

IMPULSE

Schützt Verschwiegenheit vor Rechenschaft?

Transparenz bei Telekommunikationsüberwachung
und Datenabfrage

Jan-Peter Kleinhans

Der vorliegende Impulse untersucht die Berichtspflichten deutscher Behörden und Unternehmen bzgl. Telekommunikationsüberwachung und Datenabfragen durch Sicherheitsbehörden. Was wird von staatlicher Seite aus veröffentlicht und auf welchen gesetzlichen oder freiwilligen Grundlagen geschieht dies? In welchem Umfang dürfen private Unternehmen sog. „Transparenzberichte“ veröffentlichen? Das Ergebnis lässt sich am besten als „Flickenteppich“ beschreiben, da nur zwei Behörden sehr punktuell über Anordnungen berichten, private Unternehmen mit Rechtsunsicherheiten kämpfen und über viele alltägliche Ermittlungswerkzeuge nicht berichtet wird.



Jan-Peter Kleinhans¹

In einem Urteil aus dem Jahr 2013 des Europäischen Gerichtshofs für Menschenrechte heißt es, dass es keine stabile Demokratie ohne Transparenz geben könne.² Demokratie braucht Transparenz, da nur durch sie staatliches Handeln kontrollierbar wird. Viele Initiativen des letzten Jahrzehnts, allen voran das Informationsfreiheitsgesetz³ und das Open Government Portal⁴, verdeutlichen einen Paradigmenwechsel: Der Wunsch der Bevölkerung nach mehr Transparenz über staatliches Handeln.

In einem modernen Rechtsstaat ist Transparenz kein Selbstzweck, sondern essenziell für die öffentliche Debatte und Meinungsbildung. Gerade in Bereichen, in denen die Bürgerinnen und Bürger das Vertrauen in die Regierung verloren haben, ist der Wunsch nach Transparenz groß. Dies wird durch die Diskussion über staatliche Überwachung durch Nachrichtendienste sehr gut verdeutlicht.

In der öffentlichen Debatte fehlt es an Sachlichkeit und konstruktiven Vorschlägen. Eine solche Debatte, die nicht nur wütend sondern vor allem konstruktiv ist, ist dringend notwendig, um die Effektivität, Verhältnismäßigkeit und Rechtsstaatlichkeit der verwendeten Maßnahmen zu beurteilen. Durch die hierfür notwendige Transparenz käme die Regierung ihrer Rechenschaftspflicht gegenüber den Bürgerinnen und Bürgern nach.

Um kritisch über das Thema diskutieren zu können, müsste man besser verstehen, was überhaupt passiert. Zurzeit ist es sehr undurchsichtig, wann und unter welchen Umständen persönliche Daten durch Sicherheitsbehörden erhoben werden. Ebenso, wann, durch wen und wie auf diese Daten zugegriffen werden darf.

Die vorliegende Studie untersucht daher wie viel zur Telekommunikationsüberwachung durch Behörden freiwillig oder per Gesetz veröffentlicht wird. Zusätzlich wird untersucht, welche Auskünfte die Regierung lediglich im Rahmen Kleiner und Mündlicher Anfragen erteilt. Außerdem wird analysiert, wie viel private Unternehmen öffentlich machen dürfen und welche Schritte als nächstes unternommen werden müssten, um die aktuelle Debatte über Überwachungsmaßnahmen und Datenabfragen durch Fakten zu stärken.

Berichtspflichten deutscher Behörden

Das Bundesamt für Justiz ist nach der Strafprozessordnung⁵ dazu verpflichtet, eine jährliche Statistik zu Überwachungsanordnungen zu veröffentlichen.⁶ Auch, wenn die Statistiken auf den ersten Blick sehr detailliert wirken, enthalten sie praktisch nur wenig Aussagekraft. Denn es werden lediglich Überwachungsanordnungen aufgelistet - statt den tatsächlich durchgeführten Maßnahmen. Unter einer (richterlichen) Anordnung können jedoch beliebig viele Maßnahmen durchgeführt werden. Als Beispiel sei hier die "Stille SMS" genannt. Es handelt sich dabei um ein Verfahren der Telekommunikationsüberwachung zur Standortbestimmung eines Verdächtigen. 2012 wurden fast 330.000 dieser "Ortungsimpulse" durch Zoll, Bundeskriminalamt, Bundespolizei und Verfassungsschutz versendet.⁷ Demgegenüber stehen knapp 18.000 Anordnungen zur Erhebung von Verkehrsdaten im Jahresbericht 2012 des Bundesamtes für Justiz.⁸ Gleiches gilt für die Funkzellenabfrage.⁹ Selbst eine statistische Auskunft über diese

