DIN

KoSi/KITS Whitepaper

Sichere Videotechnik

Ko·Si K·ITS

Vorwort

Sehr geehrte Leserinnen und Leser,

die Überwachung öffentlicher und halböffentlicher Räume durch Videotechnik ruft bei vielen Menschen sicherlich gemischte Gefühle hervor: einerseits ein Unbehagen vor persönlicher Überwachung, anderseits hat sie sich aber als wirksames Mittel zur Steigerung der allgemeinen Sicherheit erwiesen. Der hohe Bedarf und der vielfältige Einsatz von Sicherheitslösungen sowie die Einbindung neuer Technologien – wie der automatisierten Bildauswertung durch künstliche Intelligenz – schaffen zudem eine Konstellation, die sich durch eine hohe Komplexität mit einer unüberschaubaren Fülle von Randbedingungen auszeichnet. Es ist also höchste Zeit, die Situation zu analysieren und aufzubereiten.

Warum geschieht dies mit Fokus auf Normung und Standardisierung? Beides sind bewährte Instrumente, verschiedene Sichtweisen zusammenzubringen und gemeinsame Standpunkte zu formulieren. In Normung und Standardisierung fließen die Wissensstände der unterschiedlichen Stakeholder zusammen, um daraus gemeinsame Schlussfolgerungen zu ziehen und festzuhalten.

Die Herausforderungen in Bezug auf Videotechnik zur Sicherung öffentlicher Räume sind gewaltig: Regulatorische und gesetzliche Rahmenbedingungen wie die Datenschutzgrundverordnung müssen beachtet und sowohl technologische Entwicklungen als auch Auswirkungen auf Mensch und Gesellschaft müssen berücksichtigt und vorausgedacht werden. Doch gerade in solch komplexen Umfeldern können Normung und Standardisierung entscheidende Instrumente sein, die Vorteile einer Technologie zu nutzen und gleichzeitig die Gefahren beherrschbar zu machen. Normen und Standards reduzieren Komplexität, helfen einmal gefundene Lösungen im Markt zu etablieren und schaffen Vertrauen bei Kunden und der Öffentlichkeit.

Würden wir uns zukünftig mit einem Gefühl der Sicherheit und im Vertrauen auf eine Technologie, die in allen Belangen dem Stand der Technik und auch unseren Werten entspricht, wohlmöglich viel freier im öffentlichen Raum bewegen? Und bedarf es gesetzlicher Anpassungen oder wie können Normen und Standards eine Lösung unterstützen? Dies soll im Folgenden beleuchtet werden, um die Diskussion in der Fachöffentlichkeit anzustoßen.

Wir wünschen Ihnen eine informative Lektüre.

Dr. Michael Stephan
DIN - Mitglied der Geschäftsleitung
Bereich Normung und Standardisierung

Zu den Koordinierungsstellen

Koordinierungsstelle IT-Sicherheit

Der Austausch von Informationen ist die Voraussetzung für die Koordinierung von Aktivitäten. Die Koordinierung von Aktivitäten ist Voraussetzung, ein Wirrwarr an Regelungen zu vermeiden und Ressourcen effizient einzusetzen. Diesen Aufgaben hat sich die Koordinierungsstelle IT-Sicherheit (KITS) verschrieben.

In der KITS findet der Informationsaustausch zwischen den verschiedenen Bereichen und Domänen statt, die sich mit der Normung von IT-Sicherheitsaspekten befassen. Durch öffentliche Veranstaltungen, Workshops und Konferenzen trägt die KITS dazu bei, ein Bewusstsein für die Bedeutung von IT-Sicherheit zu schaffen und die Normung als ein Instrument zur Lösung vielfältigster Fragestellungen zu verankern.

Zu diesem Zweck wird die Kommunikation mit anderen Regelsetzern (Verbände, Vereine, Behörden), die auf dem Gebiet der IT-Sicherheit arbeiten, gefördert. Ziel ist es, diese Arbeiten gegebenenfalls sowohl bei den KITS-eigenen Aktivitäten zu berücksichtigen als auch im Sinne der Normung zu beeinflussen.

Das zentrale Entscheidungsorgan der KITS ist der Fachbeirat, in dem die anzustrengenden Koordinierungsaktivtäten festgelegt werden. Zugeordnet ist die KITS dem DIN-Präsidialausschuss FOCUS.ICT.

Die KITS wird gefördert durch das Bundesministerium für Wirtschaft und Energie.[1]

Koordinierungsstelle Sicherheitswirtschaft

Der Bereich Sicherheit umschließt ein sehr breites Spektrum von Fragestellungen und Aspekten, die zugleich eine ebenso hohe Anzahl an Branchen und Technologiefeldern betreffen. Normung und Standardisierung gestalten dabei die Rahmenbedingungen für den Sicherheitsmarkt.

Die Koordinierungsstelle Sicherheitswirtschaft (KoSi) befasst sich mit branchenübergreifenden normungs-, standardisierungs- und forschungsbezogenen Aktivitäten für die Sicherheitsbranche. Sie sorgt für eine enge Zusammenarbeit der DIN-Gremien und steht allen Interessierten der Sicherheitswirtschaft als zentraler Ansprechpartner zur Verfügung.

Ausgewählte Fachexperten aus den interessierten Kreisen bilden ein Beratergremium, das Fragen der Normung und Standardisierung in der Sicherheitswirtschaft diskutiert und inhaltliche Zielstellungen für die Arbeit der Koordinierungsstelle vorgibt.

Das zentrale Entscheidungsorgan der KoSi ist der Fachbeirat, der durch eigene, aus der Praxis herangetragene und abstrahierte Bedarfe, strategische Impulse hinsichtlich einer intensiveren Verfolgung bereits bestehender oder neu aufzunehmender Aktivitäten, in die Normung gibt.[2]

Ihr Ansprechpartner

DIN e. V.
Volker Jacumeit (Geschäftsführer KITS)
volker.jacumeit@din.de
Burggrafenstr. 6
10787 Berlin

Ihr Ansprechpartner

DIN e. V.
Andreas Schleifer (Geschäftsführer KoSi)
andreas.schleifer@din.de
Burggrafenstr. 6
10787 Berlin

Zusammenfassung

Der Einsatz von Videotechnik in Deutschland ist auch im Zeitalter der Digitalisierung noch eher verhalten, insbesondere im öffentlichen Raum. Dies ist zum einen der Komplexität des Themas geschuldet, aber auch der rechtlichen Unsicherheit im Betreiben einer videotechnischen Anlage im öffentlichen Raum, aufgrund der teilweise sehr unterschiedlichen Anforderungen in den einzelnen Bundesländern.

Die Komplexität ergibt sich sowohl aus der Technologie, der Beteiligten, als auch dem Anwendungsfeld und lässt sich durch die Betrachtung dieser drei Dimensionen etwas vereinfacht veranschaulichen. Dadurch wird klar, dass ein Nachweis über die Einhaltung der geforderten Anforderungen teilweise nur schwer zu erbringen ist, da sich nicht nur der Stand der Technik rasant weiterentwickelt. Aber es existieren noch keine anerkannten Zertifizierungsschemata. Die Planer, Hersteller, Errichter und Betreiber von videotechnischen Anlagen sehen sich einer ganzen Reihe von unterschiedlichsten Vorschriften und Richtlinien gegenüber und benötigen Orientierungshilfen und allgemein abgestimmte Verfahrensregeln.

Die internationale Normung und Zertifizierung bilden hier eine wichtige Grundlage.

Eine Konformitätsbewertung muss zudem über den gesamten Lebenszyklus einer videotechnischen Anlage durchgeführt werden und beschränkt sich nicht nur auf die Hardware, sondern bezieht sich auch auf Software und alle Aspekte des Lebenszyklus bis hin zu den Nutzern.

Damit sich Deutschland auf dem internationalen Markt auch in Zukunft gegen Technologieriesen behaupten kann, sind alle Akteure am Markt und Regelsetzer angehalten abgestimmte Regeln und Anforderungen an Videotechnik zu entwickeln. Normung und Standardisierung kann hier dabei unterstützen die Interessen der Marktteilnehmer auf europäischer und internationaler Ebene zu stärken.

Als Ergebnis dieses Whitepapers werden am Ende des Dokuments Handlungsempfehlungen formuliert.

Inhaltsverzeichnis

1 Einleitung

Die Videotechnik hat mit ihren vielfältigen Einsatzmöglichkeiten Einzug im privaten, unternehmensbezogenen, halböffentlichen und öffentlichen Raum gehalten. Die Sicherung öffentlicher Räume und öffentlich zugänglicher Liegenschaften mittels Videotechnik hat sich zu einem etablierten Werkzeug des Sicherheitsmanagements entwickelt. Der Einsatz von Videotechnik bringt unbestritten viele Vorteile mit sich, birgt aber auch Risiken, die Vorbehalte gegen diese Technik wecken.

Aufgrund dieser Vorbehalte ist der Einsatz von Videotechnik in Deutschland bisher verhalten.

Die Normung ist ein klassisches Instrument, wenn es darum geht über auseinandergehende Interessen zu verhandeln und ein ausgewogenes Ergebnis als „Stand der Technik“ festzuhalten. Dabei kann Normung zu ganz unterschiedlichen Aspekten betrieben werden, zum Beispiel um die Leistungsfähigkeit technischer Systeme offen, nachvollziehbar und vergleichbar darzustellen und somit beispielsweise als Hilfestellung im Beschaffungsprozess zu dienen. Gerade bei der Beschaffung und Errichtung von Videosystemen kommen häufig öffentliche Ausschreibungsverfahren zum Einsatz. Normen und Standards können dabei helfen, diese Verfahren zu vereinfachen und ferner, eine einheitliche Ausschreibungsgrundlage für sich wiederholende Anforderungen zu bilden.

Nicht regulierte oder standardisierte Bereiche hingegen können zu Intransparenz und mangelnder Akzeptanz neuer Technologien führen. Dies zeigt sich derzeit am fragmentierten Markt für Videotechnik, der die notwendige Transparenz für effiziente Entscheidungsprozesse nicht aufzeigt.

