Dokumente
zu Datenschutz
und Informationsfreiheit
2015

Impressum

Herausgeberin: **Berliner Beauftragte für Datenschutz und Informationsfreiheit**
Friedrichstr. 219, 10969 Berlin
Telefon: 0 30/1 38 89-0
Telefax: 0 30/2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft mbH

Stand: Januar 2016

Inhaltsverzeichnis

Vorwort

Die Zusammenarbeit der Beauftragten für Datenschutz und Informationsfreiheit auf nationaler, europäischer und internationaler Ebene hat 2015 ihren Niederschlag wieder in einer Vielzahl von Entschließungen, Beschlüssen und Arbeitspapieren gefunden, die in diesem Band zusammengefasst sind.

Die Themen reichen vom Datenschutz in Zeiten terroristischer Bedrohung über die europäische Datenschutzreform bis hin zum Datenschutz bei humanitären Hilfsmaßnahmen und tragbaren Endgeräten („Wearables“). Fragen der Transparenz beschäftigten die Datenschutzbeauftragten wie die Beauftragten für die Informationsfreiheit: Transparenzberichte privater Unternehmen über die Zugriffe staatlicher Stellen auf Datenbanken können dazu beitragen, dass diese Stellen stärker rechenschaftspflichtig werden. Der Mangel an Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP) stößt auch bei den deutschen Informationsfreiheitsbeauftragten auf Kritik.

Die in diesem Band zusammengefassten Positionen sowohl in grundsätzlichen Fragen des Datenschutzes wie auch zu neuen technischen Entwicklungen dokumentieren das hohe Maß an Übereinstimmung, das zwischen den Beauftragten für Datenschutz und Informationsfreiheit national wie international herrscht. Diese Übereinstimmung bleibt wichtig, um die künftigen Herausforderungen sowohl in Berlin als auch weltweit bewältigen zu können.

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

A. Dokumente zum Datenschutz

I. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Entschließung vor der 89. Konferenz

Keine Cookies ohne Einwilligung der Internetnutzer (vom 5. Februar 2015)

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann zum Beispiel auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy Richtlinie, Artikel 5 Absatz 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sogenannten Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Artikel 5 Absatz 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend

wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halte diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

2. Entschließungen der 89. Konferenz vom 18./19. März 2015 in Wiesbaden

Datenschutz nach „Charlie Hebdo“: Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.

- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,

- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,

- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und

- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014 – 2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist[1]. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

[1] Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Inso-

fern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o.g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer – und ggf. auch dessen Subunternehmer – den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich – wie Industrie- und Handelskammern berichten – zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Ver-

tragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden (“Predictive Policing“).

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozia-

len Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten – in einem Umfang und auf eine Art und Weise – verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für Den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und

damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

3. Entschließungen nach der 89. Konferenz

Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken (vom 9. Juni 2015)

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die

Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung (vom 14. August 2015)

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 15. Juni 2015 seinen Standpunkt zur Datenschutz-Grundverordnung abgeschlossen hat, beraten Kommission, Parlament und Rat seit Ende Juni im sogenannten Trilog über ihre verschiedenen Positionen zur Datenschutz-Grundverordnung mit dem Ziel einer Gesamteinigung und Verabschiedung des Rechtsaktes zum Jahresende 2015.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012 mehrfach öffentlich zur Datenschutzreform positioniert. Sie hat sowohl zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben als auch in einer Reihe

von Entschließungen und Stellungnahmen zu einzelnen Fragen der Datenschutzreform Position bezogen[1]. Die Konferenz hat von Anfang an das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“[2]. Dies gilt umso mehr, als die Kommission ausdrücklich das Grundrecht des Einzelnen auf Datenschutz in den Mittelpunkt gerückt hat, dem die Reform zugutekommen soll.

Deshalb ist es für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder von außerordentlicher Bedeutung, dass die Datenschutz-Grundverordnung im Vergleich zum geltenden Rechtsstand – der im Wesentlichen durch die Richtlinie 95/46/EG geprägt ist – einen verbesserten, mindestens aber gleichwertigen Grundrechtsschutz gewährleistet. Keinesfalls darf die Reform des Europäischen Datenschutzrechts dazu führen, hinter dem geltenden Datenschutzniveau zurückzubleiben. Die Konferenz betont, dass die sich aus Artikel 8 der Grundrechtecharta und Art. l6 Abs. 1 AEUV ergebenden Grundprinzipien des Datenschutzes daher nicht zur Disposition stehen dürfen. Nach wie vor fehlen spezifische Anforderungen an riskante Datenverarbeitungen, wie z. B. beim Profiling oder bei der Videoüberwachung. Auch sollen Daten für Werbezwecke weiterhin ohne Einwilligung der Betroffenen verarbeitet werden können. Gerade in Zeiten von Big Data und globaler Datenverarbeitung sind die Autonomie des Einzelnen, Transparenz und Rechtmäßigkeit der Datenverarbeitung, die Zweckbindung oder die Verantwortlichkeit des Datenverarbeiters ebenso wichtige Elemente der Grundrechtsgewährleistung wie eine starke Datenschutzaufsicht und wirksame Sanktionen.

Bei den genannten und den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der Datenschutz-Grundverordnung.

---

[1] Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 sowie Stellungnahme vom 11.6.2012; „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012; „Europa muss den Datenschutz stärken“ nebst Erläuterungen vom 13./14.3.2013; „Zur Struktur der Europäischen Datenschutzaufsicht“ vom 27./28.3.2014 sowie „Datenschutz-Grundverordnung darf keine Mogelpackung werden!“ vom 18./19.3.2015, jeweils abrufbar unter http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/DSBund Laender/Functions/DSK_table.html

[2] Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6

II. Die Vorschläge im Einzelnen

1. Der Anwendungsbereich der Datenschutz-Grundverordnung

a. Keine Ausweitung der Haushaltsausnahme!

Der Rat hat die so genannte Haushaltsausnahme in Art. 2(2)(d) Datenschutz-Grundverordnung (DSGVO) in der Weise erweitert, dass er die im Kommissionsvorschlag enthaltenen Worte „ausschließlich“ und „ohne jede Gewinnerzielungsabsicht“ gestrichen hat.

Der Vorschlag des Rates ist in einer Weise formuliert, dass ein maßgeblicher Teil der Verarbeitung personenbezogener Daten durch natürliche Personen auch dann aus dem Anwendungsbereich des Datenschutzrechts herausfiele, wenn in erheblicher Weise in das Datenschutzgrundrecht Dritter eingegriffen würde. Nach der Formulierung des Rates würde es bereits genügen, wenn die Verarbeitung zu persönlichen oder familiären Zwecken bei einer Gesamtbetrachtung lediglich einen völlig untergeordneten Zweck darstellte, um unter die Haushaltsausnahme zu fallen und damit nicht mehr dem Datenschutzrecht zu unterliegen. Ein Nutzer eines sozialen Netzwerks oder der Betreiber einer privaten Homepage würde selbst dann nicht unter das Datenschutzrecht fallen, wenn er in großem Umfang personenbezogene Daten unbeschränkt im Internet veröffentlicht, solange er die Datenverarbeitung (auch) als eine solche zu persönlichen oder familiären Zwecken deklariert. Eine derartige Erweiterung wäre nicht akzeptabel. Ebenso wenig kann die Gewinnerzielungsabsicht ein Kriterium für die Anwendung des Datenschutzrechts sein, da die Eingriffstiefe einer Datenverarbeitung hiervon nicht abhängt. Eine zu weitgehende Ausdehnung der Haushaltsausnahme stünde im Widerspruch zum primärrechtlich garantierten Grundrecht auf Datenschutz und kann deshalb im Sekundärrecht nicht umgesetzt werden.

Die Konferenz spricht sich gegen eine Erweiterung der Haushaltsausnahme in Art. 2(2)(d) DSGVO und die damit verbundene Einschränkung des Anwendungsbereichs des Datenschutzrechts aus. Die Haushaltsausnahme sollte sich daher weiterhin an dem Wortlaut von Art. 2(2) der Richtlinie 95/46/EG orientieren und nur solche Verarbeitungsvorgänge aus dem Anwendungsbereich herausnehmen, die sich ausschließlich auf persönliche und familiäre Tätigkeiten beziehen.

b. Keine weitere Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie!

Die DSGVO wird keine Anwendung finden, soweit die Richtlinie für den Bereich Polizei und Justiz (JI-RL) Anwendung finden wird. Somit bestimmt der Anwen-

dungsbereich der JI-RL zugleich den Anwendungsbereich der DSGVO. Vor diesem Hintergrund hat der Rat in den letzten Monaten verschiedene Entwürfe diskutiert, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-RL führen könnten.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche von DSGVO und der JI-RL wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der KOM enthält die JI-RL Regelungen zum „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung“. Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst ist, soweit sie der Prävention einer Straftat dient. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizeien unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JI-RL – zusammenzufassen, soll der Anwendungsbereich der RL entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die RL zu fassen.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern überhaupt ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-RL für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen zumindest sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Die Datenverarbeitung von anderen Behörden muss weiterhin von der DSGVO geregelt werden, wie es auch der gegenwärtige Rechtsrahmen vorsieht.

Die Konferenz spricht sich gegen die in der Ratsfassung hinzugefügte Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie in Art. 2(2)(e) DSGVO aus. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte von der DSGVO geregelt werden.

2. Für eine klare Definition des Personenbezugs!

Die DSGVO knüpft wie auch das geltende Recht weiterhin am Begriff des personenbezogenen Datums an. Dies ist die logische Konsequenz aus der grundrechtlichen und primärrechtlichen Gewährleistung in Art. 8 Abs. 1 EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV, wonach jede Person das Recht auf Schutz der sie betreffenden Daten hat. Deshalb kommt der Definition des personenbezogenen Datums in Art. 4(1) DSGVO eine außerordentlich hohe Bedeutung zu, denn sie entscheidet letztlich über die Anwendbarkeit des Datenschutzrechts.

Dabei muss klargestellt sein, dass eine natürliche Person auch dann als identifizierbar anzusehen ist, wenn sie innerhalb einer Gruppe von Personen von anderen Personen unterschieden und damit auch unterschiedlich behandelt werden kann. Deshalb muss die Identifizierbarkeit einer Person auch deren Herausgreifen einschließen, wie es dem Vorschlag des Parlaments in EG 23 zugrundeliegt.

Die Vorschläge von Kommission und Rat zu EG 24 führen zudem zu einer unnötig restriktiven Auslegung des Begriffs des personenbezogenen Datums, indem sie Kennnummern, Standortdaten, Online-Kennungen oder IP-Adressen nicht notwendigerweise als personenbezogene Daten ansehen. Für diese Daten gelten die gleichen Kriterien für die Bestimmung des Personenbezugs wie für jede andere Information. Deren gesonderte Erwähnung verleitet zu dem unzulässigen Schluss, dass hier andere Kriterien gelten würden. Dies widerspräche auch der Rechtsprechung des EuGH.

Die Konferenz unterstützt insoweit den Vorschlag des Parlaments zu EG 23, wonach klargestellt ist, dass die Möglichkeit des Herausgreifens einer natürlichen Person aus einer Gruppe ein Mittel zu deren Identifizierbarkeit ist.

Die Konferenz fordert, bei EG 24 dem Vorschlag des Parlaments zu folgen, der klarstellt, dass Kennnummern, Standortdaten, Online-Kennungen, IP-Adressen oder sonstige Elemente grundsätzlich als personenbezogene Daten zu betrachten sind.

3. Datensparsamkeit muss Gestaltungsziel bleiben!

Für eine möglichst grundrechtsschonende Datenverarbeitung ist es unabdingbar, dass sich Staat und Wirtschaft auf das zur Erreichung ihrer rechtlichen oder legitimen Zwecke notwendige Maß beschränken. Die allgegenwärtige Datenverarbeitung und der Einsatz von Big-Data-Technologien erzeugen eine unvorstellbare Menge an (auch personenbezogenen) Daten. Dies führt zu einer für viele als diffus bedrohlich empfundenen Situation, da auf diese Weise Unternehmen oder Behörden potentiell in der Lage sind, über jeden Einzelnen Informationen aus sämtlichen Lebensbereichen zu erfassen und beliebig auszuwerten. Gerade deshalb ist das Prinzip von Datenvermeidung und Datensparsamkeit, das seit vielen Jahren im deutschen Datenschutzrecht verankert ist, wichtiger denn je. Auf diese Weise werden Anreize für eine datenschutzfreundliche Gestaltung von Verarbeitungs- und Geschäftsprozessen geschaffen.

Dies haben die Kommission und das Parlament erfreulicherweise auch erkannt, indem sie das Prinzip der Datensparsamkeit ausdrücklich als eines der Grundprinzipien des Datenschutzes in Art. 5(1)(c) DSGVO verankert haben. Umso

unverständlicher ist es, dass der Rat in seinem Entwurf das Prinzip der Datenvermeidung aus dem Text gestrichen hat – ein fatales Zeichen zugunsten einer noch weiter ausufernden Verarbeitung personenbezogener Daten.

Die Konferenz spricht sich für eine ausdrückliche Verankerung des Prinzips der Datensparsamkeit in Art. 5(1)(c) DSGVO entsprechend der Formulierung der Kommission bzw. des Parlaments aus.

4. Keine Aufweichung der Zweckbindung!

Die Zweckbindung ist seit jeher eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Angesichts der Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Betroffene darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Art. 8 Abs. 2 der Europäischen Grundrechtecharta hat daher die Zweckbindung als tragendes Prinzip des Datenschutzes verankert.

Dementsprechend folgt der Kommissionsentwurf der DSGVO grundsätzlich dem hergebrachten Ansatz der Richtlinie 95/46/EG, indem er in Art. 5(1)(b) zunächst festlegt, dass personenbezogene Daten nur für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

Die Konzeption der geltenden Richtlinie 95/46/EG ist dadurch geprägt, dass sie eine Verarbeitung personenbezogener Daten zu anderen Zwecken nur zulässt, wenn diese neuen Zwecke mit dem Ursprungszweck vereinbar sind. Weitere Zweckänderungen lässt die Richtlinie nicht zu. Auf dieser Basis ist es in der Regel gelungen, einen starken Schutz des Rechts auf informationelle Selbstbestimmung in einen angemessenen Ausgleich mit den öffentlichen Datenverarbeitungsinteressen des Staates und den legitimen Interessen der Unternehmen zu bringen.

Hiervon abweichend hat die Kommission in ihrem Vorschlag zu Art. 6(4) DSGVO zusätzlich die Möglichkeit vorgesehen, dass personenbezogene Daten auch zu solchen Zwecken weiterverarbeitet werden dürfen, die mit dem ursprünglichen Verarbeitungszweck nicht vereinbar sind. Der Rat hat diese Ausnahme noch erweitert, indem er solche Zweckänderungen auch bei einem überwiegenden berechtigten Interesse des Verarbeiters zulassen will. Spätestens durch diese Ergänzungen werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

Das Europäische Parlament ist deshalb zu dem bewährten Ansatz der Richtlinie 95/46/EG zurückgekehrt und hat konsequenterweise Art. 6(4) DSGVO gestrichen. Dies entspricht auch einer frühzeitig erhobenen Forderung der Artikel-29-Gruppe der Europäischen Datenschutzbehörden.

Die Gewährleistung einer starken Zweckbindung ist eine unabdingbare Voraussetzung, um dem Einzelnen ein Höchstmaß an Entscheidungsfreiheit und Transparenz zu ermöglichen. Die Konferenz lehnt deshalb die vom Rat vorgeschlagene Aufweichung der Zweckbindung entschieden ab und spricht sich auf der Basis des Ratsvorschlages für eine Streichung des Art. 6(4) DSGVO aus.

5. Keinen datenschutzrechtlichen Freibrief für Statistik, Archive sowie wissenschaftliche und historische Zwecke!

Die Verarbeitung personenbezogener Daten für die im öffentlichen Interesse tätigen Archive, für die Statistik sowie für historische und für Forschungszwecke folgt aufgrund der jeweiligen Eigenarten der genannten Zweckbestimmungen zum Teil besonderen Regelungen. In allen Fällen geht es darum, die Grundrechte auf Datenschutz und Privatsphäre in einen angemessenen Ausgleich zu bringen mit wichtigen – zum Teil ebenfalls grundrechtlich – geschützten Interessen wie der Forschungsfreiheit oder den öffentlichen Interessen an der amtlichen Statistik bzw. der langzeitlichen Verfügbarmachung staatlicher Informationen durch die Archive. Dies wird grundsätzlich auch durch die Datenschutzbeauftragten des Bundes und der Länder anerkannt. Das geltende Datenschutzrecht hat diesen Ausgleich bisher angemessen hergestellt.

Der Rat geht in seinem Entwurf in verschiedener Hinsicht über diesen Ansatz hinaus und privilegiert die genannten Bereiche in unannehmbarer Weise. Einerseits soll eine Weiterverarbeitung zu den genannten Zwecken gem. Art. 5(1)(b) DSGVO generell immer möglich sein; die Zweckbindung wird insoweit aufgehoben. Andererseits soll Art. 6(2) DSGVO die (Weiter-)Verarbeitung zu den genannten Zwecken ermöglichen, ohne dass es der Rechtsgrundlagen des Art. 6(1) DSGVO bedarf. Dies würde bedeuten, dass eine Verarbeitung zu den genannten Zwecken ohne weitere Rechtsgrundlage – vorbehaltlich mitgliedstaatlicher Sonderbestimmungen in Teilbereichen nach Art. 83 DSGVO – möglich wäre und die Weiterverarbeitung personenbezogener Daten, die ursprünglich zu anderen Zwecken erhoben worden sind, weitgehend schrankenlos möglich wäre.

Hinzu kommt, dass der gegenständliche Anwendungsbereich der Privilegierung zu weit gefasst ist. Einzig für die Archive im öffentlichen Interesse bestehen insofern keine Bedenken, zumal sich zumindest die staatlichen Archive nach Art. 83 DSGVO nach dem meist ausdifferenzierten mitgliedstaatlichen Recht zu richten

haben. Bei der Privilegierung der statistischen Zwecke differenziert der Ratsentwurf hingegen nicht nach solchen der amtlichen Statistik und sonstigen statistischen Zwecken. Während für erstere im Rahmen von Art. 83 DSGVO eine Privilegierung nachvollziehbar ist, besteht im Übrigen die Gefahr, dass etwa die Betreiber von sozialen Netzwerken, Suchmaschinen, Analysetools usw. die von ihnen vorgenommene umfassende Profilbildung als statistische Zwecke deklarieren. Vergleichbare Bedenken bestehen auch gegen die Privilegierung der wissenschaftlichen Datenverarbeitung, die vom Rat nicht auf Zwecke der wissenschaftlichen Forschung beschränkt wird, sondern darüber hinausgeht.

Datenschutzrechtliche Grundsätze gelten auch für die Verarbeitung personenbezogener Daten zu Zwecken der öffentlichen Archive, der Statistik sowie für wissenschaftliche und historische Zwecke. Die Konferenz erwartet im Trilog eine differenzierte und ausgewogene Regelung zum Schutze der genannten Interessen, die die Einschränkungen der Grundrechte auf Datenschutz und Privatsphäre auf das unabdingbar Notwendige beschränkt. Jede Verarbeitung zu den genannten Zwecken bedarf einer Rechtsgrundlage im Sinne von Art. 6(1) DSGVO. Art. 6(2) DSGVO ist insofern missverständlich und sollte daher gestrichen werden. Darüber hinaus sollte – vergleichbar mit den Archiven – nur die amtliche Statistik privilegiert werden. Profilbildungen in sozialen Netzwerken, Suchmaschinen, durch den Einsatz von Analysetools usw. dürfen nicht privilegiert werden.

6. Die Einwilligung muss die Datenhoheit des Einzelnen sichern!

Recht auf informationelle Selbstbestimmung bedeutet seit jeher, dass der Einzelne grundsätzlich selbst über Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden darf. Daraus folgt unmittelbar, dass der Einzelne grundsätzlich autonom darüber bestimmen kann, ob er eine Verarbeitung seiner personenbezogenen Daten erlaubt oder nicht. Die Einwilligung ist ein wesentliches Element, um diese Autonomie wirksam zu sichern. Sie ist deshalb in Art. 8 Abs. 2 der EU-Grundrechtecharta ausdrücklich als Legitimation für die Verarbeitung personenbezogener Daten genannt.

Kommission und Parlament haben sich im Bewusstsein dieser Bedeutung dafür entschieden, dass eine Einwilligung nur dann wirksam sein soll, wenn sie ausdrücklich erfolgt. Nur bei einer ausdrücklichen Willensbekundung kann letztlich der Nachweis erbracht werden, dass sich der Einzelne der Tragweite seiner Entscheidung bewusst wird.

Der Rat verabschiedet sich in seinem Entwurf entgegen der Grundrechtecharta von diesem Grundsatz, indem er bereits eine eindeutige Willensbekundung aus-

reichen lässt. Damit wird es insbesondere den global agierenden Diensteanbietern ermöglicht, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Als datenschutzgerechte Einwilligung kann nur ein opt-in akzeptiert werden.

Es sollte zudem ein Koppelungsverbot ausdrücklich in den verfügenden Teil der DSGVO aufgenommen werden. Während Kommission und Parlament dieses in Artikel 7(4) DSGVO vorsehen, hat es der Rat gestrichen und erwähnt es lediglich in den Erwägungsgründen (EG 34).

Zur wirksamen Gewährleistung des Rechts auf informationelle Selbstbestimmung unterstützt die Konferenz den Ansatz von Kommission und Parlament, dass eine Einwilligung nur dann die Verarbeitung personenbezogener Daten legitimieren kann, wenn sie ausdrücklich abgegeben wird. In Art. 7 DSGVO sollte darüber hinaus ein Koppelungsverbot ausdrücklich geregelt werden.

7. Rechte der Betroffenen

a. Sicherstellung der Unentgeltlichkeit

Die Entwürfe der Kommission und des Parlaments sehen in Art. 12(4) DSGVO vor, dass Unterrichtungen der Betroffenen und *die auf Antrag ergriffenen Maßnahmen* zur Umsetzung der Betroffenenrechte unentgeltlich sind. Der Entwurf des Rates sieht dagegen vor, dass lediglich die Informationen gemäß Art. 14 und 14 a sowie alle *Mitteilungen* gemäß den Artikeln 16 bis 19 und 32 unentgeltlich zur Verfügung gestellt werden. Damit bleibt unklar, ob auch die Umsetzung der Betroffenenrechte selbst unentgeltlich erfolgen muss oder die verantwortlichen Stellen hierfür ggf. eine Gebühr erheben können. Dafür spricht, dass nur das Auskunftsrecht (Art. 15) ausdrückliche Regelungen zur (Un-)Entgeltlichkeit enthält (vgl. Art. 15(1) und (1b)), die übrigen Betroffenenrechte hingegen nicht.

Die Unentgeltlichkeit der Ausübung und Umsetzung der Betroffenenrechte ist unabdingbare Voraussetzung für die effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung. Gebühren für die Ausübung schrecken die Betroffenen regelmäßig von der Wahrnehmung ihrer Rechte ab.

Die Konferenz spricht sich für eine unmissverständliche Regelung aus, dass die Ausübung der Betroffenenrechte und deren Umsetzung durch die verantwortlichen Stellen unentgeltlich erfolgen müssen.

b. Keine Einschränkung der Betroffenenrechte!

Die Information der Betroffenen (Art. 14, 14 a DSGVO) versetzt diese in die Lage, Umfang und Risiko der Datenverarbeitung einzuschätzen. Sie ist die wesentliche Bedingung für die Schaffung von Transparenz. Der Entwurf des Rates sieht lediglich die Unterrichtung über die Identität der verantwortlichen Stelle, die Zwecke der Datenverarbeitung und die Rechtsgrundlage vor. Weitergehende Informationen sollen nur dann erforderlich sein, wenn sie unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.

Die Konferenz lehnt Beschränkungen der Betroffenenrechte ab. Die Formulierungen des Rates führen zu Rechtsunsicherheit und lassen Raum für Interpretationen, die zu einer Absenkung des geltenden Datenschutzniveaus führen.

Die Informationspflichten der Art. 14 und 14 a DSGVO beinhalten im Gegensatz zum Recht auf Auskunft (Art. 15) lediglich allgemeine, abstrakte Informationen über Art, Umfang und Zweck der Datenverarbeitung. Die Informationspflicht führt daher nicht zu exzessiven Bürokratiekosten, weil sie in standardisierter Form gegenüber den Betroffenen erfüllt werden kann. Die vom Europäischen Parlament vorgeschlagenen standardisierten Informationsmaßnahmen unter ergänzender Verwendung von Piktogrammen (Art. 13 a) erachtet die Konferenz für erwägenswert.

Die Konferenz spricht sich gegen Einschränkungen der Betroffenenrechte aus und unterstützt die Position des Europäischen Parlaments.

c. Wirksame Begrenzung der Profilbildung sicherstellen!

Die Datenschutzbeauftragten des Bundes und der Länder sind der Auffassung, dass die bisherigen Vorschläge für eine Regelung von Profilbildungen in Art. 20 DSGVO nicht geeignet sind, um die Bürgerinnen und Bürger im Zeitalter von Big Data, der Allgegenwart des Internets der Dinge und der in alle Lebens-, Privat- und Intimbereiche wie die Gesundheit vordringenden Technologien zur individuellen Datenerfassung und -analyse effektiv vor der Erstellung und Nutzung von Persönlichkeitsprofilen zu schützen.

Die Vorschläge von Kommission, Parlament und Rat zu Art. 20 DSGVO sind unzureichend, da keiner der Vorschläge die Profilbildung an sich besonderen Zulässigkeitsvoraussetzungen unterwirft, sondern erst das Treffen einer „automatisierten Entscheidung“ (Rat) oder einer „Maßnahme“ (KOM) auf Basis des Profilings bzw. „Profiling, das Maßnahmen zur Folge hat, die rechtliche oder ähnlich erhebliche Auswirkungen auf die Interessen der betroffenen Person hat“ (EP).

Unzulänglich ist insbesondere der Vorschlag des Rates, da er das Phänomen des Profilings in Anlehnung an Art. 15 Abs. 1 der EG-Datenschutzrichtlinie 95/46 auf das Treffen automatisierter Entscheidungen mit Rechtswirkung für den Einzelnen reduziert. Geregelt wird damit lediglich eine spezifische Folge der Datenverarbeitung im Zusammenhang mit der Auswertung von Persönlichkeitsmerkmalen, nicht aber die grundlegende Frage, zu welchen Zwecken und innerhalb welcher Grenzen Persönlichkeitsprofile überhaupt erstellt und genutzt werden dürfen. Zudem beinhaltet dieser Ansatz in der Praxis ein erhebliches Interpretations- und Umgehungspotenzial im Hinblick auf Dienste oder Anwendungen, die keine unmittelbaren Rechtswirkungen gegenüber dem Betroffenen entfalten, wie die Analyse des Nutzerverhaltens im Internet, die Analyse persönlicher Vorlieben durch ein soziales Netzwerk, die Analyse von Bewegungsdaten oder die Analyse der Körperaktivität mittels Apps und Sensoren.

Vor diesem Hintergrund plädieren die Datenschutzbeauftragten des Bundes und der Länder für eine differenzierte Regelung der Profilbildung und -nutzung in der DSGVO, die folgende Kernelemente beinhalten sollte:

- Statt der Verkürzung auf automatisierte Einzelfallentscheidungen ist ein Ansatz zu wählen, der sämtliche Profilbildungen oder darauf basierende Maßnahmen erfasst. Diesem Ansatz entspricht am ehesten der vom Europäischen Parlament zu Artikel 20 unterbreitete Regelungsvorschlag.

- Ausnahmen vom Verbot der Profilbildung bedürfen eng begrenzter klarer Erlaubnistatbestände. Wegen ihrer hohen Sensitivität sollte zudem festgelegt werden, dass besondere Kategorien personenbezogener Daten nicht in eine Profilbildung einfließen dürfen.

- In jedem Fall sollte die Verarbeitung personenbezogener Daten zu Zwecken des Profilings stets mit einem Höchstmaß an Transparenz und Informiertheit des Betroffenen einhergehen. Der Einzelne muss wissen, wann, zu welchem Zweck und in welcher Form seine Daten im Internet oder bei der Nutzung eines Dienstes auf einem Endgerät zu Profilingzwecken verarbeitet werden und muss hierzu seine ausdrückliche Einwilligung erteilen.

- Zudem sollte eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und -auswertung verwendeten Daten bestehen, letzteres flankiert von einem Verbot der (Re-)Identifizierung.

In Anbetracht der wiederholt vom EuGH festgestellten Gefahren, die von Persönlichkeitsprofilen für das Grundrecht auf Datenschutz ausgehen, fordert die Konferenz, die vorliegenden Vorschläge für eine Profilingregelung im Sinne der vorgenannten Eckpunkte substanziell zu verbessern.

8. Die datenschutzrechtliche Verantwortlichkeit gilt für jede Verarbeitung personenbezogener Daten!

Die in Kapitel IV, insbesondere in Art. 22 DSGVO geregelte Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Bestimmungen (*Accountability*) gehört zu den zentralen Grundprinzipien eines modernen Datenschutzrechts. Die für die Verarbeitung Verantwortlichen und die Auftragsdatenverarbeiter sind in jedem Falle und ohne Einschränkungen für die Einhaltung des Datenschutzrechts verantwortlich. Dies gilt ungeachtet der Art, des Umfangs, der Umstände und der Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Betroffenen. Ebenso müssen die für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeiter uneingeschränkt in der Lage sein, die Einhaltung ihrer Pflichten nachzuweisen. Risikobasierte Aspekte dürfen lediglich bei der Frage berücksichtigt werden, welche konkreten Maßnahmen zur Einhaltung der Pflichten zu treffen sind.

Es muss daher klargestellt werden, dass sich ein risikobasierter Ansatz nicht auf das „Ob“ und die Nachweisbarkeit, sondern allenfalls auf das „Wie“ der Einhaltung der Pflichten beziehen kann. Dies wird im Vorschlag der Kommission am besten verdeutlicht, in dem auf jede Relativierung verzichtet wird.

Die Konferenz spricht sich für den seitens der Kommission für Art. 22 DSGVO gewählten Ansatz aus, um zu verdeutlichen, dass die Verantwortlichkeit (*„Accountability“*) ein tragendes Grundelement des Datenschutzes ist, das als solches einem risikobasierten Ansatz nicht zugänglich ist.

9. Für die Verankerung von Gewährleistungszielen beim technischen und organisatorischen Datenschutz!

Die Verarbeitung personenbezogener Daten bedarf zum Schutz der Grundrechte nicht nur eines rechtlichen, sondern auch eines technischen und organisatorischen Schutzes. Ein modernes Datenschutzrecht muss hierfür Gewährleistungsziele definieren, an denen sich die zu treffenden Maßnahmen auszurichten haben. Dies bedeutet, dass zu den klassischen Gewährleistungszielen der IT-Sicherheit spezifische Ziele hinzutreten müssen, die sich namentlich auf den Schutz personenbezogener Daten beziehen. Deshalb sind die Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, aber auch Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in der DSGVO zu verankern. Während sich Kommission und Rat in ihren Vorschlägen zu Art. 30(2) bzw. 30(1a) DSGVO im Wesentlichen auf die klassischen Ziele Verfügbarkeit, Integrität und Vertraulichkeit fokussieren, geht der Ansatz des Parlaments in Art. 30(1a) und 30(2) DSGVO i. V. m. Art. 5(1)(ea) und (eb) am weitesten.

Die Konferenz hält eine konsequente, klare und übersichtliche Verankerung der Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in Art. 30 DSGVO für notwendig. Sie unterstützt insoweit die Zielrichtung des Parlaments, spricht sich allerdings für eine übersichtlichere Gestaltung aus.

10. Guter Datenschutz braucht betriebliche und behördliche Datenschutzbeauftragte!

Ungeachtet der materiell-rechtlichen Bestimmungen hängt das konkrete Datenschutzniveau in Behörden und Unternehmen ganz entscheidend davon ab, welche Akzeptanz der Datenschutz vor Ort genießt und wie die Datenschutzkultur ausgeprägt ist. Hierzu können die Aufsichtsbehörden für den Datenschutz Impulse liefern und durch Kontrollen und Beratungen einen entscheidenden Beitrag leisten. Diese Aktivitäten bleiben aber notwendigerweise punktuell und sind aufgrund der unterschiedlichen Rollen nicht immer konfliktfrei. Deshalb kommt der Institution der Datenschutzbeauftragten in Unternehmen und Verwaltungen eine hohe Bedeutung zu.

Es ist deshalb erfreulich, dass sowohl Kommission als auch Parlament in Art. 35 DSGVO die verpflichtende Bestellung interner Datenschutzbeauftragter vorsehen. Allerdings sind die von beiden Institutionen gewählten Kriterien, unter denen eine Bestellung verpflichtend ist, wenig überzeugend.

Bedauerlicherweise hat sich im Rat eine europaweit geltende Verpflichtung zur Bestellung von Datenschutzbeauftragten nicht durchgesetzt. Hierbei wird vor allem mit dem bürokratischen und wirtschaftlichen Aufwand argumentiert. Nach den jahrzehntelangen Erfahrungen in Deutschland überzeugt dieses Argument nicht. Der Compliance-Aufwand für die Unternehmen ist ohne die Einbindung betrieblicher Datenschutzbeauftragter nicht unerheblich; durch deren Einsatz können zudem Sanktionen und Bußgelder oftmals vermieden werden.

Die Konferenz setzt sich nach wie vor dafür ein, dass eine verpflichtende Bestellung betrieblicher und behördlicher Datenschutzbeauftragter europaweit verbindlich vorgeschrieben wird. Während es für Behörden keine Ausnahmen geben sollte, sollten Unternehmen nicht nur ab einer bestimmten Größe oder einer bestimmten Zahl Betroffener einen Datenschutzbeauftragten bestellen, sondern in jedem Falle auch dann, wenn die Datenverarbeitung mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist.

