5 Weitere Überwachungsaspekte

Als Ergänzung zu den Darstellungen in den vorherigen Kapiteln, die auf dem Buch von Bruce Schneier [Sch15] basieren, werden in diesem Kapitel weitere Überwachungsbeispiele beschrieben.

5.1 Wirksamstes Überwachungsgerät: Smartphone

Das problematischste und wirksamste Überwachungsgerät ist das Smartphone mit qualitativ hochwertigem Mikrofon und Kamera, sowie Sensoren für Lage, Beschleunigung und Temperatur. Viele Apps nutzen solche Sensoren, auch wenn man deren Funktion nicht damit in Zusammenhang bringen würde. Liegt das Smartphone nachts auf dem Bett, kann mit den Beschleunigungssensoren ein Bewegungsprofil erstellt und daraus auf eine Alkoholabhängigkeit geschlossen werden.[1] Facebook hat ein Patent angemeldet, das es dem Unternehmen ermöglicht, das Mikrofon des Smartphones ihrer Nutzer einzuschalten und die Umgebungsgeräusche aufzunehmen. Wer in den USA seine Facebook-App auf dem Handy offen hat, wird belauscht, das Mikrofon ist eingeschaltet, das Audiosignal wird an Facebook übertragen und analysiert.[2]

Die meisten Menschen haben ihr Smartphone immer dabei, können somit permanent überwacht werden. Die Mobilfunkgesellschaft weiß also immer, wo man sich gerade aufhält, welche Gaststätten man besucht, mit wem man telefoniert und welche Kontakte man hat. Damit ist noch nicht sicher, dass solche Daten auch verwendet werden, aber sie sind verfügbar. Analysten konnten auf Basis solcher Daten bis auf 20 Meter vorhersagen, wo eine Person sich in 24 Stunden vermutlich befinden wird.[3]

Standortdaten werden auch von Polizei und Regierungen genutzt. Die Polizei kann eine stille SMS an eine Mobiltelefonnummer senden, um dieses zu orten. Der Nutzer merkt davon nichts. Auch Regierungen nutzen solche Standortdaten von Handys. Die ukrainische Regierung sendete im Jahr 2014 eine SMS an Personen, die sich zu einer bestimmten Zeit an einem bestimmten Ort befanden. Der SMS-Text lautete: „Sehr geehrter Kunde, Sie wurden als Teilnehmer an einem Massenaufruhr erfasst." Aber auch Unternehmen haben großes Interesse

---

1 [Kes17], Seite 24

2 Süddeutsche Zeitung vom 29.6.2018, Seite 4 und 17, sowie [Gal17], Seite 114 -115

3 [Sch15], Seite 7

an solchen Standortdaten, zum Beispiel um Werbung zu senden, wenn man sich in der Nähe eines bestimmten Geschäfts befindet. Handy- und Ortungsdaten sind so wertvoll, dass verschiedene Firmen Kauf und Verkauf von solchen Daten als Geschäftsmodell betreiben.[4]

Auch in Deutschland werden stille SMS zur Lokalisierung von Personen verwendet. Bis 2023 gab es vom Innenministerium noch öffentliche Mitteilungen über die Häufigkeit der Versendung solcher SMS durch die Bundespolizei und das BKA. In 2022 wurden fast 100.000 solcher Nachrichten versendet, um Personen zu orten. Solche statistischen Hinweise wird es jetzt nicht mehr geben, denn das Bundesinnenministerium hat verschiedene Formen der heimlichen Überwachung nun als geheim eingestuft.[5]

5.2 Weitere Überwachungssysteme

Ein wichtiges und viel genutztes Überwachungsgerät sind Kameras. In China gab es im Jahr 2018 etwa 350 Millionen Überwachungskameras, in den USA waren es 70 Millionen. China und weitere Länder exportieren Überwachungstechnologie in Niedriglohnländer und helfen damit solchen Staaten bei der Unterdrückung von Randgruppen.[6]

Viele Menschen unterstützen die großen Internetkonzerne, Versicherungen und Staaten freiwillig, indem sie immer mehr Informationen von sich preisgeben. Es macht Spaß, sich überwachen zu lassen, zum Beispiel durch Alexa, den Sprachassistenten von Amazon. Autofahrer lassen eine Überwachung durch KFZ-Versicherer zu, um ein paar Euro an Gebühren zu sparen. In China wirbt eine Fahrradverleihfirma damit, dass das Rad Daten wie das Bewegungsprofil und Körperhaltungen in Echtzeit ins Netz überträgt. Mit dem Bezahlsystem Venmo, einer App von PayPal, können in der USA Überweisungen durchgeführt werden. Bei der Standardeinstellung werden alle Daten, also Nutzer, Beträge, Überweisungsgründe für alle sichtbar im Internet veröffentlicht. Amazon hat Patente für ein Armband, das mit Ultraschalltechnologie alle Bewegungen der Hände aufzeichnen kann.[7]

---

4 [Sch15], Seite 8

5 https://www.heise.de/news/Stille-SMS-Co-Regierung-erklaert-heimliche-Ueberwachung-komplett-fuer-geheim-9674437.html?wt_mc=nl.red.ho.ho-nl-newsticker.2024-04-04.link

