

Stellungnahme zur Vorratsdatenspeicherung 117/ME (XXIV. GP)

Die Vorratsdatenspeicherung greift grundlegend in die Privatsphäre jedes Bürgers ein und ist grundsätzlich abzulehnen.

Die Umsetzung der Vorratsdatenspeicherung bedeutet, alle Bürger unter Generalverdacht zu stellen, unabhängig davon, ob sie tatsächlich straffällig geworden sind oder nicht. Dieser Grundrechtseingriff ist abzulehnen und unverhältnismäßig!

Jedem, auch ohne speziellem Fachwissen, ist es möglich, die Vorratsdatenspeicherung zu umgehen. Schon alleine durch Wertkartenhandys und Wertkarteninternet ist es möglich, die Vorratsdatenspeicherung auszuhebeln. Wenn also jemand terroristische Zwecke verfolgt wird es wohl keine Rolle spielen, ob diese Person 1 Cent beim Vertragstarif oder 1 Euro beim Wertkartentarif pro Minute oder MB bezahlt.

Sollten jetzt also Wertkartenhandys verboten werden? Man darf nicht vergessen, dass es Personen gibt, welche, aus welchen Gründen auch immer, keinen Vertrag bekommen. Diesen bleibt nur der Weg über eine Wertkarte zu telefonieren. Auch möchte man, wenn man zB in einem Internetforum oder auf einer Seite für Partnersuche seine Telefonnummer angibt, eine anonyme Nummer haben. Denn es wäre ja auch ein Leichtes für Mitarbeiter des jeweiligen Telefonunternehmens, welcher rein zufällig auch auf Partnerschaftssuche ist, die Nummer zu „checken“.

Was kommt nach dem Verbot für anonyme Wertkarten? Ein Verbot von Partnerkarten. Dies ist das nächste Problem. Jeder, der Familienangehörige oder Freunde in seinem Vertrag als Partnerkarte hat, könnte Probleme bekommen. Der Provider weiß ja nicht, wer diese Nummern nützt. Er kennt nur den Vertragspartner. Und ob dieser nun eine oder zwei oder gar vier Nummer nützt, ist dem Mobilfunkanbieter nicht bekannt und geht eigentlich auch niemanden etwas an. Kommt dann eine Ausweispflicht für Partnerkartenbenutzer? Oder muss man sich dann im Zuge eines Verdachtes rechtfertigen, warum man nicht nur eine sondern mehrere Mobiltelefone (SIM-Karten) nutzt?

Schon alleine, wenn jemand in Verdacht gerät, geraten alle, welche mit dieser Person kommuniziert haben, unter Generalverdacht. Muss man also von jedem, bevor man eine Verbindung aufbaut, neben einem Strafregisterauszug, einen Auszug aus diversen Listen (Exekutionsregister, Klageregister, Melderegister, kriminalpolizeilichen Aktenindex, usw) verlangen, damit man weniger Angst haben muss, in Generalverdacht zu gelangen? Das verhindert soziale Kontakte. Kann ich wirklich wissen, dass mein bester Freund kein Drogendealer ist. Oder, dass eine Freundin nicht Kontakt zu einem Drogendealer hat und manchmal gerne kiff, was sie mir leider immer noch nicht gesagt hat, weil sie einfach nicht teilen will und ich heute davon erfahren habe, als man mich bei einer polizeilichen Einvernahme gefragt hat, warum ich mit der Verdächtigen Kontakt habe und was ich von ihr gekauft habe?

Ziel dieser EU-Richtlinie ist, Terrorismus und organisierte Kriminalität zu bekämpfen. Mit dem vorliegenden Entwurf jedoch werden auch andere Straftaten, welche auch ohne die Vorratsdatenspeicherung aufgeklärt werden können, einbezogen.

Sind diese Daten erst einmal gespeichert, werden auch andere an ihnen interessiert sein. Es ist auch nicht Aufgabe des Staates, Urheberrechtsverletzungen für die Privatwirtschaft zu verfolgen. Auch Ladendiebstähle werden von Kaufhausdetektiven verfolgt und erst, wenn jemand erwischt wird, die Exekutive verständigt. Auch die Aufgabe der Überwachung von Kaufhäusern übernimmt nicht der Staat. Weshalb soll es also für die Unterhaltungsindustrie eine Ausnahme geben. Es sollte allerdings angemerkt werden, dass die Privatkopie in Österreich zulässig ist, das alleinige Herunterladen ohne einen Upload eines urheberrechtlich geschützten Musikstückes oder eines Filmes zu ermöglichen also nicht verboten ist. Und sind illegale Downloader tatsächlich Verbrecher, wie es uns die Musik- und Filmindustrie weiß machen will? Höchstens, wer sie gewerblich verkauft, ist ein Gesetzesbrecher (Vergehen), aber sicher kein Verbrecher. Oder sind Raubkopierer, welche gar nicht rauben, Terroristen und müssen mitberücksichtigt werden? Natürlich, gewerbliche „Raubkopierer“, welche damit Geld verdienen, sollten zur Verantwortung gezogen werden. Für die Aufklärung jedoch sind die Urheberrechtseigentümer selbst verantwortlich. Und wenn ein Fotograf seine Bilder veröffentlicht, egal ob im Internet oder nicht, und dann werden Bilder ohne Zustimmung anderweitig veröffentlicht, muss er auch selbst, und zwar auf zivilrechtlichem Weg mit enormen Kostenrisiko, dieses

Unrecht abstellen. Hier hilft auch nicht der Staat auf Kosten der Allgemeinheit.