11. Mehr Kontrolle über Datenübermittlungen an Behörden und Gerichte in Drittstaaten!

Seit den Enthüllungen von Edward Snowden wird intensiv über einen besseren Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber Behörden und Stellen aus Drittstaaten diskutiert. Deshalb hat das Parlament einen spezifischen Art. 43 a DSGVO vorgeschlagen. Dieser stellt klar, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt werden noch vollstreckbar sind, wenn dies nicht in internationalen Übereinkommen zur Amts- oder Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten zuständigen Stellen.

Die Konferenz unterstützt diese Forderung ebenso wie die Artikel-29-Gruppe. Mit der Schaffung einer solchen Regelung wird die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Der Rat ist einer entsprechenden Initiative der Bundesregierung bedauerlicherweise nicht gefolgt.

Die Konferenz spricht sich weiterhin dafür aus, eine spezifische Rechtsgrundlage für die Datenübermittlung an Behörden und Gerichte in Drittstaaten zu schaffen, mit der insbesondere im Hinblick auf die nachrichtendienstliche Überwachung mehr Transparenz und Kontrolle geschaffen wird. Sie unterstützt den vom Parlament eingebrachten Vorschlag eines Art. 43a DSGVO.

Die Zuständigkeit sollte jedoch wie folgt geregelt werden: Haben ersuchender und ersuchter Staat ein Rechtshilfeabkommen oder einen ähnlichen internationalen Vertrag geschlossen, sollte die hierin bezeichnete Stelle für die Entgegennahme und Prüfung eines Ersuchens auf Datenübermittlung zuständig sein. In den Fällen, in denen eine zuständige Stelle nicht vertraglich bestimmt worden ist, kann diese Aufgabe nachrangig in die Zuständigkeit der Datenschutzaufsichtsbehörden fallen.

12. Für eine effektive und bürgernahe Zusammenarbeit der Datenschutzbehörden in Europa

Ein entscheidender Fortschritt der Datenschutz-Grundverordnung soll in einer verbesserten Zusammenarbeit der Datenschutzbehörden in Europa liegen. Um

dies zu gewährleisten und auf der anderen Seite den Unternehmen einen Mehrwert zu bieten, hatte die Kommission einen sog. One-Stop-Shop, einen Kohärenzmechanismus und die Einrichtung eines Europäischen Datenschutzausschusses vorgeschlagen.

Auf Vorschlag des Rats soll es eine federführende Datenschutzbehörde geben, die einem Unternehmen am Ort seiner Hauptniederlassung als hauptsächlicher Ansprechpartner zur Verfügung steht, aber auch mit allen anderen – sei es aufgrund weiterer Niederlassungen oder der Betroffenheit ihrer Bürger – betroffenen Aufsichtsbehörden kooperiert. Weiterhin hat der Rat Vorschläge zu einem sog. One-Stop-Shop gemacht, sodass Betroffene sich an die Aufsichtsbehörde und die Gerichte bei ihnen vor Ort wenden können. Um zu verbindlichen Entscheidungen ohne Beteiligung der Kommission zu kommen, schlägt der Rat darüber hinaus vor, den Europäischen Datenschutzausschuss mit verbindlichen Entscheidungsbefugnissen auszustatten. Hierzu ist der Ausschuss mit eigener Rechtspersönlichkeit auszustatten. Das vom Rat vorgeschlagene Modell ist für die Aufsichtsbehörden komplex, soll aber den Bürgerinnen und Bürgern eine ortsnahe Bearbeitung ihrer Anliegen und den Unternehmen einen Ansprechpartner für länderübergreifende Datenverarbeitungen verschaffen.

Die Konferenz unterstützt die Ziele des Ratsvorschlags zum sog. One-Stop-Mechanismus. Der effiziente Vollzug des Datenschutzrechts darf jedoch nicht durch die Untätigkeit der federführenden Datenschutzbehörde unterlaufen werden. Es ist eine Regelung zu schaffen, wonach die mitgliedstaatlichen Aufsichtsbehörden bei Betroffenheit ihrer Bürger von der federführenden Behörde ein aufsichtsbehördliches Einschreiten verlangen können, dessen Ablehnung zu einer unmittelbaren Überprüfung durch den Europäischen Datenschutzausschuss führt.

Der One-Stop-Shop soll einen ausgewogenen Ausgleich zwischen den verschiedenen Interessen schaffen, eine bürgernahe Bearbeitung von Beschwerden ermöglichen, den Unternehmen klare Ansprechpartner zur Verfügung stellen und durch die Aufwertung des Europäischen Datenschutzausschusses die notwendige Verbindlichkeit und damit Rechtssicherheit aufweisen. Die Konferenz bittet die am Trilog beteiligten Parteien gleichwohl, praktikable Verfahrensregeln festzulegen. Dies betrifft insbesondere die Frage der Verfahrensfristen und der Amtshilfe der Aufsichtsbehörden untereinander.

13. Für einen starken Beschäftigtendatenschutz

Die DSGVO überlässt die Regelung des Datenschutzes für Beschäftigte in Artikel 82 dem mitgliedstaatlichen Recht. Der Rat und die Kommission legen fest, dass die Mitgliedstaaten dabei den Rahmen der DSGVO einhalten müssen und

verzichten auf konkretere Anforderungen. Das Europäische Parlament gibt dagegen ganz konkrete Mindeststandards im Verordnungstext vor.

Die Konferenz hält es für wichtig, dass Artikel 82 DSGVO den Mitgliedstaaten in jedem Falle die Möglichkeit eröffnet, auch über den Standard der DSGVO hinausgehen zu können. Die Konferenz begrüßt den Ansatz des Parlaments, konkrete Mindeststandards für den Beschäftigtendatenschutz im Verordnungstext selbst vorzusehen.

Im Kontext der Verarbeitung von Beschäftigtendaten sollte es die Datenschutz-Grundverordnung den Mitgliedstaaten ermöglichen, im Sinne einer Mindestharmonisierung auch über das Datenschutzniveau der Verordnung hinauszugehen. Die Konferenz unterstützt den Ansatz des Parlaments, konkrete Mindeststandards festzulegen.

14. Recht auf pseudonyme Internet-Nutzung für alle Menschen in Europa schaffen!

Es gibt zahlreiche gewichtige Gründe, bei der Nutzung von Telemediendiensten auf ein Pseudonym zurückzugreifen: Dazu gehört etwa der Wunsch, einer Profilbildung unter dem realen Namen zu entgehen, sei es um sich vor rechtswidrigen Zugriffen zu schützen, sei es zur Stärkung des Schutzes bei der Nutzung sozialer Netzwerke. Ein Pseudonym kann ferner vor politischer oder rassistischer Verfolgung oder Diskriminierung und sozialer Benachteiligungen etwa wegen der sexuellen Ausrichtung schützen. Pseudonyme können schließlich verhindern, dass die private Nutzung eines Telemediums zur geschäftlichen Kontaktaufnahme durch Dritte missbraucht wird. Das ist gerade bei Berufsgeheimnisträgern wie Ärzten, Seelsorgern, Anwälten oder Sozialarbeitern nicht zuletzt zum Schutz der mit ihnen in Kontakt stehenden Personen von Bedeutung.

Das Recht, in Telemedien grundsätzlich auch unter einem Pseudonym gegenüber anderen Nutzern aufzutreten, stärkt sowohl die informationelle Selbstbestimmung Betroffener als auch die Meinungsfreiheit, ohne eine Verfolgung und Ahndung von missbräuchlichem Verhalten von unter Pseudonym auftretenden Nutzern durch den Telemedienanbieter auszuschließen. In der Europäischen Datenschutzgrundverordnung fehlt jedoch im Katalog der Rechte Betroffener eine entsprechende ausdrückliche Regelung.

Die Konferenz hält es für erforderlich, zum Schutz der Privatsphäre der Telemediennutzer eine Bestimmung aufzunehmen, die zumindest bei zu privaten Zwecken genutzten Telemedien innerhalb der EU ein Recht auf pseudonyme Nutzung verbindlich statuiert.

4. Entschließungen der 90. Konferenz vom 30. September/ 1. Oktober 2015 in Darmstadt

Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden“ hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat

vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d. h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundli-

chen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden.

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

5. Sondersitzung am 21. Oktober 2015 in Frankfurt

Positionspapier der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zu den Auswirkungen des EuGH-Urteils zum Safe-Harbor-Abkommen vom 6. Oktober 2015 (Rechtssache C-362/14) vom 26. Oktober 2015

1. Nach dem Safe-Harbor-Urteil des EuGH vom 6. Oktober 2015 ist eine Datenübermittlung aufgrund der Safe-Harbor-Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG) nicht zulässig.

2. Im Lichte des Urteils des EuGH ist auch die Zulässigkeit der Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR), in Frage gestellt.

3. Der EuGH stellt fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten ungeachtet von Kommissions-Entscheidungen nicht gehindert sind, in völliger Unabhängigkeit die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen.

4. Der EuGH fordert die Kommission und die Datenschutzbehörden auf, das Datenschutzniveau in den USA und anderen Drittstaaten (Rechtslage und Rechtspraxis) zu untersuchen und gibt hierfür einen konkreten Prüfmaßstab mit strengen inhaltlichen Anforderungen vor.

5. Soweit Datenschutzbehörden Kenntnis über ausschließlich auf Safe-Harbor gestützte Datenübermittlungen in die USA erlangen, werden sie diese untersagen.

6. Die Datenschutzbehörden werden bei Ausübung ihrer Prüfbefugnisse nach Art. 4 der jeweiligen Kommissionsentscheidungen zu den Standardvertragsklauseln vom 27. Dezember 2004 (2004/915/EG) und vom 5. Februar 2010 (2010/87/EU) die vom EuGH formulierten Grundsätze, insbesondere die Randnummern 94 und 95 des Urteils, zugrunde legen.

7. Die Datenschutzbehörden werden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen erteilen.

8. Unternehmen sind daher aufgerufen, unverzüglich ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten. Unternehmen, die Daten in die USA oder andere Drittländer exportieren wollen, sollten sich dabei auch an der Entschließung der DSK vom 27.03.2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ und an der Orientierungshilfe „Cloud Computing“ vom 09.10.2014 orientieren.

9. Eine Einwilligung zum Transfer personenbezogener Daten kann unter engen Bedingungen eine tragfähige Grundlage sein. Grundsätzlich darf der Datentransfer jedoch nicht wiederholt, massenhaft oder routinemäßig erfolgen.

10. Beim Export von Beschäftigtendaten oder wenn gleichzeitig auch Daten Dritter betroffen sind, kann die Einwilligung nur in Ausnahmefällen eine zulässige Grundlage für eine Datenübermittlung in die USA sein.

11. Die Datenschutzbehörden fordern die Gesetzgeber auf, entsprechend dem Urteil des EuGH den Datenschutzbehörden ein Klagerecht einzuräumen.

12. Die Kommission wird aufgefordert, in ihren Verhandlungen mit den USA auf die Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen. Dies betrifft insbesondere das Recht auf gerichtlichen Rechtsschutz, die materiellen Datenschutzrechte und den Grundsatz der Verhältnismäßigkeit. Ferner gilt es, zeitnah die Entscheidungen zu den Standardvertragsklauseln an die in dem EuGH-Urteil gemachten Vorgaben anzupassen.

    Insoweit begrüßt die DSK die von der Art. 29-Gruppe gesetzte Frist bis zum 31. Januar 2016.

13. Die DSK fordert die Bundesregierung auf, in direkten Verhandlungen mit der US-Regierung ebenfalls auf die Einhaltung eines angemessenen Grundrechtsstandards hinsichtlich Privatsphäre und Datenschutz zu drängen.

14. Die DSK fordert Kommission, Rat und Parlament auf, in den laufenden Trilog-Verhandlungen die strengen Kriterien des EuGH-Urteils in Kapitel V der Datenschutzgrundverordnung umfassend zur Geltung zu bringen.

6. Entschließung nach der 90. Konferenz

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres (vom 29. Oktober 2015)

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 09. Oktober 2015 seinen Standpunkt zur Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie) angenommen hat, beraten Kommission, Parlament und Rat im sogenannten Trilog über ihre verschiedenen Positionen zur JI-Richtlinie mit dem Ziel der gemeinsamen Verabschiedung von JI-Richtlinie und Datenschutz-Grundverordnung (DSGVO) im Paket zum Jahresende 2015.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Konferenz) hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012[1] mehrfach öffentlich zur Datenschutzreform positioniert. Am 26. August 2015 hat sie zu den Trilogverhandlungen zur DSGVO Stellung genommen[2]. Sie hat ferner zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben[3]. Von Anfang an hat sie das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“ und dabei auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus im Anwendungsbereich der JI-Richtlinie hingewiesen. Mit dieser Richtlinie wird eine Lücke geschlossen, denn einen Rechtsakt, der die Datenverarbeitung in den Bereichen Polizei und Justiz in

[1] Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6

[2] Trilogpapier der Konferenz zur DSGVO, abrufbar unter: https://www.datenschutz.hessen.de/entschliessungen.htm

[3] Stellungnahmen zur DSGVO und zur JI-Richtlinie vom 11.6.2012; Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012, jeweils abrufbar unter https://www.datenschutz.hessen.de/entschliessungen.htm und https://www.datenschutz.hessen.de/taetigkeitsberichte.htm4

der EU umfassend regelt, kennt das EU-Recht bislang nicht. Dies hat die Konferenz in der Vergangenheit immer wieder kritisiert[4].

Die Konferenz setzt sich für eine Richtlinie ein, die auf möglichst hohem Niveau eine Mindestharmonisierung innerhalb der Europäischen Union herbeiführt. Sie begrüßt insofern die Entwürfe von Rat und Europäischem Parlament, als beide eine Mindestharmonisierung festschreiben. Mit einer Richtlinie verbindet die Konferenz die Erwartung an den deutschen Gesetzgeber und die deutsche Rechtsprechung, weiterhin Impulsgeber für die Schaffung eines effektiven Datenschutzrechts zu bleiben.

Vor diesem Hintergrund bewertet die Konferenz die JI-Richtlinie als einen wichtigen Schritt zur Verbesserung des Datenschutzes in der Europäischen Union. Kernanliegen des Datenschutzes im Bereich der polizeilichen Datenverarbeitung ist es, Grenzen der Erfassung und Speicherung in polizeilichen Dateien zu setzen: Bürgerinnen und Bürgern müssen darauf vertrauen können, nicht in polizeilichen Dateien erfasst zu werden, wenn sie keinen Anlass für eine polizeiliche Speicherung gegeben haben. Rechtmäßig von der Polizei erhobene Daten dürfen nur unter besonderen Voraussetzungen auch für andere polizeiliche Zwecke verwendet werden. Wer beispielsweise Opfer oder Zeuge einer Straftat war, muss darüber hinaus darauf vertrauen können, dass seine Daten nur beschränkt und unter strengen Voraussetzungen von Polizeibehörden verarbeitet werden dürfen. Dieses sind nur einige grundsätzliche Forderungen, die in der JI-Richtlinie zu regeln sind. Dazu stellt die Konferenz mit Bedauern fest, dass die Regelungen dieser Grundanliegen insbesondere in der vom Rat vorgelegten Fassung häufig allgemein bleiben, sich im Wesentlichen in dem Verweis auf das nationale Recht erschöpfen oder gar gänzlich fehlen.

Einen ganz wesentlichen Impuls für das deutsche Datenschutzrecht im Bereich von Polizei und Justiz erwartet die Konferenz von den Regelungen zur Durchsetzung des Datenschutzrechts durch die Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Datenschutz muss effektiv durchsetzbar sein. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Bei den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

[4] Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S.3.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der JI-Richtlinie.

II. Die Vorschläge im Einzelnen

1. Keine Ausweitung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO!

Der Anwendungsbereich der JI-Richtlinie kann nicht isoliert betrachtet werden, sondern er bestimmt spiegelbildlich den Anwendungsbereich der DSGVO. Denn die DSGVO findet nach deren Art. 2 Abs. 2 lit. e keine Anwendung, soweit die JI-Richtlinie Anwendung findet. Vor diesem Hintergrund sind in der Vergangenheit verschiedene Entwürfe diskutiert worden, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-Richtlinie führen könnten. Auch die vorgelegte Version des Rates wirft insofern in Art. 1 Abs. 1 JI-Richtlinie Fragen auf, als der Anwendungsbereich der JI-Richtlinie um die Formulierung „zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit“ erweitert worden ist.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche der DSGVO und der JI-Richtlinie wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der Kommission enthält die JI-Richtlinie Regelungen zum „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung“. Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst sei, soweit sie nicht der Prävention einer Straftat diene. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizei unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JI-Richtlinie – zusammenzufassen, solle der Anwendungsbereich der Richtlinie entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die Richtlinie zu fassen. Die Ordnungsverwaltung solle der JI-Richtlinie unterfallen, soweit sie Ordnungswidrigkeiten verfolgt. Damit stellt der Rat seine ursprüngliche Argumentation auf den Kopf. Denn diese Ausweitung der JI-Richtlinie führt gerade dazu, dass Ordnungsverwaltungen sodann sowohl der DSGVO als auch der JI-Richtlinie unterfielen, je nachdem welche Aufgabe sie erfüllten.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-Richtlinie für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen sichergestellt sein, dass davon nicht auch noch die

Datenverarbeitung der Ordnungsverwaltung erfasst wird. Dies ist nach der vom Rat vorgelegten Fassung nicht der Fall. Die Datenverarbeitung anderer Behörden als der Polizeibehörden sollte weiterhin von der DSGVO geregelt werden.

Die Konferenz sieht die in der Ratsfassung hinzugefügte Erweiterung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO kritisch. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte, wie im Entwurf der Kommission und des Europäischen Parlaments vorgesehen, von der DSGVO geregelt werden.

2. Die Durchbrechung der Zweckbindung darf nur in engen Grenzen erfolgen!

Die Konferenz hat in ihrer Stellungnahme vom 11. Juni 2012 die Klarstellung gefordert, dass die Regelungen über die Zweckbindung nicht so verstanden werden dürfen, „dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzung für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf". Die Bedeutung der Zweckbindung wurde auch durch die Europäische Grundrechtecharta betont, in der sich in Art. 8 Abs. 2 die Zweckbindung als tragendes Prinzip des Datenschutzes findet. In der Richtlinie sollte daher die Zweckbindung (Art. 4 Abs. 1 lit. b JI-Richtlinie) insgesamt strikter gefasst werden[5].

Der Rat hat in seiner Fassung den ursprünglichen Vorschlag der Kommission in Art. 4 Abs. 2 dahingehend ergänzt, dass eine Weiterverarbeitung für einen anderen Zweck innerhalb der JI-Richtlinie zulässig ist, wenn es dafür nach anwendbarem (nationalen) Recht eine Rechtsgrundlage gibt und die Weiterverarbeitung erforderlich und verhältnismäßig ist. Der Entwurf der Kommission enthielt insofern nur allgemeine Regelungen, nach der eine Weiterverarbeitung nicht „unvereinbar" mit dem ursprünglichen Zweck der Erhebung und nicht exzessiv sein dürfe (Art. 4 Abs. 1 lit. b und c).

Die Konferenz bedauert insofern, dass der Entwurf des Rates keine ambitionierteren, strengeren Vorgaben macht. Die vorgeschlagenen Regelungen lassen nach der Auffassung der Konferenz einen zu weiten Rahmen, den auszufüllen ganz weitgehend dem nationalen Gesetzgeber überlassen wird. In Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) sollte der Begriff der Unvereinbarkeit von Datenverarbeitungen konkretisiert werden. Danach liegt eine Unvereinbarkeit vor, „wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder

[5] Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S. 5.

nicht in dieser Art und Weise hätten erhoben werden dürfen („hypothetischer Ersatzeingriff“)[6].

Die Konferenz spricht sich für strenge Vorgaben an die Durchbrechung der Zweckbindung aus und regt insofern an, den Mitgliedstaaten konkrete Vorgaben für die Weiterverarbeitung zu machen. Der Begriff der Unvereinbarkeit in Art. 4 sollte bei Abs. 1 lit. b JI-Richtlinie in der Fassung des Rates wie folgt präzisiert werden: Eine Weiterverarbeitung der personenbezogenen Daten ist als unvereinbar mit dem ursprünglichen Erhebungszweck anzusehen, wenn die Daten nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen.

3. Unverdächtige und andere besondere Personengruppen brauchen mehr Schutz!

Der Schutz unverdächtiger Bürgerinnen und Bürger sowie besondere Voraussetzungen für besondere Personengruppen stellen ein Kernanliegen des Datenschutzes im Bereich der Polizei und Justiz dar. Die Konferenz bedauert insofern die ersatzlose Streichung des Art. 5 in der Fassung des Rates und weist ausdrücklich auf die Fassung des Europäischen Parlaments zu Art. 5 hin, der sich an einer Stellungnahme der Art. 29-Gruppe orientiert.

Ziel der von der Art. 29-Gruppe vorgeschlagenen Regelung des Art. 5 ist es sicherzustellen, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen mit kürzeren Fristen gespeichert werden und dass darüber hinaus Daten anderer Personen, die nicht einer Straftat verdächtig sind, entweder gar nicht oder nur in sehr begrenzten Fällen gespeichert werden dürfen.

Die Konferenz lehnt die Streichung des Art. 5 der JI-Richtlinie in der Ratsversion ab und unterstützt Art. 5 in der Fassung des Europäischen Parlaments.

4. Datenspeicherungen sind regelmäßig auf ihre Erforderlichkeit und Verhältnismäßigkeit zu überprüfen!

Ungeachtet des Rechts auf Löschung sollten die datenverarbeitenden Stellen verpflichtet sein, die Erforderlichkeit und Verhältnismäßigkeit von Speicherungen in regelmäßigen Abständen zu überprüfen. Eine solche Verpflichtung enthält die

[6] BVerfGE 100, 313, 389; ständige Rechtsprechung.

Ratsversion im Gegensatz zu Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments nicht. Der Rat beschränkt sich in seinem Entwurf darauf, die Mitgliedstaaten zur Festlegung von Speicher- und Aussonderungsprüffristen in Verfahrensverzeichnissen („records", Art. 23 JI-Richtlinie) zu verpflichten, wenn dies möglich ist. Dies reicht nicht aus. Vielmehr fordert die Konferenz als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

Die Konferenz fordert als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen nach dem Vorbild von Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

5. Moderner Datenschutz braucht umfassende Benachrichtigungspflichten!

Benachrichtigungen gehören zu den datenschutzrechtlichen „Kernrechten" der Betroffenen. Effektiver Rechtsschutz ist nicht möglich, wenn der von einer (heimlichen) Datenerhebung Betroffene keine Kenntnis von der Erhebung und Speicherung erlangt. Die Kontrolle dieser Datenverarbeitungen ist zwar auch Aufgabe der Datenschutzaufsichtsbehörden, doch sollte auch jede Bürgerin und jeder Bürger in die Lage versetzt werden, die sie oder ihn betreffende polizeiliche Maßnahme überprüfen zu können und überprüfen zu lassen.

Die Konferenz setzt sich daher für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

Zur Wahrung der Rechte des Einzelnen und zur Gewährung effektiven Rechtsschutzes durch Aufsichtsbehörden und Gerichte setzt sich die Konferenz für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

6. Keine Sonderregelung der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren!

Die Konferenz spricht sich für eine möglichst weitgehende einheitliche Regelung der Rechte der Betroffenen im Anwendungsbereich der JI-Richtlinie aus. Dem-

gegenüber enthält Art. 17 hinsichtlich personenbezogener Daten in Gerichtsbeschlüssen oder staatsanwaltschaftlichen Verfahrensakten die Regelung, dass die Ausübung der Betroffenenrechte „im Einklang mit dem einzelstaatlichen Recht" erfolgt. Schon in ihrer Stellungnahme vom 11. Juni 2012 hatte die Konferenz eine Klarstellung zum Regelungsgehalt des Art. 17 JI-Richtlinie gefordert. Leider tragen auch die vorgelegten Fassungen von Europäischem Parlament und Rat nicht dazu bei, die notwendige Klarstellung herbeizuführen. Die Konferenz betont daher noch einmal diese Notwendigkeit, da ansonsten Zweifel an der Anwendbarkeit der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren entstehen können. Zu diesem Zweck ist die Sonderregelung des Art. 17 zu streichen und sind die Betroffenenrechte in strafrechtlichen Ermittlungen einheitlich in der JI-Richtlinie zu regeln.

Die Konferenz spricht sich für eine Streichung des Art. 17 JI-Richtlinie aus, und wiederholt ihre Forderung, dass die in Kapitel III gewährten Betroffenenrechte auch im Bereich des staatsanwaltschaftlichen Ermittlungsverfahrens Anwendung finden.

7. Klarstellung – Datenverarbeitung nach dem Stand der Technik!

Die Konferenz unterstreicht die Bedeutung des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen. Die Verpflichtung, diese Grundsätze zu beachten, wird in Art. 19 JI-Richtlinie jedoch in verschiedener Hinsicht erheblich beschränkt, unter anderem durch Bezugnahme auf „verfügbare Technologie". Dies wird dem notwendigen Grundrechtsschutz nicht gerecht, denn „verfügbar" sind auch veraltete Technologien, die nicht (mehr) die ausreichende Sicherheit bieten.

Demgegenüber stellt der „Stand der Technik" („state of the art") sicher, dass jeweils die modernsten vorhandenen Technologien einzusetzen sind. Der Stand der Technik ist eine im Europäischen Datenschutz handhabbare Definition. Sie findet seit längerem eine bewährte Anwendung in der Praxis und sollte auch in der JI-Richtlinie verwendet werden.

Der an verschiedenen Stellen gebrauchte ungenaue und dem Schutzbedarf personenbezogener Daten nicht gerecht werdende Begriff „verfügbare" Technik bzw. Technologie sollte konsequenter Weise auch in der JI-Richtlinie durch „Stand der Technik" ersetzt werden. Die Konferenz spricht sich insofern für Art. 19 in der Fassung des Europäischen Parlaments aus.

8. Datenschutz-Folgeabschätzung auch im Bereich der JI-Richtlinie!

Bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden sind Datenschutz-Folgeabschätzungen äußerst wichtig, da gerade bei dieser Verarbeitung erhöhte Risiken für den Einzelnen bestehen. Das Europäische Parlament hat eine entsprechende Regelung zur Datenschutz-Folgenabschätzung vorgeschlagen, die jedoch vom Rat abgelehnt wird.

Die vom Europäischen Parlament in Art. 25 a vorgeschlagene Bestimmung sieht eine Datenschutz-Folgenabschätzung vor, wenn die Verarbeitungsvorgänge aufgrund ihrer Natur, ihres Anwendungsbereichs oder ihrer Bestimmungszwecke eine konkrete Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellen können. Für die in Art. 25 a (2) lit. b erwähnten „biometrischen Daten" gibt es in Art. 3 Abs. 11 des Vorschlags des Europäischen Parlaments eine entsprechende Definition.

In Art. 33 des Entwurfs der Datenschutz-Grundverordnung (Ratsfassung) ist, anders als beim Richtlinien-Vorschlag, nach wie vor eine Datenschutz-Folgenabschätzung vorgesehen. Doch gerade im verarbeitungsintensiven Bereich der Strafverfolgung sind gründliche Sicherheitsvorkehrungen beim Umgang mit personenbezogenen Daten von größter Wichtigkeit, weshalb sich die Konferenz für die Aufnahme einer entsprechenden Regelung in den Richtlinienvorschlag ausspricht.

Die Konferenz setzt sich für eine Regelung der Datenschutz-Folgenabschätzung ein, die sich an Art. 25 a des Richtlinien-Vorschlags des Europäischen Parlaments orientiert. In diesem Zusammenhang befürwortet die Konferenz die Wiederaufnahme der Definition der „biometrischen Daten", wie sie vom Europäischen Parlament in Art. 3 Abs. 11 vorgesehen war.

9. Guter Datenschutz braucht behördliche Datenschutzbeauftragte!

Die Konferenz bedauert, dass der Rat es in seiner Version ablehnt, die Mitgliedstaaten zur Schaffung eines behördlichen Datenschutzbeauftragten zu verpflichten, sondern dies stattdessen in deren Ermessen stellt. Die Datenschutzbeauftragten des Bundes und der Länder haben überwiegend sehr gute Erfahrung bei der Zusammenarbeit mit den Datenschutzbeauftragten der beaufsichtigten Behörden gemacht und halten die interne Kontrolle vor Ort – neben der externen Kontrolle durch die Aufsichtsbehörden – für ein unverzichtbares Element eines flächendeckenden effektiven Datenschutzregimes.

Die Konferenz betont die Bedeutung einer verpflichtenden Bestellung eines behördlichen Datenschutzbeauftragten und spricht sich deshalb für Art. 30 des Vorschlages des Europäischen Parlaments aus.

10. Übermittlungen an Behörden und Gerichte in Drittstaaten bedürfen eines transparenten Verfahrens, der Abwägung im Einzelfall und müssen überprüfbar dokumentiert sein!

Neu an den Regelungen über die Übermittlung personenbezogener Daten in Drittstaaten ist, dass auch im JI-Bereich das Instrument des Angemessenheitsbeschlusses eingeführt werden soll. Die Konferenz ist der Auffassung, dass die geltenden Angemessenheitsbeschlüsse nicht auf den JI-Bereich übertragbar sind. Neben den Übermittlungen in Drittstaaten mit adäquatem Datenschutzniveau wird die Mehrzahl der Übermittlungen weiterhin auf der Grundlage bilateraler Abkommen und nationalen Rechts (im Einzelfall) erfolgen.

Die Konferenz fordert, in Übereinstimmung mit der Rechtsprechung des EuGH Abwägungsklauseln für alle Übermittlungen vorzusehen. Diese sollten die übermittelnde Behörde verpflichten, eine Abwägung zwischen dem Interesse an der Übermittlung und den schutzwürdigen Interessen des Betroffenen vorzunehmen. Die JI-Richtlinie sollte zugleich Dokumentationspflichten festschreiben, um die Kontrolle von Übermittlungen überprüfbar zu machen. Die Konferenz bedauert insofern die Streichung der Dokumentationspflicht in Art. 35 Abs. 2 in der Fassung des Rates. Zudem sollten die Drittstaaten über Verarbeitungsbeschränkungen (Löschfristen etc.) informiert werden.

Die Konferenz spricht sich ebenfalls für eine Art. 43 a der Parlamentsfassung der Datenschutz-Grundverordnung entsprechende Regelung aus. Danach sind Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt noch vollstreckbar, wenn dies nicht in internationalen Übereinkommen zur Amts- und Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten Stellen. Die Konferenz erkennt an, dass mit der Schaffung einer solchen Regelung insbesondere die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden wird. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Die Konferenz fordert bei jeder Übermittlung in Drittstaaten eine Abwägung im Einzelfall. Des Weiteren muss die JI-Richtlinie sicherstellen, dass Übermittlungen dokumentiert und damit kontrollierbar sind. Deshalb sollte die Dokumentationspflicht gem. Art. 35 in der Fassung der Kommission beibehalten werden. Über nationale Verarbeitungsbeschränkungen ist bei jeder Übermittlung zu informieren. Des Weiteren fordert die Konferenz eine Regelung zur Übermittlung personenbezogener Daten an Behörden und Gerichte eines Drittstaates in Anlehnung an Art. 43 a der Parlamentsfassung der Datenschutz-Grundverordnung.

11. Befugnisse der Datenschutzbehörden müssen gestärkt werden!

Datenschutz muss effektiv durchsetzbar sein. Die Konferenz erwartet von der Datenschutzreform daher eine Stärkung der Befugnisse der Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Art. 8 Abs. 3 der EU-Grundrechtecharta und Art. l6 Abs. 1 AEUV verlangen vielmehr eine wirksame Durchsetzung der Grundrechte der Bürgerinnen und Bürger. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Datenschutz muss effektiv durchsetzbar sein. Dazu fordert die Konferenz die Stärkung der Befugnisse der Datenschutzbehörden durch die JI-Richtlinie. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

II. Düsseldorfer Kreis – Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Videoüberwachung in Schwimmbädern

Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises vom 19.02.2014, Stand 10. August 2015

Da der Besuch von Schwimmbädern auch mit einigen Risiken verbunden sein kann, greifen viele Betreiber zum Hilfsmittel der Videoüberwachung, sei es, beispielsweise, um den Aufbruch von Spinden oder die unsachgemäße Benutzung der Rutsche zu verhindern. Schwimmbäder, die sich in öffentlicher Trägerschaft befinden, sind nach dem geltenden Landesrecht zu prüfen.

Ansonsten findet das Bundesdatenschutzgesetz (BDSG) Anwendung, weshalb die in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises (OH Videoüberwachung) beschriebenen Grundsätze für diese Schwimmbäder anwendbar sind.

Der Großteil der in Schwimmbädern befindlichen Kameras überwacht Bereiche, die für die Kunden zugänglich sind. Für diese öffentlich zugänglichen Räume beurteilt sich die datenschutzrechtliche Zulässigkeit nach § 6b BDSG.

Da sich die Schwimmbadbesucher im Schwimmbad zum Zweck der Freizeitgestaltung aufhalten, genießen sie besonderen Schutz (vgl. OH Videoüberwachung) und die Prüfung des Vorliegens der gesetzlichen Voraussetzungen bedarf besonderer Sorgfalt. Nach § 6b BDSG muss die Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unabhängig von der Frage eines berechtigten Interesses oder der befugten Hausrechtsausübung ist eine Videoüberwachung jedenfalls nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu Bereichen, für die ein zusätzliches Entgelt (z. B. zum Saunabereich) zu entrichten ist. Dies kann durch andere geeignete Maßnahmen, wie hohe Drehkreuze oder Schranken ohne unverhältnismäßigen Aufwand verhindert werden.

Besonderes Augenmerk ist auf das erforderliche Maß der Überwachung zu richten: Sofern die übrigen Voraussetzungen vorliegen, ist der Aufnahmebereich der Kamera ausschließlich auf den Bereich (z. B. Kassenautomaten) zu richten, den

der Zweck der Videoüberwachung betrifft. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung außerhalb der Öffnungszeiten.

Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge“) zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung Betroffenen unzulässig. Es ist nicht verhältnismäßig, einen derartigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung für eine große Zahl von Personen hinzunehmen, nur, damit das Schwimmbad im Zweifel die Möglichkeit hat, seine Haftung auszuschließen. Eine Haftung unterliegt zudem der Beweispflicht des Geschädigten. Die Rechtsprechung fordert keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen[1].

Schutzwürdige Interessen der Betroffenen überwiegen immer, wenn die Intimsphäre des Betroffenen berührt ist, weswegen eine Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna generell unzulässig ist.

Eine Videoüberwachung kann im Einzelfall zur Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen zulässig sein, sofern nicht gleichzeitig Bänke/Ablageflächen oder Umkleidebereiche erfasst werden. Voraussetzung ist, dass den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Bereich sie sich begeben. Dabei sind Bereiche, die videoüberwacht werden, von solchen, in denen keine Überwachung stattfindet, erkennbar zu trennen, beispielsweise durch farbige Markierung des Fußbodens.

Unverhältnismäßig und damit nicht zulässig ist jedenfalls die Videoüberwachung aufgrund von Bagatellschäden (z. B. Beschädigung von Haartrocknern).

[1] OLG Koblenz, Beschluss vom 07.05.2010, Az.: 8 U 810/09: Der Betreiber genügt seiner Verkehrssicherungspflicht, wenn durch Hinweisschilder mit ausformulierten Warnhinweisen oder mit Piktogrammen auf die Problempunkte eindeutig hingewiesen wird; LG Münster, Urteil vom 17.05.2006, Az.: 12 O 639/04: Der Betreiber eines Schwimmbads genügt seiner Verkehrssicherungspflicht, wenn er einen Bademeister bereitstellt, der sein Augenmerk auch – wenn auch nicht ununterbrochen – auf die besonderen Schwimmbadeinrichtungen (hier: ins Nichtschwimmerbecken führende Kinderrutsche) richtet.

Darüber hinaus sind die in der OH Videoüberwachung unter Ziffer 2.2 benannten Maßnahmen (z. B. Verfahrensverzeichnis, Vorabkontrolle, Hinweisbeschilderung) zu beachten. Dazu gehört auch, Bildschirme so zu positionieren, dass sie nicht für Dritte einsehbar sind.

Nutzung von Kameradrohnen durch Private
(Beschluss vom 15./16. September 2015)

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potentiell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr. 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6 b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a des Strafgesetzbuches (StGB)), mithin Bereiche der Intimsphäre (im Einzelnen dazu: Bundestagsdrucksache 15/2466, S. 5.) oder der Aufzeichnung des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“

Datenschutzgerechter Einsatz von optisch-elektronischen Einrichtungen in Verkehrsmitteln des öffentlichen Personennahverkehrs und des länderübergreifenden schienengebundenen Regionalverkehrs (Stand: 16.09.2015)

1. Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder sowie die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hatten unter Beteiligung des Verbandes Deutscher Verkehrsunternehmen (VDV) im Jahre

2001 Empfehlungen zur Videoüberwachung in öffentlichen Verkehrsmitteln abgestimmt.

Unter Berücksichtigung der Erfahrungen aus der Anwendungspraxis sowie auch der technischen Entwicklungen auf dem Gebiet der Videoüberwachungstechnik der letzten Jahre halten die Aufsichtsbehörden eine Fortschreibung dieser Empfehlungen nunmehr für geboten. Zudem wurde der Anwendungsbereich der ursprünglich nur für den öffentlichen Personennahverkehr (ÖPNV) geltenden Orientierungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr (SPNV) erweitert.

Im Spannungsfeld zwischen den berechtigten Interessen der Verkehrsunternehmen an einer Videoüberwachung und dem informationellen Selbstbestimmungsrecht ihrer Fahrgäste und Beschäftigten soll dieses Dokument eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben.

2. Zulässigkeit der Videoüberwachung

Maßgebliche Vorschrift für die Prüfung der Zulässigkeit von Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln ist § 6b des Bundesdatenschutzgesetzes (BDSG), sofern der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird und deshalb die Zulässigkeit des Kameraeinsatzes nach Maßgabe des jeweiligen Landesdatenschutzgesetzes zu beurteilen ist.

Soweit Kameras auch Arbeitsplätze von Beschäftigten der Verkehrsunternehmen in öffentlichen Verkehrsmitteln miterfassen (z. B. Fahrerarbeitsplätze), findet neben dieser Vorschrift ggf. auch § 32 BDSG Anwendung. Zweckmäßig ist auch der Abschluss einer Betriebsvereinbarung.

2.1 Videoüberwachung in Fahrgastbereichen

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen.

2.1.1 Wahrnehmung des Hausrechts oder berechtigter Interessen

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann zur Wahrnehmung des Hausrechts oder berechtigter Interessen insbesondere zur Verhinderung oder

Verfolgung von Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit in Betracht kommen.

Eine Videobeobachtung (sog. Monitoring) kann erfolgen, um Personen davon abzuhalten, Rechtsverstöße zu begehen (z. B. Gewalt gegen Beschäftigte, Sachbeschädigungen an Beförderungseinrichtungen). Dieser Überwachungszweck wird auf direkte Weise erreicht, wenn das Geschehen in Echtzeit durch interventionsbereites Personal beobachtet und dadurch im Notfall ein schnelles Eingreifen möglich wird.

Ist die Videoüberwachung als reine Aufzeichnungslösung ausgestaltet (sog. Black-Box-Lösung), so kann sie eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann bzw. dass Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse (z. B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren.

2.1.2 Erforderlichkeit der Videoüberwachung

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist stets einzelfallbezogen zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn die Überwachung geeignet ist, das festgelegte Ziel zu erreichen, und es hierfür kein milderes, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt.

Wenn der Zweck ausschließlich in der Beobachtung des Geschehens in Echtzeit zur direkten Intervention besteht, ist nur eine Monitoring-Lösung geeignet; eine reine Black-Box-Ausgestaltung der Videoüberwachung eignet sich wiederum zur Aufklärung von Straftaten.

Vor dem Einsatz einer Videoüberwachungsanlage müssen sich die Verkehrsunternehmen insbesondere mit zumutbaren alternativen Methoden auseinandersetzen, die in das informationelle Selbstbestimmungsrecht der Fahrgäste weniger eingreifen.

So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut Rechnung tragen wie der Einsatz von Überwachungskameras. Auch die Verwendung besonders widerstandsfähiger Sitze/Sitzbezüge sowie eine

spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine nur temporäre Videoüberwachung (z. B. nur zu bestimmten Tages- bzw. Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen. Denkbar ist es, zu Zeiten oder auf Linien, in denen eine permanente Videoüberwachung nicht erforderlich ist, die Möglichkeit einer anlassbezogenen Aktivierung der Videoüberwachung durch einen Notfallschalter für den Fahrzeugführenden oder das Begleitpersonal vorzusehen.

Nicht erforderlich ist eine Videoüberwachung zur Abwehr von Haftungsansprüchen gegen das Verkehrsunternehmen. Der Einsatz von Kameras kann nicht damit begründet werden, dass die Aufzeichnungen benötigt werden, um (unberechtigte) Ansprüche von Fahrgästen wegen Sturzverletzungen oder Beschädigungen persönlicher Gegenstände infolge (angeblich) starker Bremsungen o. Ä. abzuwehren. Zunächst ist der Betroffene in der Pflicht, seine Schadensersatzansprüche zu begründen und den Nachweis zu erbringen, dass sein Sturz unter den gegebenen Umständen für ihn unvermeidbar war und durch das Verkehrsunternehmen verursacht worden ist. Videoaufnahmen zum Beweis des Gegenteils bedarf es daher nicht.

Schließlich ist eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste unter dem Gesichtspunkt der Erforderlichkeit nicht geboten.

Ist unter Berücksichtigung dieser Kriterien die Erforderlichkeit einer Videoüberwachung insgesamt oder im vorgesehenen Umfang zu verneinen, so ist der Einsatz von Videokameras unzulässig, ohne dass es noch auf die Frage ankommt, ob ihr schutzwürdige Interessen der Betroffenen entgegenstehen.

2.1.3 Beachtung der schutzwürdigen Interessen der Betroffenen

Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen im Einzelfall erforderlich sein sollte, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Vorzunehmen ist eine Abwägung zwischen den berechtigten Interessen der Verkehrsunternehmen und dem informationellen Selbstbestimmungsrecht der von einer Videoüberwachung betroffenen Fahrgäste. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist insbesondere die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informati-

onsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes), durch den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.

So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können, einen intensiveren Eingriff dar als eine nur zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer der Fahrgäste im Verkehrsmittel: je länger der Beförderungsvorgang andauert, desto intensiver ist der von einer Videoüberwachung ausgehende Eingriff in das Recht auf informationelle Selbstbestimmung der Fahrgäste. Die informationelle Selbstbestimmung wird zudem besonders intensiv bei der Überwachung von Bereichen betroffen, in denen Menschen typischerweise miteinander kommunizieren. Hinzu kommt, dass die Fahrgäste häufig auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel ausweichen können. Zudem wird durch eine Videoüberwachung in öffentlichen Verkehrsmitteln eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine solche Überwachungsmaßnahme bieten.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann daher nur zum Schutz von Rechtsgütern erheblichen Gewichts gerechtfertigt sein.

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist im Rahmen einer abwägenden Einzelfallprüfung nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und gemäß § 6b BDSG entsprechend zu beschränken. Maßstab für eine Differenzierung können beispielsweise die Anzahl von Vorkommnissen, Schadenshöhe sowie Art von Ereignissen in der Vergangenheit (Sachbeschädigung, Missbrauch von Notrufeinrichtungen etc.) sein. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist daher nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. Bei der Beschaffung einer Videoüberwachungseinrichtung sollte darauf geachtet werden, dass die technischen Möglichkeiten für eine Differenzierung bestehen.

Da sich die Intensität des von einer Videoüberwachung ausgehenden Eingriffs in das informationelle Selbstbestimmungsrecht der Fahrgäste durch eine längere Aufenthaltsdauer in überwachten Bereichen deutlich erhöht, kann auf längeren Strecken – wie beispielsweise dem länderübergreifenden Bahnbetrieb – eine Videoüberwachung nur auf Streckenabschnitten mit häufigen und schwerwiegenden Eingriffen in Rechtsgüter erheblichen Gewichts in Betracht kommen. Nur geringfügige oder vereinzelt auftretende Beeinträchtigungen dieser Rechtsgüter können dort keine Videoüberwachung der Fahrgastbereiche rechtfertigen. Eine solche kann aufgrund ihrer hohen Eingriffsintensität auf längeren Streckenabschnitten allenfalls in Ausnahmefällen erfolgen.

2.2 Videoüberwachung von Beschäftigten

Sofern in öffentlichen Verkehrsmitteln auch Arbeitsplätze von Beschäftigten von optisch-elektronischen Einrichtungen erfasst werden (z. B. der zum Zutritt für Fahrgäste hin offene Fahrerplatz in Bussen), ist Folgendes zu beachten:

In Fällen, in denen die Erfassung der Arbeitsplätze der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, ist das Einrichten von sog. Privatzonen, d. h. das dauerhafte Ausblenden von Bereichen, in denen sich nur die Beschäftigten aufhalten, erforderlich. Vorzugsweise ist die Kamera jedoch so zu installieren, dass sich kein ständiger Arbeitsplatz im Erfassungsbereich befindet.

Wird ausschließlich der Fahrerarbeitsplatz (z. B. der durch eine Tür vom Fahrgastraum getrennte Fahrzeugführerstand) durch Kameras erfasst, richtet sich die datenschutzrechtliche Zulässigkeit einer solchen Maßnahme nach § 32 BDSG. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten der Beschäftigten durch eine Videoüberwachungsanlage kann allerdings in der Regel nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden. Denkbar ist zwar eine offene Videoüberwachung zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber seinen Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Davon kann bei einem abgeschlossenen Fahrerarbeitsplatz jedoch in aller Regel nicht ausgegangen werden. Selbst wenn in Ausnahmefällen hier eine Videoüberwachung in Betracht kommen sollte, ist der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte ist auszublenden.

Im Übrigen dürfen personenbezogene Daten eines Beschäftigten insbesondere mittels Videoüberwachung nur zur Aufdeckung einer Straftat nach Maßgabe des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden. Erforderlich sind hier zu dokumentierende tatsächliche Anhaltspunkte, die den Verdacht begründen, dass der Beschäftigte eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Liegen diese Voraussetzungen vor, ist eine Videoüberwachung gleichwohl nur für einen befristeten Zeitraum zulässig, sofern diese Maßnahme das einzige Mittel zur Überführung eines der Begehung von Straftaten konkret verdächtigten Beschäftigen darstellt. Eine dauerhafte Videoüberwachung von Beschäftigten 6ohne konkreten Verdacht ist hingegen datenschutzwidrig. Insbesondere dürfen Kameras nicht zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz verwendet werden.

Vor diesem Hintergrund muss das Verkehrsunternehmen nicht zuletzt auch dafür Sorge tragen, dass mittels der in den Fahrzeugen installierten Kameras keine Überwachung des in den Betriebshöfen mit der Reinigung, Reparatur und Wartung beauftragten technischen Personals erfolgen kann. Dies kann beispielsweise durch den Einbau diesbezüglicher Werkstattschalter oder die Kopplung des Kamerabetriebs an die Eingabe einer Linienkennung erreicht werden.

3. Maßnahmen vor Einrichtung einer Videoüberwachung

Die Verantwortung für eine datenschutzgerechte Videoüberwachung liegt auch dann beim Verkehrsunternehmen, wenn es Fahrzeuge mit eingebauter Videoüberwachungstechnik, die von anderer Seite, z. B. von der die Verkehrsleistung beauftragenden lokalen Nahverkehrsgesellschaft (LNVG) zur Verfügung gestellt worden sind, verwendet. Daher obliegt es auch dem Verkehrsunternehmen, vor der Inbetriebnahme von Videoüberwachungskameras den damit verfolgten Zweck in einer Verfahrensbeschreibung festzulegen.

3.1 Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte des Verkehrsunternehmens ist über die geplante Einrichtung einer Videoüberwachung rechtzeitig zu unterrichten, da hier die Zuständigkeit für die Durchführung der Vorabkontrolle liegt (§ 4d Abs. 5 und 6 BDSG). Er oder sie trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens „Videoüberwachung“ mit den Angaben nach § 4e Satz 1 Nrn. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar gemacht wird.

3.2 Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder / Piktogramme / Displays außen die Videoüberwachung kenntlich machen (vgl. § 6b Abs. 2 BDSG).

Der Hinweis ist so anzubringen, dass der Fahrgast ihn beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat und nicht erst von ihm gesucht werden muss, auch bei geöffneten Türen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.

Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Daher ist die verantwortliche Stelle mit ihren Kontaktdaten explizit zu nennen.

3.3 Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die zu benutzenden Datenträger, auf denen die Speicherung der Bilddaten erfolgen soll, festgelegt werden. Außerdem müssen die besonderen Gründe festgelegt werden, aufgrund derer die Beweis sichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden dürfen sowie wann die Aufzeichnung zu löschen ist. Die Beschäftigten, die Zugang zu den Aufzeichnungen haben, müssen mit ihrer Funktionsbezeichnung (nicht namentlich) bestimmt werden. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

3.4 Mitbestimmung durch die Betriebs- / Personalvertretung

Bei der Videoüberwachung von Beschäftigten handelt es sich regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten geeignet ist. Ihre Einführung und Anwendung unterliegt gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung durch den Betriebsrat. In einer Betriebsvereinbarung sollte deshalb darauf hingewirkt werden, dass die Datenerhebung und die Auswertung in so engen Grenzen gehalten werden wie möglich. Dabei werden folgende Punkte als Bestandteil einer Betriebsvereinbarung festzulegen sein:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Zweckbeschreibung
- Datenvermeidung- und Datensparsamkeit
- Empfängerin und/oder Empfänger der Daten
- Rechte der Betroffenen
- Löschungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (Anlage zu § 9 Abs. 1 BDSG), insbesondere Erstellung eines Berechtigungskonzepts.

Eine solche Betriebsvereinbarung wird dazu beitragen, die Erfüllung der gemeinsamen Aufgaben von Arbeitgeberin bzw. Arbeitgeber und Betriebsrat sicherzustellen, die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

In Unternehmen ohne Betriebsrat sollten Arbeitgeberinnen und Arbeitgeber Regelungen in Dienstanweisungen treffen.

4. Durchführung einer zulässigen Videoüberwachung

4.1 Löschungspflicht

Bei der nicht anlassbezogenen Aufzeichnung in einer Black-Box erfolgt – sofern kein Vorkommnis festgestellt wird – die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich.

Die Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist. Die Löschung soll daher im Regelfall nach 48 Stunden erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, wenn beispielsweise das Verkehrsmittel nicht innerhalb dieser Frist zu einem Ort zurückkehren kann, an dem festgestellte und aufgezeichnete Vorfälle gesondert gesichert werden können.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung; hierzu geeignete Bilder werden auf einem neuen Datenträger gespeichert und die Übrigen unverzüglich gelöscht.

4.2 Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Abs. 4 BDSG). Zweck dieser Regelung ist es, der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Die Unterrichtung hat über die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen.

4.3 Übermittlung von Videosequenzen an Polizei und Staatsanwaltschaft

Nach § 6b Abs. 3 Satz 2 BDSG können gespeicherte Videoaufnahmen zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten an Polizei oder Staatsanwaltschaft herausgegeben werden.

Können bzw. müssen angeforderte Videosequenzen zulässigerweise an Polizei oder Staatsanwaltschaft herausgegeben werden, so müssen der Grund der Übermittlung, Art und Umfang der übermittelten Videodaten, Speichermedium sowie

der Zeitpunkt der Übergabe und der Name der die Daten im Empfang nehmenden Person dokumentiert werden (vgl. Anlage zu § 9 BDSG).

4.4 Ausschreibungen

In Ausschreibungen, insbesondere durch die Verkehrsgesellschaften der Länder als Aufgabenträger für den schienengebundenen Personennahverkehr (SPNV), sind die Grundsätze dieser Orientierungshilfe zu beachten. Ausschreibungen, die z. B. pauschal eine „möglichst umfassende“ Videoüberwachung fordern, entsprechen diesen Grundsätzen nicht und richten sich auf Videoüberwachungsmaßnahmen, die mit § 6b BDSG nicht zu vereinbaren sind.

4.5 Überprüfung der Rechtmäßigkeitsvoraussetzungen

Verkehrsunternehmen, die in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, die rechtlichen Voraussetzungen für deren Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich zum Beispiel nach Ablauf eines Jahres, in dem die Kameras in Betrieb waren, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachungsanlage nicht weiter betrieben werden. Das Ergebnis der Überprüfung sollte dokumentiert werden.

III. Europäische Konferenz der Datenschutzbeauftragten

Manchester, 20. Mai 2015

Erfüllung datenschutzrechtlicher Erwartungen in der digitalen Zukunft

Präambel

Die Welt hat sich seit der Annahme des Übereinkommens 108 des Europarates und der derzeitigen Europäischen Datenschutzrichtlinie 95/46 stark verändert. Die Einzelnen erwarten zu Recht, dass die Datenschutzbehörden auf diese Veränderungen eingehen. Neue Technologien und digitale Dienste entwickeln sich ständig weiter.

Immer mehr personenbezogene Daten werden auf immer komplexer werdende und potentiell einschneidendere Art und Weise erhoben, ausgetauscht und analysiert. Die Einzelnen verlassen sich immer stärker auf das Internet zur Durchführung von Transaktionen mit öffentlichen und privaten Einrichtungen, zum Zugriff auf Informationen und zur Interaktion mit anderen.

Im Rahmen dieser sich stetig wandelnden digitalen Welt, ihrer globalen Herausforderungen, der Aktualisierung des Übereinkommens Nr. 108 und des anstehenden Reformpakets zum Datenschutz in der EU werden die europäischen Datenschutzbehörden mit zahlreichen neuen Herausforderungen konfrontiert, mit Auswirkungen auf die Ausübung ihrer Aufgaben hinsichtlich der Förderung und Verteidigung der Datenschutzrechte.

Die Suche nach dem Ort von Privatsphärenschutz und Datenschutz gestaltet sich komplex. Manche Bürger mögen die Preisgabe ihrer personenbezogenen Daten als einen Teil des modernen Lebens akzeptiert haben, was aber noch nicht bedeutet, dass sie damit den Schutz der Privatsphäre aufgegeben haben. Es gibt überzeugende Belege dafür, dass in der Praxis viele Bürgerinnen und Bürger zunehmend über den Verlust der Kontrolle über ihre persönlichen Informationen besorgt sind, da die Systeme immer komplexer werden und die Nutzung dieser Systeme in der heutigen Gesellschaft unvermeidbar ist.

Trotz großer Sorge in der Öffentlichkeit über Privatsphäre und den Schutz personenbezogener Informationen, insbesondere in einem digitalen Umfeld, gibt es ein relativ geringes öffentliches Bewusstsein über die Existenz der Datenschutzbehörden und ihrer Schlüsselrolle für den Schutz des Datenschutzrechts der Einzelnen. Dies führt nicht nur zu der Notwendigkeit, das Bewusstsein der Bürger für ihre Datenschutzrechte zu wecken, sondern auch das öffentliche Bewusstsein

für die wichtige Rolle der Datenschutzbehörden hinsichtlich des Schutzes der personenbezogenen Daten.

Indessen werden die Datenschutzbehörden zunehmend mit finanziellen und anderen Ressourcenbeschränkungen konfrontiert, während gleichzeitig die Ansprüche an sie steigen. Nicht nur muss das Recht mit der sich stetig wandelnden digitalen Welt Schritt halten, sondern auch die Fähigkeit der Datenschutzbehörden für eine wirksame Aufsicht auf nationaler und EU-Ebene sowie auf einer breiteren europäischen Ebene. Wenn die Einzelnen notwendiges Vertrauen und Zuversicht für eine erfolgreiche digitale Zukunft haben sollen, dann müssen die den Datenschutzbehörden zur Verfügung stehenden Befugnisse und Ressourcenausreichend sein, damit sie in angemessener Weise für die Wahrung der Grundrechte und Freiheiten der Einzelnen im digitalen Zeitalter eintreten können.

Es ist aber nicht nur eine Frage der Ressourcen. Es ist ebenso notwendig, dass die Datenschutzbehörden einen nachhaltigen Ansatz auf nationaler, EU-weiter und auf einer breiteren europäische Ebene annehmen, damit sie ihre Aufgaben wahrnehmen können und ihre Tätigkeiten dort gezielt ausüben können, wo die Notwendigkeit des Schutzes der Privatsphäre am größten ist, und damit sie ein eingehendes Verständnis hinsichtlich der datenschutzrechtlichen Auswirkungen neuer und bestehender Technologien haben.

***

Die Europäische Konferenz der Datenschutzbehörden

- *In Anbetracht dessen*, dass das Zusatzprotokoll zum Übereinkommen Nr. l08 des Europarats anerkennt, dass die Aufsichtsbehörden ein notwendiger Bestandteil des wirksamen Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten sind, und dass diese Behörden zur Wahrung ihrer Effektivität in völliger Unabhängigkeit handeln und über die erforderlichen Befugnisse und Ressourcen verfügen müssen, die zur Erfüllung ihrer Aufgaben erforderlich sind.

- *Auch unter Hinweis darauf*, dass in Artikel 8 der Charta der Grundrechte der Europäischen Union das Recht auf den Schutz personenbezogener Daten vorgesehen ist, und dass dieses Recht die Kontrolle über die Einhaltung der datenschutzrechtlichen Vorschriften von einer unabhängigen Aufsichtsbehörde umfasst.

- *Ferner unter Hinweis darauf*, dass die kürzlich überarbeiteten OECD-Leitlinien für den Schutz der Privatsphäre bei grenzüberschreitendem Datenverkehr eine Bestimmung enthalten, wonach die Mitgliedstaaten Behörden zur Durch-

setzung des Datenschutzes einrichten und aufrechterhalten sollten mit der für die wirksame Ausübung ihrer Befugnisse notwendigen Verwaltung sowie den nötigen Ressourcen und technologischen Fachkompetenzen.

- *Eingedenk entsprechend* der entscheidenden Rolle, die von starken, unabhängigen Datenschutzbehörden als Wächtern erwartet wird, wenn es um die Wahrung der Grundrechte und Freiheiten der Einzelnen im digitalen Zeitalter geht.

- *In der Erwägung*, dass die Datenschutzbehörden ohne die notwendigen Befugnisse und Ressourcen nicht in der Lage sind, ihrer wichtigen Rolle nachzukommen, wozu auch ein besseres Verständnis für die Sorgen und Erwartungen der Einzelnen gehört, um ihnen einen wirksamen Schutz der Privatsphäre zu bieten.

- *In der Erkenntnis*, dass dies die Einzelnen zwangsläufig ohne ausreichenden Schutz lässt und dadurch Vertrauen und Zuversicht der Öffentlichkeit in eine digitale Zukunft gefährdet werden.

- *Unter Hinweis darauf*, dass der Gerichtshof der Europäischen Union[1] sich mit der Wichtigkeit von Finanzierung und Unabhängigkeit der Datenschutzbehörden befasst hat.

- *In dem Bewusstsein*, dass auf dem Papier stehende Rechte und Pflichten durchzusetzen und zu erbringen sind, da sie ansonsten im besten Fall eine Illusion und im schlimmsten Fall eine Täuschung der Bürgerinnen und Bürger darstellen.

1. **Fordert die Regierungen der europäischen Länder**[2] auf, dafür Sorge zu tragen, dass die finanzielle Ausstattung der Datenschutzbehörden zur Erfüllung ihrer ständig steigenden Anforderungen ausreichend ist, und dafür zu sorgen, dass die von den Gesetzgebern festgelegten Bestimmungen in der Praxis ordnungsgemäß befolgt werden. Dabei ist die Notwendigkeit der gegenseitigen Zusammenarbeit zu berücksichtigen, und dies muss auf eine Art und Weise erreicht werden, bei der die notwendige Unabhängigkeit respektiert und aufrechterhalten wird.

2. **Ruft die Gesetzgeber in ganz Europa zur Sicherstellung auf**, dass die nächste Generation der Datenschutzgesetze, soweit wie möglich, in klaren und einfachen Worten abgefasst wird, und dass sie von Organisationen, Einzelnen und Datenschutzbehörden auf einfache Weise verstanden und umgesetzt werden kön-

[1] Europäische Kommission gegen Bundesrepublik Deutschland (C-518/07 vom 09. März 2010); Europäische Kommission gegen Republik Österreich (C-614/10 vom 16. Oktober 2012); Europäische Kommission gegen Ungarn (C-288/12 vom 08. April 2014).

[2] Der Begriff „europäische Länder" umfasst nicht nur die Länder der Europäischen Union und des EWR, sondern auch Mitgliedstaaten des Europarates.

nen, so dass sie das angestrebte hohe Datenschutzniveau so wirksam wie möglich in der Praxis umsetzen können.

3. **Erinnert die europäischen Datenschutzbehörden** an die Notwendigkeit:

- **ihre Anstrengungen zu erneuern** mit Blick auf die Sensibilisierung der Öffentlichkeit für Datenschutzrechte und auf die Sichtbarkeit der Arbeit der Datenschutzbehörden unter Berücksichtigung der steigenden Anforderungen und Herausforderungen;

- **geeignete Methoden** zur bestmöglichen Nutzung ihrer begrenzten Ressourcen zu wählen, um wirkliche Ergebnisse für den Datenschutz der Einzelnen zu erzielen, insbesondere im Hinblick auf die Förderung der Entwicklung einer datenschutzfreundlichen digitalen Zukunft mittels technologisch integrierter Vorkehrungen zum Schutz der Privatsphäre;

- **der Zusammenarbeit** mit Dritten, einschließlich partnerschaftlicher Teilhabe unter den europäischen Datenschutzbehörden, mit der Internationalen Konferenz und anderen Dritten – etwa anderen Regulierungsbehörden, um sicherzustellen, dass das Thema Datenschutz so weit wie möglich durch die Arbeit anderer vorangebracht und ergänzt wird;

- **der Förderung** der Entwicklung datenschutzfreundlicher Mechanismen wie Datenschutzsiegel und Verhaltenskodizes zur Förderung der Befolgung und der guten Praxis – zur Ermöglichung eines „Strebens nach oben“ und zur Schaffung von Datenschutzvorschriften;

- **der Entwicklung** eines systematischen und proaktiven Ansatzes zur Bekämpfung von pflichtwidrigem Verhalten der für die Verarbeitung verantwortlichen Stellen, deren Tätigkeiten die größte Bedrohung für die Datenschutzrechte der Bürger darstellen;

- **der umso schnelleren Reaktion** auf neue Technologien und deren Auswirkungen auf den Datenschutz. Dies umfasst die kontinuierliche Entwicklung und den Austausch des internen technischen Fachwissens;

- **der Entschlossenheit**, wenn es um die Ressourcen für die Datenschutzbehörden geht, die diese zur effektiven Gewährleistung eines hohen Datenschutzniveaus für die Einzelnen benötigen. Dies umfasst die kontinuierliche Einflussnahme auf die Diskussion über das EU-Datenschutz-Reformpaket sowie auf Diskussionen über die Aktualisierung des Übereinkommens des Europarats Nr. 108 auf der Grundlage, dass die Gesetzgeber den Datenschutzbehörden bei der Wahrung der Grundrechte auf Privatsphäre und Datenschutz keine neuen Aufgaben auferlegen sollten, ohne ihnen gleichzeitig die vollständige Erfül-

lung dieser Aufgaben durch die Bereitstellung der erforderlichen Befugnisse und Ressourcen zu ermöglichen; und

- **der weiteren Entwicklung** von Initiativen, wie die Untergruppe für die Zusammenarbeit [Subgroup on Cooperation] der Artikel 29-Datenschutzgruppe und der Arbeitsgruppe der Frühjahrskonferenz für die Europäische Zusammenarbeit, die den Austausch von Informationen, Kenntnissen und Untersuchungen über praktische Herangehensweisen ermöglichen, die für die Datenschutzbehörden bei der Bewältigung ihrer zahlreichen Herausforderungen, mit denen sie konfrontiert werden, hilfreich sind.

IV. Internationale Konferenz der Datenschutzbeauftragten

37. Konferenz, 26.–28. Oktober 2015, Amsterdam

Entschließung zu Transparenzberichten

– Übersetzung –

Die 37. Konferenz der Datenschutzbeauftragten:

a) *Im Anschluss* an und aufbauend auf der Entschließung zur Offenheit von Datenverarbeitungspraktiken, die bei der 35. Internationalen Datenschutzkonferenz 2013 in Warschau verabschiedet wurde[1];

b) *im Anschluss* an die Gemeinsame Erklärung der Europäischen Datenschutzaufsichtsbehörden, versammelt in der Art. 29-Gruppe vom 26. November 2014[2];

c) *ebenfalls im Anschluss* an die Entschließung zur Massenüberwachung, die bei der Generalversammlung der französischsprachigen Vereinigung der Datenschutzbehörden im Juni 2015 in Brüssel angenommen wurde[3];

d) *ebenso mit Bezug auf* das kürzlich beschlossene Arbeitspapier der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation („IWGDPT“) zu „Transparenzberichten: Förderung der Rechenschaftspflicht staatlicher Stellen beim Zugriff auf personenbezogene Daten, die sich im Besitz von Unternehmen befinden“ vom April 2015[4];

e) *angesichts der Tatsache*, dass der Zugriff staatlicher Stellen auf personenbezogene Daten bei Unternehmen zunehmend Gegenstand von Kontroverse und Bedenken ist, allerdings auch mit Sorge feststellend, dass dieser Zugriff intransparent bleibt angesichts der Geheimhaltung, die die Datensammlung durch Nachrichtendienste und Sicherheitsbehörden umgibt[5];

---

[1] http://icdppc.org/wp-content/uploads/2015/02/Openness-resolution.pdf

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf

[3] Association of Francophone Data Protection Authorities (AFAPDP), “Resolution on mass surveillance” (June 2015) – URL: http://www.cai.gouv.qc.ca/documents/AFAPDP_R%C3%A9solution_Surveillance-de-masse_20150626.pdf; S. auch AFAPDP, “Resolution on openness of Personal Data Practices” (September 2013) – URL: https://www.priv.gc.ca/information/conf2013/res_06_openness_e.asp

[4] Vgl. S. 88

[5] International Principles on the Application of Human Rights to Communications Surveillance, available at https://en.necessaryandproportionate.org

f) *angesichts der Tatsache*, dass Behörden manchmal die Herausgabe personenbezogener Daten von Unternehmen verlangen und dass die Rechtsgrundlage solcher Verlangen eindeutig sein muss,

g) *eingedenk des Umstands*, dass die Antworten der Unternehmen auf solche Herausgabeverlangen von Behörden sich unterscheiden, wobei teilweise eine richterliche Anordnung vor der Auskunftserteilung verlangt wird, während in anderen Fällen die Herausgabe freiwillig erfolgt[6];

h) *in Anerkennung der Tatsache*, dass staatliche Stellen und Unternehmen nicht einheitlich Unterlagen über solche behördlichen Auskunftsverlangen und die erfolgte Reaktion aufbewahren[7;]

i) *angesichts des Umstands*, dass Betroffene zunehmend besorgt darauf reagieren, dass auf personenbezogene Daten, die sie den Unternehmen allein zu dem Zweck überlassen haben, um Zugang zu einem Produkt oder einer Dienstleistung zu erhalten, von Behörden zu Zwecken der Gefahrenabwehr oder Überwachung zugegriffen wird[8;]

j) *in Anerkennung der Tatsache*, dass Unternehmen begonnen haben, Transparenzberichte zu veröffentlichen, allerdings ohne einheitliche und vergleichbare Daten;

k) *unter Hervorhebung* der Bedeutung von Transparenzberichten als eine Methode zur Information der Öffentlichkeit, Förderung der Verantwortlichkeit und Erhaltung des Vertrauens in die digitale Kommunikation und die Online-Umgebung;

Die 37. Internationale Datenschutzkonferenz kommt deshalb überein,

1. die Regierungen aufzufordern, Dokumente über die Zahl, Art und den Zweck von rechtmäßigen Auskunftsverlangen bezüglich personenbezogener Daten bei Unternehmen aufzubewahren;
2. die Regierungen aufzufordern, einheitliche, länderübergreifende Berichte zu entwickeln, um besser in klarer, leicht verständlicher Sprache zu erklären, wie oft und zu welchem Zweck Auskunft über personenbezogene Daten verlangt wird, mit dem Ziel, solche Berichte regelmäßig zu veröffentlichen;

---

[6] Access, "Transparency Reporting Index" – URL: https://www.accessnow.org/pages/transparency-reporting-index

[7] Freedom Online Coalition Working Group, "Privacy and Transparency Online" (May 2015) – URL: https://www.freedomonlinecoalition.com/wp-content/uploads/2015/05/FOC-WG3-Draft-Executive-Summary-May-2015.pdf; see also Telecom Transparency Project, "Governance of Telecommunications Surveillance" (May 2015) – URL: http://www.telecomtransparency.org/portfolio-item/the-governance-of-telecommunications-surveillance/

[8] United Nations High Commissioner for Human Rights, "The right to privacy in the digital age" (June 2014) – URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

3. die Regierungen aufzufordern, rechtliche oder verwaltungstechnische Hindernisse für Transparenzberichte zu beseitigen, ganz gleich, ob es sich um gesetzliche Verbote, Geheimhaltungsvorschriften, technische Standards oder Lizenzbedingungen handelt;
4. die Unternehmen aufzufordern, strenge Überprüfungen, einschließlich interne Untersuchungen und Berichterstattung gegenüber Vorgesetzten durchzuführen, bevor behördlichen Aufforderung zur Auskunft über personenbezogene Daten entsprochen wird, um deren Rechtmäßigkeit sicherzustellen und einheitliche Unterlagen für die Transparenzberichte aufzubewahren;
5. die Unternehmen aufzufordern, sektorübergreifend ihre internen Vorgaben zu dokumentieren und der Öffentlicheit zu erläutern, die sie für den Umgang mit Auskunftsverlangen für Zwecke der Sicherheitsbehörden erlassen haben;
6. die Unternehmen aufzufordern, Transparenzberichte zu veröffentlichen, aus denen sich die Zahl, die Art der Beantwortung und die Rechtsgrundlage von behördlichen Auskunftsersuchen bezüglich personenbezogener Daten ihrer Kunden und Beschäftigten ergibt; und
7. alle Datenschutzbehörden und sonstigen Aufsichtsbehörden für nachrichtendienstliche Tätigkeiten aufzufordern, die vertrauenswürdige, unabhängige und die gegenüber der Öffentlichkeit verantwortliche Beaufsichtigung sicherzustellen, soweit die Befugnis dazu haben.