6 [RN23], Seite 1091

7 Süddeutsche Zeitung vom 19.5.2018, Seite 2

Alle Gespräche der Umgebung aufzeichnen ist auch mit einer Mikrofon-Kette des Unternehmens „Rewind AI“ möglich. Diese kann als Halskette getragen werden und dabei alle Gespräche in der Umgebung aufzeichnen und zum Beispiel an ein iPhone übertragen, wo die Gespräche später durchsuchbar sind.[8]

Private E-Mails des E-Mail-Dienstes von Google werden von Google automatisch analysiert, teilweise von Google-Mitarbeitern gelesen und an andere Unternehmen weitergegeben.[9]

Ein amerikanisches Unternehmen, das Spyware herstellt, hat weltweit verschiedene Systeme wie Windows-, Mac-, Android-Systeme ausspioniert. Bekannt wurde dies durch eine Datenpanne, wobei Hacker in Serversysteme des Unternehmens eindrangen, und auf Daten zugriffen, die zeigten, dass das Unternehmen Malware-Aktivitäten betreibt.[10]

Auch die Bestrebungen zu Smart-City und Smart-Home liefern umfangreiche Überwachungsdaten. In einem Artikel der Süddeutschen Zeitung werden die Ziele von Smart-Home verglichen mit einem Strafvollzug in Form eines elektronisch überwachten Hausarrests.[11]

Bei vielen Internetseiten führt ein Besuch dazu, dass weitere Internetseiten aufgerufen werden, ohne dass der Nutzer dies merkt. Es gibt Werkzeuge, mit denen überprüft werden kann, auf welche anderen Seiten automatisch zugegriffen wird.

5.3 Umfassende Überwachung am PC

Verschiedene Geräte und Systeme ermöglichen eine umfassende Überwachung. Dazu geeignet ist besonders das Smartphone, das viele Menschen immer dabeihaben, wobei Überwachungsapps wie die Ortsbestimmung oft standardmäßig aktiv sind. Auch Abhörfunktionen können eingeschaltet werden, ohne dass der Nutzer dies merkt. Zu Hause können Systeme wie Alexa ständig zuhören und somit vollständig überwachen, was gesagt wird.

---

8 https://www.heise.de/news/Rewind-AI-Pendant-Mikrofon-Kette-soll-alle-Gespraeche-aufzeichnen-9333104.html

9 Süddeutsche Zeitung vom 24.9.2018, Seite 19

10 https://www.heise.de/news/Datenpanne-entlarvt-US-Spyware-Hersteller-9815496.html

11 Süddeutsche Zeitung vom 30.5.2017, Seite 10

Auch am PC werden die Techniken für eine umfassende Überwachung immer besser. So hat Microsoft ein KI-basiertes System „Recall“ realisiert, das bei beliebiger Arbeit am PC alle 5 Sekunden einen Screenshot erstellt und abspeichert. Diese Screenshots können später analysiert und durchsucht werden. Aus den Bildern werden hierbei mit einem OCR-System auch Texte erzeugt. Die gesamte Vergangenheit der Arbeit am PC wird gespeichert und man kann später in natürlicher Sprache nach bestimmten Aspekten fragen, die man mal bearbeitet hat und das System liefert die geeigneten Antworten und Bilder zurück. Zum Beispiel kann man fragen, woran man vor einer Woche gearbeitet oder was man gesucht hatte oder man kann erwähnen, dass man vor einiger Zeit mal nach einem Pizzarezept gesucht hat und möchte, dass wieder angezeigt wird, was man damals gesehen hat. Entsprechende Anfragen können in natürlicher Sprache über die Tastatur oder ein Mikrofon gestellt werden. Das System liefert die passenden Antworten und zeigt die gewünschten Bilder.[12]

Die Speicherung und Verarbeitung dieser „Recall-Funktion“ sollen lokal am PC erfolgen, solange genügend Speicherplatz verfügbar ist. Trotzdem sind die Daten nicht sicher. Es gibt bereits Tools, die unberechtigten Personen Zugriff auf diese Daten erlauben.[13] Die Funktion sollte Mitte 2024 bei Windows 11 eingeführt werden, jedoch war die Kritik an diesen Plänen so stark, dass Microsoft die Einführung verschoben hat. Des Weiteren soll die „Recall-Funktion“ zunächst auch nur einem eingeschränkten Nutzerkreis zugänglich gemacht werden. Im April 2025 wurde die Recall-Funktion wieder für Nutzer freigegeben, allerdings zunächst nicht in der EU.[14]

An den Plänen gibt es erhebliche Datenschutzbedenken und ein Schutz der Privatsphäre kann kaum gewährleistet werden. Jeder der Zugriff auf einen Computer hat, kann feststellen, welche Aktivitäten andere Nutzer wann vorgenommen haben. Dies kann natürlich auch bei der Strafverfolgung verwendet werden. Werden hierbei Computer sichergestellt, kann nicht nur auf die Dateien zugegriffen werden, die von den Nutzern aktiv gespeichert wurden, sondern Ermittler könnten auch Zugriff auf alle Aktivitäten haben, die mit diesem Computer vorgenommen wurden. Problematisch kann dies auch in Unternehmen sein, wenn Computer nur zeitweise von einem Mitarbeiter verwendet und dann an einen anderen Mitarbeiter weitergegeben werden.

