Jugendsession
Session des jeunes
Sessione dei giovani
Sessiun da giuvenils

Jugendsession 2020

05. - 08. November

> Dossier

Überwachung in der Schweiz

Wie es bisher war und was es zu beachten gibt

Autorin: Laura Hagen

Inhaltsverzeichnis

Globalisierung

Überwachung in der Schweiz

Glossar

Daten	Informationen, die in diesem Kontext von einem Computer verarbeitet werden. Können in Text, Bild, Video oder auditivem Format sein. (techfacts)
Metadaten	Eck- oder Randdaten mit Informationen z.B. wer wann wen angerufen hat und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat und die Standortinformationen des Mobiltelefons. Es können ebenso Metadaten von Informationen aus Bild- und Textdaten behoben werden. (Wikipedia)
Vorratsdatenspeicherung (VDS)	Im schweizerischen Kontext beschreibt die VDS eine gesetzliche Verpflichtung zur Speicherung von Metadaten durch Telefon-, Email- und Internetanbieter für 6 Monate. Es kann zwischen dem privaten und öffentlichen Sektor zu Unterschieden der Regelung kommen. (Wikipedia)
Datenschutz	Datenschutz definiert sich über 5 Schwerpunkte: **Gesetzmässigkeit**, **Verhältnismässigkeit**, **Zweckbindung**, **Sicherheit** und **Transparenz**. (Glossar, ZH)
Gesetzmässigkeit	Datenerhebung nur mit Zustimmung und in Einklang mit den lokalen und internationalen Gesetzen
Verhältnismässigkeit	Soll verhindern, dass zusätzliche Daten, die nicht zwingend gebraucht werden, behoben und bearbeitet werden
Zweckbindung	Das Sammeln und Bearbeiten der Daten wird strikt an einen Zweck gebunden
Sicherheit	Daten sind sicher und für Unbefugte nicht zugänglich gespeichert
Transparenz	Es ist klar und offen deklariert, wer welche Daten von wem, wofür und für wie lange sammelt und mit wem sie geteilt werden
Datensicherheit	Zu Datensicherheit gehören alle nötigen Aspekte, um den Schutz von Daten zu garantieren. Diese haben im Englischen

	folgende Ziele: Confidentiality (Vertraulichkeit), Integrity (Integrität) and Availability (Verfügbarkeit) kurz CIA. Das erste bedeutet, dass Unbefugte keinen Zugriff zu Informationen erhalten. Integrität sieht vor, dass Daten unversehrt, vor technischen Defekten und Manipulationen geschützt sind. Letzteres ist nötig, damit im Bedarfsfall die Daten verwendet werden können. (Datenschutz.org, 2020)
Privatsphäre	Privatsphäre bezieht sich auf den nicht öffentlichen Raum einer Person, welcher ausser ihr niemanden angeht. Jede*r hat das Recht, dass die privaten Angelegenheiten in Ruhe gelassen werden. (juraforum)

Worum geht es?

Zur Globalisierung gehört die Digitalisierung zwingend dazu, da diese unter anderem die Kommunikation zwischen den verschiedenen Ländern etc. deutlich vereinfacht. Dies bringt viele verschiedene Vorteile, aber auch gewisse Nachteile. Das Bedürfnis der Staaten nach nationaler und internationaler Sicherheit und Kontrolle fördert die Zunahme von Überwachung, auch auf einer globalen Ebene. Ein gutes Beispiel hierfür ist der NSA Skandal aus dem Jahre 2013, bei dem eine enorme Menge an Kommunikationsmetadaten gesammelt wurde.[1] Jedoch sind nicht nur Behörden über uns informiert. Auch Unternehmen wie Google oder Facebook sammeln Unmengen an „rohen Daten“ über ihre Nutzer*innen, aus welchen sie dann Profile erstellen, die das Verhalten der Personen prognostizieren und an Interessierte verkauft werden (Wolfie 2014).

