ALEXANDER ROßNAGEL / MONIKA DESOI / GERRIT HORNUNG

Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik

Am Beispiel der smarten Videoüberwachung

Persönlichkeitsmerkmale
Videoaufzeichnung
Selbstorganisierende Kameranetze
Technikgestaltung
Drei-Stufen-Modell

■ Die dynamische Technikentwicklung führt dazu, dass immer wieder neue technische Möglichkeiten für die Überwachung von Bürgern eingesetzt werden. Sollen diese für die Gewährleistung ziviler Sicherheit genutzt werden, ist es erforderlich, sie rechtsverträglich zu gestalten und ihren rechtsgemäßen Einsatz sicherzustellen. Da die seit langem geltenden und sehr abstrakten Regelungen des Datenschutzrechts nicht für diese neuen Anwendungen erlassen worden sind, ist es erforderlich, sie so zu konkretisieren, dass sie den neu entstehenden Risiken adäquat sind. Dabei kommt es für die Konkretisierung darauf an, ein mögliches Spannungsverhältnis zwischen Datenschutz und Ethik möglichst gering zu halten. Mit diesem Thema hat sich auch der Beitrag von Ann-Karina Wrede (ZD 2012, 321 ff.) auseinandergesetzt – allerdings in einer Weise, die Widerspruch hervorrufen muss. Daher greift der folgende Beitrag diese Fragestellung noch einmal auf und zeigt, dass das Spannungsverhältnis durch rechtsgemäße Technikgestaltung im Wesentlichen aufgelöst werden kann.

■ Due to the dynamic development of technology, one can observe a constant advance of new technologies which may be used for the surveillance of citizens. For these to be used to guarantee civil safety, it must be ensured their design and use is legally compatible. As the long applicable and rather vague provisions of current data protection law do not aim at such modern technology, it has become necessary to further define such rules so as to meet newly developed risks. To accomplish any such definition it will be essential to minimize the tension between data protection and ethics. The article by Ann-Karina Wrede (ZD 2012, 321 ff.) addresses that topic, although, in a manner which deserves fierce criticism. Henceforth, the present article will address the same question, showing that the conflict can essentially be solved by legally compatible technology design.

I. Datenschutzrechtlich zulässig, aber ethisch bedenklich?

Wrede geht in ihrem Aufsatz davon aus, dass es zu gravierenden Spannungen zwischen Recht und Ethik[1] kommen kann, wenn „Gesetze aus der analogen Welt eins zu eins in der neuen, digitalen Welt" angewendet werden. Dies könne „zur Folge haben, dass der Einsatz bestimmter Techniken bei Anwendung der bestehenden Gesetze rechtlich zwar zulässig, ethisch aber problematisch sein kann". Diese These erläutert sie an dem Fallbeispiel eines „Pilotprojekts ‚CamInSen' in der Düsseldorfer Arena". Für dieses stellt sie am Ende ihres Beitrags fest, „dass der Einsatz der ‚smarten' Kameras rechtlich sehr wohl zulässig sein kann, an diesem aber dennoch ethische Bedenken bestehen, und dass der ‚richtige' Umgang noch einem Lernprozess unterliegt".

Die Kritik an diesem Beitrag bezieht sich vor allem auf das nicht korrekt recherchierte Fallbeispiel, die fehlende Auseinandersetzung mit der dazu bereits veröffentlichten Literatur und der spezifischen Anwendung des Datenschutzrechts.

Das von *Wrede* genannte Pilotprojekt in der Düsseldorfer Arena wurde nicht vom Verbundprojekt „CamInSens" durchgeführt und hatte einen anderen Zweck als den von ihr beschriebenen.

