Internationale Arbeitsgruppe
für Datenschutz
in der Telekommunikation

675.50.26

Arbeitspapier zu Transparenzberichten:

Förderung der Rechenschaftspflicht staatlicher Stellen beim Zugriff auf personenbezogene Daten, die sich im Besitz von Unternehmen befinden

57. Sitzung, Seoul (Republik Korea), 27.-28. April 2015

– Übersetzung –

"Doveryai, no proveryai."
- Von Ronald Reagan zitiertes russisches Sprichwort, das so viel bedeutet wie "Vertraue, aber prüfe nach."

„Sind alle Einzelheiten bekannt, ist der Kopf zufrieden und die Fantasie verliert den Drang, ihre eigenen Flügel zu nutzen."
- Thomas Bailey Aldrich, amerikanischer Dichter und Schriftsteller

„Der Geheimhaltungscharakter der Sicherheitsüberwachung hindert vielerorts die Legislative, Judikative und die Öffentlichkeit an der Überprüfung staatlicher Befugnisse. Diese mangelnde Transparenz [...] führt zu wesentlichen Hindernissen bei der Vermeidung einer willkürlichen oder unbedachten Nutzung dieser Befugnisse."
- Navi Pillay, Hohe Kommissarin der Vereinten Nationen für Menschenrechte

Inhalt

Dieses Papier untersucht den Nutzen der Erstellung von Transparenzberichten durch Telekommunikationsunternehmen und Anbieter von Internetdienstleistungen für den Datenschutz und die Privatsphäre. Transparenzberichte sind nützlich, um das Vertrauen in Organisationen mit großen Beständen an personenbezogenen Daten zu fördern. Sie tragen zudem dazu bei, öffentliche Stellen für ihre Praktiken bei Auskunftsbegehren in Bezug auf diese Daten zur Rechenschaft zu ziehen.

In diesem Papier bezeichnet „Transparenzbericht" die regelmäßige Veröffentlichung von Statistiken und begleitenden Erläuterungen durch für die Verarbeitung Verantwortliche oder Auftragsverarbeiter darüber, welche personenbezogenen Daten für unternehmensfremde Zwecke an Dritte weitergegeben wurden. Der Schwerpunkt dieses Papiers liegt auf der Weitergabe an Ordnungsbehörden[1] sowie

[1] Im Sinne dieses Papiers sind unter "Ordnungsbehörden" sowohl Aufsichtsbehörden als auch Strafverfolgungsbehörden zu verstehen. In vielen Rechtssystemen versuchen Aufsichtsbehörden, Ministerien und Kommunalverwaltungen häufig, Zugang zu Daten zu erhalten, die sich im Besitz von Unternehmen befinden.

Sekretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Telefon: +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

nationale Sicherheitsbehörden, ohne andere Formen der unternehmensfremden Weitergabe auszuschließen.[2]

Obwohl sich das Papier hauptsächlich auf die Berichte von Organisationen des privaten Sektors im Bereich der Telekommunikation konzentriert, können die Beobachtungen und Empfehlungen des Papiers auch für öffentliche Stellen und außerhalb des Telekommunikationssektors tätige Organisationen relevant sein.[3]

Nicht direkt eingegangen wird in diesem Papier auf damit zusammenhängende Themen, wie die Rechtfertigungsgründe für den Zugriff durch Ordnungsbehörden oder nationale Sicherheitsbehörden auf die Akten oder Daten von Organisationen, die angemessenen gesetzlichen Grenzen für einen solchen Zugriff oder die Genehmigung und Kontrolle eingriffsintensiver Überwachungsmaßnahmen seitens der Ermittlungsbehörden.[4] Diese Themen werden in einigen anderen Arbeitsgruppenpapieren behandelt und es könnte hilfreich sein, diese in Verbindung mit diesem Papier zu lesen.[5]

Die Arbeitsgruppe unterstützt die Erstellung von Transparenzberichten, da diese das Potenzial haben, die Rechenschaftspflicht bei der Verarbeitung personenbezogener Daten zu fördern. Organisationen, die Transparenzberichte verfassen, sollten sicherstellen, dass die veröffentlichten Statistiken zuverlässig, informativ und international vergleichbar sind.[6]

Hintergrund

Um ihre öffentlichen Aufgaben wahrzunehmen, muss es staatlichen Stellen bei Bedarf möglich sein, auf Daten zuzugreifen, die sich im Besitz von privaten Organisationen befinden.[7] Ein klassisches Beispiel ist die Überprüfung der Unterlagen eines Unternehmens, um sicherzugehen, dass die Steuern korrekt bezahlt wurden. Die staatliche Nachfrage nach Unterlagen in privatem Besitz steigt seit Jahrzehnten stetig und gibt somit Anlass zu Besorgnis hinsichtlich der bürgerlichen Freiheiten und des Erfüllungsaufwands.
Umfang und Volumen staatlicher Nachfrage nach Zugriff auf Informationen in Firmenbesitz, insbesondere Informationen über Einzelpersonen, sind seit 2001 erheblich gewachsen. Dieses Wachstum

---

[2] Ein anderes Beispiel ist etwa die Weitergabe im Zuge von Notfällen oder bei Sicherheitsvorfällen.
[3] Zum Beispiel für den Finanzdienstleistungsbereich oder für Kreditauskunfteien.
[4] Für eine Diskussion vieler der allgemeinen Aspekte aus dem Bereich Datenschutz siehe Centre for Democracy and Technology, *Systematic Access to Government Data: A Comparative Analysis*, 2013. Frühere Fallstudien zum systematischen staatlichen Zugriff auf Daten des privaten Sektors sind verfügbar unter http://idpl.oxfordjournals.org/content/2/4.toc.
[5] Alle Arbeitspapiere der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation (IWGDPT) sind zu finden unter http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group. Siehe z. B. das Arbeitspapier der IWGDPT mit dem Titel Recht auf vertrauliche Telekommunikation (Berlin, September 2013) sowie die „Granada Charta" des Datenschutzes in einer digitalen Welt (Granada, April 2010).
[6] Während Unternehmen oft freiwillig Berichte vorlegen, kann es auch Rechtssysteme geben, in denen spezifischere Anforderungen an die Berichterstattung und deren Form gestellt werden. Solche Anforderungen haben natürlich gegenüber den allgemeinen Leitlinien in diesem Papier Vorrang. Größtmögliche internationale Vergleichbarkeit bleibt zwar wünschenswert, aber zusätzliche, lokal gestellte Anforderungen können trotzdem einen wertvollen Beitrag zur Förderung einer besseren Vergleichbarkeit innerhalb von Branchen und einzelnen Rechtssystemen leisten.
[7] Der Einfachheit halber werden diese im vorliegenden Papier als Informationen bzw. Unterlagen „in Firmenbesitz" bezeichnet. Dadurch soll betont werden, dass der Schwerpunkt in erster Linie auf staatlichen Anfragen an für die Verarbeitung von Daten Verantwortliche im nicht-öffentlichen Bereich oder an Auftragsverarbeiter liegt.