<u>Was genau ist Überwachung?</u>
Überwachung definiert sich über das Beobachten der Kommunikation, Handlungen oder Bewegungen einer Person. Sie kann z.B. durchgeführt werden durch abfangen, sammeln, auswählen, zurückhalten, analysieren, teilen und weiteren Gebrauch von den Daten, die man über die Zielperson besitzt. Solche Daten können von Inhalten der Kommunikation über Randdaten (Metadaten, umfassen Informationen „wie (durch welches Medium (PC, Handy…), wo, wann“) bis zu Bewegungsprofil und Tagesabläufen einer Person reichen. Das Recht auf den Schutz der Privatsphäre ist ein Menschenrecht. Daher ist ein solcher Eingriff in die Privatsphäre nur rechtsmässig, solange er gezielt und begründet ist (z.B. mit dem Interesse der öffentlichen Sicherheit). Solche Daten können aber auch zu Missbräuchen verleiten, denn anhand dieser Informationen kann man leicht Oppositionen und Widerstände kontrollieren und einschränken (Q&A Amnesty International Überwachung, 2015, S.4).

[1] https://www.bbc.com/news/world-us-canada-23123964

Es gibt verschiedene Arten von Überwachung. Einerseits öffentliche (durch Behörden und Geheimdienste vollzogene), andererseits private, die durch private Firmen und hauptsächlich aus kommerziellen Gründen stattfindet. Dazu gehören Banken, Lebensmittelgeschäfte, Versicherungen und viele mehr. Die Daten können sie z.B. durch Nutzung der angebotenen Dienstleistung (soziale Medien, Treueprogramme…) sammeln. Zusätzlich gibt es auch die „horizontale Überwachung". Hierunter versteht man das gegenseitige Überwachen von Individuen z.B. über soziale Medien. Ein Beispiel für diesen Überwachungstyp ist etwa das Stalking. Überwachung kann durch verschiedene Methoden ausgeübt werden. Es können Computer, Telefone, Kameras und Mikrophone überwacht oder bestimmte Spionage-Software wie etwa Staatstrojaner eingesetzt werden. Überwachungstechnologien werden fortlaufend weiterentwickelt, um die Überwachung zu vereinfachen und optimieren, etwa durch Drohnen oder den Einsatz von künstlicher Intelligenz. (aclu.org)

Für den Staat hat Überwachung eine strategische und sicherheitstechnische Bedeutung. Dank ihr kann man Gewohnheiten (Lebens-, Arbeits-, Mobilitätsrhythmen) feststellen, anhand welcher das Verfolgen von Straftäter*innen vereinfacht wird. Sie kann auch helfen, Abläufe im Nachhinein zu rekonstruieren und z.B. die Unschuld/ Schuld von Personen beweisen. Ebenso kann sie das Sicherheitsgefühl von Bürger*innen fördern. Deshalb wird Überwachung teilweise auch mit dem Glauben verteidigt, so Terroranschläge und extremistische Handlungen verhindern oder die Identität der Schuldigen leichter ermitteln zu können.
Private Überwachung geschieht mehrheitlich für kommerzielle Zwecke und weil Menschen bereit sind, ihre Daten preiszugeben, wenn sie dafür eine Gegenleistung erhalten. Dabei ist man sich oft nicht bewusst, was die (eher indirekten) Konsequenzen davon sein können. Ganz nach dem Motto „Ich habe ja nichts zu verbergen". (McKinnon, 2014)

Überwachung in der Schweiz:

In der Schweiz wurde vor etwas mehr als 30 Jahren der Fichenskandal aufgedeckt. Die Öffentlichkeit erfuhr, dass der Schweizer Staatsschutz (heute NDB) seit 1900 über 700'000 Menschen bespitzelt hat, ohne dass eine gesetzliche Grundlage hierfür bestand (SRF myschool). Diese Affäre zeigt, welche Konsequenzen Überwachung haben kann: z.B. Misstrauen in die Regierung oder Institutionen.

