„Daten sind wie Atome - zuviele auf einem Haufen und es wird kritisch“

Andrea 'Princess' Wardzichowski
Chaos Computer Club Stuttgart e.V.

Vortrag für die Ringvorlesung „Open Society – Open Science“
an der Hochschule der Medien, Stuttgart

http://www.cccs.de/
princess@cccs.de

Ich freue mich sehr über die Einladung zur Ringvorlesung, bedauere aber ein wenig, dass wir uns heute per Videokonferenz treffen müssen anstatt in der Hochschule selber. Corona hat unser aller Leben beeinflusst – und auch diesen Vortrag.

Nach aktueller Lage habe ich die ursprüngliche Variante des Vortrags etwas gekürzt um dem Thema „Corona und Datenschutz“ mehr Raum zu geben. Die im Vortrag nicht gezeigten Folien befinden sich aber in diesem PDF.

Mein Vortrag beginnt mit meinem Nickname. Nur durch dessen (Mit-)Verwendung kann ich andeuten, daß ich privat unterwegs bin.

Über den CCCS / über mich

Über den CCCS:

Seit Sommer 2001 Treffen
Seit Oktober 2003/4 monatliche Vortragsreihe
Spaß am Gerät, aber auch Gefahren beim bedenkenlosen Einsatz von Technik

Über mich:

Seit November 1990 im Netz aktiv
(Mail, News, IRC, Relay Parties, CCC)
Heute: CCCS e.V. (Presse), Haecksen, querulantin.de, Herbstakademie der Alumni der dt. Studienstiftung 2019, XPDays Germany 2019

In vielen großen und inzwischen auch in vielen kleinen Städten gibt es sog. Chaostreffs, die im Sinne des CCC e.V. agieren, der 1986 in Hamburg gegründet wurde.

Ich selber bin auch schon sehr lange im Netz unterwegs und habe meine Homepage aufgebaut, damit man meine aktuellen Veröffentlichungen und Vorträge eher findet, als meine Jugendsünden aus Usenet-Zeiten.

Desweiteren pflege ich selber eine gewisse Paranoia und man findet hoffentlich nur wenige Bilder im Netz, dafür aber meine Veröffentlichungen, nicht jedoch Telefonnummern und meine Wohnadresse.

Man möchte weder, daß die eigenen „Fans“, noch die Menschen, die einen nicht mögen ungefragt vor der eigenen Haustür auftauchen.

Daher drehen sich die meisten meiner Vorträge um den **Datenschutz**, aber auch andere Themen sind spannend!

Agenda

- Öffentliche und personenbezogene Daten
- Datensammlung aller Art und Datenschutzgesetze
- Internet & Smartphone
- Wo wird es kritisch und warum?
  Gesundheitsdaten!
  Risiken bei der ePA
- Corona und der Datenschutz

Heute wird es in der Hauptsache um personenbezogene Daten gehen.

Welche Speicherungen kann ich vermeiden, welche nicht?

Und an welchen Stellen schützt mich das Datenschutzgesetz bzw. die EU-DSGVO?

Was sind die Konsequenzen, wenn Daten von mir ohne meine Zustimmung veröffentlicht werden?

Was hat es für Konsequenzen, wenn es sich hier um Gesundheitsdaten handelt?

Was ist mit der geplanten elektronischen Patientenakte (ePA)?

Welche Herausforderungen an den Datenschutz hat uns die Pandemie beschert?

Öffentliche und personenbezogene Daten

**„Öffentliche Daten nützen -
private Daten schützen“**

(Grundprinzip beim CCC)

- Bisherige Vorträge dieser Reihe: offene Forschungsdaten, Open Access
- Forderung (u.a.) des CCC:
  Software in öffentlichen Projekten (Steuernfinanziert!) als Open Source herausgeben (Transparenz, Code Review, Minimierung von Hintertüren und Sicherheitslücken)
- ….bei personenbezogenen Daten allerdings ist „Schluß mit lustig“

Der CCC setzt sich schon lange dafür ein, dass öffentliche Daten zugänglich sein sollten, ebenso sollte der Programmiercode von öffentlichen Projekten der Allgemeinheit zur Verfügung stehen. Diese hat sie schließlich mit ihren Steuergeldern bezahlt.

Für personenbezogene Daten aber gilt: bei Aufbewahrung und Transfer muß mit größtmöglicher Sorgfalt vorgegangen werden.

Computer und Computernetzwerke haben die Verwaltung und Zugreifbarkeit von Daten deutlich erleichert, bergen aber auch die Gefahr, dass Daten unbemerkt verändert oder gestohlen werden können.

