Unerwünschte Follower

Unerwünschte Follower

Die Geheimdienste sammeln Bürgerdaten heute per Schleppnetz. Das kümmert keinen – bis es zu spät ist. Eine Anleitung zum Schutz gegen digitale Übergriffe.

von Ronnie Grob

1 *Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs*
2 *Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.*

Bundesverfassung der Schweizerischen Eidgenossenschaft, Art. 13 Schutz der Privatsphäre

2013 entwendete NSA-Mitarbeiter Edward Snowden eine ganze Reihe hochgeheimer Geheimdienstdokumente und machte sie nach und nach Journalisten zugänglich, die darüber schrieben. Von den bisher insgesamt über 500 von internationalen Medien publizierten Dokumenten[1] waren 321 als «Top Secret» klassifiziert. Dank diesem Leak, das einen Einblick in die tiefsten Staatsgeheimnisse liefert, blickt die Welt anders auf die Tätigkeiten der britischen und US-amerikanischen Geheimdienste. Aufgedeckt wurde, dass GCHQ und NSA nicht etwa nur dem Treiben von unter Verdacht stehenden oder gesuchten Terroristen nachgehen, sondern – vorgeblich zur Prävention – möglichst *alles* sammeln, was irgendwie an Daten verfügbar und greifbar ist. Auch wenn schon davor Hinweise auf solche Tätigkeiten publiziert wurden[2], haben die Snowden-Leaks mit internen Dokumenten unabstreitbar bewiesen, dass die Geheimdienste alles tun, was technisch möglich ist, und sich dabei um bestehende Gesetze und Einschränkungen foutieren beziehungsweise sie geschickt umgehen. Zwar hat Snowden nur die westlichen Geheimdienste überführt; doch kaum jemand wird von chinesischen oder russischen Geheimdiensten ein zurückhaltenderes Verhalten erwarten – im Gegenteil.

Die offensichtlichste Widerrede klingt denn meist so: Sind die Geheimdienste denn nicht dazu da, um zu überwachen? Korrekt. Der Staat legitimiert Geheimdienste für die gezielte Überwachung. Sie sind damit beauftragt, Personen, die Recht und Ordnung mit terroristischen Aktivitäten gefährden, zu überwachen und sie wenn möglich an diesbezüglichen Taten zu hindern. Die *anlasslose* Datensammlung per Schleppnetz jedoch ist etwas ganz anderes: Noch der kleinste Fisch wird so als potentielles Monster angesehen, über das man besser mal alles herausfindet. Um bereits alles über ihn und alle seine Verbindungen zu wissen, sollte er irgendwann mal verdächtig werden.

Ronnie Grob
ist freier Journalist und wohnt in Berlin. Er ist Mitarbeiter von Medienwoche.ch, einem digitalen Medienmagazin, von Bildblog.de, einem Medien-Watchblog, und von Presseverein.ch, der Website des Zürcher Pressevereins.

Von uns allen, die wir uns im Internet bewegen, haben NSA und GCHQ öffentliche und nichtöffentliche Daten gesammelt und gehortet: Benutzernamen, E-Mail-Adressen, Passwörter, Bewegungsdaten, persönliche Nachrichten oder Chats. Sie können darauf zugreifen, wann immer es ihnen beliebt, und nachschauen, welche Geheimnisse wir dem Geschäftspartner oder der besten Freundin per E-Mail oder WhatsApp übermittelt haben. Oder welche Informationen wir ausgetauscht haben über das vermeintlich bestens gesicherte Seitensprungportal. Kurz: jede Person, die sich im Internet bewegt, wird ohne besonderen Anlass bis in die intimsten Details hinein überwacht. Diese Überwachung findet meistens nicht in Echtzeit statt, weil das einen enormen Personaleinsatz bedeutete. Das Ziel jedoch ist, bei einem Verdacht über eine möglichst vollständige Informationslage zu verfügen. Wird eine Person als Überwachungsziel («target») definiert, so wie das beispielsweise 122 Staatschefs[3] widerfahren ist, kann nach ihr – ähnlich wie bei Google – gesucht werden. Das geschieht mit dem Datenbanksystem XKeyscore, das auch Verbindungen mit Daten herstellt, die mit E-Mail-Adressen, Facebook-Profilen oder IP-Adressen verknüpft sind. Dieser nahezu allumfassende Wissensschatz bietet ungeheure Missbrauchsmöglichkeiten – man denke nur mal an die privaten Leidenschaften von NSA-Analysten. Um XKeyscore zu benutzen, benötigen letztere nicht mal eine Genehmigung ihres Vorgesetzten, ein einfaches Formular zur Begründung reicht aus.[4] XKeyscore für private Zwecke zu nutzen, ist nicht erlaubt. Dennoch gibt es Beweise, dass NSA-Mitarbeiter genau das gemacht haben.[5] Wer sich vor diesen Übergriffen wirksam schützen will, dem bleibt nur eines übrig: seine Kommunikation komplett zu verschlüsseln und generell äusserst wachsam vorzugehen. Mehr dazu später.