Wichtige Schweizer Akteure

Nachrichtendienst des Bundes (NDB)[2]

Der Nachrichtendienst des Bundes, kurz NDB, ist ein „sicherheitspolitisches Instrument" das im Namen des Bundesrates für die „Lagebeurteilung und Prävention von Terroranschlägen, gewalttätigem Extremismus, Spionage, Verbreitung von Massenvernichtungswaffen und [...] Cyberangriffen auf kritische Infrastrukturen" zuständig ist. Unteranderem ist der NDB ebenso für die Früherkennung und Bekämpfung in den genannten Bereichen verantwortlich. (vbs.admin.ch)

Militärischer Nachrichtendienst (MDN)

[2] Der NDB kooperiert mit ausländischen Nachrichtendiensten und hat ein Budget von ca 75.6 Millionen (2018). Er berichtet jährlich über die Lage in der Schweiz im Bezug zur Sicherheit. Gesetzlcih stützt er sich auf das NDG und BWIS. (https://www.admin.ch/opc/de/classified-compilation/19970117/index.html)

Der MDN (auch NDA = Nachrichtendienst der Armee genannt) ist für den Chef der Armee und den Bundesrat tätig. Hauptsächlich beschafft er wichtige Informationen für die Armee über das Ausland und verfolgt die Entwicklungen von Streitkräften und anderen Geheimdiensten im Ausland. Zusätzlich unterstützt er den Führungsstab mit Informationen über Bedrohungen und die Umwelt und leitet Erkenntnisse für Weiterentwicklung und Ausbildung der Armee ab. Zu guter Letzt ist er auch bei der Entwicklung neuer nachrichtendienstlicher Systeme beteiligt und ist zuständig für die „Entwicklung und Durchsetzung der Nachrichtendienstdoktrin der Armee“. Bei Operationen im Inland arbeitet er mit dem NDB, sowie mit kantonalen und bundesweiten Stellen zusammen. (vtg.admin.ch)

Private Firmen und Überwachung

So genannte Datenkraken wie etwa Google (Youtube, Gmail, Google) oder Facebook (Instagram, What’s App, Messenger) sammeln Daten, die Suchverhalten, angeschaute und hochgeladene Beiträge, Standort- und Kontaktverhalten bis hin zu WLAN-Zugangspunkten und Bluetooth Signalen bschreiben. Anhand dieser Daten kann man umfängliche Profile über die Nutzer*innen und deren Interessen, Freundeskreis, Lebensstil etc. erstellen (Simon Crins, 2020). Diese Daten werden intern bearbeitet, können aber auch an Dritte weitergegeben werden, beispielsweise zum Zweck der gezielten/personalisierten Werbung. Jedoch können auch Behörden Zugang zu diesen Daten verlangen. (Andreas Maurer, 2019)

Wichtige Gesetze

NDG (Nachrichtendienstgesetz)

Das NDG ist die gesetzliche Grundlage für die Tätigkeiten des Nachrichtendienstes. Es erlaubt dem NDB unter gewissen Voraussetzungen, Informationen aus nicht öffentlichen Bereichen anzuschaffen. Gewisse Überwachungsmassnahmen (wie z.B. Kabelaufklärung) setzen eine Bewilligung von dem oder der Vorsteher*in des VBS und des Bundesverwaltungsgerichts voraus. Diese Kompetenzen werden laut NDB für „die Früherkennung und Bekämpfung von Bedrohungen für die Schweiz“ benötigt (vbs.admin.ch - Nachrichtendienstgesetz).

Bundesgesetz betreffend der Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Das BÜPF regelt die Voraussetzungen für die Überwachung und Mitwirkungspflichten privater und öffentlicher Firmen. Darunter fallen Internetanbietende, Hosting-Provider und Betreibende von Chat-Diensten. (ejpd.admin.ch, 2013; buepf.ch, 2016) Unter anderem verlangt das BÜPF von Telefon- und Internetanbietern die Speicherung sämtlicher Metadaten ihrer Nutzer*innen für 6 Monate. Auf diese können Strafverfolgungsbehörden bei Verdacht auf eine Straftat zugreifen. (PDF Amnesty Q&A S. 1 und 2)

Sozialdetektive und das Sozialversicherungsgesetz

Sozialversicherungen dienen dazu, Menschen finanzielle Sicherheit zu gewährleisten falls diese benötigt wird. Um zu verhindern, dass diese Hilfe missbraucht wird und um abzuklären, wer diese beanspruchen darf, können Sozialversicherungen geregelte Observationen durchführen. Das bedeutet, dass bei einem konkreten Missbrauchsverdacht Sozialdetektive zum Einsatz kommen dürfen. Diese beobachten die Person, dürfen Bild- und Tonaufnahmen machen und technische Instrumente zur Standortbestimmung benutzen. (Christian Raaflaub, 2018)

