

Private Datenbanken

<<TableOfContents>> = Private Datenbanken =

Die Sicherheitsbehörden des [[Datenbanken der Bundespolizeien|Bundes]] und der [[Datenbanken auf Länderebene|Länder]] und insbesondere die [[Datenbanken der Dienste|Geheimdienste]] greifen im Bedarfsfall (und dieses nicht nur bei [[129a Verfahren]]) gerne auf Datensammlungen von Unternehmen zu.

== Scoring Datenbanken ==

Ein Kreditscore (von engl. to score -punkten, score - Punktestand) ist laut der Webseite [[<http://www.ilex-recht.de/2008/bankrecht-wie-funktioniert-scoring.html>|ilex-recht.de]] ein Zahlenwert auf Basis einer statistischen Analyse, der die Kreditwürdigkeit einer Person repräsentiert. Mit Kreditscoring versuchen Unternehmen die Kreditwürdigkeit von Kunden oder Partnerunternehmen nach einem vorgegebenen Verfahren mehr oder weniger automatisiert zu ermitteln. Es ist sozusagen ein vereinfachtes [[Data Mining]].

Auf Basis von Kreditnehmer-Merkmalen wie „Kunde seit“, „Wohnort“, „Beruf“, „Sicherheiten“ werden Punkte vergeben, diese gewichtet und dann zu einer einzelnen Bonitäts-Note zusammengefasst, um mit diesem Gesamtscore die Kreditvergabe zu erleichtern. Ist die Bonität ausreichend, kann ein Kredit gewährt werden. Dabei sind die Scorings reichlich fehleranfällig wie etliche Skandale (siehe z.B. [[<http://www.spiegel.de/spiegel/0,1518,548454,00.html>|Spiegel-Artikel]]) zeigen.

=== Schufa ===

Die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) bietet ihren Kunden seit 1997 zusammen mit der Bonitätsauskunft über einzelne Verbraucher einen Scorewert auf Basis der bei ihr gespeicherten Daten an. Das ist ein Wert von 1 bis 1.000, der dem jeweiligen Verbraucher zugeordnet wird und die Wahrscheinlichkeit eines Kreditausfalles angibt. Je niedriger der Wert, desto größer die Ausfallwahrscheinlichkeit. Der Score-Wert ist abhängig vom Zweck, für den er angefragt wird - so erhalten beispielsweise Versicherungen andere Scorewerte als Mobilfunkanbieter. Jeder Verbraucher kann bei der Schufa die Scoreübermittlung zu seiner Person untersagen.

=== Infoscore === Infoscore ist das Scoring-Unternehmen von [[#arvato]].

=== World-Check ===

Besonders eklig ist World-Check von Thomson-Reuters; der Laden geriert sich als privater Geheimdienst und scort so etwas wie staatstreue.

[[https://www.vice.com/en_uk/article/pak7wb/exclusive-secret-blacklist-marking-innocents-as-

terrorists-continues-to-grow|„Thomson Reuters' World-Check apologised and compensated...”]]
(VICE, 2017-10-18) berichtet zu World-Check unter anderem:

{{{#!blockquote

- Animal rights activists have been profiled on a "terror" list.
- Trade Unionists were secretly profiled in practices that the TUC says has "echoes of the blacklisting scandal".
- Experts and MPs are warning that loopholes in the new data-protection bill could make the database exempt from oversight.
- Mortgage lenders are using the database, meaning being profiled on it could be even more disruptive than previously thought.
- A Trade Union has slammed the Information Commissioner for turning a "blind eye". }}}

(all das passierte im UK; die Aktivitäten von Thomson-Reuter in der BRD sind uns nicht bekannt).

== Kundendaten oder CRM ==

Customer-Relationship-Management, kurz CRM (dt. Kundenbeziehungsmanagement) oder Kundenpflege, bezeichnet die Ausrichtung eines Unternehmens auf ihre Kunden, was konkret eine Erfassung des Kaufverhaltens der Kunden in einer Datenbank heißt. Da in vielen Branchen (z. B. Telekommunikation, Versandhandel) die Beziehungen zwischen Unternehmen und Kunden langfristig ausgerichtet sind, soll so mittels CRM der Profit gesteigert werden. Zum Teil werden dabei auch [[Data Mining]]-Techniken angewandt.