Die U.S. Federal Trade Commission hat sich bei dieser Entschließung der Stimme enthalten, da sie Angelegenheiten außerhalb ihrer Zuständigkeit betrifft.

Entschließung zum Datenschutz bei internationalen humanitären Rettungsmaßnahmen

– Übersetzung –

Die 37. Konferenz der Datenschutzbeauftragten:

Vor dem Hintergrund, dass humanitäre Rettungsmaßnahmen den Schutz und die Hilfe notleidender Menschen bezwecken, die entweder in bewaffneten Konflikten leben oder anderen Formen der Gewaltanwendung oder Naturkatastrophen (zusammen als humanitäre Krisen bezeichnet) oft in Notsituationen ausgesetzt sind;

in dem Bewusstsein, dass solche Maßnahmen nationale und internationale Anwendungsfelder haben und durch nationales und internationales Recht, insbesondere durch das humanitäre Völkerrecht, das Flüchtlingsrecht und den internationalen Schutz der Menschenrechte geregelt sind;

unter Berücksichtigung der Tatsache, dass humanitäre Maßnahmen Akteure mit unterschiedlichen Aufgaben und Rahmenbedingungen vereinen und dass sie oft erheblicher Anstrengungen zur Koordination bedürfen;

unter Berücksichtigung der Tatsache, dass bestimmte internationale Organisationen eingerichtet worden sind, um spezielle Aufgaben nach dem Völkerrecht zu erfüllen, und unter Berücksichtigung der Vorrechte und Immunitätsregeln, die es ihnen ermöglichen soll, sie auf unabhängige Weise zu erfüllen;

angesichts der Zunahme an humanitären Krisen, in denen immer mehr Menschen humanitäre Hilfe benötigen;

unter Berücksichtigung der Tatsache, dass Datenverarbeitung ein wesentlicher Bestandteil der Aufgabenverfüllung für humanitäre Hilfsorganisationen ist und der zunehmende Einsatz technischer Lösungen im Interesse größerer Effizienz sowohl zu einer Diversifizierung der Datenarten als auch zur Zunahme der Datenflüsse führt;

in dem Bewusstsein, dass zwar einige internationale humanitäre Organisationen kürzlich einen Rechtsrahmen für die Verarbeitung dieser Daten festgelegt haben, die Festlegung solcher Regelungen durch die Gemeinschaft der humanitären Organisationen aber noch selten ist;

eingedenk der Richtlinien betreffend personenbezogene Daten in automatisierten Dateien, die von der Vollversammlung der Vereinten Nationen mit der Entschließung 45/95 vom 14. Dezember 1990 angenommen wurden, und des darin enthaltenen humanitären Vorbehalts;

eingedenk der Entschließung zu Datenschutz und größeren Naturkatastrophen, die von der Internationalen Datenschutzkonferenz am 1. November 2011 in Mexiko-Stadt beschlossen wurde;

auch in dem Bewusstsein, dass jede Richtlinie zum Datenschutz im Zusammenhang mit humanitären Maßnahmen deren Besonderheiten berücksichtigen muss, um sie nicht zu beeinträchtigen oder zu erschweren, sondern um sie eher zu erleichtern und zu unterstützen;

Die 37. Internationale Konferenz der Datenschutzbeauftragten kommt überein:

1. Die Internationale Konferenz zu verpflichten, bei künftigen Tagungen die Anforderungen des Datenschutzes im Zusammenhang mit humanitären Maßnahmen zu untersuchen;

2. Sich dafür einzusetzen, dass der Wunsch internationaler humanitärer Organisationen nach einer Zusammenarbeit bei der Entwicklung von Richtlinien aufgegriffen wird, wobei die Besonderheiten ihrer Maßnahmen und die Notwendigkeit, sie zu erleichtern, berücksichtigt werden sollten;

3. Den geschäftsführenden Ausschuss mit der Schaffung einer Arbeitsgruppe zu Datenschutz und humanitären Maßnahmen zu beauftragen, die diese Aktivitäten anleiten und koordinieren soll, und die Datenschutz-Netzwerke dazu auffordern soll, aktiv zur Arbeit der Arbeitsgruppe beizutragen.

Die Arbeitsgruppe wird der 38. Internationalen Konferenz berichten.

Begründung:

1. Humanitäre Maßnahmen dienen dem Schutz und der Hilfe verletzlicher Menschen im Zusammenhang mit bewaffneten Konflikten, anderen gewalttätigen Situationen und Naturkatastrophen häufig in Notsituationen (gemeinsam als humanitäre Krisen bezeichnet). Humanitäre Maßnahmen betreffen den nationalen wie den internationalen Bereich und sind durch nationales und internationales Recht geregelt, insbesondere durch das humanitäre Völkerrecht, das Flüchtlingsrecht und den internationalen Schutz der Menschenrechte. Es vereint Akteure mit unterschiedlichen Aufgaben und Rahmenbedingungen und erfordert oft besondere Bemühungen zur Koordinierung.

2. 2015 nahm die Zahl der humanitären Krisen in verschiedenen Weltregionen zu. Eine Rekord-Anzahl von Menschen werden voraussichtlich von humanitärer Hilfe profitieren[1]. Das System der humanitären Hilfe leistet weiterhin dringend benötigte Hilfe. Gleichzeitig stehen Teile des humanitären Systems vor großen Herausforderungen. Akteure in gewalttätigen Situationen sind zahlreicher und unterschiedlicher, einige Gebiete sind unzugänglich, und den humanitären Akteuren fehlen oft die Mittel. Technologien werden zunehmend eingesetzt, um den dringenden Bedarf an an erhöhter Effizienz, einschließlich der Identifikation von Hilfeempfängern, zu befriedigen.

3. Menschen zu identifizieren und personenbezogene Daten zu verarbeiten gehören eng mit der Aufgabenerfüllung bei humanitären Missionen zusammen. Die Einführung von Technologie erhöht die Zahl, die Art und den Fluß der erhobenen Daten. Insbesondere werden diese Daten genutzt, um das Wissen über die Hilfeempfänger zu verbessern, die Effektivität der humanitären Hilfsmaßnahmen zu stärken und den Hilfeempfängern gegenüber Rechenschaft ab-

[1] Nach Angaben des UN-Generalsekretärs hat sich „die Zahl der Menschen, die humanitäre Hilfe auf der Welt brauchen, in gerade einmal zehn Jahren verdoppelt“ (Erklärung v. 20. April 2015, New York) und hat inzwischen etwa 58 Millionen erreicht (The State of Humanitarian Aid, UNOCHA, 2015).

zulegen. Diese Entwicklung kann nützlich sein, wenn sie von hinreichenden Datenschutzgarantien begleitet wird. Wenn dies jedoch nicht geschieht, könnte diese Entwicklung den Schutz der Menschenrechte gefährden.

4. Im Zusammenhang mit humanitären Hilfsmaßnahmen enthalten die erhobenen Daten möglicherweise regelmäßig solche Daten, die im regulären Datenschutz-Kontext als sensitiv anzusehen wären und deren Verarbeitung grundsätzlich entweder verboten oder – falls erlaubt – an strikte Bedingungen und Anforderungen geknüpft wäre. Außerdem können Daten, die unter normalen Umständen nach den Datenschutzgesetzen nicht als sensitiv anzusehen wären, im Zusammenhang mit humanitären Notlagen sehr sensitiv sein.

5. Spezielle Datenschutzrisiken sind festzustellen; dazu zählen auch Überwachungssysteme, die durch Technologien wie Management-Informationssysteme, elektronische Datenübermittlungen, digitale Identitätsfeststellung und Biometrie, Mobiltelefone, aber auch durch Drohnen erhöht werden können. Auf humanitäre Organisationen, die keine Immunität oder diplomatische Vorrechte genießen, könnte Druck ausgeübt werden, um Daten, die für humanitäre Zwecke erhoben wurden, den Behörden zur Verwendung für andere Zwecke zu offenbaren (z. B. zur Kontrolle von Zuwanderung und zur Bekämpfung des Terrorismus). Die Gefahr des Datenmissbrauchs kann schwerwiegende Folgen für den Datenschutz von Flüchtlingen haben und schadet möglicherweise sowohl ihrer Sicherheit als auch den humanitären Maßnahmen im allgemeinen.

6. In den zurückliegenden Jahren sind Arbeitspapiere und Richtlinien zum Datenschutz und zum Schutz der Privatsphäre erarbeitet worden. Darunter diese: Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für eine Verordnung zur Errichtung des European Voluntary Aid Corps (zur Verwaltung der Daten von Freiwilligen, 2012), Professionelle Standards für Hilfstätigkeit, angenommen nach einem vom Internationalen Roten Kreuz geleiteten Konsultationsverfahren (2013), Zur Vorbereitung eines Verhaltenskodex: Richtlinien der GSM Association (Verband der Mobilfunkanbieter) für den Einsatz von SMS in Naturkatastrophen (2013) und die Erklärung des UN-Hochkommissars für Flüchtlinge zum Datenschutz für Flüchtlinge und andere Personen, für die der Hochkommissar verantwortlich ist (2015). Allerdings ist die Festlegung solcher Regelungen durch die Gemeinschaft der humanitären Organisationen insgesamt noch selten.

7. Die Notwendigkeit klarer Richtlinien, die humanitäre Maßnahmen nicht erschweren, sondern eher erleichtern, ist beschrieben worden: „Humanitäre Organisationen brauchen klare Richtlinien und Massstäbe, wie und von wem die Informationen, die sie erheben, verarbeitet, genutzt und gespeichert werden“ (Privacy International (2013) und World Disasters Report (2013). Ein ausführlicher Bericht der Vereinten Nationen (Humanitarianism in the Network Age

(2012)) ruft zur Entwicklung von Massstäben für eine „ethisch vertretbare Verwendung neuer Formen von Daten einschließlich Regelungen zum Datenschutz und zum Schutz der Sicherheit von Informanten."

Die U.S. Federal Trade Commission hat sich bei dieser Entschließung der Stimme enthalten, da sie Angelegenheiten außerhalb ihrer Zuständigkeit betrifft.

Quellen:

- Webseite und Berichte von UNOCHA (http://www.unocha.org/stateofaid/#hubslide-2)
- Webseite des World Humanitarian Summit (https://www.worldhumanitariansummit.org/)
- Data Protection in International Organisations and the New UNCHR Data Protection Policy: Light at the End of the Tunnel?, (http://www.ejiltalk.org/data-protection-in-international-organizations-and-the-new-unhcr-data-protection-policy-light-at-the-end-of-the-tunnel/) A. Beck and C. Kuner, 2015
- Policy on the Protection of Personal Data of Persons of Concern to UNHCR, (http://www.refworld.org/docid/55643c1d4.html) UNHCR, 2015
- Interview: Devenirs humanitaires: quelles évolutions et adaptations du système humanitaire?, (http://www.iris-france.org/61612-devenirs-humanitaires-quelles-evolutions-et-adaptations-du-systeme-humanitaire-international/) IRIS, 2015
- Professional Standards for Protection Work (https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf) carried out by humanitarian and human rights actors in armed conflict and other situations of violence, ICRC, 2013 und Webseite des ICRC (https://www.icrc.org/en/homepage) 2015
- Guidelines for the Use of SMS in Natural Disasters, (http://www.gsma.com/mobilefordevelopment/towards-a-code-of-conduct-guidelines-for-the-use-of-sms-in-natural-disasters) GSMA, 2013
- A paucity of privacy: Humanitarian, development organisations need beneficiary data protection policies, (https://www.privacyinternational.org/node/240) Privacy International, 2013
- Aiding Surveillance, (https://www.privacyinternational.org/?q=node/310) Privacy International, 2013
- Sécurité et traitement des données personnelles, (http://conflits.revues.org/17793) M. Le Rutte, 2009

V. Arbeitspapiere der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. 57. Sitzung am 27./28. April 2015 in Seoul, Republik Korea

Arbeitspapier zum Datenschutz bei tragbaren Endgeräten („Wearables“)[1]

– Übersetzung –

Allgemeiner Hintergrund und Anwendungsbereich

Die Nutzung von tragbaren Endgeräten (im folgenden „wearables“) beschreibt den Einsatz von Rechentechnik, die klein genug ist, um am Körper des Nutzers getragen werden zu können[2]. Diese Geräte weisen verschiedene Arten von Sensoren mit unterschiedlichen Fähigkeiten auf. So haben Sensoren z. B. die Fähigkeit, laufend Informationen über den Körper des Nutzers (Stimmung, Gewohnheiten, körperliche Aktivitäten, Gesundheitszustand, Geschwindigkeit, Mobilität), die Umgebung des Nutzers (Bilder, Geräusche, Temperatur, Feuchtigkeit, Aufenthaltsort, soziale Umgebung) wie auch computer-generierte Daten zur Vermittlung der Nutzererfahrung mit seiner Umwelt zu sammeln.

Viele Wearables enthalten in irgendeiner Form eine Kamera. Auch wenn eine Kamera nur einige der oben genannten Informationen erfassen würde, ist die Kamera-Funktion der Gegenstand vieler aktueller Datenschutz-Bedenken[3]. Es ist die Fähigkeit dieser Geräte, möglicherweise permanent und heimlich Bilder aufzuzeichnen, die zu vielen datenschutzbezogenen Bedenken führt, insbesondere, wenn Dritte derartigen Gegenstand solcher Aufnahmen werden.

---

[1] Dieses Arbeitspapier fußt wesentlich auf dem Bericht der Research Branch of the Office of the Privacy Commissioner of Canada „Wearable Computing: Challenges and Opportunities for Privacy Protection“, January 2014, mit weiteren Nachweisen; https://www.priv.gc.ca/information/researchrecherche/2014/wc_201401_e.asp

[2] Es gibt mehrere unterschiedliche Definitionen des Begriffs „wearable computing“. S. z. B. Steve Mann, (1996a): Smart Clothing: The Shift to Wearable Computing. In Communications of the ACM, 39 (8) pp. 23–24. Siehe Mann, Steve (2014): Wearable Computing. In: Soegaard, Mads and Dam, Rikke Friis (eds.). The Encyclopedia of Human-Computer Interaction, 2nd Ed., Aarhus, Denmark: The Interaction Design Foundation. Online verfügbar unter https://www.interactiondesign.org/encyclopedia/wearable_computing.html, gesehen am 11. März 2015. S. auch Webopedia, „wearable computing“, http://www.webopedia.com/TERM/W/wearable_computing.html) oder dictionary.com, „wearable computer“, http://dictionary.reference.com/browse/wearable+computer).

[3] Donald Melanson and Michael Gorman, “Our augmented selves: The promise of wearable computing.” Engadget. December 12, 2012. Gesehen am 8. Juli 2013.

Gegenwärtig gibt es vier Hauptbereiche auf dem Markt für Wearables[4]:

a) Geräte zur Beobachtung der Fitness, des Wohlbefindens und des Lebens (z. B. smarte Kleidung oder Sportbrillen, Aktivitätsmonitore, Schlafsensoren), die immer beliebter für diejenigen werden, die viele Aspekte ihres Lebens aufzeichnen möchten;[5]

b) Infotainment (z. B. smarte Armbanduhren, Headsets zur „Erweiterung" der Realität (augmented reality), smarte Brillen;[6]

c) Gesundheitsversorgung und medizinische Anwendungen (z. B. dauerhafte Kontrolle des Blutzuckerspiegels, Biosensoren als Pflaster);[7] und

d) Industrie, Polizei und Militär (z. B. Handterminals, am Körper angebrachte Kameras, Headsets für „erweiterte" Realität).[8]

Die Bereiche c) und d) werden in diesem Arbeitspapier nicht behandelt. Auch wenn dieses Arbeitspapier den Bereich c) – Gesundheitsversorgung und medizinische Anwendungen – nicht behandelt, ist anerkannt, dass Daten im Bereich a) – Fitness, Wohlbefinden und Beobachtung des Lebens – als Gesundheitsdaten angesehen werden können[9].

Das Zeitalter der Wearables schafft neue oder vergrößert bestehende Risiken für die Privatsphäre in der mobilen Umgebung, indem zusätzliche und möglicherweise sensitive personenbezogene Informationen in unauffälliger oder verdeckter Weise gesammelt werden. Informationen in Echtzeit über jemandes Stimmung, körperliche Fitness und Gesundheitszustand unterfallen wahrscheinlich dem Begriff der personenbezogenen Daten. Auch Informationen über eine

---

[4] „Wearable Technology Market – Global Scenario, Trends, Industry Analysis, Size, Share And Forecast, 2012 – 2018." Market Research Reports Biz. January 2013. Gesehen am 13. Juni 2013.

[5] Emily Waltz, „How I Quantified Myself: Can self-measurement gadgets help us live healthier and better lives?" IEEE Spectrum, August 30, 2012. Nachweis bei Steve Mann. „Steve Mann: My "Augmediated" Life." IEEE Spectrum. March 1, 2013. Gesehen am 14. Juni 2013.

[6] Zu den Beispielen von Wearables in dieser Kategorie gehören Google Glass (www.google.com/glass/start), Oculus Rift (www.oculus.com, gekauft von Facebook, Google Cardboard (https://developers.google.com/cardboard/), und Samsung's Gear VR (http://www.samsung.com/global/microsite/gearvr/gearvr_specs.html).

[7] Siehe Vital Connect's HealthPatch. Gesehen am 6. Januar 2014

[8] Kopin's Golden-i-Gerät wird entwickelt, um Live-Video-Streaming, mobilen Internet-Zugang, GPS-Navigation und freihändige Bedienung für Kundendienstmitarbeiter, Polizisten, Notärzte und Feuerwehrleute zu ermöglichen. Weitere Informationen unter www.mygoldeni.com/home/.

[9] Die Art.-29 Arbeitsgruppe hat festgestellt, dass es bei manchen Datenverarbeitungen bei Gesundheits- und Lifestyle-Apps und –Geräten schwierig sein kann, festzustellen, ob Gesundheitsdaten verwendet werden oder nicht – der sog. Graubereich – vgl. Brief mit Anhang der Art. 29 Arbeitsgruppe an die Europäische Kommission, DG CNECT, zum Health vom 5.2.2015; http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf (Brief) und http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocu-ment/files/2015/20150205_letter_art-29wp_ec_health_data_after_plenary_annex_en.pdf (Anhang)

gesunde Person (z. B. Herzschlag) können als sensitiv angesehen werden. Die Unterschiede zwischen einem Smartphone und vielen anderen tragbaren Geräten (Wearables) sind eher graduell als substanziell, aber es handelt sich um wichtige Unterschiede aus der Sicht des Datenschutzes.

Bei tragbaren Endgeräten scheint die Rechentechnik in der Kleidung, in Brillen und Uhren und schließlich unter der Haut zu verschwinden, wobei viele herkömmliche Hinweise entfallen, die den Einzelnen darauf hinweisen, dass solche Endgeräte vorhanden sind und verwendet werden. Dies führt zu einem zunehmenden Transparenzdefizit und erhöht in der Konsequenz die Schwierigkeit für Nutzer und andere Betroffene, informierte Auswahlentscheidungen zu treffen. Außerdem sind viele Wearables mit der Verpflichtung verbunden, mit dem Hersteller der Hardware, des mobilen Betriebssystems oder mit Anbietern von Cloud-Diensten Verbindung aufzunehmen. Dies kann dazu führen, dass der Betroffene die Kontrolle über die gesammelten personenbezogenen Daten verliert.

Es bleibt schwierig, in der Mobilkommunikation mit kleinen Displays und unregelmäßiger Aufmerksamkeit des Nutzers aussagekräftige Informationen über Datenschutz-Einstellungen zu vermitteln. Diese Design-Eigenschaften erhöhen die Schwierigkeit, Nutzern Informationen über ihre Datenschutzrechte, in verständlicher Form und so rechtzeitig zu geben, dass sie informierte Entscheidungen treffen können. Der Einsatz von Wearables verstärkt diese Herausforderungen.

Empfehlungen

Die Arbeitsgruppe empfiehlt:

- Die Verarbeitung personenbezogener Daten in und durch Wearables sollte so transparent wie möglich für den Nutzer und andere Betroffene erfolgen; bei versteckten oder miniaturisierten Geräten sollte Transparenz durch andere als visuelle Mittel sichergestellt werden. Dazu zählt auch die Transparenz der Verbindungen zu Zusatzgeräten wie Smartphones.

- Als Grundeinstellung sollten personenbezogene Daten unter der Kontrolle der Person verarbeitet werden, die das Gerät trägt. Es sollte keine Pflicht zur Herstellung einer Verbindung mit den Servern der Hard- oder Software-Hersteller, zu Plattformen oder Cloud-Diensteanbietern geben.

- Die Übermittlung oder Offenbarung von Daten setzt die klare Signalisierung gegenüber dem Nutzer des Geräts und seine informierte und ausdrückliche Einwilligung voraus.

- Die Rechte des Betroffenen, namentlich die auf Auskunft, Berichtigung und Löschung, sind zu respektieren. Insbesondere sollten Betroffene eine Möglichkeit haben, die Richtigkeit der von dem Wearable erzeugten Daten oder die auf ihrer Grundlage vorgenommene Analyse wirksam überprüfen zu lassen.

- Alle Produkte und/oder Dienste sollten vom Grundsatz der Nutzerkontrolle ausgehen. Dies sollte unter anderem einschließen:

  – Die Möglichkeit, die Funktionalität des Gerätes zu verändern (z. B. indem die Unterhaltung von Audio auf Text umgestellt wird, um den Datenschutz zu erhöhen (dynamische Nutzerkontrolle)).

  – Die Möglichkeit, die Erhebung ihrer personenbezogenen Daten vorübergehend von Fall zu Fall zu stoppen (z. B. für bestimmte Zeiträume und/oder Aktivitäten, in oder bei denen sie nicht beobachtet werden wollen).

  – Die Möglichkeit, die Granularität der Daten auszuwählen oder zu kontrollieren, die verarbeitet oder Dritten übermittelt werden.

- Einzelne sollte die Möglichkeit haben, ihre Zustimmung zur Datenoffenbarung jederzeit zu widerrufen. Sie sollten auch die Wahl haben, zur lokalen Speicherung zu wechseln (z. B. auf einem Smartphone oder einem anderen Gerät unter der Kontrolle des Nutzers) und ihre Daten zu sichern.

- Mittel zur Gewährleistung der Portabilität der Daten sollten bereitgestellt werden.

- Die Nutzung von Wearables am Arbeitsplatz wirft zusätzliche Fragen bezüglich der Wahlfreiheit der Beschäftigten auf. Beschäftigte, die sich gegen die Teilnahme an Programmen unter Einsatz von Wearables entscheiden, sollten deshalb keine Nachteile haben.

- Wenn Daten, die durch oder auf Wearables verarbeitet werden, als Gesundheitsdaten anzusehen sind, sollte ihre Weiterverarbeitung nur mit ausdrücklicher Einwilligung der Betroffenen zugelassen werden.

Zusätzlich zu diesen Empfehlungen unterstützt die Arbeitsgruppe die entsprechende Berücksichtigung der Empfehlungen in der Stellungnahme 8/2014 der Art.29-Arbeitsgruppe zu neuen Entwicklungen beim Internet der Dinge (WP 223).[10]

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_de.pdf; S. 21 ff.

Hintergrund zu den Empfehlungen[11]

Eigenschaften des Einsatzes von Wearables

Viele Wearable-Technologien, die gegenwärtig entwickelt werden oder schon auf dem Markt sind, haben verlockende Eigenschaften, die zu breiter Akzeptanz bei den Verbrauchern beitragen könnten. Beispielsweise:

a) sind sie äußerlich ansprechend gestaltet;

b) können sie nahtlos in die Kleidung integriert oder in den Körper des Nutzers implantiert werden;

c) können sie personalisiert und den Bedürfnissen des Nutzers angepasst werden und können Rückmeldungen geben;

d) können dem Nutzer nützliches Feedback geben, entweder in Echtzeit oder nicht, und direkt oder durch ein anderes intelligentes Endgerät (typischerweise ein Smartphone);

e) können die körperlichen oder geistigen Fähigkeiten des Nutzers ergänzen;

f) sind verhältnismäßig preisgünstig für den durch sie erzielten Nutzen;

g) sind handlich und bieten eine große Breite von Einsatzmöglichkeiten im persönlichen Bereich oder am Arbeitsplatz; und

h) sind verhältnismäßig einfach vom Verbraucher einzurichten und zu verwenden.

Ständige Interaktion zwischen dem Nutzer und dem Endgerät, wobei dieses „lernt", was der Nutzer erlebt, während er es erlebt, und das Darüberlegen zusätzlicher Informationen zu dieser Erfahrung sind ein Ziel der gegenwärtigen Gestaltung von Wearables.

Konsequenzen für den Datenschutz

In einer kürzlich von der Industrie finanzierten Meinungsumfrage zu den Implikationen von Wearables in Großbritannien und den USA nannten 51 % der Befragten den Datenschutz als Hindernis für den Einsatz, und 62 % waren der Auffassung, dass Google Glass und andere Wearables in irgendeiner Form reguliert werden sollten, während 20 % für ein vollständiges Verbot dieser Geräte eintraten. Forrester Research ist zu dem Schluss gekommen, dass das Potenzial der Wearables nur ausgeschöpft werden kann, wenn die Nutzer die Kontrolle über ihre eigenen Daten erhalten, wie beispielsweise entscheiden zu können, ob sie die Daten weitergeben wollen oder nicht.

[11] Dieser Teil beruht weitgehend auf dem in FN 1 genannten Forschungsbericht.

Herausforderungen für das bestehende Einwilligungsmodell

Informationen, die von Sensoren in miteinander verbundenen Objekten gesammelt werden, sei es, dass diese Objekte von einzelnen Personen getragen oder einfach mitgeführt werden, können eine gewaltige Menge an Daten erzeugen, die verknüpft, analysiert und zur Entscheidungsgrundlage gemacht werden können, ohne dass eine angemessene Transparenz, Verantwortlichkeit oder eine echte Einwilligung gegeben sind.

Diese Entwicklungen stellen grundlegende Herausforderungen für bestehende Datenschutzregeln weltweit dar. So ist es z. B. zunehmend schwierig, den Grundsatz der Zweckbindung, der die Erhebung von personenbezogenen Daten begrenzen soll, soweit nicht die Einwilligung für die Verwendung für bestimmte andere Zwecke vorliegt, in einer Welt von allgegenwärtiger Rechentechnik und mobilen Endgeräten anzuwenden. Darüber bleibt es schwierig, eine wirksame Einwilligung durch mobile Endgeräte einzuholen. Es muss mehr getan werden, um Nutzern in kreativer und aussagekräftiger Weise zu zeigen, was tatsächlich mit ihren personenbezogenen Informationen geschieht.

Neue Überwachungsmöglichkeiten

Einige Wearables sammeln Fotos, Videos, Geräusche, Orte und nehmen die allgemeine Umgebung des Gerätes auf, einschließlich der umstehenden Menschen und benachbarten Geräte. Die in mehreren dieser Wearables enthaltene Kamera wirft zahlreiche Datenschutzfragen auf. Preisgünstige, vielfältige Alltagsgegenstände wie Baseball-Mützen, MP3-Spieler und Hemdknöpfe sind mit versteckten Kameras erhältlich. Viele dieser Gegenstände können permanent und verdeckt aufzeichnen.

Über die Kamera hinaus jedoch ist eine neue Generation von Fitness-Trackertechnologie gerade dabei, Krankenversicherungen und Arbeitgebern neue Einblicke in unseren Gesundheitszustand und unser Verhalten zu geben. Eine Reihe von Versicherungen und Arbeitgebern in Nordamerika nutzen Tracking-Technologie, um ihre Versicherten und Arbeitnehmer zu überwachen und bieten ihnen finanzielle Vergünstigungen als Gegenleistung für Daten über körperliche Aktivitäten an. In Europa beginnen Versicherungen, ähnliche Verträge anzubieten.

Weitere derartige Entwicklungen sind zu erwarten. Der entstehende Bereich der „Physiolytics“[12] wird Wearables mit Big Data-Analysen verknüpfen, um Rückmeldungen und ein Empfehlungssystem für Verhaltensänderungen anzubieten.

[12] H. James Wilson, Wearables in the Workplace, Harvard Business Review, September 2013, https://hbr.org/2013/09/wearables-in-the-workplace/ar/1

Die Aggregierung von durch Wearables erhobenen Daten

Wir werden Zeugen einer neuen Generation von Herausforderungen für den Datenschutz, die aus der Verknüpfung von scheinbar belanglosen und nicht-sensitiven Splittern von personenbezogenen Informationen zur Ableitung von Einsichten in persönliches Verhalten entstehen. Wir wissen auch, dass die Verknüpfung von unzusammenhängenden Informationspartikeln, die aus verschiedenartigen Quellen gewonnen werden, zur Bildung detaillierter Profile führen kann, die einzelnen Personen zuzuordnen sind. Es ist bereits schwierig für Einzelne, informierte Entscheidungen darüber zu treffen, ob sie personenbezogene Informationen offenbaren wollen, weil sie nicht völlig absehen können, wie ihre Informationen zukünftig verknüpft und verwendet werden können. Wearables, die ständig Daten sammeln, verarbeiten und versenden, werden dieses Problem wahrscheinlich noch verschärfen.

Beschleunigung des Kontextverlusts

Menschen versuchen möglicherweise, die verschiedenen Bereiche ihres Lebens, seien es verschiedene soziale Zusammenhänge, in denen sie sich befinden, oder einfach Beruf und Privatleben, voneinander getrennt zu halten. Soziale Medien und die Online-Umgebung haben allgemein unsere Fähigkeit beeinträchtigt, diese Unterscheidung aufrechtzuerhalten. Diese Auflösung, die Sozialwissenschaftler als „Kontextverlust" bezeichnen, könnte beschleunigt werden durch Sensoren, die immer eingeschaltet sind und ständig mit dem Körper des Nutzers und anderen Geräten in der Umgebung des Nutzers interagieren.

Neue Methoden der Authentisierung, neue personenbezogene Informationen

Der Einsatz von Wearables kann so gestaltet werden, dass personenbezogene Informationen datenschutzgerecht und sicher verarbeitet werden. So wird gegenwärtig in Forschungsprojekten untersucht, wie Daten, die von Sensoren in gegenwärtig verfügbaren Smartphones erzeugt wurden, zur Identifikation und Authentisierung von Personen genutzt werden können, die ihr Smartphone bei ihren täglichen Aktivitäten bei sich führen.

Das bedeutet, dass bereits das Gehen, Joggen, Klettern und das Hinabgehen von Treppen mit einem Smartphone in der Tasche biometrische Signaturen des Nutzers erzeugen können. Obwohl dies die Sicherheit durch Authentisierung des Nutzers verbessern kann, führt es gleichzeitig zu neuen Risiken für die Privatsphäre.