---

12 https://support.microsoft.com/de-de/windows/verfolgen-sie-ihre-schritte-mit-recall-aa03f8a0-a78b-4b3e-b0a1-2eb8ac48701c

13 https://www.security-insider.de/microsoft-recall-datenschutz-dilemma-um-ki-funktion-windows-a-42aea86c03ae979b0204554d1e55b8c4/

14 https://www.heise.de/news/Microsoft-Neustart-der-Recall-KI-Funktionen-in-der-EU-spaeter-10364247.html

Die Recall-Funktion erfordert eine gute Rechenleistung und viel Speicherplatz. Eine Folge könnte sein, dass in einem weiteren Schritt die Speicherung und Verarbeitung auch in der Cloud angeboten werden. Informationen zu allen Aktivitäten würden dann vollständig auf irgendwelchen Servern irgendwelcher Unternehmen gespeichert und verarbeitet werden. Dies könnte auch zur Bildung besonders detaillierter und aussagekräftiger Profile der Nutzer missbraucht werden. Und mit solchen Daten könnte anschließend gehandelt werden.[15]

5.4 Spionage - Kinderspielzeug

In den letzten Jahren ist vermehrt Spielzeug für Kinder, ausgestattet mit Mikrofonen und Kameras, auf den Markt gekommen. Ein Beispiel ist die Puppe Cayla, deren Mikrofon immer eingeschaltet ist. Die Daten werden kabellos an ein Smartphone übertragen und gelangen von dort auf die Server des US-Konzerns Nuance Communications. Die Cayla-App fragt sehr viele Daten ab, inklusive des Adressbuches des Handys.[16] Die Bundesnetzagentur hat den Vertrieb der Puppe Cayla inzwischen verboten. Bereits gekaufte Puppen müssen zerstört werden. Eine andere Puppe (Barbie) ist nicht verboten, weil sie nicht heimlich aufnimmt, sondern die Aufnahme erfolgt nur, solange ein Knopf am Gürtel gedrückt wird. Aber auch in diesem Fall werden umfangreiche Daten, die missbraucht werden können, ins Netz übertragen. Deshalb sehen Datenschützer auch diese Puppe kritisch.

Überprüfungen zeigten auch, dass von solchen Spielzeugen Sprachdaten automatisch an ein amerikanisches Unternehmen übermittelt wurden, das darauf spezialisiert ist, biometrische Daten zu sammeln, um Authentifizierungsaufgaben zu lösen.[17]

Falls Bild-, Audio- oder Videoaufnahmen von solchen Geräten an den Hersteller kabellos übertragen werden, muss der Nutzer die volle Kontrolle hierüber

---

[15] https://www.heise.de/meinung/Microsofts-Recall-laeutet-das-Ende-des-Personal-Computers-ein-9730298.html , https://www.heise.de/news/Der-Datenschutz-Albtraum-Alles-ueber-Windows-Recall-9764002.html , https://www.heise.de/news/Recall-von-Recall-Neue-Windows-Funktion-wird-Opt-In-9753623.html und https://www.heise.de/news/Microsofts-KI-Assistent-Recall-ist-ein-Sicherheitsrisiko-9749876.html

[16] Süddeutsche Zeitung vom 18.2.2017, Seite 12

[17] [Sch19], Seite 137

haben. Auf jeden Fall verboten sind Geräte, bei denen von extern auf Mikrofon oder Kamera zugegriffen werden kann, ohne dass der Nutzer dies merkt.[18]

In den USA und einigen weiteren englischsprachigen Ländern bietet der Spielzeugherstellung Curio Kindern zwischen drei und zwölf Jahren Plüschtiere mit Mikrofon und Lautsprecher an. Für die Kommunikation mit dem Stofftier, die über einen Cloud-Server läuft, wird ein Sprachmodell von OpenAI verwendet. Das Stofftier antwortet mit einer Kinderstimme. Die Kommunikation der Kinder mit diesem KI-System kann beliebig lange laufen. Die transkribierten Gespräche werden von dem Unternehmen ausgewertet und 90 Tage lang gespeichert.[19]

Von der Bundesnetzagentur verboten wurde auch eine Kinderuhr, über die Eltern über eine App die Umgebung des Kindes abhören konnten. Das Mikrofon dieser Kinderuhr konnten die Eltern zum Beispiel auch während des Unterrichts in der Schule anschalten und so den Unterricht mitverfolgen, also die Lehrer kontrollieren.[20]

Selbst das FBI warnt ausdrücklich vor der Verwendung von Spielzeug und Puppen mit Funktechnik und Internet-Anschluss („Cloud-Pets“). Das FBI warnt auch davor, dass diese Geräte gehackt werden können und dass damit den Kindern Schaden zugefügt werden kann. Als mögliche Nachteile werden Schikane und Identitätsdiebstahl genannt.[21]

5.5 Spanische Fußball-Liga setzt Fans als Spitzel ein

Anfang Juni 2018 wurde bekannt, dass die spanische Fußball-Liga ihre Fans als Spitzel einsetzt. Die Fans erhalten eine kostenlose App für das Smartphone. Diese App liefert ihnen Informationen zu den Spielen der Fußball-Liga. Während Ligaspiele laufen, schaltet die Liga das Mikrophon des Smartphones ein, um die Umgebungsgeräusche aufzuzeichnen und zu analysieren. Über das Mikrofon des Smartphones kann so festgestellt werden, ob in diesem Raum ge-