Datensammlung per Gesetz

- **Einwohnermeldeamt**
- **Pass, Personalausweis** (RFID, Biometrie) (beim neuen ePerso sind die Fingerabdrücke ab 2021 nicht mehr optional)
- **Rundfunkbeitrag** (früher: GEZ), heute pro Haushalt, nicht nach Geräten erhoben, Meldeämter geben Daten weiter (Passus im Meldegesetz)
- **Krankenkasse** (Pflicht, auch wenn sich nicht jeder den Wiedereintritt leisten kann!)

Wenn man in Deutschland lebt, kommt man nicht darum herum, einige seiner **Daten von Gesetzes wegen abzugeben**. Ich habe zu diesem Zweck auch einmal das Meldegesetz gelesen. Das Lesen von Gesetzestexten ist für Nichtjuristen zugegebenermaßen schmerzhaft, aber für eine CCCS Referentin gelegentlich notwendig ;-)
Die Einwohnermeldeämter geben auch Daten an Mammographie-Praxen weiter, diese Praxis sollte hinterfragt werden (in meinem ToDo….)

Zwischenfrage: muß man einen Ausweis mit sich tragen?
Nein! Man muß nur Perso oder Paß besitzen, der darf aber zuhause liegen. Aus praktischen Erwägungen ist es aber besser, ihn bei sich zu haben.

Der **Rundfunkbeitrag** wird nunmehr pro Haushalt erhoben, es gibt meines Wissens fast keine Möglichkeit, diesen nicht zu entrichten. Es gibt einen Vorteil des Systems: die „Klinkenputzer“, die Nichtzahler zuhause aufgespürt haben, wurden von den Sendeanstalten entlassen. Hier gab es immer wieder abendfüllende Zwischenfälle am Rande der Legalität.

Inzwischen herrscht auch **Krankenkassenpflicht.** Die Krankenkasse hält besonders **intime und heikle Daten** vor. Daher muß man auch die Entwicklung der neuen **Krankenkassenkarte und elektronischen Patientenakte** sehr genau beobachten. Geht hier die Sicherheit flöten, ist der Zugriff und vielleicht auch die **Änderung von Gesundheitsdaten möglich!** Das Bild alleine auf der neuen eGK hilft übrigens gegen fast nichts, das war nur eine teure Aktion und wird den Mißbrauch nicht eindämmen. Als besonders gefährlich werden **Smartphone-Apps der Krankenkassen** erachtet.Das Smartphone ist kein sicheres Gerät.

Datenabgaben, denen man kaum entkommt

- **Bank** (Schufa und ähnliche)
- **Telekommunikationsanbieter** (Festnetz, mobil)
- **Videoüberwachung** (ÖPNV, Verkehrskameras)

Nicht zwingend notwendig, aber bequem:

- Versandhandel
- Rabattsysteme (Bahncardpunkte, Payback, ..)

Auch beim surfen hinterlassen wir Spuren!

Ob Erwerbseinkommen oder Sozialleistungen, Rente, Unterhalt: ohne ein **Konto bei einer Bank** kommt man heute idR. nicht aus. Die Bank weiß viel: sie weiß wo das Geld herkommt, und sie weiß, wo es hingeht.

Ich rate dazu, **Kartenzahlungen** (EC-, Kredit-, Geld-) zu **vermeiden**. Jede Kartenzahlung verursacht eine Datenspur. Die Bank sieht wo und wann Einkäufe getätigt wurden.

Weiterhin ist es heute ziemlich unmöglich, keinerlei **Telefon** zu haben. Der Telekommunikationsanbieter kennt, zumindest für einen gewissen Zeitraum, alle **Kommunikationspartner**. Im Falle von Mobilfunk auch den Sendemast, an dem ein Mobiltelefon eingebucht ist. Zumindest **grobe Lokalisierung** wäre so möglich.

Nicht entkommen kann man der allgegenwärtigen **Videoüberwachung**. Man kann aber bei allen speichernden Stellen **Auskunft verlangen**, wie lange die

Aufzeichnungen gespeichert werden. Wenige Tage sind zur Aufklärung von Sachbeschädigung und Belästigung in öffentlichen Fahrzeugen vertretbar. Ist hingegen nichts vorgefallen, sollten die Aufnahmen auch zeitnah gelöscht werden. Trauen Sie sich, fragen Sie nach!

Das Leben leichter macht in vielen Fällen der boomende **Versandhandel.** Hier lassen sich aber aus den bestellten Artikeln auch Verhaltensprofile erstellen. Bei **Amazon** kann man aber z.B. einstellen, daß möglichst wenig gespeichert wird.