Design-Überlegungen

Dynamische Nutzer-Kontrolle

Gegenwärtige Überlegungen zum Begriff der Privatheit legen es nahe, sie als einen dynamischen Zustand zu begreifen, weil die soziale und kulturelle Umgebung des Einzelnen sich ständig ändert. Eine Konstellation kreativer Auswahlmöglichkeiten sollte untersucht werden, um der Einwilligung abhängig von den jeweiligen Umständen und Vorlieben mehr Bedeutung zukommen zu lassen und um ein Übermaß an Auswahlentscheidungen bei der Nutzung von Wearables zu begrenzen. So sollten beispielweise Vorarbeiten geleistet werden, um

a) dynamisch kalibrierte Datenschutzregeln zu entwickeln, um den Bedürfnissen und Erwartungen Betroffener bezüglich des Datenschutzes zu entsprechen;

b) einfache Gestaltungselemente zu integrieren, so dass das tragbare Gerät (Wearable) die Datenschutzpräferenzen des Einzelnen widerspiegeln kann;

c) um verantwortliche Stellen dazu aufzufordern, ihre Datenschutzerklärungen um dynamische und interaktive Datenkarten und Infografiken zu erweitern, um die Beziehungen im Ökosystem der Wearables zu verdeutlichen.

Die Gestaltungsanforderungen für die Interaktion mit dem tragbaren Gerät werden Einfluß auf den Datenschutz des Nutzers haben. So führt die Nutzung eines Wearable mittels Sprachsteuerung zu ähnlichen Datenschutzproblemen wie ein in der Öffentlichkeit geführtes Telefonat. Die Möglichkeit des Nutzers zur Verhaltensänderung, vielleicht durch Umstellung der Unterhaltung von Sprach- auf Textkommunikation, wäre eine interessante Anpassung des Designs zur Verbesserung des Datenschutzes.

Entstehende Transparenz-Modelle

Es gibt beim Einsatz von Wearables Chancen und Herausforderungen für die Transparenz. So können Wearables, die die Sehkraft, das Gehör oder andere Sinne nutzen, enger mit dem Nutzer verbunden werden, so dass es in gewisser Weise leichter sein kann, die unmittelbare Aufmerksamkeit des Nutzers zu gewinnen. Auf diese Weise kann es leichter sein, Zustimmung und Information zum inneren Bestandteil des Designs eines Wearables zu machen als bei einem Smartphone. Die Gestaltung mancher Wearables setzt überhaupt keine Displays voraus, deshalb müssen neue Verfahren zur Aushandlung von Privatheit entwickelt werden.

Der Datenschutz der Nutzer ist eine Seite, aber der Datenschutz der Menschen in der Umgebung des Nutzers ist ein anderes und vielleicht schwierigeres Problem.

Es ist bereits schwierig zu wissen, wann jemand ein Smartphone oder anderes Gerät zur Aufnahme von Ton oder Bild benutzt. Im Fall von Wearables, bei denen die Computer noch nahtloser in belanglose Gegenstände integriert werden, wie Gestelle für alltägliche Brillengläser, wird die Fähigkeit anderer, die Sammlung von Daten über sie zu bemerken oder zu kontrollieren stark reduziert.

Auskunft über Daten und Kontrolle der Richtigkeit bei automatisierten Entscheidungen

Die Frage der Auskunft über personenbezogene Daten ist direkt mit der Transparenz verbunden. Es ist nicht offensichtlich, wie Betroffene feststellen können, was durch ein Wearable erhoben wird, von wem es erhoben wird und wie es genutzt und weitergegeben wird. Nutzer müssen die Möglichkeit haben, die von Institutionen als Grundlage für deren Entscheidungen gesammelten Informationen zu überprüfen, da deren Richtigkeit nicht garantiert ist.

Eine neuere Untersuchung einiger fitness-bezogener Wearables bezweifelte die Zuverlässigkeit der Messung des Kalorienverbrauchs bei wenig intensiven Tätigkeiten wie Stehen oder Saubermachen. Ungenauigkeiten bei der Erhebung solcher Daten können reale Folgen für die Nutzer dieser Geräte haben. Beispielsweise können ungenaue Messergebnisse einer neuen Methode zur Früherkennung von Alzheimer, bei der die Bewegungen von Patienten mit einem Beschleunigungsmessgerät bewertet werden, die Diagnose und Versorgung des Patienten beeinflussen. Ungenaue Messergebnisse können auch Probleme am Arbeitsplatz auslösen, wenn ein Arbeitgeber sich auf solche Geräte bei der Messung der Produktivität des Arbeitnehmers verlässt. Es wäre ein wichtiges Element der Gestaltung von Wearables, wenn die Betroffenen die Möglichkeit haben, die Richtigkeit der mit solchen Geräten erhobenen Daten oder der darauf basierenden Analyse wirksam zu überprüfen.

Sicherheitslücken

Wearables ohne angemessene Sicherheits- und Authentisierungssysteme sind angreifbar. Kompromittierte Geräte können nicht nur die personenbezogenen Informationen und den Ruf eines Nutzers gefährden, sondern auch seine Gesundheit. So könnte etwa das Abhören oder das Simulieren einer Insulin-Pumpe gravierende Folgen für die Gesundheit des Einzelnen haben. Wie ein Kommentator formulierte, „ist die Sicherheit Deiner persönlichen Daten nur so stark wie das schwächste Glied im Öko-System Deiner Selbstvermessung."

Arbeitspapier zu Transparenzberichten:
Förderung der Rechenschaftspflicht staatlicher Stellen beim Zugriff auf personenbezogene Daten, die sich im Besitz von Unternehmen befinden

– Übersetzung –

„Doveryai, no proveryai."
– Von Ronald Reagan zitiertes russisches Sprichwort, das so viel bedeutet wie „Vertraue, aber prüfe nach."

„Sind alle Einzelheiten bekannt, ist der Kopf zufrieden und die Fantasie verliert den Drang, ihre eigenen Flügel zu nutzen."
– Thomas Bailey Aldrich, amerikanischer Dichter und Schriftsteller

„Der Geheimhaltungscharakter der Sicherheitsüberwachung hindert vielerorts die Legislative, Judikative und die Öffentlichkeit an der Überprüfung staatlicher Befugnisse. Diese mangelnde Transparenz […] führt zu wesentlichen Hindernissen bei der Vermeidung einer willkürlichen oder unbedachten Nutzung dieser Befugnisse."
– Navi Pillay, Hohe Kommissarin der Vereinten Nationen für Menschenrechte

Inhalt

Dieses Papier untersucht den Nutzen der Erstellung von Transparenzberichten durch Telekommunikationsunternehmen und Anbieter von Internetdienstleistungen für den Datenschutz und die Privatsphäre. Transparenzberichte sind nützlich, um das Vertrauen in Organisationen mit großen Beständen an personenbezogenen Daten zu fördern. Sie tragen zudem dazu bei, öffentliche Stellen für ihre Praktiken bei Auskunftsbegehren in Bezug auf diese Daten zur Rechenschaft zu ziehen.

In diesem Papier bezeichnet „Transparenzbericht" die regelmäßige Veröffentlichung von Statistiken und begleitenden Erläuterungen durch für die Verarbeitung Verantwortliche oder Auftragsverarbeiter darüber, welche personenbezogenen Daten für unternehmensfremde Zwecke an Dritte weitergegeben wurden. Der Schwerpunkt dieses Papiers liegt auf der Weitergabe an Ordnungsbehörden[1] sowie nationale Sicherheitsbehörden, ohne andere Formen der unternehmensfremden Weitergabe auszuschließen.[2]

[1] Im Sinne dieses Papiers sind unter „Ordnungsbehörden" sowohl Aufsichtsbehörden als auch Strafverfolgungsbehörden zu verstehen. In vielen Rechtssystemen versuchen Aufsichtsbehörden, Ministerien und Kommunalverwaltungen häufig, Zugang zu Daten zu erhalten, die sich im Besitz von Unternehmen befinden.

[2] Ein anderes Beispiel ist etwa die Weitergabe im Zuge von Notfällen oder bei Sicherheitsvorfällen.

Obwohl sich das Papier hauptsächlich auf die Berichte von Organisationen des privaten Sektors im Bereich der Telekommunikation konzentriert, können die Beobachtungen und Empfehlungen des Papiers auch für öffentliche Stellen und außerhalb des Telekommunikationssektors tätige Organisationen relevant sein.[3]

Nicht direkt eingegangen wird in diesem Papier auf damit zusammenhängende Themen, wie die Rechtfertigungsgründe für den Zugriff durch Ordnungsbehörden oder nationale Sicherheitsbehörden auf die Akten oder Daten von Organisationen, die angemessenen gesetzlichen Grenzen für einen solchen Zugriff oder die Genehmigung und Kontrolle eingriffsintensiver Überwachungsmaßnahmen seitens der Ermittlungsbehörden.[4] Diese Themen werden in einigen anderen Arbeitsgruppenpapieren behandelt und es könnte hilfreich sein, diese in Verbindung mit diesem Papier zu lesen.[5]

Die Arbeitsgruppe unterstützt die Erstellung von Transparenzberichten, da diese das Potenzial haben, die Rechenschaftspflicht bei der Verarbeitung personenbezogener Daten zu fördern. Organisationen, die Transparenzberichte verfassen, sollten sicherstellen, dass die veröffentlichten Statistiken zuverlässig, informativ und international vergleichbar sind.[6]

Hintergrund

Um ihre öffentlichen Aufgaben wahrzunehmen, muss es staatlichen Stellen bei Bedarf möglich sein, auf Daten zuzugreifen, die sich im Besitz von privaten Organisationen befinden.[7] Ein klassisches Beispiel ist die Überprüfung der Unterlagen eines Unternehmens, um sicherzugehen, dass die Steuern korrekt bezahlt wurden. Die staatliche Nachfrage nach Unterlagen in privatem Besitz steigt seit

[3] Zum Beispiel für den Finanzdienstleistungsbereich oder für Kreditauskunfteien.

[4] Für eine Diskussion vieler der allgemeinen Aspekte aus dem Bereich Datenschutz siehe Centre for Democracy and Technology, *Systematic Access to Government Data: A Comparative Analysis*, 2013. Frühere Fallstudien zum systematischen staatlichen Zugriff auf Daten des privaten Sektors sind verfügbar unter http://idpl.oxfordjournals.org/content/2/4.toc.

[5] Alle Arbeitspapiere der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation (IWGDPT) sind zu finden unter http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group. Siehe z. B. das Arbeitspapier der IWGDPT mit dem Titel Recht auf vertrauliche Telekommunikation (Berlin, September 2013) sowie die „Granada Charta" des Datenschutzes in einer digitalen Welt (Granada, April 2010).

[6] Während Unternehmen oft freiwillig Berichte vorlegen, kann es auch Rechtssysteme geben, in denen spezifischere Anforderungen an die Berichterstattung und deren Form gestellt werden. Solche Anforderungen haben natürlich gegenüber den allgemeinen Leitlinien in diesem Papier Vorrang. Größtmögliche internationale Vergleichbarkeit bleibt zwar wünschenswert, aber zusätzliche, lokal gestellte Anforderungen können trotzdem einen wertvollen Beitrag zur Förderung einer besseren Vergleichbarkeit innerhalb von Branchen und einzelnen Rechtssystemen leisten.

[7] Der Einfachheit halber werden diese im vorliegenden Papier als Informationen bzw. Unterlagen „in Firmenbesitz" bezeichnet. Dadurch soll betont werden, dass der Schwerpunkt in erster Linie auf staatlichen Anfragen an für die Verarbeitung von Daten Verantwortliche im nicht-öffentlichen Bereich oder an Auftragsverarbeiter liegt.

Jahrzehnten stetig und gibt somit Anlass zu Besorgnis hinsichtlich der bürgerlichen Freiheiten und des Erfüllungsaufwands.

Umfang und Volumen staatlicher Nachfrage nach Zugriff auf Informationen in Firmenbesitz, insbesondere Informationen über Einzelpersonen, sind seit 2001 erheblich gewachsen. Dieses Wachstum spiegelt die wachsende Attraktivität der Daten des privaten Sektors für den Staat wider, die sich aus mehreren technologischen und wirtschaftlichen Faktoren ergibt, zu denen die folgenden gehören:

- *Verfügbarkeit von Daten:* Die Kosten für die Speicherung von Daten sind erheblich zurückgegangen und sinken weiter. Dadurch ist es möglich, große Mengen an Transaktionsdaten langfristig zu speichern.
- *Verarbeitungskapazität:* Es wurden große Fortschritte erzielt, was die Fähigkeit angeht, gewaltige Datenmengen schnell zuzuordnen, zu verarbeiten und zu analysieren. Big Data hat sich zu einem großen Geschäftsfeld entwickelt.[8] [9]
- *Spezialisierte Techniken sind jetzt Mainstream:* Waren viele datenbasierte analytische Verfahren einst einigen wenigen vorbehalten, so sind sie in der Wirtschaft (und Verwaltung) mittlerweile zum Standard geworden. Hierzu gehören etwa prädiktive Analysen, Kontaktketten („contact chaining"), die Visualisierung von Daten und die Netzwerkanalyse.
- *Neue Geschäftsmodelle:* Es haben sich neue und lukrative Geschäftsmodelle entwickelt, die auf der Analyse von Transaktionsdaten und der Verknüpfung von Datensätzen basieren. Anbieter von Cloud-Diensten besitzen Informationen von vielen Unternehmen außerhalb der jeweiligen Firmensysteme.
- *Übergang von mündlicher zu schriftlicher Kommunikation:* Der Wandel von der analogen hin zur digitalen Telefonie führte zur Entwicklung praktischer Datendienste wie SMS. Dadurch wurden die Nutzer motiviert, die nicht dauerhafte mündliche Kommunikation durch schriftliche Mitteilungen zu ersetzen, die langfristig gespeichert werden können. Beschleunigt wurde dieser Trend durch den massenhaften Umstieg auf Handys und Smartphones.
- *Massenhafte Spuren personenbezogener Daten, die Einzelpersonen unbemerkt hinterlassen:* Der Übergang von der analogen zur digitalen Telefonie hat zur Folge, dass mehr Verkehrsdaten anfallen, die gespeichert und analysiert werden können. Durch Smartphones und GPS sind Lokalisierungsdienste entstanden, die sensible Informationen erzeugen, die es zuvor nie gab. Hinzu kommen immer mehr Sensoren und die Entstehung des Internets der Dinge, die – oft ohne menschliches Eingreifen – personenbezogene Daten erzeugen.

[8] Siehe die Arbeitspapiere der IWGDPT zu Big Data und Datenschutz – Bedrohung der Grundsätze des Datenschutzes in Zeiten von Big-Data-Analysen (Skopje, May 2014) sowie zu Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes (Sopot, April 2012).

[9] Siehe 36. Internationale Datenschutzkonferenz (ICDPPC), Entschließung zu Big Data, Mauritius 2014, und 34. Internationale Datenschutzkonferenz (ICDPPC), Entschließung zu Cloud Computing, Uruguay 2012. Die Entschließungen der ICDPPC sind abrufbar unter www.icdppc.org.

- *Nutzergenerierte Inhalte:* Internetdienste und in jüngerer Zeit auch soziale Medien haben das Nutzerverhalten verändert: Viele Menschen veröffentlichen ihre persönlichen und geschäftlichen Daten nun so, dass der Regierungen leicht darauf zugreifen können – mittels Daten der Firmen oder sogar durch die komplette Umgehung betrieblicher Kontrollmechanismen.[10]

Diese technologischen und wirtschaftlichen Faktoren allein können jedoch die Zunahme staatlichen Zugriffe nicht erklären. Weitere Faktoren auf staatlicher Seite sind:

- *Öffentlich-private Verbindungen:* Die Grenzen zwischen dem öffentlichen und dem privaten Sektor sind mittlerweile fließend. Vorgehensweisen aus dem privaten Sektor wurden vom öffentlichen Sektor übernommen. Öffentliche Versorgungsbetriebe, die Zugang zu wichtigen Daten über ganze Kommunen haben, wurden zusammen mit ihren Leistungen und ihrem Datenbesitz privatisiert. Regierungen sind zu Akteuren im Daten-Ökosystem des Privatsektors geworden, sowohl als Datenquelle als auch als Nutzer von Datendiensten. Private Unternehmen haben sich zu maßgeblichen Akteuren der Ermittlungs- und Sicherheitsarbeit entwickelt.
- *Strafverfolgung und nationale Sicherheit:* Seit 2001 besteht seitens der Öffentlichkeit, der Legislative und der Gerichte eine stärkere Bereitschaft dazu, den nationalen Sicherheits- und Strafverfolgungsbelangen Vorrang gegenüber traditionellen Normen der betrieblichen Vertraulichkeit einzuräumen. Das Thema Strafverfolgung hat sich in vielen Bereichen manifestiert, darunter vor allem in der Luftfahrt[11] und auf dem Gebiet der Finanzdienstleistungen.[12] Es gibt nicht mehr nur den klassischen staatlichen Zugriff auf Firmendaten auf Grundlage zielgerichteter Ermittlungen gegen Personen, die unter dem Verdacht stehen, eine Straftat begangen zu haben. Vielmehr werden nun durch die Analyse gewaltiger Datensätze ganze Bevölkerungsgruppen überwacht, um Aktivitäten oder Personen von Interesse ausfindig zu machen. Die Schwelle für die Genehmigung von Überwachungsmaßnahmen ist in vielen Gerichtsbarkeiten gesunken. Gleichzeitig hat sich die Menge von Informationen erhöht, die mit einer einzigen Anordnung gesammelt werden können. In vielen Ländern werden Transaktionsdaten in Systemen zur Massenüberwachung nun zunehmend routinemäßig überwacht und nicht mehr nur auf der Basis einer einzelnen Ermittlung.

[10] Dieses Papier beschäftigt sich nur mit Fällen, in denen es um Informationen in Firmenbesitz geht. Alle Aspekte, die die Privatsphäre und Rechenschaftspflicht im Rahmen eines staatlichen Zugriffs auf öffentlich zugängliche Informationen betreffen oder mit der Umgehung betrieblicher Kontrollen zusammenhängen, werden hier nicht behandelt.

[11] Ein besonderer Schwerpunkt liegt auf Transaktionsinformationen zu Reisenden (oft als „Fluggastdatensätze“ oder „PNR-Daten“ bezeichnet). Siehe 29. ICDPPC, Entschließung zum Schutz von Passagierdaten, 2007.

[12] Besonders Geldwäsche und Terrorismusfinanzierung stehen dabei im Fokus.

- *Neustrukturierung von Telekommunikationsdiensten, um den staatlichen Interessen zu dienen:* Normalerweise haben sich öffentliche Stellen damit begnügt, auf Daten in Firmenbesitz dann zuzugreifen, wenn diese Daten existierten und entsprechende Firmensysteme den Zugriff ermöglichten. In den letzten Jahren haben Regierungen jedoch die Beziehung zwischen dem öffentlichen und dem privaten Sektor neu ausgerichtet. Viele Regierungen haben Gesetze erlassen und Vereinbarungen mit Netzbetreibern getroffen, um für viel Geld die Schaffung von „Hintertüren" vorzuschreiben. Diese soll einen staatlichen Zugriff auf Systeme in den Fällen ermöglichen, in denen ein solcher Zugriff aus unternehmerischen Gründen nicht nötig wäre.[13] [14]
- *Verlagerung von Aufwand vom Staat auf die Unternehmen:* Der Gebrauch herkömmlicher Durchsuchungsbefehle bleibt zwar ein wesentliches Element strafrechtlicher Ermittlungen, hat dem Staat aber eine erhebliche administrative Last auferlegt. Es wurden neue gesetzliche Instrumente entwickelt, die den Aufwand für die Lokalisierung, Sammlung und Erhebung von Daten zum Zwecke staatlicher Kontrolle auf die Unternehmen verlagert.[15]
- *Neuordnung der Speicherungsverpflichtungen zur Erfüllung staatlicher Interessen:* Regierungen haben Unternehmen nicht nur dazu aufgefordert, Informationen, die sich zum Zwecke staatlicher Kontrolle in ihrem Besitz befinden, zu erheben und zu sammeln. Sie haben auch gefordert, diese Daten über einen längeren Zeitraum aufzubewahren (auch wenn dafür keine unternehmerische Notwendigkeit besteht) für den Fall, dass öffentliche Stellenim Rahmen von Ermittlungen auf diese Informationen zugreifen müssen.[16]

Zusammengenommen führen diese Faktoren dazu, dass die Informationen, die sich im Besitz des Privatsektors befinden, eine noch attraktivere Informationsquelle als früher für öffentliche Stellen darstellen. Während Informationen früher nicht vorhanden oder unzugänglich waren, so kann der Staat heutzutage auf einen gewaltigen Informationsbestand zugreifen. Aus staatlicher Sicht ist es praktisch,

[13] Viele Länder fordern, dass digitale Telekommunikationssysteme, die Leistungen für die Öffentlichkeit erbringen, abhörfähig gemacht werden. Dieses Beispiel zeigt eindeutig, dass staatlichen Interessen Vorrang gegenüber dem Schutz der Privatsphäre in der Kommunikation eingeräumt wird. Einige Länder verbieten auch anonyme Handy-Konten.

[14] Staatliche Forderungen nach einer Hintertür sind natürlich nicht neu. Solche Forderungen gab es schon vorher im Zusammenhang mit Post- und Telegrafiesystemen sowie analogen Systemen. Ein derartiger Zugriff war für den Staat früher besonders einfach, als er im Besitz dieser Telekommunikationssysteme war oder nur mit einem einzigen Betreiber zu tun hatte. Dennoch erscheint dieser Trend noch immer beachtenswert, da der Staat nicht einfach nur administrativen Zugang zu Systemen fordert, sondern auch erhebliche und kostspielige Systemänderungen, die Auswirkungen auf viele Unternehmen haben können und manchmal dem legitimen Wunsch der Unternehmen nach der Schaffung sicherer Netzwerke zuwiderlaufen.

[15] Diese Befugnisse werden manchmal als Herausgabe- oder Unterstützungsanordnungen bezeichnet.

[16] Zum Beispiel führen In der Telekommunikationsbranche viele Länder eine Aufbewahrungspflicht für die Speicherung von Verkehrsdaten bei Telefongesprächen ein, auch wenn diese Daten nicht für unternehmerische Zwecke gebraucht werden. Im Bankensektor fordern die meisten Länder die langfristige Aufbewahrung von Kopien der Identifizierungsdokumente für Kundenkonten. Dies ist Teil des „Know-Your-Customer"-Prinzips zur Geldwäschebekämpfung. Im Telekommunikationssektor verbieten manche Länder anonyme Handy-Konten und fordern die Aufbewahrung von Kopien der Identifizierungsdokumente für Kundenkonten.

dass sich die Informationen statt innerhalb einzelner Unternehmen nun im Besitz von Anbietern von Informationsdienstleistungen und in Netzwerken befinden. Interessante Informationen sind oftmals mit zusätzlichen Informationen verknüpft, was ihren Wert steigert. Die unermessliche Menge an verfügbaren Daten hätte früher ein unüberwindbares Hindernis für eine nützliche oder rechtzeitige Analyse dargestellt. Doch die steigende Computerkapazität und Fortschritte bei Verarbeitungsverfahren ermöglichen staatlichen Stellen hochgesteckte Ziele bei der Datenerfassung und bei analytischen Projekten. Aufgrund dieser Änderungen können öffentliche Stellen Informationen nun entweder in großen Mengen sammeln oder nach Belieben darauf zugreifen.

Das Umfeld, in dem solche Projekte entstehen, ist für die staatlichen Interessen immer günstiger geworden. Viele spektakuläre Terroranschläge haben in der Öffentlichkeit Besorgnis hervorgerufen und dienten als Rechtfertigung für Maßnahmen zugunsten der nationalen Sicherheit und Strafverfolgung, mit denen öffentliche Stellen noch stärker auf Daten von Unternehmen zugreifen können.

Seit 2001 wurden zahlreiche Gesetze erlassen, die den Ordnungsbehörden größeren Zugriff auf Informationen ermöglichen, die sich im Besitz von Unternehmen befinden. Normalerweise würden diese Gesetze genau die Grenzen des Zugriffs präzise definieren und die rechtmäßigen Verfahren beschreiben, mittels derer Befugnisse ausgeübt werden können. In der Vergangenheit hätte der Zugriff auf Daten in Firmenbesitz für gewöhnlich eine richterliche Anordnung erfordert. In der elektronischen Umgebung können in Verbindung mit staatlichen Befugnissen neue Paradigmen entstehen. Während die Legislative oft versucht hat, die ursprünglichen Normen zu erhalten, haben die konstante Ausweitung von Gesetzen und Forderungen nach entwicklungsoffener Regulierung zu flexibleren Konzepten geführt, welche wiederum ausnahmslos erweiterte Zugriffsmöglichkeiten zur Folge hatten.[17]

Während das Ausmaß der rechtmäßigen Befugnisse bei Strafverfolgungsbehörden nur gelegentlich unklar ist, ist dies bei Geheimdiensten oder Sicherheitsorganisationen mit einem nationalen Sicherheitsmandat fast immer der Fall. Die Grenzen der Befugnisse und Garantien hinsichtlich der Ausübung von Befugnissen sind, wenn nationale Sicherheitsziele angeführt werden, in der Regel weniger robust oder transparent als im Bereich der Strafverfolgung. Und die Menge an zugänglichen Informationen ist für gewöhnlich viel größer.

Sowohl die Ermittlungen von Strafverfolgungsbehörden als auch das Sammeln von Erkenntnissen über die nationale Sicherheit erfolgen häufig im Geheimen.

[17] Zum Beispiel gibt es weniger strenge Voraussetzungen für den Zugriff auf Metadaten und neue Prozesse zur Echtzeit-Überwachung dynamischer Datenumgebungen. Es ist ziemlich wahrscheinlich, dass die Behörden, die eine flexiblere Rechtssprache suchen, um die Konsequenzen wissen, während die meisten Gesetzgeber nur in sehr begrenztem Maße verstehen, was sie gestatten.

Sobald jedoch die Ermittlungen abgeschlossen sind, herrscht aufgrund der Rolle einer offenen Justiz in einer freien, rechtsstaatlichen Gesellschaft ein gewisses Maß an Transparenz in Strafverfahren. Die Strafverfolgungsbehörden werden gegen den Angeschuldigten normalerweise Klagepunkte anführen und ihm die Möglichkeit geben, sich zu erklären. Falls es zu einem Gerichtsverfahren kommt, erhält der Anwalt des Angeschuldigten die entsprechenden Informationen und es kommt zu einer öffentlichen Anhörung vor Gericht. Im Gegensatz dazu wird das Sammeln von Erkenntnissen durch Geheimdienste immer geheim gehalten. Und da die strafrechtliche Verfolgung von Personen nicht zwangsläufig das beabsichtigte oder tatsächliche Ziel ist, kann es sein, dass der Schleier der Geheimhaltung nie gelüftet wird. Die Fälle, die öffentlich gemacht werden, machen wahrscheinlich nur einen kleinen Anteil der gesamten Überwachungsmaßnahmen aus.

In einer demokratischen Gesellschaft werden Maßnahmen, die staatliche Behörden im Verborgenen ergreifen, in der Regel argwöhnisch betrachtet und erzeugen Misstrauen.[18] Versuche, das öffentliche Vertrauen mit der Einführung einer gewissen Kontrolle über nationale Sicherheitsorganisationen zu stärken, waren nicht immer erfolgreich, wenn nachgewiesen wurde, dass staatliche Stellen die Öffentlichkeit und sogar die Aufsichtsgremien getäuscht haben.[19]

Während also mit Sicherheit gesagt werden kann, dass Regierungen einen größeren Zugriff als früher auf personenbezogene Daten erhalten möchten, die sich im Besitz von Unternehmen befinden, und diesen auch bekommen, ist das genaue Ausmaß dieses Zugriffs ein Stück weit unklar. In diesem Zusammenhang können Transparenzberichte eine nützliche Rolle spielen.

Transparenzberichte

Jedes Mal, wenn der Staat aus unternehmensfremden Gründen auf Daten oder Informationen in Firmenbesitz zugreift, gibt es eine staatliche Stelle, die die Informationen einholt, und ein Unternehmen, das diese Anfrage erhält und daraufhin tätig wird. Der Schwerpunkt dieses Papiers liegt vor allem auf der Berichterstattung über die Maßnahmen von Unternehmen, die solche Anfragen erhalten. Auch wenn es nicht im Mittelpunkt des vorliegenden Papiers steht, ist zu betonen, dass die Transparenz und Rechenschaftspflicht öffentlicher Stellen, die Unternehmen zur Herausgabe ihrer Daten auffordern oder verpflichten, ebenso wichtig ist. Die Arbeitsgruppe hat bereits auf die Bedeutung der Transparenz als Element der

[18] Siehe den Bericht des Europäischen Parlaments über das US-amerikanische NSA-Überwachungsprogramm, Überwachungsgremien in verschiedenen Mitgliedstaaten und ihre Auswirkung auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit in den Bereichen Justiz und Inneres, Februar 2014.

[19] Siehe z. B. den Sonderausschuss des US-Senats zum Haft- und Verhörprogramm der CIA, veröffentlicht im Dezember 2014.

Rechenschaftspflicht bei staatlichem Abhören privater Kommunikation oder im Rahmen von Überwachung hingewiesen.[20]

Die steigende Nachfrage seitens des Staates nach Informationen und personenbezogenen Daten in Firmenbesitz bereitet nicht nur Einzelpersonen und Verfechtern der Privatsphäre Sorgen, sondern auch den Unternehmen selbst. Bei einigen dieser Bedenken der Unternehmen handelt es sich ganz nüchtern um Bedenken bezüglich des Erfüllungsaufwands (der beträchtlich sein kann). Unter ethischen Gesichtspunkten haben Unternehmen Schwierigkeiten, die Herausgabe von vertraulichen personenbezogenen Daten an staatliche Behörden für unternehmensfremde Zwecke mit dem Vertrauensverhältnis in Einklang zu bringen, das sie mit ihren Kunden und anderen Geschäftspartnern pflegen möchten.

Besorgnisse bestehen ebenfalls im Hinblick auf die rechtliche Haftung, wenn Unternehmen konkurrierenden rechtlichen Verpflichtungen zum Schutz von Sicherheit und Vertraulichkeit einerseits und zur Erfüllung staatlicher Zugriffsforderungen in einem bestimmten Rechtssystem andererseits unterliegen. Die rechtlichen Schwierigkeiten nehmen noch zu, wenn es sich um ein multinationales Unternehmen handelt, das in mehreren Rechtssystemen tätig ist, und Gesetze miteinander kollidieren, oder wenn ein Auftragsverarbeiter aufgefordert wird, die Daten eines anderen Unternehmens verdeckt weiterzuleiten. Zusätzliche Schwierigkeiten gibt es im Zusammenhang mit grenzüberschreitenden Anfragen, die auf Grundlage eines Vertrags zur Rechtshilfe gestellt werden.[21]

Eine mögliche Lösung für Unternehmen besteht darin, eine eindeutige und stringente Unternehmenspolitik für den Umgang mit staatlichen Anfragen einzuführen, um sicherzustellen, dass diese kompetent und rechtmäßig bearbeitet und Fehler vermieden werden. Zu solchen Leitlinien können die Zentralisierung der Annahme von Anfragen, ein standardisierter Bearbeitungsprozess, eindeutige und an den geltenden rechtlichen Anforderungen ausgerichtete Unternehmenskriterien sowie die Beteiligung leitender und erfahrener Mitarbeiter gehören. Innenrevision, Überprüfung und Berichterstattung gegenüber der Führungsebene sind übliche Anforderungen. Unternehmen können vor der Übermittlung von Daten eine richterliche Anordnung oder ähnliches anfordern. Aufgrund der Aufmerksamkeit, die guten Praktiken, ethischen Fragen und dem Ruf eines Unternehmens geschenkt wird, denken viele Unternehmen über die Rolle öffentlicher Berichterstattung nach.

[20] Arbeitspapier der IWGDPT zur Überwachung der Telekommunikation (Auckland, 2002) und Gemeinsamer Standpunkt der IWGDPT zu zur öffentlichen Verantwortung im Hinblick auf das Abhören privater Kommunikation (Hongkong, 1998).

[21] Siehe z. B. Global Network Initiative, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Januar 2015.

2009 veröffentlichte Google seinen ersten Transparenzbericht. Innerhalb der nächsten drei Jahre folgten einige Anbieter von Telekommunikations- und Internetdiensten.[22] Im Jahr 2013 wurde dieses Vorgehen populär, als Dutzende Firmen in Nordamerika, Europa, Asien und Australien einen Transparenzbericht veröffentlichten.[23]

In der Regel geben die Unternehmen keine genauen Gründe für die Veröffentlichung eines Transparenzberichts bekannt, obwohl viele angeben, dass ihr Unternehmen dem Datenschutz eine hohe Bedeutung beimisst. Normalerweise besteht keine gesetzliche Verpflichtung zur Veröffentlichung eines solchen Berichts. Die Motivation hängt vermutlich mit der Sorge eines Unternehmens um seinen Ruf und mit seiner Eigenwahrnehmung als verantwortlicher „Corporate Citizen" zusammen. Auch das Verhalten anderer Unternehmen kann manchmal eine Rolle spielen. Die Veröffentlichung eines Berichts kann ein Versuch seitens eines Unternehmens sein, seine Vertrauenswürdigkeit unter Beweis zu stellen, indem es zeigt, dass es sein Bestes tut, um seine schwierige Doppelrolle – Zusammenarbeit bei rechtmäßigen Anfragen sowie Erfüllung seiner Verpflichtungen hinsichtlich Sicherheit und Vertraulichkeit – professionell auszufüllen. Die korrekte Bearbeitung von Anfragen zum Datenzugriff und die gleichzeitige öffentliche Berichterstattung über diesbezügliche Maßnahmen werden als Übungen in Transparenz gegenüber Kunden, Geschäftspartnern und der Öffentlichkeit betrachtet.