⁵ §100b Abs. 5 StPO

⁶ <https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html> (abgerufen 03.06.2014)

⁷ <http://heise.de/-1951371> (abgerufen 03.06.2014)

⁸ https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/uebersicht_Verkehrsdaten_2012.pdf?__blob=publicationFile&v=2 (abgerufen 03.06.2014)

⁹ Bundestag Drucksache 17/6630 (<http://dipbt.bundestag.de/doc/btd/17/066/1706630.pdf>) (abgerufen 03.06.2014)

¹ Der Autor bedankt sich bei Haya Hadidi, Annegret König, Stefan Heumann, Markus Löning und Ben Scott für Anmerkungen und Kritik.

² <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-120955> (abgerufen 03.06.2014)

³ <https://fragdenstaat.de/> (abgerufen 03.06.2014)

⁴ <https://govdata.de/> (abgerufen 03.06.2014)

und ähnliche Maßnahmen der Telekommunikationsüberwachung sind bisher nur in Antworten auf kleine Anfragen des Bundestags veröffentlicht worden.

Über Maßnahmen der Telekommunikationsüberwachung im Zuge nachrichtendienstlicher Aktivitäten muss laut G10-Gesetz¹⁰ das Parlamentarische Kontrollgremium den Bundestag in einem jährlichen Bericht informieren. Die Berichte enthalten relativ detaillierte Angaben zu den benutzten Schlagwörtern in der strategischen Fernmeldeüberwachung oder die Anzahl der überwachten Personen. Da das G10-Gesetz jedoch lediglich vorschreibt, dass das Gremium den Bundestag "über Durchführung sowie Art und Umfang der Maßnahmen"¹¹ unterrichten soll, schwankt der Detailgrad und somit die Aussagekraft der Berichte über die Jahre.

Die dritte wichtige Instanz für Statistiken über Telekommunikationsüberwachungen bzw. Datenabfragen ist die Bundesnetzagentur. Diese ist per Telekommunikationsgesetz für das "Automatische Auskunftungsverfahren"¹² verantwortlich. Laut diesem Gesetz müssen Telekommunikationsanbieter es bestimmten deutschen Behörden ermöglichen voll-automatisiert nach Bestandsdaten von Kunden suchen zu können. So kann eine Behörde zu einer Telefonnummer Namen und Anschrift des Inhabers herausfinden. Ebenso ist die Suche nach Namen möglich. Dies geschieht voll-automatisch und ohne Richterbeschluss. Für das Verfahren sind zurzeit über 100 Behörden zugelassen, die dadurch Zugriff auf die Bestandsdaten von knapp 130 Telekommunikationsunternehmen haben.¹³ Das Gesetz schreibt vor, dass die verpflichteten Unternehmen von einzelnen Abfragen keine Kenntnis erhalten dürfen.¹⁴ In ihrem Jahresbericht veröffentlicht die Bundesnetzagentur Statistiken zum Automatisierten Auskunftungsverfahren. So gab

es 2013 rund 7 Millionen Abfragen, die zu etwa 36 Millionen Auskünften führten.¹⁵ Da die Bundesnetzagentur nicht verpflichtet ist, über das Automatisierte Auskunftungsverfahren zu berichten, fehlte im Jahresbericht 2012 auf einmal die entsprechende Statistik. Dieser ist mit 160 Seiten auch deutlich kürzer als die sonstigen Jahresberichte, die meist um die 270 Seiten umfassten. Es ist zu vermuten, dass 2012 die Statistiken zum Automatisierten Auskunftungsverfahren aus Platzgründen einfach weggekürzt wurden - 2013 tauchten sie wieder auf.

