Piratenpartei Deutschland

Vorstand 2012-2014 - Beschluss #508

Antrag auf Unterzeichnung "Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung"

27 August 2013 14:02 - Veronique Schmitz

Status:	Angenommen	**Due date:**	18 September 2013
Priority:	Normal		
Assignee:	Markus Barenhoff		
Category:			
Beschlussart:	Umlaufbeschluss	**Abstimmung Thorsten:**	
Antragsteller:	Thomas Gaul	**Abstimmung Caro:**	
Sitzungsdatum:		**Abstimmung Björn:**	
Abstimmung Markus:	Ja	**Abstimmung Niqui:**	
Abstimmung Swanhild:	Enthaltung	**Abstimmung Gefion:**	
Abstimmung Katharina:	Ja	**Abstimmung Alexander:**	
Abstimmung Christophe:	Ja	**Abstimmung Stefan B:**	
Abstimmung Andreas:	Enthaltung	**Abstimmung Stephanie:**	
Umsetzungsverantwortlich:	Markus Barenhoff	**Abstimmung Sebastian:**	Abwesend
Abstimmung Sven:	Enthaltung	**Abstimmung Bernd:**	Nein
Abstimmung Klaus:	Nein		

Description

Antragsteller:

Thomas Gaul
@moonopool
@hekate15 Birgitt Piepgras
Martin 'Lama' Lange
@bengie_d bengie Basis
Florian Wagner/@BroeckelndeWand
@BerndSchreiner

Umsetzungsverantwortlich gem. Geschäftsordnung Art. 3 (2) des Bundesvorstandes:
Bundesvorstand der Piratenpartei Deutschland, hier vertreten durch Markus Barenhoff, ersatzweise die Internationalen Koordinatoren Gregory Engels und Thomas Gaul, je nach Benennung durch den Bundesvorstand

Ansprechpartner gem. Geschäftsordnung Art. 3 (2) des Bundesvorstandes:
Thomas Gaul

Antrag an den Bundesvorstand der Piratenpartei Deutschland

Der Bundesvorstand der Piratenpartei Deutschland möge beschliessen:

Wir unterstützen das Bestreben der Electronic Frontier Foundation und unterzeichnen als Piratenpartei Deutschland das folgende Dokument über "Internationale Grundsätze für die Anwendung der Menschenrechte in der

Kommunikationsüberwachung"

https://de.necessaryandproportionate.org/text
Originaltext: https://en.necessaryandproportionate.org/text

Im Volltext hier die "deutsche Übersetzung":

Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung
Translation revised by Digitalcourage e.V

Endgültige Version 10. Juli 2013

Während die Technologien, welche die staatliche Kommunikationsüberwachung unterstützen, verbessert werden, vernachlässigen die Staaten sicherzustellen, dass Gesetze und Verordnungen in Bezug auf Kommunikationsüberwachung in Einklang mit internationalen Menschenrechten stehen und die Rechte auf Privatsphäre und Meinungsfreiheit beachtet werden. Dieses Dokument versucht zu erklären, wie internationale Menschenrechte in der aktuellen digitalen Umgebung anwendbar sind, besonders vor dem Hintergrund des Wachstums und des Wandels der Technologien und Methoden der Kommunikationsüberwachung. Diese Grundsätze können zivilgesellschaftlichen Gruppen, der Wirtschaft, Staaten und anderen einen Rahmen liefern, mit dem sie bewerten können, ob aktuelle oder geplante Überwachungsgesetze oder -praktiken im Einklang mit den Menschenrechten stehen.

Diese Grundsätze sind das Ergebnis einer globalen Beratung mit Gruppen der Zivilgesellschaft, der Wirtschaft und internationalen Experten für Recht, Politik und Technologien in der Kommunikationsüberwachung.

Einleitung

Privatsphäre ist ein Grundrecht, das wesentlich ist für den Erhalt von demokratischen Gesellschaften. Es ist grundlegend für die menschliche Würde und verstärkt andere Rechte, wie Meinungs-, Informations- und Versammlungsfreiheit, und es ist nach internationalen Menschenrechtsgesetzen anerkannt.[1] Aktivitäten, die das Recht auf Privatsphäre begrenzen, einschließlich Kommunikationsüberwachung, können nur dann als gerechtfertigt gelten, wenn sie gesetzlich vorgeschrieben sind, sie notwendig sind, um ein legitimes Ziel zu erreichen, und sie dem Ziel, welches sie verfolgen, angemessen sind.[2]

Vor der öffentlichen Einführung des Internets schufen fest etablierte legale Grundsätze und der Kommunikationsüberwachung innewohnende logistische Hürden Grenzen für die staatliche Kommunikationsüberwachung. In gegenwärtigen Dekaden haben die logistischen Barrieren der Überwachung abgenommen und die Anwendung der gesetzlichen Grundsätze in neuen technologischen Kontexten sind unklarer geworden. Die Explosion der Inhalte digitaler Kommunikation und Information über Kommunikation, sogenannte „Verbindungsdaten“ - Informationen über die Kommunikation eines Individuums oder Nutzung elektronischer Geräte - die sinkenden Kosten der Speicherung und des Dataminings und die Bereitstellung von persönlichen Inhalten durch Drittanbieter machen staatliche Überwachung in einem beispiellosen Ausmaß möglich[3]Dabei haben Konzeptualisierungen der bestehenden Menschenrechtsgesetze nicht Schritt gehalten mit den modernen und sich verändernden Möglichkeiten der Kommunikationsüberwachung des Staates, der Fähigkeit des Staates, aus verschiedenen Überwachungstechniken gewonnene Informationen zu kombinieren und zu organisieren, oder der erhöhten Sensibilität der Informationen, die zugänglich werden.

