»Datenschutz«

Hinweise und Tipps

DIE LINKE.
IM BUNDESTAG

DIE LINKE.
IM BUNDESTAG

Fraktion DIE LINKE. im Deutschen Bundestag
Platz der Republik 1, 11011 Berlin
Telefon: 030/22751170, Fax: 030/22756128
E-Mail: fraktion@linksfraktion.de
V.i.S.d.P.: Ulrich Maurer, Stellv. Vorsitzender der Fraktion DIE LINKE. im Bundestag

Redaktion und Text: AK III/MdB-Büro Jan Korte

Layout: Fraktionsservice

Fotos: iStockphoto.com, Frank Schwarz

Herstellung: MediaService GmbH Druck und Kommunikation

Redaktionsschluss: August 2013

Mehr Informationen zu unseren parlamentarischen Initiativen finden Sie unter: www.linksfraktion.de

Liebe Leserin, lieber Leser,

unser Leben findet schon lange nicht mehr nur in der realen Welt statt. Im Gegenteil, ohne eine digitale Datenerfassung und -verarbeitung ist es kaum noch vorstellbar. Dabei geben wir oft völlig selbstverständlich und unbewusst eine Menge über uns preis. Im Alltag werden etliche, teils höchst persönliche Daten gesammelt: sowohl von Unternehmen als auch vom Staat. Wir meinen, Datenschutz muss Vorrang vor kommerziellen Interessen haben, und die Bürgerrechte dürfen staatlichen Überwachungsprojekten nicht untergeordnet werden. Gegen die Kommerzialisierung und Überwachung unseres Alltags hilft vor allem eines: politischer und gesellschaftlicher Widerstand. Wir sollten den Datensammlern ihren Job nicht zu leicht machen. Deshalb soll diese Broschüre mit einigen Tipps und Tricks helfen, die Kontrolle über deine Daten zu behalten.

Jan Korte, *MdB, Datenschutzbeauftragter, Mitglied im Vorstand der Bundestagsfraktion DIE LINKE*

Ob Online-, Video- und Telefonüberwachung, Überwachung durch Drohnen und Profiling – die technologischen Entwicklungen und Überwachungspraxen der letzten Jahre waren rasant und scheinen kaum aufhaltbar.

Nachdem Edward Snowden, ein 29-jähriger IT-Techniker und Mitarbeiter der Nationalen Sicherheitsbehörde der USA (NSA), Anfang Juni 2013 Dokumente leakte, ist die Totalüberwachung der globalen Internetkommunikation amtlich. Die Dokumente beweisen, dass im Rahmen der amerikanischen und britischen Geheimdienstprogramme PRISM, Boundless Informant und Tempora eine Kontrolle sämtlicher digitaler Kommunikation weltweit erfolgt.

Gibt es Möglichkeiten sich vor dieser staatlichen Totalüberwachung zu schützen?

Natürlich sollte niemand die Illusion haben, durch Selbstdatenschutz seien Daten vor Geheimdiensten oder Zugriffen Dritter sicher. Transparenz und mehr Datenschutz können nur über politischen, wirtschaftlichen, diplomatischen und öffentlichen


TEAM EDWARD
Steht auf
Freiheit

Druck gewonnen werden. Dafür setzt sich DIE LINKE im Bundestag ein. Dennoch: Selbstdatenschutz ist wichtiger denn je, denn dadurch wird allen, die an deine Daten wollen, die Arbeit erschwert. Grundprinzipien sind hierbei Datenvermeidung und Datensparsamkeit. Aber auch die Daten, die du preis gibst, kannst und solltest du schützen.

Genauere Infos findest du hier:
http://prism-break.org

Datendiebstahl & Phishing

GRUNDSÄTZLICH GILT: ALLES WAS DU IM NETZ TUST, HINTERLÄSST SPUREN.

Für geübte Kriminelle ist es ein Leichtes, beispielsweise über gefälschte E-Mails oder manipulierte Websites an die persönlichen Daten nachlässiger Internetuser zu gelangen. Oft dauert das nicht mehr als ein paar Sekunden. Du kannst dich schützen.

Mach deinen PC fit. Besonders aufwändig ist das nicht:

- Virenprogramm installieren, Firewall einsetzen und Sicherheitsupdates des Betriebssystems durchführen.
- Browsereinstellung optimieren.
- Sicherheitsstatus von unbekannten Websites überprüfen.

