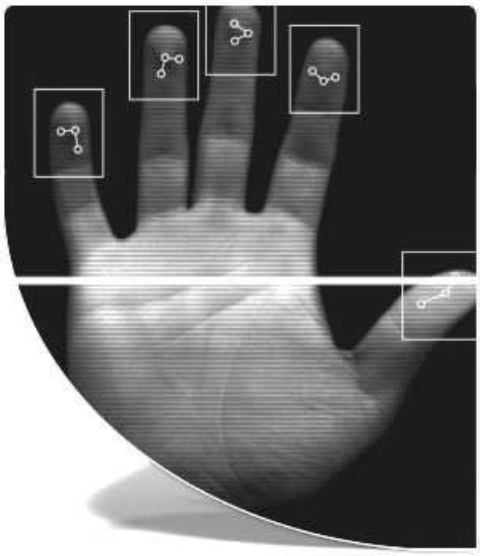
.at/tack

RAW
{rosa antifa wien}

Pretty bad Privacy

Es ist keine sonderlich neue Erkenntnis, dass sich Staaten nach immer stärkerer Überwachung "ihrer" Bürger_innen sehnen. Und doch ist in den letzten Jahren eine erhebliche Intensivierung entsprechender Bemühungen zu bemerken. Geradezu beispielhaft für die Brutalität mit der aktuell das Recht auf Privatsphäre ausgehebelt wird, ist die Art mit der Ende 2007 in einer Art "Nacht-und-Nebel"-Aktion ein neues Sicherheitspolizeigesetz durch das Parlament gepresst wurde. Ohne jegliche öffentliche Diskussion wurde damals ein Gesetz beschlossen, dessen konkreter Inhalt erst wenige Stunden zuvor bekannt wurde, das der Polizei aber erheblich verstärkte Überwachungsmöglichkeiten an die Hand gegeben hat.

So ist es seit dem 1.1.2008 möglich, dass jede_r Polizist_in mit einem simplen Formular ein x-beliebiges Handy orten lassen kann – selbst die minimale Hürde der richterlichen Anordnung hatte man mit der Gesetzesnovelle verabschiedet. Seitdem reicht ein simples Fax an den Mobilfunkanbieter_innen, um den Standort einer Person zu erfahren. Eine Möglichkeit, die geradezu nach ihrem Missbrauch schreit; was offiziell nur für "konkrete Gefahrensituationen" gedacht war, wird in der Realität wohl eine deutlich "breitere" Anwendung finden. Wer soll schon kontrollieren, ob die auf dem behördlichen Schmierzettel angegebene Begründung "Suizidgefahr" wirklich stimmt, oder ob doch nur ein_e neugierige_r Beamt_in herausfinden will, was der/die Lebenspartner_in/Nachbar_in/Kolleg_in gerade tut? Die Mobilfunkanbieter_innen haben dazu keinerlei Möglichkeit, außer sie rufen bei der angegebenen Nummer an, was im Fall eines realen Selbsttötungsversuches wohl eher weniger von Vorteil wäre. Eine Nachkontrolle der Abfragen sieht das Gesetz auch nicht vor, ganz zu Schweigen von einer Überprüfung durch ein unabhängiges Gremium. Die Chancen wenigstens im Nachhinein von einer solchen Bespitzelungsaktion zu erfahren, stehen für die Betroffenen damit wohl äußerst gering. Absurd auch die öffentlich vorgetragene Argumentation, dass die Gesetzesnovelle primär für Fälle wie die "Auffindung von vermissten Tourengehern oder Bergsteigern" notwendig ist - entsprechende Abfragen waren nämlich schon nach der alten Rechtslage längst möglich.