Die technischen Fortschritte der Videotechnik haben die Leistungsfähigkeit der Systeme enorm erhöht und den potentiellen Einsatzbereich deutlich erweitert. Für die Planung, Errichtung und den Betrieb von Videosystemen ist die Situation damit aber auch wesentlich komplexer geworden, da weitergehende regulatorische Anforderungen einzuhalten sind und nicht zuletzt die Akzeptanz der Videotechnik in der öffentlichen Diskussion nur durch Transparenz erlangt werden kann.

Verstärkt werden sowohl die Leistungsfähigkeit der Videotechnik wie auch die Vorbehalte gegen ihren Einsatz durch die allgemeine Entwicklung zur „Digitalisierung“. Digitalisierung bedeutet technisch gesehen den umfangreichen Einsatz von Informations- und Telekommunikations-Technologien (ITK). Dies bringt neue Herausforderungen mit sich, die in der Komplexität der Video-ITK, deren Vernetzung, einer angemessenen IT-Sicherheit sowie der gesetzlich geforderten Sicherstellung des Datenschutzes liegen.

In der Videotechnik müssen damit von Herstellern, Planern, Errichtern und Betreibern zukünftig neben bekannten und bewährten Regulierungen und Standards zusätzliche Anforderungen aus der Welt der ITK-Technologie und des Datenschutzes berücksichtigt werden.

Videotechnik ist durch die digitalen Komponenten und Vernetzung als Baustein eingebettet in verschiedenste IT-Konzepte, z. B. Digitalisierung der Gebäudetechnik und öffentlichen Räume oder Industrie 4.0. Kameras sind heute intelligente Komponenten mit Sensoren/Aktoren und damit ein IoT Device welches über IT-Netzwerke mit zentraler IT-Technik verbunden ist. Damit rücken die erforderlichen IT-Sicherheitsmaßnahmen für die eingesetzte Videotechnik neben den bereits bisher geltenden umfangreichen Regulierungen in den Blickpunkt dieser Technologie.

Um die Vorteile der Videotechnik trotz dieser gestiegenen Komplexität nutzen zu können, muss die Komplexität der Rahmenbedingungen reduziert werden. Normen und Standards sind hier ein Mittel, dieses zu erreichen. Das vorliegende Whitepaper soll den Weg aufzeigen, wie die Normung als Instrument eingesetzt werden kann und welche Rahmenbedingungen dabei berücksichtigt werden müssen, um dieses Ziel zu erreichen.

1 Einleitung

Es gibt divergierende Interessen, welche die Videotechnik vor große Herausforderungen stellt. Es steigt sowohl der Bedarf an Sicherheit im öffentlichen Raum, als auch ein verlässlich vertrauenswürdiger Umgang mit personenbezogenen Daten, die bei der Verarbeitung entstehen. Dies muss von den verschiedenen interessierten Kreisen zusammengebracht werden. Bei Nichtgelingen droht das Scheitern einer ganzen Technologie mit allen seinen negativen Auswirkungen.

2 Zielstellung und Aufbau

Ausgangspunkt dieses Whitepapers ist die aktuell in der Bundesrepublik Deutschland bestehende „rechtliche Unsicherheit“ im Bereich des Einsatzes von Videotechnik. Unter anderem ist es durch fehlende höchstrichterliche Rechtsprechung für Entwickler, Hersteller, Planer und Betreiber von Videosystemen schwierig, Konflikte, die sich aus verfassungsrechtlichen und spezialgesetzlichen Regelungen ergeben, zu lösen. Wenngleich der Bereich der Videosicherheit am Arbeitsplatz bereits durch Rechtsprechung des Bundesarbeitsgerichtes (BAG) „ausgeurteilt“ wurde, so zeigen sich aktuell noch erhebliche Regelungslücken und Probleme hinsichtlich des rechtssicheren Einsatzes von Videotechnik im öffentlichen und halböffentlichen Raum.

Um die Problemstellung zu strukturieren und Lösungsmöglichkeiten herauszuarbeiten, behandelt das Whitepaper das Thema anhand dreier Betrachtungsdimensionen und umfassender Aspekte wie rechtliche Rahmenbedingungen und Zertifizierungsaspekte sowie spezifischer Aspekte von zentraler Bedeutung wie die Verbindung von Videotechnik und Cloud-Computing sowie Datenhaltung.

Das Whitepaper richtet sich an **politische Entscheidungsträger und die Wirtschaft** gleichermaßen. Nur ein ganzheitliches Zusammenspiel politischer Rahmenbedingungen und Konkretisierung durch technische Standards können das Ziel der Erhöhung der öffentlichen Sicherheit unter Wahrung der gesetzlich verankerten Rechte der Betroffenen durch einen effektiven und kosteneffizienten Einsatz moderner Videotechnik leisten.

Vorrangig werden die folgenden Zielgruppen adressiert:

- Datenschutz-Aufsichtsbehörden;
- Gesetzgeber (EU, Bund und Länder);
- Nutzer/Betreiber/Beschaffer/Planer bei:
  - der öffentlichen Hand;
  - Sicherheits- und Ordnungsbehörden.

Das Whitepaper zur „sicheren Videotechnik“ richtet sich gleichwohl auch an andere **öffentliche Stellen auf Bundes- und Landesebene**. Beispielsweise kann es erste Impulse geben, wie Videotechnik gestaltet werden kann, sodass es in möglichen zivilrechtlichen, öffentlich-rechtlichen oder strafrechtlichen Verfahren Handhabung gibt, wie Videotechnik im Rahmen von Beweisverfahren einfacher zur Anwendung gelangen kann. Dabei ist insbesondere darauf abzustellen, ob die Videotechnik „sicher“ ist und, ob sie den regulatorischen Vorgaben entspricht.

Darüber hinaus soll das Whitepaper die Akteure im Markt (**Regulierer, Wirtschaft und Aufsichtsbehörden**) über die Normung als Werkzeug zur Erreichung der beschriebenen Zielsetzung informieren.

Wird das hier vorgestellte Whitepaper an **Aufsichtsbehörden für den Datenschutz** adressiert, so soll es insbesondere den Impuls dafür geben, dass diese Normen als Instrument zur Umsetzung europäischer oder (inter-) nationaler Regularien im Bereich des Datenschutzes zu betrachten sind. Daher ist es auch für die Normung unabdingbar, in einem sich schnell ändernden Bereich wie des Datenschutzes, frühzeitig die Aufsichtsbehörden auf Bundes- und Landesebene in die Initiierung des Normungsprozesses einzubinden. Nur so kann es gelingen, dass die zuständigen öffentlichen Stellen für den Einsatz von Normen gewonnen werden können.

Die vorliegende Handreichung richtet sich nicht zuletzt auch an **Nutzer und Betreiber** von Videosystemen. So sollen erste Anknüpfungspunkte gegeben werden zur weiteren Entscheidungsfindung. Hierdurch besteht die Möglichkeit, dass Videotechnik so gestaltet werden kann, dass sich Hersteller und Betreiber an den gleichen Rahmenbedingungen in Bezug auf solche technischen Anlagen orientieren können.

Der Fokus dieses Whitepapers liegt auf der **öffentlichen und halböffentlichen Nutzung** von Videotechnik, da sich die rechtlichen und

technischen Unsicherheiten in diesem Einsatz am umfangreichsten darstellen. Es wird jedoch darauf hingewiesen, dass etliche hier angesprochene Aspekte auch auf Videosicherheit im privaten Sektor übertragen werden können.

Unter öffentlichem Raum sind verschiedene Bereiche zu verstehen. Die offensichtlichsten sind hier öffentliche Plätze und Straßen. Aber auch öffentlich zugängliche Bereiche in Bahnhöfen, Flughäfen, Behörden und Firmen sind diesem gleichzusetzen. Sogar ein Privatparkplatz ist als öffentlicher Raum anzusehen, wenn er nicht mechanisch abgetrennt ist und einfach betreten werden kann.

Damit wird das Konfliktfeld „Erfassung und Verarbeitung personenbezogener Daten“ durch IT-Videotechnik soweit Bestandteil des Whitepapers sein, als es sich um technische und organisatorische Themen zur Einhaltung der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) und deren Normierungsmöglichkeiten handelt. Eine juristische Bewertung ist nicht Bestandteil dieses Whitepapers.

Die Sicherheit von IT-Technologie wird bereits durch verschiedene Regulierungen, Normung und Standards unterstützt. Diese müssen nun auch auf Videotechnik angewendet werden.

Das Whitepaper zeigt anhand der Darstellung vorliegender Konfliktfelder einerseits Handlungsnotwendigkeiten für die Gestaltung der politischen bzw. gesetzlichen Rahmenbedingungen für den Einsatz von Videotechnik im Bereich der zivilen Sicherheit auf und identifiziert andererseits Normungs- und Standardisierungsbedarfe, um den rechtssicheren Einsatz von Videotechnik nach dem heutigen Stand der Technik zu unterstützen.

Dafür wird ein Überblick über vorhandene Regelungen und Standards zusammengestellt, auf deren Basis Handlungsempfehlungen vorgeschlagen werden.

3 Betrachtungsdimensionen der Videotechnologie

3.1 Allgemein

Für eine sichere Videotechnik ist die Berücksichtigung mehrerer Dimensionen wichtig. Diese Dimensionen müssen sowohl bei der Bedarfsanalyse der Beteiligten (Abschnitt 3.2) und der Analyse der rechtlichen und regulatorischen Rahmenbedingungen (Abschnitt 4) berücksichtigt werden.

Eine Dimension stellt die **(Video-)Technologie** dar, die sich aus verschiedenen digitalen Komponenten zusammensetzt. Kameras sind z. B. heute mehr oder weniger intelligente Komponenten, die auch als Sensoren (IoT Device) verstanden werden können. Diese sind mit einem IT-Netzwerk (lokal oder Internet) verbunden. Die erfassten Bilder stehen als digitalisierte Daten in der Kamera zur Verfügung und werden entweder gleich in der Kamera oder in nachgelagerten Softwareapplikationen, die ebenfalls an das IT-Netzwerk angebunden sind, weiterverarbeitet. Das vollständige Videosystem setzt sich ggf. aus verschiedenen Produkten zusammen.

