführt werden.

Das automatisierte (Wieder-)Erkennen ermöglicht den Betreibern von „intelligenten" Videoüberwachungssystemen, mit einem geringen Aufwand festzustellen, wer sich wann wo mit wem wie lange aufgehalten hat. Durch die Verwendung von Tools zur Erkennung von Bewegungsmustern und zur automatisierten Verhaltensanalyse können darüber hinaus einfach zusätzliche sensitive Daten über eine Person gesammelt werden, die zwar in den Rohdaten bereits angelegt sind, aber bisher entweder gar nicht oder nur mit einem erheblichen Aufwand an Personal, Zeit und Kosten erkannt werden konnten. „Intelligente" Videoüberwachung hat daher gegenüber der herkömmlichen Videoüberwachung eine signifikant höhere Effektivität und bewirkt damit einen bedeutend tieferen Eingriff in die schutzwürdigen Interessen, die bei beiden Abwägungen von § 6b BDSG zu beachten sind.[26] Eingriffsvertiefend wirkt u.a., dass die „intelligenten" Videoüberwachungssysteme mit Informationen über (Wieder-)Erkennungsmerkmale Daten der Betroffenen sammeln, die diese nicht oder nur schwer ändern können. So könnten neben der Kleidung auch die Eigenart des Gangs oder andere körperliche Merkmale als biometrische Daten für die (Wieder-)Erkennung verwendet werden. Auch mit der Verhaltensanalyse werden Daten über die Betroffenen gewonnen, die von diesen oft nur schwer verändert werden können. Sie können auch nicht durch eigene Maßnahmen die in ihrem Umfang erwünschte Verarbeitung ihrer Daten ermöglichen und unerwünschte Datenverarbeitung verhindern.[27] Ihnen bleibt nur die Wahl, das Sichtfeld der Kameras zu meiden oder sich aufnehmen lassen und damit ihre Daten den Betreibern der Videoüberwachungsanlagen zu überlassen. Dies hat zur Folge, dass die Betroffenen bei der Verwendung „intelligenter" Videoüberwachungssysteme ihr Recht auf informationelle Selbstbestimmung nicht durch Selbstdatenschutz ausüben können, sondern darauf angewiesen sind, dass dieses von den Betreibern geschützt wird.

Dadurch kann sich die Abwägung in § 6b Abs. 3 BDSG zugunsten der schutzwürdigen Interessen der Überwachten verschieben. Überwiegen diese, kann die Interessenabwägung ergeben, dass eine automatisierte Analyse des Verhaltens sowie das Verfolgen von Bewegungspfaden nicht rechtmäßig ist, der Einsatz herkömmlicher Videoüberwachung dagegen schon.

Werden die „intelligenten" Videoüberwachungssysteme unter Anwendung des Drei-Stufen-Modells betrieben, geht es jedoch nicht mehr um eine bloße Ja-Nein-Entscheidung, sondern um eine differenzierte Abwägung der schützwürdigen Interessen mit einem situationsabhängigen Schutzbedürfnis des Betreibers. Dies kann zur Folge haben, dass die Interessenabwägung insoweit zugunsten der Betreiber ausfällt, als die schutzwürdigen Interessen der Betroffenen im „Normalbetrieb" weniger oder gar nicht betroffen sind. Mit Hilfe des Drei-Stufen-Modells wird die Schwere der Eingriffe in das Recht auf informationelle Selbstbestimmung auf der ersten Stufe abgeschwächt und auf der zweiten und dritten Stufe abhängig von einer Gefahrenbeurteilung dosiert. Dadurch liegt es in einem gewissen Umfang im Entscheidungsbereich des Betroffenen, ob er durch sein Verhalten in die Überwachung der zweiten oder dritten Stufe gelangt.

Die Grundeinstellung der Kamerasysteme, die die überwachten Personen in den ersten beiden Stufen nicht identifizierbar darstellt,[28] mindert einen Eingriff in das Recht auf informationelle Selbstbestimmung ab. Zwar werden auch bei der Verwendung „intelligenter Videotechnik" auf allen Stufen personenbezogene Daten erhoben. Doch beschränkt das Grundprin-

20 Siehe z.B. auch *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 323; *Laue*, Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung, 2010, 351.

