Willkommen im Überwachungsstaat Schweiz!

Ich heisse Sie ganz herzlich im Überwachungsstaat Schweiz willkommen! Seit dem ersten März 2018 dürfen Sie sich nun ganz sicher fühlen, denn die gesamte Kommunikation aller Terroristen und Verbrecher wird nun in der Schweiz lückenlos überwacht. Ganz nebenbei wird auch Ihre gesamte Internetkommunikation aufgezeichnet und für ein halbes Jahr gespeichert. Der Staat weiss nun, dass sie dieses «aufrührerische» Blog lesen. Fühlen Sie sich nun immer noch so sicher? Aber ja doch, wer ja nichts zu verbergen hat, hat auch nichts zu verlieren! Denken Sie nur einmal an unsere Firmen; die haben doch nichts zu verbergen. Oder vielleicht doch? Firmengeheimnisse? Gut, der Überwachungsstaat Schweiz garantiert uns, dass er keine Inhalte durchschnüffelt. Nein, er lässt ja nur Meta- und Verbindungsdaten speichern. Kaum ist das neue BÜPF in Kraft getreten, zeigen Recherchen des Schweizer Fernsehens, dass die Provider jedoch viel mehr speichern, nämlich die gesamte Surf-History von Internetanwendern. Somit lässt sich lückenlos nachvollziehen, wer was wo wann und wie aufgerufen hat, also auch Inhalte, sofern sich diese in keinem geschützten Bereich befinden. Das betrifft die grosse Mehrheit aller Internet-Inhalte, welche heute "zum Glück" mit permanenten Adressen versehen sind, d.h., sie verschwinden nicht einfach so.

I see you, I hear you, I'm interested in you.

Kaum hat der Europäische Gerichtshof (EUGH) die anlasslose Vorratsdatenspeicherung gekippt, stürzt sich die Schweiz in das aussichtslose Abenteuer der flächendeckenden Überwachung. Alle Internet-Nutzerinnnen sind nun auf dem Radar der staatlichen Überwachung angekommen. Alle? Nein, Technologie-Versierte können sich dieser Überwachung mit Leichtigkeit entziehen. Diese Technologien stehen auch Otto Normalverbraucher zur Verfügung. Dazu später mehr. Die Überwachung trifft also zuallerst einmal die grosse Mehrheit der unbedarften Internet-Surfer. Die Verbindungsinformationen von Herrn oder Frau Musterbürger, die manchmal klammheimlich ihren Sex-Fantasien auf dem Internet nachgehen, sind nun nachvollziehbar gespeichert. Wer dort die dünnne Linie überschreitet, könnte schon bald Probleme bekommen. Sie fühlen sich jetzt gewiss immer noch sicher vor den bösen Terroristen, die auf dem Internet Anschläge planen, oder vor den fiesen Hacker-Verbrechern, welche die IT-Infrastruktur des Bundes angreifen. Wir haben anscheinend schon vergessen, dass es für solche Planungen gar kein Internet braucht. Tatsächlich gibt es noch - wir staunen - die Offline-Kommunikation.

> Jetzt klebt ihnen der eigene Staat sprichwörtlich am Arsch.

Konsequenterweise müsste der schweizerische Total-Überwachungsstaat also sämtliche Offline-Verbindungs-Daten aller Schweizerinnen registrieren: Blocher trifft Mörgeli am Mittwoch, dem 14. März 2018, um 19:15 Uhr in der Kronenhalle in Zürich (Typ: Verbindungsdaten) - zwecks Besprechung einer Doppelkandidatur für den Bundesrat (Typ: Inhaltsdaten). Beruhigen Sie sich gleich wieder: das war nur ein fiktives Beispiel. Aber warum überwacht denn unser Staat all diese potenziell konspirativen und mutmasslich terroristischen Offline-Aktivitäten nicht mit aller Härte, wie das doch auch im Internet schon praktiziert wird? Es gibt zwei Antworten auf diese Frage. Erstens ist es nicht möglich und zweitens würde eine solche Überwachung den Schweizerinnen zu weit gehen. Im Internet ist diese Totalüberwachung jedoch technisch einfach zu realisieren. Zudem scheinen die Schweizerinnen diesen Eingriff in ihre digitale Privatsphäre hinzunehmen, obwohl sich ihre Kommunikation heute grösstenteils im Internet abspielt. Gut, die Stimmbürgerinnen haben es so - oder nicht anders - gewollt. Jetzt klebt ihnen der eigene Staat sprichwörtlich am Arsch. Ja, diese Formulierung trifft es. Immerhin betrifft diese Total-Überwachung auch die Law&Order-Fraktion, welche manchmal mehr zu verbergen hat, als wir gemeinhin annehmen. Da lohnt sich manchmal nur schon ein Blick in geleakte Datenbanken, z.B. in jene von Ashley Madison (Washington Post, engl.).

> Wer halt nichts zu verbergen hat, hat halt auch nichts verlieren, oder?

"Den Luxemburger Richtern zufolge greift die Speicherung von Telekommunikationsdaten so sehr in das Grundrecht auf Achtung des Privatlebens ein, dass die Datenspeicherung „auf das absolut Notwendige“ beschränkt werden muss." (Zitat: faz.net)
Wieder verfalle ich und Sie in ungläubiges Staunen: Die Europäer schützen ihre Bürger besser als wir Schweizer. Wir Deppen hingegen beschneiden unsere Grundrechte freiwillig auf demokratischer Basis. Gut, das muss man als Demokrat akzeptieren. Sicher werden Sie es auch akzeptieren, wenn der grosse Bruder aus Übersee an die Türe klopft und die Herausgabe von Daten verlangt. Keine Sorge, wir werden nicht Nein sagen. Sicher werden Sie es auch akzeptieren, wenn eine Hacker-Gruppe die halbe Schweiz de-anonymisiert und ihre Verbindungsdaten offenlegt. Wer garantiert Ihnen, dass genau dies nicht geschieht? Der Überwachungsstaat Schweiz auf jeden Fall garantiert das nicht, zumal er die Daten ja bei privaten oder halb-privaten Providern erheben lässt. Fühlen Sie sich noch immer sicher vor Terroristen und Online-Verbrechern? Wer halt nichts zu verbergen hat, hat halt auch nichts verlieren, oder? Sind Sie schon ein bisschen unsicher geworden? Empfinden Sie schon ein gewisses Unbehagen dem Staat gegenüber? Gut, dann schauen wir weiter.