spiegelt die wachsende Attraktivität der Daten des privaten Sektors für den Staat wider, die sich aus mehreren technologischen und wirtschaftlichen Faktoren ergibt, zu denen die folgenden gehören:

- *Verfügbarkeit von Daten:* Die Kosten für die Speicherung von Daten sind erheblich zurückgegangen und sinken weiter. Dadurch ist es möglich, große Mengen an Transaktionsdaten langfristig zu speichern.
- *Verarbeitungskapazität:* Es wurden große Fortschritte erzielt, was die Fähigkeit angeht, gewaltige Datenmengen schnell zuzuordnen, zu verarbeiten und zu analysieren. Big Data hat sich zu einem großen Geschäftsfeld entwickelt.[8] [9]
- *Spezialisierte Techniken sind jetzt Mainstream:* Waren viele datenbasierte analytische Verfahren einst einigen wenigen vorbehalten, so sind sie in der Wirtschaft (und Verwaltung) mittlerweile zum Standard geworden. Hierzu gehören etwa prädiktive Analysen, Kontaktketten („contact chaining"), die Visualisierung von Daten und die Netzwerkanalyse.
- *Neue Geschäftsmodelle:* Es haben sich neue und lukrative Geschäftsmodelle entwickelt, die auf der Analyse von Transaktionsdaten und der Verknüpfung von Datensätzen basieren. Anbieter von Cloud-Diensten besitzen Informationen von vielen Unternehmen außerhalb der jeweiligen Firmensysteme.
- *Übergang von mündlicher zu schriftlicher Kommunikation:* Der Wandel von der analogen hin zur digitalen Telefonie führte zur Entwicklung praktischer Datendienste wie SMS. Dadurch wurden die Nutzer motiviert, die nicht dauerhafte mündliche Kommunikation durch schriftliche Mitteilungen zu ersetzen, die langfristig gespeichert werden können. Beschleunigt wurde dieser Trend durch den massenhaften Umstieg auf Handys und Smartphones.
- *Massenhafte Spuren personenbezogener Daten, die Einzelpersonen unbemerkt hinterlassen:* Der Übergang von der analogen zur digitalen Telefonie hat zur Folge, dass mehr Verkehrsdaten anfallen, die gespeichert und analysiert werden können. Durch Smartphones und GPS sind Lokalisierungsdienste entstanden, die sensible Informationen erzeugen, die es zuvor nie gab. Hinzu kommen immer mehr Sensoren und die Entstehung des Internets der Dinge, die – oft ohne menschliches Eingreifen – personenbezogene Daten erzeugen.
- *Nutzergenerierte Inhalte:* Internetdienste und in jüngerer Zeit auch soziale Medien haben das Nutzerverhalten verändert: Viele Menschen veröffentlichen ihre persönlichen und geschäftlichen Daten nun so, dass der Regierungen leicht darauf zugreifen können – mittels Daten der Firmen oder sogar durch die komplette Umgehung betrieblicher Kontrollmechanismen.[10]

Diese technologischen und wirtschaftlichen Faktoren allein können jedoch die Zunahme staatlichen Zugriffe nicht erklären. Weitere Faktoren auf staatlicher Seite sind:

- *Öffentlich-private Verbindungen:* Die Grenzen zwischen dem öffentlichen und dem privaten Sektor sind mittlerweile fließend. Vorgehensweisen aus dem privaten Sektor wurden vom öffentlichen Sektor übernommen. Öffentliche Versorgungsbetriebe, die Zugang zu wichtigen Daten über ganze Kommunen haben, wurden zusammen mit ihren Leistungen und ihrem Datenbesitz privatisiert. Regierungen sind zu Akteuren im Daten-Ökosystem des Privatsektors geworden, sowohl als Datenquelle als auch als Nutzer von Datendiensten. Private Unternehmen haben sich zu maßgeblichen Akteuren der Ermittlungs- und Sicherheitsarbeit entwickelt.

---

[8] Siehe die Arbeitspapiere der IWGDPT zu Big Data und Datenschutz - Bedrohung der Grundsätze des Datenschutzes in Zeiten von Big-Data-Analysen (Skopje, May 2014) sowie zu Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes (Sopot, April 2012).

[9] Siehe 36. Internationale Datenschutzkonferenz (ICDPPC), Entschließung zu Big Data, Mauritius 2014, und 34. Internationale Datenschutzkonferenz (ICDPPC), Entschließung zu Cloud Computing, Uruguay 2012. Die Entschließungen der ICDPPC sind abrufbar unter www.icdppc.org.

[10] Dieses Papier beschäftigt sich nur mit Fällen, in denen es um Informationen in Firmenbesitz geht. Alle Aspekte, die die Privatsphäre und Rechenschaftspflicht im Rahmen eines staatlichen Zugriffs auf öffentlich zugängliche Informationen betreffen oder mit der Umgehung betrieblicher Kontrollen zusammenhängen, werden hier nicht behandelt.

