Überwachung durch "den Staat"

Inhaltsverzeichnis

Dr. Rainer Hammerschmidt, Vorstandsmitglied
MA Beate Baum, Wissenschaftliche Fachberatung

Einleitung

Überwachung durch „den Staat“ - Wo lauern die Gefahren? Wie können wir uns schützen?

Wir dokumentieren hier die Inhalte eines Vortrags zum Safer Internet Day im Antikriegscafé COOP Der Vortrag wurde von Uniwut Freies Fernsehen mitgeschnitten und steht auch zum Download in unserer Mediathek und auf unserem Youtube-Kanal. zur Verfügung.

> Aktion Freiheit statt Angst zu Gast bei Uniwut im Offenen Kanal Berlin - AlexTV: Überwachung durch "den Staat", (60 Min, HD 2Mb/s, 932MB)
> https://www.aktion-freiheitstattangst.org/images/videos/UeberwachungStaat-AlexTV-2Mb.mp4
> sowie bei Youtube: Überwachung durch "den Staat"
> https://youtu.be/rmk2MbWaVaM

Der zweite Teil dieser Vortragsreihe "Überwachung durch Unternehmen" ist unter diesem Shortlink http://a-fsa.de/d/17d erreichbar und steht ebenfalls als Video zur Verfügung.

Datenschutz – was ist das?

Zum Verständnis müssen wir uns kurz mit mit den Grundlagen der Datenschutzgesetzgebung in der EU und Deutschland auseinandersetzen.

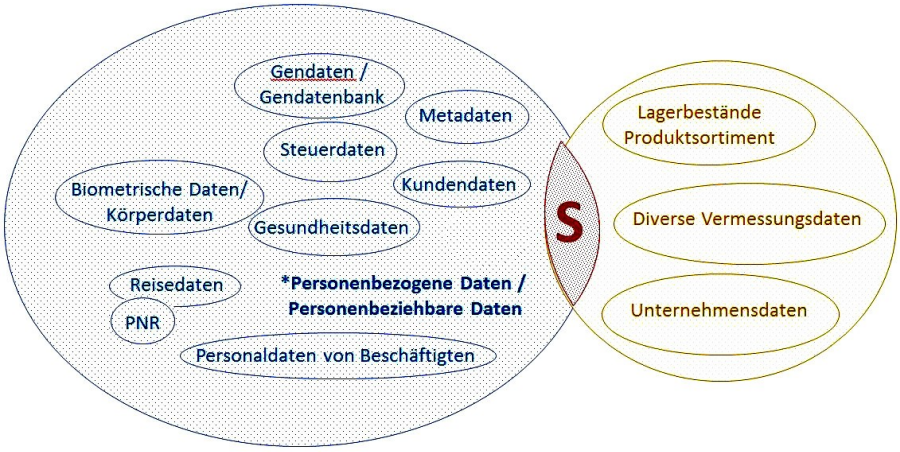
Gesetze:

- BDSG, das Bundesdatenschutzgesetz, Dez.1990
- EU Datenschutz Richtlinie, 95/46/EG, Okt. 1995
- DSGVO, EU Datenschutz Grundverordnung, Mai 2016

Ihre Kerninhalte sind

- Alle diese Gesetze betreffen nur personenbezogene Daten
- Anonymisierung und Pseudonymisierung von personenbezogenen Daten
- BDSG ist ein Gesetz mit Erlaubnisvorbehalt (Gesetz, Verordnung, Einwilligung)

Die folgende Darstellung dient zur Unterscheidung von personenbezogene Daten und anonymen Daten - In der Schnittmenge befinden sich anonymisierte oder pseudonymisierte Daten. „Erlaubnisvorbehalt“ bedeutet, dass **jegliche** Speicherung oder Verarbeitung von personenbezogenen Daten ohne eine Erlaubnis verboten ist.



Die Grundprinzipien des Datenschutzes sind

- Einwilligung (§4a)
- Datenvermeidung und Datensparsamkeit (§3a)
- Zweckbindung (§31,39)

Im internationalen Datenverkehr, insbesondere zu den USA haben wir ein Problem:

Europäischer Datenschutz ist nicht mit dem Begriff „Privacy“ (nach US Recht) vergleichbar. Es gibt in den USA keinen Datenschutz gegenüber Unternehmen, nur gegenüber dem Staat.

Überwachung durch "den Staat"

Seit Bestehen der Bundesrepublik Deutschland sind die Freiheitsrechte durch Gesetze und Verordnungen eingeschränkt worden. diese Einschränkungen finden sich im Grundgesetz selbst, zum Beispiel durch

- die Einführung eines deutschen Militärs im Jahre 1956,
- die Notstandsgesetze im Jahre 1966,
- die Einschränkung des Asylrechts 1993.

Zusätzlich wurden eine Unzahl an Gesetzen eingeführt, die unsere Freiheitsrechte beschränken. Nennen können wir hier die Einschränkung des Postgeheimnisses, die Vorratsdatenspeicherung und vieles mehr.

Vorratsdatenspeicherung

Beginnen wir mit der Vorratsdatenspeicherung. Die Vorratsdatenspeicherung beruhte ursprünglich auf der EU *Richtlinie 2006/24/EG*, die im Rahmen des Stockholm Programms auf Verlangen der Innenminister der EU-Staaten, also auch der deutschen Regierung, beschlossen wurde.

Sie wird gegen den Protest vieler gesellschaftlicher Gruppen im Jahre 2007 für die Bundesrepublik Deutschland eingeführt. Sie erlaubt die Speicherung sämtlicher Kommunikationsdaten für Telefon und Internet ohne jeglichen Anlass von jedem Menschen in Deutschland.

Nach der Verabschiedung des Gesetzes gibt es mehrere Verfassungsklagen dagegen. Mit einem Eilantrag wird das Inkrafttreten des Gesetzes gestoppt.

Im März 2010 wird das Gesetz vom Bundesverfassungsgericht für nichtig erklärt (BVerfG, 1 BvR 330/96, Absatz-Nr. (1–135) Urteil vom 12. März 2003, Wie weiter nach dem Karlsruher Urteil zur Vorratsdatenspeicherung?). Eine Klage vor dem EuGH ist ebenfalls erfolgreich. (EuGH-Urteil vom 8. April 2014)

Der EuGH stellt fest, dass jegliche anlasslosen Speicherung von Kommunikationsdaten in Europa unzulässig ist. Damit sind theoretisch auch die Gesetze zur Vorratsdatenspeicherung in anderen EU-Staaten unzulässig. In Einzelklagen wird dies für verschiedene Länder auch festgestellt (VDS in Tschechien wieder verfassungswidrig, VDS in Rumänien abgeschafft , Keine VDS mehr in Bulgarien).

Trotzdem wird zum Jahresbeginn 2017 ein neues Gesetz zur Vorratsdatenspeicherung in Deutschland beschlossen. Eingebracht wird es von Justizminister Maass, der sich zwei Monate vorher noch gegen eine Vorratsdatenspeicherung ausgesprochen hatte. Das neue Gesetz verlangt kürzere Speicherfristen als das Gesetz von 2007, verstößt aber weiterhin gegen den Grundsatz der anlasslosen Speicherung aller Kommunikationspartner.

Auch gegen dieses Gesetz wird sofort Klage beim Bundesverfassungsgericht eingereicht. Das Bundesverfassungsgericht lehnt diesmal jedoch eine Eilentscheidung dazu ab. Einzelnen Providern gelingt eine Klage auf dem Verwaltungsgerichtsweg wegen der zu hohen Kosten, die durch die Speicherung auf sie zukommen. Daraufhin stellt die Bundesnetzagentur den Provider frei, ob sie speichern wollen. Damit wird erstmals ein

Bundesgesetz durch eine Bundesbehörde zu einer "freiwilligen Angelegenheit".