Die Datengrundlage von XKeyscore kommt zustande durch angezapfte Fiberglasleitungen («Upstream») und durch den direk-

Faule Ausreden

Zur Überwachungsproblematik werden einige vermeintliche Gegenargumente aufgezählt. Wer noch nicht genau darüber nachgedacht hat, neigt dazu, Sätze zu sagen, die richtig klingen, aber falsch sind:

«Ich habe nichts zu verbergen.»

Tatsächlich? Glenn Greenwald bittet Leute, die diesen Satz äussern, dann jeweils um die Logins und Passwörter zu ihren E-Mail- und Facebook-Konten. Er wolle darin nur etwas lesen und gegebenenfalls daraus etwas veröffentlichen. Noch nicht eine Person, die angeblich nichts zu verbergen hatte, sandte ihm bislang etwas zu. Edward Snowden sagte dazu: «Zu argumentieren, dich kümmert das Recht auf Privatsphäre nicht, weil du nichts zu verbergen hast, ist nichts anderes, als zu sagen, dich kümmert die Redefreiheit nicht, weil du nichts zu sagen hast.»

«Jemand, der sich nichts zuschulden kommen lässt, hat nichts zu befürchten.»

«Wissen ist Macht», das wissen wir seit Francis Bacon. Und ein Staat, der alles weiss, während die Bürger nur wenig wissen, ist nicht nur für einen Liberalen eine Horrorvorstellung. Irgendwann geht es nicht mehr darum, wer sich etwas zuschulden hat kommen lassen, sondern darum, wer angeblich eine Gefahr darstellt. Die grenzenlose Überwachung führt direkt zurück zum Herrschaftswissen des Klerus und der Monarchie im Mittelalter, die beide mit der Aufklärung überwunden geglaubt waren.

«Wer seine Kommunikation verschlüsselt, macht sich erst recht verdächtig.»

Wer wie die Masse WhatsApp, Google, Bluewin und Dropbox nutzt statt Signal, DuckDuckGo, Protonmail und SpiderOak, macht sich womöglich weniger verdächtig als andere. Aber ist das ein Grund, sich nicht zu wehren gegen die permanente Verletzung der Privatsphäre? Haben nicht alle, die Geheimnisse gegenüber der Wirtschaft oder dem Staat schützen müssen, eine Pflicht dazu? Dennoch wird bisher kaum verschlüsselt kommuniziert, denn das setzt voraus, dass beide Seiten dies tun. Was auch Snowden herausfinden musste, der im Dezember 2012, ein halbes Jahr vor dem Medienrummel um die Snowden-Leaks, vergeblich versuchte, Greenwald zur Verwendung der PGP-Verschlüsselung zu bewegen, um ihm seine Leaks mitzuteilen.

ten Zugang zu den Servern von Service Providern wie Facebook, Skype oder Google («Prism»). Unter dem Decknamen «Poseidon» hat auch das deutsche Bundesamt für Verfassungsschutz (BfV) auf XKeyscore Zugriff. Und der Schweizer Geheimdienst? Auf Anfrage dementiert der Nachrichtendienst des Bundes (NDB), Zugriff auf XKeyscore zu haben: «Es existiert kein Abkommen und somit auch keine Datenflüsse zwischen dem NDB und der NSA.» Während der NDB Medienberichten gemäss rund 250 Mitarbeiter beschäftigen soll, arbeiten für die NSA rund 40 000 Mitarbeiter, für den GCHQ rund 6000. Das Jahresbudget aller US-Geheimdienste wurde 2013 von der «Washington Post» auf über 50 Milliarden US-Dollar geschätzt, wovon über 10 auf die NSA fielen. Zum Vergleich: das Bundesbudget der Schweiz ist für 2016 auf rund 67 Milliarden Franken veranschlagt. Neben der Industriespionage praktiziert der US-Geheimdienst auch die Überwachung politischer Strategien. Weil die US-Seite ihr Gegenüber abhört, kann sie die Strategien anderer politischer Player durch gekaperte Interna durchkreuzen. So geschehen an der UN-Klimakonferenz in Kopenhagen 2009, nach der ein Teilnehmer berichtete, dass die Vertreter der USA – aber auch Chinas – auffällig gut informiert gewirkt hätten. Schweizer Delegationen, die mit den USA verhandeln, sollten also bedenken, dass die Gegenseite das Schweizer Verhandlungsziel womöglich bereits kennt.