Nicht zuletzt kann ein Datenmissbrauch nicht ausgeschlossen werden.

Schon alleine die Tatsache, dass es in der Vergangenheit genügend Fälle von Datenmissbrauch von öffentlichen Stellen gegeben hat, sollte ein Umdenken bewirken.

Man darf auf den Fall der Familie Zogaj hinweisen, wo Mitarbeiter des Innenministeriums sensible Daten aus dem EKIS veröffentlicht haben, ohne Konsequenzen befürchten zu müssen.

Oder die Wiener Linien GmbH & Co KG, welche in der jüngeren Vergangenheit durch Datenmissbrauch aufgefallen ist. Darüber hat hauptsächlich die staatliche Wiener Zeitung berichtet.

Auch die Österreichische Post AG hebt sich durch eine übertriebene Auslegung der Richtlinie gegen Geldwäsche ab. Wer eine Nachnahmesendung erhält muss – mehr oder weniger – einen Datenstrip hinlegen. Es wird sicher viele geben, welche über eine Nachnahmesendung Geldwäsche betreiben. Ebenso verhält es sich bei einem Nachsendeauftrag.

Doch auch das Berufsförderungsinstitut (BFI) Wien, das arbeiterkammer- und gewerkschaftsbundnahe ist, ist keine Ausnahme: Ohne Angabe der Sozialversicherungsnummer ist es nicht möglich, einen Kurs zu besuchen. Selbst, wenn man ihn sofort im Vorhinein bezahlt.

Doch auch die Wiener Polizei hat so ihre Methoden. So wird bei Verdächtigen, sei es nun wegen eines Fahrlässigkeits- (zB Verkehrsunfall) oder eines Vorsatzdeliktes, zur Handynummer, welche stets verlangt wird, auf den Personalblättern festgehalten, ob es sich um ein „Wertkartenhandy“ oder ein „angemeldetes“ Handy handelt. Warum dies erhoben wird ist nicht ersichtlich und überschreitet eindeutig die Kompetenzen. Es zeigt jedoch, wie auch die Stellungnahme des Innenministeriums zur Vorratsdatenspeicherung zeigt, dass man möglichst viel wissen will und die Vorratsdatenspeicherung auch noch ausgeweitet gehört. Vielleicht sollte man über einen RFID-Chip nachdenken, der einfach jedem ohne sein Wissen mit einer Grippeimpfung eingepflanzt wird.

Es hat daher den Anschein, dass man möglichst viel über seine Kunden und Bürger wissen will – egal ob es nötig ist oder nicht. Anders ist auch nicht zu erklären, weshalb bei Spenden dem Spendenempfänger vom Spender seine Sozialversicherungsnummer bekannt gegeben werden muss.

Doch auch die Rasterfahung beim Saliera-Diebstahl, gerne auch als „Raub“ bezeichnet, hat nicht zur Aufklärung beigetragen.

Auch darf auf die illegalen Abfragen aus dem Melderegister hingewiesen werden. Selbst Anwälte haben illegal Daten aus dem Exekutionsregister an Wirtschaftsauskunftsdiensten weitergegeben, woraufhin dann doch noch im Vorjahr die direkte Abfrage abgeschafft wurde. Dies hat jedoch nichts daran geändert, die Anwälte stellen jetzt halt einfach Anträge bei Gericht und erhalten diese Informationen nun sogar kostenlos und wieder ohne Probleme.

Auch die Nichtinformation der Betroffenen muss überdacht werden. Wenn die Vorratsdatenspeicherung schon kommt sollte sie auch nur den Zweck „Terrorismus und organisierte Kriminalität“ beinhalten und nicht darüber hinausgehen. Der Betroffene ist nach Abschluss des Verfahrens, sofern es nicht zu weiteren Schritten kommt, darüber zu informieren.

So eine Regelung sollte es auch betreffend dem Zentralen Melderegister geben. Ein Mal im Jahr sollte jeder Meldepflichtige davon in Kenntnis gesetzt werden, wer über ihn Daten abgerufen hat, unabhängig davon, ob es eine Behördenabfrage oder eine private war. So könnte ein möglicher Datenmissbrauch eingeschränkt werden.