In dem von ihr beschriebenen Pilotprojekt wurde von Mai bis November 2011 in der Düsseldorfer Arena ein vom Verbundprojekt Hermes entwickelter Evakuierungsassistent für Großveranstaltungen getestet.[2] „CamInSens" hat kein Pilotprojekt in der Düsseldorfer Arena durchgeführt. Sie hat damit leichtfertig ein Forschungsprojekt, das sich gerade intensiv um eine datenschutzrechtlich und ethisch vertretbare Gestaltung und Nutzung smarter Kamerasysteme bemüht, dem Urteil unterworfen, dass hinsichtlich seiner Ergebnisse „ethische Bedenken bestehen" und ignoriert dabei die bisher veröffentlichten Ergebnisse gerade zur datenschutzadäquaten Gestaltung smarter Videosysteme.[3]

Wrede überprüft die rechtliche Zulässigkeit und ethische Vertretbarkeit des Einsatzes „smarter" Videokameras in der ESPRIT-Arena in Düsseldorf. Maßstab der rechtlichen Überprüfung sind die §§ 6b und 6a BDSG, der ethischen Beurteilung verschiedene ethische Theorien.[4] Das „Smarte" an „smarten" Videokameras wird dabei lediglich anhand der ethischen Theorien und des § 6a BDSG geprüft, nicht anhand der Ermächtigungsgrundlage des § 6b BDSG.[5]. Diese Vorschrift wird zwar ausführlich in Bezug auf das Vorliegen des unproblematisch vorliegenden Tatbestandsmerkmals „Beobachtung" geprüft, die „smarte" Technik findet aber in der Prüfung des Merkmals „Beobachtung" keine Berücksichtigung. Die Tatbestandmerkmale „Verarbeitung oder Nutzung", für die nach § 6b Abs. 3 BDSG strenge Anforderungen gelten, werden gar nicht erwähnt. Daher findet die „smarte" Technik auch keinen Eingang in die von § 6b Abs. 1 und Abs. 3 BDSG geforderte Interessenabwägung und damit in die Frage, ob der Einsatz „smarter" Videokameras erforderlich ist und keine schutzwürdigen Interessen der Betroffenen überwiegen. In die Abwägung der Interessen des Betreibers an dem Einsatz der Kameras mit den schutzwürdigen Interessen der Betroffenen finden aber durchaus ethische Elemente Eingang, die von *Wrede* nicht berücksichtigt werden..

1 Das richtige Handeln beschreibt eigentlich die Moral, Ethik ist dagegen die Lehre über moralische Aussagen. Im Folgenden wird jedoch die Bezeichnung Ethik beibehalten, um den Nachvollzug der Auseinandersetzung mit Aussagen von *Wrede,* die sich auf Ethik beziehen, nicht zu gefährden.
2 http://www2.fz-juelich.de/jsc/appliedmath/ped/projects/hermes-de/; http://subs.emis.de/LNI/Proceedings/Proceedings176/178.pdf; http://www.bmbf.de/pubRD/Hermes_Holl_Auftakt_IPF_SuRvM.pdf.
3 S. z.B. *Hornung/Desoi*, K&R 2011, 153; *Roßnagel/Desoi/Hornung*, DuD 2011, 694.
4 S. *Wrede*, ZD 2012, 321, 322 ff.
5 Hätte *CamInSens* das Pilotprojekt durchgeführt, wäre § 29b DSG NRW vorrangig gewesen.

Dies führt zu dem inhaltlichen Hauptkritikpunkt: Es darf nicht darum gehen, „Gesetze aus der analogen Welt eins zu eins in der neuen, digitalen Welt" anzuwenden und dann die neue Technik als „rechtlich zwar zulässig" anzusehen, aber ihre ethische Bedenklichkeit herauszustellen. Dadurch entsteht eine selbstinszenierte, sachlich aber vermeidbare und unfruchtbare Spannung zwischen Recht und Ethik. Vielmehr muss es darum gehen, das bestehende Datenschutzrecht so zu interpretieren, dass es – ethisch informiert – den Risiken für Grundrechte gerecht wird, und die „smarte" Technik so zu gestalten, dass sie den risikoadäquaten Anforderungen des Datenschutzrechts genügt. Dadurch werden die wesentlichen Spannungen zwischen Datenschutzrecht und Ethik vermieden.

