Jugendsession
Session des jeunes
Sessione dei giovani
Sessiun da giuvenils

Jugendsession 2022

10. - 13. November

Dossier

ÜBERWACHUNG IN DER SCHWEIZ

Autor: Alessio Suter

Inhaltsverzeichnis

Worum geht es?

Wenn heute von Videoüberwachung gesprochen wird, so ist den meisten Leuten bewusst, dass Videokameras sowohl in privaten Bereichen wie in Einkaufszentren, am Arbeitsplatz, im Aussenbereich von Privathäusern als auch im öffentlichen Raum, auf Plätzen, an Strassen, Bahnhöfen, Flughäfen etc. installiert sind. Die stetige Zunahme der Anzahl an Überwachungskameras geht einher mit neuen technologischen Entwicklungen, welche mit den Stichworten «intelligente Kameras» und «Gesichtserkennung» benannt werden. Bereits heute kann ein Netzwerk von mehreren Videokameras gemeinsam Bewegungsprofile erstellen, was das (Ver)folgen einer Person ermöglicht.

Technologien zur Gesichtserkennung sind weit verbreitet und akzeptiert. So kann man diese beispielsweise nutzen, um das eigene Smartphone zu entsperren. In der Regel greift die Gesichtserkennung nicht auf riesige Fotodatenbanken zur Bestimmung der Identität einer Person zurück – sie bestimmt und erkennt schlichtweg eine Person als den oder die Eigentümer:in des Geräts und verwehrt allen anderen den Zugriff.

Nebst dem Entsperren von Mobiltelefonen lassen sich mit der Gesichtserkennung auch Gesichter von Personen, die an bestimmten Kameras vorbeilaufen, mit Bildern von Personen auf einer Überwachungsliste abgleichen. Überwachungskameras mit Gesichtserkennungstechnologien können zudem mit weiteren Daten verknüpft und ergänzt werden. Ein Beispiel wären Informationen und Daten aus sozialen Medien und Profilen, die dort existieren. Ein Beispiel hierfür wäre China und das Sozialkreditsystem.

Überwachung ist jedoch nicht nur mittels Gesichtserkennungstechnologien möglich. Insbesondere bestimmte Tech-Konzerne kamen in der Vergangenheit in die Kritik, die Daten ihrer Nutzer:innen nicht genügend zu schützen. Bei gewissen Internetdiensten stimmen die Nutzer:innen freiwillig der Nutzung ihrer Daten zu. Häufig ist Ihnen dabei jedoch nicht klar, wozu die Daten schliesslich verwendet werden. Im gewissen Sinne können diese freiwillig zur Verfügung gestellten Daten auch zu Überwachungszwecken genutzt werden[1].

[1] Siehe hierzu Cambridge Analytica: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Glossar

- **Überwachung**: Überwachung bezeichnet die systematische Erhebung von Informationen über Objekte oder Personen. Geschieht diese im Verdeckten, wird auch von Observation gesprochen. (Wikipedia 2022)
- **Gesichtserkennung**: Die Gesichtserkennung ist ein Verfahren zur Identifizierung oder Verifizierung der Identität einer Person anhand ihres Gesichts. Gesichtserkennungs-systeme können für die Bestimmung oder Identitätsbestätigung von Personen auf Fotos, in Videos oder in Echtzeit eingesetzt werden. (Kaspersky 2022)
- **Datenschutz**: Verlangt, dass personenbezogene Daten geschützt werden. Datenschutz sichert das Grundrecht von Personen auf informationelle Selbstbestimmung. Menschen haben dadurch selbst die Freiheit zu bestimmen, wie mit ihren Daten umgegangen wird. Persönlichkeitsrechte und Privatsphäre sollen gewahrt bleiben. (Luber & Schmitz 2017)
- **Überwachungskapitalismus:** (englisch *surveillance capitalism*) ist ein vor allem von der US-amerikanischen Wirtschaftswissenschaftlerin Shoshana Zuboff geprägter Begriff, unter dem sie ein marktwirtschaftliches, kapitalistisches System versteht, das die mit technischen Mitteln von Menschen abgeschöpften persönlichen Daten dazu benutzt, Informationen über Verhaltensweisen zu sammeln, diese zu analysieren und für marktökonomische Entscheidungsfindungen aufzubereiten, um daraus Verhaltensvorhersagen generieren zu können und über deren Nutzung Gewinne zu erwirtschaften. (Zuboff 2015)
- **Biometrische Daten:** Der Begriff Biometrie bezeichnet die Wissenschaft und Technologie zur Messung und Analyse biologischer Daten. Im Bereich der Informationstechnologie bezeichnet man mit Biometrie Technologien zur Messung und Analyse körperlicher Merkmale von Menschen. Dadurch lassen sich bestimmte Merkmale wie DNA, Fingerabdruck, Retina und Iris der Augen, Stimmmuster, Gesichtsmuster sowie Eigenschaften der Hände zur Authentifizierung heranziehen. (ComputerWeekly 2008)
- **Besondere Personendaten:** Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht. Hier können zwei Kategorien unterschieden werden: Das DSG (Bundesgessetz über den Datenschutz) nennt als «sensitive» Personendaten ausdrücklich (aber nicht abschliessend) beispielsweise religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten, Angaben über die Gesundheit, Angaben über Massnahmen der sozialen Hilfe und Angaben über administrative oder strafrechtliche Verfolgungen oder Sanktionen. Als zweite Kategorie