In gewisser Weise handelt es sich bei Transparenzberichten von Unternehmen um einen Versuch der Privatwirtschaft, öffentliche Stellen zur Verantwortung zu ziehen. Letztlich sind die öffentlichen Stellen für die Zugriffsanfragen verantwortlich, die öffentlichen Unmut erzeugen oder den Kundenerwartungen zuwiderlaufen aber es sind die Unternehmen, die damit konfrontiert sind, die Informationen herauszugeben. Bei der Veröffentlichung von Berichten, die Aufschluss über die Handlungen geben, zu denen die Unternehmen verpflichtet wurden, handelt es sich um einen Versuch, öffentliche Stellen für ihr Vorgehen zur Verantwortung zu ziehen. Es gibt praktische Gründe für die Versuche von Unternehmen, staatliche Stellen zur Rechenschaft zu ziehen, und diese Versuche können mit einigen Vorteilen verbunden sein. Die Bearbeitung vielfacher Anfragen zum Datenzugriff ist für ein Unternehmen mit einem Erfüllungsaufwand verbunden. Falls das Unternehmen der Anfrage widerstandslos nachkommt, könnte es für die Behörden als „leichte Beute" eingestuft und zur bevorzugten ersten Anlaufstelle für die Beschaffung von Informationen werden. Werden die Vorgehensweisen bei der Veröffentlichung von Transparenzberichten genauer beleuchtet, kann dies dazu beitragen sicherzustellen, dass die Behörden stärker darauf achten, dass die Ausübung ihrer Zwangsbefugnisse verhältnismäßig und begründet ist. Man könnte sagen, dass die Unternehmen versuchen, das Ethos einer „transparenten Staates"

[22] 2012 veröffentlichten mindestens zwölf Unternehmen Transparenzberichte online. Quelle: Büro des Datenschutzbeauftragten, Neuseeland.

[23] Für 2013 wurden ca. 37 Transparenzberichte gezählt, die im Internet veröffentlicht wurden. Quelle: Büro des Datenschutzbeauftragten, Neuseeland.

wiederherzustellen, das im Bereich der staatlichen Überwachung einen Rückschlag erlitten hat.

Aus Sicht des Datenschutzes ist es offensichtlich schwierig, ohne Genehmigung der betroffenen Person und womöglich gegen den Wunsch und die Interessen dieser Person einem Dritten Informationen aus Firmenbesitz für unternehmensfremde Zwecke zu übermitteln. Dies war im Bereich der Strafverfolgung jedoch schon immer der Fall und das Problem wurde in der Regel dadurch gelöst, dass die strafrechtlichen Ermittlungen als legitime Ausnahme von den Geheimhaltungserwartungen anerkannt wurden. Im derzeitigen Kontext bezieht sich die Schwierigkeit auf den zunehmenden Zugriff auf Daten in Firmenbesitz, der mittlerweile eher die Regel als die Ausnahme darstellt, sowie auf die massenhafte Herausgabe von und den Zugriff auf Daten in Firmenbesitz in Echtzeit zum Zweck der Überwachung.

Um auf diese Herausforderung für die klassischen Erwartungen an den Datenschutz zu reagieren, wird nun der Notwendigkeit, dass öffentliche Stellen und Unternehmen einen rechenschaftspflichtigen Umgang mit Informationen unter Beweis stellen, größere Beachtung geschenkt. Transparenz gilt dabei als wichtiger Bestandteil. Dies kann als ein Gesellschaftsvertrag gesehen werden, in dessen Rahmen die Bürger erwarten, dass ihre Kommunikation und ihre Angelegenheiten vertraulich behandelt werden und dies nur rechtmäßigen und verhältnismäßigen Ausnahmen für Strafverfolgung und die nationale Sicherheit unterliegt, wobei die die entsprechenden Organisationen unter vertrauenswürdiger, unabhängiger Aufsicht stehen. Die Veröffentlichung von Transparenzberichten ist eine Form der öffentlichen Überprüfbarkeit, um sicherzustellen, dass die Bedingungen dieses Vertrags eingehalten werden.

Mit diesen Berichten wird die Öffentlichkeit in allgemeiner Form über die Maßnahmen staatlicher Stellen informiert. Die öffentliche Berichterstattung durch die Behörden, die Zugriff auf Daten fordern, und der Stellen, die diese Anfragen bearbeiten, fördert die Rechenschaftspflicht beider Seiten. Schließlich informieren die Berichte auch die Öffentlichkeit und den Gesetzgeber, die letztendlich darüber entscheiden, wo sie die Grenze zwischen Überwachung und Freiheit ziehen wollen.

Inhalt der Transparenzberichte

Die plötzlich zunehmende Bereitschaft von Unternehmen zur freiwilligen Veröffentlichung von Transparenzberichten führte dazu, dass eine Reihe von Statistiken erstellt wurden, die nicht immer vergleichbar sind.[24] Die Statistiken un-

[24] Die aus der fehlenden Standardisierung von Berichten entstehenden Probleme werden dargestellt in: Christopher Parsons, Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports, 2015, verfügbar über SSRN: http://ssrn.com/abstract=2546032 oder http://dx.doi.org/10.2139/ssrn.2546032.

terscheiden sich hinsichtlich ihrer Detailliertheit und Parameter; zudem werden Daten unterschiedlich (oder gar nicht) definiert.

Es gibt jedoch Spielraum, um Ordnung in das System der Berichterstattung zu bringen, da den meisten Transparenzberichten ein recht ähnlicher Ansatz zugrunde liegt. Die Berichte enthalten relevante Statistiken zu Zahl und Art staatlicher Anfragen zu Informationen in Firmenbesitz sowie zu den Ergebnissen dieser Anfragen. Die Berichte können günstigerweise auch andere Themen umfassen, die für das betreffende Unternehmen relevant sind – z. B. Anfragen zum Thema Urheberrecht und der Löschung von Daten oder zum europäischen Recht auf Vergessenwerden (Entfernung von Internetlinks). Doch so nützlich diese zusätzlichen Berichte auch sind, gehen sie über den Rahmen dieses Papiers hinaus.

Im Folgenden wird kurz auf die typischen Elemente eines Transparenzberichts eingegangen:

- *Rechtsordnung:* Unternehmen, die in mehreren Rechtsordnungen tätig sind, erhalten wahrscheinlich Anfragen von staatlichen Behörden aus verschiedenen Ländern. Die Struktur des Berichts wird dies widerspiegeln müssen. Verschiedene Länder nutzen unterschiedliche Terminologie für ähnliche Konzepte und das Unternehmen wird entscheiden müssen, ob es in allen Berichten eine Standardterminologie verwendet oder die Sprache an die Rechtsterminologie einer bestimmten Rechtsordnung anpasst. Eine nützliche Methode besteht darin, Standardterminologie zu verwenden und mithilfe einer Legende oder von Fußnoten zu erklären, wie die Begriffe im Rahmen der jeweiligen Rechtsordnung verwendet werden.
- *Berichtszeitraum:* Die Veröffentlichung eines Transparenzberichts ist keine einmalige Übung, sondern ein fortlaufender Prozess. In der Zukunft mag es vielleicht möglich sein, in Echtzeit online Bericht zu erstatten, doch bisher läuft es so ab, dass Unternehmen Jahresberichte vorlegen. Größere Unternehmen veröffentlichen ihre Berichte häufiger, in der Regel einmal alle drei oder sechs Monate. Die Berichte zeigen für gewöhnlich Trends auf und beinhalten Diagramme und Kommentare, in denen die aktuellen Zahlen mit Zahlen aus früheren Zeiträumen verglichen werden.
- *Art der Anfragen:* Staatliche Anfragen werden in unterschiedlicher Form gestellt und die meisten Berichte versuchen, diese auf eine der Rechtsordnung und der jeweiligen Branche angemessenen Weise zu vereinheitlichen. Typische Klassifizierungen beziehen sich auf die rechtliche Form der Anfragen (z. B. eine richterliche Anordnung oder ein administratives Ersuchen), die Art der von dem Unternehmen zu ergreifenden Maßnahme (z. B. Zugriff auf bestehende Daten oder Einsatz eines Gerätes zur weiteren Überwachung eines Kontos und Herausgabe von Kontobewegungsdaten an staatliche Stellen in Echtzeit) und darauf, ob die Anfrage einen straf- oder zivilrechtlichen Hintergrund hat

und ob sie von einer in- oder ausländischen Ordnungsbehörde gestellt wird.[25] Es gibt viele Unterkategorien, die ebenfalls nützlich sein können. Unternehmen neigen dazu, ihre Berichte nach den häufigsten Anfragen zu strukturieren. Dies sind in der Regel Anfragen von Stellen ihrer eigenen Rechtsordnung.

- *Anzahl der Anfragen:* Ausgangspunkt für den Bericht müssen natürlich die von staatlicher Seite gestellten Anfragen darstellen. Wird lediglich über die Anzahl der Anfragen berichtet, könnte dies verschleiern, dass es hinsichtlich der Art und des Umfangs der Anfragen erhebliche Unterschiede gibt. Dementsprechend erfassen nützlichere Berichte sowohl die Anzahl der erhaltenen Anfragen als auch die Zahl der individuellen Datensätze oder Konten, auf die sich diese Anfragen beziehen.
- *Informationsvolumen bzw. Anzahl der betroffene Personen:* Zahlen bezüglich des Umfangs und der Auswirkung der Anfragen sind in einigen, aber nicht in allen Berichten zu finden.
- *Ergebnis der Anfragen:* Transparenzberichte spiegeln nicht einfach nur wider, was der Staat von den Unternehmen verlangt hat. Sie berichten auch über die vom Unternehmen getroffenen Maßnahmen und folglich auch über das Ergebnis der Anfragen. Dies unterscheidet sich je nach Art des Unternehmens, Art der Anfragen und geltendem Recht. Zum Beispiel sollte ein Auftragsverarbeiter jede staatliche Anfrage auf Zugriff an den für die Verarbeitung Verantwortlichen weiterleiten, es sei denn, ihm ist dies gesetzlich verboten. Ein Bericht für einen Auftragsverarbeiter kann daher Statistiken zur Zahl der Weiterleitungen an für die Verarbeitungen von Kundendaten Verantwortliche enthalten und zur Zahl der Fälle, in denen der Auftragsverarbeiter die Anfrage direkt beantwortet hat. Die meisten der im Bericht enthaltenen Statistiken beziehen sich im Allgemeinen darauf, ob die Anfragen beantwortet oder abgelehnt wurden. Ist Ersteres der Fall, werden Details zur Anzahl der betroffenen Datensätze, Personen oder Konten aufgeführt. In einigen Fällen gibt es gesetzliche Einschränkungen, die die Veröffentlichung von Statistiken begrenzen oder zeitlich verschieben.
- *Kommentierung:* Eine Einführung, eine Erläuterung der verwendeten Begriffe und ein Kommentar zu den Trends ergänzen in der Regel die Statistiken. Ein gesonderter Kommentar kann im Falle unerwarteter oder außergewöhnlicher Zahlen erfolgen.

Grundsätze für die Erstellung von Transparenzberichten

Die Arbeitsgruppe empfiehlt den für die Privatsphäre und den Datenschutz zuständigen Behörden, Unternehmen dazu anzuhalten, die folgenden „Grundsätze" bei der Erstellung von Transparenzberichten zu berücksichtigen:

[25] Unternehmen könnten die Bearbeitung von Anfragen ausländischer Behörden ablehnen und dies in ihrem Bericht so festhalten.

1. ***Grundsatz der Rechenschaftspflicht:*** Unternehmen sollten in Bezug auf ihren Umgang mit staatlichen Anfragen auf die Herausgabe von Informationen zu unternehmensfremden Zwecken Rechenschaft ablegen.

2. ***Grundsatz der Transparenz:*** Unternehmen, bei denen regelmäßig staatliche Anfragen zur Herausgabe von Informationen zu unternehmensfremden Zwecken eingehen, sollten regelmäßig die Art und Menge der übermittelten Daten öffentlich machen.

3. ***Grundsatz der Verlässlichkeit:*** Transparenzberichte von Unternehmen, die auf staatliche Anfrage hin Auskunft über die Weitergabe personenbezogener Informationen geben, sollten präzise und vollständig sein.

4. ***Grundsatz, dass Berichte nicht irreführen sollten:*** Ungeachtet dessen, dass Gesetze manchmal eine zeitliche Verzögerung für die Berichterstattung vorschreiben oder der Berichterstattung Grenzen setzen[26], sollten Unternehmen, die Transparenzberichte veröffentlichen, Maßnahmen zur Vermeidung eines irreführenden Eindrucks ergreifen, der durch die Vorlage unvollständiger Statistiken entstehen würde.

5. ***Grundsatz der Vergleichbarkeit:*** Die Unternehmen sollten versuchen sicherzustellen, dass bekannt gegebene Statistiken sinnvoll mit bereits veröffentlichten Berichten und Statistiken aus anderen Transparenzberichten verglichen werden können.

6. ***Grundsatz der Zugänglichkeit:*** Transparenzberichte sollten so veröffentlicht werden, dass die Öffentlichkeit, die Medien und die relevanten Akteuren in möglichst effektiver Weise darauf zugreifen können.

Empfehlungen zur Umsetzung der Grundsätze

Bei der Veröffentlichung von Transparenzberichten handelt es sich bisher um eine freiwillige Initiative, die vom Privatsektor als Reaktion auf die staatliche Einwirkung auf öffentliche Vorstellungen von Privatsphäre ergriffen wurde. Die Arbeitsgruppe unterstützt diese Initiative und empfiehlt, dass die Transparenzberichte verbessert werden und dass noch mehr Unternehmen und Branchen solche Berichte veröffentlichen. Positiv hervorzuheben sind an dieser Stelle alle Unternehmen, die mit der Veröffentlichung von Transparenzberichten bereits begonnen haben. Allerdings ist es für ein einzelnes Unternehmen schwierig, ein Ziel

[26] Natürlich müssen die Unternehmen bei der Anwendung dieser Grundsätze und der Erstellung eines Transparenzberichts das geltende nationale Recht einhalten.

wie die Vergleichbarkeit der veröffentlichten Statistiken zu erreichen. Ebenso kann ein einzelnes Unternehmen nicht in der gesamten Branche für Transparenz sorgen. Aber je mehr Unternehmen Transparenzberichte veröffentlichen, desto vollständiger wird das Bild, das in Bezug auf das staatliche Vorgehen und die entsprechenden Maßnahmen der Unternehmen, die die personenbezogenen Daten der Bürger verwalten, entsteht. Sobald bekannte Unternehmen damit begonnen haben, Transparenzberichte vorzulegen, erhöht sich der Marktdruck auf die Mitbewerber, ebenfalls transparenter zu sein.

Die Arbeitsgruppe vertritt die Auffassung, dass neben einzelnen Unternehmen auch andere Akteure zur Förderung und Verbesserung von Transparenzberichten beitragen müssen. Diese Empfehlungen richten sich daher sowohl an Unternehmen als auch an andere Akteure. Sie versuchen, den Grundsätzen der Transparenz größere Wirkung zu verleihen.

Die Arbeitsgruppe empfiehlt:

Unternehmen

(a) Unternehmen, die staatliche Anfragen zum Zugang zu personenbezogen Informationen aus ihrem Besitz erhalten, sollten:

   i. zuverlässige Verfahren für die Annahme von und den Umgang mit staatlichen Anfragen zum Zugang zu personenbezogenen Informationen anwenden, um sicherzustellen, dass die Herausgabe von Informationen verantwortungsvoll und rechtskonform erfolgt und im Einklang mit der Unternehmenspolitik steht;

   ii. ihre Politik für den Umgang mit staatlichen Anfragen veröffentlichen;

   iii. mit der Veröffentlichung von Transparenzberichten wie in diesem Papier dargelegt beginnen (dies gilt für Unternehmen, die wiederholt staatliche Anfragen auf Zugang zu personenbezogenen Informationen erhalten);

   iv. sicherstellen, dass die von ihnen veröffentlichten Transparenzberichte verlässlich sind, indem sie dafür Sorge tragen, dass die Statistiken seriös erstellt werden und überprüfbar sind;

   v. ihre Berichte und die Terminologie so strukturieren, dass sie die firmen-, branchen-, länder- und zeitraumübergreifende Vergleichbarkeit von Statistiken fördern;

   vi. Praktiken vermeiden, die den Leser in die Irre führen können und, insbesondere falls die veröffentlichten Zahlen aufgrund von staatlichen Restriktionen unvollständig sind, auf diese Unvollständigkeit hinweisen und nach Ablauf der Restriktionen die vollständigen Zahlen vorlegen;

vii. einen Beitrag zu einer effektiveren Verbreitung der Berichte leisten, indem sie beispielsweise Maßnahmen zur Wiederveröffentlichung von Zahlen in gemeinsamen nationalen oder internationalen Verzeichnissen unterstützen;

viii. die Einheitlichkeit ihrer Vorgehensweisen bei der Erstellung von Transparenzberichten mithilfe der Grundsätze zur Erstellung von Transparenzberichten überprüfen und – falls nötig – verbessern.

Rechtsetzung

(b) Gesetzgeber, die Gesetze oder Regelungen schaffen, auf deren Grundlage Behörden Zugang zu personenbezogenen Informationen in Firmenbesitz erlangen können, sollten:

i. gewährleisten, dass die Gesetze und Regelungen angemessene, im Verhältnis zu den betroffenen öffentlichen Interessen stehende Grenzen nicht überschreiten, entsprechende Sicherungen enthalten und Mittel bereitstellen, um die öffentlichen Stellen zur Rechenschaft zu ziehen;

ii. sicherstellen, dass Verpflichtungen zur Förderung der Transparenz beim Einsatz solcher Befugnisse bestehen;

iii. unnötige Hindernisse für die Erstellung von Transparenzberichten abbauen;

iv. dafür sorgen, dass Behörden dazu verpflichtet sind, Statistiken über die Ausübung von Befugnissen beim Zugriff auf Daten in Firmenbesitz zu veröffentlichen.

Öffentliche Stellen, die Zugang zu Informationen in Firmenbesitz erlangen

(c) Öffentliche Stellen sollten:

i. Befugnisse für den Zugriff auf Daten in Firmenbesitz rechtmäßig, verhältnismäßig und nachvollziehbar ausüben;

ii. sollten offenlegen, wie sie ihre Befugnisse ausüben, z. B. durch die regelmäßige Veröffentlichung von Statistiken;

iii. die Auferlegung von Geheimhaltungspflichten vermeiden, die nicht im Verhältnis zu den berechtigten Bedürfnissen im Bereich der Strafverfolgung oder nationalen Sicherheit stehen;

iv. alle bestehenden Geheimhaltungspflichten überprüfen, um sicherzustellen, dass sie die in einer freien Gesellschaft gerechtfertigte Schwelle nicht überschreiten.

Datenschutzbehörden

(d) Datenschutzbehörden sollten:

i. die Bemühungen derjenigen Unternehmen, die freiwillig Transparenzberichte veröffentlichen, unterstützen und andere Unternehmen dazu ermutigen, dasselbe zu tun;

ii. bessere Praktiken bei der Veröffentlichung von Transparenzberichten fördern, um die Erstellung von aussagekräftigen Statistiken zu unterstützen, die zuverlässig und national und international vergleichbar sind;

iii. Bemühungen unterstützen oder einleiten, um Transparenzberichte in zentralisierten nationalen oder internationalen Verzeichnissen zugänglicher zu machen;

iv. die in den Berichten bekannt gegebenen Informationen für Ihre Arbeit nutzen.

Internationale Regierungsorganisationen

(e) Internationale Organisationen sollten:

i. die Entwicklung international vergleichbarer Metriken fördern, um den politischen Entscheidungsprozess hinsichtlich der Privatsphäre und der grenzüberschreitenden Übermittlung von personenbezogenen Daten auf eine informierte Basis zu stellen.

ii. die Bereiche identifizieren, in denen staatliche Geheimhaltungspflichten ein unnötiges Hindernis für die Transparenz darstellen, und Regierungen auf bessere Praktiken aufmerksam machen, die Offenheit fördern und Vertrauen im Internet aufbauen.

Regulierungsbehörden für Telekommunikation

(f) Die Regulierungsbehörden für Telekommunikation sollten:

i. die Erstellung von Transparenzberichten im Telekommunikationssektor unterstützen und fördern.

Branchenverbände

(g) Branchenverbände sollten:

i. in Abstimmung mit den relevanten Akteuren wie Datenschutzbehörden und der Zivilgesellschaft Handlungsempfehlungen für gute Praktiken für

die Erstellung von Transparenzberichten geben, die für ihre Branche relevant sind.[27]

Zivilgesellschaft

(h) Die Zivilgesellschaft sollte:

i. von allen relevanten Akteuren Rechenschaft einfordern (Regierungen, die Gesetze schaffen, die den Zugriff auf Daten ermöglichen; Behörden, die auf Informationen in Firmenbesitz zugreifen wollen; Unternehmen, die staatliche Anfragen bearbeiten und personenbezogene Informationen zu unternehmensfremden Zwecken herausgeben);

ii. Unternehmen dazu ermutigen, Transparenzberichte zu erstellen;

iii. die Einrichtung gemeinsamer Verzeichnisse zum Abruf der Berichte unterstützen;[28]

iv. von den im Rahmen der Transparenzberichte erstellten Statistiken Gebrauch machen.

[27] Ein Beispiel für solch eine Industrieinitiative ist der Dialog der Telekommunikationsbranche, dessen Aktivitäten auf Grundlage der Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte erfolgen, zu denen auch das Handlungsprinzip 21 gehört (Sorgfaltspflicht im Bereich der Menschenrechte), das zur externen Berichterstattung über betriebliche Praktiken mit Auswirkungen auf Menschenrechte ermutigt. Siehe www.telecomindustrydialogue.org.

[28] Zum Beispiel haben zivilgesellschaftliche Organisationen in Kanada, Hongkong, Polen und den USA Berichte veröffentlicht oder Webseiten eingerichtet, die Firmenstatistiken an einem Ort zusammenführen, oder eine vergleichende Untersuchung von Firmenberichten durchgeführt.

2. 58. Sitzung am 13./14. Oktober 2015 in Berlin

Arbeitspapier zur Verfolgung des Aufenthaltsortes auf der Basis von Meldungen von Mobilfunkgeräten

– Übersetzung –

Anwendungsbereich

1. Die Arbeitsgruppe hat bereits früher Risiken für die *„Aufzeichnung des Aufenthaltsortes und andere personenbezogenen Daten über Netzwerknutzer“*[1] identifiziert. Sie hat einen gemeinsamen Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten verabschiedet[2] und die Nutzung von „Deep Packet Inspection“ für Werbezwecke erörtert[3].

2. Dieses Arbeitspapier untersucht insbesondere die Risiken für Datenschutz und Privatsphäre, die mit der Erhebung von gerätebezogenen Informationen und der Ableitung von Aufenthaltsinformationen aus Verkehrsdaten zusammenhängen. Ein Beispiel bildet die Nutzung von Wi-Fi „probe requests“, die von Geräten wie Smartphones stammen, für die Analyse von Kundenfrequenz und Verkehrswegen im Einzelhandel.

Hintergrund

3. Kommunikationsnetzwerke erfordern die regelmäßige Aussendung bestimmter Datenpakete, um Netzwerk-Controller oder andere Geräten im Netzwerk aufzufinden oder eine Verbindung mit diesen aufrecht zu erhalten. Darüber hinaus muss den Geräten eine eindeutige Adresse zugewiesen werden, um sie in dem Netzwerk unterscheiden zu können, so dass Datenpakete von und zu dem richtigen Gerät gesendet werden können.

4. Eine einzelne drahtlose Basisstation (d. h. ein Sender und Empfänger), wie eine Mobilfunk-Basisstation oder ein Wi-Fi-Zugangspunkt, hat eine be-

[1] Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke – Allgemeine Empfehlungen, 2004. http://www.datenschutz-berlin.de/attachments/196/1_de.pdf

[2] Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, 2004. http://www.datenschutz-berlin.de/attachments/192/local_neu_de.pdf

[3] Arbeitspapier zur Nutzung von Deep Packet Inspection zu Marketing-Zwecken, 2010. http://www.datenschutz-berlin.de/attachments/737/675.41.20x.pdf

stimmte Reichweite. Außerhalb dieser Reichweite (oder der Reichweite eines Signalverstärkers) können das Endgerät und die Basisstation nicht miteinander kommunizieren. Eine einzelne Basisstation ist mit kompatiblen Geräten in Reichweite verbunden und empfängt dabei Signale von dem Gerät (unter der Annahme, dass die Netzwerkverbindungen aktiv sind). Die Signalstärke kann für die Bestimmung der Entfernung zwischen Basisstation und Gerät genutzt werden. Um die Reichweite dieses Netzwerks zu erweitern, sind mehrere Basisstationen erforderlich (die sich in der Reichweite überlappen oder nicht). Die Bewegung eines Endgeräts kann festgestellt werden, wenn es in die Reichweite einer bestimmten Basisstation kommt oder diese verlässt. Wenn sich die Reichweiten der Basistationen überlappen, kann die Entfernung zwischen dem Gerät und den verschiedenen Basisstationen genutzt werden, um mit Hilfe von Trilateration den Aufenthaltsort präziser zu berechnen[4].

5. Kommunikationsprotokolle enthalten im Allgemeinen eine Reihe verschiedener Signaltypen für bestimmte Zwecke. Z. B. definieren die IEEE 802.11 Standards für Funknetzwerke[5] Management-Frames, Kontroll-Frames und Daten-Frames. Jeder Frame, der vom Geräte des Nutzers stammt, enthält die eindeutige MAC-Adresse des Wi-Fi-Netzwerkschnittstellen-Controllers (Network Interface Controller – NIC). Ein spezieller Typ eines Management-Frames ist der „Probe Request" der von dem NIC aktiv gesendet wird, um verfügbare Netzwerke in der Umgebung zu suchen. Eine Organisation kann daher eine Reihe von Wi-Fi-Zugangspunkten (z. B. als Teil eines Wi-Fi-Netzwerks in einem Ladengeschäft) oder Frequenz-Scanner installieren und die MAC-Adresse jedes Geräts in Reichweite erfassen (unter der Annahme, dass die Wi-Fi-Einrichtung des Geräts angeschaltet ist). Da die MAC-Adresse eines bestimmten NIC normalerweise statisch ist, indiziert die Beobachtung des Wiederauftretens einer bestimmten MAC-Adresse die Rückkehr dieses bestimmten Geräts.

6. Viele dieser Geräte, besonders Smartphones, können auf das engste mit einer Einzelperson verbunden sein. Daher kann die Erhebung einer MAC-Adresse in Kombination mit Daten wie Datum und Uhrzeit leicht zur indirekten oder direkten Identifikation des Besitzers des Geräts führen.

7. Andere drahtlose Kommunikationsprotokolle wie Bluetooth und Mobiltelefon-Standards enthalten in gleicher Weise das Aussenden aktiver Signale mit eindeutigen Identifikationsnummern. Im Falle von Bluetooth ist dies die

[4] Trilateration meint den Prozess der Feststellung des Aufenthaltsortes unter Nutzung der Entfernung von bekannten Punkten. Davon zu unterscheiden ist die Triangulation, bei der der gemessene Winkel von bekannten Punkten genutzt wird.

[5] http://standards.ieee.org/getieee802/download/802.11-2012.pdf

MAC-Adresse des Bluetooth-NIC. Im GSM (Groupe Speciale Mobile, einem globalen Standard zur Mobilkommunikation) werden die „International Mobil Station Equipment Identity“ (IMEI), die „International Mobil Subscriber Identity“ (IMSI) und die „Temporary Mobile Subscriber Identity“ (TMSI) in unterschiedlichen Intervallen gesendet.

8. Geräte-Identifikatoren wie die MAC-Adresse und die IMSI enthalten außerdem Informationen über das Gerät selbst. Z. B. bestimmten die ersten drei Oktette der MAC-Adresse die Organisation, die das NIC herausgegeben hat. Dies kann Informationen über den Gerätehersteller oder den Typ des Gerätes, das verfolgt wird, offen legen. Die ersten drei Ziffern der IMSI beziehen sich auf den Länder-Code, gefolgt von der Kennung des Mobilfunkanbieters. Bluetooth und Wi-Fi-Geräte haben darüber hinaus einen konfigurierbaren Gerätenamen, der übertragen werden kann.

9. Es haben sich Diensteanbieter herausgebildet, die nicht als Kommunikationsnetzwerk fungieren und Internetzugriff anbieten, sondern die ausschließlich Dienste zur Verfolgung von Aufenthaltsinformationen auf der Basis von Scannern anbieten, um die in diesem Arbeitspapier beschriebenen Verkehrsdaten zu erheben. Sie sammeln z. B. Wi-Fi-„Probe Requests“ ohne Angebot eines Internetzugangs oder erheben Bluetooth-Signale. Die Risiken, die von Technologien zum Verfolgen von Aufenthaltsinformationen herrühren, sind auch nicht exklusiv auf den traditionellen Einzelhandel beschränkt (d. h. einzelne Ladengeschäfte oder Einkaufszentren). Viele andere Geschäftsräume einschließlich Bahnhöfen und Flughäfen nutzen diese Technologie zur Beobachtung oder zur Verfolgung von Einzelpersonen[6]. Strafverfolgungsbehörden benutzten diese Technologie ebenfalls.

10. Darüber hinaus hat das Aufkommen und der Einsatz von Bluetooth 4.x NICs (auch bekannt als „Bluetooth Low Energy“ oder BLE) zu sog. „hyper-lokalen“ Geolokalisierungsdiensten geführt. BLE-Baken arbeiten mit einer kurzen Reichweite und können von einem Gerät zur Berechnung seines Aufenthaltsortes (oder zur Veranlassung der Berechnung seines Aufenthaltsortes) mit einem hohen Grad an Genauigkeit genutzt werden.

[6] Z. B. der Flughafen Schiphol (https://www.schiphol.nl/SchipholGroup/ NewsMedia/PressreleaseItem/AmsterdamAirportSchipholFirstAirportInEuropeWithFullBeaconCoverage.htm), die Flughäfen von Barcelona und Madrid (http://cdn1.pps-publications.com/airport-business-archive/2015/ab-summer-2015.pdf) *„ermöglichen es Passagieren, Echtzeit-Informationen über Flüge, Umsteigezeiten, kommerzielle Angebote und andere Dienste durch den Einsatz von iBeacons, die auf der drahtlosen Bluetooth-Technologie basieren“*), der London City-Flughafen (http://annual.aci-na.org/sites/default/files/Collier-ACI-NA%20September%208%202014%20v2.pdf, s. die Folien zu „Passenger Journey Measurement“), der Flughafen New York JFK (http://www.citylab.com/navigator/ 2015/08/your-phone-could-help-make-airport-lines-shorter/401942/), der Flughafen Helsinki (https://www.finavia.fi/en/news-room/news/2014/a-global-first-helsinki-airports-new-technology-to-develop-the-travel-experience/) und Flughäfen im mittleren Osten (http://www.arabianaerospace.aero/middle-east-airports-going-smart-for-seamless-travel-experience.html)

11. Eine Zunahme der Anzahl von Mobiltelefonen, die mit Wi-Fi ausgerüstet sind, zusammen mit einer Zunahme des Vorkommens von Wi-Fi in Ladengeschäften und dem Bedürfnis von Organisationen nach mehr Erkenntnissen über das Kundenverhalten, hat ein Momentum für die Entwicklung und Anwendung von Technologien zur Aufenthaltsbestimmung geschaffen. Dies ist nicht auf Wi-Fi beschränkt, weil Bluetooth ebenfalls standardmäßig aktiviert sein kann oder für eigene Zwecke genutzt wird (z. B. um die Nutzung von Freisprecheinrichtungen, die Anbindung „smarter" Uhren, tragbarer Geräte oder drahtloser Kopfhörer zu ermöglichen).

12. Weil Kommunikationsfähigkeiten in eine immer weiter wachsende Anzahl von Geräten eingebaut werden, werden die Möglichkeiten zur Verfolgung dieser Geräte anwachsen. In einigen Fällen können verschiedene Geräte-Identifikatoren auf eine Einzelperson bezogen werden, um die Effektivität der Verfolgung weiter zu steigern (z. B. könnte ein Einzelner verschiedene Smartphones, Tablets, eine Uhr und ein Fitness-Armband tragen und ein vernetztes Fahrzeug benutzen).

Risiken für den Datenschutz und die Privatsphäre

13. Viele Risiken für den Datenschutz und die Privatsphäre rühren von der Tatsache her, dass die Verfolgung des Aufenthaltsorts mobiler Geräte (technisch) verdeckt stattfindet. Wie im Falle von Wi-Fi ist es zur Erhebung und Verarbeitung von Daten ausreichend, einfach an einem bestimmten Ort anwesend zu sein und ein Gerät mit sich zu führen, bei dem Wi-Fi angeschaltet ist. Der Besitzer des Geräts muss keine aktive Wahl treffen, um sich mit dem Netzwerk zu verbinden oder dies zu versuchen. Obwohl manche Technologien wie BLE eine Handlung des Nutzers zur Aktivierung der Funktion erfordern, kann die Funktion angeschaltet bleiben, oder ist sogar standardmäßig durch das Betriebssystem angeschaltet. Unter diesen Umständen ist der Nutzer sich wahrscheinlich der Möglichkeit zur Verfolgung der Aufenthaltsinformation nicht bewusst.

14. Diese Risiken sind besonders verbreitet, wenn die Verfolgung von Aufenthaltsinformationen in öffentlichen Räumen aktiviert ist, weil sich die Möglichkeiten als begrenzt erweisen könnten, darüber zeitnah angemessene Informationen zur Verfügung zu stellen.

15. Die unsichtbare Natur der Verfolgung und der Wunsch einer Organisation, eine solche Verfolgung im Geheimen vorzunehmen, um die „Nutzererfahrung" nicht zu unterbrechen, führt zu Datenschutzproblemen im Hinblick auf die Transparenz, die Verantwortlichkeit, die Kenntnis des Einzelnen und die Wahlmöglichkeiten für den Nutzer.