=== Amazon ===

amazon.de ist laut der Webseite [[<https://www.datenschutz-ist-buergerrecht.de/auskunftersuchen-amazon>]] einer der größten deutschen Internetversandhändler mit dem Schwerpunkt auf Büchern, CDs, DVDs. Amazon speichert alle Suchbewegungen seiner Kunden um somit personenbezogene Angebote per Mail an die Kunden zu verschicken. Durch den Einsatz von Cookies ist man „permanent“ bei der Nutzung der Website identifizierbar. Somit wird auch das gelegentliche „rumstöbern“ dokumentiert und zur Bildung von Kundenprofilen genutzt. Die Speicherung der Daten erfolgt in den USA, daher gelten auch schwächere datenschutzrechtliche Bestimmungen.

=== Ebay ===

Ebay speichert laut der Webseite [[<http://www.daten-speicherung.de/index.php/bussgeldverfahren-gegen-datenkrake-ebay-eingeleitet/>]] das Surfverhalten („Navigationsverhalten“) jedes Nutzers auf unbegrenzte Zeit in identifizierbarer Form auf und weiß daher, für welche Produkte sich jeder Nutzer im Laufe seines Lebens interessiert hat.

=== Payback-Systeme ===

In 61% aller Haushalte liegt laut der Webseite [[<https://www.datenschutz-ist-buergerrecht.de/node/361>]] eine Paybackkarte, damit sind rund 30

Millionen Karten momentan im Umlauf. Mit ihrem Netzwerk an Partnerunternehmen werden zahlreiche alltägliche Einkaufsprozesse abgedeckt (Tankstelle, Supermarkt, Drogerie etc) und somit entstehen personenbezogene Einkaufsprofile die tausende Daten jahrelang beinhalten. Es kann damit herausgefunden werden wer, wann, wo mit welchen anderen Artikeln zusammen bspw. Klopapier der Marke Hakle, dreilagig in blau gekauft hat. Diese Informationen werden im Netzwerk der Partnerunternehmen zur genauen Zielgruppenansprache genutzt und werden damit breit für direkte Werbung ausgetauscht. Im Ergebnis werden Kundinnen und Kunden ausspioniert und mit ungewollter Werbung überschüttet.

=== Marriott Hotelkette ===

Die Marriott-Hotelkette bekam 2007 einen [\[\[http://www.bigbrotherawards.de/2007/.cop?set_language=de| Big Brother Award\]\]](http://www.bigbrotherawards.de/2007/.cop?set_language=de) für das ausführliche Sammeln von persönlichen Vorlieben der Gäste in einer Datenbank.

=== arvato === Arvato (Tochterunternehmen von [\[\[Bertelsmann-Stiftung|Bertelsmann\]\]](https://www.datenschutz-ist-buergerrecht.de/node/358)) ist laut der Webseite [\[\[https://www.datenschutz-ist-buergerrecht.de/node/358|Datenschutz ist Bürgerrecht\]\]](https://www.datenschutz-ist-buergerrecht.de/node/358) eines der größten Dienstleistungs- und Medienunternehmen weltweit. Mit zahlreichen Tochterunternehmen werden alle möglichen Daten aus eigenen Kundenbeziehungen, durch das Kundenmanagement für andere Unternehmen und über den Zukauf von Daten generiert. Das Spektrum reicht vom klassischen Scoring durch die Firma Infoscore bis hin zum Direkt-Marketing der Tochterfirma AZ Direct.

=== paypal ===

Die Datenschutzbestimmungen des Internet-Bezahldienstes Paypal sind laut der Webseite [\[\[http://www.daten-speicherung.de/index.php/anonym-mit-paypal-zahlen/| Daten-Speicherung\]\]](http://www.daten-speicherung.de/index.php/anonym-mit-paypal-zahlen/): Unter anderem behält sich Paypal vor, in weitem Umfang Kunden- und Transaktionsdaten nicht nur unbefristet in den USA zu speichern, sondern auch an internationale Behörden, Auskunftsteile und Adresshändler zu übermitteln. Geschäftssitz ist Luxemburg, so dass Paypal mit deutschem Datenschutzrecht und Aufsichtsbehörden nicht zu fassen ist. Trotzdem ist Paypal weltweit das verbreitetste Zahlungssystem.

