International Working Group
on Data Protection
in Telecommunications

675.47.26

Arbeitspapier zum Datenschutz bei Überwachung aus der Luft

54. Sitzung, 2.-3. September 2013, Berlin

- Übersetzung -

Hintergrund

Überwachung ist das Beobachten von Verhalten, Aktivitäten oder anderen sich verändernden Informationen, um etwas oder jemanden zu beeinflussen, zu verwalten, zu steuern oder zu schützen. Sie beinhaltet häufig die Beobachtung von Individuen oder Gruppen durch Regierungsstellen, obwohl es einige Ausnahmen gibt, wie z. B. die Überwachung der Verbreitung von Krankheiten, bei der die Verbreitung einer Erkrankung in einer Gemeinschaft beobachtet wird, ohne Individuen direkt zu beobachten oder zu kontrollieren.

Überwachung aus der Luft ist das Erheben von Informationen, normalerweise von Bildern oder Videoaufnahmen, von einem Luftfahrzeug aus. Seit die Internationale Konferenz der Datenschutzbeauftragten zum ersten Mal über Luftüberwachung durch Satelliten diskutierte[1], hat es weitreichende technologische Entwicklungen gegeben. Während Satelliten-basierte Dienste wie Google Earth gegenwärtig keine besonderen Risiken für die Privatsphäre des Einzelnen bilden, solange nur Einzelbilder mit begrenzter Auflösung gesammelt werden, verhält es sich mit tief fliegenden Überwachungsplattformen wie Drohen anders. Während die Nutzung von Drohnen für militärische (Gefechts-) Zwecke Gegenstand einer – aufgrund von Geheimhaltung – begrenzten öffentlichen Debatte ist, wurde eine vergleichbare Diskussion über die zivile Nutzung dieser Technologie zum Zwecke der Sammlung von Informationen und deren Konsequenzen bisher vernachlässigt. Die Geschichte der

[1] S. Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 29. Oktober 1992, Sydney, in: Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien 1983 – 2006, S. 42; http://www.datenschutz-berlin.de/attachments/334/IWGDPT_WP_brochure.pdf

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

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

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Satellitentechnologie seit 1989 zeigt jedoch, dass Aufklärungstechnologien, die früher auf eine militärische Nutzung beschränkt waren, auch für die zivile Nutzung verfügbar werden können.

Überwachungsplattformen können für eine Vielzahl von Zwecken genutzt werden, einschließlich:

a) Fernerkundung: Die Nutzung verschiedener Sensoren (visueller, Infrarot- oder Nahinfrarot-Spektrum, Gamma-Strahlen, biologischer und chemischer), um die Gegenwart von Chemikalien, Mikroorganismen und anderen biologischen Faktoren, radioaktive Materialien, Waffen usw. zu erkennen;

b) Kommerzielle Luftüberwachung: Viehbeobachtungen, Flächenbrandkontrolle, Pipeline-Sicherheit, Gebäudesicherheit, Präzisionsackerbau, Verkehrswacht und Anti-Piraterie[2];

c) Erkundungen von Bodenschätzen: Durchführung geophysikalischer Untersuchungen zur Vorhersage der Lage von Öl-, Gas- und Mineralvorkommen, Überwachung von Öl- und Gaspipelines und vergleichbarer Infrastruktur, Vergleich der tatsächlichen Größe von Ackergrundstücken, für die Subventionen gezahlt wurden, mit Angaben in den dazugehörigen Antragsformularen[3];

d) Wissenschaftliche Forschung: Wetterbeobachtung einschließlich der Nahbeobachtung gefährlicher Wettersysteme wie Wirbelstürmen oder Nutzung in schwierigen Klimabedingungen wie in der Antarktis;

e) Suche und Rettung: Suche nach vermissten Personen, Schadensabschätzung nach Natur- (oder durch Menschen verursachte) Katastrophen; und

f) Naturschutz: Beobachtung der Bewegung von Tieren, Erkennung und Überwachung der Verbreitung von Unfällen mit Gefahrenstoffen, Waldbranderkennung, Fischereischutz, etc.

---

[2] Die US-Unternehmen Skybox Imaging und Planet Labs planen die Nutzung von Flotten leichter Mikrosatelliten zur Erdüberwachung in Echtzeit. Sie ermöglichen privaten Investoren den Kauf und das Herunterladen von Bildmaterial, vgl. http://www.nytimes.com/2013/08/11/business/microsatellites-what-big-eyes-they-have.html?_r=0 (abgerufen am 20. Oktober 2013).

