VIDEOMONITORING ZUR STURZDETEKTION UND ALARAMIERUNG - EINE TECHNISCHE UND RECHTLICHE ANALYSE -

Sebastian Bretthauer* und Erik Krempel**

*Wissenschaftlicher Mitarbeiter und Doktorand unter Professorin Spiecker gen. Döhmann, Zentrum für Angewandte Rechtswissenschaft (ZAR) am Karlsruher Institut für Technologie (KIT)
Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe, DE
sebastian.bretthauer@kit.edu; http://www.zar.kit.edu
** Wissenschaftlicher Mitarbeiter und Doktorand, Fraunhofer IOSB in Karlsruhe unter Professor Jürgen Beyerer
Fraunhofer Str. 1, 76131 Karlsruhe, DE
erik.krempel@iosb.fraunhofer.de; http://www.iosb.fraunhofer.de/

Schlagworte: ***Datenschutz, Videoüberwachung, Einzelentscheidung***

Abstract*:* *Videobasierte Sturzdetektion kann einen hohen Beitrag zur Sicherheit in Krankenhäusern und Pflegeeinrichtungen vollbringen. Sie übernimmt Aufgaben, die nicht oder nur unzureichend durch Personal geleistet werden können. Dabei sind besondere Anforderungen an den Schutz der Privatsphäre und die Akzeptanz aller Betroffenen zu stellen. Durch die technische und rechtliche Analyse einer intelligenten Videoüberwachung sollen neue Ansätze für die Zukunft erforscht werden.*

1. Einleitung

Laut Schätzung[1] des statistischen Bundesamts werden im Jahre 2050 ca. 23 Millionen Menschen in Deutschland 65 Jahre und älter sein. Das wären dann 33% unserer Bevölkerung. Fast 52.000 Menschen werden das Alter von 100 Jahren erreichen, Tendenz steigend. Der Bedarf an qualifizierten Betreuungs- und Pflegekräften wächst stetig; ihn zu befriedigen wird immer schwieriger. Dabei können moderne Technologien zukünftig in Krankenhäusern und Pflegeheimen das Personal unterstützen. Flure und Verkehrswege sollen überwacht werden, um in Notfällen sofort zu reagieren.

2. Technische Analyse

In dieser Arbeit wird ein System beschrieben, welches durch die Auswertung von Videomaterial Stürze erkennt und eine entsprechende Alarmmeldung an Mitarbeiter weiterleitet. Technisch lassen sich Systeme zur Sturzdetektion grob in drei verschiedene Klassen einteilen. Erstens: Systeme, bei denen die zu überwachenden Personen spezielle Sensoren am Körper tragen, welche Stürze erkennen und weiterleiten[2]. Zweitens: Systeme, die spezielle Sensoren direkt im Fußboden oder in

[1] https://www.destatis.de/DE/PresseService/Presse/Pressekonferenzen/2006/Bevoelkerungsentwicklung/bevoelkerungsprojektion2050.pdf.

[2] Beispiel: *Noury, N. et al.*, Microtechnologies in Medicine and Biology, Monitoring behavior in home using a smart fall sensor and position sensors, 2000.

Teppichen verbauen und damit Stürze detektieren[3]. Die dritte Klasse stellen Systeme dar, bei denen mittels optischer Sensoren - meistens Farb- oder Infrarotkameras - Stürze in überwachten Bereichen erkannt werden. Die optische Erfassung hat dabei einige Vorteile gegenüber den anderen Klassen. Da keine Sensoren am Körper getragen werden müssen, ist die Bewegungsfreiheit nicht eingeschränkt und optische Systeme bieten den gleichen Schutz für alle Personen in einem überwachten Bereich. Es können also nicht nur Stürze von überwachten Patienten sondern auch von Besuchern oder Mitarbeitern erkannt werden. Im Vergleich zu den Sensoren im Boden ist der Aufwand, ein kamerabasiertes System zu installieren, viel geringer und damit günstiger. Zu den Nachteilen der kamerabasierten Lösung zählen jedoch potenziell hohe Eingriffe in die Privatsphäre alle Betroffenen.
Im weiteren Verlauf dieser Arbeit wird ein Prototyp vorgestellt, der momentan am Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung entwickelt wird. Bei der Entwicklung stehen neben der reinen technischen Funktion auch die rechtlichen Rahmenbedingungen im Vordergrund. Das hier vorgestellte System soll die gerade abends und nachts wenig frequentierten Verkehrswege zwischen einzelnen Gebäudeteilen, sowie die Flure in den einzelnen Bereichen, überwachen. Der Prototyp selbst besteht aus drei wichtigen Komponenten.
Die erste Komponente sind mobile Endgeräte, beispielsweise Android basierte Smartphones, die an das Pflegepersonal ausgegeben werden. Jedem Smartphone ist eine Station zugeordnet, was später eine einfache räumliche Verteilung der Alarme zulässt. Somit können Alarme immer an das Smartphone weitergeleitet werden, welches sich räumlich am nächsten zum Alarm befindet. Zur Kommunikation mit diesen Endgeräten kann das häufig bereits vorhandene Wlan Netz der Einrichtungen verwendet werden.
Die zweite Komponente sind digitale Videokameras. Sie sind heute bereits häufig zur Überwachung von Gängen und Verkehrswegen oder zum Schutz vor Diebstahl installiert. Das anfallende Videomaterial wird dabei aber nicht Live durch einen Operator ausgewertet, sondern lediglich für eine nachgelagerte Auswertung erfasst. Zusätzlich ermöglichen die Algorithmen eine Anonymisierung des Videomaterials.
Die letzte wichtige Komponente sind Server zur Auswertung der digitalen Videodaten. Im Gegensatz zu klassischen Videoüberwachungssystemen sollen die anfallenden Daten durch Algorithmen verarbeitet werden und nur bei besonderen Ereignissen Menschen angezeigt werden.
Das in Abbildung 1 dargestellte System ist so gestaltet, dass es kaum in die täglichen Abläufe im Krankenhaus eingreift. Gleichzeitig soll aber eine optimale Versorgung von Notfällen sichergestellt werden. Sobald das Kamerasystem aktiv ist, werden die anfallenden Videodaten durch Algorithmen zur Notfallerkennung ausgewertet. Ein Zugriff auf die Videodaten durch das Pflegepersonal oder andere Mitarbeiter der Einrichtung ist dabei nicht möglich. Algorithmen zur Videoauswertung unterliegen immer einer gewissen Ungenauigkeit, die nicht vermieden werden kann. Da es wichtig ist alle Stürze zu detektieren, nimmt man in der Konfiguration eine gewisse Anzahl an Fehlalarmen hin, wenn das System nicht zweifelsfrei entscheiden kann was passiert. Detektiert ein Algorithmus eine Notlage (beispielsweise eine gestürzte Person), benachrichtigt das System das räumlich nächste Smartphone, das sich im Bereitschaftsmodus befindet. Wenn der zugehörige Mitarbeiter den Alarm nicht innerhalb einer bestimmten Zeit bearbeitet, wird der Alarm automatisch an einen anderen Kollegen weitergeleitet. Sobald ein Mitarbeiter den Notfall übernimmt, wird er vom System als Bearbeiter angesehen.