- *Strafverfolgung und nationale Sicherheit:* Seit 2001 besteht seitens der Öffentlichkeit, der Legislative und der Gerichte eine stärkere Bereitschaft dazu, den nationalen Sicherheits- und Strafverfolgungsbelangen Vorrang gegenüber traditionellen Normen der betrieblichen Vertraulichkeit einzuräumen. Das Thema Strafverfolgung hat sich in vielen Bereichen manifestiert, darunter vor allem in der Luftfahrt[11] und auf dem Gebiet der Finanzdienstleistungen.[12] Es gibt nicht mehr nur den klassischen staatlichen Zugriff auf Firmendaten auf Grundlage zielgerichteter Ermittlungen gegen Personen, die unter dem Verdacht stehen, eine Straftat begangen zu haben. Vielmehr werden nun durch die Analyse gewaltiger Datensätze ganze Bevölkerungsgruppen überwacht, um Aktivitäten oder Personen von Interesse ausfindig zu machen. Die Schwelle für die Genehmigung von Überwachungsmaßnahmen ist in vielen Gerichtsbarkeiten gesunken. Gleichzeitig hat sich die Menge von Informationen erhöht, die mit einer einzigen Anordnung gesammelt werden können. In vielen Ländern werden Transaktionsdaten in Systemen zur Massenüberwachung nun zunehmend routinemäßig überwacht und nicht mehr nur auf der Basis einer einzelnen Ermittlung.
- *Neustrukturierung von Telekommunikationsdiensten, um den staatlichen Interessen zu dienen:* Normalerweise haben sich öffentliche Stellen damit begnügt, auf Daten in Firmenbesitz dann zuzugreifen, wenn diese Daten existierten und entsprechende Firmensysteme den Zugriff ermöglichten. In den letzten Jahren haben Regierungen jedoch die Beziehung zwischen dem öffentlichen und dem privaten Sektor neu ausgerichtet. Viele Regierungen haben Gesetze erlassen und Vereinbarungen mit Netzbetreibern getroffen, um für viel Geld die Schaffung von „Hintertüren“ vorzuschreiben. Diese soll einen staatlichen Zugriff auf Systeme in den Fällen ermöglichen, in denen ein solcher Zugriff aus unternehmerischen Gründen nicht nötig wäre.[13][14]
- *Verlagerung von Aufwand vom Staat auf die Unternehmen*: Der Gebrauch herkömmlicher Durchsuchungsbefehle bleibt zwar ein wesentliches Element strafrechtlicher Ermittlungen, hat dem Staat aber eine erhebliche administrative Last auferlegt. Es wurden neue gesetzliche Instrumente entwickelt, die den Aufwand für die Lokalisierung, Sammlung und Erhebung von Daten zum Zwecke staatlicher Kontrolle auf die Unternehmen verlagert.[15]
- *Neuordnung der Speicherungsverpflichtungen zur Erfüllung staatlicher Interessen:* Regierungen haben Unternehmen nicht nur dazu aufgefordert, Informationen, die sich zum Zwecke staatlicher Kontrolle in ihrem Besitz befinden, zu erheben und zu sammeln. Sie haben auch gefordert, diese Daten über einen längeren Zeitraum aufzubewahren (auch wenn dafür keine unternehme-

---

[11] Ein besonderer Schwerpunkt liegt auf Transaktionsinformationen zu Reisenden (oft als „Fluggastdatensätze“ oder „PNR-Daten“ bezeichnet). Siehe 29. ICDPPC, Entschließung zum Schutz von Passagierdaten, 2007.

[12] Besonders Geldwäsche und Terrorismusfinanzierung stehen dabei im Fokus.

[13] Viele Länder fordern, dass digitale Telekommunikationssysteme, die Leistungen für die Öffentlichkeit erbringen, abhörfähig gemacht werden. Dieses Beispiel zeigt eindeutig, dass staatlichen Interessen Vorrang gegenüber dem Schutz der Privatsphäre in der Kommunikation eingeräumt wird. Einige Länder verbieten auch anonyme Handy-Konten.

[14] Staatliche Forderungen nach einer Hintertür sind natürlich nicht neu. Solche Forderungen gab es schon vorher im Zusammenhang mit Post- und Telegrafiesystemen sowie analogen Systemen. Ein derartiger Zugriff war für den Staat früher besonders einfach, als er im Besitz dieser Telekommunikationssysteme war oder nur mit einem einzigen Betreiber zu tun hatte. Dennoch erscheint dieser Trend noch immer beachtenswert, da der Staat nicht einfach nur administrativen Zugang zu Systemen fordert, sondern auch erhebliche und kostspielige Systemänderungen, die Auswirkungen auf viele Unternehmen haben können und manchmal dem legitimen Wunsch der Unternehmen nach der Schaffung sicherer Netzwerke zuwiderlaufen.

[15] Diese Befugnisse werden manchmal als Herausgabe- oder Unterstützungsanordnungen bezeichnet.

rische Notwendigkeit besteht) für den Fall, dass öffentliche Stellenim Rahmen von Ermittlungen auf diese Informationen zugreifen müssen.[16]

Zusammengenommen führen diese Faktoren dazu, dass die Informationen, die sich im Besitz des Privatsektors befinden, eine noch attraktivere Informationsquelle als früher für öffentliche Stellen darstellen. Während Informationen früher nicht vorhanden oder unzugänglich waren, so kann der Staat heutzutage auf einen gewaltigen Informationsbestand zugreifen. Aus staatlicher Sicht ist es praktisch, dass sich die Informationen statt innerhalb einzelner Unternehmen nun im Besitz von Anbietern von Informationsdienstleistungen und in Netzwerken befinden. Interessante Informationen sind oftmals mit zusätzlichen Informationen verknüpft, was ihren Wert steigert. Die unermessliche Menge an verfügbaren Daten hätte früher ein unüberwindbares Hindernis für eine nützliche oder rechtzeitige Analyse dargestellt. Doch die steigende Computerkapazität und Fortschritte bei Verarbeitungsverfahren ermöglichen staatlichen Stellen hochgesteckte Ziele bei der Datenerfassung und bei analytischen Projekten. Aufgrund dieser Änderungen können öffentliche Stellen Informationen nun entweder in großen Mengen sammeln oder nach Belieben darauf zugreifen.

Das Umfeld, in dem solche Projekte entstehen, ist für die staatlichen Interessen immer günstiger geworden. Viele spektakuläre Terroranschläge haben in der Öffentlichkeit Besorgnis hervorgerufen und dienten als Rechtfertigung für Maßnahmen zugunsten der nationalen Sicherheit und Strafverfolgung, mit denen öffentliche Stellen noch stärker auf Daten von Unternehmen zugreifen können.

Seit 2001 wurden zahlreiche Gesetze erlassen, die den Ordnungsbehörden größeren Zugriff auf Informationen ermöglichen, die sich im Besitz von Unternehmen befinden. Normalerweise würden diese Gesetze genau die Grenzen des Zugriffs präzise definieren und die rechtmäßigen Verfahren beschreiben, mittels derer Befugnisse ausgeübt werden können. In der Vergangenheit hätte der Zugriff auf Daten in Firmenbesitz für gewöhnlich eine richterliche Anordnung erfordert. In der elektronischen Umgebung können in Verbindung mit staatlichen Befugnissen neue Paradigmen entstehen. Während die Legislative oft versucht hat, die ursprünglichen Normen zu erhalten, haben die konstante Ausweitung von Gesetzen und Forderungen nach entwicklungsoffener Regulierung zu flexibleren Konzepten geführt, welche wiederum ausnahmslos erweiterte Zugriffsmöglichkeiten zur Folge hatten.[17]

Während das Ausmaß der rechtmäßigen Befugnisse bei Strafverfolgungsbehörden nur gelegentlich unklar ist, ist dies bei Geheimdiensten oder Sicherheitsorganisationen mit einem nationalen Sicherheitsmandat fast immer der Fall. Die Grenzen der Befugnisse und Garantien hinsichtlich der Ausübung von Befugnissen sind, wenn nationale Sicherheitsziele angeführt werden, in der Regel weniger robust oder transparent als im Bereich der Strafverfolgung. Und die Menge an zugänglichen Informationen ist für gewöhnlich viel größer.