Es soll ja immer wieder vorkommen, dass Behördenmitarbeiter (zB Polizisten) zB die neuen Freunde ihrer Exfreundinnen oder die Exfreundin im ZMR „googeln“. Durch die Anzeige des Unterkunftsgebers ist es ein leichtes, weitere „Nachforschungen zu privaten Zecken auf Kosten der Steuerzahler“ zu tätigen. Auch die Anzeige der Standarddokumente sollte wieder abgeschafft werden. Ebenfalls ist nicht ersichtlich, weshalb ein Familienstand im ZMR gespeichert wird. Dies wurde ja auch nicht über die Meldegesetze sondern über die e-Commerce-Gesetze, also über die Hintertür eingeführt.

Seit der Familienstand, nun sogar um „verpartnerte“ Paare erweitert, im ZMR gespeichert wird sehen sich auch die Familiengerichte bei Scheidungen veranlasst, ohne Rechtsgrundlage die Scheidungsurkunde dem ZMR im Wege der lokalen Meldebehörden zu übermitteln.

Selbst die Möglichkeit, auf den Meldezetteln ein Feld „Religionsbekenntnis“ anzubringen zeigt, wie unsensibel

die Verantwortlichen umgehen. Viele füllen Formulare einfach aus, weil es halt da steht. Hierzu sollte angemerkt werden, dass man das Religionsbekenntnis, auch die Tatsache, dass man ohne religiösen Bekenntnis ist, nicht angeben muss.

Dafür hat man sich halt den Familienstand einfallen lassen. In Wien gibt es Meldebehörden, welche vom Meldepflichtigen einen Ausweis verlangen und diesen sogar kopieren! Dafür fehlt die gesetzliche Regelung. Auch sind auf einer kompletten Ausweiskopie Daten wie Augenfarbe oder Körpergröße enthalten, welche auch die Meldebehörden nichts angehen. Oder sollen diese Daten auch bald gespeichert werden?

Auch mit Inkrafttreten der Novelle zum Sicherheitspolizeigesetz, welche in einer Nacht-und-Nebel-Aktion beschlossen wurde, haben sich die Abfragen exorbitant mehr als erhöht! Sind plötzlich die Hälfte der Österreicher in Bergnot geraten? Es war ja der Sinn, in Bergnot geratene zu finden! Wie da auch noch IP-Adressen oder Festnetzanschlüsse hineinpassen ist mehr als schleierhaft.

Das ZMR, die zunehmende Videoüberwachung, die Bildungsdokumentation und die Vorratsdatenspeicherung sind geeignet um sagen zu können, dass die Republik Österreich am Wege zu einem totalitären Staat ist. Es sollte uns aber die Vergangenheit lehren, einen anderen Weg einzuschlagen.

Die Vorgänge rund um die Totalüberwachung der (unbescholtenen) Bürger geht sogar soweit, dass es alles Dagewesene in der DDR in den Schatten stellt.

Immer mehr neue Register werden geschaffen: Fluggastregister, damit jede Behörde weiß, wer wann mit wem wohin fliegt. Alleine diese Daten auszuwerten und mit anderen zu verknüpfen, wird enorm aufwändig und kostenintensiv. Die Bürger bezahlen ihre eigene Überwachung!

Man sollte sich bewusst sein, wer das Melderegister eingeführt hat. In den Niederlanden, eines der ersten Länder mit Melderegister, hatten die Nationalsozialisten ein leichtes Spiel, aufgrund der Meldedaten „unerwünschte“ Personen zu finden. Man musste nur noch in die jeweiligen Gemeindeämter marschieren und schon wurde man fündig. Und was dann mit diesen „Personen“ geschah ist hoffentlich jedem klar.

Heute muss man nirgendwo mehr hingehen. Ohne sein Zimmer verlassen zu müssen kann man dann auf Knopfdruck feststellen, wer bei wem mit wem wo wohnt, was wer verdient (Versicherungs- und Steuerdaten) und wer mit wem kommuniziert. Wenig später wird dann auch noch der ELGA, der elektronische Krankenakt einbezogen. Dann kann man sogar auf den Gesundheitszustand schließen. Und mit dem Bildungsregister kann man nicht nur auf die Bildung, sondern auch gleich auf das Religionsbekenntnis (es könnte ja jemand am Meldezettel nicht angeben) schließen und wer eine Lernschwäche hat und Förderunterricht brauchte.

Von Österreich und seinen Bewohnern geht keine Gefahr aus (manche Politiker ausgenommen). Auch sollte nicht vergessen werden, dass der Wille in Österreich vom Volk ausgeht!

Gerät man nun, wenn das Gesetz in dieser oder sogar noch bürger(rechts)feindlicheren Form beschlossen wird, in einen Verdacht und stellt sich auf Knopfdruck heraus, dass der Verdächtige wenig Bildung und noch dazu Krebs hat, mit Veganern oder Tierschützern bzw Tierrechtlern Kontakt hält, ist es wohl eindeutig: Der hat nichts mehr zu verlieren, ist militant und ist somit dringend tatverdächtig und muss schleunigst, am besten ohne Gerichtsverhandlung, zum Schutze der Allgemeinheit eingesperrt werden und ein Flugverbot verhängt werden.