Eine weitere Dimension sind die unterschiedlichen **Beteiligten** vom Hersteller über Planer, Beschaffer, Errichter/Integratoren, Betreiber bis zum Endnutzer. Nicht alle müssen, können aber an einem Videosystem beteiligt sein. Die verschiedenen Akteure sind an der Realisierung von sicherer Videotechnik, zum Teil mit unterschiedlichen Anforderungen beteiligt. Ein Hersteller ist z. B. darangehalten, Security, Safety und Privacy by design für das Produkt oder System zu berücksichtigen sowie Bereitstellung und Aktivierung von sicheren Upgrades und Updates umzusetzen, während ein Betreiber u. a. gefordert ist, die Sicherheit der erfassten, verarbeiteten und gespeicherten Daten zu gewährleisten.

In welcher Intensität die Videotechnik gesichert werden muss hängt dann, als dritte Dimension, vom **Anwendungsfeld** und dessen Sicherheitserfordernissen und Risikobetrachtung ab. Es ist z. B. ein Unterschied, ob die Videotechnik für die Sicherheit eines Bahnhofs oder einer Haftanstalt verwendet wird. Auch der Grad der Automatisierung (Auswertung von Bewegungsdaten oder auch Entscheidungsfähigkeiten) hat Auswirkungen auf die Sicherheit. Neben den bereits geltenden Bedingungen müssen auch hier zusätzlich alle Bedingungen aus der IT-Sicherheit und dem Datenschutz berücksichtigt werden.

In Bild 1 im nächsten Abschnitt ist der Zusammenhang der beschriebenen Dimensionen grafisch für den Lebenszyklus eines Videosystems dargestellt.

3.2 Technologie

Es sind bereits Normen für Technik, Prozesse (Planung, Einbau, Wartung), Systeme und Dienstleistungen veröffentlicht worden, wie z. B. die DIN EN 62676-Reihe. Von besonderer Bedeutung für den Betreiber sind die DIN EN 62676-1-1, DIN EN 6267-1-2 und DIN EN 62676-4 „Anwendungsregeln“, die für die Aufstellung von Betriebsanforderungen, das Verfassen von Spezifikationen, die Auswahl, die Errichtung, die Inbetriebnahme, den Gebrauch und die Instandhaltung von Videosystemen verantwortlich sind.

Um die Komplexität auf technischer Seite zu reduzieren, sollten die Systeme, soweit möglich, automatische Einstellmöglichkeiten bieten. Dies gelingt bei rein technischen Aspekten wie z. B. bei der Bereitstellung von kontrastreichen Bildern oder Anpassung der Kompressionsrate normalerweise recht zufriedenstellend. Auch die Erkennung von bestimmten Anomalien in einer Szene können heute durch Verfahren des maschinellen Lernens durchaus automatisch erkannt werden. Bei Aspekten, die einer unterschiedlichen Bewertung unterliegen, sollten Systeme allerdings eher wie ein Werkzeugkasten gesehen werden, aus dem man bei der Einrichtung die passenden Einstellungen manuell abhängig von bestimmten Bedingungen wählen muss.

3 Betrachtungsdimensionen der Videotechnologie

Betrachtet man die Videotechnologie als Spezialanwendung im IoT-Umfeld wird deutlich, dass ein durchgängiges und hohes Maß an IT-Sicherheit nur mit einem ganzheitlichen Ansatz erreicht werden kann. Mit Einführung von „Edge Cloud-Computing“, als Erweiterung der (zentralen) Cloud werden die „IoT endpoints“, also auch Videosysteme noch stärker in die Cloud-Systeme eingebunden. Aus diesem Grund und um die neue Dimension der Vernetzung und den damit verbundenen erhöhten Sicherheitsrisiken Rechnung zu tragen, müssen die Sicherheitskonzepte für vernetzte Systeme neu überdacht, entwickelt und eingeführt werden.

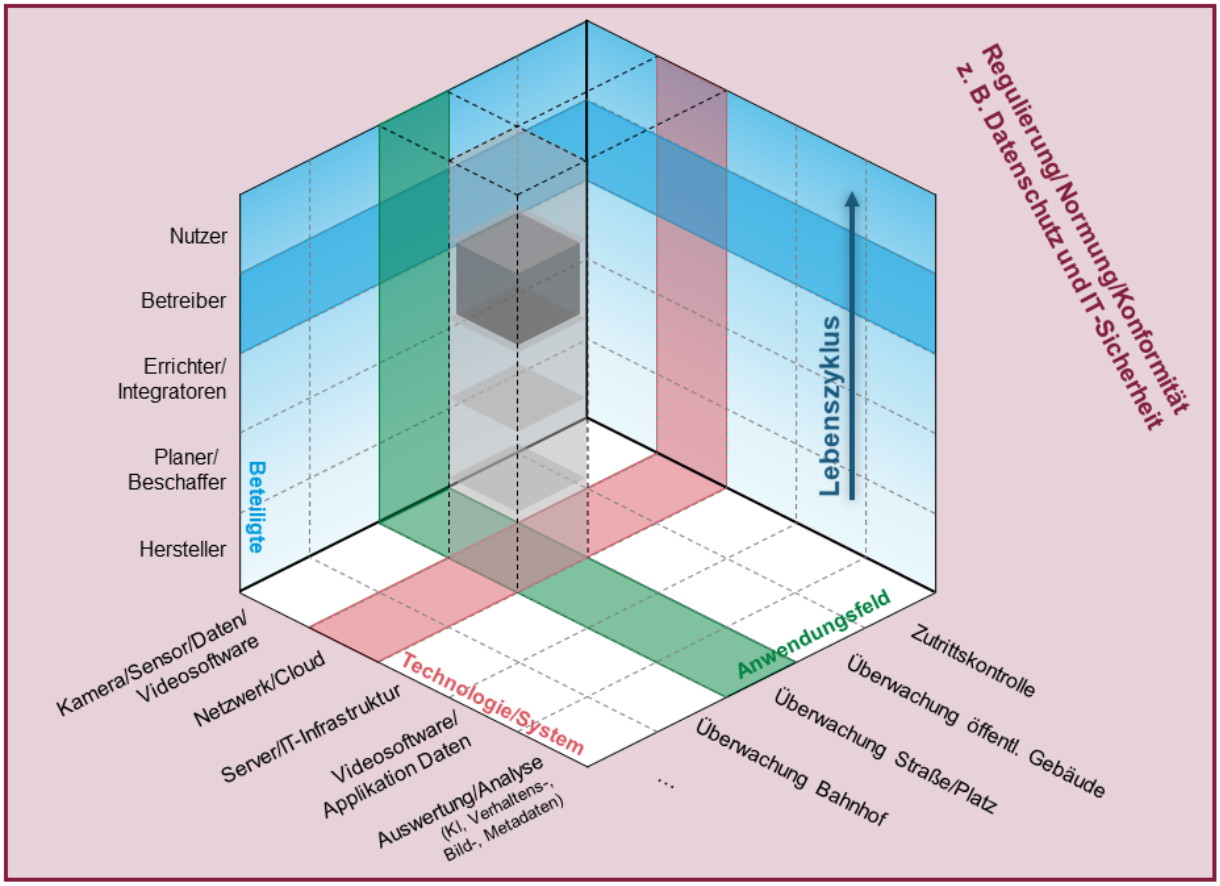

Bild 1 — Betrachtungsdimensionen der Videotechnologie

3.3 Beteiligte/Lebenszyklus

Beim Einsatz von Videotechnik müssen nicht nur Prozesse im Betrieb von Videosystemen beachtet werden, sondern der komplette Lebenszyklus. Je nach Phase im Lebenszyklus stehen andere Beteiligte mit ihren jeweiligen Bedürfnissen und Möglichkeiten im Fokus. Vorgaben zu einem sicheren Betreiben und eine Beschreibung des Lebenszyklus, sind nicht für alle Phasen vorhanden und auch nicht für die damit verbundene IT-Sicherheitsarchitektur.

Neben den im Anhang angeführten Normen/ Richtlinien bestehen heutige Ausschreibungen zumeist aus Angaben eines oder mehrerer Hersteller, die teilweise unschlüssig zusammengeführt sind. Dies führt zumeist:

- zu einem nur von einem Hersteller umsetzbaren System; oder
- zu einem nur unvollständig umsetzbaren System, bei dem die vollständigen Anforderungen von keinem Hersteller ad hoc erfüllt werden können.

Das Problem liegt also darin, dass ein Videosystem zumeist individuell aus Komponenten unterschiedlicher Hersteller zusammengefügt wird (Kameras, Bildübertragung, Bilddarstellung, Videomanagement, Bildanalyse usw.). Durch diese Vielfalt an verwendeten Komponenten entstehen immer wieder andere Schnittstellen, die sich schlecht vereinheitlichen lassen. Des Weiteren unterliegen die Produkte der Videotechnik sehr kurzen Innovationszyklen, was sie von anderen Bereichen der Sicherheitstechnik, insbesondere der Brandmelde- und Einbruchmeldetechnik, deutlich unterscheidet.

Die derzeitige Marktsituation ist geprägt von folgenden Rahmenbedingungen:

- Beschaffern fehlt eine Übersicht zu vorhandenen Regularien und Normen;
- Zertifizierung wird als Vertrauen schaffende Maßnahme angesehen;
- Ende 2018 wurde ein Leitfaden zum Referenzieren von Normen in der öffentlichen Beschaffung veröffentlicht[3];
- Durch den schnellen technischen Fortschritt fehlt vielen Beteiligten der Überblick über die Funktionalität und technische Möglichkeiten der vielen Einzelkomponenten sowie deren Kompatibilität zueinander.

Auf europäischer Ebene wird die Überarbeitung der „public procurement and repealing Directive (2014/24/EU)“ erörtert. Die derzeitige Direktive wird nur bei wenigen Ausschreibungen beachtet. Die Vergabeseite (Nutzer/Betreiber) fordert zertifizierte Produkte und Dienstleistungen von Planern und Herstellern, um die gelieferte Qualität bewerten zu können.