Die Häufigkeit, mit der Staaten Zugang zu Kommunikationsinhalten und –metadaten suchen, steigt dramatisch - ohne angemessene Kontrolle.[4] Wenn Kommunikationsmetadaten aufgerufen und analysiert werden, kann damit ein Profil einer Person, einschließlich des Gesundheitszustandes,

politischer und religiöser Ansichten, Verbindungen, Interaktionen und Interessen, erstellt werden. So werden genauso viele oder sogar noch mehr Details offengelegt, als aus dem Inhalt der Kommunikation erkennbar wäre.[5] Trotz des riesigen Potenzials für das Eindringen in das Leben eines Menschen und der abschreckenden Wirkung auf politische und andere Vereinigungen, weisen rechtliche und politische Instrumente oft ein niedrigeres Schutzniveau für Kommunikationsmetadaten auf und führen keine ausreichenden Beschränkungen dafür ein, wie sie später von Behörden verwendet werden, einschließlich wie sie gewonnen, geteilt und gespeichert werden.

Damit Staaten tatsächlich ihren internationalen menschenrechtlichen Verpflichtungen in Bezug auf Kommunikationsüberwachung nachkommen, müssen sie den im Folgenden genannten Grundsätzen entsprechen. Diese Grundsätze gelten für die Überwachung der eigenen Bürger eines Staates, die in seinem eigenen Hoheitsgebiet ausgeführt wird, sowie der Überwachung anderer in anderen Gebieten. Die Grundsätze gelten außerdem unabhängig vom Zweck der Überwachung - Strafverfolgung, nationale Sicherheit oder sonstige behördliche Ziele. Zudem gelten sie sowohl für die Aufgabe des Staates, die Rechte des Einzelnen zu respektieren und zu erfüllen, als auch für die Verpflichtung, die Rechte des Einzelnen vor Missbrauch durch nicht-staatliche Akteure, einschließlich der Wirtschaft, zu schützen.[6] Der private Sektor trägt die gleiche Verantwortung für die Wahrung der Menschenrechte, insbesondere in Anbetracht der Schlüsselrolle, die sie bei der Konzeption, Entwicklung und Verbreitung von Technologien spielt, und damit Kommunikation ermöglicht und bereitstellt und - wo erforderlich - mit staatlichen Überwachungsmaßnahmen zusammenarbeitet. Dennoch ist der Umfang der vorliegenden Grundsätze auf die Pflichten des Staates beschränkt.

Veränderte Technologie und Definitionen

„Kommunikationsüberwachung“ umfasst heutzutage Überwachung, Abhören, Sammlung, Analyse, Nutzung, Konservierung und Aufbewahrung von, Eingriff in oder Zugang zu Informationen, welche die Kommunikation einer Person in der Vergangenheit, Gegenwart oder Zukunft beinhaltet, reflektiert oder sich daraus ergibt. “Kommunikation“ beinhaltet Aktivitäten, Interaktionen und Transaktionen, die über elektronische Medien übertragen werden, wie z. B. Inhalt der Kommunikation, die Identität der an der Kommunikation Beteiligten, die Standort-Tracking, einschließlich IP-Adressen, die Uhrzeit und die Dauer der Kommunikation und Kennungen von Kommunikationsgeräten, die während der Kommunikation verwendet werden.

Traditionell wurde die Invasivität der Kommunikationsüberwachung auf Basis von künstlichen und formalen Kategorien bewertet. Bestehende rechtliche Rahmenbedingungen unterscheiden zwischen „Inhalt“ oder „Nicht-Inhalt“, „Teilnehmerinformation“ oder „Metadaten“, gespeicherten Daten oder Übertragungsdaten, Daten, die zuhause gespeichert werden oder die im Besitz eines dritten Diensteanbieters sind.[7] Allerdings sind diese Unterscheidungen nicht mehr geeignet, den Grad des Eindringens der Kommunikationsüberwachung in das Privatleben von Einzelpersonen und Verbänden zu messen. Während seit Langem Einigkeit darin besteht, dass Kommunikationsinhalte per Gesetz signifikanten Schutz verdienen wegen ihrer Fähigkeit, sensible Informationen zu offenbaren, ist es nun klar, dass andere Informationen aus der Kommunikation - Metadaten und andere Formen der nicht-inhaltlichen Daten - vielleicht sogar mehr über eine Einzelperson enthüllen können, als der Inhalt selbst und verdienen daher einen gleichwertigen Schutz. Heute könnte jede dieser Informationsarten für sich allein oder gemeinsam analysiert die Identität einer Person, deren Verhalten, Verbindungen, physischen oder gesundheitlichen Zustand, Rasse, Hautfarbe, sexuelle Orientierung, nationale Herkunft oder Meinungen enthüllen, oder die Abbildung einer Person mithilfe der Standortbestimmung, ihrer Bewegungen oder Interaktionen über einen Zeitraum,[8] ermöglichen oder auch von allen Menschen an einem bestimmten Ort, zum Beispiel bei einer öffentlichen Demonstration oder anderen politischen Veranstaltung. Als Ergebnis sollten alle Informationen, welche sich aus der Kommunikation einer Person ergeben,

diese beinhalten, reflektieren, oder über diese Person stattfinden, und welche nicht öffentlich verfügbar und leicht zugänglich für die allgemeine Öffentlichkeit sind, als „geschützte Informationen“ angesehen werden. Ihnen sollte dementsprechend der höchste gesetzliche Schutz gewährt werden.

Bei der Beurteilung der Invasivität der staatlichen Kommunikationsüberwachung, ist es notwendig, dass beides betrachtet wird: sowohl das Potenzial der Überwachung, geschützte Informationen offenzulegen, sowie der Zweck, zu der Staat die Information sammel.. Kommunikationsüberwachung, die voraussichtlich zur Offenlegung von geschützten Informationen führt, die eine Person dem Risiko der Ermittlung, Diskriminierung oder Verletzung der Menschenrechte aussetzen kann, wird eine ernsthafte Verletzung des Rechts des Einzelnen auf Privatsphäre darstellen und außerdem die Nutzung anderer Grundrechte untergraben, unter anderem das Recht auf freie Meinungsäußerung, Versammlungsfreiheit und politische Partizipation. Dies liegt darin begründet, dass diese Rechte erfordern, dass Menschen in der Lage sind, frei von der abschreckenden Wirkung der staatlichen Überwachung zu kommunizieren. Eine Festlegung sowohl des Charakters als auch der Einsatzmöglichkeiten der gesuchten Informationen wird somit in jedem Einzelfall notwendig.