Eine Evaluierung der Bundesnetzagentur über das Speicherverhalten Ende 2018 stellt jedoch fest, dass eine ganze Reihe von Providern Daten speichert und einige sogar weit über die verlangte Speicherfrist hinaus. (https://www.aktion-freiheitstattangst.org/de/articles/6744-20190102-illegale-speicherpraxis-bei-deutschen-providern.htm)

Tabelle zu Vorratsdatenspeicherung

- Vorratsdatenspeicherung 2007, neue VDS2.0 ab Jan.16
- BverfG Urteil Mär 2010 BverfG:Keine neue Vorratsdatenspeicherung,
- EuGh Urteil Apr 2014 EUGh verwirft Vorratsdatenspeicherung und
- Dez 2016 Nichtigkeit der entsprechenden Gesetze in den einzelnen Staaten EuGh kippt nationale Gesetze zur VDS
- VDS2.0 tritt ab Jan 2016 in Kraft, „muss jedoch nicht umgesetzt werden“
- Bundesnetzagentur stellt im Dez 2018 bei Providern illegales Speichern fest

Novelle zum BKA-Gesetz

Im Jahre 2008 strebt die Bundesregierung eine Novellierung des BKA Gesetzes an. Das erste BKA Gesetz war 1998 in Kraft getreten und hatte unter anderem den **Video-und Lauschangriff auf Privatwohnungen** , sowie den **Bundestrojaner**, also das Ausspähen der Daten auf privaten Rechnern, erlaubt. Dagegen wurde von verschiedenen Bürgerrechtsgruppen eine Verfassungsklage eingereicht. Im Jahre 2004 hatte daraufhin das Bundesverfassungsgericht den Video und Lauschangriff stark eingeschränkt. Der im ersten BKA-Gesetz enthaltene Bundestrojaner wurde komplett verboten mit der Begründung, dass die benutzten Programme auf den infizierten Rechnern Schreibrechte hätten. Damit könnten sie "Beweise" verfälschen oder erzeugen.

Entgegen der Zielrichtung des Bundesverfassungsgerichts beschließt die Bundesregierung im November 2008 die Novelle zum BKA Gesetz, wieder mit Vorschriften zum Video und Lauschangriff und dem Bundestrojaner. Die Proteste gegen die Novellierung des Gesetzes kommen von verschiedenen Bürgerrechtsgruppen in Deutschland, auch Aktive von Aktionen Freiheit statt Angst organisieren den Protest.

Wieder wird eine Klage beim Bundesverfassungsgericht gegen diese Einschränkungen unserer Grundrechte eingereicht. Es dauert bis zum April 2016, also acht Jahre lang, bis das Bundesverfassungsgericht eine Reihe von Änderungsanforderungen verlangt. Bis diese in das Gesetz eingearbeitet sind vergehen noch einmal fast zwei Jahre. Nach unserer Auffassung sind diese Korrekturen im Gesetz allerdings völlig unzureichend.

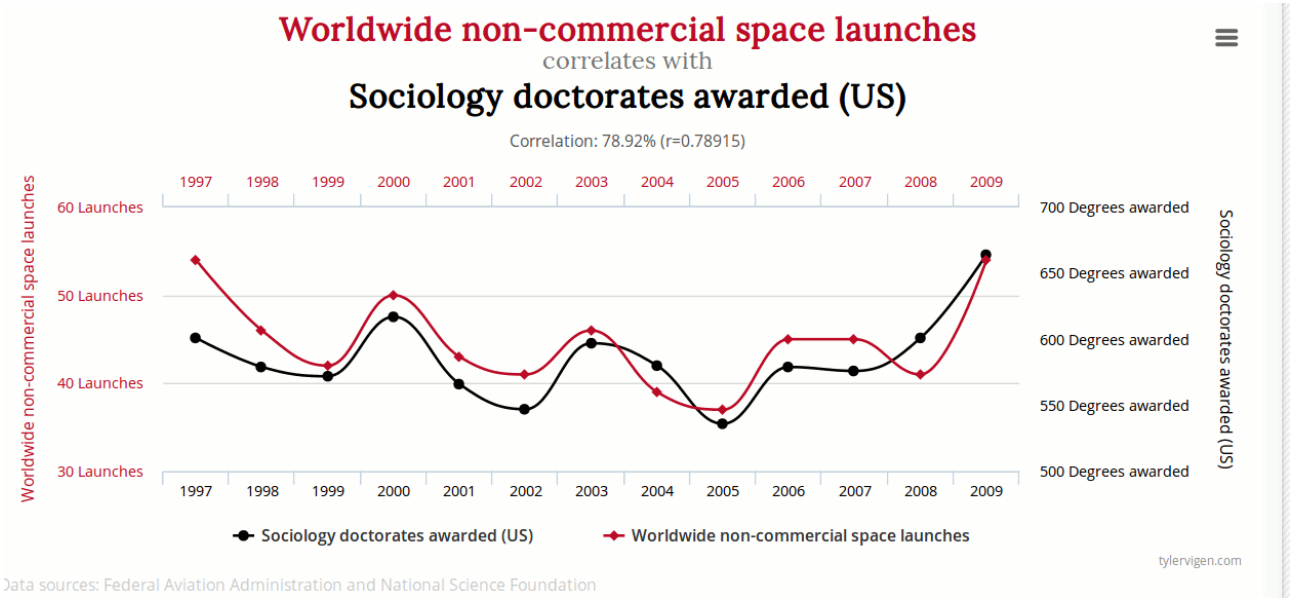
Tabelle zum BKA Gesetz

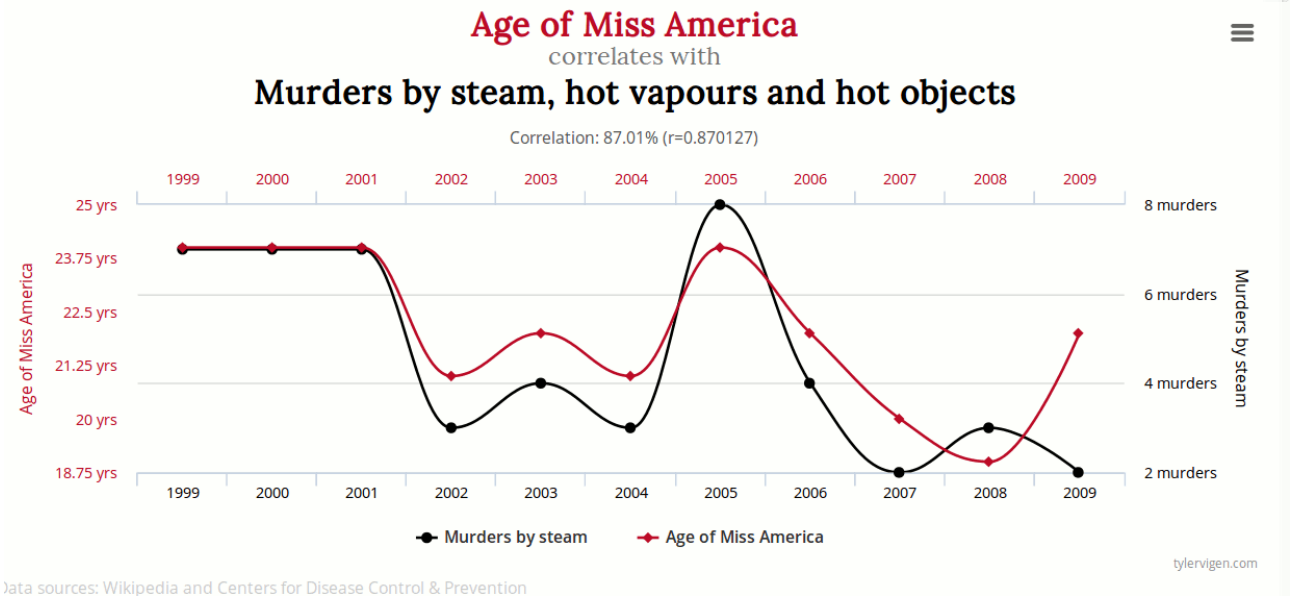
- 1998 erstes BKA-Gesetz mit Video- und Lauschangriff und Bundestrojaner
- 2004 BVerfG: Video- und Lauschangriff wird eingeschränkt, der Bundestrojaner darf nicht "schreiben" (Beweise verändern) - Dies macht ihn technisch unmöglich!
- 11.2008 erste Novellierung des BKA Gesetzes

wieder mit Video- und Lauschangriff auf Wohnungen und dem Bundestrojaner!
- Apr 2016 BVerfG Urteil zur Klage von 2008 mit Änderungsanforderungen

Rasterfahndung / Data Mining

Eine Rasterfahndung (engl. Data Mining) verbindet Daten aus verschiedenen Zusammenhängen und sucht nach Korrelationen. So kann zum Beispiel die Körpergröße und das Alter zu einem sinnvollen Zusammenhang verbunden werden. Es gibt aber genügend Beispiele (siehe Bild) wie man Zusammenhänge in Datenmengen hinein interpretieren kann, die in der Realität nicht vorhanden sind. Deshalb birgt eine Rasterfahndung große Probleme sobald sie sich auf personenbeziehbare Daten erstreckt.