[3] Beispiel: *Klack/Möllering/Ziefle/Schmitz-Rode*, Future Care Floor: A sensitive floor for movement monitoring and fall detection in home environments, 2011.

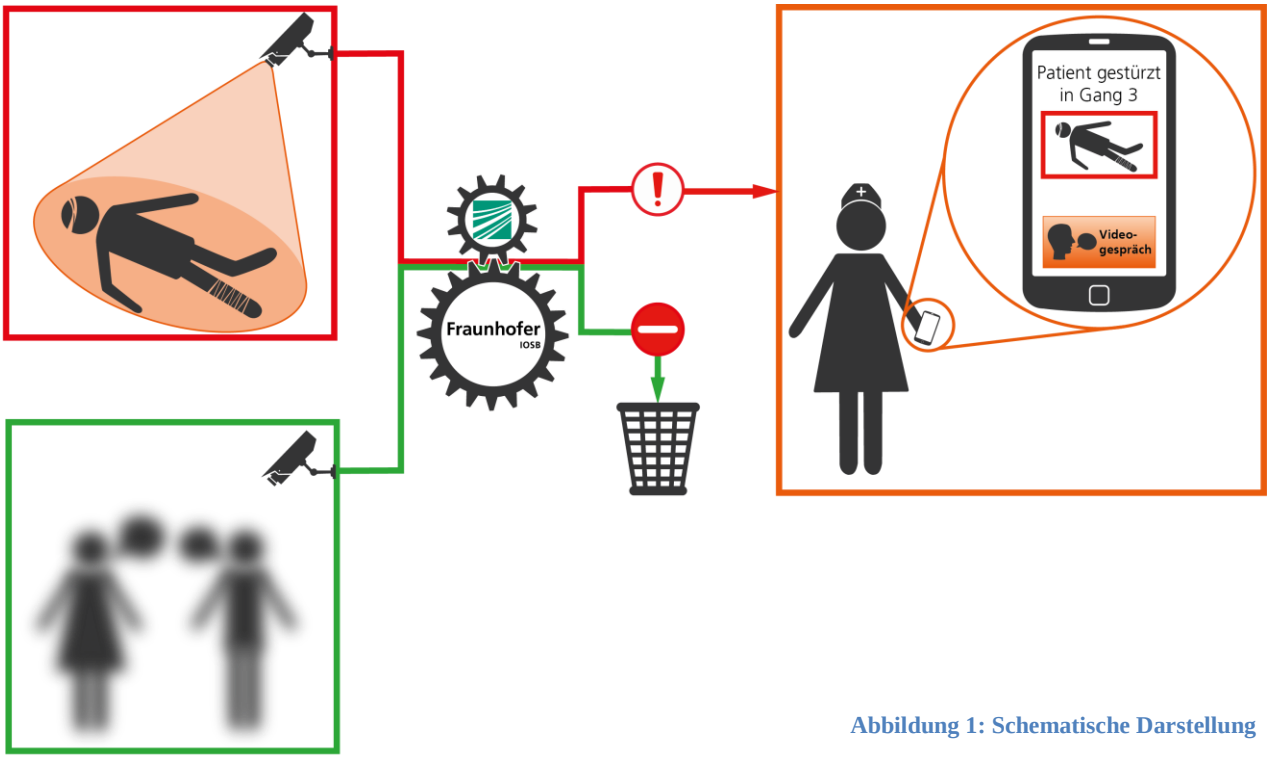

Abbildung 1: Schematische Darstellung

Damit gibt es zu jedem Vorfall immer genau einen Bearbeiter, der das Recht erhält Videomaterial zu betrachten. Um bei möglichen Fehlalarmen den Eingriff in die Privatsphäre Betroffener zu schützen, wird das Videomaterial vor der Anzeige auf dem Smartphone anonymisiert. Dazu werden beispielsweise Gesichter überdeckt, um eine Identifizierung zu verhindern. Der Bearbeiter hat nun die Möglichkeit die anonymisierte Videosequenz zu betrachten und zu bewerten. Bestätigt er den Notfall, so erhält er Zugriff auf den aktuellen Videostrom der Kamera. Er kann nun die Situation bewerten, schauen wie es dem Unfallopfer geht und welche Maßnahmen einzuleiten sind. Sollte er erkennen, dass es sich um einen Fehlalarm handelt, kann er den Vorfall verwerfen und damit das System wieder in seinen Ausgangszustand versetzen.

3. Rechtliche Analyse

Der Einsatz von intelligenten Videoüberwachungssystemen wird in der juristischen Literatur bisher nur wenig erörtert.[4] Gleichwohl handelt es sich dabei um ein Feld, dass höhere Aufmerksamkeit verdient, kommen die bisher verwendeten herkömmlichen Kamera-Monitor-Verfahren immer weniger zur Anwendung. Der Trend geht zum Einsatz von intelligenten Videoüberwachungssystemen. Unter intelligenter Videoüberwachung versteht man dabei Videoüberwachung, die sich der Videoanalyse und des Datenabgleichs bedient.[5] Ein intelligentes und autonomes optisches System kann zusätzlich zur Bildaufnahmeschaltung anwendungsspezifische Informationen aus aufgenommenen Bildern herausfiltern, verarbeiten, Event-Beschreibungen erzeugen und darauf basierende Entscheidungen treffen.[6] Solche neuartigen Systeme müssen sich auch an den rechtlichen Vorgaben orientieren bzw. - noch besser - bereits im Entwicklungsstadium rechtskonform gestaltet werden. Das erscheint jedoch oft schwierig, stammen

[4] Vgl. nur *Bier/Spiecker gen. Döhmann*, CR 2012, 610 ff.; *Roßnagel/Desoi/Hornung*, DuD 2011, 694 ff.; *Hornung/Desoi*, K&R 2011, 153 ff.; *Wrede*, ZD 2012, 321 ff.; *Roßnagel/Desoi/Hornung*, ZD 2012, 459 ff; *Winkler*, DuD 2011, 797 ff.

[5] *Müller*, Videoüberwachung in öffentlich zugänglichen Räumen, 2011, S. 17.

[6] *Winkler*, DuD 2011, 797 (797).