Bei der Annahme einer neuen Technik der Kommunikationsüberwachung oder der Ausweitung des Anwendungsbereichs einer bestehenden Technik sollte der Staat sicherstellen, ob die Informationen, die wahrscheinlich beschafft werden, in den Bereich der „geschützten Informationen“ fällt, bevor er sie einholt, und sie zur Kontrolle der Justiz oder anderen demokratischen Kontrollorganen vorlegen. Wenn man bedenkt, ob eine Information, die man mithilfe von Kommunikationsüberwachung erhalten hat, auf die Ebene der „geschützten Informationen“ aufsteigt, sind sowohl die Form als auch der Umfang und die Dauer der Überwachung relevante Faktoren. Weil tiefgreifende oder systematische Überwachung die Fähigkeit hat, private Informationen weit über seine einzelnen Teile hinaus zu offenbaren, kann es Überwachung der nicht geschützten Informationen auf ein Niveau von Invasivität heben, das starken Schutz verlangt.[9]

Die Festlegung, ob der Staat die Kommunikationsüberwachung, die geschützte Informationen betrifft, durchführen darf, muss im Einklang mit den folgenden Grundsätzen stehen.

Die Grundsätze

Gesetzmäßigkeit:
Jede Beschränkung des Rechtes auf Privatsphäre muss gesetzlich vorgeschrieben sein. Der Staat darf in Abwesenheit eines bestehenden öffentlich verfügbaren Rechtsaktes, welcher den Standard der Klarheit und Genauigkeit erfüllt, und der ausreicht, um sicherzustellen, dass Einzelne eine Benachrichtigung erhalten und seine Anwendung vorhersehen können, keine Maßnahmen einführen oder durchsetzen, die das Recht auf Privatsphäre beeinträchtigen. Angesichts der Geschwindigkeit des technologischen Wandels sollten Gesetze, die das Recht auf Privatsphäre beschränken, regelmäßig durch Instrumente eines partizipativen legislativen und behördlichen Prozesses überprüft werden.

Rechtmäßiges Ziel:
Gesetze sollten nur Kommunikationsüberwachung durch spezifizierte Behörden erlauben, um ein legitimes Ziel zu erreichen, welches einem überragend wichtigen Rechtsgut, das in einer demokratischen Gesellschaft notwendig ist, entspricht. Es darf keine Maßnahme angewendet werden, die auf der Grundlage von Rasse, Hautfarbe, Geschlecht, Sprache, Religion, politischer oder sonstiger Überzeugung, nationaler oder sozialer Herkunft, Vermögen, Geburt oder des sonstigen Status diskriminiert.

Notwendigkeit:

Gesetze, die Kommunikationsüberwachung durch den Staat erlauben, müssen die Überwachung darauf begrenzen, was zweifellos und nachweislich notwendig ist, um das legitime Ziel zu erreichen. Kommunikationsüberwachung darf nur durchgeführt werden, wenn es das einzige Mittel zur Erreichung eines rechtmäßigen Ziels ist, oder wenn es mehrere Mittel gibt, es das Mittel ist, welches am unwahrscheinlichsten die Menschenrechte verletzt. Der Nachweis der Begründung dieser Rechtfertigung in gerichtlichen sowie in Gesetzgebungsverfahren liegt beim Staat.

Angemessenheit:
Jeder Fall der gesetzlich autorisierten Kommunikationsüberwachung muss geeignet sein, das spezifische legitime Ziel, welches festgelegt wurde, zu erfüllen.

Verhältnismäßigkeit:
Kommunikationsüberwachung sollte als hochgradig invasive / (or: eindringende) Handlung angesehen werden, die in das Recht auf Privatsphäre und die Freiheit der Meinungsäußerung eingreift und die Grundlagen einer demokratischen Gesellschaft bedroht. Entscheidungen über Kommunikationsüberwachung müssen durch Abwägen der gesuchten Vorteile gegen die Schäden, die den Rechten des Einzelnen und anderen konkurrierenden Interessen zugefügt würden, getroffen werden, und sollten eine Betrachtung der Sensibilität der Informationen und der Schwere der Verletzung des Rechts auf Privatsphäre einbeziehen.

Dies erfordert insbesondere:
Sollte ein Staat Zugang zu oder die Nutzung von geschützten Informationen anstreben, die durch Kommunikationsüberwachung im Rahmen einer strafrechtlichen Untersuchung gesammelt wurden, dann muss dies auf der zuständigen, unabhängigen und unparteiischen gerichtlichen Entscheidung begründet sein, dass:

- es eine hohe Wahrscheinlichkeit gibt, dass ein schweres Verbrechen begangen wurde oder begangen werden wird;
- der Beweis eines solchen Verbrechens durch den Zugriff auf die geschützten Daten erhalten werden würde;
- andere verfügbare und weniger invasive Ermittlungsmethoden ausgeschöpft sind;
- die abgerufenen Informationen in vernünftiger Weise auf diejenigen begrenzt werden, die für die mutmaßliche Straftat relevant sind, und jede weitere gesammelte Information sofort vernichtet oder zurückgegeben wird; und
- Informationen nur von der festgelegten Behörde abgerufen und nur für den Zweck, für den die Genehmigung erteilt wurde, verwendet werden.
- Wenn der Staat mit Kommunikationsüberwachung Zugang zu geschützten Informationen zu einem Zweck erlangen will, der eine Person nicht der Strafverfolgung, Ermittlung, Diskriminierung oder Verletzung der Menschenrechte aussetzt, muss der Staat einer unabhängigen, unparteiischen und zuständigen Behörde Folgendes nachweisen:
- andere verfügbare und weniger invasive Ermittlungsmethoden wurden in Betracht gezogen;
- die abgerufenen Informationen werden in vernünftiger Weise auf die relevanten begrenzt und jede zusätzlich gesammelte Information wird sofort vernichtet oder dem betroffenen Individuum zurückgegeben; und Informationen werden nur von der festgelegten Behörde abgerufen und nur für den Zweck verwendet, für den die Genehmigung erteilt wurde.