II. Was macht „CamInSens"?

„CamInSens" hat das Ziel, ein rechtskonformes „smartes" Videoüberwachungssystem zur in-situ-Erkennung von Gefahrensituationen zu entwickeln. Hierdurch soll den Betreibern und Einsatzkräften ermöglicht werden, konkrete Bedrohungssituationen im Moment ihrer Entstehung zu erkennen und darauf zu reagieren. Dazu werden selbstorganisierende Kameranetze entwickelt, die kooperativ visuelle Daten erheben und automatisiert verarbeiten, um hieraus in Bildsequenzen des gesamten Kameranetzwerks die Trajektorien (Bewegungsmuster) einzelner Personen gewinnen zu können. Die Interpretation der Trajektorie erfolgt durch einen Vergleich mit an diesem Ort – nicht einem beliebigen Ort wie dem „Wochenmarkt"[6] – durchschnittlichen Bewegungsmustern und dient der Erkennung auffälliger Bewegungsmuster. Werden diese erkannt, wird automatisiert die Aufmerksamkeit einer Einsatzkraft in der Sicherheitszentrale auf die Trajektorie gelenkt. Die Einsatzkraft entscheidet dann über die zu ergreifende Maßnahme.

Die Aufgabe der *Projektgruppe verfassungsverträgliche Technikgestaltung (provet) des Forschungszentrums für Informationstechnik-Gestaltung (ITeG) der Universität Kassel* innerhalb des Verbundprojekts „CamInSens" besteht darin, die Chancen und Risiken solcher „smarten" Kamerasysteme für rechtliche Ziele zu untersuchen und Konzepte zu entwerfen, um die Interpretation – oder im Extremfall im Wege eines Gesetzgebungsvorschlags auch den Wortlaut – von einschlägigen Rechtsregeln einem – auch ethisch – adäquaten Umgang mit diesen Chancen und Risiken anzupassen. Soweit Klarheit besteht, wie das Datenschutzrecht fortzuentwickeln ist, werden Vorschläge erarbeitet, um das technisch-organisatorische System smarter Videoüberwachung entsprechend den risikoadäquaten und chancenwahrenden rechtlichen Anforderungen zu gestalten.

III. Rechtliche Probleme „smarter" Videotechnik

Der Einsatz „smarter" Videoüberwachungssysteme zieht verschiedene rechtliche Probleme nach sich. Sie können im Folgenden nur im Überblick dargelegt werden.[7]

Die Streubreite des Eingriffs wird gegenüber herkömmlicher Videoüberwachung vergrößert, da mit Hilfe der „smarten" Videotechnik mit geringerem Aufwand mehr Daten, wie beispielsweise Trajektorien, über eine Person erhoben und mehr Personen erfasst werden können. Darüber hinaus werden durch das Analyseverfahren Daten erhoben, die dem durchschnittlichen Betrachter durch bloße Beobachtung nicht ersichtlich sind. Ferner besteht die Möglichkeit, die Systeme mit biometrischen Datenbanken zu verknüpfen und so ggf. weitere Informationen über einen Betroffenen zu erlangen. Dadurch wird der Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG signifikant vertieft.

Gefährdungen können sich auch beim Gleichheitsgebot des Art. 3 GG ergeben. In die Software des „smarten" Systems muss durch Parameter eine Definition „durchschnittlichen" Verhaltens aufgenommen werden. Fließen dabei subjektive Vorstellungen derjenigen ein, die das System konfigurieren, können Vorurteile intensiviert und perpetuiert werden. Werden dagegen selbstlernende Algorithmen verwendet, können sogar Diskriminierungen auf Grund äußerlicher Merkmale wie Hautfarbe, Alter oder Geschlecht verhindert werden.