[18] Trierischer Volksfreund vom 1.12.2020, Seite 28

[19] https://www.heise.de/news/KI-Spielzeug-mit-Technik-von-Microsoft-OpenAI-und-Epic-Games-ueberwacht-Kinder-9576702.html?wt_mc=nl.red.ho.ho-nl-newsticker.2023-12-18.link

[20] Süddeutsche Zeitung vom 18.11.2017, Seite 12, und vom 21.11.2018, Seite 26

[21] Süddeutsche Zeitung vom 21.7.2017, Seite 9

rade ein Spiel der Fußball-Liga im Fernsehen geschaut wird. Da auch die Position des Smartphones genau bestimmt wird, weiß die Fußball-Liga auch, wo das Spiel im Fernsehen läuft und kann überprüfen, ob ein entsprechender Lizenzvertrag für die Übertragung des Spiels vorliegt.

Ziel der spanischen Fußball-Liga ist es, Gaststätten aufzuspüren, die Spiele der Fußball-Liga live übertragen, ohne hierfür eine gültige Lizenz zu besitzen. Das Einschalten des Mikros durch die Fußball-Liga erfolgt, ohne dass der Smartphone-Besitzer dies merkt. Die Fans werden so als Spitzel missbraucht, ohne es zu wissen. Diese Abhörmöglichkeit wird zwar in den AGB beschrieben, allerdings werden diese in der Regel nicht gelesen, sondern die Fans stimmen einfach zu.[22]

5.6 Identifikation bei Überweisungen

Wer im Internet aktiv ist, hinterlässt auf vielfältige Weise Spuren. Damit können zum Beispiel Personen während eines Überweisungsvorgangs identifiziert werden. Ein israelisches Unternehmen hat eine Software entwickelt, die den Zahlungsverkehr sicherer macht und im Auftrag von Banken angewendet wird.[23] Während der Ausführung einer Online-Überweisung analysiert diese Software die Mausbewegungen und die Tastatureingabe. Die Art der Mausbewegung zwischen den verschiedenen Feldern des Überweisungsformulars, die zeitlichen Zusammenhänge zwischen den einzelnen Tasten, die Reaktion auf verzögertes Anzeigen der einzelnen Zeichen, die Reaktion auf kurzes Verschwindenlassen des Mauszeigers und weitere Merkmale werden verwendet, um den Nutzer eindeutig zu identifizieren. So wird ein Profil des rechtmäßigen Kontoinhabers gebildet, das sich von den Profilen anderer Personen signifikant unterscheidet. Auf diese Weise können falsche Überweisungen nach Diebstahl einer PIN verhindert werden. Das Unternehmen gibt an, dass bei dieser Anwendung etwa 600 verschiedene Merkmale zu einer Person bestimmt werden können. Etwa 20 bis 30 dieser Merkmale reichen aus, um eine Person mit sehr hoher Trefferrate zu identifizieren.

---

[22] https://netzpolitik.org/2018/das-smartphone-als-wanze-spanische-fussball-liga-nutzt-mikros-und-gps-daten-von-fans/

[23] Die Zeit, Nr. 23, 2017, 1.6.2017, ab Seite 31

Nutzer müssen sich also nicht mehr identifizieren, sie werden aufgrund ihres Verhaltens identifiziert. Auch bei anderen Anwendungen wird an einer automatischen Identifikation von Personen auf der Basis ihres Verhaltens gearbeitet. Hierbei werden verhaltensbiometrische Profile gebildet. Solche Entwicklungen werden sehr kritisch gesehen. PINs und Passwörter kann eine Person ändern, um sich zu schützen. Sein biometrisches Profil kann man kaum noch verändern.

Die Analyse der Nutzer bei Banküberweisungen kann auch verwendet werden, um persönliche Eigenschaften zu bestimmen. Aus der Reihenfolge und aus zeitlichen Zusammenhängen zwischen einzelnen Aktionen können Rückschlüsse auf Sicherheitsbewusstsein, Ungeduld und Misstrauen gezogen werden.[24] Banken setzen zunehmend „Tracker" ein, die die Nutzer beim Besuch ihrer Webseiten beobachten und sensible Informationen sammeln.[25]

5.7 Überwachung bei Prüfungen

Prüfungen an Universitäten werden in den USA bereits seit einigen Jahren zum Teil online durchgeführt. Seit der Corona-Pandemie werden auch in Deutschland immer mehr Online-Prüfungen angeboten. Dabei kommt meist spezielle Software zum Einsatz, mit deren Hilfe überprüft werden soll, dass während der Prüfung keine unerlaubten Hilfsmittel eingesetzt werden.