21 Siehe z.B. § 31b BlnDSG, § 12 HDSG, § 20 DSG SH, § 29 DSG NW; siehe zu diesen auch *v. Zezschwitz*, Videoüberwachung, in: Roßnagel (Fn. 17), 1894 ff.

22 Zu den Ermächtigungsgrundlagen für Videoaufnahmen durch die Polizei siehe z.B. §§ 24 und 24a ASOG Bln, § 14 HSOG, § 184 LVwG SH; §§ 15 bis 15b PolG NW; siehe zu diesen z.B. *v. Zezschwitz* (Fn. 21), S. 1986 f.

23 Siehe hierzu *Scholz*, in: Simitis (Hrsg.), BDSG, 7. Aufl. 2011, § 6b Rn. 92 ff.; *Lang*, Private Videoüberwachung im öffentlichen Raum, 2007, 299 ff.

24 BT-Drs. 14/5793, 62.

25 Siehe dazu ausführlich *Hornung/Desoi*, K&R 2011, 157.

26 Siehe dazu ausführlich *Hornung/Desoi*, K&R 2011, 155 ff.

27 Dies fordern grundsätzlich *Roßnagel/Scholz*, MMR 2000, 721, 722.

28 Dies gilt nicht, wenn ein Beobachter auf der zweiten Stufe eine beobachtete Person zufällig kennt und erkennt.

zip des Drei-Stufen-Modells den Eingriff auf das Verhältnismäßige. Denn die Daten bleiben auf der ersten Stufe und in der Regel auch auf der zweiten Stufe für die Beobachter pseudonym. Ihr Personenbezug wird durch das Videoüberwachungssystem erst dann für seinen Betreiber ermöglicht, wenn in der dritten Stufe gezielt identifikationsfähige Daten erhoben werden, die dann später z.B. mit Fahndungsbildern verglichen werden können, wenn nicht ohnehin die Person festgehalten wird und sich ausweisen muss. Nach dem Drei-Stufen-Modell werden personenbeziehbare Daten erst so spät wie möglich und nur dann erhoben, wenn der Beobachter oder das System eine konkrete Gefahr für eine Person oder eine Sache erkennt. Dadurch wird ausgeschlossen, dass von jeder erfassten Person Bewegungs- und Kontaktprofile erstellt werden können. Die beobachteten Situationen sind nur für die Personen als Bewegungsprofil für einen gewissen Zeitraum nachvollziehbar, deren Verhalten so bewertet wurde, dass es die dritte Stufe erreicht hat.

§ 6a BDSG und vergleichbare Regelungen in den Landesdatenschutzgesetzen verbieten automatisierte Einzelentscheidungen, also Entscheidungen, die ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden und die für den Betroffenen eine nachteilige rechtliche Folge nach sich ziehen oder ihn sonst erheblich beeinträchtigen. Dies gilt dann, wenn die automatisiert getroffene Entscheidung auf der Auswertung von einzelnen Persönlichkeitsmerkmalen des Betroffenen beruht.[29] Gemeint sind hiermit Daten, die die Persönlichkeit des Betroffenen unter bestimmten „einzelnen Aspekten" beschreiben.[30] Nach Art. 15 Abs. 1 DSRL ist darunter auch das Verhalten einer Person zu verstehen.

Während die Entscheidung selbst nicht automatisiert gefällt werden darf, ist es zulässig, menschliche Entscheidungen – auch wenn sie für Betroffene nachteilige Folgen haben – durch automatisierte Prozesse vorzubereiten.[31] Mit Hilfe des Drei-Stufen-Modells kann genau dies sichergestellt werden. Das Modell gewährleistet, dass die aus der automatisierten Analyse der aufgenommenen Bilder gewonnenen Erkenntnisse selbst nicht unmittelbar zu einer automatisierten Entscheidung führen, sondern die automatisiert gewonnenen Erkenntnisse eine Entscheidungshilfe für die abschließende Entscheidung einer Person mit echtem Entscheidungsspielraum darstellen.