Auch das Bürgerkartenprojekt ist nicht umsonst gescheitert. Die Bürger brauchen keine Karte, welche mit einer ZMR-Anbindung mit dem Innenministerium kommuniziert. Auch kann nicht ausgeschlossen werden, dass über die „Bürgerkartenumgebung“, also die Software, um die Bürgerkarte nutzen zu können, ohne Wissen des Betroffenen ein „Bundes-Trojaner“ eingeschleust wird.

Dennoch versucht man weiterhin, die Bürgerkarte den Bürgern im wortwörtlichen Sinn aufs Aug zu drücken. E-Voting soll bequem sein. Ohne aufstehen zu müssen wählen gehen. Klingt ja nicht schlecht.

Bewerbungen im Bereich des Bundeskanzleramtes sind ohne Bürgerkarte gar nicht mehr möglich. Es ist nur noch die Online-Bewerbung mit Bürgerkarte gewünscht. Auch das ist nur ein Versuch, die Bürgerkarte zu verbreiten. Der Nutzen dieser Karte ist äußerst gering.

Ein weiterer, eindeutiger Datenmissbrauch ist jener der Bezirkshauptmannschaft Mödling. Der Einspruch betreffend einer Strafverfügung, wengleich auch etwas unglücklich formuliert, wurde mit vollem Namen und

Unterschrift eingescannt und über E-Mail an halb Österreich versandt. Jeder Empfänger konnte somit nicht nur den Einspruch, sondern auch die Daten wie Name und Anschrift der Beschwerdeführerin lesen. Da ein Eingangsstempel der Bezirkshauptmannschaft Mödling angebracht ist ist anzunehmen, dass von einem Mitarbeiter dies veröffentlicht wurde.

Doch das ist noch nicht alles: Die Eingabe der Dame, welche ein Transportunternehmen betreibt, wurde als Anhang versendet. Und in das E-Mail wurde von verschiedenen Leuten folgendes hinzugefügt: „lebt in Scheidung“, „hatte schon einige VUs [Verkehrsunfälle]“, „verdient 500 Euro am Tag und soll sich nicht aufpudeln“ hinzugefügt. Jetzt stellt sich natürlich die Frage, woher kommen diese Informationen? Wer hat da was abgerufen?

Doch die Vorratsdatenspeicherung ist erst der Anfang: Es gibt bereits Pläne, wonach auch die Abrechnungsmodalitäten (wie bezahlt der Kunde? Bar, Bankomt, Einzug, Zahlschein,...) erfasst werden soll!

Interessant erscheint, dass bereits am Morgen des letzten Tages der Begutachtungsfrist im ORF-Text auf Seite 115 zu lesen war, dass die Vorratsdatenspeicherung in dieser Form bereits im Frühjahr beschlossen werden wird. Es erscheint, als ob dies bereits ausgemacht ist und dieses Begutachtungsverfahren eine Farce ist und die Einwendungen von Bürgern und Experten nicht ernst genommen werden.

Die hier beispielhaft angeführten Missbrauchsfälle zeigen auf, wie gefährlich es ist, die Vorratsdatenspeicherung einzuführen. Neben dem problematischen Grundrechtseingriff, der in keinsten Weise gerechtfertigt ist, bringt die Vorratsdatenspeicherung mehr Gefahren eines Datenmissbrauches als Nutzen zur Terrorismusbekämpfung. Auch, dass alle Bürger mehr noch als bisher unbegründet und unverhältnismäßig unter Generalverdacht stehen dreht die Unschuldsvermutung um. Jeder ist erst dann schuldig, wenn seine Schuld rechtskräftig bewiesen ist.

Es ist somit nicht nur die Vorratsdatenspeicherung abzulehnen sondern ist auch die Novelle zum Sicherheitspolizeigesetz (Stichwort Bergsteiger mit Festnetz in Bergnot) rückgängig zu machen.

Auch ist es nicht einzusehen, weshalb die Bürger im Rahmen der Steuerleistung und der Entgelte für die Diensteanbieter die von ihnen nicht gewollte Überwachung selbst bezahlen müssen. Auch wird damit höchstens das subjektive Sicherheitsgefühl erhöht.

Auch schließe ich mich den Ausführungen der ARGE Daten an.

Im Übrigen bin ich der Meinung, dass die Republik Österreich in „Demokratische Republik Österreich“ umbenannt werden sollte!