[3] Vgl. das europäische „Integrated Administration and Control System (IACS) http://ec.europa.eu/agriculture/direct-support/iacs/index_en.htm , das auf die Verhinderung von Betrug bei Landwirtschaftssubventionen gerichtet ist. IACS beinhaltet Satellitenüberwachung.

Überwachungsplattformen

Eine Vielzahl von Plattformen[4] oder Fahrzeugen wird zur Luftüberwachung verwendet oder kann dazu verwendet werden, einschließlich:

a) Starrflügler: ein Starrflügelflugzeug ist ein Flugzeug, das mithilfe von Flügeln fliegt, die Auftrieb erzeugen, der durch die Vorwärtsbewegung des Fahrzeugs und die Form der Flügel ermöglicht wird. Die Flügel eines Starrflügelflugzeugs sind nicht notwendigerweise steif; Drachen, Hängegleiter und Flugzeuge, die „wing-warping“ oder variable Geometrie benutzen, werden alle als Starrflügelflugzeuge angesehen;

b) Drehflügler: Der Begriff Drehflügel beschreibt eine Tragfläche, die um eine annähernd vertikale Achse rotiert, wie die eines Helikopters oder Tragschraubers beim Fliegen;

c) Unbemannte Flugsysteme (Unmanned Aircraft Systems – UAS). Ein unbemanntes Fluggerät (Unmanned Aircraft – UA), landläufig als Drohne bezeichnet, ist ein Fluggerät ohne einen menschlichen Piloten an Bord. Sein Flug wird entweder autonom von Computern innerhalb des Fahrzeugs kontrolliert oder über Fernbedienung durch einen Piloten am Boden oder in einem anderen Fahrzeug. UAS können Starr- oder Drehflügler sein und einzeln oder in Schwärmen (die untereinander und mit der zentralen Kontrollinstanz am Boden kommunizieren) betrieben werden, oder

d) Sonstige: Ein Aerostat ist ein Fahrzeug, das primär durch die Nutzung von dem Auftrieb von Gasen in der Luft bleibt, die leichter sind als Luft, und die einem Fahrzeug mit fast derselben Dichte wie Luft Auftrieb gewähren. Aerostaten beinhalten Frei- und/oder Fessel-Ballons, Zeppeline oder andere steuerbare Luftschiffe, die angetrieben oder antriebslos sein können.

Jede dieser Plattformen hat verschiedene Betriebseigenschaften wie Betriebshöhe, Geschwindigkeit, Reichweite, Höchstflugdauer (d. h. wie lange kann die Plattform in der Luft bleiben), die Fähigkeit zu schweben, und Nutzlast-Kapazität.

[4] Eine andere Kategorisierung findet sich auf Seite 2 bei Stanley, J. und Crump, C., „Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft“, ACLU Report datiert Dezember 2011 (online verfügbar unter http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

Überwachungstechnologien

Verschiedene Überwachungstechnologien können von den o. g. Plattformen getragen werden; die genaue Traglast hängt von einer Reihe von Faktoren wie Aufgabe, Wetterbedingungen, Nutzlast-Kapazität, die Reichweite des Sensors, sein Sichtfeld und seine Auflösung, usw. Sensoren umfassen (sind aber nicht notwendigerweise beschränkt auf):

a) Sichtbares Spektrum: Diese Sensoren haben typischerweise die Form von Kameras, einschließlich hochauflösenden und full-motion-Videosystemen[5]; sie erlauben fortlaufende Überwachung in Echtzeit und die Speicherung des gesamten Videomaterials;

b) Infrarot (IR): Diese Art von Sensoren erkennt Energie, die vom Ziel ausgesendet oder reflektiert wird. Die meisten IR-Sensoren sind passiv, obwohl sie in Verbindung mit einer IR-Beleuchtungsquelle benutzt werden können. Sie können durch Rauch, Nebel, Dunst und andere atmosphärische Verschleierungen besser „sehen“ als Kameras für sichtbares Licht;

c) Nachtsicht: Die Fähigkeit bei schlechten Lichtbedingungen zu sehen, gestützt auf eine Kombination von ausreichendem Spektralbereich (d. h. wieviel vom elektromagnetischen (EM) Spektrum das Gerät erkennen kann) und ausreichendem Helligkeitsbereich (d. h. wieviel Licht ist notwendig, um ein brauchbares Bild zu erzeugen). Nachtsichttechnologien können grob in drei Hauptkategorien eingeteilt werden:
    1) Bildverstärkung: Diese Technologien arbeiten nach dem Prinzip der Vergrößerung der Menge empfangener Photonen aus verschiedenen natürlichen Quellen sowie Sternenlicht oder Mondlicht. Beispiele für solche Technologien umfassen Nachtgläser und Restlicht-Kameras;
    2) Aktive Ausleuchtung: Diese Technologien funktionieren nach dem Prinzip der Kopplung von Bildverstärkungstechnologien mit einer aktiven Lichtquelle im Nahinfrarot (NIR) oder Kurzwellen-Infrarot (shortwave infrared – SWIR)-Band. Ein Beispiel solcher Technologien sind Restlicht-Kameras; und