die rechtlichen Rahmenbedingungen - insbesondere die Datenschutzgesetze - häufig noch aus der vordigitalen Zeit.[7] Die rechtliche Analyse kann sich hier deshalb nur auf einen kleinen Ausschnitt beschränken. Zum einen ist die Vereinbarkeit mit § 6 a BDSG (§ 49 ÖDSG), der ein grundsätzliches Verbot automatisierter Einzelentscheidungen normiert, zu hinterfragen. Zum anderen soll auch der Entwurf einer Europäischen Datenschutzgrundverordnung berücksichtigt werden.

3.1. § 6 a BDSG

3.1.1. Allgemein

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen (§ 6 a Abs. 1 S. 1 BDSG). Die Regelung wurde in Umsetzung der Europäischen Datenschutzrichtlinie 95/46/EG (DSRL) in das BDSG aufgenommen.[8] Daher ist § 6 a BDSG stets richtlinienkonform auszulegen. Insbesondere Art. 15 DSRL liegt der deutschen Umsetzung zugrunde.[9] Der Betroffene soll nicht zum bloßen Objekt von Computeroperationen degradiert werden und es soll verhindert werden, dass bei das Persönlichkeitsrecht zentral tangierenden Entscheidungen die Verantwortung in anonymen Computersystemen verschwimmt.[10]
Der deutsche Gesetzgeber hatte primär das Scoring-Verfahren im Blick.[11] Der Einzelne darf nicht zum bloßen Objekt einer technikgestützten Verarbeitung zur Bewertung von Persönlichkeitsmerkmalen werden.[12] Die Regelung ist Ausdruck der Befürchtung, dass nur noch technische Systeme über Menschen bestimmen und der Betroffene dadurch Objekt einer rein automatisierten Bewertung seiner Persönlichkeit wird.[13] Letztendlich soll ein Mensch die persönliche Verantwortung für die zu treffende Entscheidung übernehmen.[14] Die Norm ist als Verfahrensvorschrift ausgestaltet, die zu den eigentlichen datenschutzrechtlichen Erlaubnistatbeständen hinzutritt.[15] Bei der bisherigen Videoüberwachung nach dem Kamera-Monitor-Prinzip war sie nicht einschlägig, weil dort kein System eine Entscheidung vorgenommen hat.[16]
Im Gegensatz dazu werden in intelligenten Videoüberwachungssystemen insbesondere Verhaltensweisen von Personen analysiert, um eine automatisierte Bewertung der Situation zu erhalten. Die Entscheidung, ob beispielsweise ein Alarm ausgelöst wird oder nicht, basiert auf allgemein bestimmten, vorher festgelegten Merkmalen.[17] Zunächst erfolgt die Schlussfolgerung des Systems also automatisch aufgrund der ihm vorgegebenen Parameter; eine menschliche Entscheidung, etwa durch einen nachgeschalteten Beobachter, ist erst zu einem späteren Zeitpunkt

---

[7] *Härting*, NJW 2013, 2065 (2065).