Sowohl die Ermittlungen von Strafverfolgungsbehörden als auch das Sammeln von Erkenntnissen über die nationale Sicherheit erfolgen häufig im Geheimen. Sobald jedoch die Ermittlungen abgeschlossen sind, herrscht aufgrund der Rolle einer offenen Justiz in einer freien, rechtsstaatlichen

---

[16] Zum Beispiel führen In der Telekommunikationsbranche viele Länder eine Aufbewahrungspflicht für die Speicherung von Verkehrsdaten bei Telefongesprächen ein, auch wenn diese Daten nicht für unternehmerische Zwecke gebraucht werden. Im Bankensektor fordern die meisten Länder die langfristige Aufbewahrung von Kopien der Identifizierungsdokumente für Kundenkonten. Dies ist Teil des "Know-Your-Customer"-Prinzips zur Geldwäschebekämpfung. Im Telekommunikationssektor verbieten manche Länder anonyme Handy-Konten und fordern die Aufbewahrung von Kopien der Identifizierungsdokumente für Kundenkonten.

[17] Zum Beispiel gibt es weniger strenge Voraussetzungen für den Zugriff auf Metadaten und neue Prozesse zur Echtzeit-Überwachung dynamischer Datenumgebungen. Es ist ziemlich wahrscheinlich, dass die Behörden, die eine flexiblere Rechtssprache suchen, um die Konsequenzen wissen, während die meisten Gesetzgeber nur in sehr begrenztem Maße verstehen, was sie gestatten.

Gesellschaft ein gewisses Maß an Transparenz in Strafverfahren. Die Strafverfolgungsbehörden werden gegen den Angeschuldigten normalerweise Klagepunkte anführen und ihm die Möglichkeit geben, sich zu erklären. Falls es zu einem Gerichtsverfahren kommt, erhält der Anwalt des Angeschuldigten die entsprechenden Informationen und es kommt zu einer öffentlichen Anhörung vor Gericht. Im Gegensatz dazu wird das Sammeln von Erkenntnissen durch Geheimdienste immer geheim gehalten. Und da die strafrechtliche Verfolgung von Personen nicht zwangsläufig das beabsichtigte oder tatsächliche Ziel ist, kann es sein, dass der Schleier der Geheimhaltung nie gelüftet wird. Die Fälle, die öffentlich gemacht werden, machen wahrscheinlich nur einen kleinen Anteil der gesamten Überwachungsmaßnahmen aus.

In einer demokratischen Gesellschaft werden Maßnahmen, die staatliche Behörden im Verborgenen ergreifen, in der Regel argwöhnisch betrachtet und erzeugen Misstrauen.[18] Versuche, das öffentliche Vertrauen mit der Einführung einer gewissen Kontrolle über nationale Sicherheitsorganisationen zu stärken, waren nicht immer erfolgreich, wenn nachgewiesen wurde, dass staatliche Stellen die Öffentlichkeit und sogar die Aufsichtsgremien getäuscht haben.[19]

Während also mit Sicherheit gesagt werden kann, dass Regierungen einen größeren Zugriff als früher auf personenbezogene Daten erhalten möchten, die sich im Besitz von Unternehmen befinden, und diesen auch bekommen, ist das genaue Ausmaß dieses Zugriffs ein Stück weit unklar. In diesem Zusammenhang können Transparenzberichte eine nützliche Rolle spielen.

Transparenzberichte

Jedes Mal, wenn der Staat aus unternehmensfremden Gründen auf Daten oder Informationen in Firmenbesitz zugreift, gibt es eine staatliche Stelle, die die Informationen einholt, und ein Unternehmen, das diese Anfrage erhält und daraufhin tätig wird. Der Schwerpunkt dieses Papiers liegt vor allem auf der Berichterstattung über die Maßnahmen von Unternehmen, die solche Anfragen erhalten. Auch wenn es nicht im Mittelpunkt des vorliegenden Papiers steht, ist zu betonen, dass die Transparenz und Rechenschaftspflicht öffentlicher Stellen, die Unternehmen zur Herausgabe ihrer Daten auffordern oder verpflichten, ebenso wichtig ist. Die Arbeitsgruppe hat bereits auf die Bedeutung der Transparenz als Element der Rechenschaftspflicht bei staatlichem Abhören privater Kommunikation oder im Rahmen von Überwachung hingewiesen.[20]

Die steigende Nachfrage seitens des Staates nach Informationen und personenbezogenen Daten in Firmenbesitz bereitet nicht nur Einzelpersonen und Verfechtern der Privatsphäre Sorgen, sondern auch den Unternehmen selbst. Bei einigen dieser Bedenken der Unternehmen handelt es sich ganz nüchtern um Bedenken bezüglich des Erfüllungsaufwands (der beträchtlich sein kann). Unter ethischen Gesichtspunkten haben Unternehmen Schwierigkeiten, die Herausgabe von vertraulichen personenbezogenen Daten an staatliche Behörden für unternehmensfremde Zwecke mit dem Vertrauensverhältnis in Einklang zu bringen, das sie mit ihren Kunden und anderen Geschäftspartnern pflegen möchten.

---

[18] Siehe den Bericht des Europäischen Parlaments über das US-amerikanische NSA-Überwachungsprogramm, Überwachungsgremien in verschiedenen Mitgliedstaaten und ihre Auswirkung auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit in den Bereichen Justiz und Inneres, Februar 2014.

[19] Siehe z. B. den Sonderausschuss des US-Senats zum Haft- und Verhörprogramm der CIA, veröffentlicht im Dezember 2014.

[20] Arbeitspapier der IWGDPT zur Überwachung der Telekommunikation (Auckland, 2002) und Gemeinsamer Standpunkt der IWGDPT zu zur öffentlichen Verantwortung im Hinblick auf das Abhören privater Kommunikation (Hongkong, 1998).