=== Deutsche Bahn ===

Bahncard-Besitzer, die Punkte sammeln, ermöglichen der Bahn zu speichern, wann und wohin sie gefahren sind (Zumindestens bei zuggebundenen Fahrkarten, bei zugungebundenen Fahrkarten gibt es nur eine ungefähre Einschätzung). Die Bahncard 100 war (oder ist immer noch) mit einem [\[\[RFID\]\]](https://www.bigbrotherawards.de/2007/.com)-Chip ausgestattet. So konnte die Bahn feststellen, welche ICs oder ICEs von Bahncard 100 Besitzern benutzt wurden. Dafür gab es dann 2007 auch einen [\[\[https://www.bigbrotherawards.de/2007/.com|Big Brother Award\]\]](https://www.bigbrotherawards.de/2007/.com).

==== Bahncard ====

Bahncard-Besitzer, die Punkte sammeln, ermöglichen der Bahn zu speichern, wann und wohin sie gefahren sind (Zumindestens bei zuggebundenen Fahrkarten, bei zugungebundenen Fahrkarten gibt es nur eine ungefähre Einschätzung). Diese Daten können von den Sicherheitsbehörden

abgefragt werden, falls sie den oder die Bahncardbesitzer für verdächtig halten. Die Bahncard 100 war (oder ist immer noch) mit einem [\[\[RFID\]\]](#)-Chip ausgestattet. So konnte die Bahn feststellen, welche ICs oder ICEs von Bahncard 100 Besitzern benutzt wurden. Dafür gab es dann 2007 auch einen [\[\[https://www.bigbrotherawards.de/2007/.com|Big Brother Award\]\]](https://www.bigbrotherawards.de/2007/.com). Inwieweit es für verdächtige Personen, die nur eine Bahncard 25 oder 50 besitzen, eine Spezialanfertigung ebenfalls mit RFID-Chip gibt, ist nicht bekannt.

==== e-Ticket ====

Das e-Ticket (d.h. Handy Ticket) wird nach [\[\[http://www.lawblog.de/index.php/archives/2011/11/29/leitfaden-fr-lauscher/|lawblog\]\]](http://www.lawblog.de/index.php/archives/2011/11/29/leitfaden-fr-lauscher/) zum Feststellen der Daten sämtlicher Funkzellen, die der Nutzer durchfahren hat, benutzt.

==== Videoüberwachung ====

Die größeren Bahnhöfe sind standardmäßig mit [\[\[Videoüberwachung\]\]](#) ausgestattet. Dafür gab es 2006 für die Deutschen Bahn einen [\[\[http://www.bigbrotherawards.de/2000/.gov|Big Brother Award\]\]](http://www.bigbrotherawards.de/2000/.gov). Zwischen Bundespolizei und Deutscher Bahn gibt es einen Nutzungsvertrag, so dass die Bundespolizei die Videoüberwachung jederzeit nutzen kann.

vgl [\[\[Videoüberwachung#Videoüberwachung der Bundespolizei bei der DB\]\]](#)

=== Google ===

Google speichert mit Hilfe von [WikiPedia:Cookies](#) und [WikiPedia:IP Adressen](#), wer wann und wonach gesucht hat. Desweiteren ermöglichen die Zusatzfunktionen, wie Google Ads oder Google Analytics Ausforschungen auch außerhalb der Benutzung von Google. Die Sicherheitsbehörden greifen gerne auf diese Datensammlung zu.