16. Diese Risiken für den Datenschutz und den Schutz der Privatsphäre beinhalten:

    a. Die verdeckte Erhebung einer Reihe von Informationen wie gerätespezifischen Identifikatoren, die leicht mit bestimmten Einzelpersonen verknüpft werden können;

    b. Die Beobachtung des Aufenthaltsortes einer Einzelperson, ihres Weges und ihrer Aufenthaltszeit;

    c. Die Verfolgung einer Einzelperson über Zeiträume hinweg, einschließlich wiederholter Besuche an einem bestimmten Ort[7] oder innerhalb der Reichweite des Wi-Fi-Netzwerks;

    d. Die potenzielle Sensitivität der erhobenen Daten oder von Informationen, die aus dem Aufenthaltsort des Einzelnen abgeleitet werden können;

    e. Die Erhebung und Kombination von Aufenthaltsinformationen aus verschiedenen Netzwerken und/oder von verschiedenen Aufenthaltsorten, um ein vollständiges Bild der Bewegung eines Einzelnen in einem breiten Ausmaß zu erstellen (z. B. Verknüpfung von Daten verschiedener Einzelhändler oder deren Erhebung durch einen Netzwerkanbieter, der in verschiedenen Einrichtungen tätig ist);

    f. Die Kombination von Aufenthaltsdaten mit anderen Online- und Offline-Informationen, z. B. Kundenbindungskarten, soziale Medien, (abgeleitete) demografische Daten, Bankkarten- und Überweisungs-Historie oder Videoüberwachung (mit oder ohne zusätzlichen Analyse-Technologien), die zu einer überschießenden Erhebung von Daten führen könnte;

    g. Die Probleme, die erhobenen Daten in adäquater Weise zu de-identifizieren oder zu anonymisieren;

    h. Das Fehlen von Transparenz und Information des Nutzers. Dies wird weiter verstärkt bei Beschränkungen des Geräts wegen seiner Größe oder der Größe seines Displays;

    i. Das Fehlen einer einfachen und effektiven Möglichkeit für den Nutzer, die Erhebung von Daten entweder durch Einwilligung oder Widerspruch je nach den gesetzlichen Anforderungen in dem jeweiligen Rechtsraum zu kontrollieren[8];

[7] Aufenthaltsort in diesem Zusammenhang könnte das Innere und Äußere des Geländes einer Organisation und die Verfolgung über verschiedene Liegenschaften einschließen.

[8] Vgl. Federal Trade Commission, Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices, https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers (Das Unternehmen bot nicht wie versprochen eine Widerspruchsmöglichkeit in den Geschäften an).

j. Die Erstellung schwarzer oder weißer Listen auf Basis der erhobenen Informationen;

k. Die Erhebung von Daten von Arbeitnehmern oder anderen Einzelpersonen, die häufig in einem Gebiet präsent sind und die Möglichkeit, diese Daten für unspezifische oder inkompatible Zwecke einschließlich der Überwachung der Arbeitsleistung oder für Disziplinarmaßnahmen zu nutzen;

l. Zugriff auf die Daten durch Strafverfolgungsbehörden;

m. Fehlende Netzwerksicherheit, die zu einem Versagen des Schutzes gegen das Abhören von Kommunikation führt oder Versagen, die erhobenen Daten adäquat zu schützen;

n. Die Nutzung von Informationen zur Profilbildung, für Werbung oder Direktmarketing;

o. Das Fehlen klarer Verantwortlichkeiten der beteiligten Organisationen aufgrund der Vielzahl der Beteiligten.

17. Wenn ein Gerät sich mit dem Netzwerk verbindet (z. B. für den Zugang zum Internet über Wi-Fi, anstatt das der Netzwerkbetreiber nur die „Probe Request" überwacht), ist auch ein Potenzial zur Überwachung oder zum Abhören der Kommunikation selbst gegeben.

18. Technologien zur Aufenthaltsbestimmung können genutzt werden, um Informationen zu sammeln, die möglicherweise nicht durch das Telekommunikationsgeheimnis im klassischen Sinne geschützt sind.

Empfehlungen

19. Organisationen, die den Einsatz von Technologien zur Bestimmung des Aufenthaltsortes erwägen, sollten abschätzen, ob, und wenn ja unter welchen spezifischen Bedingungen die Anwendung der Verfolgung des Aufenthaltsortes von Mobilgeräten nach der anwendbaren Datenschutzgesetzgebung in ihrem jeweiligen Rechtsraum gestattet ist.

20. Im Lichte der oben beschriebenen Risiken für den Datenschutz und den Schutz der Privatsphäre wird empfohlen, das Organisationen eine Vorabkontrolle (Privacy Impact Assessment – PIA) durchführen, um sicherzustellen, dass sie alle einschlägigen Risiken vor der Anwendung eines solchen Systems berücksichtigen und minimieren.

21. Organisationen, die die Nutzung von Technologien zur Verfolgung des Aufenthaltsortes erwägen, sollten die einschlägigen von Industrieverbänden für die beabsichtigte Nutzung und Anwendung entwickelten Verhaltensregeln bekannt sein[9] [10] [11]. Die Organisationen werden daran erinnert, dass die Einhaltung von Verhaltensregeln nicht automatisch die Einhaltung aller Anforderungen des national anwendbaren Rechts einschließlich der notwendigen Informationen und Wahlmöglichkeiten für die Nutzer beinhaltet.

22. Anbieter und andere Nutzer solcher Analysetechnologien einschließlich der Hersteller von Produkten, von Betriebssystemen und Entwickler von Apps müssen die Beeinträchtigung der Privatsphäre berücksichtigen, die sich aus der Verfolgung des Aufenthaltsortes ergibt, und bestrebt sein, die Erhebung von Daten zu minimieren, die Aufbewahrungsfristen für Daten zu begrenzen und datenschutzfreundliche Voreinstellungen zu wählen.

23. Zusätzlich zur Einhaltung des anwendbaren Datenschutzrechts und unter Berücksichtigung der Ergebnisse der Vorabkontrolle einschließlich einer Untersuchung, ob eine weniger in die Privatsphäre eingreifende Technologie existiert, die genutzt werden könnte, sollten die folgenden Schutzmaßnahmen beachtet werden:

    a. **Information der Betroffenen** – Organisationen müssen sicherstellen, dass ausreichende Informationen vorhanden sind, einschließlich einer Auswahl von physikalischer und digitaler Kennzeichnung, um Betroffene in klarer Weise darüber zu informieren, dass eine Technologie zur Bestimmung des Aufenthaltsortes verwendet wird. Die Information muss die Zwecke der Erhebung und die verantwortliche Organisation klar benennen. Es wird empfohlen, dass die Industrie einen Standard für ein Symbol entwickelt, dass in dem betreffenden Bereich verwendet werden kann, um die Betroffenen darauf hinzuweisen, dass die Technologie eingesetzt wird, ähnlich den Hinweisen zur Videoüberwachung. Besondere Aufmerksamkeit muss den Beschäftigten, Angestellten oder anderen Einzelpersonen gewidmet werden, die, wenn sie nicht von der Überwachung ausgeschlossen werden, Gegenstand überschießender Datenerhebung werden könnten;

    b. **Begrenzung der Datenerhebung** – Eine Erhebung sollte nur stattfinden, nachdem der Betroffene angemessen informiert worden ist. Organisati-

[9] Future of Privacy Forum, Mobile Location Analytics Code of Conduct. http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf

[10] Network Advertising Initiative, Mobile Application Code. http://www.networkadvertising.org/code-enforcement/mobile

[11] Digital Advertising Alliance, Application of self-Regulatory Principles to the Mobile environment. http://www.aboutads.info/DAA_Mobile_Guidance.pdf

onen sollten die die Beobachtung und die Erhebung von Daten außerhalb ihres Firmengeländes unterlassen. Dies kann durch die sorgfältige Platzierung von Empfängern, die Begrenzung der Erhebung von Daten auf Stichproben und auf spezifische Zeiträume oder Tageszeiten (z. B. während der Öffnungszeiten eines Ladengeschäfts) erreicht werden. Die Häufigkeit der Erhebung sollte auf das für den angestrebten Zweck notwendige Maß beschränkt werden. Die Nutzung von „air gaps" zur Schaffung von nicht-zusammenhängenden Gebieten, in denen Daten erhoben werden und die Beschränkung der Erhebung auf Gebiete, die für den angegebenen Zweck relevant sind, sollten das Risiko der Verletzung der Privatsphäre ebenfalls reduzieren. Organisationen sollten ebenfalls die Festlegung von „Privatsphäre-Zonen" anstreben, in denen als Folge von technischen oder physikalischen Maßnahmen eine Überwachung nicht stattfinden kann. Dies kann in besonders sensiblen Bereichen von Bedeutung sein, wie Toiletten oder Räumen, die der Ersten Hilfe oder dem Gebet gewidmet sind. In Rechtssystemen, in denen eine Überwachung außerhalb des Geländes einer Organisation im Einklang mit den gesetzlichen Bestimmungen durchgeführt werden kann, sollten angemessene Sicherungen zum Schutz der Privatsphäre der Betroffenen vorhanden sein;

c. **Anonymisierung von Daten ohne Zeitverzug** – Organisationen sollten die Löschung oder Anonymisierung von Daten anstreben, sobald diese in ihrer ursprünglichen Form nicht mehr benötigt werden;

d. **Angemessene Aufbewahrungsfristen von Individualdaten** – In Fällen, in denen eine eindeutige rechtliche Grundlage für die Verarbeitung personenbezogener Daten existiert, sollten Organisationen Methoden anwenden, um eindeutige Identifikatoren, wie MAC-Adressen in eine Form umzuwandeln, die das Potenzial zur Beeinträchtigung der Privatsphäre reduziert. Wenn z. B. die Erkennung wiederholter Besuche nicht beabsichtigt ist, kann eine Pseudonymisierung des Identifikators dies verhindern und trotzdem eine ausreichende Analyse der täglichen Kundenfrequenz und der genommenen Wege liefern. Am Ende der gesetzlich erlaubten Speicherungsfrist sollten die betreffenden Daten anonymisiert oder wirksam gelöscht werden. Eine vergleichende Analyse von Ereignissen über verschiedene Berichtsperioden (z. B. die Veränderung von Prozentsätzen von Besuchen in einem bestimmten Zeitraum) kann durch den Vergleich von aggregierten Daten über verschiedene Zeiträume durchgeführt werden;

e. **Einwilligung für die Kombination mit anderen Informationen** – Die Betroffenen sollten umfassend informiert werden, wenn Aufenthaltsinformationen mit anderen Informationen wie z. B. Aufzeichnungen über Geschäftsvorgänge zusammengeführt werden sollen. Dies ist insbeson-

dere relevant, wenn Aufenthaltsinformationen als ein Merkmal zu existierenden Kundenbindungssystemen hinzugefügt werden soll, z. B. durch Hinzufügen der Funktionalität von BLE-Baken zu der existierenden Smartphone-App eines Händlers. Das Akzeptieren eines Updates durch den Nutzer über den App-Store ist wahrscheinlich nicht ausreichend, um als vollständige Information angesehen zu werden. Die Gesetzgebung in einigen Rechtssystemen kann auch die ausdrückliche Einwilligung für bestimmte Arten personenbezogener Daten verlangen[12];

f. **Einwilligung zur Weitergabe von Individualdaten an Dritte** – Organisationen sollten Daten, die zur Identifizierung eines Einzelnen verwendet werden könnten, nicht ohne die gültige, informierte Einwilligung des Betroffenen an Dritte weitergeben (dies schließt die Weitergabe von Daten an andere Kunden oder an einen einzelnen Dritten, der die Analyse von Aufenthaltsinformationen anbietet, ein), soweit es dafür nicht eine gesetzliche Ausnahme gibt; und

g. **Implementierung eines einfachen und effektiven Mittels zur Kontrolle der Erhebung** – Organisationen sollten auch ein System etablieren, das es den Einzelnen erlaubt, die Erhebung solcher Daten auch in den Fällen zu kontrollieren, wo dies nicht ausdrücklich durch das anwendbare Datenschutzrecht gefordert wird. Organisationen sollten gut sichtbar auf die Existenz von Wahl- und Kontrollmöglichkeiten in dem Gebiet hinweisen, in dem die Daten erhoben werden. Dies sollte das Angebot einer leicht zugänglichen, klar beschriebenen und effektiven Möglichkeit einschließen, die Kontrolle auszuüben. Es wird empfohlen, dass ein einheitlicher Mechanismus von allen Anbietern von Aufenthaltsinformationsanalysediensten unterstützt wird und dass der Einzelne seine Präferenz nur einmal ausdrücken muss. Wenn die Verfolgung auf der informierten Einwilligung basiert, muss der Einzelne in die Lage versetzt werden, seine Einwilligung in einfacher und dauerhafter Weise zurückzuziehen. Wo dies technisch möglich ist, werden aussagekräftige Prüfprotokolle empfohlen, die es den Endnutzern ermöglichen, zu wissen, wann und für welche Zwecke Daten über ihre Endgeräte von wem erhoben worden sind. Nutzer sollten auch in die Lage versetzt werden, alle oder Teile der vorher gesammelten Daten zu löschen.

24. Technologien zur Verfolgung des Aufenthaltsortes dürfen nicht zum Abhören des Inhalts von Kommunikation verwendet werden. Im Hinblick auf die strikt persönliche Nutzung der meisten Smartphones besteht eine Notwendigkeit

[12] Z. B. verlangt die Europäische Datenschutzrichtlinie 95/46/EG die ausdrückliche Einwilligung für die Verarbeitung spezieller Kategorien von Daten wie rassische oder ethnische Herkunft, oder in Bezug auf Gesundheit oder Sexualleben. Ähnliche Anforderungen können auch in den gesetzlichen Bestimmungen anderer Rechtsordnungen vorkommen.

für ein hohes Maß an Schutz der Kommunikationsdaten, die von diesen Geräten erzeugt werden, auch jenseits des traditionellen Anwendungsbereichs des Fernmeldegeheimnisses.

25. Gerätehersteller und Hersteller von Netzwerkprotokollen sollten das Potenzial zum Eindringen in die Privatsphäre im Blick behalten, dass aus der Nutzung persistenter Identifikatoren und anderen öffentlich gesendeten Signalen entsteht. Es wird empfohlen, dass, wo dies technisch möglich ist, ein Mechanismus angeboten wird, um solche Identifikatoren in nutzerdefinierten Intervallen zurückzusetzen und dass andere Maßnahmen zum Schutz der Privatsphäre standardmäßig aktiviert sind.

Arbeitspapier zu intelligenter Video-Analysetechnik

– Übersetzung –

Gegenstand

Zunehmend werden intelligente Video-Analysetechniken[1] eingesetzt, um Personen zu erkennen und zu verfolgen, damit ihnen auf sie zugeschnittene Werbung, erhöhte Sicherheit und Kundendienstleistungen geboten werden können. Diese Techniken setzen dazu detaillierte Reichweitenmessungs-Informationen und neue Kanäle und Medien zur Kommunikation mit Einzelnen ein. So soll der Markt für digitale Beschilderung im Jahr 2020 ein Volumen von 23,76 Mrd. US $ erreichen, wobei er schnell mit einer Wachstumsrate von 8,18 % zwischen 2015 und 2020 wachsen soll.[2]

Dieses Papier beschäftigt sich mit dem Einsatz von intelligenter Video-Analysetechnik sowohl im privaten wie im öffentlichen Bereich. Die in diesem Papier untersuchten Techniken werden eingesetzt, um Personen oder Objekte zu erkennen und zu verfolgen, ohne sie zu identifizieren. Dieses Papier bezieht sich auf Weiterentwicklungen von vorhandenen Videoüberwachungssystemen, isolierten smarten Kameranetzen oder digitalen Beschilderungssystemen durch die Ergänzung um intelligente Video-Analysemöglichkeiten wie auch durch neue, speziell entwickelte Systeme, die diese Technologien mit einbeziehen. Dieses Arbeitspapier untersucht die Folgen dieser Technologien für den Datenschutz und enthält Empfehlungen für transparente und datenschutzfreundliche Einsatzmöglichkeiten.

Andere Technologien, die darauf abzielen, Personen mithilfe von Videotechnik und rechnergestützte Bilderfassung wie biometrische Gesichtserkennung oder Kennzeichenerfassungssysteme zu identifizieren, sind nicht Gegenstand dieses Papiers. Sie werden nur insoweit behandelt, als die Unterschiede bezüglich ihrer Auswirkungen auf den Datenschutz deutlich gemacht werden sollen, da bei ihnen besondere Datenschutzgesichtspunkte zum Tragen kommen.

Es sollte berücksichtigt werden, dass erhebliche Folgen für den Datenschutz und den Schutz der Privatsphäre wie auch für andere Menschenrechte eintreten, selbst

[1] Andere Begriffe umfassen Video-Analyse, Video-Inhaltsanalyse, anonyme Video-Analyse, digitale Beschilderung, digitale Reichweitenmessung/Nutzeransprache, digitale Out-of-Home-Werbung/Netze.

[2] S. http://www.marketsandmarkets.com/PressReleases/digital-signage.asp. Digitale Out-Of-Home-Werbung, d. h. Werbung, die Verbraucher erreicht, während sie nicht zuhause sind (auf öffentlichen Plätzen, auf der Reise, in Warteräumen und/oder in speziellen kommerziellen Umgebungen wie Einkaufspassagen) wächst ständig, während Zeitungs-, Zeitschriften- und Radiowerbung permanent zurückgeht.

wenn das Ziel der Technologie nicht die Identifikation oder das Herausgreifen Einzelner ist, deren Bilder durch von Kameras erfasst werden.[3]

Hintergrund

Während die Verfolgung von Nutzern und personalisierte Werbung im Internet[4] bereits ständig passieren, sind solche datengetriebenen Ansätze für die Reichweitenmessung bei Werbung auf der Straße und personalisierter offline-Werbung (digitale Beschilderung) für Verbraucher in der realen Welt noch nicht so gut entwickelt. Werbeflächen, selbst digitale, werden nicht dafür verwendet, um bestimmte soziodemografische oder nutzungsbezogene Messungen durchzuführen, die bei der Online-Werbung üblich sind, wie etwa Informationen darüber, wer die Werbung ansieht, für wie lange und um festzustellen, wie groß die Erfolgsrate einer bestimmten Werbekampagne ist. Darüber hinaus können gewöhnliche Videoüberwachungssysteme für Sicherheitszwecke nicht feststellen, ob sich eine Person vor der Kamera befindet, ob ein geschützter Gegenstand gestohlen wurde oder welche Teile eines Geschäfts oder einer Einkaufspassage besonders stark frequentiert werden. Technologie zur intelligenten Videoanalyse kann diese Information bereitstellen. In naher Zukunft ist zu erwarten, dass Plakate erkennen können, wann und wie lange wir sie ansehen, welchen Geschlechts und wie alt wir sind. Smarte Videokamera- und digitale Beschilderungssysteme können Netzwerke von Sensoren und Anzeigen verwalten und neue Möglichkeiten der Reichweitenmessung und Interaktion mit dem Verbraucher anbieten.

Es gibt auch ein zunehmendes Interesse an sogenannten interaktiver Werbung, die digitale Anzeigetafeln mit Bewegungserkennungssystemen kombiniert, um Personen zur Interaktion oder zum Spiel mit dem Werbetreibenden zu veranlassen – Werbung wird auf diese Weise zum Spiel.

Intelligente Videoanalyse ermöglicht es einer Reihe von Organisationen einschließlich Einzelhändlern, Museen, Flughäfen und Werbetreibenden, die Arten von Personen besser zu bestimmen, denen sie begegnen, diesen ihre Dienstleistungen besser anzupassen und effektiver mit ihnen zu kommunizieren. Aufgrund der Fähigkeit, Gesichter und Gegenstände vor der Kamera oder einer Anzeigetafel zu erkennen und zu verfolgen, und einen Teil ihrer Informationen (wie Alter, Geschlecht, Bewegung und Aufmerksamkeitsspanne, usw.) zu bewerten, kann intelligente Videoanalyse zu folgenden Zwecken eingesetzt werden:

[3] Vgl. den Abschnitt „Konsequenzen der intelligenten Videoanalyse für den Datenschutz“, unten S. 5

[4] Die Arbeitsgruppe hat sich mit diesen Problemen bereits in ihren Arbeitspapieren zu Webtracking und Privatsphäre sowie zur Nutzung von Deep Packet Inspection zu Marketingzwecken auseinandergesetzt, vgl. http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Management

- von Informationsschaltern,
- Erkennung und Optimierung von häufigen Laufwegen, Wärmebilder (heatmaps) zur Laden- und Regal-Optimierung,
- Reichweitenmessungsstatistiken und -analysen wie
  - Höhe- und Tiefpunkte der Besucherzahlen,
  - Zahl und Demografie der Besucher,
  - Vergleich solcher Messungen mit anderen Zeiträumen oder Orten (z. B. zwischen verschiedenen Filialen eines Einzelhandelsunternehmens)
- Erkennung oder Vorhersage von Schlangen oder anderen Engpässen,
- Optimierung des Arbeitskräfteeinsatzes.

Werbung und Preisbildung

- Analyse der Zeitspanne, die mit der Interaktion mit einem Werbeplakat oder Produkten verbracht wird,
- kundenabhängige Werbung,
- kundenabhängige Preisbildung, dynamische Rabattierung, Bonuspunkte und andere Kaufanreize.

Sicherheit und Schutz vor Gefährdung

- Erkennung und Alarmierung bei vergessenen, gestohlenen oder weggetragenen Gegenständen,
- Verletzung von virtuellen Sicherheitslinien,
- Erkennung von Unfällen und ungehörigem/gefährlichem Verhalten[5], und
- Erkennung von Massenansammlungen, Überfüllung usw.

Intelligente Videoanalyse wird Bildverarbeitungstechniken nutzen, um Eigenschaften wie die Art des Gegenstandes, Bewegung, Richtung und Geschwindigkeit innerhalb eines Rahmens festzustellen. Dies wird als eine Frage von Erkennung und Klassifizierung gestellt („Enthält dieses Bild ein Gesicht?“ oder „Ist dies das Gesicht eines Mannes oder einer Frau?“), nicht aber als Frage der Identifizierung („Ist dies John Smith?“ oder „Hat diese Person ein Zutrittsrecht?“). Ein Beispiel für einen typischen Datensatz eines Einzelhandelsgeschäfts, das mit intelligenter Videoanalyse-Technik ausgestattet ist, wäre etwa: Datum des

[5] Z. B. Erkennung und Aktivierung von Sicherheitsmaßnahmen, wenn eine Person in einer U-Bahn-Station ins Gleis fällt.

Eintritts: 12.5.2014, Zeit: 12:02, Geschlecht: männlich, geschätztes Alter: 35, Dauer der Kameraaufnahme; 3 Sekunden, Position: Linker Haupteingang. Diese Daten können graphisch und analytisch verarbeitet werden, um dem Ladeninhaber Informationen zur Geschlechts- und Altersverteilung der Kunden, über die Zahl und Häufigkeit der Besucher, ein Wärmebild (heatmap) des Geschäfts und andere wertvolle Informationen zu geben. Digitale Anzeigetafeln könnten für gezielte Werbung verwendet werden (z. B. Rasurprodukte für Männer, wenn männliche Besucher erkannt werden), Besucher dazu anzuregen, mit der Werbung zu interagieren (z. B. ein Spiel zu spielen, um Bonus- oder Rabattpunkte zu verdienen, indem Gestenerkennung einbezogen wird, durch berührungsempfindliche Bildschirme und die Integration von Smartphones) oder sogar Besucher dazu zu bewegen, dass sie ihr Verhalten im Geschäft mit ihrer Kundenkarte verknüpfen.

Der Umfang möglicher Anwendungen ist nahezu grenzenlos, und praktische Fallstudien reichen von sozialen bis hin zu rein überwachungsorientierten Zwecken. Ein jüngstes Beispiel enthält eine Anzeigenkampagne, die eine verletzte Frau zeigt, um das Bewusstsein für häusliche Gewalt zu erhöhen. Eine kreative Einsatzmöglichkeit von Videoanalyse bestand darin, dass die Dauer der Aufmerksamkeit des Betrachters für die Anzeige registriert wurde, die Zählung der Betrachter aktualisiert und das Bild der Frau langsam so verändert wurde, dass eine Heilung erkennbar war, um so zu verdeutlichen, dass schon bloße Aufmerksamkeit hilft.[6] Andere Einsatzformen von Videoanalyse sind möglicherweise nicht so positiv besetzt.[7]

Die Entwicklung der intelligenten Videoanalyse konvergiert mit anderen Trends wie Mobilkommunikation, sozialen Netzwerken, Cloud-Diensten und interaktiven Diensten. Interaktionen mit Verbrauchern sind stärker in den Vordergrund getreten und erfolgen über zahlreiche Kanäle mit der schnellen Zunahme der Smartphone-Nutzung und neuen mobilen Technologien wie Near Field Communication, Sendern und genaueren Möglichkeiten standortbezogener Dienste. Digitale Werbung auf der Straße kann mit ortsbezogener mobiler Werbung kombiniert werden, indem Big-Data-Technik genutzt wird, um denselben mobilen Kunden auf größeren, wirkungsvolleren Bildschirmen zu erreichen und Werbetreibende in die Lage zu versetzen, bildschirmübergeifende, ortsbezogene Strategien umzusetzen.[8] Die wachsende Zahl digital vernetzter Anzeigetafeln, von denen immer mehr mit Video- und Standortanalyse ausgestattet sind, wird in naher Zukunft zu neuen Risiken für den Datenschutz führen.

---

[6] http://www.oceanoutdoor.com/ocean-news/case-studies/womens-aid-and-ocean-amplify-the-violent-face-of-abuse-with-the-worlds-first-visually-powered-dooh-campaign/

[7] Nach Medienberichten wird das Lächeln der Beschäftigten der Keihin Electric Express Railway in Japan von fortgeschrittenen Videosystemen verfolgt und computergestützt ausgewertet (http://www.economist.com/node/21553408)

[8] http://www.iab.net/iablog/2015/01/top-5-trends-in-DOOH.html

Konsequenzen der intelligenten Videoanalyse für den Datenschutz

Obwohl Personen nicht identifiziert werden, sind die Konsequenzen der intelligenten Videoanalyse für die Privatsphäre, den Datenschutz und andere Menschenrechte immer noch erheblich. Solche Technologien werden von Sicherheitsbehörden eingesetzt, um unangemessenes oder unerwünschtes Verhalten auf öffentlichen Plätzen (z. B. das Schlafen auf Parkbänken) zu erkennen, um Warnungen bei anderen Verstößen anzuzeigen (z. B. Abspielen aufgezeichneter Botschaften, um das Überqueren der Straße bei Rot, das Wegwerfen von Abfall oder das verbotene Parken zu rügen) oder sogar für geschlechts- oder herkunftsbezogene Entscheidungen. Die Übertragung der Kontrolle von den Überwachten zu den Überwachern, die durch solche Systeme herbeigeführt werden kann, führt möglicherweise zu einem Einschüchterungseffekt und verletzt eventuell die Versammlungsfreiheit, das Verbot der Diskriminierung und andere Grundrechte.[9]

Datenschutzrisiken bestehen im nicht-öffentlichen Bereich, sind aber vielleicht weniger sichtbar.[10] Einzelne haben das Recht zu wissen, wer Daten über sie zu welchen Zwecken sammelt und gegenwärtig erwarten nur wenige von uns, dass Kameras unser Alter und Geschlecht bestimmen und uns auf unserem Weg durch die Einkaufspassage verfolgen können. Einige vertreten die Auffassung, dass dies eine Einweg-Spiegel-Gesellschaft entstehen lässt, wenn Verbraucher nicht über solche Praktiken informiert werden und keine Möglichkeit haben, die Überwachung im Einzelhandel, in öffentlichen oder anderen Räumen zu kontrollieren oder der Analyse ihres Verhaltens für Werbezwecke oder zur Steigerung des Gewinns zuzustimmen.[11]

Wirtschaftsverbände[12] und Datenschutzexperten[13] [14] [15] haben bereits gewarnt, dass ein angemessener Umgang mit den Risiken für die Privatsphäre, den Datenschutz

[9] Siehe Adams, Andrew A. und Ferryman, James M., The Future of Video Analytics for Surveillance and ist Ethical Implications (12. November 2012). Security Journal, demnächst erscheinend, abrufbar unter SSRN: http://ssrn.com/abstract=2174255

[10] Das kann in unterschiedlichen Formen auftreten, von nicht-eingriffsintensiven Zählungen der Betrachter über mittelschwere Eingriffe bei geschlechtsspezifischer Werbung bis hin zu starken Eingriffen durch die Erkennung von ungehörigen oder rechtswidrigen Aktivitäten, rein personalisierter Werbung, Schaffung von schwarzen Listen usw.

[11] Dixon, Pam: The One-Way-Mirror-Society. Privacy Implications of the new Digital Signage Networks, 2010. Abrufbar unter http://www.worldprivacyforum.org/wp-content/uploads/2013/01/onewaymirrorsocietyfs.pdf

[12] Siehe Digital Signage Federation: Digital Signage Privacy Standards. Abrufbar unter: 2011, http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002–2011%20%283%29.pdf

[13] S. Center for Democracy and Technology (CDT). A Framework for Digital Signage Privacy, 2010. Abrufbar unter: https://www.cdt.org/files/pdfs/A_Framework_for_Digital_Signage_Privacy-Center_for_Democracy_and_Technology-March_2010.pdf

[14] Vgl. Information and Privacy Commissioner, Ontario. White Paper: Anonymous Video Analytics (AVA) technology and privacy, 2011. Abrufbar unter: http://www.ipc.on.ca/images/Resources/AVAwhite6.pdf

[15] Vgl. Federal Trade Commission (FTC) report Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. Abrufbar unter: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

und die Transparenz entscheidend ist, um das Vertrauen der Verbraucher zu gewinnen. Vertrauen ist eine grundlegende Voraussetzung für das weitere Wachstum und die Entwicklung von digitaler Straßenwerbung, die gegenwärtig der Hauptanwendungsbereich von Videoanalyse ist.[16] Darüber hinaus zeigte eine Untersuchung[17] aus dem Jahr 2009, dass 90 % der jungen Erwachsenen in den USA Werbung ablehnen, die aufgrund der Offline-Aktivitäten einer Person auf diese zugeschnitten ist. Einige Verbände von Anbietern haben Maßnahmen für eine Selbstregulierung ergriffen, indem sie Verhaltenskodizes[18] und Richtlinien[19] zur Beachtung des Datenschutzes bei digitaler Straßenwerbung beschlossen haben. Sie haben erkannt, dass ein proaktiver und rechtzeitiger Ansatz notwendig ist, um eine Regulierung durch Gesetzgeber zu vermeiden, wie es bei der Regulierung des Web-Tracking und der Werbung in der Europäischen Union der Fall war. Es gibt auch Beispiele für Regulierung auf nationaler Ebene wie in Frankreich.[20]

Die Konsequenzen intelligenter Videoanalyse für die Privatsphäre und den Datenschutz unterscheiden sich abhängig vom Grad der Komplexität und den Fähigkeiten solcher Systeme. Die meisten Untersuchungen, die sich mit diesen Fragen befassen, unterscheiden zwischen drei Kategorien oder Ebenen. Die Unterteilung in gemeinsame Kategorien ist hilfreich, um die große Spannbreite von Lösungen und Konsequenzen für den Datenschutz zu behandeln, indem man auf die Gemeinsamkeiten bestimmter Anwendungen schaut. Für die Zwecke dieses Papiers werden Technologien oder Systeme der intelligenten Videoanalyse in die folgenden drei Kategorien unterteilt:

Erkennung (Detektion). In diesen Fällen wird der Einzelne einfach wie ein Objekt behandelt, während seine oder ihre persönlichen Eigenschaften wie Geschlecht oder Alter nicht vorhergesagt werden. Bilder werden nicht zwingend gespeichert, Daten werden aggregiert und die Verwendung für Werbezwecke ist begrenzt. Informationen über individuelle Eigenschaften werden weder erhoben noch verarbeitet. Beispiele sind die Erkennung gestohlener oder wegbewegter Gegenstände, Verletzungen eines Sicherheitsbereichs, Wärmebilder von Geschäften, Informationsschalter, Gestenerkennung und die Beobachtung der Länge von Menschen-Schlangen.

---

[16] http://www.digitalsignageconnection.com/how-emerging-privacy-issues-could-impact-digital-signage-success

[17] Americans Reject Tailored Advertising. Abrufbar unter: https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf

[18] Vgl.: POPAI – THE GLOBAL ASSOCIATION FOR MARKETING AT RETAIL, Digital Signage Group. Best Practices: Recommended Code of Conduct for Consumer Tracking Research, 2010. Abrufbar unter: http://www.popai.com/docs/DS/2010dscc.pdf

[19] Vgl.: Digital Signage Federation Privacy Standards: www.DigitalSignageFederation.org

[20] Das Umweltschutzgesetz "Grenelle II„ (2010-788 vom 12. Juli 2010) gibt der französischen Datenschutzbehörde (CNIL) die Befugnis, den Einsatz von Geräten für die Messung von Betrachterzahlen von digitalen Werbetafeln in öffentlichen Räumen wie Einkaufspassagen, Bahnhöfen und Flughäfen zu regulieren. Jedes System, das automatisch die Betrachter einer digitalen Werbetafel misst oder das die Eigenschaften oder das Verhalten von Personen analysiert, die in der Nähe solcher Werbetafeln vorbeigehen, bedarf der vorherigen Genehmigung durch die CNIL.