Besorgnisse bestehen ebenfalls im Hinblick auf die rechtliche Haftung, wenn Unternehmen konkurrierenden rechtlichen Verpflichtungen zum Schutz von Sicherheit und Vertraulichkeit einerseits und zur Erfüllung staatlicher Zugriffsforderungen in einem bestimmten Rechtssystem andererseits unterliegen. Die rechtlichen Schwierigkeiten nehmen noch zu, wenn es sich um ein multinationales Unternehmen handelt, das in mehreren Rechtssystemen tätig ist, und Gesetze miteinander kollidieren, oder wenn ein Auftragsverarbeiter aufgefordert wird, die Daten eines anderen Unternehmens verdeckt weiterzuleiten. Zusätzliche Schwierigkeiten gibt es im Zusammenhang mit grenzüberschreitenden Anfragen, die auf Grundlage eines Vertrags zur Rechtshilfe gestellt werden.[21]

Eine mögliche Lösung für Unternehmen besteht darin, eine eindeutige und stringente Unternehmenspolitik für den Umgang mit staatlichen Anfragen einzuführen, um sicherzustellen, dass diese kompetent und rechtmäßig bearbeitet und Fehler vermieden werden. Zu solchen Leitlinien können die Zentralisierung der Annahme von Anfragen, ein standardisierter Bearbeitungsprozess, eindeutige und an den geltenden rechtlichen Anforderungen ausgerichtete Unternehmenskriterien sowie die Beteiligung leitender und erfahrener Mitarbeiter gehören. Innenrevision, Überprüfung und Berichterstattung gegenüber der Führungsebene sind übliche Anforderungen. Unternehmen können vor der Übermittlung von Daten eine richterliche Anordnung oder ähnliches anfordern. Aufgrund der Aufmerksamkeit, die guten Praktiken, ethischen Fragen und dem Ruf eines Unternehmens geschenkt wird, denken viele Unternehmen über die Rolle öffentlicher Berichterstattung nach.

2009 veröffentlichte Google seinen ersten Transparenzbericht. Innerhalb der nächsten drei Jahre folgten einige Anbieter von Telekommunikations- und Internetdiensten.[22] Im Jahr 2013 wurde dieses Vorgehen populär, als Dutzende Firmen in Nordamerika, Europa, Asien und Australien einen Transparenzbericht veröffentlichten.[23]

In der Regel geben die Unternehmen keine genauen Gründe für die Veröffentlichung eines Transparenzberichts bekannt, obwohl viele angeben, dass ihr Unternehmen dem Datenschutz eine hohe Bedeutung beimisst. Normalerweise besteht keine gesetzliche Verpflichtung zur Veröffentlichung eines solchen Berichts. Die Motivation hängt vermutlich mit der Sorge eines Unternehmens um seinen Ruf und mit seiner Eigenwahrnehmung als verantwortlicher „Corporate Citizen“ zusammen. Auch das Verhalten anderer Unternehmen kann manchmal eine Rolle spielen. Die Veröffentlichung eines Berichts kann ein Versuch seitens eines Unternehmens sein, seine Vertrauenswürdigkeit unter Beweis zu stellen, indem es zeigt, dass es sein Bestes tut, um seine schwierige Doppelrolle – Zusammenarbeit bei rechtmäßigen Anfragen sowie Erfüllung seiner Verpflichtungen hinsichtlich Sicherheit und Vertraulichkeit – professionell auszufüllen. Die korrekte Bearbeitung von Anfragen zum Datenzugriff und die gleichzeitige öffentliche Berichterstattung über diesbezügliche Maßnahmen werden als Übungen in Transparenz gegenüber Kunden, Geschäftspartnern und der Öffentlichkeit betrachtet.

In gewisser Weise handelt es sich bei Transparenzberichten von Unternehmen um einen Versuch der Privatwirtschaft, öffentliche Stellen zur Verantwortung zu ziehen. Letztlich sind die öffentlichen Stellen für die Zugriffsanfragen verantwortlich, die öffentlichen Unmut erzeugen oder den Kundenerwartungen zuwiderlaufen aber es sind die Unternehmen, die damit konfrontiert sind, die Informationen herauszugeben. Bei der Veröffentlichung von Berichten, die Aufschluss über die Handlungen geben, zu denen die Unternehmen verpflichtet wurden, handelt es sich um einen Versuch, öffentliche Stellen für ihr Vorgehen zur Verantwortung zu ziehen. Es gibt praktische Gründe für die Versuche von Unternehmen, staatliche Stellen zur Rechenschaft zu ziehen, und diese Versuche können

[21] Siehe z. B. Global Network Initiative, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Januar 2015.

[22] 2012 veröffentlichten mindestens zwölf Unternehmen Transparenzberichte online. Quelle: Büro des Datenschutzbeauftragten, Neuseeland.

[23] Für 2013 wurden ca. 37 Transparenzberichte gezählt, die im Internet veröffentlicht wurden. Quelle: Büro des Datenschutzbeauftragten, Neuseeland.

mit einigen Vorteilen verbunden sein. Die Bearbeitung vielfacher Anfragen zum Datenzugriff ist für ein Unternehmen mit einem Erfüllungsaufwand verbunden. Falls das Unternehmen der Anfrage widerstandslos nachkommt, könnte es für die Behörden als „leichte Beute" eingestuft und zur bevorzugten ersten Anlaufstelle für die Beschaffung von Informationen werden. Werden die Vorgehensweisen bei der Veröffentlichung von Transparenzberichten genauer beleuchtet, kann dies dazu beitragen sicherzustellen, dass die Behörden stärker darauf achten, dass die Ausübung ihrer Zwangsbefugnisse verhältnismäßig und begründet ist. Man könnte sagen, dass die Unternehmen versuchen, das Ethos einer „transparenten Staates" wiederherzustellen, das im Bereich der staatlichen Überwachung einen Rückschlag erlitten hat.

Aus Sicht des Datenschutzes ist es offensichtlich schwierig, ohne Genehmigung der betroffenen Person und womöglich gegen den Wunsch und die Interessen dieser Person einem Dritten Informationen aus Firmenbesitz für unternehmensfremde Zwecke zu übermitteln. Dies war im Bereich der Strafverfolgung jedoch schon immer der Fall und das Problem wurde in der Regel dadurch gelöst, dass die strafrechtlichen Ermittlungen als legitime Ausnahme von den Geheimhaltungserwartungen anerkannt wurden. Im derzeitigen Kontext bezieht sich die Schwierigkeit auf den zunehmenden Zugriff auf Daten in Firmenbesitz, der mittlerweile eher die Regel als die Ausnahme darstellt, sowie auf die massenhafte Herausgabe von und den Zugriff auf Daten in Firmenbesitz in Echtzeit zum Zweck der Überwachung.