Schutzmaßnahmen:

- Cookie kontrollieren (vgl. Einstellungen)
- Abschalten von Java-Skript nur wenn benötigt wieder aktivieren; realistisch geht das eher mit Browser-Erweiterungen wie [ublock origin](#) oder [noscript](#).
- Die Verwendung von Proxies ([\[\[https://privacy.net/proxy-servers-vs-vpns|Erklärung dazu\]\]](https://privacy.net/proxy-servers-vs-vpns)) wie [\[\[http://dontknow.me/at/?|dontknow.me\]\]](http://dontknow.me/at/?|dontknow.me) oder [\[\[http://anonymouse.org/anonwww_de.html|anonymouse.org\]\]](http://anonymouse.org/anonwww_de.html).
- Die Verwendung von Google-Proxies, wie [\[\[https://ssl.scroogle.org/|scroogle.org\]\]](https://ssl.scroogle.org/).

vgl [\[\[Überwachungstechnik#Google-Datenbank\]\]](#)

=== Mailanbieter ===

==== GMX ====

GMX bekam im Jahre 2000 den Big Brother Award. In der [\[\[http://www.bigbrotherawards.de/2000/.comm|Laudatio\]\]](http://www.bigbrotherawards.de/2000/.comm) wird erwähnt, dass GMX die

Dienstleistung kostenloser E-Mail mit zielgruppenspezifischer Werbung finanziert. Wer GMX nutzen möchte, bezahlt daher das Angebot mit Angaben nicht nur zum Wohnort sondern auch zum Familienstand, der Ausbildung, dem beruflichen Status usw. GMX erstellt daraus nach eigenen Angaben anonyme Nutzerprofile. Dieses Data-Mining dürfte sich im Rahmen des Datenschutzes bewegen, sei aber unerfreulich.

=== Soziale Netzwerke ===

Grundsätzlich stellst Du als Benutzer laut der Webseite [[<https://www.datenschutz-ist-buergerrecht.de/was-geschieht-mit-deinen-daten/unterwegs-im-netz/soziale-netzwerke>|Datenschutz ist Bürgerrecht]] zwei Arten von Informationen zur Verfügung. Zum einen persönliche Angaben, die Du bewusst angibst, und zum anderen Nutzungsdaten, die aus den Aktionen auf der Webseite herausgelesen werden. All diese Daten werden danach nicht nur von Bekannten gelesen, sondern werden auch von anderen Leuten und Institutionen genutzt. Auch kann es bei sozialen Netzwerken immer wieder zu Sicherheitslücken kommen. Hierdurch gelangen die in den Sozialen Netzwerken gespeicherten Daten ungewollt in die Hände Dritter.

===== facebook =====

facebook ist insbesondere beim [[ULD]] [[Schleswig-Holstein]] in der Kritik (neben sonstigen Datenschutzproblemen), weil facebook durch den like-me-Button auch Profile von Personen erstellt, die nicht Mitglied bei facebook sind. Deswegen hat der ULD angekündigt Webseitenbetreiber mit Sitz in Schleswig-Holstein zu verpflichten auf den Like-Button zu verzichten. Bei einem Treffen mit dem Cheflobbyisten von facebook wurde laut [[<http://www.datenschutz.de/news/detail/?nid=5077>|PM des ULD vom 7.09.2011]] kein Kompromiss erzielt. Wogegen bei einem Treffen mit dem Bundesinnenminister ein Kompromiss erzielt wurde, indem facebook eine freiwillige Selbstverpflichtung eingeht. Der Bundesinnenminister ist für die Datenschutzkontrolle laut einer [[<http://www.datenschutz.de/news/detail/?nid=5078>|PM des ULD vom 8.09.2011]] nicht zuständig und kann daher auch nicht solche Vereinbarungen treffen.

== Telekommunikationsdienstleister ==

Telekommunikationsdienstleister speichern [[TK-Verkehrsdaten]] (d.h. wer telefoniert mit wem und wie lange und von wo (Funkzelle bei Handys) zum technischen Betrieb und zur Abrechnung. Daneben sind sie noch gezwungen eine [[Abhörschnittstelle]] für die Sicherheitsbehörden zur Verfügung zu stellen.

vgl [[TK-Verkehrsdaten]]