> nennt das DSG die Persönlichkeitsprofile. Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, womit ebenso die Gefahr der Grundrechtsverletzung besteht. Der Begriff der «besonderen Personendaten» fasst die beiden Kategorien zusammen. (DSB-BS 2022)

Situation in der Schweiz

Es gibt eine Vielzahl an unterschiedlichen Formen der Überwachung. So werden beispielsweise auch Patient:innen auf der Intensivstation oder der Zustand einer Staumauer systematisch «überwacht». Das vorliegende Dossier befasst sich aber primär mit der Gesichtserkennung sowie der Überwachung im Internet.

Gesichtserkennung

Die Gesichtserkennungstechnologie ist ein brisantes Thema, das derzeit weltweit heftige Debatten auslöst. Einerseits gilt die Gesichtserkennungstechnologie als äußerst effizient. Sie ist schnell und Befürworter:innen behaupten, sie sei objektiv bei der Erfüllung von Aufgaben. Andererseits wird befürchtet, dass die in diesen Systemen innewohnenden Verzerrungen und Ungenauigkeiten zu Diskriminierung von Frauen oder People of Colour führen können. Ebenso wird die Gefährdung grundlegender Menschenrechte befürchtet, wie z. B. unsere Freiheit, gegen Maßnahmen zu protestieren, mit denen wir nicht einverstanden sind.

Vorteile

Die Gesichtserkennung wird als etwas beworben, was unser Leben bequemer macht. Wir müssen nicht mehr mühsam ein Passwort in unser Telefon eingeben oder unseren Ausweis am Flughafen vorzeigen. Stattdessen reicht unser Gesicht aus, um zu bestätigen, wer wir sind. In Osaka wurden an vier Bahnhöfen Gesichtserkennungssysteme eingeführt, mit denen Menschen durch Scannen ihres Gesichts ohne Fahrkarte oder Ausweis durchgelassen werden. Ein Beamter des Verkehrsministeriums erklärte, man werde "die Tatsache als Vorteil hervorheben, dass Passagiere mit großem Gepäck die Schranken passieren können, indem sie einfach ihr Gesicht zeigen, anstatt nach einem Fahrschein zu suchen". (Aszodi & Norga 2021)

Ein weiteres Argument ist, dass die Gesichtserkennung für mehr Sicherheit sorge. Es heißt, die Biometrie biete ein höheres Maß an Sicherheit, dass eine Person, die versucht, auf einen Dienst zuzugreifen oder eine Transaktion durchzuführen, auch wirklich existiert. Die Befürworter:innen der Biometrie weisen darauf hin, dass Passwörter, PINs und andere persönliche Identifizierungsdaten durch Datenschutzverletzungen kompromittiert werden können, so dass

Betrüger auf Konten zugreifen können, die traditionelle Authentifizierungsmethoden verwenden. Im Gegensatz dazu ist es für eine andere Person als Dich selbst schwieriger, Deinen Fingerabdruck an Ort und Stelle bereitzustellen. Was die Strafverfolgung angeht, so argumentieren die Befürworter:innen der Gesichtserkennung, dass die Polizei dadurch Verdächtige leichter aufspüren kann und effizienter Videomaterial analysieren könnte.

Nachteile

Weltweit fordern verschiedene Akteure, dass Gesichtserkennungstechnologien entweder in bestimmten Bereichen, für bestimmte Nutzungen oder komplett verboten werden sollen (Amnesty International 2021).