Datenschutzgesetz

- Bundesdatenschutzgesetz, seit Mai 2018: EU-DSGVO
- Landesdatenschutzgesetze
- Angepasste Datenschutzgesetze
- Zweckbindung bei der Datenerhebung
- Datensparsamkeit
- Datenschutzbeauftragter (Bundes-, Landes-, Firmen, KK, öffentliche Stellen, Schulen, Hochschulen...)

=> **Volkszählungsurteil**, Informationsfreiheitsgesetz, Transparenz bei der Verarbeitung von **personenbezogenen Daten**

Hier in der Bundesrepublik Deutschland gilt so gut wie überall eines der **Datenschutzgesetze**, die **personenbezogene Daten**, deren Speicherung und Verarbeitung, schützen. Seit Mai 2018 haben wir europaweit hohe Standards.

Grundsätze sind hierbei immer eine **Zweckbindung** bei der Erhebung von Daten (sie dürfen nicht anlaßlos erhoben werden), sowie die **Datensparsamkeit** (es dürfen nur die Daten erhoben werden, die für einen Zweck auch notwendig sind).

Jede Stelle, die personenbezogene Daten speichert, muß einmal im Jahr **kostenlos Auskunft** darüber geben, welche Daten sie gespeichert hat (auch die Schufa! Die verlangen ganz frech trotzdem Gebühren).

Allerdings nimmt nicht jede Stelle und nicht jede Firma es so genau mit dem Datenschutz: gelegentlich muß man einmal **nachfragen**, ob alles mit rechten Dingen zugeht, notfalls auch öfter als einmal. **Verstöße** können beim Landes- und Bundesdatenschutzbeauftragten gemeldet werden! (Habe dies auch schon gemacht!)

Firmen und öffentliche Stellen müssen zudem einen eigenen Datenschutzbeauftragen bestellen, der für Anfragen dieser Art zur Verfügung stehen muss!

Was aber ist mit Firmen, die ihren Hauptsitz und ihre **Server und Speicher nicht in Deutschland** stehen haben? Hier ist Vorsicht geboten!

Freiwillige Datensammlungen / Internet

- Webseite
- Blog
- Teilnahme an Foren (früher News/Usenet), Leserbriefe
- Social Media (facebook, instagram, tiktok, twitter, Xing, whatsapp)
  hier auch: Verbreitung von Fotos!
- Wunschliste bei Amazon....
- Webseiten von (Sport-)Vereinen
- Nicht unterschätzen: social hacking

Völlig freiwillig ist hingegen die **aktive Teilnahme** am Internet. Wer nur Webseiten sichtet und private E-Mails schreibt, hinterläßt zwar auch an vielen Stellen **Datenspuren**, die wenigsten davon sind aber öffentlich.

Wer **aktiv Inhalte ins Netz stellt**, diskutiert oder Fotos veröffentlicht, sollte sich überlegen, ob er/sie dies mit seinem **richtigen Namen** tun will und wieviel davon **die Welt** wirklich wissen muss.
Denkfalle ist oft, daß man das nur „für Freunde und Familie“ schreibt/veröffentlicht. In Wahrheit sind viele Dinge, auch aus sozialen Netzwerken, für die Welt lesbar.

Denkanstoß: Nehmen Sie ein Stück alte Tapete und kreieren Sie darauf Ihre „Homepage“ und lassen Sie dies auch Ihre Kinder tun. Danach meditieren Sie gemeinsam darüber, ob Sie das Werk im Hausflur eines Mietshauses, auf der Straße vor dem Haus oder an der Bushaltestelle für alle sichtbar aufhängen würden, mit der Folge, daß JEDER, Freund und Feind, die Infos lesen kann. Auch: **welche Schlüsse** auf den Geschmack und die Vorlieben könnte jemand aus der Amazon Wunschliste ziehen?

Unterschätzt wird die Gefahr bei **Webseiten von Sportvereinen**. Während Schulen inzwischen gelernt haben, keine erkennbaren Fotos und Namen zu veröffentlichen, sind Kinder über Ihre Sportvereine oft **leicht find- und stalkbar.** Denn: Die Vereine freuen sich ja, wenn jemand an Wettbewerben teilnimmt etc.pp. Klären Sie auf!

Social hacking: aushorchen des Gesprächspartners durch lockere Plauderei. Buchtip: die Trilogie von Stieg Larsson.