Einteilung (Klassifizierung). Diese Anwendungsformen der intelligenten Videoanalyse erheben und verarbeiten die erkannten Bilder, um Aussagen über das Geschlecht, das Alter oder über das Verhalten zu treffen, so dass der Einzelne im Regelfall nicht herausgegriffen oder identifiziert wird. Daten werden für die an bestimmte Kundensegmente gerichtete oder angepasste Werbung verwendet, aber sie werden nicht mit anderen Daten verknüpft, die die Identifikation des Einzelnen ermöglicht (z. B. mit Daten aus Kundenbindungsprogrammen, Smartphone-Daten). Zu den Beispielen gehören digitale Werbetafeln, die Alter und Geschlecht der Betrachter erkennen und segment-spezifische Werbung anzeigen (z. B. für Senioren, Frauen in der Altersgruppe von 20 – 30 Jahren usw.). Es muss betont werden, dass in dem Maße, in dem die Zahl der Datenarten mit Bezug auf eine einzelne Person steigt, auch die Wahrscheinlichkeit der Identifikation wächst, da sie mit größerer Wahrscheinlichkeit in dieser Kombination nur einmal vorkommen. Auch wenn diese Art der Datenverarbeitung nicht auf die Identifikation von Personen abzielt, werden diese bestimmten Marktsegmenten zugeordnet, und deshalb können Einzelpersonen aufgrund der Klassifizierung unterschiedlich behandelt werden, je nach dem welchem Segment sie zugeordnet werden. Dies birgt Risiken der Diskriminierung oder Stigmatisierung (aufgrund des Geschlechts oder der Rasse).[21]

Identifikation. Der Zweck der Datenverarbeitung ist die Identifikation oder das Herausgreifen Einzelner und die Ausspielung oder das Angebot von personalisierter Werbung, Diensten und Maßnahmen. Erhobene Daten allein oder in Verbindung mit anderen Daten ermöglichen das Herausgreifen oder die Identifikation des Einzelnen. Zu den Beispielen gehören intelligente digitale Werbeanzeigen, die Einzelpersonen identifizieren, Verknüpfungen mit Kundenbindungsprogrammen oder Profilen aus sozialen Netzwerken, Systeme zur biometrischen Gesichtserkennung, automatische Kennzeichenerfassungssysteme, usw.

Videoanalyse, die zur Erkennung (Detektion) und Einteilung (Klassifizierung) führt, stellt eine Verarbeitung personenbezogener Daten dar und bedarf als solche einer angemessenen Behandlung der Risiken. Bei Zugrundelegung des Datensparsamkeitsprinzips, indem keine Bilder oder aus Bildern abgeleitete eindeutige Kennzeichen[22] gespeichert werden, kann ein wirksamerer Datenschutz des Einzelnen erreicht werden. Die sorgfältige Anbringung von Videokameras, um

[21] Es sollte in diesem Zusammenhang betont werden, dass die Zahl der Klassen und der strukturelle Reichtum der erhobenen Daten eine Rolle bei der Identifikation einer Person spielen kann. Die Abgrenzung zwischen bloßer Erkennung (Detektion), Einteilung (Klassifizierung) und Identifizierung hängt unter bestimmten Umständen sehr stark von der Zahl der Personen ab, die „gezählt" und einer Gruppe zugeordnet wurden. Um das Risiko der Identifizierung zu verringern, sollten nur diejenigen Attribute genutzt werden, die unbedingt für das Einteilungskriterium erforderlich sind, und eine Mindestgröße für jede Gruppe sollte festgelegt werden.

[22] Eine gewisse Vorhaltung von Daten, wenngleich vorübergehend, kann in bestimmten Fällen nötig sein. Das sind möglicherweise nicht die Rohdaten, sondern ein relevanter Extrakt oder eine Ableitung aus den Bilddaten, die für Vergleichszwecke benötigt werden.

sensitive Bereiche auszusparen, bietet eine andere Form des Schutzes.[23] Dennoch werden auch in der Phase der Erkennung und Einteilung personenbezogene Daten verarbeitet, wenngleich nur für eine kurze Zeitspanne, was immer noch Auswirkungen auf den Einzelnen haben kann.[24]

Empfehlungen

Die Arbeitsgruppe ist der Auffassung, dass intelligente Videoanalyse zwar eine Reihe von Vorteilen in verschiedenen Bereichen wie Sicherheit, Verwaltung, und Werbung haben kann, dass Datenschutz und Schutz der Privatsphäre gleichwohl respektiert werden müssen.

Rechtmäßigkeit und Fairness

Intelligente Videoanalyse sollte nur unter Bedingungen eingesetzt werden, die im Verhältnis zu den Auswirkungen auf die Privatsphäre und den Datenschutz angemessen sind. Unter Berücksichtigung der Gemeinsamkeiten von Detektions- und Klassifikationsanwendungen sollten die Grundsätze der Rechtmäßigkeit und der Fairness in erster Linie durch angemessene Transparenzvorkehrungen beachtet werden. Personen sollten vollständig darüber informiert und darauf hingewiesen werden, dass intelligente Videoanalyse eingesetzt wird, und sie sollten in eindeutiger und verständlicher Weise darüber aufgeklärt werden, was dies für sie bedeutet. Der Einsatz von intelligenter Videoanalyse im öffentlichen Bereich, insbesondere für Zwecke der Strafverfolgung und Gefahrenabwehr, sollte jedenfalls gesetzlich geregelt werden.

Identifikationsanwendungen, bei denen der Einzelne herausgegriffen oder identifiziert wird, sind rechtmäßig nur unter strengeren Bedingungen zulässig. Rechtsgrundlagen können die Einwilligung des Einzelnen, ein Gesetz oder Verfahren der Vorabgenehmigung nach nationaler Gesetzgebung sein. Andere Ansätze wie Gütesiegel, Normen oder Zertifizierung können auch in Betracht kommen. Die bloße Ankündigung und die Möglichkeit des Widerspruchs reichen für die Anwendung von Videoanalyse zu Identifikationszwecken wahrscheinlich nicht aus, da diese Anwendung datenschutzrechtlich intensiver in die Rechte des Einzelnen eingreift Außerdem wären verschiedene Systeme mit Widerspruchsmöglichkeiten bei den unterschiedlichen Anbietern von digitalen Werbetafeln sehr nutzerunfreundlich. Die Arbeitsgruppe legt den Anbietern von interaktiven Werbetafeln

[23] Federal Trade Commission, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (2012), https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies, S. 13.

[24] Ein eindeutiges Beispiel wäre die falsche Zuordnung zu einem Segment – eine Person wird fälschlich als Mann angesehen (oder umgekehrt) und ihm wird eine geschlechtsspezifische oder ethnisch-basierte Werbung angezeigt. Andere Konsequenzen wären vorstellbar, wenn etwa eine Person versehentlich als betrunken in der Öffentlichkeit, angeblich bei einem Einbruch oder Diebstahl identifiziert wird.

dringend die Entwicklung von nutzerfreundlichen Widerspruchs- oder Einwilligungsmöglichkeiten nahe[25].

Besondere Aufmerksamkeit sollte der Verarbeitung von besonderen Datenkategorien gelten, wie etwa von Gesundheitsdaten oder Daten über die ethnische Herkunft, die zu Diskriminierung oder anderen negativen Folgen für die Betroffenen führen kann. Die Erhebung oder Verarbeitung solcher Datenarten durch Verfahren der intelligenten Videoanalyse sollten ausdrücklich vermieden werden. Darüber hinaus sollte für eine faire Datenverarbeitung keine automatisierte Einzelentscheidung auf Bewertungen des Verhaltens durch intelligente Videoanalyse-Systeme gestützt werden (insbesondere im Fall der Profilbildung aufgrund von sensitiven Daten wie Rasse oder Gesundheit). Solche Entscheidungen setzen zumindest die Überprüfung durch einen Menschen voraus.

Transparenz

Personen sollten angemessen über die Verwendung intelligenter Videoanalyse informiert werden. Es ist durchaus vernünftig zu erwarten, dass der Einzelne wissen will, von wem und zu welchen Zwecken Daten über sein oder ihr Geschlecht, Alter und Bewegungen erhoben und verarbeitet werden. Betroffene sollten wissen, wann sie „normaler" Kameraüberwachung ausgesetzt werden, die lediglich Bilder speichert, oder ob das System ihre Bewegungen verfolgen, ihr Verhalten beurteilen und ihre Aufmerksamkeitsspanne gegenüber bestimmten digitalen Anzeigetafeln messen kann. Wie bereits betont wurde, ist die Frage der Transparenz bereits von verschiedenen Akteuren als eine der wichtigsten Voraussetzungen zur Vertrauensbildung und zur Sicherung des künftigen Wachstums und der Entwicklung intelligenter Videoanalyse-Lösungen erkannt worden, insbesondere im Bereich der digitalen Straßenwerbung und der digitalen Beschilderung.[26] Intransparente Anwendungen[27] könnten das Vertrauen der Nutzer gravierend beeinträchtigen und Wachstum und Entwicklung gefährden.

Um sicherzustellen, dass die Betroffenen vollständig informiert werden, empfiehlt die Arbeitsgruppe, dass die Unternehmen ein gestuftes Verfahren verwenden, um ein angemessenes Transparenzniveau zu erreichen. Bei einem solchen Verfahren

[25] Vgl. Article 29 Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[26] http://www.digitalsignageconnection.com/how-emerging-privacy-issues-could-impact-digital-signage-success

[27] Ein Beispiel für eine inakzeptable Anwendung ist eine personalisierte digitale Anzeigenkampagne für Motoröl in London. Wenn Fahrzeuge sich der digitalen Anzeigetafel näherten, wurden Bilder mit den Fahrzeugkennzeichen erhoben und mit einer Fahrzeug-Datenbank abgeglichen. Die Anzeigetafel zeigte dann eine auf das jeweilige Fabrikat und Fahrzeugmodell zugeschnittene Werbeanzeige. Die Kampagne wurde aufgrund von Problemen in Bezug auf Transparenz und Rechtmäßigkeit schnell eingestellt.

wird die wesentliche Information bei der Erhebung gegeben, die durch detailliertere Informationen auf verschiedenen Kanälen ergänzt werden kann, z. B. auf Plakaten in der Nähe, durch Faltblätter oder Informationen auf Webseiten.

Bei der Datenerhebung sollten Verbraucher einen klaren, hervorgehobenen Hinweis darauf erhalten, welche Geräte ihre persönlichen Daten verarbeiten, so dass der Einzelne sicher sein kann, in welchem Bereich das Gerät (bzw. die Geräte) aktiv ist bzw. sind. Soweit möglich sollte der Hinweis erkennbar in der Nähe jedes Geräts angebracht werden, dass die Daten sammelt (ein Hinweis für eine ganze Einkaufspassage oder ein Flughafengebäude ist nicht ausreichend). Vorhandene Hinweise auf die Arbeitsweise von herkömmlichen Videoüberwachungssystemen wären ohne Modifikation unzureichend und der Einsatz von nicht-gekennzeichneten oder versteckten Geräten oder Sensoren sollte nicht zugelassen werden. Die Entwicklung gemeinsamer standardisierter Piktogramme könnte in der Zukunft möglich sein, was die Erkennbarkeit für die Nutzer vereinfachen und verbessern würde.

Der Hinweis sollte die folgenden Informationen enthalten:

- den Zweck des Geräts/Systems,
- Information über die verantwortliche Stelle,
- Information über die erhobenen Daten,
- Nutzer der erhobenen Daten,
- Information darüber, ob die Daten mit anderen Daten verknüpft werden,
- wo weitere Informationen und Details in Erfahrung gebracht werden können.

Um vollständig transparent und fair zu sein, sollte der Hinweis auch die wesentlichen Zusicherungen enthalten (wie die Information, dass Bilder oder aus den Bildern abgeleitete eindeutige Kennzeichen nicht gespeichert und dass die Daten nicht mit anderen Quellen verknüpft werden).

Schließlich sollten detaillierte Informationen über das System für Einzelne leicht zugänglich sein, etwa durch eine im Internet veröffentlichte Datenschutzerklärung, über Telefon oder durch Informationspunkte vor Ort.

Verhältnismäßigkeit (Datensparsamkeit und -bevorratung)

Um den Grundsatz der Verhältnismäßigkeit zu beachten, sollte das Konzept „Privacy by Design“ (datenschutzgerechte Technikgestaltung) umgesetzt werden. Betreiber von Systemen der intelligenten Videoanalyse sollten Datenschutz-Folgeabschätzungen durchführen, um die Risiken zu erkennen und nötige Sicherheitsmaßnahmen rechtzeitig zu ergreifen. Umgehende Löschung der Bilder oder

der aus den Bildern abgeleiteten eindeutigen Kennzeichen, sofortige Anonymisierung der erhobenen Daten und die Löschung historischer Rohdaten können die Risiken wesentlich verringern.

Zusätzlich sollten Betreiber prüfen, ob der Verarbeitungszweck tatsächlich eine ständige Analyse erfordert, oder ob zeitliche und geografische Begrenzungen die Erreichung des Zwecks ebenso zulassen würden. So kann der Einsatz des Systems beispielsweise auf die Öffnungszeiten oder Arbeitstage begrenzt werden und Abschaltzeiten können in Betracht gezogen werden (wobei die Messung nur an jedem zweiten Tag oder in jeder zweiten Woche oder nach anderen Stichproben erfolgt). Schließlich und insbesondere sollten Betreiber berücksichtigen, dass Videoanalyse an bestimmten Orten wie Saunen, Schwimmbädern, Gotteshäusern und Krankenhäusern verboten sein kann.

Zweckbindung

Berücksichtigung der Zweckbindung kann durch richtige Hinweise und Maßnahmen zur Verantwortlichkeit erreicht werden, die die Verwendung der erhobenen Daten begrenzen. Daten sollten nicht für Zwecke verwendet werden, die nicht ausdrücklich festgelegt und den Betroffenen mitgeteilt wurden. Es besteht ein reales Risiko, dass Daten, die für bestimmte Zwecke wie Verwaltung oder Sicherheit erhoben wurden, für andere im Wesentlichen unvereinbare Zwecke wie Werbung oder Überwachung verwendet werden. Es gibt auch eine reale Gefahr, dass Daten für neue Zwecke verwendet werden (bekannt als „schleichende Zweckentfremdung"), und zwar hinter dem Rücken der Betroffenen, was zu neuen, unvorhergesehenen Datenschutzrisiken führen wird.

Datenqualität

Die Frage der Datenqualität ist in diesem Zusammenhang von besonderer Bedeutung. Fragen der Richtigkeit und Aktualität der Daten sollten bei der Datenschutz-Folgenabschätzung genau analysiert werden und verschiedene alternative Verfahren sollten vorgesehen werden.

Es ist hervorzuheben, dass alle Anwendungen von intelligenter Videoanalyse innerhalb bestimmter Bandbreiten von Genauigkeit funktionieren und deshalb zu einer nicht ganz genauen Erkennung von Personen, Gegenständen und Bewegungen führen können. Die Folgen einer ungenauen Erkennung werden vom Zweck des Videoanalyse-Systems abhängen.

Dies ist von besonderer Bedeutung beim Einsatz von Videoanalyse im öffentlichen Bereich, vor allem, wenn sie von Sicherheitsbehörden verwendet wird (z. B. zur Erkennung von ungewöhnlichen Bewegungen oder ungewöhnlichem Verhal-

ten im öffentlichen Raum). Fragen der Genauigkeit können in diesem Fall gravierende Folgen für den Einzelnen haben.[28]

Datensicherheit

Angemessene Verfahren und Maßnahmen sollten eingesetzt oder ergriffen werden, um sicherzustellen, dass die Daten vor unbefugtem Zugriff, vor Veränderung oder Zerstörung geschützt sind. Besondere Aufmerksamkeit sollte der Frage gewidmet werden, wie die Datenschutzrisiken erkannt und begrenzt werden können, die mit der Verwendung von Anonymisierungstechniken verbunden sind.[29] Dies sollte ebenfalls berücksichtigt werden, wenn die Zwecke und der Umfang der erhobenen Daten im Rahmen der Datenschutz-Folgeabschätzung beurteilt werden.

Rechte des Betroffenen

Detektions- und Klassifizierungsaufgaben erfordern nicht die Speicherung der verarbeiteten Bilder oder irgendwelcher aus den Bilddaten abgeleiteten eindeutigen Kennzeichen, denn sie können mit aggregierten Daten und Statistiken durchgeführt werden. Deshalb sind die Daten nicht personenbezogen. Anwendungen zur Identifizierung unterscheiden sich davon natürlich erheblich. In diesen Fällen spielt das Recht auf Zugang zu den eigenen Daten, auf Berichtigung oder Löschung unrechtmäßig erhobener oder falscher Daten eine wichtige Rolle, z. B. bei Videoanalyse-Systeme, die Gesichtserkennung, Kennzeichenerfassung, personalisierte Werbung und andere Technologien verwenden.

[28] Dasselbe kann auch im privaten Bereich gelten (z. B. im Fall der Videoerkennung von Kfz-Kennzeichen und der Erstellung von schwarzen Listen von Fahrern etwa durch Tankstellen).

[29] Vgl. z. B. Article 29 Working Party Opinion on anonymization techniques, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

B. Dokumente zur Informationsfreiheit

I. Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

1. Entschließungen der 30. Konferenz am 30. Juni 2015 in Schwerin

Mehr Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP)!

Die Bundesregierung hat sich dafür ausgesprochen, noch im Jahr 2015 das geplante Freihandelsabkommen (Transatlantic Trade and Investment Partnership, TTIP) zwischen der EU und den Vereinigten Staaten von Amerika zu verabschieden. Mit dem geplanten Abkommen würde die derzeit weltgrößte Freihandelszone entstehen.

Seit der Aufnahme der Verhandlungen zwischen der EU und den USA im Jahr 2013 wurden deren Intransparenz und der spärliche Informationsfluss kritisiert. Als Reaktion auf diese Kritik hat die EU-Handelskommissarin Cecilia Malmström im November 2014 mehr Transparenz versprochen. In diesem Rahmen hat sich die Europäische Kommission dazu verpflichtet, die Öffentlichkeit darüber zu informieren, mit wem sich ihre führenden Politiker und höheren Beamten treffen und einen erweiterten Zugang zu Dokumenten im Zusammenhang mit den Verhandlungen über eine transatlantische Handels- und Investitionspartnerschaft mit den Vereinigten Staaten zu ermöglichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) sieht diese Initiative als einen wichtigen ersten Schritt hin zu mehr Offenheit und mahnt deren Fortführung und Ausweitung dringlich an. Sie hebt die Notwendigkeit größtmöglicher Transparenz in den Verhandlungen für eine lebendige öffentliche Debatte hervor, in der die Bürgerinnen und Bürger vollständig über die Auswirkungen auf ihr tägliches Leben informiert werden. Die Informationsfreiheitsbeauftragten fordern im Sinne von Open Government Data, der Öffentlichkeit neben zusammenfassenden und erläuternden Informationen vermehrt Originaldokumente zur Verfügung zu stellen, um es den Bürgerinnen und Bürgern zu ermöglichen, sich eine eigene Meinung von den Inhalten und dem Ablauf der Verhandlungen zu bilden. Hierzu gehören auch Informationen über die Positionen

und Forderungen der USA sowie von Lobbyisten. Eine umfassende Offenlegung von Informationen zu TTIP auf EU- sowie auf Bundes-Ebene soll so früh und so weit wie möglich erfolgen. Erst wenn Originaldokumente aus den Bereichen Umwelt-, Arbeitnehmer- und Verbraucherschutz bekannt sind, kann beurteilt werden, ob es zu einer Absenkung europäischer Standards kommt.

Die IFK fordert die Bundesregierung und die Europäische Kommission dazu auf, in den Verhandlungen mit den USA darauf zu bestehen, dass für Streitigkeiten zwischen den Handelspartnern öffentlich tagende hoheitliche Gerichte geschaffen werden. Nur dadurch kann die notwendige Transparenz gewährleistet werden.

Auch Kammern sind zur Transparenz verpflichtet!

Immer wieder verweigern sich berufsständische Kammern den Transparenzanforderungen der jeweiligen Informationszugangsgesetze.

Berufsständische Kammern nehmen hoheitliche Aufgaben auf Bundes- und Länderebene wahr. Für die jeweiligen Berufsgruppen besteht eine gesetzliche Pflicht zur Mitgliedschaft, die Kammern sind für Berufszulassungen zuständig und haben oft weitgehende Sanktionsmöglichkeiten.

Informationen, die im Rahmen ihrer Tätigkeit anfallen, unterfallen den Informationszugangsgesetzen von Bund und Ländern. Dies gilt auch für Jahresabschlüsse und Angaben zu Einnahmen, Ausgaben und Rückstellungen der Kammern. Für die Verpflichtung der Kammern ist es unerheblich, ob Antragstellende Kammermitglieder sind und welche Motive zur Antragstellung führten. Öffentlich-rechtliche Körperschaften befinden sich in weiten Bereichen nicht in Konkurrenz zu Marktteilnehmern – Wettbewerbsnachteile können sich zumeist nicht ergeben. Folglich stehen schutzwürdige Betriebs- und Geschäftsgeheimnisse einem Informationszugang in der Regel nicht entgegen.

Ansprüche auf Informationszugang sind unverzüglich, spätestens jedoch innerhalb der in den Informationszugangsgesetzen des Bundes bzw. der Länder genannten Fristen zu erfüllen. Eine Entscheidung darf nicht auf Gremiensitzungen verschoben, sondern sollte im Rahmen der regulären Geschäftsführung getroffen werden. Im Übrigen sind transparenzpflichtige Informationen der berufsständischen Kammern in den bereits vorhandenen Informationsregistern zu veröffentlichen.

Die Informationsfreiheitsbeauftragten in Deutschland fordern daher die berufsständischen Kammern auf, ihren Transparenzverpflichtungen nachzukommen.

2. Entschließung zwischen der 30. und 31. Konferenz

Informationsfreiheit 2.0 – endlich gleiches Recht in Bund und Ländern![*] (vom 4. Dezember 2015)

Vor zehn Jahren hat der Deutsche Bundestag das Informationsfreiheitsgesetz verabschiedet und damit für solche Länder, die bislang noch kein derartiges Gesetz kannten, ein Beispiel gegeben. Inzwischen besteht in elf Ländern ein Recht auf Zugang zu Verwaltungsinformationen, ohne dass die Antragsteller ihr Einsichtsinteresse begründen müssen.

Trotz einer flächendeckenden Entwicklung hin zu mehr Verwaltungstransparenz besteht weiterhin Handlungsbedarf. So zeigen weder Bayern noch Hessen Bestrebungen, Informationsfreiheitsgesetze zu schaffen. Die niedersächsische Landesregierung hat zwar beschlossen, einen Entwurf vorzulegen, berät aber noch über die Einzelheiten. In Sachsen soll bis spätestens 2019 ein Informationsfreiheitsgesetz geschaffen werden. Indes enttäuscht der lange erwartete Gesetzentwurf der baden-württembergischen Landesregierung durch viele überflüssige Einschränkungen. Das brandenburgische Beispiel zeigt, dass auch die Novellierung vorhandener Gesetze dazu dienen kann, das Rad durch die Schaffung neuer Ausnahmen zurückzudrehen. Die Umsetzung der Evaluation des Informationsfreiheitsgesetzes des Bundes steht noch aus. Ob dort – ebenso wie bereits in den Transparenzgesetzen von Hamburg und Bremen – Verwaltungen verpflichtet werden, bestimmte Informationen von sich aus im Internet zu veröffentlichen, ist ungewiss. In Rheinland-Pfalz tritt zum 01. Januar 2016 als erstem Flächenland ein solches Transparenzgesetz in Kraft. Es umfasst auch das im Übrigen bundesweit eingeführte Recht auf Zugang zu Umweltinformationen. Auch in Thüringen und Nordrhein-Westfalen ist laut Koalitionsvertrag beabsichtigt, das derzeitige Informationsfreiheitsgesetz zu einem Transparenzgesetz fortzuentwickeln.

Nach Auffassung der Informationsfreiheitsbeauftragten sollten moderne Regelungen über den Informationszugang in Form effektiver Transparenzgesetze

1. der herkömmlichen Informationserteilung auf Antrag eine Pflicht der Verwaltung zur proaktiven Veröffentlichung von Informationen in Open-Data-Portalen zur Seite stellen,
2. Ausnahmen vom freien Zugang zu Informationen nur in einem unbedingt erforderlichen Maß enthalten,
3. neben klassischen Verwaltungen auch Unternehmen der öffentlichen Hand einbeziehen und

[*] bei Stimmenthaltung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

4. der vorhandenen Rechtszersplitterung auf dem Gebiet der Informationsfreiheit entgegenwirken und das Umweltinformationsrecht mit dem Informationsfreiheitsrecht zusammenführen.

Sowohl bei der Novellierung vorhandener als auch bei der Schaffung neuer Regelungen muss die Erhöhung der Transparenz oberstes Ziel sein. Nach Auffassung der Informationsfreiheitsbeauftragten gibt es keinen vernünftigen Grund dafür, dass einige Länder noch immer kein Recht auf voraussetzungslosen Zugang zu Informationen haben.

Die Informationsfreiheit hat dort, wo sie eingeführt wurde, zu mehr staatlicher Transparenz, einer besseren Informiertheit der Bürger und einer offeneren Verwaltungskultur geführt. Transparenzgesetze und Open-Data-Plattformen im Internet haben diese Wirkung in erfreulicher Weise befördert. Die Befürchtung von Kritikern, dass Verwaltungen von einer Antragsflut überrannt würden, hat sich nicht bewahrheitet.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Gesetzgeber in Bund und Ländern auf, die positiven Erfahrungen mit der Informationsfreiheit in Deutschland anzuerkennen und die Einheitlichkeit der Lebensbedingungen auch im Bereich der Verwaltungstransparenz herzustellen.

II. Internationale Konferenz der Informationsfreiheitsbeauftragten (ICIC)

Entschließung der 9. Konferenz vom 21. – 23. April 2015 in Santiago de Chile

In Santiago de Chile fand am 21. April 2015 im Zusammenhang mit der 9. Internationalen Konferenz der Beauftragten für die Informationsfreiheit, ICIC, eine private Arbeitssitzung statt, an der 33 Beauftragte aus 25 Ländern teilnahmen.

Gemäß dem Arbeitsprogramm, das vom Rat für Transparenz als Gastgeber und Veranstalter dieser Sitzung vorgeschlagen wurde, bildeten die Beauftragten vier Arbeitsgruppen zum Zweck der Untersuchung folgender Themen:

1. Erfahrungsaustausch über die Zusammenarbeit und in Bezug auf die Verwaltung und Umsetzung von Gesetzen über den Zugang zu Informationen.
2. Die Inanspruchnahme der Mediation und anderer Formen alternativer Streitbeilegung bei Streitigkeiten von Bürgern mit öffentlichen Behörden als Instrument zur Beschleunigung des Zugangs zu Informationen: Vorteile, Nachteile und die wichtigsten Ergebnisse.
3. Ermittlung von Messverfahren in der Umsetzung öffentlicher Politiken der Transparenz und das Recht auf Zugang zu öffentlichen Informationen.
4. Vergleichende Rechtsprechung.

Schlussfolgerungen und Vereinbarungen der oben erwähnten Arbeitsgruppen sind nachstehend aufgeführt:

1. Schlussfolgerungen und Gruppenvereinbarungen über den „Erfahrungsaustausch über die Zusammenarbeit und in Bezug auf die Verwaltung und Umsetzung von Gesetzen über den Zugang zu Informationen“

1.a) Abkommen über die Zweckmäßigkeit des Strebens nach der Einrichtung eines ständigen Mechanismus für die ICIC durch eine einfache, funktionelle, unbürokratische Struktur, die sich folgender Notwendigkeiten annimmt:

- Untersuchung der Funktionsweise von anderen Netzen,
- Fortsetzung und Nachbereitung der auf den Sitzungen erörterten Themen,

- Förderung und Koordinierung des Austausches von Erfahrungen und bewährter Verfahren,
- Alle relevanten Informationen werden zugänglich gemacht und der Prozess der Einführung neuer Rechtsvorschriften und institutioneller Rahmenbedingungen wird gefördert und unterstützt.

1.b) Für die Entwicklung eines Vorschlags für diese funktionelle Struktur wurde die Beauftragung einer Arbeitsgruppe vereinbart, die aus mindestens drei und maximal fünf Ländern besteht, alles Mitglieder der ICIC, die die mögliche Struktur für diesen Koordinationsmechanismus im Einklang mit den ermittelten Erfordernissen gründlich untersucht.

Die Arbeitsgruppe besteht aus folgenden Mitgliedern: The Office of the Information Commissioner of Canada, the Office of the Scottish Information Commissioner, Indonesia Information Commissioner, the Federal Institute for Access to Public Information and Data Protection of Mexico, the Institute for Access to Public Information of Honduras, und dem Council for Transparency of Chile (Das Bundesinstitut von Mexiko für den Zugang zu öffentlichen Informationen und den Schutz der Daten, das Institut von Honduras für den Zugang zu öffentlichen Informationen, und der Chilenische Rat für die Transparenz).

2. Schlussfolgerungen und Gruppenvereinbarungen über die „Inanspruchnahme der Mediation und anderer Formen alternativer Streitbeilegung bei Streitigkeiten von Bürgern mit öffentlichen Behörden als Instrument zur Beschleunigung des Zugangs zu Informationen: Vorteile, Nachteile und die wichtigsten Ergebnisse".

2.a) Die Wichtigkeit der Umsetzung von Formen der alternativen Streitbeilegung in den Bereich des Rechts auf Zugang zu öffentlichen Informationen wird anerkannt.

2.b) Diese Formen der alternativen Streitbeilegung sollten ein partizipatives Instrument sein, bei dem sowohl die Bürger als auch öffentliche Organe bei den Verfahren zur Lösung des Konflikts notwendig sind.

2.c) Diese Formen der alternativen Streitbeilegung sollten die besondere Beschaffenheit des Rechts auf Zugang zu öffentlichen Informationen berücksichtigen.

2.d) Diese Formen der alternativen Mechanismen zur Streitbeilegung und ihre Verfahren sollten einer Bewertung unterzogen werden.

2.e) Die Teilnehmer dieser Konferenz verpflichten sich zum Austausch bewährter Praktiken der alternativen Streitbeilegung für das Recht auf Zugang zu öffentlichen Informationen.

3. Schlussfolgerungen und Gruppenvereinbarungen zur „Ermittlung von Messverfahren in der Umsetzung öffentlicher Politiken der Transparenz und das Recht auf Zugang zu öffentlichen Informationen".

3.a) Systematische Erstellung eines Katalogs der bestehenden internationalen Maßnahmen (OECD, OAS, usw.) und Bewertung der Relevanz dieser Indikatoren.

3.b) Bewertung der Notwendigkeit der Entwicklung eines einheitlichen Bewertungsmodells.

3.c) Bewertung der Möglichkeit der Schaffung neuer Indikatoren für die gemeinsame Messung.

3.d) Erstellung von Kommunikationsstrategien über die Ergebnisse dieser Messungen, um sie richtig zu verstehen.

3.e) Mitteilung bewährter Praktiken der verschiedenen nationalen Systeme für die Messung.

4. Schlussfolgerungen und Gruppenvereinbarungen über „Vergleichende Rechtsprechung".

4.a) Stärkung der regionalen Plattformen der vergleichenden Rechtsprechung zur Schaffung eines zukünftigen Netzwerks, das mit allen Mitgliedern der Organisation auf nationaler, regionaler- bzw. Bundesebene geteilt wird.

4.b) Erstellung eines aktualisierten Verzeichnisses mit den allgemeinen Angaben der Organe, die den Informationszugang sicherstellen, ihre Kontaktdaten und die genauen Daten, um eine reibungslose und effektive Kommunikation zwischen den Mitgliedern der Organisation zu ermöglichen. Die Informationen werden von den Mitgliedern auf freiwilliger Basis übermittelt. Die erste Liste wird auf der 9. Internationalen Konferenz der Beauftragten für die Informationsfreiheit erstellt.

4.c) Sobald Punkt 4b abgeschlossen ist, werden die Stellen, die den Informationszugang gewährleisten, Links zu den jeweiligen Websites mitteilen, auf denen die besondere Rechtsprechung eines jeden Mitglieds der Organisation veröffentlicht wird.

4.d) Freiwillige Aktualisierung – per Adressenliste der Mitglieder der Organisation, der Entscheidungen der Organe, die den Informationszugang sicherstellen oder von Gerichten, die für auf das Recht auf Informationszugang wichtig sind oder einen Einfluss darauf ausüben, und auch Aktualisierungen der Verordnungen zu diesem Thema.

4.e) Im Fall von nationalen Organisationen, die ihre Aufgaben mit regionalen oder Bundesbehörden teilen, beschloss der Ausschuss, den nationalen Organisationen die Anweisung zu geben, die lokalen Organe einzubeziehen und ihnen die in dieser Sitzung getroffenen Vereinbarungen mitzuteilen.

4.f) Schließlich wurde vereinbart, den Chilenischen Rat für die Transparenz als technisches Sekretariat zu benennen, das für die Verwaltung der Informationen, die von den Mitgliedern der Organisation geliefert werden, zuständig ist, während ansonsten keine andere besondere Stelle benannt wird.

5. Abschlusserklärung

In Anbetracht der Wichtigkeit des Rechts auf Informationszugang brachten die Beauftragten und Aufsichtsbehörden als Vertreter von 25 Ländern die folgenden wichtigen Herausforderungen an dieses Recht auf Ihrer Plenarsitzung zum Ausdruck:

- Die anhaltenden Ungleichheiten, die die Wahrnehmung des Rechts auf Informationszugang für alle Bürger einschränken
- Der Rückschritt des Rechts auf Informationszugang aufgrund der Billigung von Gesetzgebungen und öffentlichen Politiken, die im Widerspruch zu diesem Recht stehen
- Das Recht auf Informationszugang wird in Ländern mit einer größeren digitalen Kluft erschwert
- Die fehlende angemessene Finanzierung, Unterstützung und Unterhaltung der Aufsichtsorgane.

Aus diesem Grund fordern wir die Regierungen, zivilgesellschaftliche Organisationen, die internationale Gemeinschaft und Bürger dazu auf, weiterhin wachsam zu sein und zusammenzuarbeiten zum Schutz, Förderung und Stärkung eines effektiven Rechts auf Informationszugang. Wir, die Beauftragten und Aufsichtsbehörden engagieren uns für die Zusammenarbeit mit allen Akteuren, die an der Erfüllung dieses Zieles beteiligt sind.

6. Nächstes Treffen

Die l0. Internationale Konferenz der Beauftragten für Informationsfreiheit findet 2017 in Bali, Indonesien, statt, und sie wird vom indonesischen Beauftragten für die Informationsfreiheit ausgerichtet.