Sachdokumentation:

Signatur: DS 81

Permalink: www.sachdokumentation.ch/bestand/ds/81

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

Geht es in Richtung Datenparadies?

Die Schweiz und Cloud Computing in der Post-Snowden-Ära

foraus - Diskussionspapier / Nr. 26 / November 2015
Programm Global Governance

foraus
Forum Aussenpolitik
Forum de politique étrangère
Forum di politica estera

Executive Summary

Die Gewährleistung des Schutzes digitaler Daten, die von einem Dienstanbieter gespeichert werden (Daten in einer Cloud), weist einen doppelten, und zwar ökonomischen und ethischen, Vorzug auf, von dem die Schweiz profitieren kann. Vor diesem Hintergrund gliedert sich dieses Diskussionspapier in vier Teile.

Der erste einleitende Teil soll die Problematik der Überwachung von gespeicherten digitalen Daten in der Post-Snowden-Ära kontextualisieren. Der zweite Teil hebt einige der wichtigsten Argumente der moralischen und politischen Philosophie hervor und zeigt, dass diese wahrlich gute Gründe liefert, dem Privatleben - und demnach dem Datenschutz - aus Gründen im Zusammenhang mit Autonomie, Menschenwürde und zwischenmenschlicher Intimität einen Wert einzuräumen. Der dritte Teil ist eine Bestandsaufnahme über die Errungenschaften der aktuellen Schweizer Datenschutzgesetzgebung und über den komparativen Vorteil, den sie digitalen Unternehmen, insbesondere gegenüber dem Hostingland der Clouding-Giganten, den USA, bietet. Es scheint, dass

- das US-amerikanische Recht an sich in Bezug auf den Schutz von digitalen Daten, die in den Vereinigten Staaten elektronisch gespeichert werden, wie im Fall des Clouding, lückenhaft ist;
- die Schweiz die Privatsphäre in Bezug auf die digitalen Daten vergleichsweise stärker schützt.

Im vierten und letzten Teil schlagen wir drei Empfehlungen für Gesetzgeber und Entscheidungsträger vor.

- Sicherheitseinbehalt. Die Schweiz muss sich nicht, wie dies die Vereinigten Staaten oder Frankreich praktizieren, auf Rechtsvorschriften stürzen, die den Schutz digitaler Personendaten auf dem Altar der Sicherheit opfern.
- Unabhängige Überwachung. Es besteht die Notwendigkeit einer durch eine unabhängige Stelle durchgeführten Überwachung von staatlichen Eingriffen in Bezug auf Daten in einer Cloud. Sollten sich Eingriffe als notwendig erweisen, müssen die Achtung des Grundsatzes der Verhältnismässigkeit und die strikte Beschränkung der Datenbeschaffung auf die als notwendig definierten Elemente sowie die Einhaltung der Speicherdauer durch eine unabhängige Behörde sichergestellt werden. Somit scheint die Stärkung der Rolle von Datenschutzbeauftragten eine Notwendigkeit darzustellen: Es ist daher wünschenswert, die institutionelle Unabhängigkeit der Datenschutzbeauftragten zu fördern, indem man ihnen ausreichende Handlungsmöglichkeiten garantiert und ihnen eine institutionelle Position einräumt, durch die sie vor dem Druck seitens der Exekutive geschützt sind.
- Verantwortung des Privatsektors. Den Hosting-Unternehmen kommt eben-

falls eine Rolle zu, um die Schaffung eines Schweizer Informationsparadieses zu initiieren. Vom Gesichtspunkt der Wahrung des Datenschutzes in Bezug auf die Cloud müssen die Nutzer sich nicht nur auf die Behörden, sondern auch auf die Dienstanbieter verlassen können. Letztgenannte müssen demnach über zuverlässige Mittel verfügen, um eine gewisse Transparenz in Bezug auf die Art und Weise, wie sie die ihnen anvertrauten Daten verwalten, gewährleisten zu können.