Um auf diese Herausforderung für die klassischen Erwartungen an den Datenschutz zu reagieren, wird nun der Notwendigkeit, dass öffentliche Stellen und Unternehmen einen rechenschaftspflichtigen Umgang mit Informationen unter Beweis stellen, größere Beachtung geschenkt. Transparenz gilt dabei als wichtiger Bestandteil. Dies kann als ein Gesellschaftsvertrag gesehen werden, in dessen Rahmen die Bürger erwarten, dass ihre Kommunikation und ihre Angelegenheiten vertraulich behandelt werden und dies nur rechtmäßigen und verhältnismäßigen Ausnahmen für Strafverfolgung und die nationale Sicherheit unterliegt, wobei die die entsprechenden Organisationen unter vertrauenswürdiger, unabhängiger Aufsicht stehen. Die Veröffentlichung von Transparenzberichten ist eine Form der öffentlichen Überprüfbarkeit, um sicherzustellen, dass die Bedingungen dieses Vertrags eingehalten werden.

Mit diesen Berichten wird die Öffentlichkeit in allgemeiner Form über die Maßnahmen staatlicher Stellen informiert. Die öffentliche Berichterstattung durch die Behörden, die Zugriff auf Daten fordern, und der Stellen, die diese Anfragen bearbeiten, fördert die Rechenschaftspflicht beider Seiten. Schließlich informieren die Berichte auch die Öffentlichkeit und den Gesetzgeber, die letztendlich darüber entscheiden, wo sie die Grenze zwischen Überwachung und Freiheit ziehen wollen.

Inhalt der Transparenzberichte

Die plötzlich zunehmende Bereitschaft von Unternehmen zur freiwilligen Veröffentlichung von Transparenzberichten führte dazu, dass eine Reihe von Statistiken erstellt wurden, die nicht immer vergleichbar sind.[24] Die Statistiken unterscheiden sich hinsichtlich ihrer Detailliertheit und Parameter; zudem werden Daten unterschiedlich (oder gar nicht) definiert.

Es gibt jedoch Spielraum, um Ordnung in das System der Berichterstattung zu bringen, da den meisten Transparenzberichten ein recht ähnlicher Ansatz zugrunde liegt. Die Berichte enthalten relevante Statistiken zu Zahl und Art staatlicher Anfragen zu Informationen in Firmenbesitz sowie zu den Ergebnissen dieser Anfragen. Die Berichte können günstigerweise auch andere Themen umfassen, die für das betreffende Unternehmen relevant sind– z. B. Anfragen zum Thema Urheberrecht und

[24] Die aus der fehlenden Standardisierung von Berichten entstehenden Probleme werden dargestellt in: Christopher Parsons, *Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports*, 2015, verfügbar über SSRN: http://ssrn.com/abstract=2546032 oder http://dx.doi.org/10.2139/ssrn.2546032.

der Löschung von Daten oder zum europäischen Recht auf Vergessenwerden (Entfernung von Internetlinks). Doch so nützlich diese zusätzlichen Berichte auch sind, gehen sie über den Rahmen dieses Papiers hinaus.

Im Folgenden wird kurz auf die typischen Elemente eines Transparenzberichts eingegangen:

- *Rechtsordnung:* Unternehmen, die in mehreren Rechtsordnungen tätig sind, erhalten wahrscheinlich Anfragen von staatlichen Behörden aus verschiedenen Ländern. Die Struktur des Berichts wird dies widerspiegeln müssen. Verschiedene Länder nutzen unterschiedliche Terminologie für ähnliche Konzepte und das Unternehmen wird entscheiden müssen, ob es in allen Berichten eine Standardterminologie verwendet oder die Sprache an die Rechtsterminologie einer bestimmten Rechtsordnung anpasst. Eine nützliche Methode besteht darin, Standardterminologie zu verwenden und mithilfe einer Legende oder von Fußnoten zu erklären, wie die Begriffe im Rahmen der jeweiligen Rechtsordnung verwendet werden.
- *Berichtszeitraum:* Die Veröffentlichung eines Transparenzberichts ist keine einmalige Übung, sondern ein fortlaufender Prozess. In der Zukunft mag es vielleicht möglich sein, in Echtzeit online Bericht zu erstatten, doch bisher läuft es so ab, dass Unternehmen Jahresberichte vorlegen. Größere Unternehmen veröffentlichen ihre Berichte häufiger, in der Regel einmal alle drei oder sechs Monate. Die Berichte zeigen für gewöhnlich Trends auf und beinhalten Diagramme und Kommentare, in denen die aktuellen Zahlen mit Zahlen aus früheren Zeiträumen verglichen werden.
- *Art der Anfragen:* Staatliche Anfragen werden in unterschiedlicher Form gestellt und die meisten Berichte versuchen, diese auf eine der Rechtsordnung und der jeweiligen Branche angemessenen Weise zu vereinheitlichen. Typische Klassifizierungen beziehen sich auf die rechtliche Form der Anfragen (z. B. eine richterliche Anordnung oder ein administratives Ersuchen), die Art der von dem Unternehmen zu ergreifenden Maßnahme (z. B. Zugriff auf bestehende Daten oder Einsatz eines Gerätes zur weiteren Überwachung eines Kontos und Herausgabe von Kontobewegungsdaten an staatliche Stellen in Echtzeit) und darauf, ob die Anfrage einen straf- oder zivilrechtlichen Hintergrund hat und ob sie von einer in- oder ausländischen Ordnungsbehörde gestellt wird.[25] Es gibt viele Unterkategorien, die ebenfalls nützlich sein können. Unternehmen neigen dazu, ihre Berichte nach den häufigsten Anfragen zu strukturieren. Dies sind in der Regel Anfragen von Stellen ihrer eigenen Rechtsordnung.
- *Anzahl der Anfragen:* Ausgangspunkt für den Bericht müssen natürlich die von staatlicher Seite gestellten Anfragen darstellen. Wird lediglich über die Anzahl der Anfragen berichtet, könnte dies verschleiern, dass es hinsichtlich der Art und des Umfangs der Anfragen erhebliche Unterschiede gibt. Dementsprechend erfassen nützlichere Berichte sowohl die Anzahl der erhaltenen Anfragen als auch die Zahl der individuellen Datensätze oder Konten, auf die sich diese Anfragen beziehen.
- *Informationsvolumen bzw. Anzahl der betroffene Personen:* Zahlen bezüglich des Umfangs und der Auswirkung der Anfragen sind in einigen, aber nicht in allen Berichten zu finden.
- *Ergebnis der Anfragen:* Transparenzberichte spiegeln nicht einfach nur wider, was der Staat von den Unternehmen verlangt hat. Sie berichten auch über die vom Unternehmen getroffenen Maßnahmen und folglich auch über das Ergebnis der Anfragen. Dies unterscheidet sich je nach Art des Unternehmens, Art der Anfragen und geltendem Recht. Zum Beispiel sollte ein Auftragsverarbeiter jede staatliche Anfrage auf Zugriff an den für die Verarbeitung Verantwortlichen weiterleiten, es sei denn, ihm ist dies gesetzlich verboten. Ein Bericht für einen Auftragsverarbeiter kann daher Statistiken zur Zahl der Weiterleitungen an für die Verarbeitungen von Kundendaten Verantwortliche enthalten und zur Zahl der Fälle, in denen der Auftragsverarbeiter die Anfrage direkt beantwortet hat. Die meisten der im Bericht enthaltenen Statistiken beziehen sich im Allgemeinen darauf, ob die Anfragen beantwortet oder abgelehnt wurden. Ist Ersteres der Fall, werden Details zur Anzahl der betroffenen Datensätze,