So erschreckend die aktuelle Gesetzeslage bereits ist, bleibt doch die alte Erkenntnis, dass von Innenminister_in zu Innenminister_in weiter an der Schraube der repressiven Begehrlichkeiten gedreht wird. Entsprechend meldete sich unlängst die aktuelle Innenministerin Maria Fekter zu Wort, die es sich offenbar zur Aufgabe gemacht hat, die letzten Hürden für die polizeiliche Totalüberwachung auszuhebeln. Geht es nach den Vorschlägen der Ministerin sollen die Behörden künftig einen direkten Zugriff auf die Standortdaten bekommen - ganz ohne die ach-so-umständlichen Anfragen an die Mobilfunkbetreiber. Beinahe schon von komödiantischem Talent zeugt dabei der Umstand, dass sich die Ministerin nicht einmal die Mühe gemacht hat, neue Argumente heranzukarren: Statt dessen wird einfach die Begründung von 2007 recycelt, schon wieder gilt es die offenbar äußerst gefährdete Spezies der Tourengeher_innen zu retten: "Wenn die Betreiber (..) keinen Journaldienst haben, müssen wir warten", so die Fektersche' Erkenntnis. Also gilt es der Polizei die vollkommen unregulierte Totalüberwachung aller Handy-NutzerInnen zu ermöglichen, natürlich nur zum Wohle der Tourengeher_innen. Gaaaanz, ganz ehrlich.

Internetbespitzelung

Gänsehaut kann auch der zweite Teil der 2008 in Kraft getretenen Novelle des Sicherheitspolizeigesetzes hervorrufen: Erlaubt er doch eine breite Überwachung des Internets. Die Ausforschung der so genannten IP-Adressen - eine eindeutig zuordenbare Nummer, die jeder Internetanschluss zur Funktion benötigt - ist den Behörden nun ebenfalls vollständig freigegeben. Auch wenn es in der Realität in den letzten Jahren wohl nur wenige Fälle gegeben hat, in denen Richter_innen der Polizei tatsächlich ihre Begehrlichkeiten in diesem Bereich verweigert haben, fällt hier doch eine erhebliche Hemmschwelle, die behördliche Spionage wird zum "Kinderspiel". Und die Erfahrung zeigt: Vorhandene Möglichkeiten werden von den Behörden immer ausgenutzt, die Rechtslage spielt dabei nur eine untergeordnete Rolle oder wird im Fall des Falles nachträglich angepasst.

Verblüffend ist auch ein weiterer Punkt des entsprechenden Paragraphen, der wohl nicht ganz unbeabsichtigt äußerst schwammig formuliert wurde: Die

Imp. M.H.V.: Rosa Antifa Wien, 1070 Wien

Ausforschung einer hinter einer bestimmten Nachricht im Internet steckenden Person. Was alles unter den unscharfen Begriff “Nachricht” fallen soll, wird nicht näher definiert. Und ohne sich dabei zu sehr in technischen Details zu verlieren: Dies ist derzeit nicht so ohne weiteres möglich, dazu müssten die Provider alle Verbindungsdaten mitspeichern - etwas, das aktuell gegen das Telekommunikationsgesetz verstoßen würde, wie selbst die Internet-Anbieter_innen herausstreichen. Worum geht es also wirklich? Wie die meisten dieser Regelungen ergibt auch diese nur Sinn mit einem Blick auf die Zukunft. Da soll nämlich die sogenannte Vorratsdatenspeicherung kommen, die den nächsten großen Überwachungsschritt für das Internet darstellen wird, und die eben die monatelange Aufbewahrung der besagten Verbindungsdaten vorschreibt. Ein Zugriff auf diese Informationen wäre dann aber wieder nur über eine richterliche Anordnung möglich, über den Umweg des neuen Sicherheitspolizeigesetzes haben sich die Lauschbehörden aber schon im Vorfeld eine Hintertür gesichert - immerhin sind bei diesem dann solche Abfragen ganz ohne diese Beschränkung möglich.

Für die Zukunft kursieren aber noch ganz andere Pläne: Ohne sonderlich gut verbergen zu können, dass er keinerlei Ahnung von der Materie hat, hatte bereits Innenminister Platter angekündigt, dass der sogenannte “Behörden-Trojaner” kommen soll. Mittlerweile unter dem euphemistischen Begriff “Remote Forensic Software” (RFS) angepriesen, handelt es sich dabei um ein Programm, das von außen auf den Computer einer zu bespitzelnden Person eingeschleust werden soll, um hier sämtliche Aktivitäten - ob privat oder beruflich - minutiös mitverfolgen zu können. Als Schreckgespenst für die Einführung solcher Maßnahmen müssen die “organisierte Kriminalität” einerseits und die “Terrorismusgefahr” andererseits herhalten, viel weiter bemüht mensch sich hierzulande auch gar nicht in die Tiefe zu gehen. Weder, was den realen Einsatz noch, was die technische Realisierbarkeit anbelangt, denn da würde sich schnell eine Fülle von grundlegenden Problemen zeigen.