So lässt sich angesichts der obigen Überlegungen sagen, dass sich der Schweiz eine äusserst seltene Gelegenheit eröffnet, zwei Fliegen auf einen Schlag zu treffen: Förderung des Privatlebens durch Kultivieren von Wachstum und Förderung des Wachstums durch Kultivieren des Privatlebens. Wirtschaftskreise und zahlreiche Verfechter von bürgerlichen Freiheiten haben allen Grund, in diesem Zusammenhang Hand in Hand zu arbeiten. Aber sie kennen seit langem die Devise «Lachen und Weinen zugleich»: In einem Kontext, der so vertraut ist, dass es beinahe natürlich scheint, dürfte das Ende des Bankgeheimnisses Erstgenannten Kummer bereiten und Letztgenannten Grund zur Freude sein. Die digitale Wirtschaft in der Post-Snowden-Ära setzt sich auf recht aussergewöhnliche Weise für eine neuartige Verbindung ein: Die Unternehmer im digitalen Umfeld haben ein Interesse daran, philosophische Erwägungen in ihr Business Model zu integrieren; und Verfechter des Privatlebens haben ein Interesse daran, von der Schlagkraft der Wirtschaftskreise zu profitieren. Auf diese Weise entsteht ein positiver Kreislauf. In der Post-Snowden-Ära kann die Schweiz wirtschaftliche Gelegenheiten in einer Grössenordnung von Milliarden Dollar wahrnehmen, die nicht nur einen monetären, sondern ebenfalls einen ethischen Wert aufweisen. Warum sollte man eine solch willkommene Gelegenheit nicht nutzen, das Steuerparadies in ein digitales Paradies zu verwandeln?

Autoren

Jean Busché

ist Student der Politischen Theorie an der Universität Genf und Mitbegründer des Start-Ups CR2. Er interessiert sich insbesondere für die Sammlung und Verwendung von persönlichen Daten und hat zu diesem Thema die Publikationen «Vidéosurveillance: mise en perspective du cas genevois et point de vue éthique» für das Büro der Genfer Datenschutz- und Öffentlichkeitsbeauftragten («Préposés à la Protection des Données et à la Transparence») veröffentlicht.

Nicolas Tavaglione

ist Doktor der Politikwissenschaft und spezialisiert in politischer Philosophie und Ethik. Er hat unter anderem folgende Publikationen veröffentlicht: «Le dilemme du soldat. Guerre juste et prohibition du meurtre», Labor et Fides, 2005; «Gare au gorille. Plaidoyer pour l'Etat de droit», Labor et Fides, 2010; und «Dernières nouvelles du zoo. Chroniques politiques», Éditions du Courrier, 2014. Zurzeit ist er als unabhängiger Forscher tätig.

Impressum

Zitieren

foraus - Forum Aussenpolitik, 2015, *Geht es in Richtung Datenparadies? Die Schweiz und Cloud Computing in der Post-Snowden-Ära*, Diskussionspapier Nr. 26, Genf.

Dank

Der vorliegende Text wurde im Rahmen des Projekts FNS «Bound to Cooperate: Mapping Swiss Security» (Fonds UN 8546) verfasst. Die Verfasser möchten Stephan Davidshofer (DSPRI, Universität Genf), Isabelle Dubois (AdHoc Resolutions), Matteo Gianni (DSPRI, Universität Genf), Daniel Högger (*foraus*), Pascal Kotté (CloudReady) und Jean-Henry Morin (CUI, Universität Genf) für deren wertvolle Ratschläge und aufschlussreiche Kommentare danken. Dank geht auch an Pablo Diaz für seine logistische Unterstützung. Zudem danken die Autoren auch der Agentur eyeloveyou GmbH in Basel für die Realisierung der Infographik und weiterer graphischer Arbeiten sowie der DSwiss AG (Zürich), welche die Übersetzung des französischen Originaltextes ins Deutsche initiiert und ermöglicht hat.