Gesetzliche Grundlagen

Bundesverfassung Art. 13 Schutz der Privatsphäre
1 Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.
2 Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Bundesverfassung **Art. 36** Einschränkungen von Grundrechten
Grundrechte dürfen nur basierend auf einer gesetzlichen Grundlage eingeschränkt werden. Starke Einschränkungen müssen im Gesetz schon festgelegt sein, ausser der Fall sei nicht anders abwendbar. Das öffentliche Interesse oder der Schutz von Grundrechten anderer muss grösser sein, als der Eingriff. Jedoch muss er verhältnismässig sein und die Grundrechte per se sind unveränderlich.

Europäische Menschenrechtskommission (EMRK), Artikel 8 Recht auf Achtung des Privat- und Familienlebens
1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit sowie der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Uno-Pakt 2, Art. 17
1 Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.
2 Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Was läuft aktuell in der Politik?

Interpellation 19.3868: Der Nachrichtendienst beschnüffelt weiterhin gesetzeswidrig legale politische Tätigkeiten. Welche Kontroll- und Disziplinarmassnahmen beschliesst der Bund?
Diese Interpellation hinterfragt die illegale Überwachung von politisch anerkannten Parteien und Organisationen durch den NDB, die durch einen Medienbericht am 23.05.2019 aufgedeckt wurde. Daraufhin wurde die Geschäftsprüfungsdelegation (GPDel) und der EDÖB zu sofortigen Kontrollmassnahmen durch die Grüne Partei aufgefordert. Der BR erwiderte, dass es zu keiner illegalen Überwachung kam. Gestützt auf das NDG darf der NDB Dokumente und andere Informationen die öffentlich Quellen oder „Meldungen von Drittbehörden zu Demonstrationen mit Gewaltpotential“ entspringen, in gewissen Systemen des NDBs ablegen. Die Bedingung hierfür ist dass die Information einen Bezug zu den Aufgaben des NDBs hat. Generell unterliegt der NDB einer Datenbearbeitungsschranke: er darf keine Informationen über die politische Betätigung und über die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit in der Schweiz erfassen und bearbeiten.

Interpellation 19.4438 : Totalüberwachung in der Schweiz?
Da der Schweiz Angebote für „intelligente[r] Technologie zur Gesichtserkennung“ gemacht wurden, stellt Herr Grüter hier folgende Fragen an den Bundesrat. Was sind die rechtlichen Grundlagen und inwieweit werden Datenschutz und Schutz der Privatsphäre berücksichtigt? Die Antwort lautet, dass es auf die DSG gestützt ist und die Daten nur verhältnismässig und zweckgebunden verarbeitet werden, so wie es vom Gesetz verlangt wird. Die zweite Frage befasst sich mit der Situation in Europa. Biometrische Daten (wie z.B. für die Gesichtserkennung nötig) dürfen nicht bearbeitet werden. Nur wenn ein überwiegendes öffentliches Interesse besteht, kann eine Bearbeitung genehmigt werden. Auf die Frage, ob die Auswertung der Daten von einem Menschen oder durch eine KI geschieht, antwortete der BR, dass im aktuellen Gesetz nicht differenziert ist, wer die Auswertung übernimmt. Jedoch haben Betroffene das Recht zu verlangen, dass eine natürliche Person eine Entscheidung überprüft. Der BR betont ebenso, dass kantonal und national ausreichende Vorschriften existieren, die eine Überwachung von Bürger*innen durch solche Systeme verhindern.

Weitere Interpellationen, Motionen etc. die lesenswert sind:

- 20.3323 : Überwachung von Personen aufgrund von Entlassung
- 19.4031 : Loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Garantir le principe de proportionnalité
- 19.1052 : Surveillance exercée par les groupes d'entreprises. Il faut mieux protéger les employés
- 19.5283 : Frais de surveillance téléphonique
- 19.4322 : Le Palais fédéral est-il surveillé par le Service de renseignement de la Confédération?