Für Beschaffer und Betreiber ist derzeit kaum vorhersagbar, ob ein System in Bezug auf Datenschutz und Prozesssicherheit abnahmefähig ist und rechtssicher betrieben werden kann.[4] Zum einen durch die Vielzahl an Teilkomponenten als auch dadurch, dass es hierfür derzeit noch keine Grundlage (z. B. Datenschutz-Zertifizierung) gibt.

Beim Datenschutz bzw. Datensicherheit sind grundsätzlich zwei Typen, je nach Schutzzielen, zu berücksichtigen:

1) Personenbezogene Daten (PII, en: Personal Identifyable Information): die personenbezogenen Daten unterliegen den einschlägigen Regulierungen, z. B. DSGVO.

2) Zugriffsschutz auf sonstige Daten (Betriebsgeheimnisse, Patente etc.): die Maßnahmen hierfür sind sicher ähnlich (z. B. Verschlüsselung), aber nicht identisch zu den unter 1 genannten Schutzzielen.

Das Videosystem stellt hierbei nicht das eigentliche Problem für den Betreiber dar, sondern die Bewertung und Verarbeitung der erhobenen Daten.

Öffentliche Stellen beispielsweise, die beabsichtigen den öffentlichen Raum mittels Videotechnik zu sichern, sind verpflichtet entsprechende Anlagen so zu planen, zu errichten und zu betreiben, dass jeder Bürger insbesondere sein verfassungsmäßig garantiertes Recht auf informationelle Selbstbestimmung geschützt sieht. „Kein Eingriff in Grundrechte ohne gesetzliche Grundlage und Rechtfertigung“ – dieser Grundsatz ist in der Bundesrepublik Deutschland von fundamentaler Natur, insbesondere wenn es um den Einsatz von Videotechnik im öffentlichen Raum geht. Dies hat zur Folge, dass Betreiber öffentlicher Videosicherheitsanlagen zahlreiche verfassungsrechtliche und spezialgesetzliche Rahmenbedingungen beachten und befolgen müssen, insbesondere bei Erfassung und Verarbeitung von personenbezogenen Daten. Diese sind durch die DSGVO und das BDSG reguliert sowie ggf. durch weitere branchenspezifische Regulierungen und Standards.

Auch die Entsorgung von Speichermedien der Videotechnik muss datenschutzgerecht gestaltet werden, sodass unbefugte Dritte nicht die Möglichkeit haben auf gespeicherte Videodaten zugreifen zu können. Dies beinhaltet insbesondere nicht nur die Anwendung entsprechender anforderungsgerechter Verfahren, sondern

auch die „sichere“ Vernichtung dahingehend, dass nur diejenigen Dienstleister für Datenträgervernichtungen in Anspruch genommen werden, die eine besondere Eignung und Qualifikation vorweisen können. Diese Handhabe muss insbesondere zur Wahrung von verfassungsrechtlich garantierten Rechten gewahrt werden. Eine entsprechende internationale Norm (ISO/IEC FDIS 21964, Teil 1 bis Teil 3), nach der Daten-Controller und Dienste-Anbieter sich zertifizieren lassen können, um die Zerstörung und Entsorgung von Datenträgern sachgerecht sicherzustellen, wurde 2018 veröffentlicht und kann als Handlungsempfehlung zur Umsetzung herangezogen werden. Diese Internationale Norm ist inhaltsgleich mit der deutschen Normenreihe DIN 66399.

Für die Löschung von personenbezogenen Daten aus den Datenbanken wird empfohlen, ein Löschkonzept zu entwickeln und einzusetzen, das alle Aspekte nach der aktuellen, länderspezifischen Regulierung berücksichtigt.[5] Auch hierzu werden derzeit entsprechende Internationale Standards bei ISO/IEC („Deletion Concept of PII“) diskutiert und werden dem Markt in Kürze zur Verfügung stehen. Im Regelfall ist das Löschkonzept und deren Umsetzung entsprechend anzupassen, um die gesetzeskonforme Umsetzung sicherzustellen.

3.4 Anwendungsfeld

Die zu beachtenden Rahmenbedingungen sind neben den oben genannten Punkten auch abhängig vom Anwendungsfeld der Videotechnik. Dies bringt zusätzliche Unsicherheiten mit sich, da die Komplexität der Planung und des Betriebs durch die unterschiedlichen Regelungen erhöht wird.

Die Anforderungen an die IT-Sicherheit für den Bereich der Videotechnik, die von den Marktteilnehmern zu erfüllen sind, hängen dabei sehr stark von folgenden Punkten ab:

- **Ziel-Markt**
  Öffentlicher Raum;
- **Produktausprägung**
  Stand-alone (onsite/offline), Vernetzt (Cloud, AI) usw.
- **Einsatzszenarien**
  Zum Beispiel Zutrittskontrolle mit Gesichtserkennung, Sicherung von öffentlich zugänglichen Firmengeländen und kritischen Infrastrukturen, Sicherung von öffentlichen Bereichen, Dokumentation von Einsätzen (Body Cams) usw.
- **Einsatzzweck**
  Es lassen sich verschiedene Einsatzgebiete unterscheiden. Zum einen Anlagen für den präventiven Einsatz, bei der eine Echtzeitanalyse durchgeführt wird, um schon im Vorfeld des eigentlichen Schadens sichernde Maßnahmen zu ergreifen. Zum anderen Anlagen zur Nachverfolgung, bei denen Daten auch länger gespeichert werden, um eine forensische Analyse durchführen zu können.

Für die Anwendung von Videotechnik durch Polizeibehörden lassen sich zusätzlich vier Szenarien anhand der landesspezifischen Polizei- und Ordnungsgesetze (Gefahrenabwehrrecht) unterscheiden, die unterschiedliche Anforderungen an die Ausgestaltung der Videotechnik mit sich bringen:

- die Videosicherheit bei öffentlichen Veranstaltungen;
- an gefährdeten Orten;
- bei gefährdeten Objekten; und
- der Einsatz sogenannter „Bodycams“.

3 Betrachtungsdimensionen der Videotechnologie

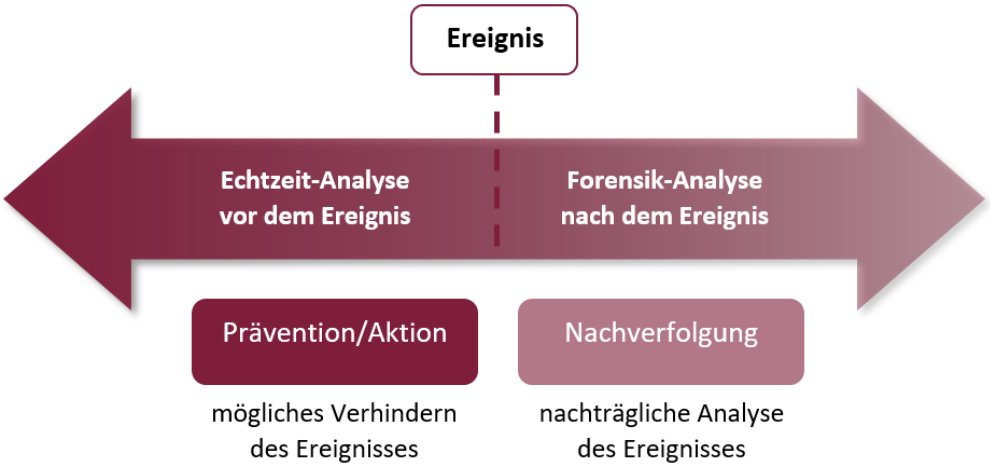

Bild 2 — Ereignis-Prävention vs. Ereignis-Nachverfolgung

4 Rechtliche und regulatorische Rahmenbedingungen für den Einsatz von Videotechnik

4.1 Analyse Ist-Zustand

Basis für eine rechtssichere Nutzung von Videotechnik zur Sicherung des öffentlichen Raumes ist das (bereits oben dargestellte) verfassungsmäßig garantierte Recht auf informationelle Selbstbestimmung.

Die folgende Liste gibt zunächst eine Übersicht über vorhandene gesetzliche Regelungen. Durch die Komplexität des Themenbereiches kann dies keine abschließende Liste sein und es kommen ggf. landesspezifische Gesetzgebungen mit dazu:

1) **National**
   - Grundgesetz als verfassungsrechtliche Grundlage;
   - Spezialgesetzliche Grundlagen, wie
     - Bundesdatenschutzgesetz (BDSG);
     - Telekommunikationsgesetz (TKG);
     - IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) – Version 2.0 wird vsl. Mai 2021 vom Bundesrat beschlossen;
     - Telemediengesetz (TMG) für Internetdienste.

2) **Europäisch**
   - NIS Richtlinie[6]
   - Datenschutz-Grundverordnung[7]
   - EU Cybersecurity Act[8]

Die vorhandenen Regulierungen und Gesetze können dem Tempo der technologischen Entwicklung kaum Schritt halten.

Insbesondere ist auf deutscher und europäischer Ebene auf den Geltungsbereich der DSGVO zu verweisen. Demnach ist die Verarbeitung personenbezogener Daten nur dann gestattet, wenn hierfür ein entsprechender Erlaubnistatbestand im Sinne der Art. 6 und 9 DSGVO einschlägig ist. Die Abwägung, welcher Erlaubnistatbestand im Falle des Einsatzes von Videotechnik einschlägig ist, hängt vom Zweck der Sicherung sowie einer entsprechenden Interessenabwägung ab. Demnach macht es z. B. einen Unterschied, ob ein öffentlicher Platz oder ein Waldweg überwacht werden soll.