www.foraus.ch

www.forausblog.ch

Inhaltsverzeichnis

1. Einführung

Ira Hunt, damals Chief Technology Officer der CIA, erklärte: «[...] versuchen wir grundsätzlich alles zu sammeln, was wir sammeln können und behalten es für immer»[1]. Diese Aussage zeigt das Ausmass des Problems, das durch die Enthüllungen von Edward Snowden im Mai 2013 aufgeworfen worden ist. Die Welt stellte mit Erstaunen fest, dass PRISM, ein allumfassendes Programm zur Überwachung elektronischer Kommunikation, existiert, das sowohl auf die «Feinde» als auch die «Freunde» der Vereinigten Staaten ausgerichtet ist und teilweise auf der erzwungenen Mitarbeit von Netz- und Telefonie-Giganten wie Google, Amazon oder Verizon[2] basiert. Plötzlich bekommt der Begriff der «Spionage» in der internationalen öffentlichen Meinung eine völlig neue Färbung. Mit mehr als 3 Milliarden Internetnutzern im Jahr 2015[3] ist ein großer Teil der Weltbevölkerung betroffen. In Bezug auf die Schweiz sind 80 Prozent der Bevölkerung regelmässig online[4]. Von dieser Überwachung ist demnach jeder oder fast jeder betroffen und das Thema der Freiheiten online stellt eine der grössten Herausforderungen dieser Zeit dar.

Die klassische Spionage, um die es in den Romanen von John Le Carré geht, ist eine reaktive und zielgerichtete Spionage: Dabei geht es um die Überwachung eines oder mehrerer genau identifizierter Individuen, mit dem Zweck, geäusserte Verdächtigungen, die durch Vorabinformationen geschürt werden, zu überprüfen. Die Spionage lässt sich in diesem Fall auf der Grundlage eines hinreichenden Verdachts rechtfertigen. Bei der Massenüberwachung, auf die Edward Snowden aufmerksam machte, geht es um eine präemptive und willkürliche Spionage, bei der ein Maximum an Personen überwacht werden soll. Willkürliche Spionage war auch vor Snowden bestens bekannt. Sie galt jedoch als eine Form der totalitären Einschüchterung in Anlehnung an die Politische Polizei, die hinter dem Eisernen Vorhang bis 1989[5] agierte. Die Enthüllungen von Snowden bringen eine unbequeme Wahrheit ans Licht: Willkürliche Spionage ist nicht nur in totalitären Regimen zu finden, sondern sie gehört – unter dem Deckmantel der Prävention, der Vorsorge und des Sicherheitspragmatismus – zum Aktionsrepertoire liberaler Demokratien. Hiermit sind wohlgemerkt nicht alle Menschen einverstanden. So ist eine der interessantesten Konsequenzen aus den Snowden-Enthüllungen ökonomischer Art. Im August 2013, also nur drei Monate nach Bekanntwerden des Skandals, veröffentlichte The Information Technology & Innovation Foundation einen alarmierenden Bericht:

Bei der Massenüberwachung, auf die Edward Snowden aufmerksam machte, geht es um eine präemptive und willkürliche Spionage, bei der ein Maximum an Personen überwacht werden soll.

1 Zitiert in Sébastien Desreux, Big Mother veille sur vous et vous surveille, éd. H&K, 2013, S. 11.

2 Für weitere Einzelheiten zur Snowden-Affaire, siehe Antoine Lefébure, L'affaire Snowden. Comment les Etats-Unis espionnent le monde, La Découverte, 2014. Für eine gründliche Analyse der technischen Überwachungsmittel der NSA, siehe Desreux, op. cit..

3 ITU 2015: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx konsultiert am 12.08.2015.

4 Zahlen OFS 2014: http://www.bfs.admin.ch/bfs/portal/fr/index/themen/16/04/key/approche_globale.indicator.30106.301.html?open=5 konsultiert am 12.08.2015.

5 Vgl. Margareta Los, «Looking into the future: surveillance, globalization and the totalitarian potential», in D. Lyon (ed.), Theorizing Surveillance. The Panopticon and beyond, Willan Publishing, Oxford, 2006, S. 69-94