[5] Die U.S. Army erwarb kürzlich eine 1.8 Gigapixel-Kamera zur Nutzung in ihren Drohnen. Diese Kamera (Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System – ARGUS IS) bietet 900 mal so viele Pixel wie eine 2-Megapixel-Kamera eines Mobiltelefons; sie wurde zu niedrigen Kosten unter Nutzung von 368 Kamera-Mikrochips aus Mobiltelefonen gebaut. Sie kann Objekte am Boden in 65 Meilen Entfernung aus einer Höhe von 20.000 Fuß verfolgen. Vgl. *US Army unveils 1.8 gigapixel camera helicopter drone*, BBC NEWS (29. Dezember 2011), http://www.bbc.com/news/technology-16358851 . Ein aufschlussreiches Video ist verfügbar unter: http://www.youtube.com/watch?v=QGxNyaXfJsA , abgerufen am 2. April 2013.

3) Wärmebild-Aufklärung: Diese Technologien funktionieren durch Erkennung der Temperatur-Differenz zwischen den Hintergrund- und den Vordergrund-Objekten.

d) Radar: Radar nutzt Funkwellen des Hochfrequenz-Spektrums, um die Entfernung, Höhe, Richtung oder Geschwindigkeit eines Objekts zu bestimmen. Radar kann auch dazu genutzt werden, Objekte am Boden wie z. B. Fahrzeuge zu identifizieren und zu verfolgen (beispielsweise unter Nutzung von luftgestütztem Schrägsichtradar (Side Looking Airborne Radar – SLAR)); und

e) Spezialsensoren: Eine Reihe von Spezialsensoren (z. B. zur Erkennung von Spuren chemischer, biologischer, nuklearer, radiologischer und explosiver Materialien; Nummernschild-Scanner; akustische Sensoren, etc.) können ebenfalls von luftgestützten Überwachungsplattformen getragen werden.

Kombinationen dieser Sensortypen können Organisationen die Möglichkeit zur Durchführung von Luftüberwachung unter beinahe jeglichen Bedingungen bieten.

Auswirkungen auf die Privatsphäre

Es gibt eine Reihe von Aspekten der Überwachung, die Datenschutzbedenken hervorruft, einschließlich der Tatsache, dass Überwachung unsichtbar, intrusiv, willkürlich und kontinuierlich ist.[6] Obwohl diese Aspekte im Zusammenhang mit elektronischer Kommunikation beschrieben wurden, sind sie auch auf die Luftüberwachung anwendbar:

a) Unsichtbar: Abhängig von der Größe, der Einsatzhöhe, der Fähigkeiten der Sensoren usw., kann es unmöglich sein, Luftüberwachung (entweder die Plattform selbst oder die genutzten Sensoren) zu entdecken. Die von der Überwachung Betroffenen müssten auf deren Aufdeckung durch die Organisation selbst bauen, die die Überwachung durchführt oder auf die Aufdeckung durch einen Dritten. Die von unsichtbarer Überwachung Betroffenen haben weniger Möglichkeiten, die Organisation zur Verantwortung zu ziehen, die die Überwachung durchführt;

[6] Freiwald, Susan: „A First Principles Approach to Communications Privacy“, veröffentlicht in Stanford Technology Law Review (2007 STAN. TECH. L. REV. 3), datiert 2007. Abrufbar unter http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf .

b) Intrusiv: Der Bandbreite möglicher Operationsbedingungen für Plattformen zur Luftüberwachung und die Fähigkeiten ihrer Sensoren verstärken die Intrusivität von Luftüberwachung (sie können fast alles und jedes „sehen“);

c) Willkürlich: Luftüberwachung deckt im allgemeinen ein Gebiet ab, das Individuen und Aktivitäten einschließt, die eine Überwachung nicht erfordern, was in der überschießenden Sammlung von Informationen resultiert; und

d) Kontinuierlich: Aufkommende Plattformen zur Luftüberwachung kombinieren zunehmende Betriebsdauer und die Fähigkeit, auf ein Gebiet zu „starren“, um eine wirksame, fortdauernde Überwachung eines beliebigen Gebiets zu erzeugen[7].