Je mehr Daten durch das Videosystem erhoben werden und je mehr Informationen aus den Daten gewonnen werden können, desto mehr gesetzliche und regulatorische Vorgaben sind einzuhalten. Eine festinstallierte Kamera mit geringer Auflösung mit analoger Bildaufzeichnung ist demnach einfacher zu realisieren als ein System mit hochauflösender Kamera, welches mit einer nachgeschalteten Datenanalyse – vielleicht noch unter Einsatz einer KI – weitergehende Informationen gewinnen kann. So sind heutzutage Videosysteme in der Lage, mittels Analyse der aufgezeichneten Daten Personen anhand ihrer Laufbewegung zu identifizieren oder gar das Geschehen im überwachten Bereich zu erkennen. Solche Systeme unterliegen strengeren Auflagen an Datenschutz und Datensicherheit.[9] Je nach Einsatzgebiet und Örtlichkeit folgen möglicherweise weitere Anforderungen an das System oder an die Genehmigungs- oder Verarbeitungsprozesse. Beispielhaft sei hier die Fragestellung, wer das Recht hat die gewonnenen Daten zu nutzen, angesprochen: das Stichwort ist hier das Recht am eigenen Bild. Letztlich ist der Betreiber einer Anlage verantwortlich für die Einhaltung all dieser Aspekte. Da diese aber die ganzen Regeln nicht selbst überblicken und umsetzen können, müssen den Beauftragten Regeln an die Hand gegeben werden, die auch umsetzbar sind und die Konformität dem Betreiber möglichst transparent dargestellt werden kann.

Aus Sicht des geltenden Datenschutzes ist bei der Etablierung von Videotechnik an mehr oder weniger öffentlichen Orten (ebenso jedoch auch auf Firmengeländen) darauf zu achten, in welchem Umfang die Überwachung stattfindet. Vor dem Hintergrund des immer schnelleren technischen Fortschritts ist es problemlos möglich, mittels Videotechnik und entsprechender Software Bewegungsprofile zu erstellen oder besondere Kategorien personenbezogener Daten zu erheben (z. B. bei modernen Videosicherheitsgeräten, die so hochauflösend sind, sodass unter anderem die Marmorierung der Iris [biometrische Daten] problemlos aufgezeichnet werden kann). Normen und

Standards sollten so gewählt werden, dass diese mit regulatorischen Vorgaben einhergehen und dabei nicht nur den technischen Fortschritt im Auge haben.

Aus Sicht der IT-Sicherheit ergibt sich bei der Wahrung von Sicherheitszielen eine besondere Handhabung hinsichtlich Videotechnik. So wird z. B. innerhalb des BSI IT-Grundschutzes die Nutzung von Videotechnik angeraten. Im Baustein INF.2 (Anforderung INF.2.A24) wird darauf verwiesen, dass Videosicherheit konsistent in das gesamte Sicherheitskonzept eingebettet werden sollte. Dies zeigt auf, welchen hohen Stellenwert Videotechnik im Bereich des Schutzes der Integrität von IT-Systemen, so insbesondere bei Rechenzentren von und für öffentliche Stellen, innehat. Durch die fortschreitende Digitalisierung ist davon auszugehen, dass der Schutz von solchen Anlagen stetig zunehmen wird. Gleichwohl – und dies erkennt der IT-Grundschutz ebenso an – sind dabei die Interessen des Schutzes von natürlichen Personen und damit derer personenbezogener Daten hinreichend zu beachten.

Selbst die beste gesetzliche Regelung ist zur Realisierung nur dann geeignet, wenn sie in den vielfältigen Handlungsfeldern der Videotechnik auch umgesetzt werden kann. Ein technisches Mittel in Videosystemen mit automatischer Videoanalyse die Privatsphäre zu schützen ist z. B. die anschließende automatische Verschleierung von erfassten Personen, damit am Bedienplatz beim Betrachten von Live-Videos oder Aufzeichnungen diese nicht mehr erkennbar sind. Aus diesem Grunde empfiehlt es sich ausdrücklich, eine genaue Definition von Einsatzfeldern von Videotechnik herbeizuführen. Dies zielt insbesondere auf die Unterscheidung zwischen präventiver und repressiver Videosicherheit ab. Also auf den Umstand, wie lange die Videodaten zur Auswertung vorgehalten werden. Bei einem präventiven Einsatz beispielsweise kann eine Echtzeit-Überwachung mit kurzen Speicherfristen zum Tragen kommen, wohingegen beim repressiven Einsatz der Technik auch Speicherdauern von mehreren Tagen bis hin zu Wochen erforderlich werden können.

Insbesondere im Bereich des Betriebes von Videosystemen haben Planer, Errichter und Betreiber bei der Konzeption des Sinns und Zwecks der jeweiligen Anlage europäische und nationale Vorschriften hinsichtlich des Schutzes personenbezogener Daten (Stichwort Datenschutz) zu beachten.

In all den Fällen, in denen durch ein Videosystem personenbezogene Daten erhoben und verarbeitet werden (dies ist kraft Natur der Sache immer der Fall) finden so zunächst die harmonisierten „Grundvorschriften“ der DSGVO Anwendung.

Durch die Schwerpunktsetzung auf öffentliche Stellen finden jedoch zusätzlich immer noch die Datenschutzgesetze der Bundesländer Anwendung. Durch teilweise sehr divergierende Regelungen zwischen einzelnen Bundesländern wird es für Errichter und Planer immer schwerer, Planungsansätze, die in einem Bundesland zum Tragen kommen, auf eine Anlage, die in einem anderen Bundesland betrieben werden sollen, zu übertragen. Dies zeigt sich beispielsweise bei der Löschung von Aufnahmedaten aus der Videosicherheit. Nach § 30 Abs. 5 ThürDSG sind diese Daten vom Grundsatz her unverzüglich zu löschen, wohingegen die Regelung zur Videosicherheit in Sachsen-Anhalt in Form des § 8 DSAG LSA diesbezüglich keine Regelung enthält.

Diese Divergenz zwischen den einzelnen Bundesländern setzt sich auch im Bereich der Ausübung der Aufgaben der Aufsichtsbehörden fort. Durch den föderalistischen Gliederungsansatz der Bundesrepublik Deutschland existieren 16 Aufsichtsbehörden der Länder sowie eine Aufsichtsbehörde des Bundes. Durch ihre rechtliche Unabhängigkeit bei der Bewertung datenschutzrechtlicher Sachverhalte entstehen regelmäßig erhebliche Abweichungen zwischen den Ansichten der einzelnen Länder. Dies hat wiederum zur Folge, dass grundsätzliche Abwägungen im Bereich des Datenschutzes von Betreibern von Videosicherheitsanlagen immer konkret auf Basis der jeweils aufgestellten Forderungen von Gesetzgeber und individueller Aufsichtsbehörde beachtet werden müssen.

Die vorgenannten Anmerkungen zeigen, dass auch der Bereich Datenschutz im deutschen Kontext der bekannten „Kleinstaaterei“ entspricht, welcher deutlich erhöhte Arbeitsaufwände für Planer, Errichter und Betreiber zur Folge haben. Aus diesem Grunde erscheint der Grundsatz, einheitliche Regelungen im Bereich des Datenschutzes zum Zwecke der Harmonisierung zu schaffen, wichtiger denn je.

Aufgabe des demokratisch legitimierten Gesetzgebers auf Bundes- und Länderebene muss es daher sein, einheitliche, länderübergreifende Regelungen im Bereich des Datenschutzes hinsichtlich Videotechnik zu treffen, die es allen am Prozess beteiligten Stellen ermöglicht, auf Basis eines einheitlichen normativen Werkes, welches sich auf nationale, europäische oder internationale Normen stützen soll, effizienter und produktiver ihrer jeweiligen Aufgabe nachzukommen.

4.2 Ausblick

Bei der Überarbeitung der Radio Equipment Direktive (RED)[10] ist zu erwarten, dass Cybersecurity Aspekte aufgenommen werden. Damit wären für Kameras, die ihr Bild per Funk übertragen, automatisch Cybersicherheitsanforderungen mandatorisch einzuhalten. Wie diese Anforderungen erfüllt werden können ist noch Gegenstand der Diskussionen; Normungsaufträge der Kommission hierzu werden in der Folge erwartet. Dies ist für den Bereich Videotechnik aufmerksam zu beobachten.

5 Konformitätsbewertung

5.1 Analyse Ist-Zustand

Es ist festzuhalten, dass bereits Zertifizierungsschemata für Technik, Prozesse und Dienstleistungen existieren, ein (einheitliches) Zertifizierungsschema nach der DSGVO gibt es jedoch noch nicht.

Die unter Experten diskutierte Frage, ob eine Produktzertifizierung und eine Zertifizierung nach der DSGVO als europäische Rechtsnorm kombiniert werden können, führt schlussendlich zu folgendem Ergebnis, wobei hauptsächlich zwischen zwei Zertifizierungsgegenständen unterschieden wird:

- Produktzertifizierung[11]; und
- die Zertifizierung von Organisationen/ Prozessen.[12]

Eine Produktzertifizierung im technisch-digitalen Bereich zielt auf Cybersecurity, also Informationssicherheit im weiten Sinne, eines endgültigen Produktes ab, wohingegen eine Zertifizierung nach Art. 42 DSGVO den Datenschutz, also den Schutz personenbezogener Daten als eigenständiges Schutzziel anstrebt. Dies hat zur Folge, dass beide Zertifizierungen verschiedene Schwerpunkte setzen.

Es zeigt sich gleichwohl noch ein weiteres Problemfeld auf. Wird z. B. ein Videosystem mit zahlreichen Komponenten errichtet, von denen nur wenige eine Produktzertifizierung aufweisen, so lässt sich aufgrund dieser einzelnen Zertifikate kein Rückschluss darauf ziehen, ob das Gesamtsystem auch zertifiziert bzw. überhaupt zertifizierbar ist. Selbst bei einer Anlage, bei der alle Produkte zertifiziert sind, ist nicht direkt ableitbar, ob das gesamte System auch entsprechende Anforderungen erfüllen würde, wenn Produkte verschiedener Anbieter und verschiedener Anwendungsbereiche zusammen eingesetzt werden.

Es stellt sich daher die Frage, unter welchen Voraussetzungen an die bereits bestehenden Zertifizierungsprogramme angeknüpft werden kann. Aktuell sind insbesondere die Nachfolgenden genutzt:

- Informationssicherheitsmanagement nach ISO/IEC 27001;
- Privacy Information Management nach ISO/IEC 27701 (nur in Verbindung mit ISO/IEC 27001);
- Informationssicherheitsmanagement nach BSI IT-Grundschutz (in Verbindung mit dem Standard-Datenschutzmodell oder der ISO/IEC 27001);
- Rahmenwerk für Datenschutz (E DIN EN ISO/IEC 29100:2020-03);
- Qualitätsmanagement nach ISO 9001;
- Servicemanagement nach ISO 20000.