Bereits im März des Jahres 2000 stellen die deutschen Datenschutzbeauftragten auf ihrem jährlichen Treffen fest, dass eine Rasterfahndung auf personenbeziehbare Daten

nach dem BDSG unzulässig ist, auch weil bei der Erhebung der Daten in der Regel verschiedene Zweckbestimmungen vorgelegen haben müssen.

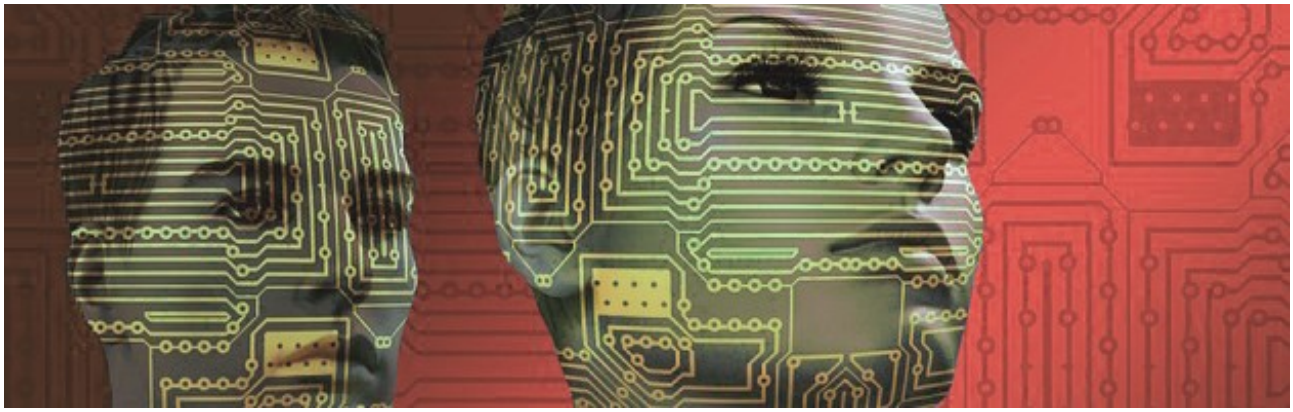
Trotzdem wird Rasterfahndung nach den Anschlägen von 9/11 in der Bundesrepublik über alle ausländischen Studenten in Deutschland durchgeführt. Ein marokkanischer Student klagt dagegen und das Bundesverfassungsgericht stellt im April 2006 fest, dass so etwas **nur im Rahmen "konkreter Gefahr"**, etwa für die Sicherheit des Bundes oder eines Landes oder des Leben eines Bürgers, durchgeführt werden darf.

Trotz dieser Einschränkung durch das Bundesverfassungsgericht wurden in den letzten Jahren immer mehr Polizeidatenbanken miteinander verbunden und die Suche in diesen stellt praktisch stets eine Rasterfahndung dar.

Tabelle zur Rasterfahndung

- März 2000 Entschließung von Deutschen Datenschutzbeauftragten: Data Mining unzulässig auf personenbeziehbaren Daten (Zweckbindung)
- 2001 wurde diese praktiziert, ein marokkanischer Student klagt vor dem BverfG Urteil zu Rasterfahndung: die Rasterfahndung wird dahingehend eingeschränkt, dass sie nur im Rahmen „konkreter Gefahr“, etwa für die Sicherheit des Bundes oder eines Landes oder das Leben eines Bürgers, durchgeführt werden darf.

Biometrische Daten in Ausweis und Pass



Seit dem Jahr 2005 ist ein biometrisches Foto in Reisepässen verpflichtend, im November 2007 bekommt der elektronische Reisepass zusätzlich eine Fingerabdruck zum biometrischen Foto.

Im November 2010 erleben wir die Einführung eines elektronischen Personalausweises (ePerso), der ebenfalls ein biometrisches Foto verlangt und die Möglichkeit der Speicherung eines Fingerabdrucks zur angeblich sicheren Identifikation "anbietet".

Zeitgleich zur Einführung des ePersos zeigt der Chaos Computer Club, dass dieses Dokument und seine Daten leicht zu hacken sind. (https://www.aktion-freiheitstattangst.org/de/articles/1498-20100824-daten-von-euem-personalausweis-ausgelesen.htm und https://www.aktion-freiheitstattangst.org/de/articles/1501-20100826-pressemitteilung-zum-hack-des-elektronischen-personalausweis.htm)

Klagen vor dem EuGH gegen die EU-Verordnung zu

biometrischen Daten in Pässen werden im Oktober 2013 abgewiesen.

Die angeblich sichere Identifikationsmöglichkeit im ePerso wird von den Menschen nicht angenommen. Von 40 Millionen ausgegebenen Ausweisen bis zum Jahr 2016 wird nur bei 4 Millionen diese Funktion verlangt. Dies geschieht auch, weil es kaum sinnvolle Anwendungen für die „sichere Identifikation“ gibt. Daraufhin wird im Frühjahr 2017 die Funktion „sichere Identifikation“ zwangsweise für alle danach ausgegebenen Ausweise verpflichtend. Die Menschen müssen sich nun nach Erhalt des Ausweises um die Sperrung der Funktion selbst bemühen. (https://www.aktion-freiheitstattangst.org/de/articles/6440-20180415-die-odyssee-des-biometrischen-abbilds.htm)

Tabelle zu biometrischen Daten in Pass und Ausweis

- 2005 Einführung biometrisches Foto in Reisepässen verpflichtend
- Nov 2007 Fingerabdruck im Reisepass (ePass)
- Nov 2010 Einführung elektronischer Personalausweis (nPA, ePerso) mit Möglichkeit des Fingerabdrucks als „sichere Identifikation“
- Einführung trotz Ausweis-Hack durch den CCC im Aug 2010
- Okt 2013 EuGH weist Klage gegen EU-Verordnung zu biometrischen Daten in Pässen ab
- Mai 2017: die sichere Identifikation“ im ePerso wird zwangsweise angeschaltet

Versammlungsrecht

Tabelle zum Versammlungsrecht

- Im Grundgesetz garantiert und seit 1953 ein Bundesgesetz
- Unnötigerweise werden länderspezifische Versammlungsrechtsgesetze eingeführt, Bayern Juli 2008, Schleswig-Holstein 2015, ...
- Inhalt sind Verschärfungen bei Videoüberwachung, "Einlass"-Kontrollen, Meldepflicht für Ordner mit persönlichen Daten, ...

Zensus 2011 - Die "neue" Volkszählung

Bei der Volkszählung 1981 hatte sich eine breite Protestbewegung gegen die Erfassung gewehrt, so dass diese durch ein Bundesverfassungsgerichturteil im Jahre 1983 massiv eingeschränkt wurde. Das BVerfG definiert ein **Grundrecht auf informationelle Selbst-bestimmung.**

Im Gegensatz zu diesem Proteststurm läuft die Volkszählung 2011 ohne nennenswerte Proteste ab. Aktion Freiheit statt Angst hatte zur Volkszählung 2011 angemerkt, dass die Fragen zur Religionszugehörigkeit zu detailliert und die Pseudonymisierung der Fragebogen nicht sicher seien.

Tabelle zum Zensus

- Volkszählung 1987 (sollte 1981 stattfinden) unter großen Protesten

- 1983 BverfG Urteil schränkt die Volkszählung radikal ein und definiert das **Grundrecht auf informationelle Selbstbestimmung**
- EU-Verordnung von 2008 bestimmt eine Zählung ab 2011 jeweils alle 10 Jahre,
- Kosten allein für die BRD 600.000.000 €,
- Kritisch: Fragen zu Religionszugehörigkeit, Pseudonymisierung nicht sicher,
- Frühjahr 2011: Kampagne gegen den Zensus stößt auf Desinteresse

Die bundeseinheitliche Steuerliche Identifikationsnummer (Steuer ID)

Nachdem das Vorhaben eines elektronischen Gehaltsnachweises (Elena) an Software-schwierigkeiten und Widerständen in den Unternehmen gescheitert war, wurde im Juli 2007 eine bundeseinheitliche Steueridentifikationsnummer (Steuer ID) eingeführt. Diese Einführung steht im Gegensatz zu einer Bundesverfassungsgerichtsentscheidung, die eine eindeutige Personenkennzeichnung verbietet (wegen Bezugs zur Bevölkerungskennzahl im 3. Reich).

Viele Jahre wurde die Steuer-ID auch lediglich im Zusammenhang mit der Steuererklärung genutzt. 2018 wird jedoch bekannt, dass auch die Verknüpfung der Polizei- und anderer Datenbanken mit dem Primärschlüssel der Steuer-ID durchgeführt werden soll (https://www.aktion-freiheitstattangst.org/de/articles/4508-20140912-steuer-id-wird-zur-personenkennzahl.htm).