Die Überwachung durch diese Systeme kann sehr umfassend sein. Zur Identifikation der zu prüfenden Person wird meist eine Kamera (zum Beispiel Webcam des Laptops) verwendet, dabei kann auch eine automatische Gesichtserkennungssoftware eingesetzt werden. Auch eine Verhaltenskontrolle einschließlich Augenbewegungen kann verwendet werden. Häufig muss der Prüfling auch einen Scan des gesamten Raumes, zum Beispiel mit einer Smartphone-Kamera zulassen. Das gesamte Verhalten des Kandidaten während der Prüfung und der verwendete Rechner können teilweise permanent überwacht und automatisch analysiert werden. Ein Unternehmen aus München hat 2021

[24] Die Zeit, Nr. 23, 2017, 1.6.2017, Seite 32

[25] Die Zeit, Nr. 41, 2017, 5.10.2017, Seite 25

für ein entsprechendes System einen BigBrotherAward (siehe Abschnitt 9.2) erhalten, da der Einsatz dieses Systems als schwerer Eingriff in die Privatsphäre bewertet wurde.[26]

5.8 Autonomes Fahren

Voraussetzung für „Autonomes Fahren“ sind Sensoren, die die gesamte Umgebung eines Fahrzeugs erfassen. Solche Fahrzeuge haben eine Vielzahl von Sensoren, wie Kameras sowie Ultraschall- und Radargeräte, die kontinuierlich riesige Mengen an Daten sammeln und verarbeiten. Die Datenerfassung dient dem sicheren Betrieb des autonomen Fahrens einerseits und einer Fehleranalyse, falls es zum Beispiel zu einem Unfall kommt, andererseits. Die Daten werden also auch aufgezeichnet und irgendwo gespeichert.

Diese Datenquellen werden inzwischen auch polizeilich für Ermittlungszwecke verwendet. Die Polizeibehörde von San Francisco hat sogar ein Schulungsdokument erstellt, um darzustellen, welches Ermittlungspotenzial die Daten von autonomen Fahrzeugen haben. Die Daten aus autonomen Fahrzeugen können mit den Daten aus festinstallierten Überwachungskameras verknüpft und so für vielfältige Ermittlungszwecke genutzt werden.[27]

Das Netzwerk Datenschutzexpertise hat 2020 ein Gutachten erstellt, das zeigt, in welchem Umfang Tesla-Fahrzeuge auch personenbezogene Daten sammeln und die europäischen Vorgaben des Datenschutzes verletzen. Mit 8 Kameras sowie Ultraschall- und Radarsensoren wird die Umgebung bis zu einer Entfernung von 250 Metern „gescannt“. Zu den erfassten personenbezogenen Daten gibt das Unternehmen nicht an, auf welcher Rechtsgrundlage die Erfassung beruht und es wird auch nicht der Zweck der Erfassung hinreichend angegeben, sodass Artikel 5 der Datenschutz-Grundverordnung der EU (DSGVO) verletzt wird. Zum Beispiel werden beim automatisierten Einparken auch Personen und die Kennzeichen anderer Fahrzeuge erfasst. Auch eine dauerhafte Erfassung der Umgebung ist möglich. Die erfassten Daten werden teilweise in die USA und eventuell weitere Staaten übertragen. Auch dies widerspricht der

[26] https://haxko.space/themen/datenschutz/proctoring/ und FIfF-Kommunikation 2+3, 2021, Seite 58-59

[27] https://www.heise.de/news/San-Francisco-Polizei-verwendet-Robo-Autos-als-rollende-Spione-7092196.html?affiliateId=17957

Rechtsprechung des Europäischen Gerichtshofs (EuGH). Das Gutachten bemängelt auch, dass es keine Datenschutz-Folgenabschätzung gibt. Denn durch die systematische umfangreiche Überwachung im öffentlichen Straßenraum kann auch davon ausgegangen werden, dass Bewertungen der Fahrzeugführer erfolgen und so sehr sensible Daten automatisch erzeugt werden.[28]

5.9 Gesundheit

Im Gesundheitswesen gibt es vielfältige Interessen an Überwachung. Dies kann der Verbesserung der Situation von Patienten dienen, aber auch das Ziel haben, Unternehmen Informationen für Werbemaßnahmen zu liefern.

Gesundheitsdaten sind auch für Hacker lukrativ. Kliniken und Arztpraxen sind häufig Ziel von Cyber-Angriffen, hierbei werden teilweise auch Patientendaten erbeutet. Auf der Jahreskonferenz des FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, www.fiff.de) im Oktober 2017 hat Stefan Jäger in seinem Vortrag „IT-Sicherheit im Gesundheitswesen“ berichtet, dass es im Internet einen Schwarzmarkt für Gesundheitsdaten gibt, wobei je Patient 50 bis 100 US$ bezahlt werden.

Über Online-Tracking-Codes gingen persönliche Daten der Versicherten eines amerikanischen Gesundheitsunternehmens an Google, Microsoft und X (vormals Twitter). Im Mai 2024 hat das Unternehmen die 13,4 Millionen Betroffenen über diesen Datenschutzverstoß informiert.[29]

Viele Menschen liefern freiwillig über Fitnessgeräte umfangreiche Gesundheitsdaten an irgendwelche Internetunternehmen. Fitnessgeräte und -armbänder übertragen Bewegungs- und Gesundheitsdaten ins Netz. Apple bietet eine Armbanduhr an, die nicht nur permanent den Puls messen, sondern auch ein Elektrokardiogramm (EKG) erstellen kann. Mit dem Versprechen besser zu schlafen, bieten verschiedene Apps für Handys die Analyse von Schlafverläufen an, wobei mit Bewegungssensor und Mikrofon umfangreiche Daten gesammelt und auf irgendwelche Server übertragen werden. Hieraus sind auch Informationen über Gesundheitsaspekte ableitbar. Die Dating-App Grindr erfasst von ihren Nutzern den HIV-Status und gibt diese Information an Dritte weiter.