[8] *Kamlah*, in: Plath, BDSG, 2013, § 6a Rn. 1.

[9] *Kamlah*, in: Plath, BDSG, 2013, § 6a Rn. 1.

[10] *Dammann/Simitis*, EG-DSRL, Art. 15 Rn. 2.

[11] *Schaffland/Wiltfang*, BDSG, § 6a Rn. 1; BT-Drs. 14/4329, S. 37.

[12] *Scholz*, in: Simitis, BDSG, 7. Aufl. 2011, § 6a Rn. 3; *Bier/Spiecker gen. Döhmann*, CR 2012, 610 (614).

[13] *Bergmann/Möhrle/Herb*, BDSG, 46. Lfg. 2013, § 6a Rn. 3.

[14] *Dammann/Simitis*, EG-DSRL, Art. 15 Rn. 1; *Mackenthun*, in: Taeger/Gabel, BDSG, 2010, § 6a Rn. 1.

[15] *von Lewinski*, in: Wolff/Brink, BeckOK BDSG, § 6a Rn. 1.

[16] So auch *Hornung/Desoi*, K&R 2011, 153 (158).

[17] *Bier/Spiecker gen. Döhmann*, CR 2012, 610 (614).

vorgesehen.[18] Man wird deshalb in Zukunft nicht mehr nur die Einsatzszenarien und -zwecke genauer untersuchen müssen, sondern muss vor allem die eingesetzte Technik wesentlich differenzierter als bisher betrachten.[19]

3.1.2. Ausschließlich automatisierte Verarbeitung personenbezogener Daten

Die Geltung des Verbots nach § 6 a Abs. 1 S. 1 BDSG greift nur, wenn die Entscheidung auf Grund einer ausschließlich automatisierten Verarbeitung personenbezogener Daten erfolgt. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat (§ 6 a Abs. 1 S. 2 BDSG).
Eine automatisierte Verarbeitung meint die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen (§ 3 Abs. 2 S. 1 BDSG). Als Datenverarbeitungsanlagen versteht man Anlagen zum automatisierten Handhaben von Daten.[20] Intelligente Videoüberwachungssysteme sind als Datenverarbeitungsanlagen zu qualifizieren, da sie ein besonders hohes Maß an automatisierter Verarbeitung aufweisen.
Die Entscheidung darf nicht *ausschließlich* aufgrund der automatisierten Verarbeitung ergehen. Sinn und Zweck der Regelung ist der Schutz des Betroffenen vor computergestützten Entscheidungen, denen er ausgeliefert zu sein scheint, da ihm keine Möglichkeit gegeben wird, seinen Standpunkt gegenüber einem Menschen darzulegen und die computergestützte Entscheidung durch diesen Menschen überprüfen zu lassen.[21] Die natürliche Person, welche die Letztentscheidung trifft, muss eine ausreichende Datengrundlage besitzen, um von der automatisierten Entscheidung abweichen zu können.[22] Die Norm untersagt somit die unmittelbare Anwendung des automatisiert erzeugten Ergebnisses auf einen Sachverhalt.[23]
Keine ausschließlich automatisierte Entscheidung liegt aber dann vor, wenn durch das automatisierte Verfahren eine Entscheidung vorbereitet wird, dann aber eine abschließende Beurteilung durch einen Menschen erfolgt, der das Ergebnis inhaltlich verantwortet.[24] Wird die letzte Entscheidung nach individueller Bewertung im Einzelfall von einem Menschen getroffen, so darf sie sich durchaus auf einen automatisiert erzeugten Entscheidungsvorschlag stützen.[25]
Das Merkmal der ausschließlich automatisierten Verarbeitung personenbezogener Daten bedarf an dieser Stelle hinsichtlich des hier vorgestellten Systems einer näheren Betrachtung.
Die Verarbeitung der personenbezogenen Daten erfolgt automatisiert, da das System selbst entscheidet, in welchen Fällen es einen Sturz detektiert und somit einen Alarm auslöst. Allerdings erscheint fraglich, ob es sich um eine (Letzt-)Entscheidung handelt, die *ausschließlich* auf einer automatisierten Verarbeitung beruht.
Teilt man den (technischen) Geschehensablauf in seine Einzelbestandteile auf, so kann man zu dem Ergebnis kommen, dass eine ausschließlich auf eine automatisierte Verarbeitung erfolgte Entscheidung gegeben ist. Zunächst verarbeiten Algorithmen die anfallenden Daten. Erst wenn ein Algorithmus einen Sturz detektiert, erfolgt ein Alarm vom System. Danach wiederum wird ein

---

[18] *Bier/Spiecker gen. Döhmann,* CR 2012, 610 (614).

[19] Ebenso *Hornung/Desoi*, K&R 2011, 153 (158).

[20] *Dammann,* in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 79.

[21] BT-Drs. 16/10529, S. 13.

[22] BT-Drs. 16/10529, S. 13.