Im Juli 2007 eingeführt (für den geplanten aber "verstorbenen" elektronischen Gehaltsnachweis - ELENA) trotz Ressentiments gegen eine Bevölkerungskennzahl

Bestandsdatenauskunft

Im Mai 2013 wird ein Gesetz zur Bestandsdatenauskunft beschlossen. Damit ist ein automatischer Zugriff der Sicherheitsbehörden auf personenbezogene Daten bei den Telefon- und Internetprovidern möglich. Vorher mussten diese Daten einzeln, meist per Fax abgefragt werden. Auch gegen dieses Gesetz gibt es eine Verfassungsbeschwerde, die noch nicht verhandelt wurde.

Tabelle zur Bestandsdatenauskunft

- Mai 2013 Gesetz zum automatischen Zugriff der Polizei/relevante Behörden auf Daten der Provider zum Abrufen von personenbezogenen Daten (Name, Adresse und IP-Adresse).
- Sep 2013 Verfassungsbeschwerde, diese wurde noch nicht verhandelt
- Abmahnwelle als Ergebnis der Einführung der Bestandsdatenauskunft (obwohl Abmahnanwälte keine relevanten Behörden sind!)

Gemeinsames Terrorismusabwehrzentrum

Die Verknüpfung der Datenbanken verschiedener Sicherheitsbehörden (Polizei und Geheimdienste) wurde durch die Schaffung von „Abwehrzentren“ ergänzt.

Diese Zusammenarbeit von Polizei und Geheimdienst stellt eine Aufhebung des Trennungsgebots aus dem Polizeibrief der Alliierten von 1948 dar. Nach den Erfahrungen mit der Gestapo sollte das Entstehen einer großen Sicherheitsbehörde verhindert werden.

(https://www.aktion-freiheitstattangst.org/de/articles/1518-20100905-verfassungsschutz-und-bka-sollen-verstaerkt-mitarbeiter-austauschen.htm)

Tabelle zu „Abwehrzentren“

- Dez 2004 GTAZ (Terror)
- Jan 2007 GIZ (Internet?)
- Nov 2012 GETZ (Extremismus)
- 40 Behörden sind daran beteiligt
- Aufhebung des Trennungsgebots von Polizei und Geheimdiensten

Das GTAZ versagt im Fall Amri total. Obwohl dort mehrfach (8-mal?) über ihn gesprochen wird, sieht keine Behörde Handlungsbedarf. In den Gesprächen ist auch das BAMF beteiligt, wo Amri mehrfach (4-mal?) mit verschiedenen Namen registriert ist.

Flugreisedatenspeicherung

Die anlasslose Speicherung von Flugreisedaten (Passenger Name Records, PNR) nahm ihren Anfang auf Druck der USA. Diese hatten angekündigt keine Reisenden aus der EU, Kanada und Australien einreisen zu lassen, wenn diese nicht vor dem Flug ihre Daten mitgeteilt hätten. Das Abkommen der EU mit den USA, Australien und Kanada tritt 2013 in Kraft.

Von jedem Reisenden werden 60 verschiedene Daten gespeichert und über 15 Jahre aufbewahrt. Das sind Daten zur Reise, zur Person, zu Essgewohnheiten, zu Reisepartnern, u.v.m.

Im Jahre 2015 beschließt das EU-Parlament im zweiten Anlauf ein ähnliches Gesetz für Reisen innerhalb der EU. Einige Staaten in der EU fordern sogar die Ausweitung solcher Datenerhebungen auf Bus- und Schiffsreisen.

Aktion Freiheit statt Angst protestierte dagegen in mehreren Aktionen auf dem Flughafen Tegel (Scannt mein Gepäck)

Tabelle zu Flugreisedatenspeicherung

- USA 2013 Vertrag EU; USA; Kanada und Australien
- Mai 2014 Ablehnung der Einführung innerhalb der EU durch das EU-Parlament
- 2015 Einführung innerhalb der EU (nach den Anschlägen von Paris)
- Kampagnen von Bürgerrechtsgruppen dagegen, z.B. auf dem

Flughafen Tegel
- Eine Erweiterung der Datenerhebung auf Bus- und Bahnreisen ist in Diskussion

EU-Bevölkerungsregister

Bei der Betrachtung der Terrorismusabwehrzentren war von 40 Behörden innerhalb Deutschlands die Rede, die gemeinsam Zugriff auf unsere Daten haben möchten. Beim EU Bevölkerungsregister geht es darüber hinaus um den Zugriff auf die Datenbanken der EU. Das sind z.B.:

- SIS, Schengen Informationssystem
- VIS, Visa-Datenbank
- EURODAC, EU Fingerabdruckdatei
- FRONTEX, EU Agentur zur Grenzsicherung
- EU-Lisa, EU Datenbankverbund
- EASO, European Asylum Support Office
- ECRIS, EU-weite Straftäterdatei

Wir sehen also:

> *Die Innenminister tragen Ideen nach Brüssel, aus denen dann der angebliche Zwang oder die Notwendigkeit entsteht, solche Gesetze zu beschließen.*
>
> *Das BVerfG erklärt die Gesetze anschließend (leider oft nach Jahren) für nichtig. Erneut wird von der Politik ähnliches beschlossen. Die Politiker bleiben unbelehrbar!*
>
> *Alle genannten Gesetze waren unverhältnismäßig und meist auch verfassungswidrig!*

EU-Forschung zur „Sicherheit“/Surveillance

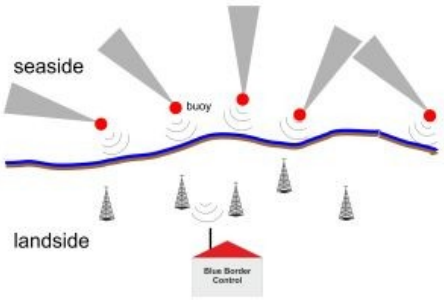
Achtung: man beachte die verschleiernde deutsche Übersetzung!

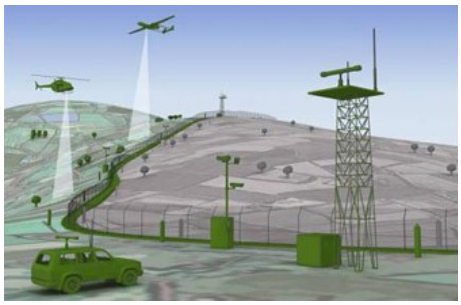
1,4 Mrd. € ist das Budget für das Forschungsprogramm FP7, z.Zt. läuft das Nachfolgeprogramm FP8 Horizon2020.

Ein paar Beispiele aus FP7

- INDECT 2009-2014, ein kleines Projekt mit nur 15 Mio,
  "Intelligent information system observation, searching and detection for security of citizens in urban environment"
- Ziel des Projekts ist die Verknüpfung von Videoüberwachung und Facebook,
- In Polen war zur Fussball EM eine Testlauf im Stadion geplant. Die polnische Polizei konnte damals noch ihre Beteiligung ablehnen.
- Die Gesichtserkennungsprojekte der Bundespolizei am Bahnhof Südkreuz versuchten ähnliches.
- (https://www.aktion-freiheitstattangst.org/de/articles/6343-20171001-videoueberwachung-ein-eingriff-in-die-informationelle-selbstbestimmung.htm)

Die offiziellen Bilder mit denen für diese „Forschungs-“ Projekte geworben wird.





TALOS

Einige große Brüder von Indect:

- SFLY - Ein Schwarm fliegender Mini-Hubschrauber
- ADABTS - Automatische Erkennung von abnormen Verhaltensweisen und Bedrohungen in überfüllten Räumen
- ACTIBIO - Unauffällige Authentifizierung unter Verwendung tätigkeitsbezogener und weicher biometrischer Daten
- AMASS - Autonomous Maritime Surveillance Systems
- SAMURAI - Suspicous and Abnormal behaviour Monitoring Using cameRas And Intelligence
- TALOS - Transportable Autonomous patrol for Land bOrder Surveillance

Snowden Enthüllungen

Über viele Jahre richtete sich der Protest von Bürgerrechtlern wegen der Einschränkung von Freiheitsrechten gegen die öffentliche Verwaltung und die Polizei. Die Arbeit der Geheimdienste war, da in der Regel geheim, mit wenigen Ausnahmen kaum ein Thema. Es wurde vermutet, dass im Bereich der Geheimdienste die gesetzlichen Beschränkungen oftmals übergangen wurden. Es fehlten jedoch die Beweise.