== Banken ==

Banken speichern laut der Webseite [[<http://www.finanztip.de/recht/steuerrecht/bankgeheimnis.htm>|Finanztip]] Kontonummern, Ein- und Ausgänge, speziell EC-Karten Abhebungen und Bezahlungen zur Kontrolle für den Kontoinhaber_in. Daneben müssen die Banken die [[Kontodaten]] für die Wikipedia:BaFin bereithalten. Diese gibt sie wiederum an [[Datenbanken der Bundespolizeien|Polizei]] und [[Datenbanken Sozialamt|Sozialämter]] weiter.

vgl [[Kontodaten]]

== Private Sicherheitsfirmen ==

Private Sicherheitsfirmen vermehren sich exponentiell. Teilweise werden dies von den Ordnungsämtern, bei zweifelhafter Rechtsgrundlage, eingesetzt. Inwieweit sie Daten mit der [[Datenbanken der Bundespolizeien|Polizei]] austauschen ist meist nicht bekannt. Volker Eick meint in einem [[<http://www.bigbrotherawards.de/2000/.gov/informationen-zum-preistraeger-der-kategorie-behoerden-und-verwaltung>|Artikel]] zu den Datenschutzrechtlichen Aspekten, dass anders als die Polizei private Sicherheitsdienste nicht dem Gebot der Verhältnismäßigkeit unterliegen. Sie unterliegen auch keinen Einschränkungen beim Einsatz von z.B. Überwachungskameras. In der Praxis würde ein reger Datenaustausch zwischen Privaten und Polizei statt stattfinden, nicht zuletzt durch personelle Verbindungen im Rahmen sog. "Old Boy Networks" zwischen ehemaligen Polizisten und ihren alten Kollegen. In einem [[<http://www.trend.infopartisan.net/trd0804/050804.html>|Artikel der Onlinezeitschrift trend von 2004]] werden etliche Datenschutzverletzungen von privaten Sicherheitsdiensten, insbesondere die freimütige Weitergabe von Daten durch die Polizei, aufgelistet.

=== Links zu Artikeln über Private Securitys ===

- [[<http://www.trend.infopartisan.net/trd0804/050804.html>| trend:]] Die private Stadtsicherheit
- [[<http://www.heise.de/tp/r4/artikel/33/33209/1.html>|Telepolis-Artikel:]] Sicherheit im Privaten Raum
- [[<http://de.indymedia.org/2010/12/297053.shtml>|Indy-Artikel:]] (Öfftl.) Private Sicherheit vs. Bürgerrechte
- [[<http://de.indymedia.org/2010/09/289134.shtml>|Indy-Artikel:]] Rechtswidriges PPP in Plauen
- [[<http://de.indymedia.org/2004/12/100646.shtml>|Indy-Artikel:]] Staat und Sicherheitswirtschaft
- [[<http://de.indymedia.org/2009/03/243284.shtml>|Indy-Artikel:]] Provinzpresse zu Studiproteste
- [[<http://de.indymedia.org/2007/10/197854.shtml>|Indy-Artikel:]] Solidarität mit dem Streikenden Bahnpersonal

=== Private Terrordatenbank ===

Laut [[<http://www.kriminologie.uni-hamburg.de/wiki/index.php/World-Check>|Krimpedia]] gibt es eine private Datenbank World-Check in der Informationen zu derzeit ca. 400.000 Personen gespeichert sind. Die Datenbank wird von der in London ansässigen Firma „Global Objectives“ betrieben, die 2000 von dem Südafrikaner David Leppan gegründet wurde. Neben Banken und Unternehmen zählen auch etwa 300 [[Geheimdienste]] zu den Kunden der Firma, die in der Datenbank auch detaillierte Informationen (Finanzströme, Reiseaktivitäten) zu ca. 30.000 vermeintlichen TerroristInnen abrufen können. Damit zählt World-Check zur größten privaten "Terrorismus-Datenbank". Die in der Datenbank gespeicherten Informationen werden von einem internationalen Team aus ca. 450 ExpertInnen unterschiedlicher Professionen und Fachgebiete

erstellt. Als mögliche Einsatzbereiche für die Datensammlung werden neben der Terrorismusprävention und -bekämpfung auf der [\[\[http://www.world-check.com|Webseite des Unternehmens\]\]](http://www.world-check.com) auch das Vorgehen gegen Betrug, Korruption, Geldwäsche und Drogenhandel benannt.