Im „Normalbetrieb" der ersten Stufe werden keinerlei für die Betroffenen erhebliche oder nachteilige Entscheidungen gefällt. Mit Erreichen der zweiten Stufe soll die Aufmerksamkeit des Beobachters auf das „auffällige Verhalten" gelenkt werden. Dieser kann dann grundsätzlich manuell den Übergang in die dritte Stufe einleiten, nachdem er das weitere Verhalten der gezielt überwachten Person eigenständig analysiert hat. Sofern dieser Übergang künftig durch das System erfolgt, liegt zwar eine automatisierte Entscheidung vor. Diese dient aber noch immer lediglich der Vorbereitung einer abschließenden Entscheidung einer natürlichen Person, die auch nach § 6a BDSG zulässig ist. Auch in diesem Fall stellt die automatisierte Analyse also keine Mitbestimmung der Letztentscheidung des Beobachters dar. Vielmehr dient sie dieser nur, da der Beobachter die Meldung des Systems, dass eine eindeutige Situation vorliegt, inhaltlich auf ihre Stimmigkeit mit den Gesamtumständen der überwachten Situation überprüfen muss, bevor er entscheidet, welche weitergehenden Maßnahmen eingeleitet werden. Erst die Einleitung der Gefahrenabwehrmaßnahmen oder der Strafverfolgung stellt eine erhebliche nachteilige Folge für den Betroffenen dar. Die Einleitung dieser Maßnahmen liegt aber jenseits des Drei-Stufen-Modells der Erkenntnisgewinnung und ist nur manuell durch einen hierzu befugten Beobachter möglich.

Der Übergang von einer Stufe der Informationserhebung und -auswertung zur nächsten stellt selbst keine rechtliche Folge oder sonstige erhebliche nachteilige Folge dar. Zwar vertieft sich der Eingriff in das Recht auf informationelle Selbstbestimmung jeweils mit Erreichen der nächsten Stufe. Auch reicht eine interne Entscheidung der verantwortlichen Stelle für die Erfüllung der tatbestandlichen Voraussetzungen aus, denn der Betroffene muss von der Entscheidung noch nicht in Kenntnis gesetzt worden sein.[32] Die automatisierte Entscheidung zur nächsten Stufe überzugehen, stellt dennoch keine erheblich beeinträchtigende oder rechtlich nachteilige Folge für die Betroffenen dar. Das „intelligente" System bewertet das Verhalten der Überwachten. Dabei stellt es entweder fest, dass das Verhalten nicht vom „normalen" Verhalten abweicht oder es macht den Experten auf die Situation aufmerksam. Im ersten Fall bewertet das System das Veralten positiv, das heißt, die Bewertung bewirkt keine nachteilige Folge. Im zweiten Fall vertieft die Bewertung des Systems den Informationseingriff, bewirkt aber keine rechtliche Folge, da es lediglich den Beobachter auf die ungewöhnliche Situation aufmerksam macht und ihm diese optimal präsentiert. Der Experte muss dann selbst die Entscheidung treffen, ob das abweichende Verhalten rechtliche Konsequenzen nach sich zieht. Sie bewirkt auch keine erhebliche Beeinträchtigung. Eine solche ist erst anzunehmen, wenn die Bewertung eine diskriminierende Wirkung durch eine nachhaltige Beeinträchtigung der wirtschaftlichen oder persönlichen Belange des Betroffenen bewirkt.[33] Diese Wirkung wird im Regelfall erst durch die Gefahrenabwehrmaßnahmen, nicht durch eine weitere und präzisere Beobachtung der Situation erzielt.

4 Die Stufenübergänge

Mit Hilfe des Drei-Stufen-Modells kann eine verhältnismäßige Videoüberwachung realisiert werden.

4.1 Basis der ersten Stufe

Auf der ersten Stufe werden die beobachteten Personen vom System nur für kurze Zeit erfasst und bleiben dem Beobachter gegenüber unsichtbar oder können vom ihm zumindest nicht identifiziert werden. Damit ist der Informationseingriff geringer als bei der heutigen Videoüberwachung. Die „intelligenten" Systeme erfassen zwar die Bilder des beobachteten Geschehens und analysieren das Verhalten der Überwachten. Sie müssen sie zu diesem Zweck wiedererkennen, wenn sie den Aufnahmebereich einer Kamera verlassen und in den Fokus einer anderen Kamera gelangen. Die Analysen laufen aber automatisch im Hintergrund ab. Der Beobachter sieht allenfalls Überblicksbilder aus großer Entfernung, abstrakte Darstellungen der Bewegungen oder über-

29 *Scholz* (Fn. 23), § 6a Rn. 21 ff.