Auch deshalb sind die Enthüllungen von Edward Snowden im Juni 2013 ein wichtiger Meilenstein. Seine Veröffentlichungen über die Arbeit der US Geheimdienste, insbesondere die NSA, machte mit einem Schlag klar, dass praktisch jeder Mensch auf der Erde von diesen Diensten beobachtet wird.

Beispielhaft für diese Überwachung sind die folgenden Programme:

- PRISM = alles wird gespeichert
- XkeyScore = alles ist durchsuchbar
- TAO (Tailored access operation) = alle wichtigen Router (Bsp. Cisco) haben seit Jahren Hintertüren

Extra für die umfassende Speicherung der Daten von Milliarden Menschen wurde ein neuer NSA Standort im US Bundesstaat Utah gebaut (https://www.aktion-freiheitstattangst.org/de/articles/3921-20131014-stromschwankungen-in-ueberwachungszentrum.htm und https://www.aktion-freiheitstattangst.org/de/articles/4039-20131209-nsa-sumpf-trocken-legen.htm)

Trotzdem hat Bundeskanzlerin Merkel im Herbst 2013 noch gesagt:
„Es gibt keine massenhafte Überwachung“

Wir können uns gern darüber streiten, ob die Speicherung jeder sechsten Mail oder jedes sechsten Telefongespräches von jedem Menschen oder die totale Speicherung von aller Kommunikation von jedem sechsten Menschen als massenhaft zu bezeichnen ist. Klar ist jedoch geworden, dass damit über jeden Menschen ein Profil angelegt wurde, dass bei Bedarf Auskunft über seine Tätigkeiten, Vorlieben, Bewegungen, Gedanken möglich macht.

Erst als bekannt wurde, dass auch Behörden der EU, der deutsche Botschafter in der Türkei, und selbst das Handy der Kanzlerin abgehört wurden, nahmen die Abstreitversuche seitens der Bundesregierung ab. Im mehrjährigen NSA-Untersuchungsausschuss versuchte man stattdessen die Beteiligung des Bundesnachrichtendienstes (BND) an den Spionageprogrammen der USA herunterzuspielen.

Das Ergebnis der Arbeit des Untersuchungsausschusses brachte zwar einiges vorher Unbekanntes an das Tageslicht, er führte jedoch nicht zu einer Beschränkung der Befugnisse des BND oder der Zusammenarbeit mit den USA. Es wurde im Gegenteil ein BND Gesetz verabschiedet, welches verschärfend regelte, dass die Selektionslisten von NSA und BND der Geheimhaltung unterliegen, dass es keinen Quellenschutz für Journalisten zu Themen des Geheimdienstes gibt. Als Beruhigungspille

wurde der SPD dafür ein G-10 Gesetz-Beauftragter eingeführt, der den G-10 Ausschuss zukünftig lenken soll. (https://www.aktion-freiheitstattangst.org/de/articles/5741-20160921-petition-gegen-bnd-gesetz.htm)

Ist das Vorgehen der Geheimdienste (irgendwie) rechtmäßig?

- Die NSA darf in Deutschland spionieren, (nach US Recht)
- der BND darf in den USA spionieren (nach BRD Recht)
- dann werden die Daten (entgegen der nationalen Gesetze) ausgetauscht
- US-Dekret 12333: Eine automatische Sammlung (gathering) ist in den USA keine "Datensammlung".
- Hans-Jürgen Papier, bezeichnete die Auslandsaufklärung des BND als „insgesamt rechtswidrig“
- NSA-Ausschussmitglieder haben auf Herausgabe der Selektionslisten geklagt und verloren
- Die Reaktion der Bundesregierung im Sep. 2016: Ein BND Gesetz, welches regelt:
- BND-Selektorenlisten (Suchbegriffsliste) werden nach neuem Gesetz rechtmäßig,
- kein Quellenschutz für Journalistinnen,
- Einsetzen eines G10-Gesetz-Beauftragter, der den G10-Ausschuss lenkt, der aus 8 Bundestagsabgeordneten besteht, die über Geheimdienstaktivitäten informiert werden müssen/sollten.

Aktion Freiheit statt Angst trägt im Juni 2014 dem Whistleblower Edward Snowden als Dank für seine Enthüllungen die Ehrenmitgliedschaft in unserem Verein an. Er nimmt diese an. (https://www.aktion-freiheitstattangst.org/de/articles/5705-ehrenmitglied-edward-snowden.htm)

Cyberwar

"Cyberwar" I

Wir haben also durch die Enthüllungen von Edward Snowden gelernt, dass Geheimdienste und Militär weltweit weit jenseits aller rechtlichen Aufträge arbeiten. Wir formulieren deshalb folgende Vermutung:

Es gibt eine virtuelle Zusammenarbeit bzw. Duldung von Kriminellen durch den Staat

Dazu eine kleine Auswahl von Beispielen:

- Melissa Virus (Virus Schaden 80 Mil.$, 100.000 betroffene Rechner weltweit) Programmierer Dav Smith wurde gedrängt ab 1999 für das FBI tätig zu sein
- I Love You-Virus, (Mai 2000, 10 Mrd.$ Schaden weltweit, O. de Guzman aus Manila) nutzt Einträge aus dem persönlichen Adressbuch von Microsoft Outlook (Windows), und löscht zusätzlich Dateien auf dem PC
- Elliptic Curve Random Generator (Algorithmus zur Bestimmung von Zufallszahlen) wird 2007 vom National Institute of Standards and Technology (NIST) zum Standard definiert.
- Kurz nach Veröffentlichung durch das NIST wurden Vermutungen laut, der Algorithmus enthalte eine Hintertür, welche sich im September 2013 aus den Snowden Enthüllungen bewahrheitete.
- ECRG wird noch heute in der Verschlüsselung im Mobilfunk verwendet und ist in Sekunden knackbar!

Einige Beispiele, die nicht auf die USA zurückzuführen sind:

- Estland: April 2007 Bot-Netze verüben DDoS Angriffe auf staatliche PCs in Estland staatliche Organe, darunter das estnische Parlament, der Staatspräsident sowie diverse Ministerien, Banken und Medien wurden zeitweilig lahmgelegt.
  Die russische Regierung wurde als Verursacher vermutet.
- Litauen: Juli 2008 Bot-Netze verüben DDoS Angriffe auf staatliche PCs in Litauen, ähnliche Folgen wie in Estland

Und wieder Beispiele aus den USA:

- MHET (Mobile Handset Exploitation Team – NSA- Untergruppe) „verunsichert“ 2010/2011 SIM Karten-Hersteller, wie GEMALTO (u.a. Hersteller der eGK)
- MHET und GHCQ (Engl. Geheimdienst) sollten das Fundament der mobilen Kommunikation knacken (Snowden-Enthüllung, 2013)
- Stuxnet - Programm zur Steuerung von Urananreicherungszentrifugen im Iran bis zur deren Zerstörung, Juni 2010
- Im Juni 2013 klagt das US-Justizministerium General James E. Cartwright wegen Leaks an. Stuxnet-Projektleiter General James E. Cartwright, der 2.-höchste Militär der USA hatte nach Vermutung der Behörde Details zu Stuxnet in einem Interview mit der New York Times genannt, die schließlich zur Enttarnung des 50 Mio.$ teuren Sabotage-Programms führte.

„Cyberwar II“ - Drohnenkrieg

Die Zusammenarbeit von Militär und Geheimdiensten wird besonders im völkerrechtswidrigen Drohnenkrieg der USA deutlich. Während die Geheimdienste durch Aufzeichnung und Verfolgung von Telefongesprächen den Aufenthaltsort von Verdächtigen feststellen, schickt das Militär Kampfdrohnen zur Tötung (meist nicht nur) der Verdächtigen.

Verdächtige und auch viele Unbeteiligte werden getötet allein aufgrund von Daten von Geheimdiensten. Die Hinrichtung von Menschen ohne ihre Anhörung, die Möglichkeit einer Verteidigung, ein ordentliches Verfahren vor einem Richter widerspricht den Menschenrechten.

Darüber hinaus ist die Entwicklung von Kampfdrohen der Weg zu einer autonomen Waffentechnologie. Bereits heute können die Fluggeräte bei Ausfall der Funkverbindung selbstständig Entscheidungen treffen. So sind sie in der Regel programmiert in diesen Fällen zu ihrem Ausgangspunkt zurück zu fliegen. Aufgrund der fehlenden Funkverbindung weiß dort jedoch niemand ob sie in friedlicher Absicht kommen oder vom „Feind“ gehackt wurden.