Der Staat bricht ein

Schließlich ist das Einbringen und der Betrieb eines solchen Trojaners nicht gerade ein triviales Unterfangen: Muss er doch, um erfolgreich zu sein, eine Sicherheitslücke auf dem Zielrechner ausnutzen, sowie eine eventuell vorhandene Firewall und einen Viren-Checker austricksen. Von den Unwägbarkeiten des Einsatzes von Betriebssystemen jenseits von Windows und fortgeschrittener Abwehrmaßnahmen mal ganz zu schweigen. Und dann bliebe da natürlich noch die Frage, wie denn sicher gestellt werden soll, dass der Trojaner nicht selbst Sicherheitslücken öffnet und Einfallstor für andere Schädlinge wird (die dann auch das Untersuchungsergebnis verfälschen könnten). Ganz zu Schweigen von der praktischen Unmöglichkeit für Betroffene den Behauptungen der Behörden etwas entgegenzusetzen.

Der recht offensichtlichen Erkenntnis, dass sich so ein Behördentrojaner eigentlich viel besser für den Masseneinsatz eignen würde, also etwa um festzustellen, wer in Online-Tauschbörsen aktiv ist, oder wer sich welche “verdächtigen” Webseiten ansieht, hat das Ministerium jenseits von Abwiegelei recht wenig entgegenzusetzen. Die Behörden könnten die bei einem Masseneinsatz entstehende Datenmenge gar nicht richtig auswerten, so die offizielle Position. Ein Argument, das vielleicht aktuell noch eine gewisse Gültigkeit haben mag, in einigen Jahren werden aber wohl auch dafür die nötigen Verarbeitungsmöglichkeiten vorhanden sein, die behördliche Aufrüstung schreitet schließlich auch in diesem Bereich rasant voran.

Beschaffungskriminalität?

Erklären müsste das Innenministerium dann auch noch, woher dieser sagenumwobene Alleskönner-Trojaner eigentlich kommen soll, immerhin ist die Entwicklung eines solchen Programms nicht gerade eine triviale Aufgabe. So werden die behördlichen Spitzel wohl fallweise nicht um einen externen Zukauf herum kommen, doch auch so etwas ist nicht ganz einfach. Denn wenn das Ganze effektiv sein soll, müssten die ausgenutzten Sicherheitslücken bislang noch unbekannt sein. Entsprechende Informationen und dazu passende Tools gibt es zwar im Netz tatsächlich zu kaufen, allerdings werden diese um nicht gerade wenig Geld am virtuellen “Schwarzmarkt” gehandelt; ob sich das Innenministerium wirklich solcherart versorgen lassen

Die **IMSI** (International Mobile Subscriber Identity) ist eine einzigartige 15-stellige Nummer die zur Identifizierung einer einzelnen Benutzer_in in einem Mobilfunknetz dient.

IMSI-Catcher sind Geräte, die dazu dienen die IMSI auszulesen, den Standort eines Mobiltelefons festzustellen sowie die darauf getätigten Gespräche abzuhören. Handys buchen sich immer bei der Funkzelle mit dem stärksten Signal ein, dies nutzt der IMSI-Catcher, in dem er selbst ein stärkeres Funksignal anbietet und so alle Anrufe in einem gewissen Umkreis auf sich zieht. Dabei werden auch Daten von Unbeteiligten erfasst, ohne dass diese davon erfahren.

Eine **IP-Adresse** (Internet-Protocol-Adresse) dient zur eindeutigen Adressierung von Rechner_innen und anderen Geräten in einem IP-Netzwerk. Das bekannteste Einsatzgebiet, in dem IP-Adressen verwendet werden, ist das Internet. Allen am Internet teilnehmenden Rechner_innen wird eine IP-Adresse zugeteilt. Die IP-Adresse entspricht funktional der Rufnummer in einem Telefonnetz.