[25] Unternehmen könnten die Bearbeitung von Anfragen ausländischer Behörden ablehnen und dies in ihrem Bericht so festhalten.

Personen oder Konten aufgeführt. In einigen Fällen gibt es gesetzliche Einschränkungen, die die Veröffentlichung von Statistiken begrenzen oder zeitlich verschieben.

- *Kommentierung:* Eine Einführung, eine Erläuterung der verwendeten Begriffe und ein Kommentar zu den Trends ergänzen in der Regel die Statistiken. Ein gesonderter Kommentar kann im Falle unerwarteter oder außergewöhnlicher Zahlen erfolgen.

Grundsätze für die Erstellung von Transparenzberichten

Die Arbeitsgruppe empfiehlt den für die Privatsphäre und den Datenschutz zuständigen Behörden, Unternehmen dazu anzuhalten, die folgenden „Grundsätze" bei der Erstellung von Transparenzberichten zu berücksichtigen:

1. ***Grundsatz der Rechenschaftspflicht***: Unternehmen sollten in Bezug auf ihren Umgang mit staatlichen Anfragen auf die Herausgabe von Informationen zu unternehmensfremden Zwecken Rechenschaft ablegen.

2. ***Grundsatz der Transparenz:*** Unternehmen, bei denen regelmäßig staatliche Anfragen zur Herausgabe von Informationen zu unternehmensfremden Zwecken eingehen, sollten regelmäßig die Art und Menge der übermittelten Daten öffentlich machen.

3. ***Grundsatz der Verlässlichkeit***: Transparenzberichte von Unternehmen, die auf staatliche Anfrage hin Auskunft über die Weitergabe personenbezogener Informationen geben, sollten präzise und vollständig sein.

4. ***Grundsatz, dass Berichte nicht irreführen sollten:*** Ungeachtet dessen, dass Gesetze manchmal eine zeitliche Verzögerung für die Berichterstattung vorschreiben oder der Berichterstattung Grenzen setzen[26], sollten Unternehmen, die Transparenzberichte veröffentlichen, Maßnahmen zur Vermeidung eines irreführenden Eindrucks ergreifen, der durch die Vorlage unvollständiger Statistiken entstehen würde.

5. ***Grundsatz der Vergleichbarkeit*:** Die Unternehmen sollten versuchen sicherzustellen, dass bekannt gegebene Statistiken sinnvoll mit bereits veröffentlichten Berichten und Statistiken aus anderen Transparenzberichten verglichen werden können.

6. ***Grundsatz der Zugänglichkeit*:** Transparenzberichte sollten so veröffentlicht werden, dass die Öffentlichkeit, die Medien und die relevanten Akteuren in möglichst effektiver Weise darauf zugreifen können.

Empfehlungen zur Umsetzung der Grundsätze

Bei der Veröffentlichung von Transparenzberichten handelt es sich bisher um eine freiwillige Initiative, die vom Privatsektor als Reaktion auf die staatliche Einwirkung auf öffentliche Vorstellungen von Privatsphäre ergriffen wurde. Die Arbeitsgruppe unterstützt diese Initiative und empfiehlt, dass die Transparenzberichte verbessert werden und dass noch mehr Unternehmen und Branchen solche Berichte veröffentlichen. Positiv hervorzuheben sind an dieser Stelle alle Unternehmen, die mit der Veröffentlichung von Transparenzberichten bereits begonnen haben. Allerdings ist es für ein einzelnes Unternehmen schwierig, ein Ziel wie die Vergleichbarkeit der veröffentlichten Statistiken zu erreichen. Ebenso kann ein einzelnes Unternehmen nicht in der gesamten Branche für Transparenz sorgen. Aber je mehr Unternehmen Transparenzberichte veröffentlichen, desto vollständiger wird das Bild, das in Bezug auf das staatliche Vorgehen und die entsprechenden Maßnahmen der Unter-

[26] Natürlich müssen die Unternehmen bei der Anwendung dieser Grundsätze und der Erstellung eines Transparenzberichts das geltende nationale Recht einhalten.

nehmen, die die personenbezogenen Daten der Bürger verwalten, entsteht. Sobald bekannte Unternehmen damit begonnen haben, Transparenzberichte vorzulegen, erhöht sich der Marktdruck auf die Mitbewerber, ebenfalls transparenter zu sein.

Die Arbeitsgruppe vertritt die Auffassung, dass neben einzelnen Unternehmen auch andere Akteure zur Förderung und Verbesserung von Transparenzberichten beitragen müssen. Diese Empfehlungen richten sich daher sowohl an Unternehmen als auch an andere Akteure. Sie versuchen, den Grundsätzen der Transparenz größere Wirkung zu verleihen.