---

[28] [Wei20] und https://www.heise.de/news/Studie-zum-Datenschutz-Elektroautos-von-Tesla-duerften-nicht-zugelassen-werden-4934095.html

[29] https://www.heise.de/news/US-Versicherer-gab-Millionen-Patientendaten-ueber-Tracking-Tools-an-Drittanbieter-9701893.html?wt_mc=nl.red.ho.ho-nl-newsticker.2024-04-30.link

Über Fitness-Tracker können sogar militärische Geheimnisse aufgedeckt werden.[30]

In den USA ist ein Medikament mit eingebautem Sender zugelassen worden. Wenn die Tablette in den Magen gelangt und aufgelöst wird, wird ein schwaches elektrisches Signal an ein Pflaster gesendet, das auf die Brust geklebt ist. Dieses liefert die Information über Bluetooth an ein Smartphone, das die Daten ins Internet übertragen kann. So kann überwacht werden, ob Patienten ihre Medikamente regelmäßig einnehmen.[31]

Im Mai 2025 berichtet heise von einem Selbstversuch einer Forscherin, die eine „smarte Pille" geschluckt hat, welche anschließend verschiedene Daten per Funk aus dem Magen und dem Darm sendet. Gemessen werden Temperatur und ph-Wert sowie Werte, die auf entzündliche Darmerkrankungen hinweisen. Durch die Einnahme von Getränken konnte die Wirkung der Sensoren unmittelbar nachgewiesen werden.[32]

Viele Menschen können sich sogar vorstellen, sich einen Chip implantieren zu lassen, um den Gesundheitszustand permanent zu überwachen. Eine vom ZDF im Herbst 2024 durchgeführte Umfrage hat ergeben, dass vor allem junge Menschen im Alter von 25 bis 34 Jahren sich ein solches Implantat vorstellen können. Die Zustimmung bei Männern war hierbei deutlich größer als bei Frauen.[33]

In einem Interview mit der Süddeutschen Zeitung kritisiert Christiane Woopen, Professorin für Ethik und Theorie der Medizin, das übermäßige Sammeln von Daten durch Fitnesstracker und andere Geräte[34]. Sie betont, dass das Leben nicht nur nach solchen Daten ausgerichtet werden darf, sondern dass zum Beispiel auch Meditation oder Gespräche mit Freunden für das Wohlbefinden und die Gesundheit wichtig sein können. Sie betont insbesondere, dass Gesundheit nicht wichtiger ist als Freiheit und ein selbstbestimmtes Leben. Frau Woopen sieht auch eine Gefahr für die Solidarität in unserer Gesellschaft. Die Digitalisierung ermöglicht es, die Lebensweise einer Person detailliert zu erfassen. Krankenkassen bieten Boni oder Prämien für gesunde Lebensweisen an, die mit entsprechenden Daten belegt werden. Dies kann dazu führen, dass diejenigen diskriminiert werden, die nicht bereit sind, all diese Daten über sich zu liefern.

---

30 https://www.heise.de/newsticker/meldung/Fitnesstracker-Strava-Aktivitaetenkarte-legt-Militaerbasen-und-Soldaten-Infos-in-aller-Welt-offen-3952875.html

31 Süddeutsche Zeitung vom 16.11.2017, Seite 14

32 https://www.heise.de/news/Smarte-Pille-funkt-aus-Magen-und-Darm-10393622.html

33 https://www.zdfheute.de/panorama/ki-chip-implantat-gesundheit-tracking-100.html

34 Süddeutsche Zeitung vom 11.9.2018, Seite 21

Dirk Heckmann, Professor für IT-Recht, warnt in [Hec15] vor einer Determinierung des Menschen im digitalen Gesundheitswesen. Über das Internet der Dinge, smarte Geräte und Kleidung oder eingepflanzte Chips kann ein lückenloses Gesundheitsprofil erstellt werden, was schließlich zu einem „perfekten Menschen" führen kann. Wer nicht mitmacht, könnte sozial isoliert werden und Nachteile zum Beispiel bei Versicherungen oder der Berufswahl haben.

5.10 Überwachung und Bewertung in China

Besonders weit verbreitet sind Überwachungskameras in China. Überwachungskameras werden in China auch genutzt, um Daten für ein Bewertungssystem zu liefern. In einem „sozialen Bonitätssystem" (Punktesystem) soll jeder Chinese bewertet werden. Das Vorhaben zur Bewertung der Bürger in China wird in der nächsten Kurseinheit (IUG 2) genauer behandelt. Auch Touristen, die nach China reisen, werden überwacht. Dazu wird an der Grenze eine App auf deren Smartphone installiert, die umfangreiche Daten vom Smartphone ausliest und auf irgendwelche Server überträgt.[35]

Überwachungspraktiken an Grenzen gibt es nicht nur in China, sondern auch in vielen anderen Staaten. Wer ein Visum für die USA beantragt, muss seine Nutzernamen bei sozialen Medien und E-Mail-Adressen (auch veraltete) preisgeben. Auch in den USA müssen Einreisende teilweise ihr Handy und ihren Computer zur Untersuchung abgeben und entsperren.[36]

5.11 Pegasus

Viele Staaten haben ein Softwaresystem Pegasus von einem israelischen Softwareunternehmen gekauft, um damit unter anderem Journalisten, Menschenrechtsaktivisten und politische Gegner, aber auch Staatsoberhäupter anderer Staaten zu überwachen und sensible Daten zu erobern. Mit dieser Software sollen vor allem Smartphones infiziert werden, um zum Beispiel Gespräche auf-