30 *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 6a Rn. 7.

31 Dazu *Hornung/Desoi*, K&R 2011, 157 f.

32 *Scholz* (Fn. 223), § 6a Rn. 16 f.

33 Siehe z.B. *Scholz* (Fn. 23), § 6b Rn. 28.

haupt kein Bild. Er kann nicht auf einzelne Menschen zoomen. Er hat auch keine Einsicht in die einzelnen Analyseprozesse. Ihre Ergebnisse werden dem Beobachter erst bei Erreichen der zweiten Stufe sichtbar. Die erste Stufe wird deshalb auf der Basis der geltenden Erlaubnistatbestände im bisherigen Umfang zulässig sein. Wird die Videoüberwachung nur an gefährdeten oder gefährlichen Orten genutzt, ist sie nach den polizeilichen Ermächtigungsgrundlagen zulässig.[34] Wird sie von anderen Behörden oder privaten Sicherungskräften genutzt, wird sie – wegen der Abmilderung des Eingriffs in das Recht auf informationelle Selbstbestimmung – in der Regel auch der doppelten Abwägung nach § 6b Abs. 1 und 3 BDSG gerecht. Diese wird in der Regel zu Gunsten der Betreiber der „intelligenten" Videoüberwachungsanlagen ausfallen, wenn die Daten nur kurzfristig erhoben, analysiert und im „Nicht-Treffer-Fall" wieder automatisch gelöscht werden. Dieses Vorgehen trägt dem Grundsatz der Datenvermeidung und Datensparsamkeit Rechnung.

4.2 Übergang zur zweiten Stufe

Der Übergang in die zweite Stufe kann nach Feststellung eines Gefahrenverdachts oder einer abstrakten Gefahr erfolgen. Ein Gefahrenverdacht liegt dann vor, wenn aus Sicht eines verständigen objektiven Betrachters Anhaltspunkte für eine Gefahr vorliegen, der Beobachter sich dabei aber bewusst ist, dass die Anhaltspunkte noch nicht zu einer abschließenden Beurteilung ausreichen.[35] Dieses Besorgnispotential besteht etwa dann, wenn beobachtet wird, dass eine Gruppe angetrunkener Männer eine fremde Person am Weiterlaufen hindert oder ein Mann sehr eng hinter einer älteren Dame herläuft. Im ersten Fall kann aus der Situation eine ausreichende Wahrscheinlichkeit abgeleitet werden, dass im weiteren Verlauf des Geschehens eine Körperverletzung begangen wird. Im zweiten Fall kann es als ausreichend wahrscheinlich eingeschätzt werden, dass die Handtasche der älteren Dame entwendet wird. In solchen Fällen ist der Beobachter berechtigt, weitere Informationseingriffe zur Gefahrenerforschung durchzuführen.[36] Eine abstrakte Gefahr liegt vor, wenn eine Sachlage festgestellt werden kann, die nicht im konkreten Fall, aber wissenschaftlich statistisch, nach allgemeiner Lebenserfahrung oder nach polizeilicher Expertenmeinung in der Vielzahl der Fälle zu einer Gefahr führt.[37] Dies kann beispielsweise der Fall sein, wenn Personen als hilfsbedürftig anzusehen sind, sich in gefährlichen Zonen aufhalten oder sich in Schaden provozierende Situationen begeben.