Du solltest persönliche Daten im Internet immer erst eingeben, wenn du dich auf einer sicheren Website befindest.

Als Faustregel gilt: eine Website ist sicher, wenn in der Statuszeile des Browsers ein kleines Schloss erscheint und die Adresse der Homepage mit »https://« beginnt.

Oft hilft es auch schon, sich neben den technischen Maßnahmen auf seinen gesunden Menschenverstand zu verlassen: Ein Geldinstitut oder seriöse Firmen fordern dich niemals per E-Mail dazu auf, Links anzuklicken, um anschließend deine persönlichen Daten einzugeben.

Wenn du dir unsicher bist, ob es sich um einen Phishing-Angriff (einen Versuch über gefälschte Websites, E-Mails oder Chat-Nachrichten an deine Daten zu gelangen) handelt, frag einfach bei deiner Bank oder dem Onlineshop nach.

Passwörter

Vergleicht man den Computer mit einem Haus, sind Passwörter das Schloss der Eingangstür. Je mehr Sicherheitsvorkehrungen du triffst, desto schwieriger wird es für andere

hereinzukommen. Gleiches gilt für deinen Computer. Das Passwort schützt nicht nur deine Daten, es schützt auch deine Identität vor Missbrauch.

In Onlineshops beispielsweise hält lediglich das Passwort einen Dritten davon ab, Dinge in deinem Namen und auf deine Rechnung zu bestellen. Auch in sozialen Netzwerken kommt es nicht selten vor, dass Profile gehackt werden.

Dich davor zu schützen ist nicht schwer:

- Anonymisiere deine Passwörter. Verwende weder deinen Namen noch dein Geburtsdatum oder ähnliches.
- Verwende keine Wörter, die sich im Duden finden lassen.
- Vermeide Zeichen, die auf der Tastatur nebeneinander liegen. Also nicht: asdfgh12345.
- Dein Passwort sollte mindestens 8 Zeichen lang sein. Benutze Klein- und Großbuchstaben, Ziffern und Sonderzeichen. Am besten ist eine wilde Kombination aus allem.
- Nur du kennst das Passwort. Gib es an niemanden weiter. Speichere es

nicht in den Browsereinstellungen. Achte darauf, dass dich niemand beobachtet, wenn du es eingibst.

– Benutze für jeden Account ein anderes Passwort. Ändere es regelmäßig. Schreib es nirgends auf.

TIPP!

Gut lassen sich Passwörter merken, wenn du sie aus einem Satz ableitest. Ein sicheres Passwort ist, wie folgendes Beispiel zeigt: 2013 das A und O zum Schutz meiner Daten – EsPi2013dA&OzSmD.

Das alles schützt dich leider nicht vor staatlicher Schnüffelei. Das Gesetz zur »Bestandsdatenauskunft« erlaubt es den Sicherheitsbehörden, Zugriff auf deine Daten auf dem Smartphone und sogar auf deine E-Mail-Passwörter zu bekommen. Auch an deine PIN und PUK fürs Handy und die Passwörter zu Dropbox-, Google- und Facebook-Konten will der Staat schon bei Verdacht auf Ordnungswidrigkeiten bequem über eine elektronische Verbindung mit deinem Internet- oder Telefonanbieter gelangen. Dagegen hilft nur politischer Widerstand!

E-Mail

Kommunikation über E-Mail ist alltäglich geworden. Aber auch hier solltest du ein paar Dinge beachten, um deine Daten zu schützen:

Überprüfe Absender und Betreff, bevor du eine E-mail öffnest! Wenn dir etwas komisch vorkommt, lösch die Mail ungeöffnet.

Vorsicht bei den Anhängen. Dateien mit den Endungen .com, .exe, .bat, .do*, .xl*, .ppt, .scr oder .vbs enthalten nicht selten Schadsoftware. Öffne sie nur, wenn du den Absender kennst und eine solche Datei von ihm erwartest. Ist das nicht der Fall, solltest du die Mail löschen.

Benutze zwei Mail-Accounts. Eine Adresse für seriöse Kommunikation, die andere zur Registrierung bei sozialen Netzwerken, zum Shoppen oder für Online-Games. Letztere sollte übrigens keine Hinweise auf deine Identität geben.

Facebook & Co.