Zuständige gerichtliche Behörden:
Bestimmungen in Bezug auf die Kommunikationsüberwachung müssen von zuständigen gerichtlichen Behörden, die unparteiisch und unabhängig sind, festgelegt werden. Die Behörde muss:

- getrennt sein von der Behörde, welche die Kommunikationsüberwachung durchführt,
- vertraut sein mit den relevanten Themen und fähig sein, eine gerichtliche Entscheidung über die Rechtmäßigkeit der Kommunikationsüberwachung, die benutzte Technologie und Menschenrechte zu treffen, und
- über entsprechende Ressourcen verfügen, um die ihr übertragenen Aufgaben auszuführen.

Rechtsstaatliches Verfahren:
Ein rechtsstaatliches Verfahren verlangt, dass Staaten die Menschenrechte jedes Einzelnen respektieren und garantieren, indem sie rechtmäßige Prozesse versichern, die jegliche Beeinträchtigung der Menschenrechte ordnungsgemäß und gesetzlich spezifiziert regeln, die konsistent durchgeführt werden, und die der allgemeinen Öffentlichkeit zugänglich sind. Insbesondere bei der Bestimmung seiner oder ihrer Menschenrechte hat jeder das Recht auf ein faires und öffentliches Verfahren innerhalb einer angemessenen Frist von einem unabhängigen, zuständigen und unparteiischen rechtmäßig

gegründeten Gericht,[10] außer in Notfällen, wenn für Menschenleben Gefahr in Verzug ist. In solchen Fällen, muss innerhalb einer vernünftigen und realisierbaren Frist eine rückwirkende Autorisierung eingeholt werden. Lediglich das Risiko der Flucht oder Zerstörung von Beweismitteln soll niemals als ausreichend für eine rückwirkende Autorisierung angesehen werden.

*Benachrichtigung des Nutzers:*Personen sollten über die Entscheidung der Autorisierung einer Kommunikationsüberwachung informiert werden. Es sollten ausreichend Zeit und Informationen zur Verfügung gestellt werden, so dass die Person die Entscheidung anfechten kann. Des Weiteren sollte sie Zugang zu dem Material bekommen, welches für den Antrag der Autorisierung vorgelegt wurde. Eine Verzögerung der Benachrichtigung ist nur unter folgenden Bedingungen gerechtfertigt:

- Die Benachrichtigung würde den Zweck, für den die Überwachung genehmigt ist, ernsthaft gefährden oder es besteht eine unmittelbare Gefahr für Menschenleben, oder
- Die Erlaubnis einer Verzögerung der Benachrichtigung wird durch die zuständige Justizbehörde zum Zeitpunkt der Genehmigung der Überwachung erteilt; und
- Die betroffene Person wird benachrichtigt, sobald die Gefahr aufgehoben ist, oder innerhalb einer vernünftigen realisierbaren Frist, je nachdem, welches zuerst zutrifft, aber in jeden Fall zu dem Zeitpunkt zu dem die Kommunikationsüberwachung abgeschlossen ist. Die Verpflichtung zur Benachrichtigung liegt beim Staat, aber in dem Fall, dass der Staat dem nicht nachkommt, sollten Kommunikationsdiensteanbieter die Freiheit haben, Personen über die Kommunikationsüberwachung freiwillig oder auf Anfrage zu benachrichtigen.

Transparenz:
Staaten sollten bezüglich der Nutzung und des Umfangs der Techniken und Befugnisse der Kommunikationsüberwachung transparent sein. Sie sollten mindestens die gesammelten Informationen über die Anzahl der genehmigten und abgelehnten Anfragen, eine Aufschlüsselung der Anfragen nach Dienstanbieter und nach Ermittlungsart und -zweck veröffentlichen. Staaten sollten Personen genügend Informationen liefern, um zu gewährleisten, dass sie den Umfang, die Art und Anwendung der Gesetze, welche die Kommunikationsüberwachung erlauben, zu verstehen. Staaten sollten Diensteanbieter befähigen, die von ihnen angewendeten Prozesse zu veröffentlichen, wenn sie staatliche Kommunikationsüberwachung bearbeiten, an diesen Prozessen festzuhalten und Berichte der staatlichen Kommunikationsüberwachung zu veröffentlichen.

Öffentliche Aufsicht:
Staaten sollten unabhängige Aufsichtsmechanismen schaffen, die Transparenz und Verantwortung der Kommunikationsüberwachung gewährleisten.[11] Aufsichtsmechanismen sollten die Befugnis haben, auf alle potenziell relevanten Informationen über staatliche Maßnahmen, wenn notwendig auch auf geheime oder als Verschlusssachen gekennzeichnete Informationen zuzugreifen; zu beurteilen, ob der Staat seine rechtmäßigen Fähigkeiten legitim nutzt; zu beurteilen, ob der Staat die Informationen über den Einsatz und den Umfang der Techniken und Befugnisse der Kommunikationsüberwachung transparent und genau veröffentlicht hat; und regelmäßige Berichte und andere für die Kommunikationsüberwachung relevante Informationen zu veröffentlichen. Unabhängige Kontrollmechanismen sollten in Ergänzung zur Aufsicht geschaffen werden, die bereits über einen anderen Teil der Regierung zur Verfügung steht.