Ahnungslose Elite, aktive Wirtschaft

Was die neusten technischen Ausspähmöglichkeiten angeht, sind Kaderbeamte oft ahnungslos. Der Deutsche Bundestag etwa bezog seinen Internetzugang von der US-Firma Verizon und lieferte so seine Kommunikation der NSA auf dem Silbertablett. Und die Schweizer Armee benutzt zur Kommunikation WhatsApp – nicht nur im Kriegsfall ein Fiasko. Die Schweizer Wirtschaft dagegen hat längst reagiert und einige zukunftsweisende Produkte entwickelt, die Schutz gegen die Übergriffe versprechen. Proton Technologies AG aus Genf, ein Anbieter eines verschlüsselten E-Mail-Diensts namens Protonmail.com, sammelte im November 2015 in drei Tagen 50 000 US-Dollar per Crowdfunding, nachdem die Website durch DDoS-Attacken vorübergehend lahmgelegt worden war.

Die Blackphone SA aus Genf und die Silent Circle SA aus Le Grand-Saconnex (GE) haben das Blackphone 2 auf den Markt gebracht, ein abhörsicheres Smartphone, das seit Oktober 2015 für rund 1000 Franken erhältlich ist. Die TelePhoenix AG aus Emmetten (NW) bietet mit OpusTel eine App für verschlüsselte Telefongespräche an. Und die Threema GmbH aus Pfäffikon (SZ) verkauft eine verschlüsselte Messaging-App, die bereits millionenfach heruntergeladen wurde – 80 Prozent der Nutzer sind aus Deutschland. Die Wirtschaft hat es also bereits verstanden: Privatsphäre wird man sich künftig, wie auch guten Journalismus, leisten müssen. Oder andersherum: wer nichts investiert, wird von Müll zugeballert – und dabei ausgespäht werden.

Über die Gründe für die weitverbreitete Ahnungslosigkeit der verantwortlichen Elite, die im Zweifel auch noch die idiotischste

Massnahme für mehr vermeintliche Sicherheit billigt, kann man nur mutmassen. Hat es – neben dem ungeheuren Druck durch die Medien – damit zu tun, dass ältere Menschen, die die überwiegende Mehrheit der politischen Entscheidungsträger in der Schweiz oder in Deutschland stellen, weniger Kenntnisse des Internets, dafür ein grösseres Sicherheitsbedürfnis haben? «Die Überwachungsdebatte reisst die herkömmlichen Parteifronten nieder. Ich bekomme genau so viel Zuspruch von links wie von rechts», sagte Journalist Glenn Greenwald dazu, der als Erster Inhalte aus den Snowden-Files publizierte: «Entscheidend ist das Alter. Jüngere Leute neigen dazu, Snowden und mich zu unterstützen. Ältere schlagen sich eher auf die Seite der Regierung.» Der mit einer Klage öffentlich ausgetragene Streit zwischen den Schweizer Jungsozialisten und dem Zürcher SP-Regierungsrat Mario Fehr, der auf Staatskosten für 486 500 Euro Schadsoftware einkaufte, ist dafür exemplarisch. Denn auch in anderen Parteien gibt es eine Altersgrenze bei der Einschätzung der Sachlage, die Gräben gehen quer durch alle Parteien. Die Problematik verstanden haben bisher nur wenige, im Schweizer Parlament etwa Balthasar Glättli (Grüne) oder Franz Grüter (SVP). Tatsächlich sind die meisten führenden Politiker und Journalisten nicht mal bereit, sich ein Grundverständnis dazu anzueignen – sie zucken mit den Schultern, wenn man sie auf das Thema Überwachung anspricht. Auch viele Wirtschaftsvertreter – immerhin durch Industriespionage in ihrem Geschäftsmodell gefährdet – verhalten sich so, als gäbe es gar keine Überwachungsprobleme.