Die Cloud Computing[6]-Industrie der USA erleide massive finanzielle Verluste - Kunden bevorzugten, ihre Daten bei Unternehmen an Standorten hosten zu lassen, die nicht unter den Foreign Intelligence Surveillance Act und den Patriot Act fallen, welche die Nachrichtendienste autorisieren, von privaten Unternehmen die Übermittlung der elektronischen Daten ihrer Nutzer zu verlangen. «[...] unter den aktuellen Bedingungen dürften die amerikanischen Anbieter von Cloud-Diensten in den kommenden Jahren zwischen 10 und 20 Prozent des ausländischen Marktes verlieren», so der Bericht abschliessend[7]. Die geschätzten Verluste belaufen sich auf eine Summe zwischen 21,5 Milliarden Dollar (niedrig geschätzt) und 35 Milliarden Dollar (hoch geschätzt). Forrester Research, ein an der NASDAQ notiertes Unternehmen, das Marktforschungsergebnisse und Analysen über die Informationstechnologie anbietet, geht von einer vollkommen anderen Grössenordnung aus und beziffert die Verluste auf 180 Milliarden Dollar[8]. An dieser Stelle kommt nun die Schweiz ins Spiel. «Geld auf Schweizer Konten verstecken? Das ist out. Probieren Sie doch mal etwas wirklich Wertvolles aus: und zwar Daten», schreibt im Jahr 2014 eine junge spanische Journalistin[9]. Und genau darum geht es. Artmotion, ein Schweizer Anbieter von Cloud Computing-Diensten mit Verschlüsselung, gibt ein Umsatzwachstum in Höhe von 45 %[10]. Tobias Christen, CEO von DSwiss, einem Unternehmen, das die SecureSafe-Anwendung für Mobiltelefone entwickelt hat, spricht von einer Umsatzsteigerung in Höhe von 150 %[11]. MIT Technology Review schreibt hierzu: «For Swiss Data Industry, NSA Leaks Are Good As Gold»[12]. Kunden, die sich von US-Unternehmen abwenden, stellen in der Tat ein Potenzial dar, das von mehreren europäischen Unternehmen umworben wird. Wir möchten im Folgenden aufzeigen, dass die Post-Snowden-Ära im Rahmen der digitalen Wirtschaft eine aussergewöhnliche Gelegenheit bietet, und zwar Wirtschaftsförderung und Schutz des Privatlebens - und demnach Schutz der Freiheit - miteinander zu verbinden. Im vorliegenden Fall lässt sich sagen, dass das, was für die bürgerlichen Freiheiten gut ist, und zwar ein wirksamer und vor Ausnahmebefugnissen sicherer Datenschutz, auch für das Wachstum positiv ist. Eine solche Allianz ist selten genug und sollte begrüsst und mit äusserster Sorgfalt kultiviert werden. Unsere Hauptbotschaft lautet wie folgt: Aus Gründen, die sich auf den politischen und moralischen Wert des Privatlebens und gleichzeitig auf die ökonomische Rationalität beziehen, sollte die Schweiz ihre Datenschutzgesetze

«Unter den aktuellen Bedingungen dürften die amerikanischen Anbieter von Cloud-Diensten in den kommenden Jahren zwischen 10 und 20 Prozent des ausländischen Marktes verlieren»

6 Bezeichnet die gemeinsame Nutzung von IT-Ressourcen via Internet wie die Speicherung.

7 Daniel Castro, «How Much Will PRISM Cost the U.S. Cloud Computing Industry?», The Information Technology and Information Foundation, August 2013, S. 4 [Online eingesehen am 16. April 2015: http://www2.itif.org/2013-cloud-computing-costs.pdf]

8 James Staten, «The Cost of PRISM Will Be Larger Than ITIF Projects», Forrester Research Inc., August 2013 [Online eingesehen am 16. April 2015: http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects]

9 Laura Secorun Palet, «From Banking Paradise to Data Hub», Ozy, Juli 2014 [Online eingesehen am 16. April 2015: http://www.ozy.com/pov/david-drummond-on-snowden-the-nsa-and-google/30081]

10 David Gilbert, «Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations», International Business Times, 4. Juli 2013 [Online eingesehen am 16. April 2015: http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613]

11 Persönliche Kommunikation, 17. April 2015.

12 Russ Juskalien, «For Swiss Data Industry, NSA Leaks Are Good As Gold», MIT Technology Review, 18. März 2014 [Online eingesehen am 16. April 2015: http://www.technologyreview.com/news/525546/for-swiss-data-industry-nsa-leaks-are-good-as-gold/]

stärken und den Sirenengesängen widerstehen, die nach dem Modell des amerikanischen Patriot Act die Ausweitung von Überwachungsbefugnissen fordern. Das neue Nachrichtendienstgesetz muss unter diesem Gesichtspunkt Gegenstand äusserster Wachsamkeit seitens der Wirtschaft wie auch der Verfechter bürgerlicher Freiheiten sein.

Wir möchten im Folgenden aufzeigen, dass die Post-Snowden-Ära im Rahmen der digitalen Wirtschaft eine aussergewöhnliche Gelegenheit bietet, und zwar Wirtschaftsförderung und Schutz des Privatlebens - und demnach Schutz der Freiheit - miteinander zu verbinden.