Gegner:innen wiederum warnen davor, dass Passwörter, PINS und Identifizierungsdaten für Konton geändert werden können, falls diese gehackt werden. Falls wiederum biometrische Daten aus welchem Grund auch immer in die falschen Hände gelangen, können sich Betroffene kaum gegen Identitätsdiebstähle oder andere Missbräuche ihrer biometrischen Daten schützen (schliesslich können wir nicht unsere DNA oder Fingerabdrücke einfach so verändern). Das Wissen, dass wir leicht identifiziert werden können, kann zudem dazu führen, dass wir uns aus Angst vor negativen Konsequenzen selbst zensieren. Menschen, die wissen, dass sie identifiziert und in eine Datenbank aufgenommen werden, werden so möglicherweise von der Wahrnehmung ihrer politischen Grundrechte (z.B. Teilnahme an einer Demonstration) abgeschreckt. Dies ist besonders schädlich in Situationen, in denen Regierungen das Demonstrationsrecht unrechtmäßig eingeschränkt haben, um öffentliche Kritik zu unterdrücken.[2] Neuere und mit Kameras ausgestattete Technologien wie etwa Drohnen vergrössern den Einsatzbereich von Gesichtserkennung zu Überwachungszwecken zusätzlich. (SKP 2021)

Überwachung im Internet

Überwachung geschieht im Internet auf unterschiedliche Arten und zu unterschiedlichen Zwecken (Infosec 2022). Bei Treueprogrammen werden etwa gezielt Daten über die persönlichen Aktivitäten gesammelt, auf deren Basis dann Gutschriften oder Rabatte gewährt werden. Eine weitere und weit verbreitete Form sind Dienste, die zwar gratis angeboten werden, deren Geschäftsmodell aber auf der Auswertung persönlicher Daten beruht. Darunter fallen etwa die bekanntesten sozialen Medien, welche zu einem grossen Teil durch zielgerichtete Werbung finanziert werden. Meist gibt ein:e Nutzer:in ein Zugeständnis ab, dass er oder sie mit der Sammlung, Verarbeitung und Auswertung dieser Daten einverstanden ist. Wichtig in diesem

[2] https://netzpolitik.org/2019/petition-fuer-komplettverbot-von-gesichtserkennung-in-den-usa-gestartet/

Zusammenhang sind etwa sogenannte *Cookies*, welche das Anlegen von Nutzerprofilen durch Browser oder Webseiten ermöglichen (Ionos 2020).

Bei den vorher genannten Beispielen geht die Überwachung meist von Unternehmen aus. Daneben gibt es aber auch staatliche Überwachung im Internet wie etwa die Vorratsdatenspeicherung, bei welcher die Nutzung von Internet und weiteren Telekommunikationstechnologien der Bürger:innen systematisch erhoben und (in der Schweiz für 6 Monate) gespeichert wird. Diese dient zwar dem Zweck der Verbrechensaufklärung, greift aber gleichzeitig auch in die Grundrechte ein.

Vorteile

Ein Vorteil ist, wie bereits oben erwähnt, dass solche Dienste für die Nutzer:innen oft kostenlos sind. Dies, da Werbetreibende bereit sind, mehr für eine Platzierung zu bezahlen, wenn diese auf ihre Zielgruppe zugeschnitten ist. Gerade auf den sozialen Medien werden die Daten aber nicht nur für personalisierte Werbung eingesetzt. Alle angezeigten Beiträge sind an die jeweilige Person angepasst, basierend auf persönlichen Daten und vergangenem Verhalten. Dies soll es ermöglichen, Nutzer:innen nur diejenigen Beiträge anzuzeigen, die sich tatsächlich interessieren.

Geht es um Strafverfolgung, dann sind die Vorteile ziemlich eindeutig. Da Kommunikation heutzutage oft über technologische Hilfsmittel wie Smartphone und/oder das Internet erfolgen, ermöglicht die Vorratsdatenspeicherung die Nachverfolgung ebendieser Kommunikation während den Ermittlungen. Die Nützlichkeit der Vorratsdatenspeicherung bedarf aber weiterer Prüfung. (SKP 2021)

Nachteile

Die Nachteile von Überwachung im Internet betreffen zumeist die Privatsphäre der Nutzer:innen. Grundsätzlich garantiert die Bundesverfassung den Anspruch auf Schutz der Privatsphäre und beinhaltet insbesondere auch den Schutz vor Missbrauch der persönlichen Daten.