Das kurzzeitige Verschwinden der Statistik zum Automatisierten Auskunftungsverfahren aus dem Jahresbericht der Bundesnetzagentur verdeutlicht, wie wichtig gesetzlich vorgeschriebene Berichtspflichten sind. Die Unternehmen dürfen und können über das Automatisierte Auskunftungsverfahren nicht berichten - dies kann nur die Bundesnetzagentur. Und diese berichtet zur Zeit freiwillig, über ein Verfahren, bei dem das Bundesverfassungsgericht die Gefahr eines leichtfertigen Eingriffs in die Grundrechte feststellte.¹⁶

Transparenzberichte durch Unternehmen

Während Transparenzberichte bei US-amerikanischen IT-Unternehmen schon lange zum guten Ton gehören, machte in Deutschland der E-Mail Anbieter Posteo erst vor kurzer Zeit den Anfang.¹⁷ Dem Bericht ging ein ausführliches juristisches Gutachten voraus, das klären sollte, ob und in welchem Ausmaß Posteo über Anfragen von Sicherheitsbehörden berichten darf.¹⁸ Um für eine bessere Rechtssicherheit für Posteo zu sorgen, hatte der Bundestagsabgeordnete Hans-Christian Ströbele (B90/Grüne) sogar bei der Bundesregierung nachgefragt, ob entsprechende Statistiken durch E-Mail Anbieter, bzw. Service Provider, veröffentlicht

¹⁰ §14 Abs. 1 Satz 2 G10-Gesetz

¹¹ ibid.

¹² §112 TKG (<https://www.jurion.de/Gesetze/TKG-1/112>) (abgerufen 03.06.2014)

¹³ Siehe Jahresbericht 2013 Bundesnetzagentur, S. 102

¹⁴ §112 Abs. 1 Satz 6 TKG

¹⁵ <http://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/Publikationen/Berichte/berichte-node.html> (abgerufen 03.06.2014)

¹⁶ 1 BvR 1299/05

¹⁷ https://posteo.de/site/transparenzbericht_2013 (abgerufen 03.06.2014)

¹⁸ https://posteo.de/Gutachten_Transparenzbericht.pdf (abgerufen 03.06.2014)

werden können.¹⁹

Die Unsicherheit über das gesetzlich Zulässige entsteht durch den Umstand, dass Berichte von privaten Unternehmen im Gesetz keine Beachtung finden. Durch Interpretation der relevanten Gesetzestexte lässt sich lediglich - relativ unstrittig - ableiten, dass die jeweilige Verschwiegenheitspflicht privater Unternehmen, in Bezug auf Telekommunikationsüberwachungen, durch die Veröffentlichung von Statistiken nicht verletzt wird. Obwohl die relevanten Gesetze den Unternehmen explizit eine Verschwiegenheitspflicht vorschreiben, bezieht sich diese regelmäßig nur auf Auskünfte über laufende Ermittlungen – um eine Vereitelung der Ermittlungsmaßnahmen zu verhindern. Nach derzeitiger juristischer Meinung verletzen Unternehmen durch die Veröffentlichung von aggregierten Statistiken diese Verschwiegenheitspflicht daher jedoch nicht. Dass die Gesetze hier einigen Interpretationsraum bieten, zeigt die Tatsache, dass die Bundesnetzagentur wohl zwischenzeitlich Vodafone die Veröffentlichung eines Transparenzberichtes untersagt hatte - das Bundesjustizministerium dies aber, wie erwähnt, gegenüber Hans-Christian Ströbele eindeutig erlaubte.²⁰ Hier widersprachen sich also zwei Bundesbehörden zum gleichen Sachverhalt - die Bundesnetzagentur verbot vorübergehend, was das Bundesjustizministerium erlaubte. Selbst wenn Transparenzberichte durch das Gesetz explizit erlaubt wären, gäbe es jedoch trotzdem noch erhebliche Dunkelziffern bei Telekommunikationsanbietern. So gibt es einige Verfahren der Telekommunikationsüberwachung und Datenabfrage, über die private Unternehmen auch mittels Statistiken nicht aufklären können, da sie nicht involviert sind oder dies per Gesetz verboten ist. Hierzu zählen u.a.:

• **IMSI-Catcher:** Lediglich durch Kleine Anfragen im Bundestag weiß man, wie

häufig IMSI-Catcher zur Identifizierung, Standortbestimmung und Überwachung von Mobiltelefon-Besitzern eingesetzt wurden. So setzten Bundeskriminalamt, Bundespolizei und Zollkriminalamt 2011 rund 120 mal IMSI-Catcher zur strafprozessualen Verfolgung ein.