Entscheidungsgrundlagen : Schlüsselargumente (Pro und Kontra Argumente)

Vorratsdatenspeicherung (VDS)

Pro	Kontra
- Vereinfacht das Verfolgen von Kriminellen; insbesondere von Täter*innen, die im Internet Verbrechen begehen, beispielsweise Kinderpornografie. (Meike Laaff, 2008) - Die VDS kann Menschen ein Gefühl von Sicherheit verleihen. - Im Normalfall ist ein Eingriff nur temporär und kaum wahrnehmbar. - Wenn es für die Öffentlichkeit und das allgemeine Wohl der Betroffenen wichtig ist, dann sollte ein Eingriff in die Privatsphäre einer Person gerechtfertigt werden können. - Zu viel Datenschutz könnte für die Wirtschaft und Innovation schädlich sein, da die Daten für bestimmte Konzerne essentiell sind.[3]	- Studien zeigen, dass die generelle Verwendung von Metadaten keinen Nutzen bei der Prävention von Delikten leistet. (Michael Kilchling et al., 2011) - Die VDS greift in die Privatsphäre ein, ist sehr kostspielig und verletzt das Recht auf Privatsphäre und Meinungsfreiheit. - Da die meisten Systeme nicht auf Sicherheit und Privatsphäre „by design“ erstellt sind, gibt es ein hohes Missbrauchspotential. U.a. können durch Cyberattacken auf sensible Daten zugegriffen werden. - Auch wenn es „nur“ Metadaten sind, kann man viel über die Person in Erfahrung bringen[4].

[3] https://thewire.in/tech/data-privacy-digital-economy
[4] Vgl. https://chadsansing.github.io/curriculum-testing/expanded-privacy-curriculum/pros-and-cons.html und http://www.vorratsdatenspeicherung.de/content/view/83/87/lang,en/

Überwachung unter Corona

Durch die Corona-Krise hat sich die Situation weiter verschärft. Im Namen der Sicherheit (und zur Kontrolle, ob sich die Bevölkerung an die vom Bundesrat verordneten Empfehlungen hält), wurden erweiterte Überwachungskompetenzen für den Staat eingeführt, wenn auch mehrheitlich zeitlich beschränkt.[5]

Contact und Proximity Tracing

Hierunter versteht man das Nachverfolgen von den gepflegten Kontakten einer infizierten Person. Dies kann analog oder digital (durch z.B. die SwissCovid App) geschehen und bezweckt, dass Menschen, die mit einer infizierten Person in Kontakt gekommen sind getestet oder in Quarantäne gestellt werden. Dadurch soll die Verbreitung des Virus verhindert oder zumindest verlangsamt werden.

- Eine Simulationsstudie der WHO hat gezeigt, das Contact Tracing in Kombination mit anderen Massnahmen erfolgreich sein kann (WHO, 2019). - Vor allem im Ländervergleich kann man feststellen, dass Länder, welche Contact Tracing verwenden, die Pandemie verhältnismässig unter Kontrolle haben. (Elisabeth Buchwald 2020) - Laut dem Bundesrat ist die SwissCovid App datenschutzfreundlich, da Daten nicht alle zentral auf einem Server sind. Sie werden zudem automatisch nach 20 Tagen gelöscht und die Freiwilligkeit besitzt einen hohen Stellenwert. (newsd.admin.ch)	- Proximity Tracing ist eine sehr teure Massnahme. Allein die Entwicklung der App kostete mehrere Millionen Franken (Wikipedia, 2020). - Die Nutzung einer App fürs Proximity Tracing ist nur sinnvoll, wenn mindestens 60%-70% der Bevölkerung sie installiert hat. (David Uberti, 2020) - Es besteht grosses Missbrauchspotential bezüglich Sicherheit und Datenschutz

Online Plattformen

Gleichzeitig wurde auch die Nutzung von online-Tools oder Plattformen durch Schulen, Universitäten und Arbeitgeber gefördert, welche das „e-schooling“ und „home-office“ ermöglichen.