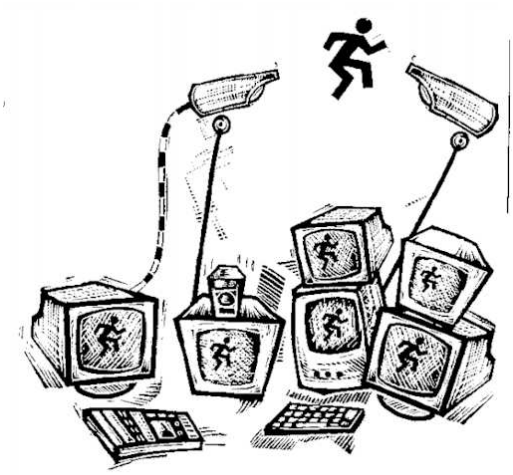
will? Wobei: Die Vorstellung eines Bieter_innenkampfes zwischen einer staatlichen Behörde und professionellen Spammer_innen um die neueste Sicherheitslücke hat einen gewissen absurden Reiz. Alternativ könnte die Software natürlich auch bei einem "befreundeten" Geheimdienst besorgt werden, ein Vorgehen, bei dem dann wieder zu klären wäre, wie sichergestellt werden soll, dass diese nicht gleich die Gelegenheit nutzen um "mitzulauschen".

Dass selbst eine "intraministerielle Arbeitsgruppe", die wohl kaum einer prinzipiellen Ablehnung gegenüber Überwachungsmaßnahmen verdächtigt werden kann, in einer offiziellen Expertise kaum ein gutes Haar an den Platterschen Allmachtsträumen gelassen hat, scheint auch die neue Ministerin wenig zu stören. Allen rechtlichen und gesellschaftspolitischen Bedenken zum Trotz steht der Beschluss eines entsprechenden Gesetzes weiterhin auf der Agenda der Koalition. Dass sich darin zumindest die von den Expert_innen eingeforderten klaren Schranken für den Einsatz des Behördentrojaners wiederfinden werden, darf angesichts der Erfahrung mit der letzten Sicherheitspolizeigesetz-Novelle ernsthaft bezweifelt werden.

Kontrollwahn

Aber warum denn auch? Immerhin geht es bei Überwachung im Kern ja ohnehin um etwas ganz anderes: Soziale Kontrolle auszuüben, abweichendes Verhalten "aufzuspüren" und so die eigenen gesellschaftlichen Normen zu zementieren. Kameras werden ja auch nicht wirklich dazu angebracht, um Verbrechen zu verhindern, dazu taugen sie nämlich schlicht nicht. Dies lässt sich leicht am Beispiel England demonstrieren: Dort gibt es mittlerweile Gegenden, die vollständig von Kameras erfasst werden; nach den Argumenten der Überwachungsbefürworter_innen müsste es sich also dort bereits um weitgehend Kriminalitäts-freie Zonen handeln. Doch die Realität sieht anders aus. Denn während die Zahl der Kapitalverbrechen gleich geblieben ist - Überraschung! Mord und Totschlag passieren also tatsächlich in den seltensten Fällen mit jahrelanger genauer Planung, tolle Erkenntnis - sinkt die Bereitschaft zur Zivilcourage - anstatt selbst einzuschreiten, wird sich zunehmend auf die staatlichen Überwacher_innen verlassen und "weg gesehen".