Dienste im Internet, welche persönliche Daten sammeln und verarbeiten müssen deshalb bereits vor der Nutzung die explizite Zustimmung der Benutzer:innen zur Sammlung und Verarbeitung bestimmter Daten einholen. Die neue Datenschutzverordnung der EU erlaubt zudem eine stärkere Kontrolle über die eigenen personenbezogenen Daten, welche teilweise auch für die Schweiz gilt (Steiger 2019). Es gibt auch Fälle, in denen die Sammlung und Verarbeitung personenbezogener Daten durch Private illegal erfolgt, etwa bei Betrugsversuchen im Internet oder Identitätsdiebstahl.

Geht die Überwachung vom Staat aus, muss ein überwiegendes öffentliches Interesse vorwiegen und die Massnahme muss verhältnismässig sein. Während es sich bei der Aufklärung von Straftaten zumeist um ein Anliegen von grossem öffentlichem Interesse handelt, ist nicht klar, ob daraus auch die Legitimität der präventiven Sammlung von Telekommunikationsdaten folgt. Also, ob es angemessen oder eben verhältnismässig ist, mit diesem Argument die Nutzungsdaten aller Nutzer:innen während mehrerer Monate präventiv zu speichern. (SKP 2021)

Fazit

Überwachung gibt es in allen erdenklichen Formen, oft wird darunter aber das systematische Verfolgen einer Person inklusive Sammlung relevanter persönlicher Daten verstanden. Das vorliegende Dossier hat versucht, diesen Aspekt von Überwachung am Beispiel der Gesichtserkennung sowie der Überwachung im Internet etwas genauer zu beleuchten. Beide Beispiele sollen verdeutlichen, dass es sich bei Überwachung um ein Spannungsfeld handelt. Auf der einen Seite die möglichen Vorteile für die einzelnen Nutzer:innen sowie für die Gesellschaft als Ganzes, auf der anderen Seite der Datenschutz und das in der Verfassung festgeschriebene Recht auf den Schutz der Persönlichkeit. Zudem wurde aufgezeigt, dass aus neuen Technologien auch neue Zwecke und Mittel zur Überwachung folgen können, welche eine konstante Diskussion zum Thema Überwachung erfordern.

Gesetzliche Grundlagen

Bundesverfassung Art. 13: Schutz der Privatsphäre[3]

Legt fest, dass jede Person «Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs» sowie «auf Schutz vor Missbrauch ihrer persönlichen Daten» hat.

Artikel 28-28l Zivilgesetzbuch (ZGB): Schutz gegen Verletzungen der Persönlichkeit[4]
Legt die Grundlage für den Schutz vor einer widerrechtlichen Persönlichkeitsverletzung fest. Zudem werden die zur Verfügung stehenden Massnahmen und Zuständigkeiten definiert.

Bundesgesetz über den Datenschutz (DSG)[5]
Definiert den Geltungsbereich inklusive der zulässigen Ausnahmen sowie die im Zusammenhang mit dem Datenschutz relevanten Begriffe. Das totalrevidierte Datenschutzgesetz, welches neu etwa auch biometrische Daten als besonders schützenswert definiert, tritt per 1. September 2023

[3] https://www.fedlex.admin.ch/eli/cc/1999/404/de#art_13
[4] https://www.fedlex.admin.ch/eli/cc/24/233_245_233/de#art_28
[5] https://www.fedlex.admin.ch/eli/fga/2020/1998/de

in Kraft. Eine Übersicht zu den wichtigsten Änderungen stellt das Bundesamt für Justiz zur Verfügung (QR-Code weiter unten).

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)[6]
Legt die Grundlage für die Überwachung des Post- und Fernmeldeverkehrs, welche in Vollzugs- und Strafverfahren durchgeführt wird. Es beinhaltet Mitwirkungspflichten insbesondere für Anbieterinnen von Fernmelde- und Kommunikationsdiensten und legt Aufbewahrungsfristen sowie Auskunftsrechte fest.

Nachrichtendienstgesetz (NDG)[7]
Legt die Grundlage für die Tätigkeiten des Nachrichtendienstes und regelt die Zusammenarbeit mit Privatpersonen und anderen Behörden.

Europäische Datenschutzgrundverordnung (DSGVO)[8]
Die neue Datenschutzverordnung der EU, welche die Regeln zur Verarbeitung personenbezogener Daten festlegt. Gilt zwar nicht direkt für Schweiz, jedoch für Unternehmen, welche Waren oder Dienstleistungen in der EU anbieten oder Daten von EU-Bürger:innen im Internet beobachten.

Was passiert aktuell in der Politik?