• **Funkzellenabfragen:** Informationen über die Häufigkeit und das Ausmaß von Funkzellenabfragen sind bisher auch nur durch Kleine und Mündliche Anfragen ans Tageslicht gekommen. Bei einer Funkzellenabfrage werden alle Mobilfunkteilnehmer einer Funkzelle ermittelt. Abhängig von der räumlichen Größe der Funkzelle und der Teilnehmerdichte werden unter Umständen mehrere zehntausend Mobilfunkteilnehmer erfasst. Als Ermittlungsinstrument wurde es durch die Landes- und den Bundesdatenschutzbeauftragten scharf kritisiert. So wurde durch das Bundeskriminalamt allein zur Untersuchung der NSU-Mordfälle mittels Funkzellenabfragen über 20 Millionen Datensätze analysiert, was zur Überprüfung von mehr als 13.000 Bestandsdaten führte.

• **Stille SMS:** Wie zuvor erwähnt, ist die "Stille SMS" ein weiteres Ermittlungswerkzeug, um Verkehrsdaten (Standort) von Mobiltelefonbesitzern zu gewinnen. Diese Maßnahme wird tagtäglich durch die verschiedenen Sicherheitsbehörden eingesetzt. Statistiken wurden bisher auch nur durch Kleine Anfragen veröffentlicht.

• **Automatisches Auskunftsverfahren:** Das im Telekommunikationsgesetz (TKG) geregelte Verfahren verbietet es den Unternehmen, von den einzelnen behördlichen Anfragen Kenntnis zu nehmen. So kann (und darf) die Telekom in ihrem jetzigen Transparenzbericht nicht über Abfragen mittels Automatisiertem Auskunftsverfahren berichten. Einzige Stelle, die hier Bericht erstatten könnte, ist die Bundesnetzagentur, die jedoch nicht zur Veröffentlichung verpflichtet ist.

¹⁹ <http://www.stroebele-online.de/themen/rechtspolitik/7545932.html>
(abgerufen 03.06.2014)

²⁰ <http://www.wiwo.de/unternehmen/it/transparenzbericht-50-000-telekom-anschluesse-ueberwacht/9846554.html> (abgerufen 03.06.2014)

Transparenz staatlicher Telekommunikationsüberwachung in Deutschland

Von den drei staatlichen Behörden, die Statistiken zur Telekommunikationsüberwachung veröffentlichen, sind nur zwei dazu gesetzlich verpflichtet - das Bundesamt für Justiz und die G10-Kommission. Das Bundesamt für Justiz berichtet zwar auf den ersten Blick sehr detailliert, allerdings nur über die Anzahl gerichtlicher Anordnungen und gerade nicht über die Häufigkeit einzelner Maßnahmen, wodurch die Statistik deutlich an Aussagekraft verliert. Die gesetzlichen Berichtspflichten der G10-Kommission lassen so viel Interpretationsraum übrig, dass der Detailgrad über die Jahre schwankt. Die dritte Behörde, die Bundesnetzagentur, müsste über das Automatisierte Auskunftsverfahren überhaupt nicht berichten. Mangels Transparenzpflicht verschwand in der Vergangenheit daher die Statistik auch zeitweise aus dem Jahresbericht.

Die privaten Telekommunikationsunternehmen wiederum sind nicht zur Veröffentlichung von Transparenzberichten verpflichtet. Es gibt hierzu auch keinerlei gesetzliche Vorgaben. Somit hängt es vom Selbstverständnis des Unternehmens ab, ob und in welchem Umfang Statistiken zu staatlichen Überwachungsmaßnahmen erstellt werden. Weiterhin ist die Rechtslage zumindest in Teilbereichen strittig. Doch selbst wenn Unternehmen berichten, müssen laut Gesetz bestimmte Maßnahmen, wie das Automatisierte Auskunftsverfahren, selbst als Statistik unerwähnt bleiben. Somit kann sich kein Gesamtbild ergeben.