Die anlasslose Massenüberwachung ist nicht nur für Politiker, Ärzte, Bankiers, Rechtsanwälte, Geistliche und alle anderen auf Vertraulichkeit bauenden Personengruppen höchst problematisch, sondern auch und vor allem für uns Journalisten. Wie sollen wir etwa eine Quelle schützen können, wenn der Staat über die Metadaten und die Inhalte verfügt? Selbst wenn Informant und Informierter die elektronische Kommunikation komplett vermeiden und sich im Wald treffen, ist ihr Zusammenkommen aufgrund der Standortdaten ihrer Telefone nachweisbar. Ebenso verdächtig machen sie sich, wenn ihre beiden Geräte zur gleichen Zeit während Stunden nicht aktiv waren. Geheimdienste im Besitz all dieser Daten sind so gut über Identität und Handeln der beiden informiert, dass ihr Wissen sogar den Erkenntnissen einer Untersuchungskommission oder eines regulären Ermittlungsverfahrens überlegen ist. Wenn potentielle Informanten und Whistleblower gut beraten sind, eine unverschlüsselte Kontaktaufnahme zu Journalisten zu scheuen, so liegt die Problematik der Massenüberwachung für die freie Gesellschaft offen. In der Schweiz wird man Whistleblowern auch aus anderen Gründen nur abraten können, Journalisten mit vertraulichen Informationen auf Missstände aufmerksam zu machen. Die im September 2015 aufgrund zu hoher Kompliziertheit vom Parlament an den Bundesrat zurückgewiesene Gesetzesvorlage verunmöglicht es praktisch, dass sich Informanten straffrei an die Medien wenden können.

Die Technik der Zukunft wird uns noch viel mehr Überwachungsmöglichkeiten bieten. Reiskorngrosse RFID-Transponder zum Beispiel oder in Kontaktlinsen eingebaute Kameras. Mit Sicherheit werden die bisherigen Massnahmen verfeinert: Die toten Winkel der Welt, in denen ein Geschehen von keiner Kamera mitgefilmt wurde, werden weniger, was auch daran liegt, dass Kameras mobil werden; man muss kein Prophet sein, um zu vermuten, dass die lärmigen, schwerfälligen Drohnen von heute auf die Grösse von Moskitos schrumpfen werden. Um den automatischen Autonotruf eCall zu ermöglichen, muss von 2018 an in jeden der in der EU zugelassenen Neuwagen eine SIM-Karte eingebaut sein. Wie lange es wohl dauert, bis jedes Fahrzeug – selbstverständlich zur allgemeinen Sicherheit – online sein und seinen Standort melden muss?

Was der Bund darf

«Nachrichtendienste beschaffen durch Kommunikationsüberwachung und aktives Eindringen in Informatiksysteme vertrauliche Informationen auf breiter Front. Sie können diese möglicherweise auch verfälschen oder sogar Prozesse oder Infrastrukturen manipulieren. Die Durchdringung der Kommunikation ist tief, fast flächendeckend und systematisch, entsprechend den Mitteln, die eingesetzt werden: Provider werden gesetzlich zur Datenherausgabe gezwungen, es bestehen verdeckte Zugänge zu den Hauptsträngen der Kommunikation, zudem wurden systematisch Verschlüsselungen aufgebrochen oder geschwächt, sogar internationale Kryptostandards beeinflusst. Ein Beispiel ist die landesweite Aufzeichnung von Mobiltelefondaten – unter dem Namen Mystic der Metadaten (verbundene Telefonnummern, Gesprächszeit und -dauer usw.) oder unter dem Namen Somalget auch der Kommunikationsinhalte (Bahamas und mindestens ein weiteres Land). Auch der im Februar 2015 bekannt gewordene mutmassliche Cyberangriff durch die NSA und den GCHQ auf einen der grössten Hersteller von SIM-Karten für Mobiltelefone entspricht dem Anspruch der Nachrichtendienste der Five-Eyes-Staaten, möglichst viele Kommunikationsinhalte potentieller Ziele abzufangen.»