Data-Retention: Geheimdienste wollen mehr - futurezone.ORF.at

Kategorie: KONTROLLE | 23.11.2009 | Erstellt um 06:00 Uhr

Während in Österreich noch über den Gesetzestext zur Einführung der Vorratsdatenspeicherung diskutiert wird, arbeiten Polizei und Geheimdienste im Telekom-Standardisierungsinstitut ETSI bereits eine neue Serie von "optionalen" Datenfeldern in den Überwachungsstandard ein: Einzelabrechnungen, Bankverbindung, Volumen von Up- und Downloads. Sie wollen alle Details über die Bewegungen der Bürger in den Netzen erfassen.

"Über Österreich merkte der Vorsitzende an, dass nun etwas Bewegung zur nationalen Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung zu erkennen sei", heißt es im Sitzungsprotokoll. Die zugehörige Sitzung der ETSI-Arbeitsgruppe SA3-LI ("Lawful Interception") fand von 3. bis 5. November in Scottsdale (US-Bundesstaat Arizona) statt.

Nachdem nun auch Österreich nach langer Verzögerung die EG-Richtlinie zur Vorratsdatenspeicherung umsetzt, dürften die Erfinder der Überwachungsstandards sehr zufrieden sein. Denn sie planen bereits die umfangreiche Ausweitung der verdachtsunabhängigen Speicherung sämtlicher Telefonverbindungs- und Handystandortdaten.

Der Vorsitzende des übergeordneten Technischen Komitees TC LI, Peter van der Arend, gab in Scottsdale bekannt, dass für die in Arbeit befindliche technische Spezifikation zur Vorratsdatenspeicherung erneut eine Reihe von Ergänzungen, Zusätzen und Abänderungsanträgen eingetroffen seien, die nun eingearbeitet würden.

Angeschwollen 1.5.1

Man sei gerade dabei, die Version 1.5.1 auszuarbeiten, teilte Van der Arend den nach Arizona angereisten Mitgliedern der Arbeitsgruppe mit.

Schon die derzeit kursierende Version 1.3.1 vom September mit dem Titel "Gesetzmäßige Überwachung (LI), Umgang mit Vorratsdaten und Übergabe-Schnittstelle für Anforderung und Übergabe der Daten" zeigte sich gegenüber den ersten Entwürfen stark angeschwollen. Die technische Spezifikation umfasst bereits 89 Seiten - und laufend kommen neue Datenfelder hinzu, die in der aktuell gültigen EG-Richtlinie 2006/24/EG überhaupt nicht genannt werden.

Der PUK-Code

Alleine im Abschnitt B 2.2.4.1, den "Subscribed Telephony Services", kam ein Dutzend solcher "optionaler Parameter" dazu: Anbindung, Art und Zeitdauer des Kundenvertrags, geografischer Ort von beim Kunden installierten Geräten, eine Liste der IMEI- und MAC-Adressen aller vom Provider gestellten Endgeräte. Und falls es sich denn um ein Service handelt, das mit einer SIM-Card betrieben wird, hätten die Überwacher gerne auch die PUK-Codes des betreffenden Endgeräts dazu.

PUK ist der "Pin Unlock Key", der anders als der PIN-Code nicht vom Besitzer des Handys verändert werden kann. Über den PUK erlangt man volle Kontrolle über das betreffende Endgerät und kann es nach Belieben manipulieren.

Umsetzung in Österreich

Das Infrastrukturministerium legte am Freitag den Entwurf zur Änderung des Telekommunikationsgesetzes vor, mit dem die EG-Richtlinie zur Vorratsdatenspeicherung (Data-Retention) umgesetzt werden soll. Die Koalition streitet noch darüber, ob die Polizei auch ohne Anlass jederzeit auf die IP-Adressen aller Bürger zugreifen darf. In der Vorratsdatenspeicherung werden alle Handystandort- und Verbindungsdaten aller Bürger verdachtsunabhängig für sechs Monate gespeichert.

- Data-Retention: Gesetzesentwurf liegt vor (<http://futurezone.orf.at/stories/1632296/>)
- Data-Retention: Anwälte für Minimalvariante (<http://futurezone.orf.at/stories/1631282/>)

Bankverbindungen, P2P

Vom nächsten Abschnitt B 2.2.4.2, den "Abrechnungsdetails", die in der EU-Richtlinie zur Vorratsdatenspeicherung überhaupt nicht vorkommen, sind Datenfelder für Einzelabrechnungen des Providers vorgesehen samt Einzahlungsort und Zeitpunkt, Währung und Zahlungsart des betreffenden Kunden.

Auf diese Weise kommt auch die Bankverbindung zum Datenkonvolut dazu.

Im Annex E 2.4 zum Thema "Netzzugang" - laut EU-Richtlinie müssen nur Ort und Zeit der Einwahl, benutzte IP-Adresse sowie Dauer der Verbindung gespeichert werden - wünscht man sich noch ein paar weitere Informationen dazu. Zum Beispiel den Benutzernamen für das Log-in und den Umfang des dann abgewickelten Datenverkehrs, übersichtlich in Up- und Downloads gegliedert.