Transparenz über staatliche Telekommunikationsüberwachung in Deutschland lässt sich daher am besten als "Flickenteppich" charakterisieren: Punktuell werden einzelne Zahlen relativ losgelöst vom Kontext veröffentlicht und lassen so kaum Rückschlüsse auf das Gesamtbild zu. Dies ist besonders bedenklich, da Verfahren zur Telekommunikationsüberwachung und Datenabfrage als Ermittlungsinstrumente für Sicherheitsbehörden immer wichtiger

werden. Die eingesetzten Verfahren und Techniken werden zudem stetig leistungsfähiger und günstiger im Einsatz. Daher sind die in dieser Studie beschriebenen Verfahren zu alltäglichen Ermittlungswerkzeugen deutscher Sicherheitsbehörden avanciert. Die Bürgerinnen und Bürger erhalten jedoch über Durchführung und Ausmaß dieser Formen der Überwachung und Datenabfrage wenig bis gar keine Auskünfte.

Lediglich durch gezielte Anfragen im Bundestag und investigativen Journalismus werden einzelne Zahlen bekannt, die dann wiederum isoliert und außerhalb des Kontexts betrachtet werden. So kann keine informierte, gesellschaftliche Debatte und letztlich auch keine Meinungsbildung entstehen - nur verständliche Empörung und ein Ohnmachtsgefühl gegenüber staatlicher Überwachung.

Ein Weg zu mehr Transparenz

Einige kleine Schritte würden bereits helfen, für deutlich mehr Transparenz zu sorgen. Die relevanten Statistiken, wie z.B. über "Stille SMS" oder Funkzellenabfragen, sind schon vorhanden, sonst wären entsprechende kleine Anfragen im Bundestag unbeantwortet geblieben. Die folgenden Punkte stellen daher erste Schritte dar, um mehr Transparenz bei staatlicher Telekommunikationsüberwachung zu schaffen:

- Das Bundesamt für Justiz sollte nicht nur über (richterliche) Überwachungsanordnungen berichten, sondern Statistiken zu den tatsächlich durchgeführten Maßnahmen erstellen. Es ist nicht nachvollziehbar, warum auf der einen Seite über die akustische Wohnraumüberwachung sehr detailliert berichtet wird – eine Maßnahme, die zwar sehr invasiv ist, aber auch nur sehr selten zum Einsatz kommt - auf der anderen Seite aber alltägliche Ermittlungswerkzeuge, wie die Funkzellenabfrage oder der IMSI-Catcher, im Dunkeln bleiben.
- Im Gesetz zur Bundesnetzagentur sollten Berichtspflichten dezidiert festgehalten

werden, insbesondere für das Automatisierte Auskunftsverfahren. Weiterhin sollten die einzelnen Behörden, die Zugriff auf das Abfragesystem haben, genannt werden - die bisher veröffentlichte Zahl von 102 Behörden hat wenig Aussagekraft.

- An zentraler Stelle im Gesetz sollte geregelt werden, von welchen staatlichen Maßnahmen Telekommunikationsunternehmen Statistiken veröffentlichen dürfen.

- Orientierung an den Tshwane Prinzipien: Für eine langfristige, in sich schlüssige Strategie zur Veröffentlichung von Daten sollte sich an den 50 Tshwane Prinzipien orientiert werden. Diese Prinzipien für nationale Sicherheit und das Recht auf Information wurden von 22 Institutionen und 500 Experten aus über 70 Ländern als Best Practice entwickelt. Letztes Jahr wurden sie sowohl durch das Europäische Parlament, als auch den Europarat befürwortet. Die Tshwane Prinzipien sollen den nationalen Gesetzgebern als Leitfaden bei der Modernisierung von Datenschutz- und Geheimdienstgesetzen dienen.

Eine klare und konsistente Gesetzgebung bzgl. Transparenz bei Maßnahmen der Telekommunikationsüberwachung und Datenabfrage würde nicht nur die derzeitige Debatte über staatliche Überwachung versachlichen. Vielmehr ist Transparenz über das Vorgehen der Sicherheitsbehörden zwingend notwendig, um über die Effektivität und Verhältnismäßigkeit staatlicher Überwachung zu urteilen. Dies würde weiterhin dazu beitragen einen Teil des Vertrauens in die Regierung wiederherzustellen.