[35] Süddeutsche Zeitung vom 3.7.2019, Seite 3

[36] Süddeutsche Zeitung vom 5.7.2019, Seite 4

zuzeichnen und die Kommunikation über Messengerdienste abzufangen. Mikrofon und Kamera eines Smartphones können dabei aktiviert werden, ohne dass der Nutzer dies merkt. Die Schadsoftware kann auf einem Smartphone mit sogenannten Zero-Click-Exploits installiert werden, ohne dass die Zielperson irgendeinen Link anklicken muss. Lediglich die Rufnummer des Smartphones muss bekannt sein. Mitte 2021 wurden die Ergebnisse einer groß angelegten Untersuchung zur Verwendung von Pegasus bekannt. Die Ergebnisse zeigen, dass vor allem autoritäre Staaten diese Software gegen politische Gegner einsetzen.[37]

Für die mit Pegasus überwachten Personen ist die Vergangenheit durchsuchbar und die Gegenwart kontrollierbar. Alle auf einem Smartphone gespeicherten Daten können übermittelt werden, auch Fotos und Adressbuch. Mit bestimmten Apps wird der Standort übermittelt. Selbst verschlüsselte Chats und Gespräche können überwacht werden. In Deutschland verwenden das Bundeskriminalamt (BKA) und der Bundesnachrichtendienst (BND) Pegasus. Es ist aber nicht bekannt, welche Ziele und Zielpersonen damit verfolgt werden.[38]

Israel hat mehrere NGOs (Nichtregierungsorganisationen) der Palästinenser zu Terrororganisationen erklärt und deren Mitglieder mit der Pegasus-Software überwacht. Auch die polnische Regierung soll die Software gekauft haben, um politische Gegner auszuspionieren und Wahlen zu eigenem Gunsten zu beeinflussen. Die spanische Regierung hat mindestens 65 Politiker und Aktivisten Kataloniens unter anderem mit Pegasus abgehört. Dazu gehört auch der Regionalpräsident Kataloniens.[39]

In mindestens 45 Staaten soll die Pegasus-Software eingesetzt worden sein, unter anderem in Saudi-Arabien, Marokko, Indien, Thailand und Ungarn. Etwa 12.000 bis 13.000 Ziele werden jährlich mit dieser Software verfolgt. Jeder Verkauf der Software muss von Israel genehmigt werden. Nach Veröffentlichung dieser Überwachungspraxis durch ein internationales Journalistenkonsortium hat die israelische Regierung die Zahl der Länder, in die diese Software exportiert werden darf, eingeschränkt. Insbesondere das Journalistennetzwerk „Forbidden Stories“ und Amnesty International haben wesentlich dazu beigetragen, diese Überwachungspraxis publik zu machen.[40]

---

[37] FIfF-Kommunikation 2+3, 2021, Seite 9, 42, 43, Süddeutscher Zeitung vom 19. Juli 2021

[38] Süddeutsche Zeitung vom 8.9.2021, Seite 2, vom 9.10.2021, Seite 6, und vom 11.2.2022, Seite 11

[39] Süddeutsche Zeitung vom 9.11.2021, Seite 6, vom 5.1.2022, Seite 6, und vom 19.7.2022, Seite 7

[40] Süddeutsche Zeitung vom 19.7.2022, Seite 7, und vom 23.8.2022, Seite 6

5.12 Online-Plattformen

Die Federal Trade Commission (FTC) ist eine Bundesbehörde der USA und nimmt unter anderem Aufgaben des Verbraucherschutzes wahr. FTC hat im September 2024 einen Bericht zur Überwachungspraxis durch die digitalen Medien veröffentlicht. Der Bericht stützt sich auf eine vierjährige Untersuchung zu Praktiken der großen Internetkonzerne, wie Amazon, Google, Meta und viele weitere. Der Bericht kritisiert, dass Grundrechte der Bürger bedroht und die Rechte von Kindern und Jugendlichen nicht hinreichend geschützt werden. Aus wirtschaftlichen Gründen betreiben diese Unternehmen ein riesiges Überwachungsnetzwerk mit erheblichen Gefahren für die Betroffenen, wie zum Beispiel Identitätsdiebstahl und Stalking. Die Konzerne praktizieren einen umfassenden Datenaustausch bezogen auf ihre Nutzerprofile.[41]

5.13 Staatliche Überwachung in Deutschland

Eine Auswertung der Transparenzberichte von den vier „Big-Tech-Unternehmen“ Apple, Meta, Google und Microsoft hat ergeben, dass Deutschland besonders viele Nutzerinformationen von diesen Konzernen abfragt und erhält. Pro Einwohnerzahl liegt Deutschland bezüglich solcher Abfragen auf Platz 2 hinter den USA. In einem Zeitraum von 10 Jahren hat Deutschland seit 2013 zu 709.400 Konten Nutzerinformationen abgefragt. Begründet werden solche Abfragen mit strafrechtlichen Ermittlungen. Im Jahr 2022 gab es einen Anstieg solcher Abfragen um 38% im Vergleich zum Vorjahr. Die meisten Anfragen von unseren Behörden hat Google erhalten. Von den vier untersuchten Unternehmen hat Apple die wenigsten Anfragen erhalten, war dafür aber am auskunftsfreudigsten. Nicht alle Anfragen an die Unternehmen werden vollständig beantwortet. Bei Apple liegt die Offenlegungsquote bei 82 %, bei Microsoft bei 67 % und bei den anderen Unternehmen dazwischen.[42]