[23] *Scholz,* in: Simitis, BDSG, 7. Aufl. 2011, § 6a Rn. 15; *Bergmann/Möhrle/Herb*, BDSG, §6a Rn. 6.

[24] *Weichert,* in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 6a Rn. 2.

[25] *Scholz,* in: Simitis, BDSG, 7. Aufl. 2011, § 6a Rn. 16 m.w.N.

anonymisierter Videostream übertragen. Wenn der Beobachter denkt einen Sturz erkannt zu haben, kann er auf das Klarbild umschalten. Die Schlussfolgerung des Systems - ob also ein Sturz vorliegt oder nicht - ergeht aber automatisch aufgrund der ihm vorgegebenen Parameter. Eine menschliche Entscheidung erfolgt erst zu einem späteren Zeitpunkt.[26] Der erste Schritt der Verarbeitung von personenbezogenen Daten - nämlich die Erkennung ob überhaupt ein Sturz vorliegt oder nicht - ist aber eine ausschließlich automatisierte Entscheidung.

Nimmt man allerdings eine Gesamtbetrachtung des Überwachungsvorgangs vor, so findet eine Letztentscheidung durch eine natürliche Person statt.[27] Das Überwachungssystem schlägt nur in denjenigen Fällen Alarm, in denen es einen Sturz detektiert. Ob dann tatsächlich ein Sturz vorliegt - oder möglicherweise ein Fehlalarm erzeugt wird - muss durch den Beobachter eigenverantwortlich entschieden werden. Die Letztentscheidung bezieht sich also darauf, dass der Beobachter die Sturzsituation beurteilen und bewerten kann und nach Bedarf Hilfe schicken kann. Demnach liegt keine ausschließlich auf eine automatisierte Verarbeitung von personenbezogenen Daten gestützte Entscheidung vor.

Bei dem hier vorgestellten System ist es vorzugswürdig eine Gesamtbetrachtung des Überwachungsvorgangs vorzunehmen. Das Kamerasystem schaltet nämlich überhaupt nur dann auf ein Klarbild um, wenn ein Sturz detektiert wird. Die Ausgangssituation bleibt dabei aber unverändert. Eine Person stürzt, das Videosystem detektiert den möglichen Sturz und der Beobachter als Letztentscheider erhält das Klarbild übertragen, sodass er nun selbst die Situation bewerten kann. Ihm obliegt es festzustellen, ob tatsächlich eine gefährliche Situation gegeben ist oder es sich um einen Fehlalarm handelt. Da das übertragene Klarbild alle relevanten Informationen enthält, kann der Beobachter eine Letztentscheidung treffen, die auf einer ausreichenden Datengrundlage beruht.

Anders hingegen könnte ein intelligentes Überwachungssystem dann zu beurteilen sein, wenn schon im „Ausgangsszustand“ bestimmte Parameter voreingestellt und festgelegt sind, die es dem Beobachter nicht mehr ermöglichen, aufgrund einer tauglichen Datengrundlage die Situation zu bewerten. Die Software/Hardware könnte so programmiert werden, dass nur noch bestimmte Gruppen von Menschen überwacht werden und alle anderen Personen aus dem Videobild ausgeblendet werden.[28] Erhält der Beobachter dann am Monitor nur noch ein verändertes Bild der Realität, so wird man nicht mehr davon sprechen können, dass keine ausschließlich automatisierte Entscheidung vorliegt. Denn welche Personen von dem System überwacht werden bzw. selbstständig vom Kamerasystem „herausgerechnet“ werden, unterliegt nicht mehr der Entscheidung der natürlichen Person selbst, sondern wird einzig und allein von dem intelligenten Videoüberwachungssystem als solches getroffen. Selbst wenn man das „Herausfiltern“ von Personen aus einem Videobild als (rechtlich) positiv bewertet, da die so Betroffenen gerade nicht mehr überwacht werden, stellt sich doch die Frage, inwieweit der Mensch hier nicht zum bloßen Objekt der Technik gemacht wird. Der Einzelne soll aber gerade nicht zum bloßen Objekt einer technikgestützten Verarbeitung werden.[29]

Handelt es sich im vorliegenden Fall um keine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung, so mag das bei anderen intelligenten Überwachungssystemen abweichend zu bewerten sein. Deutlich wird jedenfalls, dass in Zukunft eine rechtliche Bewertung „der“ intelligenten Videoüberwachung immer weniger möglich sein wird.[30]

---

[26] In diese Richtung *Bier/Spiecker gen. Döhmann*, CR 2012, 610 (614).

[27] In diese Richtung geht auch das Drei-Stufen-Modell von *Roßnagel/Desoi/Hornung*, DuD 2011, 694 (699).

[28] Vgl. auch *Hornung/Desoi*, K&R 2011, 153 (156).

[29] So auch *Scholz*, in: Simitis, BDSG, 7. Aufl. 2011, § 6a Rn. 3.

[30] So bereits *Hornung/Desoi*, K&R 2011, 153 (158).