Klare Vorgaben bzgl. Berichtspflichten der zuständigen Behörden entlasten diese nicht nur, sondern sind vor allem als Teil der Rechenschaftspflicht der Bundesregierung gegenüber den Bürgerinnen und Bürgern zu verstehen. Hier besteht dringender Bedarf seitens der Bundesregierung strikter zwischen notwendiger Verschwiegenheitspflicht über Ermittlungsmaßnahmen auf der einen Seite und jener Rechenschaftspflicht

gegenüber den Bürgerinnen und Bürgern auf der anderen Seite abzuwägen.

Jan-Peter Kleinhans ist seit 2014 Mitarbeiter der stiftung neue verantwortung im Programm „Europäische Digitale Agenda“. Dort kümmert er sich hauptsächlich um das Privacy Project. Zuvor arbeitete er bei und schrieb für Netzpolitik.org, vorrangig über die Snowden Enthüllungen, Datenschutz und Überwachungstechnologien. Vor seiner Zeit in Berlin studierte er Soziologie mit dem Schwerpunkt „Digitale Medien und Gesellschaft“ (MA) an der Uppsala Universität in Schweden. Seit seinem Studium der Wirtschaftsinformatik (BA) an der Technischen Universität Darmstadt beschäftigt er sich mit Überwachungstechnologie, dem Internet und den Auswirkungen auf unsere Gesellschaft.

Die stiftung neue verantwortung ist ein unabhängiger, gemeinnütziger und überparteilicher Think Tank mit Sitz in Berlin. Sie fördert kreatives, interdisziplinäres und sektorübergreifendes Denken zu den wichtigsten gesellschaftspolitischen Themen und Herausforderungen des 21. Jahrhunderts. Durch ihr Fellow- und Associateprogramm ermöglicht sie den intensiven Austausch junger Experten, Praktiker und Vordenker aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Das Privacy Project möchte dazu beitragen, eine breite, gesellschaftliche Debatte über den Schutz von Privatheit im Internet anzustoßen und dieses Thema auf die politische Agenda zu setzen. Es verfolgt dieses Ziel auf zweierlei Weise. Einerseits hat das Projekt zum Ziel, möglichst viele gesellschaftlichen Gruppen zusammenbringen, die das gemeinsame Interesse eint, diesen Themenkomplex auf die politische Agenda zu setzen. Dazu gehören sowohl Bürger- und Menschenrechtsgruppen und Nichtregierungsorganisationen wie auch Berufsverbände und Wirtschaftsunternehmen. Zweitens möchte das Projekt einen Beitrag dazu leisten, eine konstruktive Auseinandersetzung zum Thema Überwachung und Grundrechtsschutz anzustoßen. Hierzu werden Workshops mit Experten aus Behörden, Unternehmen und Universitäten durchgeführt. Ziel der Workshops ist es, Themenbereiche zu identifizieren, bei denen politischer Handlungsbedarf besteht, um Grundrechte und Privatheit im Internet besser zu schützen.

Impressum

Jan-Peter Kleinhans
jkleinhans@stiftung-nv.de

stiftung neue verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin
T. +49 30 81 45 03 78 80
F. +49 30 81 45 03 78 97
www.stiftung-nv.de
info@stiftung-nv.de

Gestaltung:
Pentagram Design, Berlin

Schlusslektorat:
Franziska Wiese

Kostenloser Download:
www.stiftung-nv.de



Dieser Beitrag unterliegt einer Creative Commons-Lizenz (CC BY-NC-SA). Die Vervielfältigung, Verbreitung und Veröffentlichung, Veränderung oder Übersetzung von Inhalten der stiftung neue verantwortung, die mit der Lizenz „CC BY-NC-SA“ gekennzeichnet sind, sowie die Erstellung daraus abgeleiteter Produkte sind unter den Bedingungen „Namensnennung“, „Nicht-Kommerziell“ und „Weiterverwendung unter gleicher Lizenz“ gestattet. Ausführliche Informationen zu den Lizenzbedingungen finden Sie hier:

<http://creativecommons.org/licenses/by-nc-sa/3.0/de/>