Auf Grundlage des bereits seit Juni 2019 in Kraft getretenen Cybersecurity Acts der Europäischen Union scheint nunmehr die Grundlage geschaffen worden zu sein, auch für sichere Videotechnik Rahmenbedingungen zu schaffen. Dies folgt nicht zuletzt vor dem Hintergrund, dass eine verpflichtende Zertifizierung von IKT-Produkten und ITK-Systemen, zu denen bekanntermaßen auch Videosysteme zugehörig sind, nicht unwahrscheinlich sein wird. Fraglich ist jedoch, welche Nachweise ein Antragsteller bei einer verpflichtenden Zertifizierung erbringen muss. Grundsätzlich wird hier zwar auf den Einsatzzweck der Videotechnik abzustellen sein, grundlegend werden jedoch Rahmenbedingungen für jede Anlage gelten müssen.

Videokameras werden als Produkt in Systemen eingebaut und in Kombination mit verschiedenen weiteren Techniken eingesetzt. Eine reine Zertifizierung des einzelnen Bauteils gibt keine Aussage über die Funktionsfähigkeit und Sicherheit des gesamten Systems. Eine Betrachtung der Einzelkomponenten im System, inklusive Einbau, Wartung und Instandhaltung führt von der klassischen Produktzertifizierung zur Systemzertifizierung inklusive Personenzertifizierung über den gesamten Lebenszyklus. Hier können z. B. zertifizierte Planer und Errichter Vertrauen schaffen.

Ein Videosystem im Betrieb unterliegt Veränderungsprozessen, z. B. Ausbau und Integration neuer Komponenten. Dieses

Wachsen der Anlage kann nicht mit einer Einzelabnahme zum Zeitpunkt der Installation abgedeckt werden. Vielmehr ist hier ein Änderungsmanagement über den Lebenszeitraum erforderlich.

Neben den gesetzlich vorgeschriebenen und etablierten Zertifikaten für die Produktzulassungen (CE-Kennzeichen usw.), auf die in diesem Dokument nicht weiter eingegangen wird, bieten die internationalen, europäischen sowie nationalen Normen und die dazugehörigen Konformitätsnachweise eine wichtige technische Orientierung zur Planung und dem Betrieb von Videosystemen.

5.2 Ausblick

Die Formulierung der Anforderungen an IT-Sicherheit/Cybersecurity und Datenschutz für den Einsatz der Videosicherheit muss in einem logischen Zusammenhang mit der seit Juni 2019 geltenden europäischen Gesetzgebung zur IT-Sicherheit, dem EU Cybersecurity Act (EU CSA), gesehen werden.

Im Zuge der Umsetzung des EU CSA fordert die deutsche Wirtschaft eine europäische horizontale Cybersicherheitsregulierung, die den EU CSA mit dem Ansatz des „Neuen Rechtsrahmen“ (New Legislative Framework, NLF) zusammenführt[13]. Mit dem EU CSA wurde der zuständigen Behörde ENISA[14] ein ständiges Mandat zur Erstellung und Einführung eines „EU Certification Frameworks“ erteilt. ENISA hat damit begonnen, an Sektor spezifischen Schemata zur Zertifizierung zu arbeiten.

Die geplanten Schemata zur Zertifizierung für die Bereiche IoT, Cloud sowie Common Criteria könnten dabei je nach den oben angeführten Anwendungsszenarien auch eine Relevanz für die Videosicherheit haben. Abzuwarten ist, ob in Zukunft auch ein dediziertes Zertifizierungsschema für Videosicherheit/-technik entwickelt und veröffentlicht wird.

6 Handlungsempfehlungen

6.1 bezüglich der gesetzlichen und regulatorischen Rahmenbedingungen

6.1.1 Um einen sicheren Einsatz von Videotechnik zur Bewachung des öffentlichen Raumes zu gewährleisten wird es erforderlich sein, Normen und Standards einheitlich festzulegen. Insbesondere bei der Etablierung einheitlicher Regelungen muss der Gesetzgeber hinsichtlich klarer Vorgaben aktiv werden. Die beim Bund angesiedelten Aufsichtsbehörden sollen dabei frühzeitig dahingehend einbezogen werden, dass sie aufgrund ihrer Erfahrungen im Bereich Videotechnik mögliche Problemfelder aufzeigen und bei der Erarbeitung von Lösungen unterstützen.

6.1.2 Die NIS-Direktive wird derzeit überarbeitet. Hier sollten sich die Interessierten Kreise aktiv einbringen, um die Anforderungen der Videotechnik dort einfließen zu lassen. Über die Normung können Unternehmen frühzeitig (auch auf europäischer Ebene) Impulse liefern, auf denen die Gesetzgebung zum Datenschutz aufbauen kann. Besonders sind hier Zertifizierungsprogramme genannt, deren Grundlagen durch Normung und Standardisierung gelegt werden.

6.1.3 Bei der Erarbeitung, Veröffentlichung und Realisierung neuer Regelungen sollen insbesondere den technologieorientierten öffentlichen Stellen des Bundes Aufgaben hinsichtlich der Erarbeitung von Standards in folgenden Bereichen zukommen:

- Verbindliche Anforderungen zur Einhaltung von bestehenden Regelungen inklusive Normen;
- Verlässlichkeit für Planung, Errichtung, Betrieb und Rückbau, Genehmigungsbehörden und Anwender;
- Verlässlich vertrauenswürdige Lieferkette;
- Technologieoffenheit für Zukunft (u. a. KI);
- Transparenz für alle Beteiligten;
- Abnahmetests, Zertifizierungen (dokumentierte Abnahme durch Errichter);
- Prozessbeschreibung „sicherer Betrieb des Videosystems“ (Übergabe vom Errichter an Betreiber).

6.1.4 Datenschutz- bzw. Aufsichtsbehörden auf Bundes- und Landesebene sollten frühzeitig in die Initiierung und Erarbeitung von Normungsvorhaben/-prozessen mit eingebunden werden. Die Mitarbeit von Aufsichtsbehörden an Normungsvorhaben ersetzt allerdings nicht deren Anerkennung, hilft aber dabei Normen frühzeitig zur Anerkennungsreife zu bringen.

6.1.5 Die Anerkennung von Normen und Standards zur Umsetzung des Datenschutzes durch Verweise in Gesetzen und Verordnungen, bzw. in EU-Richtlinien und EU-Verordnungen (da der Datenschutz europäisch verankert ist), sollte stärker genutzt werden, um Rechtssicherheit und Vertrauen bei den Beteiligten zu schaffen.

6.1.6 Insbesondere, wenn es darum geht, den öffentlichen Raum mit Videotechnik auszustatten, wird es erforderlich sein, dass alle Hersteller und Errichter die gleichen Standards verwenden. Aus diesem Grunde wird sich als probates Mittel sicherlich empfehlen, ausdrücklich in öffentlichen Ausschreibungen entsprechender Aufträge (gleich welcher Vergabeform) auf die einzuhaltenden Normen hinzuweisen. Empfehlenswert wäre auch, um einen möglichst großen Teilnehmerwettbewerb eröffnen zu können, eine frei zugängliche Veröffentlichung der Standards über das DIN oder über eine entsprechende Plattform. Eine entsprechende Plattform müsste durch die interessierten Kreise oder die öffentliche Hand finanziert werden.

6.1.7 Bei der Beschaffung und Einrichtung von Videotechnik muss entschieden werden, ob die Sicherheit durch „Security by design“ und/oder „Security by default“ erreicht werden kann bzw. soll. Diese beiden Ansätze schließen sich nicht unbedingt gegenseitig aus.

6.1.8 Es wird empfohlen, die gesamte internationale Normenfamilie IEC 62676 als europäische Norm zu übernehmen und sie somit auch als nationale DIN-Norm zu übernehmen. Außerdem wäre eine Vereinheitlichung von Applikationsvorschriften, die heute weitgehend national oder durch Nutzer-Vorgaben geregelt werden, wünschenswert. Hierbei ist aber zu beachten, dass Funktionsanforderungen je Anwendung unterschiedlich sind (z. B. das Identifizieren, Erkennen oder Beobachten sind unterschiedliche Anforderungen). Die unterschiedlichen gestellten Anforderungen von Datenschutzbeauftragten, Errichtern und Datensicherheits-beauftragten müssen alle beachtet und in Einklang gebracht werden.

6.1.9 Beim Einsatz von Videotechnik müssen nicht nur Prozesse im Betrieb von Videosystemen betrachtet werden, sondern der komplette Lebenszyklus. Vorgaben zu einem sicheren Betreiben und eine Beschreibung des Lebenszyklus, sind nicht für alle Phasen vorhanden und auch nicht für die damit verbundene IT-Sicherheitsarchitektur.

6.1.10 Den Akteuren (Betreiber, Errichter usw.) von Videosystemen sollten Regeln an die Hand gegeben werden, die auch umsetzbar sind und die Konformität möglichst transparent darstellen.

6.1.11 Die Vielfältigkeit des Föderalismus beim Datenschutz macht es notwendig, einheitliche Grundsätze und Regelungen zu erarbeiten, um der Wirtschaft eine klare Hilfestellung zu geben; dies ist wichtiger denn je. Ebenso muss das Standard-Datenschutz-Modell vereinheitlicht angewandt und auch europäisch bzw. international verwendbar gemacht werden.

6.2 für die Normung und Standardisierung

6.2.1 Eine Datenbank mit anzuwendenden Normen, Standards und Vorschriften sollte verfügbar sein und ständig aktuell gehalten werden. Dies dient allen, vom Hersteller bis zum Nutzer, und kann ein durchgängiges Verständnis über die zu berücksichtigenden Anforderungen bieten. Eine solche Liste ließe sich priorisieren z. B. nach folgenden Punkten:

- Herstellung von Rechtssicherheit für die Anforderungen zur Einhaltung der DSGVO, der technischen Abnahmefähigkeit und zur Einhaltung während des Lebenszyklus bzw. Betriebes;
- Technische Fähigkeit vs. systemtechnische Sicherheit;
- Was benötigt man als Hersteller, Planer usw. unbedingt?;
- Security-Management der Gesamtsysteme für den Betrieb.