3.2. Entwurf einer Europäischen Datenschutzgrundverordnung

3.2.1. Allgemein

Seit geraumer Zeit ist der Entwurf einer Europäischen Datenschutzgrundverordnung[31] (DS-GVO-E) allgegenwärtig. Tritt er in Kraft, so wird die DS-GVO-E unmittelbar geltendes Recht in jedem Mitgliedstaat und in allen ihren Teilen verbindlich (Art. 288 AEUV). Damit geht die DS-GVO-E grundsätzlich den nationalen Regelungen vor. Ausnahmen können nur dort in Betracht kommen, wo sie Öffnungsklauseln zugunsten der Mitgliedstaaten vorsieht. Wegen der insgesamt jedoch wenigen und engen Öffnungsklauseln[32] ist davon auszugehen, dass eine Vielzahl von bereichsspezifischen Gesetzen - sowie das BDSG selbst - Rechtsgeschichte werden.[33] Damit gilt § 6 a BDSG auch nicht mehr, der gerade im Bereich der aufkommenden intelligenten Videoüberwachung von besonderer Bedeutung ist.
Trotz der immer besser werdenden technischen Möglichkeiten im Bereich der Videoüberwachung und der damit verbundenen Gefahren, enthält der DS-GVO-E keine ausdrückliche Regelung für (intelligente) Videoüberwachung. Das ist bedauerlich, da nach Schätzungen in Deutschland 400.000[34] und in Großbritannien 4.500.000[35] Videokameras installiert sind. Deshalb müssen sich (intelligente) Videoüberwachungssysteme in Zukunft an den Vorschriften der DS-GVO-E messen lassen.

3.2.2. Zur (intelligenten) Videoüberwachung

3.2.2.1. Anwendungsbereich der DS-GVO-E

Nach Art. 2 Nr. 1 DS-GVO-E gilt die Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Art. 4 Abs. 3 DS-GVO-E definiert das Merkmal der Verarbeitung. Dabei orientiert sich der DS-GVO-E an der DSRL.[36] Leider versäumt der Gesetzgeber an dieser Stelle aber das Merkmal der „Automatisierung“ näher zu definieren, sodass der erforderliche Grad der Automation nicht genauer eingegrenzt wird. *Seifert* schlägt vor, dass man sich daher an der Auslegung der DSRL orientiert.[37] Demnach setzt eine automatisierte Verarbeitung voraus, dass sich der automatische Prozess nicht nur auf den Datenträger, sondern auch auf die Daten mit ihrer inhaltlichen Dimension bezieht.[38] Im Bereich der Videotechnik liegt eine automatisierte Verarbeitung dann vor, wenn etwa eine programmgesteuerte Erfassung nach personenbezogenen Merkmalen erfolgt.[39] Dies ist bei Videosystemen mit integrierter oder zumindest anschließbarer Gesichts- oder Stimmerkennung oder

---

[31] Vorschlag einer Datenschutz-Grundverordnung, KOM(2012) 11 endgültig vom 25.01.2012.

[32] Vgl. hierzu *Piltz/Krohm*, PinG 2013, 56 (58).

[33] *Piltz/Krohm*, PinG 2013, 56 (59).

[34] Vgl. hierzu nur: http://www.foebud.org/pd/pd143, zuletzt abgerufen am 18.12.2013.

[35] Vgl. hierzu nur: http://www.sueddeutsche.de/digital/ueberwachungskameras-in-grossbritannien-die-toten-augen-von-london-1.199517, zuletzt abgerufen am 18.12.2013.

[36] So auch *Seifert*, DuD 2013, 650 (651).

[37] *Seifert*, DuD 2013, 650 (651).

[38] *Scholz*, in: Simitis, BDSG, 7. Aufl. 2011, § 6b Rn. 18.

[39] *Scholz*, in: Simitis, BDSG, 7. Aufl. 2011, § 6b Rn. 18.

bei selektiver Erfassung der Videobilder anhand anderer personenbezogener Informationen zu bejahen.[40]
Der Anwendungsbereich ist demnach auch bei intelligenten Videoüberwachungssystemen eröffnet. Sie ermöglichen in spezieller Weise die selektive Erfassung von Videobildern anhand bestimmter personenbezogener Informationen. Das hier vorgestellte System wird erst dann aktiv, wenn es den Sturz einer natürlichen Person detektiert. Um das zu erkennen, müssen Algorithmen die erfassten Daten selbstständig auswerten und interpretieren.