Schließlich könnten Eingriffe in die von Art. 2 Abs. 1 GG geschützte allgemeine Handlungsfreiheit oder in andere Grundrechte entstehen. Wer unsicher ist, ob abweichende Verhaltensweisen erfasst, verwendet oder weitergegeben werden, könnte versuchen, nicht durch solche Verhaltensweisen aufzufallen und sich stattdessen zum ordnungsgemäßen, polizeigerecht-disziplinierten Freiheitsgebrauch verpflichtet sehen.[8]

Auf einfachgesetzlicher Ebene ist in erster Linie die Frage der Ermächtigungsgrundlage für den Einsatz der „smarten" Videoüberwachungskameras problematisch. Da der Gesetzgeber 2001 im Gesetzgebungsverfahren zum Erlass des § 6b BDSG zumindest biometrische Verfahren erwähnte[9] und insoweit offenbar davon ausging, dass der Tatbestand einen technischen Fortschritt mit umfasst, wird auch die „smarte" Videotechnik von der Norm umfasst. In § 6b Abs. 1 BDSG wird aber lediglich die Zulässigkeit der „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung)" geregelt. Die für die „smarte" Videotechnik erforderlichen Analyseverfahren beschränken sich nicht ausschließlich auf die optische Erfassung der Videobilder, sondern verarbeiten darüber hinaus mittels informatischer Algorithmen die Videosequenzen. Die „smarte" Analyse ist daher nicht unter § 6b Abs. 1, sondern unter § 6b Abs. 3 BDSG zu subsumieren, der die weitere Verarbeitung und Nutzung der Videodaten regelt. Die Anwendung hat zur Folge, dass beim Einsatz „smarter" Videokameras eine doppelte Erforderlichkeitsprüfung und Interessenabwägung durchzuführen ist, die sowohl in § 6b Abs. 1 BDSG als auch in § 6b Abs. 3 BDSG gefordert wird. Dabei sind die gegenüber der herkömmlichen Videoüberwachung intensiveren Grundrechtseingriffe zu berücksichtigen, die häufig zu einem Überwiegen der schutzwürdigen Interessen der Betroffenen führen werden.[10]

Um die Intensität der Grundrechtseingriffe abzuschwächen und die Umsetzung verfassungs- und datenschutzrechtlicher Vorgaben zu gewährleisten, wurden im Projekt „CamInSens" aus den rechtlichen Vorgaben der informationellen Selbstbestimmung und des BDSG Bewertungskriterien erarbeitet und für ihre Umsetzung technische Gestaltungsvorschläge entwickelt, die bei der Gestaltung und beim Einsatz des „smarten" Videoüberwachungssystems umgesetzt wurden. In diese Bewertungskriterien sind weitgehend die Aspekte mit eingegangen, die *Wrede* in ihrer ethischen Bewertung berücksichtigt sehen will.[11]

Mit dem Drei-Stufen-Modell wurden ein zentrales Bewertungskonzept und aus ihm abgeleitet geeignete Gestaltungsvorschläge bereits veröffentlicht.[12] Durch das Drei-Stufen-Modell wird

6 So aber *Wrede*, ZD 2012, 321, 324.

7 S. ausführlich und unter Abgrenzung zur wissenschaftlichen Erfassung „herkömmlicher" Videoüberwachungssysteme *Hornung/Desoi*, K&R 2011, 153, 155 ff.; *Roßnagel/Desoi/Hornung*, DuD 2011, 694 ff.; die vorliegende Darstellung verzichtet auf die Darstellung dieser Diskussion; s. dazu die Nw. in den beiden angegebenen Texten.

8 BVerfGE 65, 1, 43; *Dolderer*, NVwZ 2001, 130, 132.

9 BT-Drs. 14/5793, 62.

10 S. zu der rechtlichen Problematik „smarter" Videotechnik ausf. *Hornung/Desoi*, K&R 2011, 153, 155 ff.

11 *Wrede*, ZD 2012, 321, 324.