== Anfragen der Polizei ==

=== Rechtslage ===

Im Rahmen eines Ermittlungsverfahrens können Daten privater sichergestellt (dabei stimmt die private Stelle der Auslieferung an die Polizei zu) oder, mit i.d.R. gerichtlicher Anordnung, beschlagnahmt (wenn der Eigentümer die Daten der Polizei nicht freiwillig gibt) werden. Daten verhalten sich hier aus StPO-Sicht wie Dinge.

Außerhalb des Strafverfahrens sehen inzwischen etliche Landes-[\[\[Polizeigesetze\]\]](#) spezielle Kompetenzen zur Nutzung privater Daten im [\[\[Prävention\]\]sbereich](#) vor.

Bundesweit sieht [\[\[http://bundesrecht.juris.de/tmg/_14.html|§ 14 Telemediengesetz\]\]](http://bundesrecht.juris.de/tmg/_14.html) ein Zugriffsrecht auf Bestandsdaten für [\[\[Datenbanken der Bundespolizeien|Polizeien\]\]](#) und [\[\[Geheimdienste\]\]](#) vor, und zwar sowohl zur Strafverfolgung als auch zur Gefahrenabwehr. Bestandsdaten sind dabei Daten, die für die "Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses" zwischen Nutzer`In und Provider "erforderlich sind". Dazu gehören also insbesondere Dinge wie Login und Passwort, aber auch Kontoverbindungen und Klarnamen.

In der Praxis unterhalten größere "Internetfirmen" extra Kontaktstellen für die Behörden, die häufig ziemlich unbürokratisch Auskunft geben. Statistiken dazu gibt es nicht viele.

=== Anfragen bei google ===

Laut [\[\[http://www.spiegel.de/netzwelt/netzpolitik/0,1518,770886,00.html|Spiegel\]\]](http://www.spiegel.de/netzwelt/netzpolitik/0,1518,770886,00.html) vom Juni 2011 gab es bei google im zweiten Halbjahr von 2010 insgesamt 768 Anfragen über Google-Anwender von Deutschen Behörden. Drei Vierteln dieser Anfragen kam laut Spiegel der Konzern ganz oder teilweise nach. Die vom Spiegel erwähnten

[\[\[http://www.google.com/transparencyreport/governmentrequests/userdata/|Statistiken zu Regierungsanfragen sind auf der Google-Seite\]\]](http://www.google.com/transparencyreport/governmentrequests/userdata/) zu finden, die allerdings nach Eigenauskunft unvollständig sind. Dennoch mögen die 1500 Anfragen (die u.U. jeweils zahlreiche Einzelnutzer betroffen haben können), die Google demnach 2010 aus der BRD erhalten hat, eine Vorstellung vom Umfang geben. Google will davon im zweiten Halbjahr 24% abgelehnt haben.

=== Anfragen bei Sozialen Netzwerken ===

Laut einer [\[\[http://www.ulla-jelpke.de/news_detail.php?newsid=1993|Antwort der Bundesregierung auf eine kleine Anfrage der Linke von 2011\]\]](http://www.ulla-jelpke.de/news_detail.php?newsid=1993) nutzen [\[\[BKA\]\]](#), [\[\[Bundespolizei\]\]](#) (BPol) und [\[\[Zoll\]\]](#) fallbezogen u.a. offen zugängliche Informationen aus sozialen Netzwerken und dort wird auch verdeckt ermittelt. Von Mitte 2009 bis Mitte 2011 hat das [\[\[BKA\]\]](#) 6 verdeckte Ermittler in Netzwerken eingesetzt und viermal von den Sozialen Netzwerken Informationen aus nicht-öffentlichen Profilen bekommen (vgl. [\[\http://annalist.noblogs.org/post/2011/07/15/polizei-in-

sozialen-netzwerken/#comment-29880|annalist]]).