92 Prozent der 14- bis 29-jährigen sind in sozialen Netzwerken angemeldet. Facebook oder Google+ sind fester Bestandteil unseres Alltags. Sie geben Auskunft über unsere Vorlieben, Stimmungen, Aufenthaltsorte oder Verabredungen. Das, was ursprünglich privat war, wird auf sozialen Netzwerken öffentlich.

Wenn du dich in sozialen Netzwerken bewegst, sollte dir immer bewusst sein, dass

- alles, was du im Netz tust, Spuren hinterlässt – was einmal online ist, bleibt auch da.
- soziale Netzwerke nicht mehr nur der privaten Kommunikation dienen. Auch Arbeitgeber, Vermieter, Versicherungen sogar die Polizei und das Ordnungsamt aber auch Kriminelle nutzen die Online-Plattformen zur Verfolgung ihrer Interessen oder Informationsgewinnung.


Find us on:
facebook

Überleg dir immer ganz genau, was du von dir preisgeben willst und schütze deine Privatsphäre, indem du folgende Regeln beachtest:

Zur Anmeldung nur die nötigsten Daten preisgeben! Verwende zur Registrierung deine anonyme Mailadresse, für dein Profil ein Synonym und ein Foto, dass deine Identität nicht verrät.

Erstelle ein sicheres Passwort. Nutze das Angebot von zusätzlichen Sicherheitsmechanismen wie Email-Benachrichtigung bei jedem Login, zusätzliche Sicherheitscodes oder Einmalpasswörter.

Verfeinere die vordefinierten Privatsphäreeinstellungen!

Mach sensible Daten wie deine Telefonnummer oder deine Anschrift für andere unsichtbar!

Schränke die Sichtbarkeit deiner Posts, Fotos und Termine auf deine Freunde ein.

Verlinkungen und Markierung durch andere brauchen deine Genehmigung.

Lies die Datenschutzbestimmungen. Widersprich der Weitergabe deiner Daten an Dritte. Schließ den Zugriff von Kooperationspartnern des Netzwerkes auf deine Daten aus.

Vermeide es, Spiele oder andere Minianwendungen über soziale Netzwerke zu nutzen. Diese werden meist durch Dritte angeboten, die es auf deine Daten abgesehen haben.

Nimm nur Freundschaftsanfragen von Personen an, die du auch tatsächlich kennst.

Überprüfe selbst die Auffindbarkeit deiner Profildaten im Netz über eine Suchmaschine.

TIPP!

Letztendlich gilt: Gib nur das preis, was andere auch über dich wissen dürfen – auch nach langer Zeit noch.

Google & Suchmaschinen

Egal, was du wissen willst, Google hat innerhalb weniger Sekunden eine Antwort parat – wie praktisch. Was viele aber nicht wissen, ist, dass Google jede Eingabe durch das Ablegen von Cookies (kleine Programme, die auf deinem Rechner abgelegt werden und dem Entsender ständig Informationen über dein Surfverhalten liefern) protokolliert und das Ganze für anderthalb Jahre anonymisiert speichert. Dabei wird nicht nur der Suchbegriff, sondern auch die Uhrzeit und das Datum der Suche, sowie deine IP-Adresse aufbewahrt.

So kann Google gezielte Aussagen über deine Interessen, politische Einstellung, Religionszugehörigkeit und nicht selten auch über deinen Beruf und dein Einkommen machen. Dementsprechend kann von Personen, die Suchmaschinen oft nutzen, ein regelrechtes Profil angelegt werden. So wird es möglich, dir gezielte Werbeangebote zu machen. Google entscheidet also, was dich zu interessieren hat. Das Schalten gezielter Werbeangebote ist übrigens die Haupteinnahmequelle des Konzerns.


.google.com
Maps
News
Shopping
Gmail
more
Google
google
google maps
google.com
google translate
google earth
google images
google voice
google docs
google tv
google scholar
google books
Google Search

Das kannst du tun, um deine Daten und die freie Wahl zu behalten:

- Wechsel zu einer anderen Suchmaschine.
- ***Lösche Cookies. Und zwar nach jedem Internet-Besuch. Das funktioniert ganz einfach über deine Browsereinstellungen:***
- bei Firefox: Extras – Einstellungen – Datenschutz – Cookies – Cookies beibehalten bis »Firefox geschlossen wird«
- oder immer den privaten Modus verwenden
- bei Internet Explorer: Extras – Internetoptionen – Datenschutz – Datenschutzstufe einstellen.