6.2.2 Gerade Planer und Betreiber von Anlagen benötigen ein durchgängiges Verständnis für vorhandene technische und gesetzliche Anforderungen. Der Planer agiert häufig als Berater des Beschaffers und benötigt einen Leitfaden, mit Hilfe dessen er sich schnell und zielgerichtet einen Überblick über technische (z. B. Normen) und gesetzliche Anforderungen für sein geplantes System/die zu beschaffende Technik erhalten kann.

6.2.3 Die größten Hürden bzgl. der gesetzlichen Vorgaben mit weitreichenden Konsequenzen bei Nichteinhaltung sind durch die DSGVO gegeben. Hier empfiehlt es sich bedarfsgerechte Lösungen zu entwickeln, die durch eine entsprechende rechtliche Bewertung und der Einführung eines umfänglichen Datenschutzkonzeptes abgerundet werden. Hierbei sind die

jeweiligen branchenspezifischen Anforderungen zu berücksichtigen, die über die reine DSGVO hinausgehen: Stichwort Löschkonzepte für Daten. Was internationale Normen angeht, ist hier insbesondere die neue Norm ISO/IEC 27701 zu erwähnen. Sie stellt eine Ergänzung zur bestehenden ISO/IEC 27001 dar und deckt den Bereich des sog. Privacy Information Management System ab (PIMS). Der Standard deckt den Data Privacy Bereich übergeordnet ab und ist für den Regelbetrieb ausgelegt. Er ist nicht vollständig dazu geeignet, um explizit die Konformität mit bestehenden Gesetzten (DSGVO) zu überprüfen, sondern betrachtet die notwendigen Prozesse, um ein PIMS zu organisieren bzw. zu implementieren. Die DSGVO erwartet aus Art. 42/43 eine Produktzertifizierung, wobei ISO 27001/ISO 27701 nur als Managementsystem zertifiziert werden kann. Dieses Thema muss noch aufgelöst werden. Weitere Normen, die z. B. das Thema „Privacy by Design“ abdecken, sind derzeit bei CEN/CENELEC in Arbeit, z. B. EN 17592.

6.2.4 Es wird empfohlen ein modulares Zertifizierungsschema/-modell zu entwickeln, das die Zertifizierung vereinheitlicht und einfacher macht. Als Ansatz könnte Bild 1 dienen mit den Feldern „Technik“, „Beteiligte“ und „Anwendungsfeld“.

6.2.5 Beschaffer sehen sich bei Ausschreibungen bestimmten Herausforderungen gegenüber wie z. B. die einfache Umsetzbarkeit der Anforderungen bei gleichzeitig bestehender Schwierigkeit der schriftlichen Darstellung der Anforderungen. Grundlagen/Normen/ Richtlinien haben hierbei Vor- und Nachteile, da sie einerseits Erleichterungen bringen können (Musterausschreibung), aber gleichzeitig auch die Individualität der einzelnen Anforderungen einschränken können. Es muss also die Frage beantwortet werden, welche Festlegungen einem Planer helfen können rechtssichere Konzepte/Angebote zu erstellen.

Wichtige Punkte für die Beschaffung von Videotechnik ist die Feststellung der Konformität mit den gängigen Gesetzen im EU Raum, die für den Marktzugang von Produkten relevant sind, wie z. B. die Product Safety Directive (PSD) sowie die Radio Equipment Directive (RED), falls es sich um funkgestützte Systeme handelt.

6.2.6 In einem Whitepaper hat der BDEW[15] für Energieversorger grundsätzliche Sicherheitsanforderungen und Umsetzungshinweise und für Steuerungs- und Telekommunikationssysteme zusammengestellt. Es werden Sicherheitsanforderungen für Einzelkomponenten, für Gesamtsysteme aus zusammengesetzten Komponenten und Anwendungen als auch an Wartungsprozesse, Projektorganisation und Entwicklungsprozesse vorgestellt. Dabei wird für jede Anforderung auf die Normen ISO/IEC 27001 und ISO/IEC 27019 und deren Unterpunkte hingewiesen. Für die organisatorischen Maßnahmen, ein geeignetes Sicherheits-, Risiko- und Awareness-management, wird auf die oben genannten Normen verwiesen. Das Papier könnte als eine Quelle oder als Vorlagenbeispiel für mögliche Sicherheitsanforderungen an Videosysteme herangezogen werden.

6.2.7 Wünschenswert wäre ebenfalls ein Engagement zu diesem Thema der relevanten Verbände in Zusammenarbeit mit dem DIN e. V.

6.3 bei Beschaffern, Planern, Herstellern und Dienstleistern

6.3.1 Die Sicherheitsarchitektur von Systemen muss nachweisbar sein, sowohl durch Transparenz in der Lieferkette als auch mit Hinblick auf Haftungsaspekte. Hier kann eine Zertifizierung auf Basis des Standes der Technik Vertrauen schaffen.

6.3.2 Die Einhaltung von bestehenden Normen für Managementsysteme von Informationstechnik (ISMS = Information Security Management System), z. B. ISO/IEC 27001 und ähnliche, kann dafür sorgen ein Mindestmaß an Vertrauen zu schaffen und ein ausreichendes Sicherheitsniveau zu erreichen. Dies gilt insbesondere für den Regelbetrieb solcher Anlagen.

6.3.3 Alle Beteiligte wie Beschaffer, Planer, Hersteller und Dienstleister müssen sich aktiv in der Normung und Standardisierung beteiligen, sodass sie mithelfen können, die Anforderungen zu gestalten, die notwendig und leistbar sind.

6.4 für die Konformitätsbewertung

6.4.1 Für Konformitätsbewertung im Bereich IT-Sicherheit und Cybersecurity stehen den Marktteilnehmern verschiedene Möglichkeiten zur Verfügung. Für alle Verfahren ist der Verweis auf internationale Normen essentiell. Eine Konformitätserklärung nach einem „Self-Assessment“ mit etablierten Normen als Grundlage der Prüfung bildet hier den Einstieg für die Konformitätsüberprüfung.

6.4.2 Zertifizierungen im engeren Sinne können durch akkreditierte Stellen vorgenommen werden. Ein Self-Assessment bzw. Audit sollte ebenfalls möglich sein. Auch hier dienen internationale Nomen als Grundlage zur Prüfung. (Für die Überprüfung der DSGVO-Konformität sind die Normen und Zertifizierungsprogramme noch in Arbeit.)

6.4.3 Im Kontext von Cloud Dienstleistungen kann hier auf Code of Conducts (COC), wie zum Beispiel den EU Cloud Code of Conduct, hingewiesen werden.[16] Neben dem EU Cloud COC gibt es auch weitere Methoden, die schon angewendet werden wie z. B. das CSA STAR Programm.[17]

6.4.4 Zukünftige Videosysteme könnten so gestaltet werden, dass sie über sich selbst Auskunft geben. Im Arbeitskreis Qualitätsinfrastruktur Digital (QI Digital)[18] wird derzeit untersucht, wie ein automatisiertes Monitoring bzw. Zertifizierung ermöglicht werden könnte. Dies ließe sich eventuell auch auf Videotechnik erweitern. Dies wäre wünschenswert, da Systeme immer komplexer werden und eine Zertifizierung auf diesem Wege beschleunigt werden könnte.

6.4.5 Um sichere Produktlebenszyklen (Patches, Wartung) gewährleisten zu können, sollten Hersteller durch Standards unterstützt werden.

6.4.6 Für Errichter und Betreiber sollten Security-Härtungsvorgaben der Hersteller und Vorgaben für eine sichere Integration in bestehende Systeme oder zur Errichtung neuer Systeme mit Hinweis auf die unbedingte Befolgung vorhanden sein.

6.4.7 Nach der Errichtung sollte die Abnahme nach einem Katalog bzw. Standard erfolgen, der Aspekte der Informationssicherheit (Schwachstellentest, Stresstest, Penetration-Test usw.) sowie des Datenschutzes abdeckt.

6.4.8 Der Betreiber sollte regelmäßig die Systeme auf Sicherheit testen und ein sicheres Änderungsverfahren sowie datenschutzkonforme Entsorgung gewährleisten.

6.4.9 Um eine hohe Transparenz zu gewährleisten, sollte erarbeitet werden, welche Maßnahmen zu ergreifen sind, um die DSGVO zu erfüllen, da es hier noch immer große Unsicherheiten gibt.

A Veröffentlichungen zum Thema Videotechnik

Die folgende Liste gibt eine Übersicht über veröffentlichte Dokumente, die zumindest in Teilaspekten das Thema „Sichere Videotechnik“ beinhalten. Durch die Komplexität des Themenbereiches kann dies keine abschließende Liste sein. Es wurde keine Gewichtung in Bezug auf die Bedeutung des gelisteten Dokuments für Sichere Videotechnik vorgenommen.