Internet & Smartphone

- Durchdringen heute unsere Welt und das reale Leben
- Das Internet hat Zugang zu Wissen unglaublich erleichtert
- Eine Telefonzelle und Internet mit sich zu tragen ist superpraktisch
- Durch Stalker digital aufgespürt werden eher nicht
- Am Rande: es gibt auch Suchtgefahren
- Und: will ich mein ganzes Leben EINEM Gerät anvertrauen?

Das Smartphone hat den Zugang zum Internet noch einmal radikal erleichtert.

Inzwischen birgt es allerdings auch die Gefahr, durch „Apps für alle Lebenslagen“ zum ausgelagerten Gehirn zu werden.
Was passiert, wenn ich es verliere oder es kaputtgeht? Kaum jemand hat noch Telefonnummern im Kopf. Backup und Updates scheinen bei einem so wichtigen Gerät geboten, werden aber von normalen Nutzern kaum im erforderlichen Maße durchgeführt.

Normalerweise würde ich jetzt auch ins Publikum fragen, wer noch Telefonnummern auswendig kann ;-)

Zu den Suchtgefahren: „Muß man immer mal hingucken“. Beschreibung einer 3jährigen für „Smartphone“.

Wo wird es kritisch und warum?

- Wo ich freiwillig personenbezogene Daten abgebe, schützt mich kein Datenschutzgesetz
- Werde ich aber gezwungen, personenbezogene Daten von Dritten verarbeiten zu lassen (Meldegesetz, ePA) muß ich mich darauf verlassen können, dass diese ausreichend gesichert sind
- **Die heikelsten Daten sind unsere Gesundheitsdaten.**

  Kann die elektronische Patientenakte datenschutz- und sicherheitskonform umgesetzt werden?
  Und was ist mit dem Datenschutz in Corona-Zeiten?
  Auch hier ist unsere Gesundheit betroffen und vieles andere!

In der Vergangenheit ist es schon einmal passiert, dass **Daten von Einwohnermeldeämtern ungeschützt ins Netz** gelangt sind. Hier greift genau dieser Punkt: wenn andere meine Daten schon verarbeiten (müssen), dann müssen sie aber auch sehr gut darauf aufpassen.

Ich empfehle, mit der **Wohnadresse** sparsam umzugehen, gerade wenn man als Frau alleine lebt. Gleiches gilt für das Geburtsdatum. Zum Beispiel in Arztpraxen gilt dies am Telefon als einfache Authentifizierungsmethode.

Ist das **Geburtsdatum** weithin öffentlich bekannt, wird Identitätsdiebstahl um einiges einfacher.

In dem Zusammenhang stellt sich zwangsläufig die Frage: können unsere Gesundheitsdaten ausreichend geschützt werden, obwohl viele Stellen darauf zugreifen können müssen bei der Umsetzung der elektronischen Patientenakte?

Zusammenführung von Daten und wie schnell ich ein „schlechter“ Patient werden kann

- Ohne berechtigtes Interesse ist weder Speichern noch Zusammenführen von Daten erlaubt
- USA: Arbeitgeber erfährt vom Einkaufsverhalten eines Angestellten: zuviel Alkohol – Kündigung
- Gefahren: was, wenn der Versandhändler meine Kleidergröße an die Krankenkasse weitergäbe? Oder der Supermarkt meine Einkäufe?
- Beliebt: Fitnessarmbänder und dazugehörige „Gesundheitsapps“ - da freuen sich die Krankenkassen schon drauf…..

Wir sehen, dass gerade rund um das Thema Gesundheit viele Gefahren lauern.

Was ist, wenn ich die Süßigkeiten nur für meine normalgewichtigen Familienmitglieder einkaufe und gar nicht für mich? Die Krankenkasse bekommt dennoch ein falsches Bild.

Besonders auf „Gesundheitsapps“ freuen sich die Krankenkassen. Sie dokumentieren z.B. wieviele Schritte ich täglich mache. Dabei ist nicht einmal klar, ob es 10.000 Schritte am Tag sein sollten für ein „gesundes“ Leben oder auch 6.000 reichen. Idee ist, Patienten, die sich vermeintlich gesund verhalten, Rabatte einzuräumen. Aber die Kasse sieht nicht, ob man das Armband nicht dem Hund um den Hals gebunden hat und der nun meine Schritte macht. Und was ist, wenn ich die Schrittzahl nicht mehr halten kann? Wenn Krankheiten hinzukommen, unverschuldet? Bin ich dann plötzlich ein schlechter Patient?