Die zweite Stufe ermöglicht technisch die Verfolgung einzelner Objekte und Personen, die Speicherung der Videodaten und deren Analyse. Aus Sicht des Beobachters und zum Zweck der Beobachtung spielt es aber keine Rolle, um welche Person es sich genau handelt. Auf der zweiten Stufe wird zwar gezielt beobachtet, es erfolgt aber immer noch keine gezielte Erfassung zum Zweck der Identifizierung. Dies entspricht der geringeren Legitimation durch einen Gefahrenverdacht oder eine abstrakte Gefahr im Vergleich zu einer für die dritte Stufe geforderten konkreten Gefahr.[38] Da die gezielte und eventuell auch längere Verfolgung einen tieferen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, als die allgemeine Beobachtung auf der ersten Stufe, kann sie nur dann zulässig sein, wenn ein legitimes Interesse an der genaueren Beobachtung nicht einer Gesamtszene, sondern einer einzelnen Person besteht. Dies ist nur dann der Fall, wenn die Voraussetzungen zum Übergang in die zweite Stufe festgestellt wurden.

4.3 Übergang zur dritten Stufe

Der Übergang in die dritte Stufe darf nur nach Feststellung einer konkreten Gefahr[39] oder einer Straftat eingeleitet werden. Dies wäre etwa der Fall, wenn ein tätlicher Angriff erfolgt, die Tasche entwendet wird, jemand über einen Zaun in eine abgesperrte Zone steigt oder mit einem Gegenstand wirft. Für den Beobachter oder für das beobachtende System muss sich der Gefahrenverdacht oder die abstrakte Gefahr soweit konkretisiert haben, dass ein besonnener Beobachter annehmen muss, dass ohne ein Einschreiten bei unverändertem Fortgang der Geschehnisse ein Schaden für ein Rechtsgut entsteht.

Erst in der dritten Stufe wird die Situation für die Einsatzleitung sehr präzise dargestellt und für Beweiszwecke gespeichert. Zugleich werden von allen Beteiligten die Merkmale aufgenommen, die anschließend eine Identifizierung der Person ermöglichen. Dieser Eingriff in die informationelle Selbstbestimmung ist wiederum tiefer, als die Datenverarbeitung in der zweiten Stufe. Für sie wird ein legitimes Interesse gefordert zu wissen, um welche Person es sich genau handelt. Dieses Interesse ist bei der Feststellung einer konkreten Gefahr oder einer Straftat als Voraussetzungen für den Übergang auf die dritte Stufe gegeben.

Für den Übergang in die zweite oder in die dritte Stufe können nur die Feststellungen und Bewertungen des Beobachters oder des „intelligenten" Videoüberwachungssystems ex ante entscheidend sein. Zu fordern ist eine Beobachtung und Auswertung, die sich auf aktuelle Tatsachen stützt und für die Prognose des weiteren Geschehens aufgrund verfügbarer Erfahrungssätze induktiv zur Feststellung einer – je nach Stufe unterschiedlichen – ausreichenden Wahrscheinlichkeit für einen Schaden oder eine Straftat gelangt. Stellt sich nachträglich heraus, dass tatsächlich doch keine Gefahr bestand und keine Straftat verübt wurde, wird der Übergang in die zweite oder dritte Stufe dadurch nicht rechtswidrig, wenn das System oder der Beobachter die „Scheingefahr" ex ante nicht erkennen konnte.[40] Andernfalls wäre eine vorbeugende und vorsorgende Beobachtung zur Gefahrenabwehr kaum durchführbar, weil die Rechtsunsicherheit sowohl für die Beobachtenden als auch für den Einsatz von Überwachungssystemen zu hoch wäre.[41]

Allerdings ist zu fordern, dass bei automatischer Beobachtung und Verhaltensanalyse die gleichen Anforderungen an die „Sorgfalt" und „Besonnenheit" der Sachverhaltswürdigung gestellt werden,

34 Siehe Fn. 21.

35 Siehe z.B. *BVerwGE* 72, 300 (315); *Schenke,* Polizei- und Ordnungsrecht, 6. Aufl., 2009, Rn. 83; *Denninger* (Fn. 10), Rn. 48; *Pieroth/Schlink/ Kniesel* (Fn. 11), § 4 Rn. 50 ff.; *Gusy* (Fn. 11), Rn. 195.