3.2.2.2. Rechtmäßigkeit der Videoüberwachung

Die Rechtmäßigkeit der Videoüberwachung folgt einem Grundprinzip des deutschen Datenschutzrechts, in dem Art. 6 DS-GVO-E die Zulässigkeit der Datenverarbeitung unter den Vorbehalt einer Einwilligung des Betroffenen oder einer gesetzlichen Erlaubnis stellt.[41]
Beim Einsatz von intelligenten Videoüberwachungssystemen im Krankenhaus kommen als Erlaubnistatbestände Art. 6 Nr. 1 lit. d) und Art. 6 Nr. 1 lit. f) DS-GVO-E in Betracht. Gemäß Art. 6 Nr. 1 lit. d) DS-GVO-E muss die Verarbeitung nötig sein, um lebenswichtige Interessen der betroffenen Person zu schützen oder gemäß Art. 6 Nr. 1 lit. f) DS-GVO-E muss die Verarbeitung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich sein, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Der Schutz der Gesundheit und des Lebens kann den Tatbestand des Art. 6 Nr. 1 lit. d) DS-GVO-E erfüllen. Die intelligente Videoüberwachung in einem Krankenhaus soll Stürze erkennen, sodass schneller und effektiver Hilfe geleistet werden kann. In anderen Bereichen, beispielsweise der Videoüberwachung durch Unternehmen, kann Art. 6 Nr. 1 lit. f) DS-GVO-E einschlägig sein.[42]
Daneben kommt es bei der DS-GVO-E auf eine Auslegung an, die gerade im Kontext der Videoüberwachung auf europäischer Ebene schwierig werden wird.[43] Bei diesem Thema ist nämlich eine völlig unterschiedliche Sensibilität in den einzelnen Mitgliedsstaaten zu berücksichtigen.[44] Während die Videoüberwachung in der deutschen Öffentlichkeit kontrovers und kritisch diskutiert wird[45], ist sie in Großbritannien viel weiter verbreitet.[46]
Die sehr offenen, weiten und unbestimmten Erlaubnistatbestände des Art. 6 DS-GVO-E tragen in diesem Kontext aber nicht zu einer einheitlichen europäischen Auslegung bei. Das ist jedoch gerade das Ziel der DS-GVO-E, die eine Vollharmonisierung auf europäischer Ebene anstrebt.[47]
In der derzeitigen Fassung ist die DS-GVO-E (noch) nicht geeignet auf einem so sensiblen Feld, rechtssichere und rechtsklare Regelungen vorzugeben.[48] Die Erlaubnistatbestände sind zu allgemein formuliert. Unklar ist auch, ob die derzeitigen Regelungen überhaupt mit dem Bestimmtheitsgebot

---

[40] *Scholz*, in: Simitis, BDSG, 7. Aufl. 2011, § 6b Rn. 18.

[41] *Seifert*, DuD 2013, 650 (652).

[42] So *Piltz/Krohm*, PinG 2013, 56 (61); *Seifert*, DuD 2013, 650 (652).

[43] *Piltz/Krohm*, PinG 2013, 56 (61).

[44] *Piltz/Krohm*, PinG 2013, 56 (61).

[45] Vgl. beispielsweise http://www.derwesten.de/staedte/duesseldorf/polizei-muss-videoueberwachung-in-der-duesseldorfer-altstadt-abbauen-id8731473.html, zuletzt abgerufen am 18.12.2013.

[46] *Kühling*, EuZW 2012, 281 (281); *Piltz/Krohm*, PinG 2013, 56 (61).

[47] So auch *Kühling*, EuZW 2012, 281 (281).

[48] So auch *Piltz/Krohm*, PinG 2013, 56 (61); *Seifert*, DuD 2013, 650 (654).

nach Art. 52 Abs. 1 EU-Grundrechte-Charta vereinbar sind.[49] Wünschenswert wäre eine spezifische Videoüberwachungsnorm, die gleichzeitig auch neuartige Techniken wie intelligente Überwachungssysteme mit in den Blick nimmt. Als Vorbild für eine europäische Norm könnte § 6 b BDSG (§ 50 a ÖDSG) dienen. Dieser müsste dann aber noch hinsichtlich intelligenter Überwachungssysteme angepasst werden.

3.2.2.3. Auf Profiling basierende Maßnahmen, Art. 20 DS-GVO-E

Art. 20 DS-GVO-E enthält eine vergleichbare Regelung wie § 6 a BDSG. Eine natürliche Person hat das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihrer beruflichen Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens besteht.
Auch hier geht es um das Recht des Betroffenen, keiner Maßnahme unterworfen zu werden, die auf Profiling basiert. Grundlage dieser Bestimmung ist Art. 15 Abs. 1 DSRL über automatisierte Einzelentscheidungen.[50]
Bei intelligenten Videoüberwachungssystemen muss Art. 20 DS-GVO-E berücksichtigt werden. Die Vorschrift setzt zunächst eine rein automatisierte Verarbeitung voraus. Deshalb muss eine Abgrenzung zwischen automatisierter Verarbeitung und rein automatisierter Verarbeitung vorgenommen werden. Die Verordnung selbst definiert aber nur die Verarbeitung in Art. 4 Abs. 3 DS-GVO-E. Da bereits die Beantwortung der Frage, was überhaupt eine automatisierte Verarbeitung ist, nicht einfach zu beantworten ist[51], verkompliziert sich das Problem dahingehend, dass nun auch noch eine Abgrenzung zwischen automatisiert und rein automatisiert notwendig ist.
Sodann muss die Maßnahme gegenüber dem Betroffenen eine rechtliche Wirkung entfalten oder ihn in maßgeblicher Weise beeinträchtigen. Eine rechtliche Wirkung kann ein Verwaltungsakte entfalten oder auch die Ablehnung eines Kredits.[52] Entscheidend ist nicht, ob die rechtliche Wirkung positiv oder negativ ist. Die DSRL spricht in Art. 15 DSRL noch von „rechtlichen Folgen". Ob zwischen rechtlicher Folge und rechtlicher Wirkung ein Unterschied besteht, bleibt offen. Alternativ kann auch eine Maßnahme ausreichend sein, die den Betroffenen in „maßgeblicher Weise beeinträchtigt". Art. 15 DSRL spricht noch von „erheblich beeinträchtigender Entscheidung". Die neue Regelung übernimmt diese strenge Formulierung nicht mehr. Damit ist das Merkmal offener gefasst. Das erscheint insgesamt ein „weniger" zu sein. Dennoch wird man auch nach der neuen Formulierung jeden Einzelfall für sich beurteilen müssen. Fraglich ist, ob die maßgebliche Beeinträchtigung objektiv oder subjektiv zu bestimmen ist.
Im Bereich der (intelligente) Videoüberwachung zielt diese darauf ab, dass eine Verhaltensanalyse von Personen erfolgt. Die hier vorgestellte Sturzdetektion ist so ein Fall. Das Kamerasystem identifiziert ein „abnormales" Verhalten und schlägt dann Alarm, sodass der Beobachter die Möglichkeit hat, über den Monitor die Situation zu bewerten. Deshalb muss Art. 20 DS-GVO-E grundsätzlich bei (intelligenten) Videoüberwachungssystemen berücksichtigt werden.