Integrität der Kommunikation und der Systeme:
Um die Integrität,
Sicherheit und Privatsphäre der Kommunikationssysteme zu gewährleisten, und in Anerkennung der Tatsache, dass Abstriche bei der Sicherheit für staatliche Zwecke fast immer die Sicherheit im Allgemeinen infrage stellen, sollten Staaten die Dienstleister oder Hardware- oder Softwarehändler nicht zwingen, Überwachungs- oder Beobachtungsfunktionen in ihre Systeme einzubauen oder bestimmte Informationen lediglich für Zwecke der staatlichen Überwachung zu sammeln oder zu speichern. A priori Vorratsdatenspeicherung oder Sammlung sollte nie von Dienstleistern gefordert werden. Personen haben das Recht, sich anonym zu äußern; Staaten sollten daher auf die zwingende Identifizierung der

Nutzer als Voraussetzung für die Leistungserbringung verzichten.[12]

Schutzmaßnahmen für die internationale Zusammenarbeit:
Als Reaktion auf
die Veränderungen der Informationsflüsse und Kommunikationstechnologien
und -dienstleistungen, kann es notwendig sein, dass Staaten Hilfe von
einem ausländischen Dienstleister anfordern. Dementsprechend sollten die
gemeinsamen Rechtshilfeverträge und andere Vereinbarungen, die von den
Staaten eingegangen wurden, sicherstellen, dass in Fällen, in denen die
Gesetze mehr als eines Staates für die Kommunikationsüberwachung
angewendet werden können, derjenige verfügbare Standard mit dem höheren
Schutzniveau für den Einzelnen angewendet wird. Wo Staaten Unterstützung
für Zwecke der Strafverfolgung suchen, sollte der Grundsatz der
beiderseitigen Strafbarkeit angewendet werden. Staaten dürfen gemeinsame
Rechtshilfeprozesse und ausländische Anfragen nach geschützten
Informationen nicht nutzen, um inländische gesetzliche Beschränkungen
der Kommunikationsüberwachung zu umgehen. Gemeinsame Rechtshilfeprozesse
und andere Vereinbarungen sollten klar dokumentiert werden, öffentlich
zugänglich sein und dem Schutz des fairen Verfahrens unterliegen.

Schutzmaßnahmen gegen unrechtmäßigen Zugang:
Die Staaten sollten
Gesetze erlassen, welche illegale Kommunikationsüberwachung durch
öffentliche oder private Akteure kriminalisieren. Die Gesetze sollten
ausreichende und erhebliche zivil-und strafrechtliche Sanktionen, Schutz
für Whistleblower und Wege für die Wiedergutmachung von Betroffenen
enthalten. Die Gesetze sollten vorsehen, dass alle Informationen, welche
in einer Weise gesammelt wurden, die mit diesen Grundsätzen unvereinbar
ist, in einem Verfahren als Beweise unzulässig sind, genauso wie
Beweise, die von solchen Informationen abgeleitet sind. Die Staaten
sollten außerdem Gesetze erlassen mit der Maßgabe, dass das Material
zerstört oder der Person zurückgegeben werden muss, nachdem das durch
Kommunikationsüberwachung gesammelte Material, zu dem Zweck genutzt
wurde, zu welchem es bereitgestellt wurde.

Begründung:

Bereits im Juli 2013 hat die EFF (Electronic Frontier Foundation) nach
einem langen Abstimmungsprozeß den vorstehenden 13 Grundsätze
formuliert. Gerade während dieses Wahlkampfes, wo jeden Tag neue
Enthüllungen über staatliche Überwachung die Schlagzeilen prägen, ist
eine eindeutige Positionierung der PIRATEN sehr wichtig. Die von der EFF
formulierten Grundsätze decken sich mit den programmatischen Aussagen
der Piratenpartei und lesen sich in weiten Teilen wieAbschriften aus dem
Wahlprogramm. Die Piratenpartei sollte diese Gelegenheit wahrnehmen,
einerseits die internationalen NGOs zu unterstützen und andererseits ein
weiteres Mal klarzustellen, dass PIRATEN im Bundestag sich auch als
parlamentarischer Arm dieser Bewegung verstehen und verhalten werden.

*Annex: */Hinweise auf das Parteiprogramm:/

http://wiki.piratenpartei.de/Bundestagswahl_2013/Wahlprogramm#Freiheit_und_Grundrechte

Die Piratenpartei Deutschland setzt sich für einen starken Datenschutz
und das Prinzip der informationellen Selbstbestimmung ein. Dies umfasst
nicht nur die sparsame Erhebung, zweckgebundene Verarbeitung und Nutzung
sowie die eingeschränkte Weitergabe von personenbezogenen Daten, sondern
ebenso die Stärkung der Rechte des Einzelnen, grundsätzlich selbst über
die Preisgabe und Verwendung personenbezogener Daten zu bestimmen. Im
Sinne des Prinzips der Informationssicherheit muss die Vertraulichkeit
bei Übertragung und Zugriff sowie die Integrität der gespeicherten Daten
gewährleistet sein.

Die Piratenpartei Deutschland lehnt die verdachtsunabhängige
Durchleuchtung der Bürger und den gläsernen Kunden ab. Im digitalen
Zeitalter liegen immer mehr personenbezogene Informationen in

elektronischer Form vor, werden automatisiert verarbeitet und verknüpft oder weitergegeben – auch über Ländergrenzen hinweg und zwischen den öffentlichen und nicht-öffentlichen Bereichen. Ohne Wissen der Betroffenen kann die wachsende Datenflut automatisiert zu Persönlichkeitsprofilen zusammengefügt und im schlimmsten Fall gegen sie verwendet werden – z. B. durch das so genannte Kreditscoring oder die Erstellung von Surf- und Bewegungsprofilen."