Die folgende Liste zeigt, dass der Einsatz von Kampfdrohnen völkerrechtswidrig und zu verurteilen ist:

- illegal, Mord, Kriegsverbrechen → autonome Waffen
- senkt Schwelle zum Krieg, weltweites Kriegsgebiet
- schwerere Erkennbarkeit des wirklichen Täters
- „Chirugische Schläge“ sind eine Mär, durchschnittlich 28 Tote um eine „Zielperson“ zu töten (https://www.aktion-freiheitstattangst.org/de/articles/3661-20130612-obama-wegen-kriegsverbrechen-gesucht.htm und https://www.aktion-freiheitstattangst.org/de/articles/5647-20160707-ungestraft-ueber-100-unbeteiligte-ermordet.htm und https://www.aktion-freiheitstattangst.org/de/articles/5754-20160930-internationaler-drohnenangriff-toetet-15-zivilisten.htm)
- hebelt Gewaltenteilung aus (Anklage, Verteidigung, Richter, Urteil)
- Völkerrecht wird verletzt, Haager Landkriegsordnung (Krieg gegen Zivilisten)
- Macht projizieren, ohne Verwundbarkeit zu erlauben
- Gefahr automatisierter Kriege

Leider hat sich der Bundestag im Juni 2018 für die Beschaffung von sechs israelischen Kampfdrohnen entschieden, nachdem ein entsprechender Beschluss im Jahr davor noch abgelehnt wurde. (https://www.aktion-freiheitstattangst.org/de/articles/6513-20180611-kampfdrohnen-beschaffung-verhindern.htm) Obwohl bereits mit bewaffneten Drohnen geübt wird, gibt es in dem Bundestagsbeschluss noch die Einschränkung, dass vor der Nutzung der Waffen eine ethische Diskussion, bzw Anhörung durchzuführen sei. Die Vereinbarung mit der Wartungsfirma Airbus sieht jedoch bereits wöchentliche Übungen mit Waffen auf harte und

weiche Ziele (Menschen) vor. (https://www.aktion-freiheitstattangst.org/de/articles/6684-20181110-bundeswehr-drohnen-sollen-mit-waffen-ueben.htm)

Vor der Gefahr "autonomer Kriege" warnt auch ein Beispiel (https://www.aktion-freiheitstattangst.org/de/articles/5789-20161102-kuenstliche-intelligenz-erfindet-eigene-verschluesselung.htm) von Google. Deren Forschungslabore hatten 2 KI Instanzen Verschlüsselung lernen lassen. Nach 15.000 Versuchen konnten sich die Programme verschlüsselte Nachrichten schicken, die eine 3. Instanz nicht entschlüsseln konnte (und auch die menschlichen Programmierer nicht).

Welche Gefahr automatisierte Drohnen darstellen können, zeigt auch der Film über Slaughterbots, kleine Drohnen mit „kleinen“ Sprengsätzen, die massenhaft gegen bestimmte Personengruppen einsetzbar sind. (https://www.aktion-freiheitstattangst.org/de/articles/6259-20171118-keine-drohnen-kein-einstieg-in-automatisierte-kriege.htm und https://www.youtube.com/watch?v=9CO6M2HsoIA)

"Cyberwar III" - Datenleaks

Datenleaks werden allgemein zur Cyberkriminalität gezählt, obwohl sie eigentlich kriminelle Aktivitäten aufdecken!

Einige Beispiele:

- Irak-Leak durch Manning, 2010 (veröffentlicht auf Wikileaks, dank Julian Assange)
- Snowden-Enthüllungen, 2013
- Panama Papers durch Zeitungsredaktionen, 2016
- Shadow Brokers Leak: Im Sommer 2016 entlarven sie Softwaremanipulation des Equation Teams (Untergruppe der NSA) und bestätigen, dass bei den Netzwerkherstellern seit Jahren Hintertüren in Geräte und Software eingebaut wurden.

Durch diese Leaks wurden Verbrechen offen gelegt !
Es erfolgt jedoch keine Bestrafung der Verantwortlichen - sondern deren Aufdecker !

"Cyberwar IV" – Datenpannen

„Datenpannen passieren einfach“. Ursache sind Softwarefehler, gelangweilte oder gestresste Administratoren. Bei diesen Datenpanne nehmen wir an, dass keine böse Absicht vorlag, es war nur ein Fehler eines Programmierers, eines Administrators und schon geraten Millionen unserer Daten in falsche Hände. Hier ein paar Beispiele (von insgesamt einigen Hundert, die wir schon auf unseren Webseiten dokumentiert haben):

- Juni 2015 WDR: Massive Datenschutz-Lücke bei Patientendaten, der eGK (elektronische Gesundheitskarte)
- Aug 2015: Hacker steuern Hightech-Scharfschützengewehr eines US-Waffenherstellers aus der Ferne (https://www.aktion-freiheitstattangst.org/de/articles/5093-20150806-ferngesteuertes-gewehr-ferngesteuert.htm)
- Nov 2015: Daten von 19 Millionen ADAC-Mitgliedern sind im Netz lesbar
- Dez 2015: BVG E-Tickets speichern Bewegungsdaten der Berliner Nutzer
- März 2016: 20 Autotypen mit Komfort-Schlüssel waren sehr leicht zu knacken (ADAC)
- Aug 2016: 60 Millionen Dropbox Nutzer gehackt

- Sep 2016: Yahoo meldet die Daten von 500 Millionen Accounts gestohlen, real waren es über 1 Milliarde.
- Verschlüsselung im deutschen DE-Mail-Dienst ist bis heute unsicher
- DE-Mail bringt nur Verluste, anfangs musste die Post 5€/Mail draufzahlen. Die jetzt eingeführte gute Ende-zu-Ende-Verschlüsselung mit PGP macht den ganzen Dienst völlig überflüssig.
- Windows10 „telefoniert“ in 8h 5500-mal „nach Hause“

Das Bundesamt für die Sicherheit in der Informationstechnik warnt vor der Nutzung von Windows 10. Windows XP als ehemals verlässliches Betriebssystem wird von Microsoft nicht mehr unterstützt. So bleibt als letzte Alternative, wenn man denn Windows unbedingt braucht nur Windows 7. Window 8 hat eine unmögliche Oberfläche und Windows 10 siehe oben. ;-))

Das US-Militär weiß das wohl auch, denn die US Atom-U-Boote laufen weiter unter Windows XP. Dafür gibt es extra einen Support-Vertrag mit Microsoft. (https://www.aktion-freiheitstattangst.org/de/articles/5367-20160125-atomkrieg-weiter-mit-windowsxp.htm)

Diverse weitere Pannen auf unserer Webseite sind unter diesem Link zu finden: https://www.aktion-freiheitstattangst.org/cgi-bin/searchart.pl?suche=panne&sel=meta

"Cyberwar V" - Fazit

- Staaten bauen Hintertüren (Backdoors) ein und machen dadurch Systeme angreifbar für Jeden!
- Staaten bauen unsichere Verschlüsselungssysteme.
- Staaten verbieten sichere Systeme bzw. deren Export. *)
- Das Ergebnis sind unzählige Hacks und Datenpannen.
- Wenn Staaten an solchen Aktivitäten beteiligt sind, ist das Teil des Cyberwars und kann zu ernsten kriegerischen Auseinandersetzungen führen!
- Der Bau und das Zulassen unsicherer Systeme gefährdet den Frieden und in jedem Fall die Funktion unseres Gemeinwesens.

*) In Frankreich war bis in die 90-er Jahre Verschlüsselung verboten. Durch die EU-Datenschutzrichtlinie war dies nicht mehr möglich.

Machen wir es noch einmal mit einem realen Beispiel deutlich:

> Eine britische Zeitung hat die 15.000 Worte aufgelistet, bei deren Erscheinen in E-Mails oder am Telefon die Programme der Geheimdienste Alarm schlagen. Das wäre eine der so geheimen Selektionslisten, die selbst die Mitglieder im NSA Untersuchungsausschuss nicht zu sehen bekommen sollten.

Der normale Wortschatz in der Umgangssprache liegt bei 5000-7000 Worten. Wenn man Dampfdruckkochtopf, Grippe, Brücke, Bombe, ... vermeidet, bleibt von einer normalen Unterhaltung nicht viel übrig. (https://www.aktion-freiheitstattangst.org/de/articles/3778-20130805-ich-habe-doch-nur-einen-kochtopf-zu-verbergen.htm)

Zensurbestrebungen - Gefahren für die Informationsfreiheit

Schon seit einigen Jahren nennen sich die Datenschutzbeauftragten Beauftragte für Datenschutz **und** Informationsfreiheit, denn beides gehört zusammen. Aus diesem Grund wollen wir auch kurz auf Bestrebungen „des Staates“ eingehen, unsere Informationsfreiheit einzuschränken.