12 *Roßnagel/Desoi/Hornung*, DuD 2011, 694 ff.

ie Intensität der Überwachung und damit des Grundrechtseingriffs abhängig vom Grad der Feststellung einer Gefahr auf jeder Stufe so gering wie möglich gehalten. Hierfür werden die Kamerasysteme so ausgestaltet, dass sie in der Grundeinstellung so wenige (Wieder-)Erkennungsmerkmale der überwachten Personen übertragen und aufnehmen wie möglich. Dies wird durch die Verwendung von Anonymisierungs- oder Pseudonymisierungsverfahren auf den ersten beiden Stufen des Modells ermöglicht. Erst bei Vorliegen von Anhaltspunkten für Prognosen zu unterschiedlich wahrscheinlichen Gefahren werden schrittweise weitere Details der überwachten Situation erhoben und gespeichert. Das Drei-Stufen-Modell soll in erster Linie den Eingriff in das Recht auf informationelle Selbstbestimmung so gering wie möglich gestalten. Darüber hinaus kann das Modell auf Grund der Anonymisierung oder Pseudonymisierung der überwachten Personen auf den ersten beiden Stufen den Eingriff in die o.g. Grundrechte abmildern. Wenn „smarte" Videoüberwachung nach dem Drei-Stufen-Modell ausgestaltet wird, kann daher die in § 6b Abs. 1 und Abs. 3 BDSG geforderte Abwägung zwischen den Interessen der Betreiber der „smarten" Videoüberwachungsanlagen und damit des dahinter stehenden Schutzauftrags und den schutzwürdigen Interessen der Betroffenen zu Gunsten der Betreiber ausfallen, weil die Eingriffe weniger intensiv sind.

- **1. Stufe:** Auf der ersten Stufe werden die Personen, abhängig von den Einsatzanforderungen, anonymisiert oder pseudonymisiert dargestellt. Der Übergang in die zweite Stufe (gezielte Personenverfolgung) erfolgt automatisch durch die Software oder manuell durch den Beobachter. Voraussetzung ist, dass ein Verhalten festgestellt wurde, das hinreichende Anhaltspunkte enthält, um bei verständiger und besonnener Lagebeurteilung eine Situation anzunehmen, die erfahrungsgemäß eine Gefahr verursacht (Gefahrenverdacht).
- **2. Stufe:** In der zweiten Stufe werden sich auffällig verhaltende Personen gezielt mit Zoomfunktion auf ihrem weiteren Weg überwacht, ohne dass dabei die biometrischen Merkmale der Person erfasst werden. Die markierte Person wird getrackt und ihr weiteres Verhalten daraufhin überprüft, ob es auf eine Gefahrensituation schließen lässt. Der Übergang in die dritte Stufe (Personenerkennung) kann ebenfalls automatisch oder manuell erfolgen, 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.
- **3. Stufe:** In der dritten Stufe wird die Situation in Detailschärfe auf den Monitor übertragen, die Videobilder werden so aufgenommen und gespeichert, dass das Geschehen später zu Beweiszwecken nachvollzogen werden und die verdächtige Person identifiziert werden kann. Mit Eintreten in die dritte Stufe können weitergehende Maßnahmen der Gefahrenabwehr und der Strafverfolgung erforderlich sein, die aber nicht mehr automatisiert, sondern nur noch manuell durch eine Person mit einem echten Ermessensspielraum eingeleitet werden dürfen.

IV. Das Drei-Stufen-Modell und das Spannungsverhältnis Datenschutz – Ethik

Fließt die mehrfach erhöhte Eingriffsintensität in die Prüfung der Erforderlichkeit und die Interessenabwägung des § 6b Abs. 3 BDSG ein, wird die Abwägung in der Regel zu Gunsten der schutzwürdigen Interessen der Betroffenen ausfallen, wenn „smarte" Videotechnik eingesetzt werden sollte. Dies führt zu der Konsequenz, dass Videoüberwachung mittels „smarter" Technik bei normaler Ausgestaltung nur in Ausnahmefällen eingesetzt werden darf. Sie ist nur zulässig, wenn zumindest eine besondere Begründung hinsichtlich der Erforderlichkeit (besondere Bedrohungsszenarien, gefährdete Objekte) besteht. Wird dies nicht beachtet, kann die Abwägung ergeben, dass zwar die Beobachtung durch optische-elektronische Einrichtungen als solche nach § 6b Abs. 1 BDSG zulässig, die automatische Analyse nach § 6b Abs. 3 Satz 1 BDSG aber unzulässig ist.[13] Dies wird – ohne konkrete Anhaltspunkte für ein realistisches Bedrohungsszenario – in der Regel bei einem Einsatz „smarter" Videotechnik in Fußballarenen der Fall sein. Stadien sind nämlich grundsätzlich keine besonders gefährdeten Objekte wie beispielsweise Flughäfen, in denen der Einsatz dieser Technik eher rechtfertigungsfähig ist.