Diese Charakteristiken geben Anlass zu einigen spezifische Befürchtungen hinsichtlich des Schutzes der Privatsphäre[8]:

a) Schleichende Ausweitung des Einsatzes („Mission Creep“): Obwohl die meisten Menschen die Nutzung von Luftüberwachung (z. B. für die Entdeckung und Überwachung von Naturkatastrophen) oder zur Nutzung unter spezifischen, begrenzten Umständen bei der Strafverfolgung wahrscheinlich unterstützen würden, scheint es unvermeidlich, dass zukünftig weitere Privatsphäre-invasive Nutzungen für solche Technologien gefunden werden;

b) Verfolgung: Die Fähigkeit, die Überwachung einer erweiterten Fläche über erweiterte Zeiträume aufrechtzuerhalten, birgt die Möglichkeit, dass Individuen und Fahrzeuge fortlaufend verfolgt werden können;

c) Proliferation, weil die Kosten für UAS-Technologien rapide fallen. UAS können von Privatpersonen zur Nutzung als „persönliche“ oder „Do it yourself“-UAS gekauft oder gebaut werden.

---

[7] Die U.S. Air Force hat die Gorgonenblick- („Gorgon Stare“) Technologie entwickelt, eine kugelförmige Anordnung von neun Kameras, die in eine Drohne eingebaut und fähig ist, Bewegtbilder ganzer Städte aufzunehmen („With Air Force’s Gorgon Drone ‘we can see everything‘“, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html)

[8] Eine Erörterung der verschiedenen potentiellen Datenschutzbedenken findet sich auf Seite 11 bei Stanley, J. und Crump, C., „Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft“, ACLU Report datiert Dezember 2011 (abrufbar unter http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

Intrusiver für die Privatsphäre als Videoüberwachung

Die Auswirkungen von Videoüberwachung auf die Privatsphäre sind seit Jahren Gegenstand von Debatten gewesen, und viele Datenschutzbehörden haben Richtlinien zu den notwendigen Sicherungsmaßnahmen bei deren Nutzung herausgegeben. Wie oben erläutert verfügen Luftüberwachungssysteme aus verschiedenen Gründen über ein größeres Potenzial zur Verletzung der Privatsphäre als Videoüberwachungssysteme, einschließlich:

- Luftüberwachungssysteme können viel mehr verschiedene Sensoren nutzen als Videoüberwachungssysteme.
- Die Installation von Videoüberwachung erfordert normalerweise den Zugang zu und die Kontrolle über die entsprechenden Grundstücke; diese ist für Luftüberwachungssysteme nicht erforderlich, insbesondere für Orte im Freien.
- Abhängig von der Flughöhe und anderen Faktoren (z. B. Miniaturisierung) können Luftüberwachungssysteme von den überwachten Personen schwieriger – wenn nicht unmöglich – zu entdecken sein als die meisten Videoüberwachungssysteme.
- Luftüberwachungssysteme können ohne jegliche Verzögerung angewandt werden; sie benötigen keine Installation oder Konfigurationen vor Ort.

Dies deutet in klarer Weise darauf hin, dass die Sicherungsmaßnahmen für Videoüberwachungseinrichtungen, obwohl sie einen Minimalstandard anzeigen, im Zusammenhang mit Luftüberwachungssystemen nicht als ausreichend angesehen werden können und durch spezifische, den verschiedenen Luftüberwachungssystemen und Nutzungsszenarien angemessene Maßnahmen angepasst und ergänzt werden müssen.

Daher sollten bestimmte neue, essentielle Sicherungsmaßnahmen auf nationaler Ebene von den Gesetzgebern unter Berücksichtigung möglicher Unterschiede zwischen dem öffentlichen und dem privaten Sektor verabschiedet werden. Darüber hinaus werden internationale Vereinbarungen notwendig sein, um die Herausbildung eines „globalen Panoptikums“ zu verhindern, da Luftüberwachung nicht an Landesgrenzen Halt macht.