- Gibt die Möglichkeit, weiterhin zu arbeiten, ohne die eigene Gesundheit und die der anderen zu gefährden. - Daten/Dokumente sind auch zu späteren Punkten aufrufbar und man kann sich individuell organisieren, um das Material zu bearbeiten.	- Das Nachvollziehen wer was und wann tut (bzw. online ist) kann eine Gefahr für die Meinungsfreiheit darstellen, da man „gefährliche“ Meinungen identifizieren kann. - Datensicherheit und Datenschutz der gewählten Plattformen wurde teilweise vernachlässigt oder nicht genügend von Lehrpersonen/Schulen überprüft/ recherchiert Z:B. bei Zoom (Paul Wagenseil 2020)

Überwachung in der Zukunft (Überwachung = Normalzustand Risiko)

Wie es mit der Überwachung in der Zukunft aussieht, ist offen. Insbesondere in Krisenzeiten können Überwachungsmassnahmen helfen, für Ordnung zu sorgen. Jedoch besteht jederzeit auch das Risiko einer ungerechtfertigter Massenüberwachung, die stumm akzeptiert wird.

[5] https://www.republik.ch/2020/06/24/watchblog-wo-unsere-rechte-eingeschraenkt-werden

- Sicherheit und Freiheit schliessen sich nicht aus. Beide können in einer Balance koexistieren. - „Wer nichts zu verbergen hat, hat nichts zu befürchten“, da die Überwachung in diesem Falle die Unschuld beweisen würde. - Jüngere Generationen haben kein Problem damit, Informationen über sich mit der Welt zu teilen. - KIs steigern die Effizienz von Überwachung, was die Kosten minimieren könnte.	- Es besteht das Risiko, dass die Bevölkerung mit Angst und Panik gezwungen wird, einschränkende Massnahmen (wie Echtzeitüberwachung) zu akzeptieren. Man gewöhnt sich an die neue Situation und die Aufhebung kann in Vergessenheit geraten. (Thomas Macaulay, 2020) - Der Einsatz von KI in diesem Kontext ist gefährlich, da sie diskriminierend und voreingenommen sein kann.

Weiterführende Links / Willst du mehr wissen?

Links	QR Code
Allgemeine Argumente über Überwachung https://www.debatingeurope.eu/de/focus/argumente-fuer-und-gegen-staatliche-ueberwachung/	
Amnesty International über Überwachung https://www.amnesty.ch/de/themen/ueberwachung/ueberwachung-in-der-schweiz	
Digitale Gesellschaft Schweiz über Überwachung https://www.digitale-gesellschaft.ch/category/uberwachung/	

Quellenverzeichnis

Aclu.org: Surveillance technologies, aclu.org https://www.aclu.org/issues/privacy-technology/surveillance-technologies [29.08.2020]

Amnesty International (2020): Überwachungsmassnahmen müssen auch unter Notrecht verhältnismässig sein (06.04.2020) https://www.amnesty.ch/de/themen/coronavirus/dok/2020/ueberwachungsmassnahmen-muessen-auch-unter-notrecht-verhaeltnismaessig [13.08.2020]

Buchwald, Elisabeth: What we can learn from South-Korea and Singapore's efforts to stop coronavirus (besides wearing masks), MarketWatch, (06.04.2020) https://www.marketwatch.com/story/what-we-can-learn-from-south-korea-and-singapores-efforts-to-stop-coronavirus-in-addition-to-wearing-face-masks-2020-03-31 [13.08.2020]

buepf.ch (2016): Referendum BÜPF https://www.buepf.ch/ [13.08.2020]

Crins, Simon (2020): Datenkraken- Was wissen Google, Facebook und co?, Mediabasics.org (15.02.2020) https://mediabasics.org/datenkraken-was-wissen-google-facebook-und-co [13.08.2020]

Datenschutz.og (2020): Datensicherheit: Massnahmen für den Schutz von Daten, Datenschutz.org (21.07.2020) https://www.datenschutz.org/datensicherheit-massnahmen/ [13.08.2020]

ejpd.admin.ch: Überwachung des Fernmeldeverkehrs: zeitgemässe und klare Rechtsgrundlage (27.02.2013) https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2013/2013-02-271.html [13.08.2020]

Glossar,ZH: Grundsätze des Datenschutzes, https://www.debatingeurope.eu/de/focus/argumente-fuer-und-gegen-staatliche-ueberwachung/ [29.08.2020]

Juraforum: Privatsphäre- Regelung im Gesetz, Juraforum https://www.juraforum.de/lexikon/privatsphaere [13.08.2020]