36 Siehe z.B. *Pieroth/Schlink/Kniesel* (Fn. 11), § 4 Rn. 50 ff.; *Schenke* (Fn. 34), Rn. 88.

37 Siehe z.B. *BVerwG*, DVBl. 2002, 1562; *Pieroth/Schlink/Kniesel* (Fn. 11), § 4 Rn. 10.

38 Siehe z.B. *Pieroth/Schlink/Kniesel* (Fn. 11), § 4 Rn. 9 ff.

39 Siehe Fn. 11.

40 Zur Anscheinsgefahr siehe z.B. *Denninger* (Fn. 10), Rn. 47 f ; Pieroth/Schlink/Kniesel (Fn. 11), § 4, Rn. 48 ff.

41 Dies schließt Schadensersatzansprüche bei einem Schaden durch unrichtige Verarbeitung und Nutzung der erhobenen Daten nicht aus, wenn dadurch dem Betroffenen ein Schaden entstanden ist oder ein erheblicher Eingriff in sein Persönlichkeitsrecht erfolgt ist – siehe hierzu z.B. die Voraussetzungen von §§ 7 und 8 BDSG und vergleichbare Regelungen der Länder.

wie dies gegenüber menschlichen Beobachtern der Fall ist. Dies ist vor dem Einsatz in einem Zulassungsverfahren zu prüfen.

5 Das Drei-Stufen-Modell und die Erlaubnistatbestände

Das Drei-Stufen-Modell ist für „intelligente" Videoüberwachung von den verfassungsrechtlichen Vorgaben und den datenschutzrechtlichen Grundsätzen her entwickelt worden. Es kann immer dann zu Anwendung gelangen, wenn es um die Verhinderung von Schäden und damit im weitesten Sinn um öffentliche oder private Gefahrenabwehr geht. Wie die Videoüberwachung kann es in vielen Anwendungsbereichen zum Einsatz kommen. Für diese bestehen jeweils spezifische Erlaubnistatbestände oder es gelten die allgemeinen Generalklauseln des BDSG oder der Landesdatenschutzgesetze. Am Beispiel der Erlaubnistatbestände aus dem Polizeirecht, der Generalklausel des § 6b BDSG und der spezifischen Regelung im geplanten Beschäftigtendatenschutz wird im Folgenden gezeigt, wie das Drei-Stufen-Modell bei der Anwendung der Erlaubnistatbestände genutzt werden kann.

Im Polizeirecht bestehen spezifische Regelungen zur Gefahrenabwehr mit präzisen Zulässigkeitsvoraussetzungen für die bisherige Form der Videoüberwachung. Sie berücksichtigen nur die Möglichkeiten, die Videotechnik zu ihrer Entstehungszeit bot. Dementsprechend erlauben sie nur, „mittels Bildübertragung" bestimmte Situationen zu „beobachten und auf(zu)zeichnen" (§ 14 Abs. 4 HSOG) oder „Bild- und Tonaufzeichnungen" anzufertigen (§ 24 ASOG Bln). Das Tracking von Personen, die Auswertung ihres Verhaltens und die von einer automatisierten Bewertung abhängige Steuerung der Kameras, ihrer Aufnahmewinkel und -ausschnitte, sind darüber hinausgehende Eingriffe in die Rechte der beobachteten Personen, die von diesen sehr präzis gehaltenen Erlaubnistatbeständen nicht erfasst sind. Vorschriften wie z.B. § 14 Abs. 4 HSOG oder § 24 Abs. 1 ASOG Bln reichen dafür nicht aus. Sollte ein neuer Erlaubnistatbestand geregelt werden, wenn die Videoüberwachungssysteme den notwendigen Reifegrad erreicht haben, sollte in der Abfassung der Erlaubnis das Drei-Stufen-Modell berücksichtigt werden.

Bei privaten Sicherungskräften wird die Zulässigkeit der Nutzung solcher Systeme über § 6b BDSG gesteuert. Für die Beobachtung und Datenerhebung kommt nach Abs. 1 die Zulässigkeit zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegt Zwecke in Betracht. Es dürfen außerdem keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dient die Beobachtung mit optisch-elektronischen Einrichtungen der Vermeidung von Schäden für den Betreiber, handelt es sich also um Maßnahmen der privaten Gefahrenabwehr, erfordert die Abwägung der Betreiberinteressen mit den schutzwürdigen Interessen der Betroffenen die Anwendung des Drei-Stufen-Modells. Informationseingriffe, die nicht durch das Drei-Stufenmodell gedeckt sind, werden grundsätzlich Anhaltspunkte dafür bieten, dass schutzwürdige Interessen der Betroffenen überwiegen.