Der Einzelne muss einen durchsetzbaren und unentgeltlichen Anspruch auf Selbstauskunft, Korrektur, Sperrung oder Löschung der eigenen personenbezogenen Daten haben und über ungewollte Datenabflüsse aus Unternehmen und Behörden unverzüglich und lückenlos informiert werden. Um das bestehende Auskunftsrecht zu einer Mitteilungpflicht weiterzuentwickeln, fordert die Piratenpartei die Einführung des Datenbriefes und die Verankerung desselben in den Bundesdatenschutzgesetzen des Bundes und der Länder. Firmen, Behörden und Institutionen, die personenbezogene Daten verarbeiten, übermitteln oder speichern, sollen dazu verpflichtet werden, die betroffenen Personen jährlich mit einem Datenbrief über die Art, den Zweck und – im Fall von Behörden und mit staatlichen Aufgaben beliehenen Institutionen – die rechtliche Grundlage der Speicherung zu informieren. Die Weitergabe von Daten an Dritte soll kommuniziert und begründet werden."

Zu diesem Ziel soll die völlige Unabhängigkeit der Kontrollstellen entsprechend der EU-Datenschutzrichtlinie und der Rechtsprechung des Europäischen Gerichtshofes (EuGH) sichergestellt werden. Die Kontrollbehörden müssen entsprechend ihren Aufgaben ausgestattet werden, damit sie ihre Aufsichts- und Kontrollfunktion auch ausüben können.

Für Unternehmen sowie öffentliche Stellen fordert die Piratenpartei darüber hinaus rechtlich anerkannte freiwillige Datenschutz- und Datensicherheitsprüfungen (Audits) sowie Zertifizierungen durch die unabhängigen Behörden."

Die Piratenpartei Deutschland lehnt die Vorratsdatenspeicherung (VDS) von Telekommunikations-Verbindungsdaten grundsätzlich ab. Zweck und Mittel dieser Überwachungsmaßnahme stehen aus Sicht der PIRATEN nicht in einem ausgewogenen Verhältnis. Die anlasslose Speicherung ist ein weiterer Schritt in Richtung schrankenloser Telekommunikationsüberwachung und stellt die Bevölkerung unter Generalverdacht."

Auch andere Formen der verdachtsunabhängigen Datenerfassung, wie z. B. die Hotelmeldepflicht oder das Nachfolgeprojekt des elektronischen Entgeltnachweis-Verfahrens ELENA, OMS (Optimiertes Meldeverfahren in der sozialen Sicherung), beurteilt die Piratenpartei kritisch.
Die Piratenpartei lehnt die anlasslose Erfassung, Speicherung und den Abgleich biometrischer Daten aufgrund des hohen Missbrauchspotenzials ab. Grundsätzlich soll die Erhebung biometrischer Merkmale freiwillig erfolgen und durch unabhängige Stellen kontrolliert und bewertet werden. Der Aufbau zentraler Biometriedatenbanken für polizeiliche Zwecke oder die Versicherungswirtschaft muss unterbleiben. Ausweis- und Passdokumente müssen auch ohne biometrische Merkmale gültig sein – auch im Ausland. "

Gegen Überwachungssoftware: Transparenz und Quellcode-Offenlegung

Die Piratenpartei Deutschland spricht sich deutlich gegen die Herstellung, Wartung, Betreuung und Erhaltung von Überwachungssoftware aus. Sie verurteilt den kommerziellen Handel mit Überwachungssoftware, einschließlich Dienstleistungen für Überwachungssoftware. Überwachungssoftware ist jede Software, die Dritten Zugang zu nicht-öffentlichen Daten, Kommunikationen und Aktivitäten eines Rechensystems verschaffen kann, ohne dass die eigentlichen Nutzer des Rechensystems darüber Kenntnis haben. Der Grund für diese Position ist, dass Überwachungssoftware sowohl im Inland wie weltweit eingesetzt wird, um Menschenrechte wie das Recht auf Privatsphäre auszuhebeln. Häufig

werden die so erhaltenen privaten Daten genutzt, um Regimegegner zu verfolgen und sogar zu foltern, und um Bewegungen für mehr Demokratie zu bekämpfen.

Um aktiv gegen Überwachungssoftware vorzugehen, fordert die Piratenpartei eine gesetzliche Pflicht bei Herstellern und Dienstleistern von Überwachungssoftware, volle Transparenz über alle Produkte, und über alle Vertragspartner und Kunden, die Überwachungssoftware und Dienstleistungen nutzen, herzustellen. Desweiteren fordert die Piratenpartei die gesetzliche Pflicht zur Offenlegung des vollständigen Quellcodes von Überwachungssoftware. Die Offenlegung all dieser Informationen hat an die Öffentlichkeit zu geschehen, das bedeutet: nicht nur an ein parlamentarisches Kontrollgremium. "

Betroffene von Überwachungsmaßnahmen müssen informiert werden

Verdeckte Überwachungsmaßnahmen laden zum Missbrauch ein. Deswegen müssen Betroffene von staatlichen Abhör- und Überwachungsmaßnahmen grundsätzlich benachrichtigt werden. Die derzeitigen Regelungen zur Benachrichtigungspflicht sind aufgrund der zahlreichen Ausnahmen wirkungslos. Die Piratenpartei setzt sich daher dafür ein, dass die überwachende Behörde ohne Ausnahme alle ihr bekannten Betroffenen einer Überwachungsmaßnahme innerhalb einer festen, nicht verlängerbaren Frist benachrichtigen und über die erfassten Daten informieren muss.
Keine Bundes- oder Staatstrojaner "

Für die Piratenpartei sind verdeckte Eingriffe in informationstechnische Systeme durch den Staat nicht mit Grundrechten und Rechtsstaat vereinbar. Wir setzen uns daher für die Abschaffung der Befugnisse für staatliche Behörden zum Verwanzen solcher Systeme ein. "