Empfehlungen

Die zunehmende Nutzung von Luftüberwachung wird wahrscheinlich Bedenken darüber verstärken, wie die individuelle und kollektive Privatsphäre im täglichen Leben geschützt werden kann, egal ob sie von Strafverfolgungsbehörden oder anderen Einrichtungen der öffentlichen Verwaltung, oder von Privatunternehmen, oder von Bürgern zu Freizeitzwecken betrieben wird. Wenn Luftüberwachung

ein zunehmend normaler Bestandteil der heutigen Gesellschaft wird, und die Gesellschaft deren Gegenwart als normal akzeptiert, ist es vorstellbar, dass die Erwartungen der Gesellschaft an den Schutz der Privatsphäre in der Öffentlichkeit ernstlich untergraben werden könnten. Es ist wichtig, eine angemessene Balance zwischen den Bedürfnissen der Strafverfolgung, der öffentlichen Sicherheit etc. auf der einen Seite und den legitimen Interessen der Individuen am Schutz der Privatsphäre auf der anderen Seite sicherzustellen. In diesem Sinne gibt die Arbeitsgruppe die folgenden Empfehlungen:

a) Die Nutzung von Luftüberwachung sollte auf spezifische Zwecke[9] beschränkt werden (z. B. die Suche nach vermissten Personen, die Überwachung von Grenzen, legitime private Zwecke, wie den Zugang zu Informationen durch Journalisten);

b) Die Nutzung personenbezogener Daten, wie beispielsweise Bildern, die durch Behörden aus der Luft gesammelt werden, sollten unter Richtervorbehalt stehen;

c) Die Öffentlichkeit sollte über die Nutzung von Luftüberwachung im größtmöglichen Ausmaß unterrichtet werden; dies erfordert z. B., dass jedes UAS mit der Fähigkeit, Informationen über eine Datenverbindung zu übertragen, seine GPS-Positionsdaten, Fähigkeiten und Angaben zum Eigentümer (z. B. die Behörde, das Unternehmen oder die Privatperson, die für die jeweilige Plattform oder das jeweilige Fahrzeug verantwortlich ist), in Echtzeit an eine geeignete Behörde übermittelt wird und dass diese Behörde die Aufenthaltsinformationen als „Open Data“ in Echtzeit verfügbar macht;

---

[9] Die American Civil Liberties Union (ACLU) beschreibt die folgenden Auflagen für die Nutzung von Drohnen:

a) **Nutzungsbeschränkungen:** Drohnen sollten von Strafverfolgungsbehörden nur unter Richtervorbehalt oder in Notfällen angewendet werden, oder wenn es spezifische und benennbare Gründe zu der Annahme gibt, dass die Drohne Beweismittel in Bezug auf eine bestimmte Straftat sammeln wird;
b) **Datenspeicherung:** Bilder sollten nur aufbewahrt werden, wenn der berechtigte Verdacht besteht, dass sie Beweismittel für ein Verbrechen enthalten oder für eine laufende Untersuchung oder ein laufendes Gerichtsverfahren relevant sind;
c) **Richtlinien:** Nutzungsrichtlinien für innerstaatliche Drohnen sollten durch die Repräsentanten der Öffentlichkeit festgelegt werden und nicht durch Polizeibehörden; die Richtlinien sollten klar, schriftlich und der Öffentlichkeit zugänglich sein; und
d) **Missbrauchsverhinderung & Verantwortlichkeit:** Die Nutzung innerstaatlicher Drohnen sollte Gegenstand offener Überprüfungen und angemessener Aufsicht zur Verhinderung von Missbrauch sein.

Siehe http://www.aclu.org/blog/tag/domestic-drones ; siehe auch die bei EPIC aufgeführten Quellen unter http://www.epic.org/privacy/drones , in der verschiedene Gesetzentwürfe erwähnt werden, die diese Themen betreffen und gegenwärtig im U.S.-Kongress behandelt werden.

d) Die Überwachung sollte auf eine Fläche beschränkt werden, die so klein wie möglich ist (durch Begrenzung der Sichtfelder des Sensors), um die Wahrscheinlichkeit für eine „überschießende Erhebung“ zu minimieren;

e) Es sollten stringente Kontrollen darüber eingeführt werden, wie Luftüberwachungsinformationen genutzt werden können und wer auf diese Informationen Zugriff hat. Für Notfälle (z. B. die Suche nach vermissten Personen) können Ausnahmen gemacht werden; und

f) Es sollte immer eine menschliche Kontrollinstanz eingebunden sein, so dass, falls es Probleme oder ungewöhnliche Umstände gibt (z. B., dass das UAS in ein Wohngebiet abdriftet), diese so schnell wie möglich angegangen werden können.

Die Arbeitsgruppe wird die Entwicklungen in diesem Bereich im Lichte der sich rasant entwickelnden Technologie weiterhin genau beobachten.