Online-Shopping

Auch beim Online-Shopping spielen Cookies eine nicht unwesentliche Rolle. Online-Händler legen gern Profile ihrer Kundinnen und Kunden an. In puncto Shopping ist das besonders brisant, denn hier gibst du deine Bankdaten an.

Deshalb gilt auch hier:

- Vor dem Einloggen Cookies löschen.
- Falls der Online-Shop, in dem du einkaufen willst, das Zulassen von Cookies verlangt, solltest du nach der Bestellung Cookies in deinem Browser wieder deaktivieren.
- Kaufe nur bei seriösen Anbietern. Informiere dich vorab über den Shop.
- Bankdaten nur auf verschlüsselten Homepages angeben.
- Shoppen nur am eigenen Rechner. Die Benutzung offener W-Lan-Netze solltest du vermeiden.

Smartphones und Apps

Smartphones sind zu unseren täglichen Begleitern geworden. Mal eben schauen, wann die nächste Bahn kommt, den Status im sozialen Netzwerk aktualisieren oder ein Foto schießen, bearbeiten und schnell hochladen. Dabei ist dein Telefon eine wirklich lukrative Informationsquelle für Dritte. Es kann beispielsweise Bewegungsprofile erstellen und genau sagen, wann du dich wo aufgehalten hast, es zeigt, welche Interessen du hast, wer deine Freunde sind und vieles mehr.

Aus diesem Grund solltest du es genau wie deinen Computer vor Angriffen und Missbrauch schützen:

- Benutze Sicherheitscodes und PIN-Abfrage. Ändere sie regelmäßig
- Aktiviere die W-LAN und Bluetooth Funktion nur, wenn du sie brauchst. Schalte sie danach wieder aus. Gleiches gilt für die Ortungsfunktion.
- Vermeide die Nutzung öffentlicher Hotspots.

– Tätigkeiten, die eine Eingabe sehr persönlicher Daten erfordern, solltest du nur vom heimischen PC aus erledigen.

Insbesondere sind es aber die Hersteller der Apps, die sich für deine Daten interessieren. Deshalb solltest du folgendes beachten:

– Prüfe vor dem Runterladen, ob die App von einem seriösen Anbieter erstellt wurde. Gerade bei kostenlosen Anwendungen ist das oft nicht der Fall.

– Will die App auf dein Adressbuch, dein Fotoalbum oder aktuelle Standortposition zugreifen, obwohl das nicht erforderlich ist? Lösch sie oder überleg dir, ob du die App wirklich brauchst. Oft gibt es auch gute Alternativen, die deine Privatsphäre respektieren!

– Aber nicht nur in der digitalen Welt ist es wichtig, deine Daten zu schützen. Auch im alltäglichen Leben haben es Staat und private Unternehmen auf unsere Daten abgesehen.

Datenhandel & Meldedaten

Nicht selten erhalten wir Werbebriefe von Firmen, zu denen wir nie Kontakt hatten oder werden von Gewinnspielanbietern angerufen, obwohl wir denen niemals unsere Daten gegeben haben. Das ist auch nicht notwendig – es gibt mittlerweile einen richtigen Markt, auf dem Daten ähnlich wie Obst und Gemüse gehandelt werden. Ursprung sind dabei die Meldeämter. Denen ist es erlaubt – soweit du einwilligst – deine Daten zu Werbezwecken an private Unternehmen gegen Geld weiterzugeben. So kommt es, dass sie letztlich bei Adresshändlern landen.

Du kannst deine Daten schützen, indem du ganz einfach die Einwilligung zur Weitergabe bei der zuständigen Meldebehörde verweigerst. Falls du dir unsicher bist, wie genau du das anstellen sollst, findest du entsprechende Vorlagen im Netz oder fragst einfach beim zuständigen Meldeamt nach.

Private Unternehmen dürfen deine Daten übrigens immer nur dann weitergeben, wenn du ihnen das erlaubst. Bevor du also irgendetwas unterschreibst, solltest du dir die Datenschutzbestimmungen durchlesen und auch deinem Geschäftspartner die Einwilligung zur Weitergabe von Daten an Dritte verweigern. Bereits erteilte Einwilligungen können übrigens jederzeit widerrufen werden.