---

[49] Hierzu *Borowsky*, in: Meyer, Charta der Grundrechte der Europäischen Union, 3. Aufl. 2010, Art. 52 Rn. 20.

[50] Vorschlag einer Datenschutz-Grundverordnung, KOM(2012) 11 endgültig vom 25.01.2012, S. 10.

[51] Siehe oben.

[52] So für § 6a BDSG *Bergmann/Möhrle/Herb*, BDSG, § 6a Rn. 12.

4. Fazit

Der Aufsatz konnte nur einen sehr kurzen technischen und rechtlichen Überblick geben. Dennoch ist deutlich geworden, dass intelligente Videoüberwachungssysteme immer häufiger zur Anwendung kommen. Die rechtlichen Normen - sowohl die deutschen Datenschutzregelungen als auch der DS-GVO-E - sind noch nicht an diese neuen technischen Gegebenheiten angepasst. Die jetzige Fassung der DS-GVO-E deckt das Feld der (intelligenten) Videoüberwachung bei weitem nicht ab. Selbst für die klassische Videoüberwachung gibt es in der DS-GVO-E keine explizite Regelung. Hier sollte der Europäische Gesetzgeber handeln. Die teils weiten und unbestimmten Erlaubnistatbestände in der DS-GVO-E sind jedenfalls nicht geeignet, um (intelligente) Videoüberwachung erschöpfend zu regeln.[53] Als Vorbild könnte die deutsche Norm des § 6 b BDSG dienen, die jedoch ebenfalls noch an die neuartigen technischen Möglichkeiten angepasst werden muss.

5. Literatur

Bergmann, Lutz/Möhrle, Roland/Herb, Armin, BDSG Kommentar, Boorberg Verlag, Stuttgart (2012)

Bier, Christoph/Spiecker gen. Döhmann, Indra, Intelligente Videoüberwachungstechnik: Schreckensszenario oder Gewinn für den Datenschutz?, CR 2012, 610-618

Dammann, Ulrich/Simitis, Spiros, EG-Datenschutzrichtlinie Kommentar, Nomos-Verlag, Baden-Baden (1997)

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (Hrsg.), BDSG, BUND Verlag, 3. Auflage, Frankfurt am Main (2009)

Härting, Niko, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065-2071

Hornung, Gerrit/Desoi, Monika, „Smart Cameras" und automatische Verhaltensanalyse, K&R 2011, 153-158

Klack, Lars/Möllering, Christian/Ziefle. Martina/Schmitz-Rode, Thomas, Future care floor: A sensitive floor for movement monitoring and fall detection in home environments, Wireless Mobile Communication and Healthcare, 2011, 211-218

Kühling, Jürgen, Auf dem Weg zum vollharmonisierten Datenschutz!?, EuZW 2012, 281-282

Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, Nomos-Verlag, 3. Auflage, Baden-Baden (2010)

Müller, Lucien, Videoüberwachung in öffentlich zugänglichen Räumen, Nomos-Verlag, Baden-Baden (2011)

Noury, N./Herve, T./Rialle, V./Virone, G./Mercier, E./Morey, G./Moro, A./Porcheron, T, Monitoring behavior in home using a smart fall sensor and position sensors, Microtechnologies in Medicine and Biology, 1st Annual International, Conference On. 2000, 607-610

Piltz, Carlo/Krohm, Niclas, Was bleibt vom Datenschutz übrig?, PinG 2013, 56-61

Plath, Kai-Uwe (Hrsg.), BDSG – Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, Dr. Otto-Schmidt Verlag, Köln (2013)

Roßnagel, Alexander/Desoi, Monika/Hornung, Gerrit, Gestufte Kontrolle bei Videoüberwachungsanlagen, DuD 2011, 694-701

Roßnagel, Alexander/Desoi, Monika/Hornung, Gerrit, Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik, ZD 2012, 459-462

Schaffland, Hans-Jürgen/Wiltfang, Noeme, BDSG Kommentar, Erich Schmidt Verlag, Berlin

Seifert, Bernd, Neue Regeln für die Videoüberwachung?, DuD 2013, 650-654

Simitis, Spiros (Hrsg.), BDSG Kommentar, Nomos-Verlag, 7. Auflage, Baden-Baden (2011)

Taeger, Jürgen/Gabel, Detlev (Hrsg.), BDSG Kommentar, Verlag Recht und Wirtschaft, Frankfurt am Main (2010)

Winkler, Thomas, Vertrauenswürdige Videoüberwachung, DuD 2011, 797-801

Wrede, Ann-Karina, Spannungsverhältnis zwischen Datenschutz und Ethik, ZD 2012, 321-324

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, Verlag C.H. Beck, München (2013)

[53] In diese Richtung auch *Seifert*, DuD 2013, 650 (654).