---

41 https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services und https://www.heise.de/news/FTC-Bericht-Massenueberwachung-durch-Online-Plattformen-ist-ausser-Kontrolle-9956430.html

42 https://www.heise.de/news/Ueberwachung-Deutschland-fragt-europaweit-die-meisten-Nutzerdaten-ab-9860933.html , https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf und https://surfshark.com/government-requests-for-user-data

Die bekanntesten Institutionen in Deutschland mit Überwachungsaufgaben sind der Bundesnachrichtendienst (BND), das Bundesamt für Verfassungsschutz (BfV) und der Militärische Abschirmdienst (MAD). Kaum bekannt, aber inzwischen vielleicht der größte Geheimdienst in Deutschland ist das Militärische Nachrichtenwesen (MilNW) der Bundeswehr. Diese Organisation mit knapp 7000 Beschäftigten arbeitet ohne gesetzliche Grundlage und ohne Kontrolle. Die Aufgaben des MilMW richten sich vor allem auf das Ausland, wo Gespräche über Funkgeräte und Handys abgehört und Internetdaten systematisch und automatisiert ausgewertet werden. Der ehemalige Bundesdatenschutzbeauftragte Ulrich Kelber beklagt zahlreiche datenschutzrechtliche Verstöße des MilMW und kritisiert die fehlende Rechtsgrundlage dieser Organisation. Während es für BND und MAD strenge Vorgaben für Überwachungstätigkeiten gibt, können diese durch das MilMW übergangen werden.[43]

Die Aktivitäten des BND wurden 2020 durch das Verfassungsgericht eingeschränkt (siehe Abschnitt 8.2). Zuvor wurde bekannt, dass der BND am Frankfurter Internetknoten DE-CIX etwa 1,2 Billionen Nachrichten täglich abfangen kann. Gegen diese Praxis gab es einige Klagen.[44]

Insgesamt gibt es in Deutschland umfangreiche Überwachungsaktivitäten. Das Bundesjustizministerium und das Bundesinnenministerium haben Anfang 2024 das Max-Planck-Institut (MPI) zur Erforschung von Kriminalität, Sicherheit und Recht in Freiburg damit beauftragt, eine Überwachungsgesamtrechnung für Deutschland zu erstellen, d.h. die Überwachungsbefugnisse und - maßnahmen von Behörden in Deutschland zu erfassen und zu bewerten.[45]

Der Bericht des MPI vom Januar 2025 kommt zu dem Ergebnis, dass bei den Überwachungsmaßnahmen die Abfragen von Telekommunikationsverkehrsdaten und der Inhalte dieser Kommunikationen in allen Bundesländern dominieren. In diesem Projekt wurde ein hoher Handlungsbedarf zur Erfassungspraxis von Behörden festgestellt, denn um die Verhältnismäßigkeit staatlicher

---

43 https://www.heise.de/news/Forscher-Abhoertruppe-der-Bundeswehr-agiert-auf-verfassungsrechtlich-duennem-Eis-9868331.html

44 https://www.de-cix.net/de/unternehmen/medien/pressemitteilungen/stellungnahme-der-de-cix-management-gmb-h-zum-urteil-des-bundesverfassungsgerichts-am-19-mai-2020-bnd-gesetz und https://www.golem.de/news/de-cix-bnd-kann-1-2-billionen-verbindungen-pro-tag-abzweigen-2005-148515.html

45 https://www.bmjv.de/SharedDocs/Publikationen/DE/Fachpublikationen/2025_Forschungsbericht_Ueberwachungsgesamtrechnung.pdf , https://www.heise.de/news/Ueberwachung-Eine-Gesamtrechnung-mit-offenen-Posten-10370672.html und https://www.telepolis.de/features/Ueberwacht-Deutschland-seine-Buerger-zu-viel-10374779.html

Eingriffe in die Freiheitsrechte der Bürger prüfen zu können, sind Dokumentations- und Transparenzregeln zu befolgen, die derzeit offenbar nicht immer eingehalten werden.

Als ein wesentliches Ergebnis der Untersuchungen wird in dem Bericht angegeben: „Die Gesamtheit der sicherheitsrechtlichen Befugnisnormen ist in quantitativer und normtechnischer Hinsicht von einem sehr hohen Komplexitätsniveau gekennzeichnet. Die Gesamtzahl von 3.228 Befugnissen und Befugnisvarianten, auf deren Basis die hier einbezogenen Sicherheitsbehörden Überwachungsmaßnahmen anordnen und durchführen können, ist nur noch schwer zu überblicken. Dabei ist zu berücksichtigen, dass einige Überwachungsmaßnahmen mit mutmaßlich hoher Praxisrelevanz, wie etwa die Zugriffe auf Finanz- und Kontodaten, hier noch nicht einmal eingerechnet sind.“[46]

[46] https://www.bmj.de/SharedDocs/Publikationen/DE/Fachpublikationen/2025_Forschungsbericht_Ueberwachungsgesamtrechnung.pdf?__blob=publicationFile&v=6 , Seite 106

Gesamter Inhalt dieser Kurseinheit