In Abschnitt 2 untersuchen wir einige philosophische Argumente zu Gunsten des Rechts auf Privatleben. In Abschnitt 3 nehmen wir eine Bestandsaufnahme über die Errungenschaften der aktuellen Schweizer Datenschutzgesetzgebung und über den komparativen Vorteil, den sie digitalen Unternehmen weltweit bietet, vor. In Abschnitt 4 schlagen wir abschliessend einige Grundsätze vor, die Gesetzgeber und politische Entscheidungsträger beachten sollten.

2. Schutz des Privatlebens

In den Denkerkreisen von Silicon Valley wird das Privatleben als etwas Überholtes betrachtet. Unzählige Male bereits wurde sein Ende von den Vertretern der sogenannten «Kalifornischen Ideologie» verkündet[13]. Eric Schmidt, CEO von Google, brachte 2009 mit einem klassischen Argument den Ball ins Rollen: «Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun»[14]. 2010 legte Mark Zuckerberg dann noch nach: «Die Leute finden es angenehm, nicht nur Informationen und andere Dinge zu teilen, sondern dies auch stärker öffentlich und mit einer grösseren Anzahl von Menschen zu tun. Die soziale Norm ist einfach etwas, das sich über die Jahre verändert hat»[15]. Vint Cerf, der als einer der Gründerväter des Internet gilt und die Position des «Chief Internet Evangelist» von Google bekleidet, fasste die Thematik im Jahr 2013 mit folgenden Worten zusammen: «Privatleben könnte einfach eine Anomalie sein»[16]. Kühnen Unternehmen kann nicht vorgeworfen werden, ihr Business Model auf philosophische Lehrsätze zu stützen, auch wenn sie auf diese Weise Robert Musil widersprechen, der behauptet, «[...] dass es gerade nur noch die Kaufläden gibt, wo man ohne Weltanschauung etwas bekommt»[17]. Wir möchten jedoch andeuten, dass sie sich irren und sich das Privatleben nicht so einfach begraben lässt, wie dies von den Netzgiganten und den Anhängern der Massenüberwachung gewünscht ist.

Die einfachste Art und Weise, das Privatleben zu charakterisieren, ohne es indessen mit der persönlichen Freiheit, der individuellen Autonomie oder der vor staatlichen Eingriffen geschützten und im Kern der liberalen Tradition liegenden «Privatsphäre» zu verwechseln, ist informationell: Ich habe ein Privatleben, wenn ich den Zugriff anderer auf meine personenbezogenen Informationen kontrolliere. Und ich habe ein Recht auf Privatleben, wenn ich das Recht habe, den Zugriff anderer auf meine personenbezogenen Informationen zu kontrollieren[18]. Kontrolle liegt dann vor, wenn ich in der Lage bin, zu entscheiden, wer Zugriff auf meine personenbezogenen Informationen hat, wann und wie der Zugriff erfolgt und wie die auf diese Weise verfügbare Information genutzt wird. Ein derartiger Ansatz hat zwei Vorteile. Zunächst entspricht er unserem intuitiven Verständnis des Begriffs. So bringt es die Juristin Ruth Gavison sehr treffend zum Ausdruck: «Unser Interesse am Privatleben [...] hängt mit unseren Sorgen bezüglich der Zugänglichkeit durch andere zusammen: in wie weit sind wir anderen bekannt, in wie weit haben Dritte physischen Zugriff auf uns und in wie weit sind wir Gegenstand der Aufmerksamkeit anderer»[19].

13 Richard Barbrook & Andy Cameron, «The Californian Ideology», Science as Culture 6.1 (1996): 44-72 [Online zugänglich: http://www.imaginaryfutures.net/2007/04/17/the-californian-ideology-2/]. Für eine sorgfältige Untersuchung der Debatte um Cyber-Politik, siehe Fred Turner, From Counterculture to Cyberculture, University of Chicago Press, 2006. Für eine methodische Kritik, siehe Evgeny Morozov, To Save Everything Click Here, Penguin, 2013.