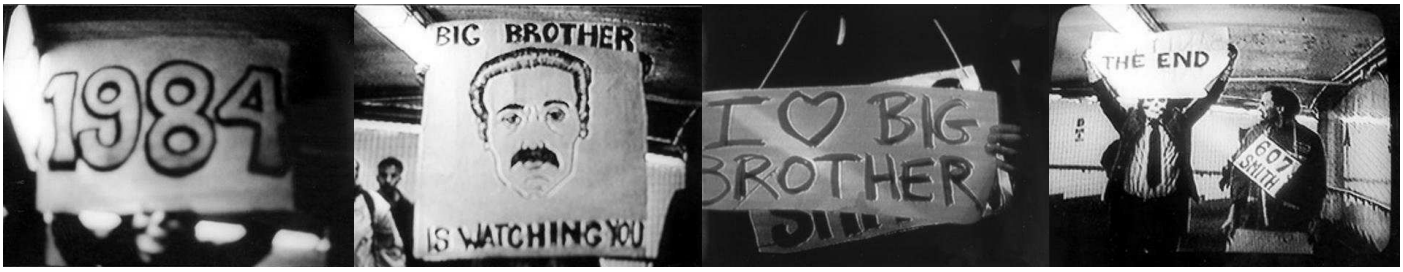
Was aber tatsächlich passiert, ist, dass unerwünschte soziale Phänomene wie skatende Kids, öffentlicher Drogenkonsum und Obdachlosigkeit weiter aus den Innenstädten heraus und an den Rand der Gesellschaft verdrängt werden. Damit zumindest die etwas betuchteren Einwohner_innen und auch der Tourismus nicht durch solche "Unannehmlichkeiten" belästigt werden, so die nicht sonderlich neue aber immer konsequenter umgesetzte Maxime. Angst schüren, um das eigene verlogene Bild der "Idealgesellschaft" auf dem Rücken derer, die sich am wenigsten wehren können, zusammenzulügen.



Doch nicht nur der Staat, auch Unternehmen streben nach immer stärkerer Kontrolle: Betriebe, die die Mails ihrer Angestellten lesen oder gar protokollieren, wann diese wie oft auf die Toilette gehen - etwa um anstehende Schwangerschaften herauszufinden und "rechtzeitig" eine Kündigung auszusprechen - sind bereits trauriger Alltag. Ein besonders eindrückliches Beispiel dafür, wie schnell auch "Durchschnittsbürger_innen" in den Überwachungsfokus kommen können, lieferte vor nicht all zu langer Zeit der Lebensmitteldiskonter Lidl, der seine Angestellten in Deutschland mittels Privatdetektiv_innen und Kameras ausspionieren ließ. Natürlich nur zum "Schutz vor Dieben" wurden hier teilweise recht private Details eifrig mitprotokolliert. Gleich aus mehrfacher Sicht erschreckend auch ein aktueller Vorfall bei der Österreichischen Bundesbahn: Beinahe flächendeckend hatte man hochsensible Krankenstandsdaten illegal abgespeichert, auf diesem Wissen basierend, hatte man dann Mitarbeiter_innen offen drangsaliert, um vermeintliche "schwarze Schafe" mit "vorgetäuschten Krankenständen" aufzuspüren. Doch anstatt diesen Missstand anzuprangern, änderte die Diskussion in Windeseile ihren Fokus, nicht die Überwachung der Mitarbeiter_innen sondern die Verdammung des angeblichen "Krankfeierns" rückte in den Mittelpunkt des öffentlichen Interesses. Als nächster Schritt dann, dass was in solchen Fällen immer in Österreich folgen muss: Die Suche nach dem "Verräter" schließlich ist ja hierzulande noch immer nicht der Skandal sondern dessen Aufdecker_in das Problem.

Kameras, immer und überall

Gerade die Kamerüberwachung feiert momentan aber ohnehin in so ziemlich allen Lebensbereichen einen zweiten Frühling. So verwundert es nicht, dass gleich mehrere Schulen Kameras in den Gängen anbringen wollen. Vorerst natürlich "nur" für schwere Delikte ("Laufen auf dem Gang"?, Butterbrotklau?), die Realität in anderen Ländern zeigt jedoch, dass, einmal angebracht, schnell die "Wünsche" nach einem breiteren Einsatz folgen. So gibt es in England bereits Forderungen, die Kameras auch gegen das "Schummeln"



bei Prüfungen einsetzen zu dürfen, in den USA sind teilweise bereits Kameras auf den Toiletten zu finden - der Kampf gegen den Drogenhandel muss hier argumentativ herhalten.

Schule, Arbeit und öffentlichen Raum hatten wir ja schon, da darf der Privatbereich natürlich nicht zurückstehen: So hat die Stadt Wien vor nicht all zu langer Zeit die Überwachung von Müllanlagen und Garagen in acht Wiener Gemeindebauten gestartet. Die Bekämpfung von "Vandalismus" soll es in diesem Fall Wert sein Dinge des privaten Alltags unter die Kamerakontrolle zu stellen. (Na? Wieder mal nicht ordentlich Müll getrennt? Bist du sicher, dass die Menschen hinter der Kamera das wirklich nicht interessiert?)