Ebenso gibt es WeightWatcherApps, die helfen sollen, die Punkte einzuhalten. Aber wer hindert mich daran, Essen dort einfach nicht einzutragen?

Wir stellen fest: es ist nichts offenkundig und einfach interpretierbar.

Eine Personenkennziffer für alles - praktisch oder pervers?

- **Beispiel Dänemark**: lebenslange Nummer aus Geburtsdatum und vier weiteren Stellen.
  Wird für Anmeldung bei Kindergarten, Schule, Ausbildung, Arzt benötigt
  => Zugang zu allen Informationen!
  (Quelle: Sendung mit der Maus, 8.3.2020)
- **Beispiel DDR:** Personenkennziffer, Stasi, Überwachung, böse.
- **Beispiel Bundesrepublik** heute: Lebenslange Steuernummer. Aber wir sind ja die Guten!

Es ist aus vielen Gründen unklug, alle Erfordernisse des Lebens an eine Nummer oder ein Gerät (Smartphone) zu koppeln. Ebenso muß man die Entwicklung beim ePerso beobachten. Derzeit stehen immer noch nicht viele Anwendungsmöglichkeiten zur Verfügung.

Mein Test der Einkommenssteuererklärung mit Lesegerät und Perso online beim Finanzamt steht noch aus.

Und hier kommen wir wieder zur **Gesundheit.** Über die eigene Gesundheit bzw. Krankheit spricht man nicht sofort und nicht mit jedem. Des sei gerade auch den Menschen gesagt die „nichts zu verbergen“ haben. Man geht mit erblichen, psychischen, Geschlechts- und auch ganz normalen Krankheiten einfach nicht überall hausieren.

Das Beispiel Dänemark zeigt, wie dünn die Grenze der Daten zum Gesundheitswesen dort ist.

Können Datenpannen ausgebügelt werden?

- Fehlbuchungen bei der Bank: ja.
- Fehler bei der Schufa: ja.
  Bei häufig vorkommenden Namenskombinationen aber schwierig!
  (es gibt auch ein Recht auf Korrektur falscher Daten).
- Jemand lädt Bilder ins Internet hoch:
  nicht mehr einzufangen
  Steigerung: Nacktbilder.
- Meine Gesundheitsdaten gelangen von der Krankenkasse ins Internet und von dort aus an **irgendwen** und meinen Arbeitgeber: DatenGAU.

Eines haben immerhin unsere Politiker zwischendrin begriffen: **wird auch nur eine einzige Patientenakte öffentlich**, ist das Vertrauen in das gesamte System dahin.

Es ist allerdings sehr schwierig, **Server im Internet 100%ig** abzusichern, so dass nur authorisierte Nutzer (also der Patient, Arzt, Apotheke) zugreifen kann, ein Angreifer aber nicht. Es stellt sich daher die Frage, ob die elektronische Patientenakte überhaupt umgesetzt werden kann.

Ebenso: **was passiert, wenn Daten unbemerkt verändert werden?** Diabetes zu haben oder nicht kann im Notfall lebensbedrohlich sein, wenn die Information falsch vorliegt.

Und:es hat GRÜNDE, warum der Arbeitgeber die zugrundeliegende Krankheit bei einer Krankschreibung eben NICHT erfährt. Nicht wenige Arbeitgeber rufen Ärzte an und bedrohen das Personal, die Diagnose herauszugeben!

Gesundheit, Krankenkassenkarte, elektronische Patientenakte (ePA) (1)

- **Bisherige Krankenkassenkarte:** nur Stammdaten (Adresse, Geburtsdatum)
- **Geplante ePA:** Alle Daten liegen zentral auf Servern im Internet
  sollen aber nur berechtigten Personen (mir selber, Arzt, Apotheke) nach Freigabe zugänglich sein
- **Vortrag beim 36C3:** eine Arzt- oder Praxiskarte widerrechtlich zu erlangen ist EINFACH:
  “Hacker hin oder her – die elektronische Patientenakte kommt!“
  https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt
- **Hauptproblem:** Ausgabe der Karten darf eigentlich nur nach erfolgreicher **persönlicher Identifizierung** (z.B. postident) erfolgen

Wie bereits angedeutet, ist die sichere Speicherung von Daten bei gleichzeitigen Zugriffsmöglichkeiten von mehreren authorisierten Stellen nicht auf einfache Weise sicher zu bewerkstelligen.

Eine große Herausforderung besteht auch bei der Ausgabe der zugehörigen Karten. Anders als bei der Gesundheitskarte bisher, darf diese nicht per Post verschickt werden.