Kilchlig et al. (2011): Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsdaten, Max-Planck-Institut für ausländisches und internationales Strafrecht, Newsd.admin.ch https://www.newsd.admin.ch/newsd/message/attachments/61311.pdf [29.08.2020]

Macaulay, Thomas (2020): Snowden warns: The surveillance state we're creating now will outlast the coronavirus – temporary securitycan soon become permanent, The next web, (25.03.2020) https://thenextweb.com/neural/2020/03/25/snowden-warns-the-surveillance-states-were-creating-now-will-outlast-the-coronavirus/ [15.03.2020]

Maurer, Andreas (2019): Erfolg für Schweizer Ermittler: Google rückt Daten von hunderten Nutzern raus, Watson (30.11.2019) https://www.watson.ch/digital/schweiz/501785528-erfolg-fuer-schweizer-ermittler-google-rueckt-daten-von-hunderten-nutzern-raus [13.08.2020]

McKinnon, Ashton (2014): Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone Surveillance, National Association of Administrative Law Judiciary, https://digitalcommons.pepperdine.edu/naalj/vol34/iss2/6/ [29.08.2020]

Meike, Laaff (2008): Freiheit oder Sicherheit?, fluter. (10.11.2008) https://www.fluter.de/freiheit-oder-sicherheit [13.08.2020]

PDF Amnesty International Q&A Überwachung, 2015 https://www.amnesty.ch/de/laender/europa-zentralasien/schweiz/dok/2015/privatsphaere-statt-massenueberwachung/q-a-zu-uberwachung.pdf)

Raaflaub, Christian. (2018): Sozialdetektive: Es darf wieder gefilmt werden, swissinfo.ch (25.11.2018) https://www.swissinfo.ch/ger/politik/abstimmung-25-november-2018_aenderung-des-bundesgesetzes-ueber-den-allgemeinen-teil-des-sozialversicherungsrechts/44561840 [13.08.2020]

SRF myschool: Die Fichenaffäre. https://www.srf.ch/sendungen/myschool/die-fichenaffaere [13.08.2020]

Techfacts – Ihre Experten für neue Medien: Was sind Daten? https://www.techfacts.de/ratgeber/was-sind-daten zuletzt abgerufen am 30.08.2019

Ubert, David. (2020): Apps to track the new coronavirus have an old problem: getting the downloads, The Wallstreet Journal (28.04.2020) https://www.wsj.com/articles/apps-to-track-the-new-coronavirus-have-an-old-problem-getting-the-downloads-11588115728 [15.08.2020]

vbs.admin.ch: Nachrichtendienst des Bundes, https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.html [13.08.2020]

vbs.admin.ch: Nachrichtendienstgesetz, https://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/nachrichtendienstgesetz.html#faq [13.08.2020]

vtg.admin.ch: Militätischer Nachrichtendienst (MDN, https://www.vtg.admin.ch/de/organisation/kdo-op/mnd.html [28.08.2020]

Wagenseil, Paul. (2020): Zoom's security issues: Here's everything that's gone wrong (so far), Tomyguide, (02.08.2020) https://www.tomsguide.com/news/zoom-security-privacy-woes [15.08.2020]

Wolfie, Christl (2014), Kommerzielle digitale Überwachung im Alltag - Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Herausforderungen anhand ausgewählter Problemfelder und Beispiele, Cracked labs – Institut für Kritische Digitale Kultur. https://crackedlabs.org/dl/Studie_Digitale_Ueberwachung_Kurzfassung.pdf)

WHO (2019): Non-pharmateucical public health measures for mitigating the risk and impact of epidemic and pandemic infleunza, Global Influenza Programme, 2019. (https://apps.who.int/iris/bitstream/handle/10665/329438/9789241516839-eng.pdf#page=9)

Wikipedia (2020): Metadaten, Wikipedia (14.03.2020) https://de.wikipedia.org/wiki/Metadaten#Metadaten_bei_der_Kommunikation_im_Internet [29.08.2020]

Wikipedia (2020): SwissCovid, Wikipedia (13.08.2020) https://en.wikipedia.org/wiki/SwissCovid#Costs [15.08.2020]

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

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 vom *Amnesty International* und des *Center for Security Studies ETHZ*