Geheimdienste schreiben die Standards

Dass ein technisches Regelwerk wie jenes zur Vorratsdatenspeicherung so weit über die Vorgaben der EU-Richtlinie hinausschießt, erklärt sich zum Teil aus der Genese dieser technischen Spezifikationen.

6 von 13

105/SN-117/ME XXIV. GP - Stellungnahme zum Entwurf elektronisch übermittelt

Für sie zeichnet nämlich das National Technical Assistance Center (NTAC) verantwortlich, eine Schnittstelle im britischen Innenministerium zum Inlandsgeheimdienst MI5, aber auch zum militärischen General Communication Headquarters (GCHQ).

Über das NTAC laufen auch sämtliche Polizei- und Gerichtsanfragen zur Entschlüsselung abgefangener oder beschlagnahmter Daten. Das dafür nötige Know-how aber ist ebenso wie die formale Zuständigkeit in Cheltenham beim GCHQ angesiedelt.

Eskalierendes Muster

Und weil im Technischen Komitee TC-LI bzw. der Arbeitsgruppe SA3LI die Vorgaben vom niederländischen Gegenstück zum britischen NTAC namens PIDS (Platform Interceptie Decryptie en Signaalanalyse), dem deutschen Bundesverfassungsschutz sowie Innenministeriumsbeamten aus Frankreich stammen, ist die Wunschliste insgesamt derart angeschwollen.

Sie spiegelt ziemlich genau wider, nach welchem Muster die Überwachung der Netzwerke im Wechselspiel zwischen Politik, Geheimdiensten und Polizei in den letzten zehn Jahren eskaliert.

Wenn es nach einigem Hin und Her wie im Fall der Richtlinie zur Vorratsdatenspeicherung schließlich zu einer Einigung kommt, sind die radikalsten und überschießendsten Ansätze, die in der Regel aus England und/oder Frankreich kommen, darin abgemildert, schaumgebrems oder gar nicht enthalten.

Einschlägige Links

Etwas aufschlussreicher als die Links zu den offiziellen ETSI-Pages sind jene zu Sites von Dritten, die etwa direkten Zugang zu allen einschlägigen LI-Dokumenten und ETSI-Standards auf Chinesisch bieten. Auszug aus einer Linksammlung, die von den Studenten des Studiengangs Medientechnik der FH St. Pölten beige stellt wurde.

- ETSI-Überwachungsstandards auf Chinesisch (http://www.ptsn.net.cn/standard/std_query/show-etsi-23341-1.htm)
- Direkter Zugang zu den LI-Standarddokumenten (<http://www.tech-invite.com/Ti-etsi-standards-LI.html>)
- ETSI TC LI historisch: Der Griff der Geheimdienste nach dem Internet (<http://www.heise.de/tp/r4/artikel/7/7447/1.html>)
- Offizielle Page zum Data-Retention-Standard (http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31485)
- ETSI TC LI offiziell (<http://www.etsi.org/Website/Technologies/LawfulInterception.aspx>)
- National Technical Assistance Center (<http://security.homeoffice.gov.uk/ripa/encryption/ntac/>)

Optionale Revision der Politik

Sodann beginnt ein von den oben genannten Institutionen besetztes Subkomitee, die technischen Anforderungen der Überwacher auszuformulieren. Das geschieht vorerst einmal entlang dem Buchstaben der Richtlinie, dann kommen die Sonderwünsche an die Reihe.

Nach und nach wird dann in ein- und denselben Überwachungsstandard, der sich auf eine EU-Richtlinie beruft, all das hineingeschrieben, was in den EU-Gremien nicht konsensfähig war.

Bis auf drei, die etwas mit Richtlinienetext zu tun haben, werden denn auch sämtliche neuen Felder zur Vorratsdatenspeicherung in der Version ETSI TS 102 657 1.3.1 als "optional" eingestuft. Die technische Voraussetzung ist damit gegeben, dass auf nationaler Ebene genau das umgesetzt werden kann, was in EU-Gremien keine Mehrheit fand.

Russische Verhältnisse

Am 1. Dezember trifft der harte Kern der LI-Überwacher auf Einladung der British Telecom im walisischen Cardiff zusammen, bereits am 9. Februar ist wieder ein reguläres Treffen angesagt, diesmal in Rom.

Ein weiteres Anzeichen für die Globalisierung der Vorratsdatensammelwut ist das für 2010 geplante Treffen in St. Petersburg. Schließlich ist das einladende Russische Zentralinstitut zur Erforschung und Entwicklung der Kommunikation (ZNIIS) ein "Stakeholder" im "Lawful Interception"-Komplex des ETSI. Das ZNIIS kann seit Jahren im Technischen Komitee TC LI jederzeit Abänderungsanträge für neue Überwachungsoptionen einbringen.

(futurezone/Erich Moechel)

Bezirkshauptmannschaft Mödling
Poststelle

- 5. Mai 2009

Daniela T. [REDACTED]

Kennz.:

Beilagen.