Nichts zu verbergen?

Überwachung durchdringt mittlerweile alle Bereiche unseres Lebens: Sei es der Arbeitsplatz, sei es unser Gesundheitszustand - alles wird mehr und mehr erfasst und ausgewertet, mit unklaren Auswirkungen auf die Zukunft. Dem werfen Überwachungsbefürworter_innen gerne den Stehsatz "Wer nichts zu verbergen hat, hat nichts zu befürchten" entgegen. Doch dieser ist so einfach, wie verheerend falsch. Nicht nur, dass er einer vollständigen Selbstaufgabe der Privatsphäre gleichkommt, wer weiß denn schon, was in ein paar Jahren als "verwerfliche" Tat oder Eigenschaft angesehen wird? (Nur so zu Erinnerung und als Beispiel: Vor nicht all zu langer Zeit gab es in diesem Land noch eine Reihe von Paragraphen gegen Homosexualität.) Wer will, dass die nächsten Arbeitgeber_innen wissen, dass mensch mal ein Alkoholproblem oder auch gesundheitliche Schwierigkeiten hatte? Wer will, dass die eigenen sexuellen Vorlieben offen gelegt werden? Nichts zu verbergen? Wirklich? Sollen wir dagegen wetten?

Vergessen sollte dabei auch nicht werden, dass aktuell uninteressante Daten in der Zukunft schnell mal "relevant" werden können. Sei es bei einem Regimewechsel oder auch "nur" bei Gesetzesverschärfungen, Informationen, die einmal gesammelt wurden, werden dann auch genutzt werden. Darauf können wir uns wohl alle "verlassen". Auch schreit die allgegenwärtige Überwachung geradezu nach ihrer kommerziellen "Zweitverwertung". Schon jetzt gibt es eine Reihe von Firmen, die sich auf den Verkauf von ausgearbeiteten Profilen über einzelne Konsument_innen spezialisiert haben, eine Branche, die mit den zunehmenden Informationen aus staatlicher und privater Überwachung wohl nicht gerade an Bedeutung verlieren wird.

Ein Punkt bei dem wir uns aber auch alle an der sprichwörtlichen eigenen Nase nehmen müssen: Immerhin sind es gerade all die ach-so-verlockenden Vorteilskarten, über die massiv Informationen über unser Konsumverhalten - und damit auch über unsere Lebensverhältnisse - gesammelt werden. Auch die oft recht unbedarfte Weitergabe von persönlichen Informationen auf diversen Online-Plattformen macht es Unternehmen und staatlichen Behörden wesentlich einfacher, einen recht tiefen Einblick in unser aller Privatleben zu bekommen.

Stopp!

Trotzdem gilt zunächst mal: Was wir tun, geht nur uns selbst und sonst niemanden etwas an. Was wir mitteilen wollen, ist unsere persönliche Angelegenheit und nicht die von Möchtegern-alles-wissenden Behörden. Bei all der aktuellen Überwachungsmanie stellt sich oft die simple Frage: Wie hat die Menschheit eigentlich bisher überlebt?

Herausgestrichen sei, dass der vorliegende Text natürlich nur einen relativ kleinen Ausschnitt aus der gesamten Überwachungsthematik bieten kann. All zu umfangreich sind gerade aktuell die Wunschlisten der staatlichen Behörden, mit denen sie ihr Arsenal an Spitzelmöglichkeiten aufrüsten wollen.

Bunt statt paranoid!

Aber um es abschließend noch mal klar auszusprechen: Es geht bei all diesen Maßnahmen um Kontrolle. Eine Kontrolle, die keinen Platz für Freiheit, Individualität und Kritik zulässt. Und genau diesen Bestrebungen gilt es entschieden entgegenzutreten, für eine bunte Gesellschaft jenseits von normierenden Allmachtsvorstellungen und steter Paranoia.

{rosa antifa wien}

Stand: September 2009

Kontakt-Infos

elektronisch:
http://www.raw.at / raw@raw.at
https://www.n3tw0rk.org (Diskussionsboard)

postalisch:
Rosa Antifa Wien
c/o Rosa Lila Tip
Linke Wienzeile 102
A-1060 Wien