International Working Group
on Data Protection
in Telecommunications

675.51.16

Arbeitspapier zu intelligenter Video-Analysetechnik

58. Sitzung, 13.-14. Oktober 2015, Berlin (Deutschland)

– 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.

[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.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

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 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.

---

[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

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:

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 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 Verbrau-

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

[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)

chern 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.

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,

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

[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.

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 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]

---

[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

[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 vom12. 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.

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.

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 segmentspezifische 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]

[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

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 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.

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.

[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 ethnischbasierte Werbung angezeigt. Andere Konsequenzen wären vorstellbar, wenn etwa eine Person versehentlich als betrunken in der Öffentlichkeit, angeblich bei einem Einbruch oder Diebstahl identifiziert wird.

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 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.

[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

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 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

[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.

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 Verhalten 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]

---

[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

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.

Über die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („ Berlin Group“)

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (englisch: International Working Group on Data Protection in Telecommunications - IWGDPT, auch bekannt als “Berlin Group”) besteht aus Vertretern von Datenschutz-Aufsichtsbehörden und Organisationen aus aller Welt, die sich mit dem Schutz der Privatsphäre beschäftigen. Die Arbeitsgruppe wurde 1983 im Rahmen der Internationalen Datenschutzkonferenz auf Initiative des Berliner Beauftragten für Datenschutz gegründet, der seither ihren Vorsitz führt. Seit ihrer Gründung hat die Arbeitsgruppe eine Vielzahl von Empfehlungen („Gemeinsame Standpunkte“ und „Arbeitspapiere“) mit dem Ziel verabschiedet, den Schutz der Privatsphäre in der Telekommunikation zu verbessern. Seit Anfang der neunziger Jahre beschäftigt sich die Gruppe insbesondere mit dem Schutz der Privatsphäre im Internet.

Weitere Informationen über die Arbeitsgruppe sowie eine Broschüre mit allen von der Gruppe verabschiedeten Dokumenten sind auf der Webseite der Arbeitsgruppe abrufbar: http://www.berlin-privacy-group.org.