Stempel:



Bezirkshauptmannschaft Mödling
Bearbeiterin: Frau Walcher
Bahnstrasse 2
2340 Mödling

0911664

Betreff: VERWALTUNGSSTRAFVERFAHREN - EINSPRUCH

Sehr geehrte Frau Walcher,

haben Sie faule Schweine nichts anderes zu tun als arbeitende Menschen zu sikkieren und abzuzocken??

Ich soll 80.- Euro zahlen weil ich über eine LINIE gefahren bin?

Ich will den Beweis sehen !!!!!!!!!!!

Wissen Sie eigentlich Sie faule BRUT in der BEZIRKSHAUPTMANNNSCHAFT dass ich als Transportunternehmerin für jeden Kunden den ich verfahre von der DHL 27.- Euro erhalte, egal wohin ich liefern muss, egal wie viel KILO!!!

Das bedeutet ich habe jetzt 3 Kunden umsonst verfahren nur weil ich über eine LINIE gefahren bin??? Ihr seid doch alle nicht mehr ganz dicht im Kopf!! Wo ist da das Verhältnis!!!! ????

Ich habe 2 Patenkinder die mich 28.- Euro im Monat kosten. Diese armen Kinder leben davon 3 Monate!!!

Mein Mann musste schon seine Firma schließen weil iHr Bürokratenarschlöcher nichts anderes zu tun habt als UNTERNEHMER in ihrer Arbeit zu stören.

In diesem Land ist man schon ein Verbrecher wenn man eine LINIE überfährt!! Aber wissen Sie was. Ich setze mich gerne 26 Stunden in die HÄFN. Da habe ich mal Urlaub uns SIE SCHEIß STAAT zahlen mal für mich!!!

Und ernähren mich!! Da habe ich endlich mal Zeit ein Buch zu lesen und Fern zu schauen so wie Sie fette Schweine es jeden TAG auf meine Kosten tun!!

Nicht nur ich immer nur für EUCH SCHMAROTZER!!!

Sagen Sie mir Bescheid wo ich in die HÄFN gehen soll. Ich bin bereit.

Sie sehen von mir keinen CENT mehr.

Sie glauben wohl ich stehe jeden Tag auf nur um EUCH MADEN ZU ERNÄHREN!!

Sie glauben wohl ich hab nichts anderes zu tun als auf die Post zu fahren und Eure idiotischen Strafen abzuholen=????????

Der liebe Teufel lacht sich tot wenn er sieht was wir hier auf Erden fabbrizieren!!!

Daniela T. [REDACTED]

[REDACTED]

BEHÖRDENANFRAGE

aus dem Zentralen Melderegister

ANFRAGEDATEN

Familienname:

Vorname:

Geburtsdatum:

 [REDACTED]
 N [REDACTED]
 [REDACTED].19[REDACTED]

Im Zentralen Melderegister scheinen folgende Meldedaten auf:

[REDACTED] N [REDACTED] [REDACTED] 19[REDACTED] ZMR-Zahl [REDACTED] Akad. Grad [REDACTED] Familienname [REDACTED] Vorname N [REDACTED] Name vor 1. Ehe [REDACTED] Staatsangehörigkeit Bosnien und Herzegowina Auskunftssperre [REDACTED] Reisedokumente Reisedokument-Art Reisepass Ausstellungsstaat Bosnien und Herzegowina Ausstellungsbehörde [REDACTED] Reisedokument-Art Reisepass Ausstellungsstaat Bosnien und Herzegowina Ausstellungsbehörde [REDACTED] Standarddokumente Dokumentart Heiratsurkunde Ausstellungsstaat Bosnien und Herzegowina Ausstellungsbehörde [REDACTED] Dokumentart Geburtsurkunde Ausstellungsstaat Bosnien und Herzegowina Ausstellungsbehörde [REDACTED] Tagesdatum: [REDACTED].200[REDACTED] Uhrzeit: [REDACTED] Seite: 1 von 3	Geschlecht Männlich Familienstand unbekannt Geburtsdatum [REDACTED].19[REDACTED] Geburtsstaat Bosnien und Herzegowina Geburtsbundesland [REDACTED] Geburtsort L [REDACTED] Zugezogen von [REDACTED] Verzogen nach [REDACTED] Dokumentnummer [REDACTED] Ausstellungsdatum [REDACTED] Ablaufdatum [REDACTED] Dokumentnummer [REDACTED] Ausstellungsdatum [REDACTED] Ablaufdatum [REDACTED] Dokumentnummer [REDACTED] Ausstellungsdatum [REDACTED] Ablaufdatum [REDACTED] Dokumentnummer [REDACTED] Ausstellungsdatum [REDACTED] Ablaufdatum [REDACTED]
---	---