Nach dem Entwurf der Bundesregierung[42] ist entsprechend § 32f Abs. 1 Satz 1 BDSG-E Videoüberwachung von Beschäftigten in nicht öffentlich zugänglichen Bereichen des Betriebs[43] u.a. zulässig, wenn sie (2.) zur Wahrnehmung des Hausrechts, (3.) zum Schutz des Eigentums, (4.) zur Sicherheit des Beschäftigten, (5.) zur Sicherung von Anlagen und (6.) zur Abwehr von Gefahren für die Sicherheit des Betriebs dient. Sie muss zur Wahrung wichtiger betrieblicher Interessen erforderlich sein und darf nach Art und Ausmaß der Videoüberwachung keine Anhaltspunkte dafür bieten, „dass schutzwürdige Interessen der Betroffenen am Ausschluss der Datenerhebung überwiegen". Wie bei § 6b BDSG fordert die Abwägung der wichtigen betrieblichen Interessen mit den schutzwürdigen Interessen der Betroffenen beim Einsatz „intelligenter" Videoüberwachungssysteme einen nach dem Gewicht der Interessen, aber vor allem nach der zu bewertenden Wahrscheinlichkeit einer Gefahr einen differenzierten Einsatz der Technik. Auch hier werden Informationseingriffe, die nicht durch das Drei-Stufenmodell gedeckt sind, in der Regel keine wichtigen betrieblichen Interessen berühren und Anhaltspunkte dafür bieten, dass schutzwürdige Interessen der Betroffenen überwiegen.[44]

6 Ausblick

Das Drei-Stufen-Modell stellt aus rechtlicher Hinsicht den optimierten Ablauf einer zunächst anlasslosen Überwachung mittels „intelligenter" Videoüberwachungssysteme dar. Es soll darüber hinaus Überwachungspersonal helfen, abstrakte juristische Kriterien, wie beispielsweise den Verhältnismäßigkeitsgrundsatz, für die rechtmäßige Anwendung von „intelligenter" Videoüberwachung mit Hilfe eines Stufenschemas für den praktischen Einsatz handhabbar zu machen. Schließlich soll es auch dem Gesetzgeber helfen, differenzierte Erlaubnistatbestände zu formulieren, die dem Verhältnismäßigkeitsprinzip gerecht werden. Da auf der ersten und zweiten Stufe die überwachten Personen pseudonymisiert dargestellt werden müssen und erst nach Feststellung bestimmter Gefahrenschwellen von einer Stufe in die nächste gewechselt werden kann, wird auch der Möglichkeit des Erstellens von Bewegungs- und Kontaktprofilen und damit eines der größten Probleme des Datenschutzrechts, des Missbrauchs dieser Profile, vorgebeugt. Durch das Drei-Stufen-Modell wird daher das Prinzip der Verhältnismäßigkeit eingehalten.

Das Drei-Stufen-Modell wurde am Beispiel „intelligenter" Videoüberwachungstechnik entwickelt. Sein Konzept ist aber auch auf andere Überwachungstechniken anwendbar, die zur öffentlichen oder privaten Gefahrenabwehr im weitesten Sinn eingesetzt werden sowie unterschiedlich weitreichende und detaillierte Information erheben und damit unterschiedliche tiefe Eingriffe in Informationsgrundrechte ermöglichen. Es ermöglicht nämlich eine technisch-organisatorische Ausprägung praktischer Konkordanz zwischen Freiheit und Sicherheit.

42 BT-Drs. 17/4230.

43 Die Videoüberwachung in öffentlich zugänglichen Bereichen wird durch § 6b BDSG gesteuert – siehe BT-Drs. 17/4230, 19.

44 Dies ist der Defaultwert: „Schutzwürdige Interessen der Betroffenen stehen einer Videoüberwachung in Betriebsräumen der Interessenvertretungen regelmäßig entgegen", BT-Drs. 17/4230, 19.