Ein Beispiel:

Innenminister De Maizière macht vor Weihnachten 2016 (https://www.aktion-freiheitstattangst.org/de/articles/1204-gtaz.htm) einen Vorschlag für ein Abwehrzentrum gegen Desinformation. Er will dieses Orwellsche Wahrheitsministerium beim Kanzleramt einrichten.
Als Grund nennt er: *Diverse Falschmeldungen und Hass-Sprache „Hate Speech“ im Internet, die via sozialen Netzwerken verbreitet werden und die kommenden „Wahlen beeinflussen könnten“.*

Er übersieht damit absichtlich das Problem:

- Reglementierende Eingriffe und Zensur-Gefahren drohen, denn:
- Was ist eine Falschmeldung? (Journalismus, Meinungsäußerungen, Satire, ...)
- Eingriffe in die freie Meinungsäußerung und Pressefreiheit drohen!
- Die Regierung macht sich zum Richter, auch über jede Opposition!
- Das Internet wird bereits durch vorhandene Gesetze geregelt, es ist kein rechtsfreier Raum!
- Wir brauchen keine weitere bürokratische Behörde!
- Es existieren ausreichend Straftatbestände für Beleidigungen, Verunglimpfungen etc...
- Für den Umgang mit Hate-Speech im privaten Bereich gibt es Hilfe z.B. auf der österreichischen Webseite von Zara http://zara-training.at/

Datenschutz und Informationsfreiheit gehören zusammen

- Privatsphäre des Einzelnen ist ein fundamentales Grundrecht - rechtlich spätestens seit dem Volkszählungsurteil von 1983
- Grundsatz sollte sein: Persönliche Daten schützen - Öffentliche Daten nützen!
- Datenschutz ist nicht alles - Informationsfreiheit gehört dazu!
- Beispiel "Initiative Transparente Zivilgesellschaft"
  will Behörden, Vereine, Wirtschaft zu freiwilliger Offenheit über ihre Daten bewegen
  https://www.transparency.de/Initiative-Transparente-Zivilg.1612.0.html
- Wer die Initiative unterstützen will muss 10 Informationen über seine Organisation auf seine Webseite angeben?
  https://www.transparency.de/Zehn-Informationen.1613.0.html

Initiative Transparente Zivilgesellschaft

- Die Initiative zeigt auf, was für Vereine eine Selbstverständlichkeit sein sollte,

Behörden sind da schwerfälliger und die Wirtschaft ist offensichtlich unwilliger

- Die aufgedeckten/gesammelten Daten sind wichtig für Möglichkeiten und Tätigkeiten zur Korruptionsaufdeckung
  https://www.transparency.de/Global-Corruption-Report.2169.0.html

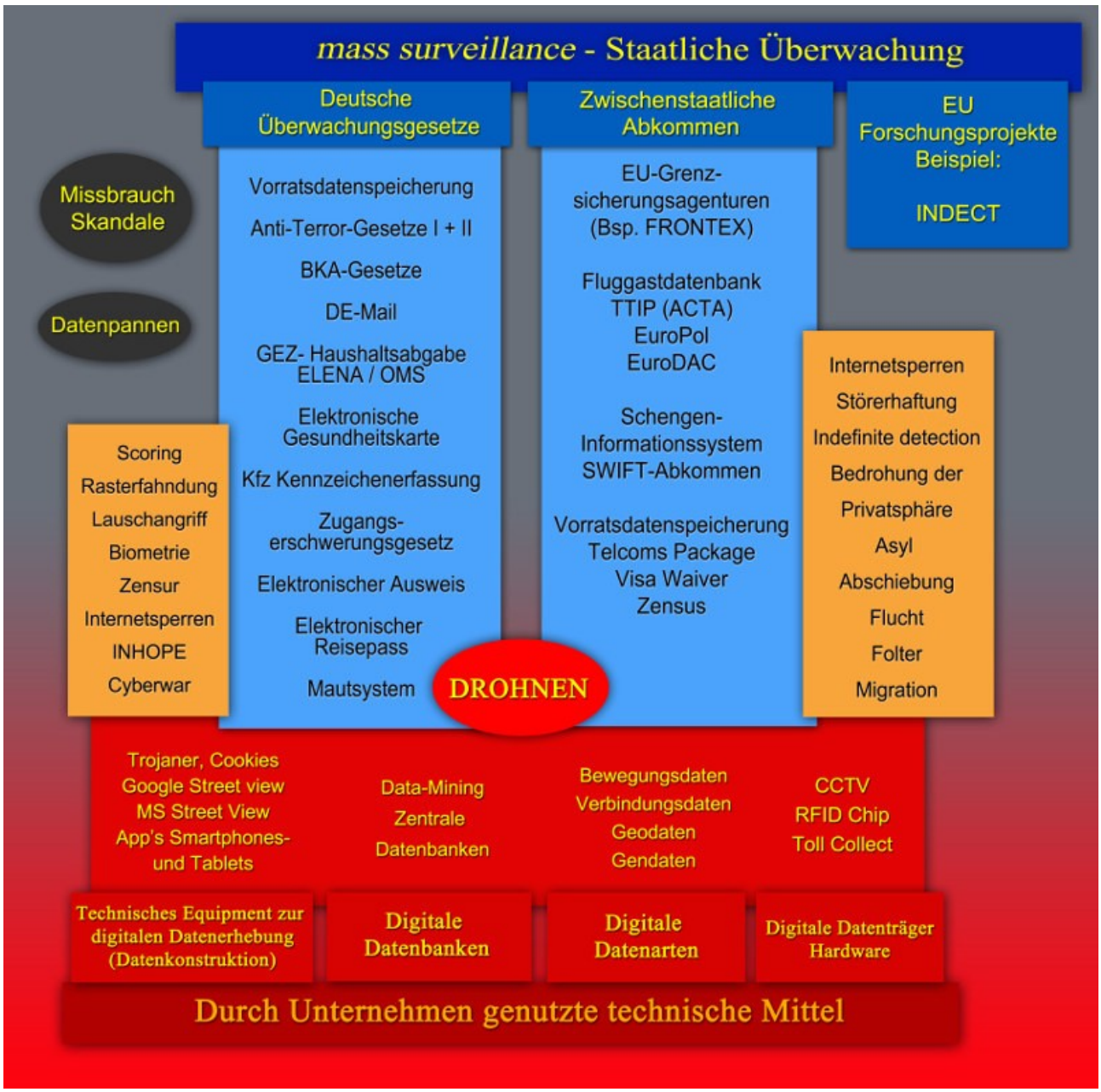
Fazit

Themenbaum Überwachung durch "den Staat"

Als Hilfe, um den Weg durch den Dschungel der Gefahren für unsere Freiheitsrechte zu finden, haben wir drei Themenbäume in unserem Web dargestellt. Wir haben sie in folgende Bereiche aufgeteilt

- Menschenrechte und Grundrechte
- Überwachung „durch den Staat“
- Überwachung durch Unternehmen

Hier ein Blick auf den Themenbaum Überwachung durch "den Staat" (https://www.aktion-freiheitstattangst.org/de/themenbaum.htm)



Alle aufgeführten Begriffe sind im Web mit Links zu Artikeln dazu hinterlegt. Allerdings sind diese Links einem gewissen Alterungsprozess unterworfen und evtl. nicht immer aktuell. In solchen Fälle hilft die Suchfunktion.

Was kann man selbst tun?

- Eigenverantwortung beim Umgang mit seinen Daten
- Verantwortung gegenüber Freunden und Anderen!
- Datensparsamkeit – Datenvermeidung
- Einhaltung der Zweckbindung

Wie kann man das erreichen?

Man sollte bei der Auswahl seiner Software kritisch sein. Nicht immer ist das kostenlose Programm das günstigste. Aber es gibt Offene Software (Open Source), die quelloffen vorliegt. In solchen Programmen haben Hunderte und manchmal sogar Tausende von Entwicklern über den Code geschaut und kontrolliert, dass keine Hintertüren eingebaut sind und die Daten nur zu den wirklichen Zwecken des Programms genutzt werden.