Die Arbeitsgruppe empfiehlt:

Unternehmen

(a) Unternehmen, die staatliche Anfragen zum Zugang zu personenbezogen Informationen aus ihrem Besitz erhalten, sollten:

i. zuverlässige Verfahren für die Annahme von und den Umgang mit staatlichen Anfragen zum Zugang zu personenbezogenen Informationen anwenden, um sicherzustellen, dass die Herausgabe von Informationen verantwortungsvoll und rechtskonform erfolgt und im Einklang mit der Unternehmenspolitik steht;
ii. ihre Politik für den Umgang mit staatlichen Anfragen veröffentlichen;
iii. mit der Veröffentlichung von Transparenzberichten wie in diesem Papier dargelegt beginnen (dies gilt für Unternehmen, die wiederholt staatliche Anfragen auf Zugang zu personenbezogenen Informationen erhalten);
iv. sicherstellen, dass die von ihnen veröffentlichten Transparenzberichte verlässlich sind, indem sie dafür Sorge tragen, dass die Statistiken seriös erstellt werden und überprüfbar sind;
v. ihre Berichte und die Terminologie so strukturieren, dass sie die firmen-, branchen-, länder- und zeitraumübergreifende Vergleichbarkeit von Statistiken fördern;
vi. Praktiken vermeiden, die den Leser in die Irre führen können und, insbesondere falls die veröffentlichten Zahlen aufgrund von staatlichen Restriktionen unvollständig sind, auf diese Unvollständigkeit hinweisen und nach Ablauf der Restriktionen die vollständigen Zahlen vorlegen;
vii. einen Beitrag zu einer effektivere Verbreitung der Berichte leisten, indem sie beispielsweise Maßnahmen zur Wiederveröffentlichung von Zahlen in gemeinsamen nationalen oder internationalen Verzeichnissen unterstützen;
viii. die Einheitlichkeit ihrer Vorgehensweisen bei der Erstellung von Transparenzberichten mithilfe der Grundsätze zur Erstellung von Transparenzberichten überprüfen und – falls nötig – verbessern.

Rechtsetzung

(b) Gesetzgeber, die Gesetze oder Regelungen schaffen, auf deren Grundlage Behörden Zugang zu personenbezogenen Informationen in Firmenbesitz erlangen können, sollten:

i. gewährleisten, dass die Gesetze und Regelungen angemessene, im Verhältnis zu den betroffenen öffentlichen Interessen stehende Grenzen nicht überschreiten, entsprechende Sicherungen enthalten und Mittel bereitstellen, um die öffentlichen Stellen zur Rechenschaft zu ziehen;
ii. sicherstellen, dass Verpflichtungen zur Förderung der Transparenz beim Einsatz solcher Befugnisse bestehen;
iii. unnötige Hindernisse für die Erstellung von Transparenzberichten abbauen;
iv. dafür sorgen, dass Behörden dazu verpflichtet sind, Statistiken über die Ausübung von Befugnissen beim Zugriff auf Daten in Firmenbesitz zu veröffentlichen.

Öffentliche Stellen, die Zugang zu Informationen in Firmenbesitz erlangen

(c) Öffentliche Stellen sollten:

i. Befugnisse für den Zugriff auf Daten in Firmenbesitz rechtmäßig, verhältnismäßig und nachvollziehbar ausüben;

ii. sollten offenlegen, wie sie ihre Befugnisse ausüben, z. B. durch die regelmäßige Veröffentlichung von Statistiken;

iii. die Auferlegung von Geheimhaltungspflichten vermeiden, die nicht im Verhältnis zu den berechtigten Bedürfnissen im Bereich der Strafverfolgung oder nationalen Sicherheit stehen;

iv. alle bestehenden Geheimhaltungspflichten überprüfen, um sicherzustellen, dass sie die in einer freien Gesellschaft gerechtfertigte Schwelle nicht überschreiten.

Datenschutzbehörden

(d) Datenschutzbehörden sollten:

i. die Bemühungen derjenigen Unternehmen, die freiwillig Transparenzberichte veröffentlichen, unterstützen und andere Unternehmen dazu ermutigen, dasselbe zu tun;

ii. bessere Praktiken bei der Veröffentlichung von Transparenzberichten fördern, um die Erstellung von aussagekräftigen Statistiken zu unterstützen, die zuverlässig und national und international vergleichbar sind;

iii. Bemühungen unterstützen oder einleiten, um Transparenzberichte in zentralisierten nationalen oder internationalen Verzeichnissen zugänglicher zu machen;

iv. die in den Berichten bekannt gegebenen Informationen für Ihre Arbeit nutzen.

Internationale Regierungsorganisationen

(e) Internationale Organisationen sollten:

i. die Entwicklung international vergleichbarer Metriken fördern, um den politischen Entscheidungsprozess hinsichtlich der Privatsphäre und der grenzüberschreitenden Übermittlung von personenbezogenen Daten auf eine informierte Basis zu stellen.

ii. die Bereiche identifizieren, in denen staatliche Geheimhaltungspflichten ein unnötiges Hindernis für die Transparenz darstellen, und Regierungen auf bessere Praktiken aufmerksam machen, die Offenheit fördern und Vertrauen im Internet aufbauen.

Regulierungsbehörden für Telekommunikation

(f) Die Regulierungsbehörden für Telekommunikation sollten:

i. die Erstellung von Transparenzberichten im Telekommunikationssektor unterstützen und fördern.

Branchenverbände

(g) Branchenverbände sollten:

i. in Abstimmung mit den relevanten Akteuren wie Datenschutzbehörden und der Zivilgesellschaft Handlungsempfehlungen für gute Praktiken für die Erstellung von Transparenzberichten geben, die für ihre Branche relevant sind.[27]

[27] Ein Beispiel für solch eine Industrieinitiative ist der Dialog der Telekommunikationsbranche, dessen Aktivitäten auf Grundlage der Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte erfolgen, zu denen auch das Handlungsprinzip 21 gehört (Sorgfaltspflicht im Bereich der Menschenrechte), das zur externen Berichterstattung über betriebliche Praktiken mit Auswirkungen auf Menschenrechte ermutigt. Siehe www.telecomindustrydialogue.org.

Zivilgesellschaft

(h) Die Zivilgesellschaft sollte:

i. von allen relevanten Akteuren Rechenschaft einfordern (Regierungen, die Gesetze schaffen, die den Zugriff auf Daten ermöglichen; Behörden, die auf Informationen in Firmenbesitz zugreifen wollen; Unternehmen, die staatliche Anfragen bearbeiten und personenbezogene Informationen zu unternehmensfremden Zwecken herausgeben);

ii. Unternehmen dazu ermutigen, Transparenzberichte zu erstellen;

iii. die Einrichtung gemeinsamer Verzeichnisse zum Abruf der Berichte unterstützen,;[28]

iv. von den im Rahmen der Transparenzberichte erstellten Statistiken Gebrauch machen.

[28] Zum Beispiel haben zivilgesellschaftliche Organisationen in Kanada, Hongkong, Polen und den USA Berichte veröffentlicht oder Webseiten eingerichtet, die Firmenstatistiken an einem Ort zusammenführen, oder eine vergleichende Untersuchung von Firmenberichten durchgeführt.