Genau wie bei Perso und Reisepass muss sich die Person oder der Arzt ausweisen, um die Karte zu erlangen, weil an ihr mannigfaltige Funktionen hängen, die nicht in falsche Hände kommen dürfen. Das ist aber aktuell weniger geplant denn je.

Beispiel: auch bei der Ausgabe von S/MIME Zertifikaten zum Signieren und Verschlüsseln von E-Mails wird eine persönliche Identifizierung im Deutschen Forschungsnetz verlangt. Hier sind aber idR. viel weniger heikle Daten im Spiel.

CCC Mitglieder hatten im og. Vortrag erklärt, wie leicht sie an die Arzt- und Praxiskarten kommen konnten.

Gesundheit, Krankenkassenkarte, elektronische Patientenakte (ePA) (2)

- 26. Mai 2020, Pressemeldung des CCC: “Geplantes Patienten-Datenschutzgesetz schützt Patienten nicht“:

  “Mit den neuen Regelungen soll die Verpflichtung zur sicheren Identifikation des Versicherten bei Kartenbeantragung vollständig entfallen. Die Ausgabe der Gesundheitskarte wird nur noch auf niedrigem Sicherheitsniveau vorgeschrieben.“
- Könnte die ePA auf einem USB-Stick die Lösung sein? (Ja, ist auch nicht sicher, kann auch verlorengehen)

Quelle: https://www.ccc.de/de/updates/2020/pdsg

Das ist der „Trick“ man definiert „niedriges Sicherheitsniveau“ und muss schon nichts mehr tun, um die Sicherheit bei der Ausgabe der Karten zu erhöhen.

Wieviel muss der CCC NOCH zeigen, dass es schiefgeht?

USB-Sticks sind zwar auch alles andere als „sicher“, aber was, wenn jeder seine Akte auf einem Stick bei sich hätte? Die Karte trägt man ja auch mit sich herum. Ja, beides kann auch verlorengehen, aber die Kasse hat ja alle Befunde.

Corona und der Datenschutz

- Kartenzahlung statt Bargeld
- Registration von Kontaktdaten beim Restaurantbesuch:
  Name, Datum, Uhrzeit
  Adresse, Mailadresse ODER Telefonnummer
  unklar: ein Gast am Tisch oder alle?
  Aufbewahrung 4 Wochen
  => tragbar in meinen Augen!
- Klappt nicht mehr: Gesichtserkennung

Was ich nicht gern mache: mit Karte zahlen. Egal ob EC mit Pin, Unterschrift („berührungslos“ habe ich deaktivieren lassen) oder Kreditkarte: alles hinterlässt eine unnötige Datenspur bei der Bank.

Jetzt aber wird das bargeldlose Zahlen angepriesen als „hygiensicher“. Ist es aber nicht in allen Fällen (Pin eingeben).

Allerdings wurde ich auch noch nicht dafür kritisiert, dass ich weiterhin bar zahle. An vielen Stellen geht es auch nicht anders: auf dem Wochenmarkt.

Corona-Verordnung Gaststäetten vom 16. Mai gültig ab 2, Juni 2020:

https://www.baden-wuerttemberg.de/en/service/aktuelle-infos-zu-corona/verordnung-gastronomie/

Die Regelungen für Restaurantbesuche sind datenschutztechnisch soweit in Ordnung. Papier kann problemlos nach 4 Wochen geschreddert werden, ein unbemerkter Zugriff ist schwerer möglich als bei Datenspeichern.

Und das ist Haecksen-Humor: so lästig die Gesichtsmasken sind, Gesichtserkennung klappt damit nicht, daher darf man sie beim Autofahren nicht tragen :)

...und dann war da noch das mit der Corona-App….

- Beginn der Corona-Krise: Bundesregierung befragt RKI und die Infektionsforschung an der Charite
- Gesundheitsministerium: fragt keinen und verliert 3-4 Wochen wertvolle Entwicklungszeit durch beharren auf zentrale Speicherung bei der Corona-Warn-App
- Freitag, 24.4.2020: CCC: „Corona-Tracing-App: Offener Brief an Bundeskanzleramt und Gesundheitsministerium“
- Sonntag, 26.4.2020, Tagesschau auf ARD um 12: Das Gesundheitsministerium ist nun auch für ein dezentrales Verfahren.
- Dienstag, 2.6.2020: SAP und Deutsche Telekom AG veröffentlichen Source Code zur Corona-App auf Github

https://www.ccc.de/de/updates/2020/corona-tracing-app-offener-brief-an-bundeskanzleramt-und-gesundheitsminister

https://www.zeit.de/digital/2020-05/corona-app-open-source-projekt-programmcode-quellcode

Ich war ein bißchen verwundet, die beratungsresistent das Gesundheitsministerium war. An anderen Stellen war die Regierung ja durchaus in der Lage, die entsprechenden Experten zu fragen. So wurde wertvolle Zeit für die Entwicklung vergeudet.