BEHÖRDENANFRAGE

aus dem Zentralen Melderegister

Wohnsitze

Straße	[REDACTED]	
Postleitzahl	[REDACTED]	
Ortsgemeinde	[REDACTED]	
Unterkunftgeber	L [REDACTED]	
Gemeldet	[REDACTED] 05 - [REDACTED] 07	Hauptwohnsitz
Straße	[REDACTED]	
Postleitzahl	[REDACTED]	
Ortsgemeinde	[REDACTED]	
Unterkunftgeber	Z [REDACTED]	
Gemeldet	[REDACTED] 05 - [REDACTED] 05	Hauptwohnsitz
Straße	[REDACTED]	
Postleitzahl	[REDACTED]	
Ortsgemeinde	[REDACTED]	
Unterkunftgeber	[REDACTED]	
Gemeldet	[REDACTED]	
Straße	[REDACTED]	
Postleitzahl	[REDACTED]	
Ortsgemeinde	[REDACTED]	
Unterkunftgeber	R [REDACTED]	
Gemeldet	[REDACTED] 06 - [REDACTED] 07	Nebenwohnsitz
Straße	[REDACTED]	
Postleitzahl	[REDACTED]	
Ortsgemeinde	[REDACTED]	
Unterkunftgeber	[REDACTED]	
Gemeldet	[REDACTED]	

Tagesdatum: [REDACTED] 07

Uhrzeit: [REDACTED]

Seite: 2 von 3

Behördenabfrage

>> <<

Zurück

Weiter

Suche

Behördenabfrage

– Behördenabfragen

Überblick erstellen

Details anzeigen

+ Einstellungen

+ Sicherheitsbehördenabfrage

+ Aviso

+ Avisoabfrage

Logout

☒ Bundesgesetz/Abfrage durch Gemeindeorgane

☐ sonstige Abfrage

Begründung

ZMR-Zahl

Familienname

Vorname

Name vor 1. Ehe

Geburtsdatum

Geburtsort

Staatsangehörigkeit

Staatsangehörigkeit auswählen...

Postleitzahl

Ort

Straße

Hausnummer

Stiege

Türnummer

Suchoptionen

☐ historisch

☐ formalisiert

☐ Ergebnis drucken

Standarddokumente liefern

☒ Keine

☐ Bürger hat zugestimmt

☐ Aufgrund gesetzlicher Bestimmungen



Interessentensuche Nr:2488

Beschreibung der offenen Stelle(n):

Stellenbezeichnung:

Schwimmbhallenwart/SchwimmbhallenwartinEntsprechungsGr: **A5**VerwendungsGr: **v4/1**

Stellenanzahl:

1

Stellenbeschreibung:

Beaufsichtigung der Schwimmbetriebe-Verhinderung von Unfällen, gegebenenfalls erste Hilfeleistung; Kontrolle über die Einhaltung der Schwimmpläne (Tages-, Wochen- und Semesterpläne); Technische Sicherung des Schwimmbetriebes; Messen und Einstellen des PH-Wertes; Desinfektion; Wartung und Überwachung des Chlorgasraumes - Regelmäßiges Ein- und Ausschalten der Chlorgaszufuhr; Anschließen der Chlorgasflaschen mit Atemschutzgerät; Technische Beaufsichtigung des Saunabetriebes; Aufsicht, betreffend Einhaltung der Hausordnung und der Hygienevorschriften etc.

Da wir die Möglichkeiten des modernen E-Governments nutzen, bitten wir Sie, sich ausschließlich über unser [Online-Bewerbungsformular](#) zu bewerben.

Art der Stelle

Teilzeitarbeit

☐ Beamte ☒ Beamte und VB☒ nein ☐ 40 Std/Woche

Befristung

☒ nein ☐ bis

Mindestalter:

Höchstalter:

Informationen zur aufnehmenden Behörde:

Dienststelle:

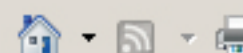
Sportzentrum SchmelzDienstort: **Auf der Schmelz 6**

Adresse:

1150 WienBewerbungsfrist **19.01.2010**

Kontaktperson:

Sabine HOSCHKETelefon: **01/4277/28632**



Diese Website möchte das folgende Add-On ausführen: "MSXML 5.0" von "Microsoft Corporation". Klicken Sie hier, wenn Sie der Website vertrauen und die Ausführung zulassen.

Bundeskanzleramt - Personalmanagement
Bühlhausplatz 2
1114 Wien

E-Government
www.bka.gv.at

BUNDESKANZLERAMT

Bewerbung online

Mit diesem Online-Formular können Sie Ihre Bewerbungsdaten an das Personalmanagement der Bundeskanzleramt übermitteln.

Bitte beachten Sie

[Hinweise zum Verfahren / Formular](#)

* **Feld muss ausgefüllt sein**

Ausfüllhilfe

Fehlerhinweise

Auswahl der Bürgerkartenumgebung *



Signatur im Gerät

Weiter

Abbrechen