Wir schlagen also vor

- Open Source statt Kommerz d.h.:
  - Mozilla Firefox, opera, ... statt M$ Explorer
  - Mozilla Thunderbird statt Outlook
  - Mail-Postfach z.B. bei Posteo.de, mailbox.org
  - statt bei Google, Yahoo, Microsoft, iCloud, web.de, gmx
- Gegen Malware und „neugierige Skripte“
  - schützende Plug-Ins im Browser verwenden,
  - z.B. noScript gegen Java, Ghostery, AdBlockPlus, ...
- Alternative Soziale Netzwerke nutzen
  - Diaspora, Telegram, Threema, Signal - statt Facebook & Twitter
- Firewall installieren
  - möglichst wenige Verbindungen erlauben, ca. 5-10 statt 65.000
- Verschlüsselung nutzen:
- beim Surfen https statt http nutzen,
- Tor Browser nutzen (der über verschiedene Hops geht und die eigene Identität verschleiern kann)
- Mail mit pgp signieren und verschlüsseln (mit dem Plug-In Enigmail)
- Plug-In Mailvelope nutzen, wenn man Mails unbedingt im Browser lesen muss
- Bitmessage als Alternative zu normaler Mail verwenden (erzeugt keine Metadaten und kommt ohne Mail-Provider aus)
- eigene Daten verschlüsselt & getrennt von den Programmen abspeichern/aufbewahren

Falsche „Argumente“

Für die anschließende Diskusson haben wir ein paar "Totschlagargumente" zur Einstimmung mitgebracht:

Ich habe nichts zu verbergen	Doch, deine Privatsphäre, dein Leben! nichts-zu-verbergen.de/
So viele Daten können die gar nicht auswerten.	Falsch! Je mehr Daten, desto differenzierter das Bild von dir!
Ich bin doch gar nicht interessant, wer sollte MICH überwachen?	Alle und jeder wird grundsätzlich überwacht.
Wenn ich verschlüssele, dann bin erst recht verdächtig!	Alle und jeder wird grundsätzlich verdächtigt.
Die hacken eh alles.	Falsch! Hacken kostet Zeit. Mit einem guten 12 Zeichen-Passwort ist man relativ sicher.

Wir danken den Whistleblowern Edward Snowden, Julian Assange, Chelsea Manning, William Binney, Jakob Applebaum, Brandon Bryant, Cian Westmoreland, ...

Linksammlung

Staatliche Überwachung

Bestandsdatenauskunft https://www.aktion-freiheitstattangst.org/de/articles/3534-20130415-bestandsdaten-ausser-kontrolle.htm

Bevölkerungsregister https://www.aktion-freiheitstattangst.org/de/articles/5856-20161226-auf-dem-weg-zu-einem-bevoelkerungsregister.htm

Biometrische Daten in Pass und ePerso, 2010 https://www.aktion-freiheitstattangst.org/de/articles/1203-biometrie.htm

Biometrie, Hack des ePerso https://www.aktion-freiheitstattangst.org/de/articles/1501-20100826-pressemitteilung-zum-hack-des-elektronischen-personalausweis.htm

BKA Gesetz, Nov. 2008 https://www.aktion-freiheitstattangst.org/de/articles/97-20090206-bka-gesetz.htm

Urteil zur **Rasterfahndung** https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html

GTAZ https://www.aktion-freiheitstattangst.org/de/articles/1204-gtaz.htm

PNR: https://www.aktion-freiheitstattangst.org/de/articles/5304-20151209-keine-vorratsspeicherung-unserer-flugreisedaten.htm

PNR, Bruse Schneier http://www.schneier.com/essay-052.html

PNR, Edward Hasbrouck https://hasbrouck.org/articles/PNR.html

VDS: https://www.aktion-freiheitstattangst.org/de/articles/1329-20100514-gegen-die-eu-richtlinie-zur-vorratsdatenspeicherung.htm

https://www.aktion-freiheitstattangst.org/de/articles/1279-20100419-keine-neue-vorratsdatenspeicherung.htm

Steuer-ID https://www.aktion-freiheitstattangst.org/de/articles/1541-20100915-steuer-id-wird-zum-eindeutigen-schluessel.htm

Zensus 2011 https://www.aktion-freiheitstattangst.org/de/articles/1895-20110218-zensus-2011-schon-wieder-eine-volkszaehlung.htm

EU-Forschung

https://www.aktion-freiheitstattangst.org/de/articles/659-20091009-interessante-zusammenfassung-zum-fp7-sicherheitsforschung-in-der-eu.htm

http://www.iq-wireless.com/en/r-and-d-service/amass-automatic-system-for-surveillance-of-the-blue-border

http://imi-online.de/download/SL-JW-EUSicherheitsforschung-AusdruckFeb2010.pdf

http://www.iq-wireless.com/en/r-and-d-service/amass-automatic-system-for-surveillance-of-the-blue-border

https://stop-orwell2020.org

INDECT u. EU-Forschung https://www.aktion-freiheitstattangst.org/de/articles/1917-indect.htm

Erich Möchel der Staat als Krimineller https://media.ccc.de/v/fiffkon16-4003-cyber_der_staat_als_krimineller_/download

Liste Ueberwachungsgesetze https://www.aktion-freiheitstattangst.org/de/articles/1892-ueberwachungsgesetze.htm

BDSG Text: https://www.gesetze-im-internet.de/bdsg_1990/

Erläuterungen: https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz

EU DS-GVO http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

59. Konferenz der DSB vom 14./15. März 2000, Data Warehouse, Data Mining und Datenschutz

https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/59DSK-DataWarehouse_DataMiningUndDatenschutz.pdf

"Initiative Transparente Zivilgesellschaft" https://www.transparency.de/Initiative-Transparente-Zivilg.1612.0.html

Nichts zu verbergen http://www.nichts-zu-verbergen.de/

Hacks

I love You https://de.wikipedia.org/wiki/ILOVEYOU

Stuxnet https://de.wikipedia.org/wiki/Stuxnet

Ellip.Curve Random Generator 2007 NIST Standard

http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115

Estland, April 2007 https://de.wikipedia.org/wiki/Internetangriffe_auf_Estland_2007

Litauen, Juli 2008 http://www.zdnet.com/article/300-lithuanian-sites-hacked-by-russian-hackers/

MHET, 2011 http://www.heise.de/newsticker/meldung/Geheimdienste-unterwandern-SIM-und-Kreditkarten-2555685.html

Shadow Brokers Leak, Sommer 2016

http://www.spiegel.de/netzwelt/web/shadow-brokers-cisco-und-fortinet-bestaetigen-sicherheitsluecken-a-1108277.html

http://thehackernews.com/2016/08/nsa-hack-russia-leak.html

http://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html

Manning Collateral Murder Video, 2010 http://www.zeit.de/1999/15/199915.36_bulk.xml

Snowden Veröffentlichungen, Juni 2013

https://www.aktion-freiheitstattangst.org/de/articles/3885-20131001-was-ist-neu-an-prism-tempora.htm

Liste Datenpannen https://www.aktion-freiheitstattangst.org/cgi-bin/searchart.pl?suche=panne&sel=meta

Gefahren durch Drohnen https://www.aktion-freiheitstattangst.org/de/articles/3310-20121215-drohnen-die-unsichtbare-gefahr.htm

Arbeitnehmerdatenschutz

Historie - Arbeitnehmerdatenschutzgesetz https://www.aktion-freiheitstattangst.org/de/articles/903-historie-arbeitnehmerdatenschutzgesetz.htm

Gefeuert, weil sie App löschte https://www.aktion-freiheitstattangst.org/de/articles/4949-20150514-frau-gefeuert-weil-sie-ueberwachungs-app-loeschte.htm

Verbraucherdatenschutz

eGK https://www.aktion-freiheitstattangst.org/de/articles/571-20090906-verbraucherdatenschutz.htm#egk

ELENA https://www.aktion-freiheitstattangst.org/de/articles/571-20090906-verbraucherdatenschutz.htm#elena

Gläserner Bürger https://www.aktion-freiheitstattangst.org/de/articles/571-20090906-verbraucherdatenschutz.htm#glas

Software-Ergonomie https://www.aktion-freiheitstattangst.org/de/articles/860-softwareergonomie.htm

„Nutzen“ von sozialen Netzwerken http://www.matthes-seitz-berlin.de/buch/facebook-gesellschaft.html

Steuerung durch soziale Netzwerke https://www.aktion-freiheitstattangst.org/de/articles/5839-20161212-online-manipulation-von-waehlern.htm

Smart-TV https://www.aktion-freiheitstattangst.org/de/articles/4777-20150210-vom-fernseher-zu-hause-ausspioniert.htm

Zensur

https://www.transparency.de/Initiative-Transparente-Zivilg.1612.0.html

Hate-Speech bei Zara Österreich

http://zara-training.at/