Aber es zeigt sich: der CCC wird doch gelegentlich gehört!

Und Sie erinnern sich an eine eingangs erwähnte Forderung nach Open Source in staatlichen Projekten: dies wurde mit der App nun umgesetzt!

….und wie soll die Corona-Tracing-App nun funktionieren?

- Im Grundsatz: es muss nur erfasst werden, **DASS** sich zwei Smartphones begegnet sind, aber nicht **WO** und nicht **WER**
- Die Smartphones zweier Personen tauschen bei passender Nähe und ausreichend langem Kontakt per Bluetooth IDs aus, die aber keinen Rückschluß auf Personen zulassen
- Wird ein Smartphoneinhaber positiv getestet, gibt er das in der App ein, die die Konkakte und einen zentralen Server informiert.
- „Knackpunkte“: bluetooth ist nicht besonders zuverlässig, wie sind die Schwellwerte bei Entfernung und Zeit, wieviele Menschen nehmen teil, geben sie zuverlässig ein, wenn sie positiv sind?

  => die App kann nur EIN Baustein bei Bekämpfung der Pandemie sein

https://www.ccc.de/de/updates/2020/contact-tracing-requirements

https://netzpolitik.org/2020/faq-corona-apps-die-wichtigsten-fragen-und-antworten-zur-digitalen-kontaktverfolgung-contact-tracing-covid19-pepppt-dp3t/#anonymes%20Tracing

Gute Erklärung der App: ZDF Heute Sendung, Samstag 6.6.2020, 19 Uhr → Mediathek!

Offene Fragen: werden hinreichend viele Menschen die App nutzen? Wird sie, wie die Masken zum Teil, die Menschen wieder unvorsichtiger werden lassen, denn sie werden ja dann gewarnt? Eine 100%ige Zuverlässigkeit kann nicht gegeben sein.

Was macht das Ausland?

Land	Stand	Speicherung	Bedingung	Nutzer	Bevölkerung
Großbritannien	20.5.20	Zentral 28 Tage		60.000	66.435.550
Schweiz “SwissCovid“	31.5.20	dezentral	Kontakt 15 Min.	„mehrere Tausend“	8.603.990
Österreich “StoppCorona“	31.5.20	Dezentral, 48h, OpenSource		77.000 “am ersten Wochenende“	8.858.775
Frankreich “StopCovid“	2.6.20	Zentral noch nicht für Apple	Kontakt 15 Min. Abstand 1m		66.993.000
Island	2.6.20			37%	356.991
Italien	3.6.20	Zentral			60.262.701

Quellen:

https://www.zeit.de/digital/2020-05/corona-app-nhs-grossbritannien-tracing-datenschutz-menschenrecht/komplettansicht

https://www.zeit.de/digital/internet/2020-05/tracing-app-coronavirus-oesterreich-schweiz/komplettansicht

Island: 37% ca. 132.000

Denkanstöße

- „K.I. Wer das Schicksal programmiert“
  Roman von Christian J. Meier
  Science Fiction? Eine K.I. berechnet Krankheitsverläufe
  https://www.heise.de/tp/features/Digitale-Herren-ueber-die-Gesundheit-4652983.html
- Das DNA-Müsli von mymüsli
  https://netzpolitik.org/2020/mymuesli-vermarktet-dna-ernaehrungstests/
- Aus o.g. Artikel: in den USA haben private Verarbeiter von DNA-Informationen Daten ohne Zustimmung ans FBI gegeben

Warum gehen wir fahrlässig mit unseren Daten um?

- **Jugendliche**: wollen kommunizieren,
  wollen präsent sein,
  wollen beliebt in der „peer group“ sein
- **Senioren**: höheres Sicherheitsbedürfnis durch subjektives Unsicherheitsgefühl
- **Erwachsene** „in der Mitte“?????
- 1980er: Eltern und Lehrer gehen in Deutschland (West) auf die Straße gegen die Volkszählung
- Deutschland (Ost): Die Stasi sammelt Daten ohne Grenzen

  => Der Überwachungsstaat nebenan ist weg.
  Offenbar erinnert sich keiner mehr, daß er/sie nicht überwacht werden wollte.