Piraten gegen Cyberwar

Offene und verdeckte Aktionen von staatlichen, privaten und öffentlichen Organisationen, die den Cyberspace als Konfliktdomäne nutzen und die Zivilbevölkerung gefährden, lehnen wir dezidiert ab. Schadsoftware, die in der Lage ist Menschenleben durch Angriffe auf gesellschaftliche Versorgungsnetzwerke (Stichwort: KRITIS) zu gefährden, betrachten wir als inakzeptables Sicherheitsrisiko und fordern ein Bekenntnis von Regierungen, im speziellen der deutschen Regierung, zu friedenserhaltenden Maßnahmen, gemäß den internationalen Konventionen zur Verbesserung des friedlichen menschlichen Zusammenlebens durch Technik auf der Welt. Die Piratenpartei Deutschland fordert alle Regierungen dieser Erde auf, die globalen Informations- und Kommunikationsnetze gemeinsam zu schützen und als ein hohes gemeinschaftliches Gut aller Menschen anzuerkennen.″

Innere Sicherheit

Sicherheit in Freiheit

Bewahrung und Ausbau unserer Bürger- und Freiheitsrechte sind für uns zentrale politische Herausforderungen. Die steigende Zahl von Überwachungsgesetzen und Überwachungsmaßnahmen unter Verweis auf den ‚internationalen Terrorismus' und andere ‚Bedrohungen', der mangelnde Bestand solcher Gesetze vor der Verfassung, die teils für rechtswidrig erklärten Maßnahmen gegen politischen Protest und die wiederkehrenden Skandale bei deutschen Geheimdiensten belegen gravierenden Handlungsbedarf.

Nationale Kriminalpräventionsstrategie

Um schon den Ursachen von Kriminalität entgegenzuwirken, wollen wir den Schwerpunkt unserer Sicherheitspolitik auf die Förderung von Kriminalpräventionsmaßnahmen und -projekten legen, deren Wirksamkeit - anders als bei Überwachungsmaßnahmen - wissenschaftlich erwiesen ist (z. B. Präventionsprojekte mit Jugendlichen aus sozial gefährdeten

Familien). Besonders wichtig ist uns dies bei Kindern und Jugendlichen. Wir wollen dazu eine nationale Präventionsstrategie entwickeln.

Sicherheitsbewusstsein stärken

Die gefühlte Sicherheit ist eine wichtige Voraussetzung für unser persönliches Wohlbefinden. Forschungsergebnisse zeigen aber, dass das hohe Maß an Sicherheit in Deutschland verbreitet unbekannt ist und dass das Kriminalitätsrisiko teilweise weit überschätzt wird. Wir wollen ein Programm zur Stärkung des Sicherheitsbewusstseins und zur sachlichen Information über Kriminalität in Deutschland auflegen, um verzerrten Einschätzungen und Darstellungen der Sicherheitslage entgegen zu wirken.

Systematische Evaluierung von Überwachungsbefugnissen und -programmen

Vor Kriminalität zu schützen ist eine wichtige staatliche Aufgabe. Sie kann nach unserer Überzeugung nur durch eine intelligente, rationale und evidenzbasierte Sicherheitspolitik auf der Grundlage wissenschaftlicher Erkenntnisse erfüllt werden. Um kluge Sicherheitsmaßnahmen fördern und schädliche Maßnahmen beenden zu können, wollen wir, dass eine dem Bundestag unterstellte Deutsche Grundrechteagentur alle bestehenden und neu zu schaffenden Befugnisse und Programme der Sicherheitsbehörden systematisch und nach wissenschaftlichen Kriterien auf ihre Wirksamkeit, Kosten, schädlichen Nebenwirkungen, auf Alternativen und auf ihre Vereinbarkeit mit unseren Grundrechten untersucht (systematische Evaluierung). Auf dieser Grundlage können wir sodann Grundrechtseingriffe aufheben oder verhindern, wo dies ohne Einbußen an Sicherheit – also ohne Einfluss auf die Kriminalitätsrate – möglich ist oder wo sich der Eingriff als unverhältnismäßig erweist. Wir wollen auch auf Maßnahmen verzichten, deren Effizienz so gering ist, dass die dadurch gebundenen Mittel an anderer Stelle mehr zu unserer Sicherheit beitragen können.

Privatsphäre rechtstreuer Bürger achten

Zur Bewahrung unseres historischen Erbes an Freiheitsrechten und zur Sicherung der Effektivität der Gefahrenabwehr und Strafverfolgung treten wir dafür ein, dass eine staatliche Informationssammlung, Kontrolle und Überwachung künftig nur noch gezielt bei Personen erfolgt, die der Begehung oder Vorbereitung einer Straftat konkret verdächtig sind. Zum Schutz unserer offenen Gesellschaft und im Interesse einer effizienten Sicherheitspolitik wollen wir auf anlasslose, massenhafte, automatisierte Datenerhebungen, Datenabgleichungen und Datenspeicherungen verzichten. In einem freiheitlichen Rechtsstaat ist eine derart breite Erfassung beliebiger unschuldiger Personen nicht hinnehmbar und schädlich.

Freiheitspaket verabschieden

Unnötige und exzessive Überwachungsgesetze der letzten Jahre wollen wir mit einem „Freiheitspaket“ wieder aufheben, darunter

- die Übertragung exekutiver Polizeibefugnisse einschließlich Online-Durchsuchung auf das Bundeskriminalamt,
- gemeinsame Dateien von Polizeien und Geheimdiensten,
- die flächendeckende Erhebung biometrischer Daten sowie deren Speicherung in RFID-Ausweisdokumenten,
- die lebenslängliche Steuer-Identifikationsnummer,
- das elektronische Bankkontenverzeichnis,
- die verpflichtende elektronische Gesundheitskarte,
- die Überwachung von Wohnungen, von Ärzten, Rechtsanwälten, Geistlichen,
- Abgeordneten und anderen Vertrauenspersonen,
- den Identifizierungszwang für Handy- und Internetnutzer,
- das Verbot anonymen elektronischen Bargeldes (Zahlungskarten) über 100 Euro sowie
- die Auslieferung von Personendaten an die USA und andere Staaten ohne wirksamen Grundrechtsschutz.