14 Christophe Lagane, «Google et la vie privée: petites et grosses perles d'Eric Schmidt», Silicon.fr, 2012 [Online eingesehen am 29. April 2015: http://www.silicon.fr/google-et-la-vie-privee-petites-et-grosses-perles-deric-schmidt-43955.html]

15 http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov

16 http://techcrunch.com/2013/11/20/googles-cerf-says-privacy-may-be-an-anomaly-historically-hes-right/.

17 Robert Musil, L'homme sans qualités, Band 1, fr. Übs. Ph. Jacottet, Seuil, 1956, S. 304.

18 Siehe z. B. Adam Moore, «Privacy: Its Meaning and Value», American Philosophical Quarterly 40:3, 2003; S. 215-227.

19 Ruth Gavison, «Privacy and the Limits Of Law», The Yale Law Journal 89:3, 1980, S. 421-471; hier: S. 423.

Zweitens ist der Ansatz, wie wir im weiteren Verlauf noch sehen werden, eng mit dem Bundesdatenschutzgesetz verknüpft und ermöglicht es, seine philosophische Kohärenz in den Vordergrund zu rücken. Von diesem Gesichtspunkt aus wird unser Recht auf Privatleben insoweit unrechtmässig oder rechtmässig durchkreuzt, als wir daran gehindert sind, den Zugang Dritter zu unseren personenbezogenen Informationen zu kontrollieren. Technisch betrachtet können diese Verletzungen des Rechts auf Privatleben dem Modell der Beschränkung oder dem Modell des Diebstahls folgen: Bei einer Einvernahme bin ich gezwungen, bestimmte personenbezogene Informationen offenzulegen; im Falle der Überwachung werden mir bestimmte personenbezogene Informationen gestohlen. In beiden Fällen können wir von einer intrusiven Informationsbeschaffung sprechen.

Die Verletzungen des Privatlebens gehen jedoch über die Sammlung von Informationen hinaus und können später im Rahmen der Informationsverarbeitung bzw. -verbreitung erfolgen[20]. Die Verarbeitung der gesammelten Information kann sich, auch ohne Intrusion, beispielsweise in den Fällen als problematisch erweisen, in denen eine einem Empfänger X für einen Zweck Y freiwillig mitgeteilte Information später für einen Zweck Z verwendet wird, dem ich niemals zugestimmt habe. Aus

20 Daniel J. Solove, «A Taxonomy of Privacy», University of Pennsylvania Law Review 154:3, 2006; S. 477-564.

Das 2000 in Kraft getretene «Safe Harbor»-Abkommen beschränkt den Datenaustausch von Europa in die USA. Das Abkommen ist bestrebt folgendes Problem zu lösen: Die europäische Gesetzgebung zum Schutz der Privatsphäre sieht vor, dass persönliche Daten der europäischen Bürger nur an Länder, die einen genügenden Schutz gewährleisten, weitergegeben werden können. Die USA erfüllten die verlangten Schutzauflagen Ende der 1990er Jahre nicht. Um ein Einfrieren der wirtschaftliche Beziehungen zwischen den USA und Europa zu vermeiden, haben das US Wirtschaftsministerium und die Europäische Kommission ein Abkommen getroffen: US Unternehmen können sich freiwillig einer Reihe von Datenschutzprinzipien unterwerfen, die von Europa als ausreichend eingeschätzt werden. Ungefähr 4500 US Unternehmen machten vom «Safe Harbor»-Abkommen Gebrauch.

Das Abkommen erlitt einen Rückschlag durch ein Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015. Kritiker sprechen in diesem Zusammenhang von einer vollständigen Aushöhlung von «Safe Harbor». Nach Einschätzungen des Gerichtshofes im Rechtsstreit zwischen dem österreichischen Datenschutzaktivisten Max Schrems und Irland – dem europäischen Hauptsitz von Facebook – bot das «Safe Harbor»-Abkommen keinen genügenden Schutz mehr: Ob sie nun den «Safe Harbor»-Prinzipien angehören oder nicht, die US Unternehmen können keinen ausreichenden Schutz gegen Nachrichtendienste der Regierung wie die NSA gewährleisten. Folglich konnte von nun an jeder europäische Staat selbst entscheiden, ob die Daten seiner Bürger in die USA ausgetauscht werden dürfen oder nicht. Dieser Entscheid stürzte die US Firmen und die Anbieter von Clouding-Dienstleistungen in eine grosse Unsicherheit. Bereits etablierte Datenaustauschpraktiken und Hauptsitze von Internetriesen wie Facebook sind einem nie dagewesenen und permanenten Risiko von Rechtsstreiten ausgesetzt.