Nachrichtendienst des Bundes (NDB), Lagebericht «Sicherheit Schweiz 2015», Seite 65, Kapitel «Verbotener Nachrichtendienst und Angriffe auf Informationsinfrastrukturen»

http://www.vbs.admin.ch/internet/vbs/de/home/documentation/publication/snd_publ.html

Die vollständige Digitalisierung der Gesellschaft ist in vollem Gange und vermutlich unumkehrbar. Was elektronisch vorhanden ist, wird überwacht, und die Querverbindungen sind immer leichter zu ziehen: Bankkonto, Kreditkarte, Krankenkassenkarte, Kundenkarte, Standortdaten, Browserverlauf, Activity Tracker. Wer nicht elektronisch komplett abstinent lebt, wird überwacht. Gleichzeitig können sich immer weniger erlauben, sich gegen den Fortschritt zu sperren, der Identität, Schlüssel, Kommunikation und Geld in einem Gerät vereint. Bargeldlose Zahlungen in Zusammenhang mit Kundenkarten machen bereits jetzt kleinste Handelstransaktionen individuell verfolgbar. Der Druck, das Bargeld, eine der letzten Bastionen der Privatsphäre, abzuschaffen, nimmt zu. Weil die Kontrolle des Staats so auch noch die letzten Lücken schliessen kann. Und was wartet am Ende? Das Totalitäre.

Der Kontrollverlust über die persönlichen digitalen Daten ist sicher auch bedenklich, wenn private Unternehmen ihn verursachen. Doch im Markt verteilt sich die Macht über die Informationen, kein einzelner Teilnehmer verfügt über alle Daten. Wenn der Staat jedoch alles sammelt, was privat anfällt, so gelangt er zum totalen Durchblick. Das Herrschaftswissen, das die Kirchen dem Volk über Jahrhunderte hinweg erfolgreich vorgaukelten, wird real. Weiss der Staat alles, kann er damit eine ohnmächtige Bevölkerung kontrollieren. Und was folgt den Kontrollen? Sanktionen gegen jene, die von der Norm abweichen. Ausgrenzung. Zugriffsverweigerung. Nachteile. Wie schnell jemand zu einem Ausgestossenen werden kann, haben wir in den letzten Jahren mehrfach miterlebt: Christian Wulff und Jörg Kachelmann, oder auch Christoph Mörgeli, sind bedenkenswerte Beispiele. Wie Geheimdienste im Besitz kompromittierender Informationen hier mitspielen können, wenn sie es für notwendig erachten, kann man sich lebhaft vorstellen.

Unerreichbare absolute Sicherheit

Von 1970 bis 2014 starben in Europa 6231 Menschen durch Terrorismus. In der Schweiz kam es zu 92 Todesfällen, wovon allein 47 Tote beim Anschlag auf einen Swissair-Flug nach Tel Aviv 1970 ums Leben kamen.[6] Zum Vergleich: im Schweizer Strassenverkehr sind im gleichen Zeitraum 38 014 Personen umgekommen.[7] Glenn Greenwald schreibt dazu: «Eine Bevölkerung, die körperliche Unversehrtheit über alle anderen Werte stellt, gibt letztlich die Freiheit auf und ermöglicht den Regierenden absolute Machtfülle, um dafür das illusorische Versprechen völliger Sicherheit zu erhalten. Absolute Sicherheit ist bloss eine Chimäre, die man vielleicht anstreben, aber nie erreichen kann.»[8] Die Anschläge in Paris vom 13. November 2015 haben es gezeigt: Trotz gigantischen Datensammlungen, grossem Überwachungsapparat und permanent erhöhter Wachsamkeit nach dem Anschlag auf die Redaktion des Satiremagazins «Charlie Hebdo» kann der Staat die Bürger nur bedingt vor Wahnsinnigen mit Maschinengewehren schützen – Terroristen überdies, die zu einem Grossteil aus eigenen Landsleuten bestehen. Die bereits bestehenden etwa 300 Massnahmen des Antiterrorplans Vigipirate fruchteten offenbar nicht. Darum ging die Assemblée Nationale einen Schritt weiter. Sie rief offiziell den Ausnahmezustand aus und ermächtigte die Polizei, ohne richterliche Anordnung Wohnungen zu durchsuchen und Personen präventiv unter Hausarrest zu stellen. Es versteht sich von selbst, was kommen musste: am 9. Februar 2016 entschied die Assemblée Nationale, das ursprünglich befristete Gesetz in der Verfassung zu verankern. Stimmt auch der Senat zu, muss die Reform noch in einer gemeinsamen Sitzung beider Parlamentskammern mit einer Dreifünftelmehrheit verabschiedet werden. Der US-amerikanische, kurz nach 9/11 verhängte «Patriot Act» hat es vorgemacht. Die Medien, welche die sensationsträchtigen Terrorereignisse – nicht zuletzt zum eigenen Vorteil – bewirtschaften können, und die durch sie eingeschüchterten Parlamentarier und Bürger helfen den Behörden dabei, Freiheiten mit dem Argument der Sicherheit zu begraben.