=== Die Erfahrungen von Rechtsanwälten ===

Thomas Stadler:

{{{#!blockquote Seit vielen Jahren liefern Provider und Portalbetreiber den Ermittlungsbehörden oftmals ohne großen Widerstand alle möglichen Daten auf Anfrage hin. Das Spektrum reicht von Bestandsdaten bis hin zu konkreten Kommunikationsinhalten. Oft genug werden hierbei durch die Behörden auch die gesetzlichen Vorgaben nicht beachtet. In vielen Fällen genügt faktisch ein Fax einer Polizeidienststelle oder KPI mit einer "Auskunftsanfrage" und die Behörden bekommen die gewünschten Daten auf dem Silbertablett. }}}}

Quelle: [[<http://www.internet-law.de/2011/01/daten-auf-dem-silbertablett.html>|www.internet-law.de]]

Udo Vetter:

{{{#!blockquote Praktisch alle großen Anbieter arbeiten mit den deutschen Behörden zusammen, auch wenn sie (offiziell) gar keinen Sitz in Deutschland oder der EU haben. Wer also denkt, seine Daten bei Google, Facebook oder Twitter seien schon irgendwie vor dem Zugriff deutscher Behörden geschützt, irrt. Ich habe noch nie erlebt, dass einer der Global Player im Web 2.0 einen deutschen Gerichtsbeschluss ignoriert oder sich ihm widersetzt hat. Wie auch – den Verantwortlichen des Anbieters drohen Ordnungsgelder und Zwangshaft. Wohlgemerkt, wir reden über richterlich angeordnete Maßnahmen. Unter diesem Level gibt es aber noch die einfachen Anfragen der Polizei, welche Person hinter einem Account steht. Diese Anfragen sind zahlenmäßig viel häufiger. Denn die Polizei fragt mittlerweile schon fast routinemäßig und inflationär Bestandsdaten ab, wenn sie eine Anzeige mit Internetbezug auf den Tisch bekommt. Die meisten Internetanbieter haben für die Polizei sogar eigene Faxanschlüsse geschaltet. Um die Auskunft zu erhalten, genügt dann ein einfaches Musterschreiben des Polizeibeamten. Die Begründung tendiert regelmäßig gegen Null ("Ermittlungsverfahren wegen Warenbetrug", "üble Nachrede/Beleidigung"). Aber die Auskunft wird, so jedenfalls meine Erfahrung, anstandslos erteilt. Wenn man die Provider kritisieren möchte, dann an diesem Punkt. }}}}

Quelle: [[<http://www.lawblog.de/index.php/archives/2011/01/09/stapelweise-gerichtsbeschlusse/>|www.lawblog.de]]

== Durchsuchung von offenen Quellen ==

Nach einem [[<http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/>|Artikel der Zeitschrift wired]] von 2009 benutzt der CIA Crawler der Firma [[<http://www.iqt.org/>|In-Q-tel]] um im Netz Twitter, Facebook, Blogs und andere Soziale Medien nach verdächtigen Inhalten zu durchsuchen. In dem Artikel wird das Problem gesehen, dass die Crawler dazu benutzt werden könnten, missliebige politische Inhalte und Gruppierungen aufzuspüren. In einer Antwort der Bundesregierung auf eine Anfrage der Linken von 2011 wird behauptet, dass BKA, BPol und Zoll keine [[Data Mining]]-Software zur Verarbeitung von Daten aus Sozialen Netzwerken benutzen. Und es wird erläutert, dass für Polizeibehörden des Bundes und Nachrichtendienste bestimmte Vorschriften dabei gelten. Was nach der

[[<http://annalist.noblogs.org/post/2011/07/15/polizei-in-sozialen-netzwerken/>|Interpretation des Blogs annalist]] wohl bedeutet, dass Letztere sehr wohl [[Data Mining]] betreiben würden. Zu Einsatz von Data Mining Tools auf offene Quellen von sozialen Netzwerken der Polizei Thüringen gibt es eine [[<http://haskala.de/2011/08/15/nutzung-sozialer-netzwerke-zu-fahndungszwecken/>|Anfrage der Linken]] aus Thüringen, wobei die Antwort noch aussteht (September 2011).

Version #1

Erstellt: 2025-10-27 22:37:12 UTC von Datenschutz Migration Bot

Zuletzt aktualisiert: 2025-10-27 22:37:12 UTC von Datenschutz Migration Bot