1986 fing ich mit „der Computerei“ an. Damals wurde **gegen die Volkszählung** demonstriert, denn erstmals sollten die Daten am Computer erfasst werden. Personen waren dann viel leichter auffindbar, als wenn man im Keller regaleweise Ordner hätte durchsuchen müssen.

Denkanstoß: wie würde die Stasi mit den technischen Möglichkeiten von heute vorgehen?

Viele der „Gadgets“ aus **James-Bond-Filmen** waren visionär und sind nun als normale Produkte im Handel erhältlich. Die Spionage ist im täglichen Leben angekommen.

Unklar bleibt, warum so viele Menschen sich so sehr exponieren.
Warhol: 15 Minuten Ruhm?

Soziale Netzwerke, Vor- und Nachteile

- Zunächst: das Internet ist ein wunderbarer Raum zum **Kommunizieren** und zur **Wissensgewinnung**!
- „früher“: alle Freunde durchtelefonieren.
  Heute: alle per facebook oder whatsapp einladen
- Auch: **Sportvereine** haben keine „Telefonkette“ mehr. Aber hat auch **jedes Kind unbeschränkt Internetzugang**?
- Werden Menschen ohne Smartphone **abgehängt**?
- Bekommen Menschen ohne Internetzugang **weniger Rabatte**?
- Datenspuren (Äußerungen, Fotos)
- Daten liegen oft **im Ausland unter unklarer Rechtslage!**

Noch nie war es so leicht, **an Wissen zu gelangen**, wie heute. Früher endete mein Wissenshunger an dem Füllstand der Hamburger Öffentlichen Bücherhalle. Mehr als dort war für mich nicht zugänglich. Heute kann man auf unzählige Wissensdatenbanken zugreifen. Kernkompetenz ist zweifellos **„gut suchen“ können und die Bewertung von Quellen.**

Wenn man sich an **gewisse Regeln** hält, kann man viel Spaß haben und auch viele tolle Menschen kennenlernen. Die „Regeln“ sollten wie Verkehrsregeln begriffen werden. Diese hat man verinnerlicht und man begreift sie auch nicht als Last, sondern einfach als sinnvoll.

Wichtig: das Leben muß auch ohne Internet lebbar sein, ohne Nachteile! Nicht jeder will und kann am Internet teilnehmen. Manche Menschen haben nicht das Geld, einen Rechner und Internetzugang zu unterhalten. **Dafür gibt es hier in der Bibliothek Leihrechner!**

Zusammenfassung / Was tun?

- **Daten,** die vorhanden sind, können **ge- und mißbraucht** werden
- Daten, die gar nicht erst anfallen, **können nicht mißbraucht werden**
- **Lösung für die ePA: USB-Stick?**
- **Datensparsamkeit** leben.
- **Nachfragen:** welche Daten sind von mir gespeichert?
- **Umgebung aufklären**, warum man z.B keine Fotos im Internet will.
- **Kinder aufklären**, dass sie auch mal „nein“ zu Fotos sagen dürfen oder dass nicht jede/r ihren Namen kennen muss.

  => die digitale Selbstverteidigung aufnehmen

Die gute Nachricht: Sie sind den Datensammlern und der Informationsüberflutung nicht hilflos ausgeliefert.

Wenn Sie ein bißchen wachsam bleiben und Dinge **hinterfragen**, sind Sie schon einen großen Schritt weiter!

Auch: Berührungslose Zahlfunktion der EC Karte abschalten lassen.

Auch Sie müssen als Erwachsener im Internet nicht überall mit Ihrem richtigen Namen auftreten, nutzen Sie ein Pseudonym! Sagen sie auch ihren Kindern, dass sie im Netz nicht den echten Namen verwenden. Auch nicht Wohnadresse und Telefonnummer.

Mobbing und auch Cybergrooming (also Kontktaufnahme älterer Menschen zu Jüngeren) findet im Stillen statt. Bringen Sie herüber, dass Ihr Kind mit Ihnen reden kann. Schimpfen Sie nicht und machen Sie sich nicht lustig, wenn Ihr Kind gemobbt wird oder auf einen evtl. Pädophilen hereingefallen ist, sonst erfahren Sie so etwas nie wieder.

Veranstaltungstips

Cryptoparty: fallen bis auf weiteres leider aus

Regelmäßige **Vorträge**: idR. 2. Donnerstag im Monat, Stadtbibliothek, 19:30
Donnerstag, 18.6.2020: Die Corona-App
Anmeldung erforderlich, Audio wird gestreamt

Fragen / Diskussion

?

?

?