> Wir haben unsere Freiheit einer trügerischen Sicherheit geopfert.

Unsere digitale Wirtschaft, die nun im Kanton Zug soeben zum Cryptocurrency-Eldorado werden möchte, preist gerne die Sicherheit ihrer Infrastruktur an. Damit ist nun leider Schluss, denn der Staat kann nun von jedem Anbieter von Telekommunikations-Dienstleistungen die Erhebung und Herausgabe von Verbindungsdaten verlangen. Organisationen und Firmen, welche ihre berechtigten Geheimnisse Schweizer Firmen anvertrauen möchten, werden es sich jetzt zwei Mal überlegen. Standortvorteile, ganz zu schweigen von unseren Grundrechten, haben wir also auch gleich einer zweifelhaften Sicherheit geopfert. So, jetzt sollten wir langsam an den Punkt gekommen sein, an dem wir feststellen, dass wir einen riesigen Fehler gemacht haben: Wir haben unsere Freiheit einer trügerischen Sicherheit geopfert. Ja, diese Sicherheit ist trügerisch, denn ich zeige Ihnen nun, wie Terroristen oder auch Sie als unbescholtene Bürgerin dieser Überwachung spielend und legal entgehen können. Wenn Sie Ihre Privatsphäre zurück haben wollen, lesen Sie weiter! Nein, das ist keine Anleitung zu Straftaten, nein, das ist digitale Selbstverteidigung für rechtskonforme Bürgerinnen.

- Surfen Sie in einem öffentlichen Netz! Easy
- Nutzen Sie den Tor-Browser. Er anonymisiert ihre IP-Adresse. Empfohlen gerade oder auch in öffentlichen Netzen.
- Betreten Sie ganz legal das Dark Web mit I2P oder freenetproject.org. Das sind getarnte und verschlüsselte Netze auf der bestehenden Internet-Infrastruktur. Dort lässt sich ganz legal und sicher kommunizieren. Verbrechen sind dort natürlich auch möglich, aber damit wollen wir nichts zu tun haben, wie im richtigen Leben halt.
- Für ein bisschen Fortgeschrittenere: Nutzen sie die tor-basierte Linux-Distribution Whonix in virtuellen Maschinen auf einem dedizierten Computer. Da gucken Überwacher wirklich in die Röhre. Da spielt es fast keine Rolle in welchem Netz Sie sich bewegen. Edward Snowden empfiehlt die Linux-Distribution «Tails».
- Mieten Sie sich ein VPN bei einem vertrauenswürdigen Anbieter! Ihre Aktivitäten lassen sich nicht nachvollziehen. Anmerkung: Schweizer VPN-Anbieter müssen nun natürlich Verbindungsdaten erheben. (Ade Standortvorteil!) Wichtig: Meiden Sie den Gratis-VPN-Anbieter hola.org. Er macht Sie ungefragt zu einem Exit-Knoten, der ihre IP-Adresse mit den Handlungen anderer in Verbindung bringt.
- Nutzen Sie das relativ neue Zeronet in Verbindung mit Tor. Die Daten sind überall und nirgends. Ziemlich kreativer Ansatz, der die Anfänge eines dezentralen Netzes ohne Server skizziert! Horror für Überwachungs-Freaks.
- Nutzen Sie für vertrauliche Kommunikation einen sicheren verschlüsselten Messenger auf ihrem Mobilgerät. Nein, Whatsapp ist nicht sicher, Skype ist nicht

sicher. Nutzen Sie: Signal, Telegram oder Threema. Bei letztem Messenger muss man jetzt leider, leider sagen: Achtung, Standort Schweiz! Etliche vielversprechende Messenger-Apps sind in Arbeit.
- Am besten leiten Sie die ganze Kommunikation Ihres Mobilgerätes über Tor oder ein VPN Ihrer Wahl.
- Achten Sie bei Webseiten darauf, dass die Verbindung verschlüsselt über HTTPS hergestellt wird. 

- Deaktivieren Sie Plug-Ins wie Adobe Flash. Diese Software ist unsicher und fehlerhaft. Videos können heute ohne dieses Plug-in abgespielt werden. (Der Tor-Brower schliesst solche Lücken von Vorherein aus.)
- Zum Schluss: INFORMIEREN SIE SICH ÜBER DIE SOFTWARE, DIE SIE EINSETZEN! Vertrauen Sie weder mir noch den Anbietern von Software blind.

So, nun sind Sie einigermassen vor staatlicher Verfolgung geschützt. Merken Sie sich ferner: Sollten Geheimdienste oder Hacker gezielt auf ihre Geräte zugreifen wollen, können Sie sich dagegen nahezu nicht wehren. Gehen Sie nun trotzdem ganz anonym und entspannt Ihrer ehrlichen Arbeit nach. Noch was: Wenn Sie wissen wollen, wie Sie sich gegen die penetrante Online-Werbe-Industrie schützen können, lesen Sie meinen letzten Beitrag.

Ansonsten viel Spass im Überwachungsstaat!