Du kannst im Übrigen durchaus mal bei verschiedensten Unternehmen nachfragen, welche Daten sie von dir besitzen, wie sie diese erhalten haben und wozu sie die Informationen verwenden. Sie sind verpflichtet, dir zu antworten. Unkorrekte Informationen müssen sie löschen. Zur Vorgehensweise findest du auch hier wieder allerhand Infos und Musterschreiben im Netz.

Kunden- & Rabattkarten

Sicherlich besitzt du auch die eine oder andere Kunden- und Rabattkarte. Angefangen vom Supermarkt über die Apotheke bis zum Drogeriemarkt– nahezu alle Dienstleister bieten sie an. Hast du dich schon einmal gefragt, was die Unternehmen davon haben? Durch die auf deiner Karte gespeicherten Daten ist es mittels genauer Analyse möglich, dein Kaufverhalten zu analysieren und dir gezielt Werbung zukommen zu lassen. Zum Beispiel weiß deine Kundenkarte ganz genau, welche Medikamente du benötigst, welche Hygieneartikel du wie oft kaufst oder ob du dir ab und zu mal eine Flasche Wein kaufst. Darüber hinaus kann sie genaue Auskunft darüber geben, für wie viel du wann, wo und zu welcher Zeit Artikel gekauft hast. Danach richtet sich dann auch wieder die Werbung, die du bekommst. Andere Informationen werden dir vorenthalten.

Du schützt deine Daten natürlich am besten, indem du auf Kundenkarten verzichtest. Falls du das nicht möchtest, solltest du zumindest darauf

achten, dass du keine Einwilligung in die Weitergabe deiner Daten erteilst. Nähere Informationen kannst du dir auch auf Nachfrage bei dem jeweiligen Unternehmen einholen.

TIPP!

Die als Prämien für treue Kunden angebotenen Waren sind selten günstiger, als wenn du sie direkt im Laden kaufst.

Datenschutz bei Arbeitsagentur und Jobcenter

Bei der Beantragung von Sozialleistungen musst du teilweise Informationen preisgegeben, die sehr intim sind. Oft betreffen sie nicht nur dich. Auch Personen aus deinem Umfeld werden einbezogen. In den meisten Fällen braucht die Sachbearbeiterin oder der Sachbearbeiter die Daten als Grundlage für die Berechnung verschiedenster Ansprüche.

Trotzdem: Auch gegenüber Behörden musst du nicht alles kundtun. Vor allem benötigt die Behörde jedoch deine Einwilligung, um Informationen an andere Stellen und Dritte zu übermitteln. Diese musst du nicht erteilen. Auch bei den Arbeitsagenturen kannst du dich erkundigen, welche Daten von dir gespeichert sind und gegebenenfalls deren Löschung verlangen.

Arbeitgeber

Im Übrigen musst du auch gegenüber deiner Arbeitgeberin und deinem Arbeitgeber nicht alles preisgeben. Beispielsweise müssen bei einem Bewerbungsgespräch nicht alle Fragen tatsächlich beantwortet werden. Erlaubt sind Fragen nach der fachlichen Qualifikation, Fragen, die deinen Privatbereich betreffen (beispielsweise nach Gewerkschafts-, Partei- oder Religionszugehörigkeit), dürfen nicht gestellt werden. Es ist dein gutes Recht, solche Fragen nicht oder unwahr zu beantworten.

Checkliste für deinen Datenschutz

Nachdenken: Was willst du über dich preisgeben und welche Konsequenzen hat das

PC startklar machen: Virenprogramm installieren; Firewall einrichten, Updates durchführen

Browsereinstellungen überarbeiten

Passwörter sicher machen und erneuern

Privatsphäreeinstellungen in den sozialen Netzwerken verfeinern

Smartphone aufräumen: Datenschutzeinstellungen überprüfen, unnötige Apps löschen

Weitergabe der Meldedaten beim Bürgeramt widersprechen

Auskunft über den Datenbestand bei Unternehmen einholen und gegebenenfalls die Löschung der Daten verlangen

Linksammlung

Weitere Informationen zum Datenschutz und den angesprochenen Themen findest du unter anderem auf folgenden Websites:

www.linksfraktion.de

www.bfdi.bund.de

www.bsi-fuer-buerger.de

www.datenschutz.de

www.datenschutzzentrum.de

www.dgb.de

www.verbraucherzentrale.de

www.vz-berlin.de

www.vorratsdatenspeicherung.de

www.linksfraktion.de