Der Wunsch nach Sicherheit ist zutiefst menschlich. Der Wunsch nach Privatsphäre und nach Freiheit aber eben auch. Die Bürger müssen sich in jedem Fall vor der Verletzung der Privatsphäre schützen dürfen und weiterhin selbst entscheiden können, welche Geheimnisse sie wem preisgeben. Selbstverständlich nutzen auch Kriminelle die Möglichkeiten der Verschlüsselung und erschweren so die Terrorabwehr – aber Kriminelle nutzen auch Küchenmesser. Dass die bestehenden Überwachungsmöglichkeiten zur Terrorabwehr zielgerichteter genutzt werden müssen, ist offensichtlich, aber auch ein Gemeinplatz. Weil Geheimdienste geheim sind, bleiben ihre Tätigkeiten so oder so undurchschaubar, völlig unabhängig davon, welcher Aufsicht sie unterstehen und welche Gesetze auch immer sie einschränken sollen. Ihre Regulierung ist vor allem per Budget und Personalpolitik möglich. Besser wäre es, den Staatsapparat auch in diesem Bereich kleinzuhalten und einzusehen, dass es absolute Sicherheit nicht geben kann. Und zu erkennen, dass wir zumindest ein Stück weit mit der Terrorgefahr leben müssen. So wie wir mit Erdbeben, Vulkanausbrüchen, Verkehrsunfällen und Flugzeugabstürzen leben müssen. Wer absolute Sicherheit erlangen will, befürwortet einen totalitären Staat. Wer frei bleiben will, muss etwas Unsicherheit ertragen können. ‹

[1] Vollständig einsehbar zum Beispiel auf https://snowdenarchive.cjfe.org/
[2] Matthew M. Aid: The Secret Sentry: The Untold History of the National Security Agency. New York: Bloomsbury Press, 2009 (Kapitel 16: «Crisis in the Ranks The Current Status of the National Security Agency»).
[3] «Überwachungsskandal: NSA speicherte mehr als 300 Berichte über Merkel», Spiegel.de, 29. März 2014:
http://www.spiegel.de/politik/deutschland/ueberwachung-nsa-speicherte-mehr-als-300-berichte-ueber-merkel-a-961414.html
[4] Glenn Greenwald: Die globale Überwachung. München: Droemer-Verlag, 2014, Seite 225.
[5] «NSA-Mitarbeiter spähten Partner oder Ex-Freundinnen aus», Derstandard.at, 28. September 2013
http://derstandard.at/1379292401433/NSA-Mitarbeiter-spaehten-Partner-oder-Ex-Freundinnen-aus
[6] National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database (GTD), University of Maryland. http://www.start.umd.edu/
[7] Bundesamt für Statistik/ASTRA: Entwicklung der Anzahl Getöteter im Strassenverkehr nach Monaten, 1963–2013. http://www.bfu.ch/de/Documents/04_Forschung_und_Statistik/02_Statistik/Zeitreihen/PDF/D_USV.WT.02.pdf
[8] Glenn Greenwald: Die globale Überwachung. München, Droemer-Verlag, 2014, Seite 295.

Pegida-Anhänger, Ende 2014 in Dresden. Die Bewegung der «besorgten Bürger» – oder «Bauchstalinisten», wie sie Kurt Imhof vielleicht genannt hätte – ist mittlerweile über ein Jahr alt und zieht immer noch regelmässig Hunderte am Montagabend auf die Strasse.
Bild: Milan Bures / The New York Times / Redux / laif.