22.022 Geschäft des Bundesrates: Bundesgesetz zum Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben. Diese Botschaft des Bundesrates beschreibt die geplante Umsetzung diverser Massnahmen zur Schaffung von rechtlichen Grundlagen für das «E-Government», also die Inanspruchnahme von behördlichen Dienstleistungen der Verwaltung

21.3855 Motion: Archivierungspflicht des Nachrichtendienstes und Persönlichkeitsschutz stärken. Diese Motion behandelt den Umgang des Nachrichtendienstes des Bundes (NDB) mit nicht mehr benötigten Daten und deren Archivierung.

[6] https://www.fedlex.admin.ch/eli/cc/2018/31/de
[7] https://www.fedlex.admin.ch/eli/cc/2017/494/de
[8] https://dsgvo-gesetz.de/

Interessante Links

Links	QR Code
Amnesty International – Überwachung https://www.amnesty.ch/de/themen/ueberwachung/ueberwachung	
Eidgenössischer Datenschutzbeauftragter (EDÖB) - Datenschutz https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html	
Humanrights.ch - Menschenrechte https://www.humanrights.ch/de/ipf/menschenrechte/	
Bundesamt für Justiz – Totalrevision des Datenschutzgesetzes https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/dsg-uebersicht-aenderungen.pdf.download.pdf/dsg-uebersicht-aenderungen-d.pdf	

Quellenverzeichnis

Amnesty International. (2021). *Grundrechte Schützen-Gesichtserkennung stoppen*. [online] https://www.amnesty.ch/de/themen/ueberwachung/gesichtserkennung/dok/2021/grundrechte-schuetzen-gesichtserkennung-stoppen [05.10.2022]

Aszodi, N. & Norga, A. (2021): *Gesichtserkennung: Vor-und Nachteile*. [online] https://www.liberties.eu/de/stories/gesichtserkennung-vorteile-nachteile/43708 [05.10.2022]

ComputerWeekly. (2008): *Biometrie*. [online] https://www.computerweekly.com/de/definition/Biometrie [05.10.2022]

Datenschutzbeauftragter des Kantons Basel-Stadt (DSB-BS). (2022). *Was sind Personendaten?* [online] https://www.dsb.bs.ch/datenschutz/was-sind-personendaten.html [05.10.2022]

Eidgenössischer Datenschutz und Öffentlichkeitsberater (EDÖB). (2022). *Datenschutz*. [online] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html [05.10.2022]

humanrights.ch. (2018). *Videoüberwachung in der Schweiz - unübersichtlich oder gar nicht geregelt*. [online] https://www.humanrights.ch/de/ipf/menschenrechte/privatsphaere/unuebersichtliche-videoueberwachung-schweiz [05.10.2022]

Infosec. (2018). *Was bedeutet «regelmäßige und systematische Überwachung»?* [online] https://www.infosec.ch/blog/was-bedeutet-regelmaessige-und-systematische-ueberwachung/ [05.10.2022]

Ionos. (2020). Was sind Cookies? [online] https://www.ionos.de/digitalguide/hosting/hosting-technik/was-sind-cookies/ [05.10.2022]

Kaspersky. (2022). *Die Gesichtserkennung – Definition und Erläuterung*. [online] https://www.kaspersky.de/resource-center/definitions/what-is-facial-recognition [05.10.2022]

Luber, S. & Schmitz, P. (2017). *Was ist Datenschutz?* [online] https://www.security-insider.de/was-ist-datenschutz-a-604115/ [05.10.2022]

Schweizerische Kriminalprävention (SKP). (2021). Überwachung. [online] https://www.skppsc.ch/de/wp-content/uploads/sites/2/2021/07/skp_info_2_21.pdf [05.10.2022]

Steiger, S. (2017). *Leitlinien: Wann gilt die DSGVO / GDPR in der Schweiz und anderswo ausserhalb der EU?* [online] https://steigerlegal.ch/2019/11/17/dsgvo-gdpr-leitlinien-schweiz-dsgvo-3/ [05.10.2022]

Wikipedia. (2022). *Überwachung*. [online] https://de.wikipedia.org/wiki/%C3%9Cberwachung [05.10.2022]

Zuboff, S. (2015). *Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology*.

SAJV | Projektleitung Jugendsession
projektleitung@jugendsession.ch
www.jugendsession.ch

SAJV CSAJ
Schweizerische Arbeitsgemeinschaft der Jugendverbände
Conseil Suisse des Activités de Jeunesse
Federazione Svizzera delle Associazioni Giovanili
Federaziun Svizra da las Uniuns da Giuventetgna

Dieses Thema wurde erarbeitet mit der Unterstützung des *Bundesamtes für Justiz BJ* und der *Digitalen Gesellschaft Schweiz*.