Neue Überwachungspläne stoppen

Um den fortschreitenden Abbau der Bürgerrechte seit 2001 zu stoppen,

fordern wir ein Moratorium für weitere Grundrechtseingriffe im Namen der Kriminalitätsbekämpfung, solange nicht die systematische Überprüfung der bestehenden Befugnisse abgeschlossen ist. Insbesondere lehnen wir ab

- eine flächendeckende Protokollierung aller unserer Telefon- oder Internetverbindungen (Vorratsdatenspeicherung) gleich für welche Dauer,
- eine Vorratsspeicherung von Flug-, Schiff- und sonstigen Passagierdaten,
- eine systematische Überwachung des Zahlungsverkehrs oder sonstige Massendatenanalyse (Stockholmer Programm der EU),
- den Einsatz von Überwachungsdrohnen sowie
- den Einsatz von Rasterfahndungs-Software in Online-Netzwerken.

Grundrechtskonformität der Gesetzgebung stärken
In den letzten Jahren musste das Bundesverfassungsgericht immer häufiger Gesetze aufheben, die unsere Grund- und Freiheitsrechte verletzten. Zur Verhinderung verfassungswidriger Gesetze wollen wir einem Drittel des Deutschen Bundestages oder zwei Fraktionen das Recht geben, ein Rechtsgutachten des Bundesverfassungsgerichts zur Verfassungskonformität eines Gesetzesvorhabens einzuholen. Der Bundespräsident soll darüber hinaus das Recht erhalten, bei verfassungsrechtlichen Zweifeln vor der Ausfertigung eines Gesetzes das Bundesverfassungsgericht anzurufen. Nach dem Vorbild anderer Verbandsklagerechte wollen wir Bürgerrechtsorganisationen die Möglichkeit eröffnen, stellvertretend für die Allgemeinheit vor den Fachgerichten und dem Bundesverfassungsgericht gegen Grundrechtsverletzungen zu klagen.

Sicherheitsforschung demokratisieren

Die Sicherheitsforschung aus Steuergeldern wollen wir demokratisieren und an den Bedürfnissen und Rechten der Bürgerinnen und Bürger ausrichten. In beratenden Gremien sollen künftig neben Verwaltungs- und Industrievertretern in gleicher Zahl auch Volksvertreter sämtlicher Fraktionen, Kriminologen, Opferverbände und Nichtregierungsorganisationen vertreten sein. Eine Entscheidung über die Ausschreibung eines Projekts soll erst getroffen werden, wenn eine öffentliche Untersuchung über die Auswirkungen des jeweiligen Forschungsziels auf unsere Grundrechte (impact assessment) vorliegt.
Die Entwicklung von Technologien zur verstärkten Überwachung, Erfassung und Kontrolle von Bürgerinnen und Bürgern lehnen wir ab. Stattdessen muss die Sicherheitsforschung auf sämtliche Optionen zur Kriminal- und Unglücksverhütung erstreckt werden und eine unabhängige Untersuchung von Wirksamkeit, Kosten, schädlichen Nebenwirkungen und Alternativen zu den einzelnen Vorschlägen zum Gegenstand haben."

http://wiki.piratenpartei.de/Parteiprogramm(Grundsatz / Parteiprogramm)

"Weltweite Anerkennung und Schutz selbstbestimmter geschlechtlicher oder sexueller Identität bzw. Orientierung
Verfolgung aufgrund der geschlechtlichen oder sexuellen Identität bzw. Orientierung ist Unrecht. Wenn solche Verfolgung im Herkunftsland offiziell oder inoffiziell von staatlicher oder nichtstaatlicher Seite betrieben wird, muss sie als Asylgrund anerkannt werden. Die Betroffenen müssen ihre Geschlechtsidentität oder sexuelle Orientierung hierfür nicht nachweisen.
In vielen Ländern der Welt werden Menschen wegen ihrer geschlechtlichen oder sexuellen Identität bzw. Orientierung diskriminiert oder kriminalisiert, wenn sie von der dort jeweils gültigen Norm abweicht.
Eine solche Diskriminierung oder Kriminalisierung lehnen wir ab.
Abweichende geschlechtliche oder sexuelle Identität bzw. Orientierung darf ferner nicht als Krankheit oder Perversion eingestuft werden."

History

#1 - 27 August 2013 14:03 - Veronique Schmitz

aus OTRS übernommen https://support.piratenpartei.de/otrs/index.pl?Action=AgentTicketZoom;TicketID=91182

#2 - 04 September 2013 19:15 - Veronique Schmitz

- Due date changed from 04 September 2013 to 18 September 2013

vertagt auf die nächste Sitzung

#3 - 05 September 2013 07:33 - Anonymous

- Abstimmung Klaus set to Nein

Inhaltlich ist alles töfte, der Antrag ist aber ein Paradebeispiel für Symbole ohne Wert. Nichtmal eine PM als Ergebnis der Unterzeichnung wurde vorgesehen, geschweige denn andere konkrete Folgen/Ergebnisse. Wir können das unterzeichnen, es passiert danach aber genau: Nichts. Meine negative Meinung zu diesen folgenlosen Unterstützungsbeschlüssen ist bekannt, daher auch hier wieder: Nein.

#4 - 25 September 2013 18:31 - Bernd Schlömer

- Abstimmung Bernd set to Nein

#5 - 26 September 2013 07:27 - Anonymous

- Status changed from Offen to Angenommen

- Abstimmung Sebastian set to Abwesend

- Abstimmung Markus set to Ja

- Abstimmung Swanhild set to Enthaltung

- Abstimmung Katharina set to Ja

- Abstimmung Sven set to Enthaltung

- Abstimmung Christophe set to Ja

- Abstimmung Andreas set to Enthaltung

#6 - 29 November 2013 11:34 - Anonymous

Die Umsetzung hier ist immer noch offen, Stand heute hat die Piratenpartei das Dokument nicht unterzeichnet.