Wird die „smarte" Videoüberwachungsanlage dagegen nach dem Drei-Stufen-Modell gestaltet, werden biometrische Merkmale Betroffener nur dann erkennbar dargestellt und aufgezeichnet, wenn ein Gefahrenverdacht besteht – anders als beim Einsatz herkömmlicher Videokameras nach dem gegenwärtigen Stand der Technik, bei denen ständig biometrische Merkmale erkennbar dargestellt und aufgezeichnet werden. Daher wird der Eingriff in das Recht auf informationelle Selbstbestimmung durch rechtsadäquat gestaltete „smarte" Videosysteme vermindert. Werden zusätzlich selbstlernende Algorithmen verwendet, wird darüber hinaus der Eingriff in das Diskriminierungsverbot vermieden oder vermindert.

Die ethischen Probleme, die *Wrede* aufwirft, stellen sich daher in „CamInSens" entweder nicht mehr oder werden stark reduziert. Werden selbstlernende Algorithmen verwendet, wird das durchschnittliche Verhalten eines Fußballfans Maßstab zur Überprüfung durchschnittlichen Verhaltens. Da bei der großen Anzahl von Personen in einem Stadion eine große Bandbreite von menschlichem Verhalten erfasst wird, wird die Toleranzschwelle für abweichendes Verhalten entsprechend groß sein. Ob auffälliges Verhalten vorliegt, das Folgemaßnahmen durch das Sicherheitspersonal rechtfertigt, wird von einem Menschen mit echtem Ermessensspielraum entschieden. Insoweit werden die Fragen, die *Wrede* bei der Überprüfung ethischer Maßstäbe nach der deontologischen Theorie aufwirft, zu Gunsten der Grundrechte der Stadionbesucher beantwortet. Auch die „Schäden", die *Wrede* im Rahmen ihrer ethischen Überprüfung nach der teleologischen Theorie am Recht auf informationelle Selbstbestimmung anspricht, werden durch das Drei-Stufen-Modell erheblich verringert oder mangels personenbezogener Daten sogar vermieden. Auf Grund der Letztentscheidungskompetenz einer Person mit einem echten Ermessensspielraum wird ferner sichergestellt, dass die Folgemaßnahmen nicht den von ihr angesprochenen „Sockenhochzieher" treffen. Die geringere Eingriffsintensität ermöglicht in den Anwendungsfällen, in denen Eingriffe vermieden werden können, „smarte" Videosysteme zur verbesserten Erfüllung des Schutzauftrags einzusetzen und dadurch auch die nach der teleologischen Theorie zu berücksichtigenden Chancen zu realisieren.

V. Ergebnis

Wird Datenschutzrecht nicht aus der analogen Welt eins zu eins in die digitale Welt übertragen, sondern risikoadäquat fortentwickelt, werden Datenschutzrecht und Ethik zu vergleichbaren Ergebnissen gelangen. Werden „smarte" Videoüberwachungsanlagen – wie in dem Verbundprojekt „CamInSens" – nach dem Drei-Stufen-Modell gestaltet, entsteht kein gravierendes Spannungsverhältnis zwischen Datenschutz und Ethik.

13 Ausf. *Hornung/Desoi*, K&R 2011, 153, 157.

Prof. Dr. Alexander Roßnagel
ist Professor für Öffentliches Recht an der Universität Kassel, wissenschaftlicher Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnikgestaltung (ITeG).

Monika Desoi
ist Wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel.

Prof. Dr. Gerrit Hornung, LL.M.
Ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau, der auch in das Institute of IT-Security and Security Law (ISL) der Universität eingebunden ist.

Der Text ist i.R.d. BMBF-geförderten Projekts „Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung Personen-induzierter Gefahrensituationen (CamInSens)", FKZ 13N10814, entstanden.