Bezeichnung	Titel
CWA 17147	Guidelines for the evaluation of installed security systems, based on the STEFi dimensions
DGUV Information 215-612	Kredit- und Finanzdienstleistungsinstitute — Anforderungen an die sicherheitstechnische Ausrüstung von Geschäftsstellen
DGUV Information 215-613	Kredit- und Finanzdienstleistungsinstitute — Betrieb
DIN 33450	Graphisches Symbol zum Hinweis auf Beobachtung mit optisch-elektronischen Einrichtungen (Video-Infozeichen)
DIN CEN/TS 14383-4	Vorbeugende Kriminalitätsbekämpfung — Stadt- und Gebäudeplanung — Teil 4: Laden und Bürogebäude; Deutsche Fassung CEN/TS 14383-4:2006
DIN CEN/TS 16850, DIN SPEC 14001	Schutz und Sicherheit der Bürger — Leitfaden für das Sicherungsmanagement in Gesundheitseinrichtungen
DIN EN 13149	Öffentlicher Verkehr — Planungs- und Steuerungssysteme für Straßenfahrzeuge — Teil 1: WORLDFIP Definitions- und Anwendungsrichtlinien für bordeigene Datenübertragung
DIN EN 13200-7	Zuschaueranlagen — Teil 7: Eingangs- und Ausgangsanlagen und Wege
DIN EN 16334	Bahnanwendungen — Fahrgastalarmsystem — Systemanforderungen
DIN EN 16763	Dienstleistungen für Sicherheitsanlagen
DIN EN 50130, VDE 0830-1	Alarmanlagen — Leitfaden für Einrichtungen von Alarmanlagen zur Erreichung der Übereinstimmung mit EG-Richtlinien. Normenreihe für folgende Produktfamilien: • Brandmeldeanlagen; • Einbruch- und Überfallmeldeanlagen; • Video-Überwachungsanlagen; • Zutrittskontrollanlagen; • Personen-Hilferufanlagen.
DIN EN 50131, VDE 830-2	Alarmanlagen — Einbruch- und Überfallmeldeanlagen Normenreihe
DIN EN 50132-5-3, VDE 0830-7-5-3	Alarmanlagen — CCTV-Überwachungsanlagen für Sicherungsanwendungen — Teil 5-3: Videoübertragung — Analoge und digitale Videoübertragung
DIN EN 50134, VDE 0830-4	Alarmanlagen — Personen-Hilferufanlagen Normenreihe
DIN EN 50136, VDE 0830-5	Alarmanlagen — Alarmübertragungsanlagen und –einrichtungen Normenreihe

A Veröffentlichungen zum Thema Videotechnik

Bezeichnung	Titel
DIN EN 50398-1, VDE 0830-6-1	Alarmanlagen — Kombinierte und integrierte Alarmanlagen — Teil 1: Allgemeine Anforderungen
DIN EN 50486	Einrichtungen für Audio- und Video-Hauskommunikationssysteme
DIN EN 50518, VDE 0830-5-6	Alarmempfangsstellen (AES) Normenreihe
DIN EN 50600-2-5, VDE 0801-600-2-5	Informationstechnik — Einrichtungen und Infrastrukturen von Rechenzentren — Teil 2-5: Sicherungssysteme
DIN EN 62267, VDE 0831-267	Bahnanwendungen — Automatischer städtischer schienengebundener Personennahverkehr (AUGT) — Sicherheitsanforderungen (IEC 62267:2009)
DIN EN 62676, VDE 0830	Videoüberwachungsanlagen für Sicherheitsanwendungen Normenreihe
DIN EN 62841	Digital living network alliance (DLNA) Interoperabilitäts-Leitfäden für Geräte im Heimnetzwerk — Teil 4: Digitale Rechte Management (DRM) Interoperabilitätslösungen
DIN EN 62944	Audio-, Video- und Multimediasysteme und –geräte — Barrierefreiheit des digitalen Fernsehens — Funktionale Festlegungen
DIN EN 63044-1, VDE 0849-44-1	Allgemeine Anforderungen an die elektrische Systemtechnik für Heim und Gebäude (ESHG) und an Systeme der Gebäudeautomation (GA) — Teil 1: Allgemeine Anforderungen (IEC 23/734/CDV:2016)
DIN EN ISO 22311	Sicherheit und Schutz des Gemeinwesens — Videoüberwachung — Datenschnittstellen
DIN SPEC 91282	Terminologie für das Securitymanagement von Verkehrsinfrastrukturen
DIN VDE 0826	Überwachungsanlagen, Normenreihe mit u. a. Gefahrenwarnanlagen, Smart Home
DIN VDE 0833-1, VDE 0833-1	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall Normenreihe
DIN VDE V 0825, VDE V 0825	Überwachungsanlagen — Drahtlose Personen-Notsignal-Anlagen für gefährliche Alleinarbeiten Normenreihe
DIN VDE V 0827, VDE V 0827	Notfall- und Gefahren-Systeme — Notfall- und Gefahren-Reaktions-Systeme (NGRS) Normenreihe
DIN 66399-Reihe	Büro- und Datentechnik — Vernichten von Datenträgern
DIN EN ISO/IEC 15408-1:2020-06	Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell
IEC 62443-2-1 Ed. 1.0	Industrial communication networks — network and system security — Part 2-1: Establishing an industrial automation and control system security program
IEC 62820 Ed. 1.0	General requirements for building intercom systems
IEC 62851	Alarm and electronic security systems – Social alarm systems Normenreihe

A Veröffentlichungen zum Thema Videotechnik

Bezeichnung	Titel
IEC 68039	Alarm and electronic security systems Normenreihe
ISO/IEC 27001	Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen
ISO/IEC 27002	Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen
ISO/IEC 27017	Informationstechnik — Sicherheitsverfahren — Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste
ISO/IEC 27018	Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung
ISO/IEC 27701	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO/IEC 21964	Informationstechnik — Bürogeräte — Vernichten von Datenträgern Normenreihe
ISO/TS 7240	Fire detection and alarm systems Normenreihe
VDI 6004 Blatt 3	Schutz der Technischen Gebäudeausrüstung — Vandalismus und Zerstörung
VDI 6010	Sicherheitstechnische Einrichtungen — Systemübergreifende Funktionen
VdS 2132	VdS-Richtlinien für die Anerkennung von Errichterunternehmen für Feuerlöschanlagen
VdS 2364	VdS-Richtlinien für Videoüberwachungsanlagen — System-anforderungen — Kategorie I
VdS 2365 (Reihe)	VdS-Richtlinien für Videoüberwachungsanlagen — Anforderungen an Videoüberwachungssysteme der Kategorie II Teil 1: Allgemeine Anforderungen; Teil 2: Systemanforderungen und Prüfmethoden; Teil 3: Bilderzeugung Anforderungen an Anlageteile; Teil 4: Bildaufzeichnung Anforderungen an Anlageteile; Teil 5: Bildübertragung.
VdS 2366	VdS-Richtlinien für Videoüberwachungsanlagen — Planung und Einbau
VdS 2465 (Reihe)	VdS-Richtlinien für Gefahrenmeldeanlagen — Übertragungsprotokoll für Gefahrenmeldungen
VdS 3403	VdS-Richtlinien für die Anerkennung von Errichterunternehmen für Gefahrenmeldeanlagen (GMA)
VdS 3426	Installationsattest für eine Videoüberwachungsanlage (VÜA)

A Veröffentlichungen zum Thema Videotechnik

Bezeichnung	Titel
VdS 3455	Praxishandbuch Gefahrenmeldetechnik — Wissenswertes für den Errichteralltag aus den Bereichen Einbruchmeldetechnik, Videoüberwachungstechnik und mechanischer Sicherungstechnik
VdS 3463	VdS-Richtlinien für Gefahrenmeldeanlagen — Anlageteile zur videobasierten Perimeterüberwachung — Anforderungen und Prüfmethoden
VdS 3847	Videokameraeinrichtungen zur visuellen Brandüberwachung — Anforderungen und Prüfmethoden
VdS 4143	Sicherheitsleitfaden Perimeterschutz
VDV 301-2-11	IBIS-IP Beschreibung der Dienste — VideoLiveService
VDV 301-2-12	IBIS-IP Beschreibung der Dienste — VideoRecordingService
VDV 4012	Stand und Trends – Einsatz von Videobildanalyse im ÖPNV-Umfeld
	BDEW Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme
	BHE-Planungsratgeber „Videosicherheit“

[1] www.din.de/go/kits
[2] www.din.de/go.kosi
[3] https://www.din.de/de/din-und-seine-partner/public-affairs/aktuelles/normen-in-der-oeffentlichen-beschaffung-327478
[4] Es gibt Normen für die IT-Sicherheits Management Prozesse (ISO/IEC 27001, ISO/IEC 27002), als auch verschiedene internationale Normen im Bereich Datenschutz (ISO/IEC 27701). Je nach Anwendung müssen weitere Normen herangezogen werden.
[5] DIN 66398. Derzeitig in DIS-Umfrage auf ISO-Ebene als ISO/IEC 27555. Bei CEN/CENELEC gibt es auch ein entsprechendes Arbeitspapier mit Titel: „Video Surveillance“. Anleitung für Sektor spezifische Implementierung.
[6] Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
[7] Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung
[8] Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).
[9] Zum Beispiel Datenschutzfolgenabschätzung.
[10] Richtlinie 2014/53/EU.
[11] Bei Produktzertifizierungen wird die Übereinstimmung mit Anforderungen an das Produkt bestätigt.
[12] Bei Zertifizierungen von Organisationen wird das Vorhandensein und die Einhaltung von Prozessen und Maßnahmen bestätigt (z. B. ISO 9001, ISO 29990).
[13] BDI-DIN-DKE-Positionspapier: https://www.din.de/resource/blob/788010/50c9e8bdb9890fa70935963033a2b34f/2021-bdi-din-dke-position-cybersicherheit-europa-de-final-data.pdf
[14] Agentur der Europäischen Union für Cybersecurity
[15] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, 8. Mai 2018, BDEW Bundesverband der Energie- und Wasserwirtschaft e. V
[16] https://eucoc.cloud/en/about/about-eu-cloud-coc/ (Red. Hinweis: EU Cloud CoC liegt derzeit dem EDPB zur abschließenden Freigabe vor; AUDITOR steht ebenfalls im laufenden Prüfverfahren durch DAkkS in Deutschland).
[17] Cyber Security Alliance; https://cloudsecurityalliance.org/star/

[18] https://www.bundesregierung.de/dmide/vorhaben/arbeits-kreis-qualitaets-infra-struktur-digital-qi-digital--1794052

DIN e. V.
Am DIN-Platz
Burggrafenstr. 6
10787 Berlin
Telefon: +49 30 2601-0

Koordinierungsstelle Sicherheitswirtschaft
Andreas Schleifer
E-Mail: Andreas.Schleifer@din.de
Internet: www.din.de/go/kosi

Koordinierungsstelle IT-Sicherheit
Volker Jacumeit
E-Mail: Volker.Jacumeit@din.de
kits@focusict.de
Internet: www.din.de/go/kits