diesem Grund sieht das Bundesdatenschutzgesetz Folgendes vor: «Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde»[21]. Die Bearbeitung der Information kann allerdings auch dann problematisch sein, wenn diese nicht ausreichend gegen Indiskretionen Dritter gemäß Art. 7 des Bundesgesetzes geschützt ist: «Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden». Schließlich kann es auch bei Verbreitung der Information zu Verletzungen des Privatlebens kommen, wenn ein «Inhaber einer Datensammlung» laut Bundesgesetz «ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile» bekanntgibt[22]. Bei einer unsachgemässen Bearbeitung kann die betroffene Person die Nutzung ihrer personenbezogenen Informationen nicht mehr kontrollieren; im Falle einer ungerechtfertigten Verbreitung kann sie nicht mehr kontrollieren, wer Zugang zu ihren personenbezogenen Informationen hat. In beiden Fällen kommt es zu einem Verlust der Kontrolle, einem Verlust von Privatleben und schließlich zu einer Verletzung des Rechts auf Privatleben. Es gibt daher auf der Grundlage der einschlägigen Schweizer Gesetzgebung eine kohärente philosophische Auffassung des Rechts auf Privatleben. Welche Bedeutung kommt dieser zu? Schliesslich hat Mark Zuckerberg nicht ganz unrecht: Der Erfolg der sozialen Netzwerke zeugt von einem zeitgenössischen Geschmack für Selbstdarstellung, der vielleicht in der Tat eine Evolution der Sitten im Hinblick auf die Intimgrenzen verrät[23]. Wir müssen jedoch Folgendes klarstellen: Aus einer tatsächlichen Erwägung lässt sich keine normative Schlussfolgerung ziehen, ohne sich dessen zu bedienen, was die Philosophen als naturalistisches Scheinargument bezeichnen. Selbst wenn als Tatsache angenommen würde, dass das Privatleben statistisch betrachtet im Jahr 2015 weniger populär als im Jahr 1950 ist, könnte daraus weder geschlossen werden, dass das Privatleben weniger Wert besässe noch dass das Recht auf Privatleben kein gerechtfertigter Anspruch mehr sei. Es besteht jedoch kein Zweifel daran, dass unmittelbar nach dem 11. September das Verbot der Folter weniger populär geworden ist, zumindest in bestimmten Kreisen. Aber niemand hätte daran gedacht, dass dies ausreichen würde, um zu beweisen, dass das Verbot weniger begründet sei. Wir können daher die soziologischen Erwägungen beiseite lassen und uns eher den moralischen und politischen Argumenten zu Gunsten des Rechts auf Privatleben zuwenden.

Hierzu existiert ausreichend Literatur und wir sind unweigerlich in unseren Ausführungen zu knapp[24]. Die Argumente zu Gunsten des Rechts auf Privatleben lassen sich in zwei Gruppen untergliedern: Ein erster Ansatz unterstreicht den individuellen Wert des Privatlebens, und ein zweiter den kollektiven Wert. Bezüglich des individuellen Wertes des Privatlebens sind drei grundsätzliche Überlegungen anzuführen. Zunächst ist das Privatleben von wesentlicher Bedeutung für die individuelle Autonomie – d. h. die Fähigkeit, sein Leben auf der Grundlage einer sachlichen persönlichen Beurteilung triftiger Handlungsmotive zu gestalten. Seit John Stuart Mill[25] wird davon ausgegangen, dass

21 Bundesdatenschutzgesetz, Art. 4.

22 Bundesdatenschutzgesetz, Art. 12.

23 Siehe z. B. George Kateb, «On Being Watched and Known», Social Research 68:1, 2001, S. 269-295.

24 Einen guten Überblick liefert Ferdinand Schoeman (éd.), Philosophical Dimensions of Privacy. An Anthology, Cambridge University Press, 1984.

25 John Stuart Mill, De la liberté, fr. Übs. L. Lenglet, Gallimard «Folio», 1990.

der Konformismus ein grundlegendes Hindernis für die Autonomie ist: Im Bemühen, den Erwartungen anderer gerecht zu werden, handle ich nicht auf der Grundlage meiner informierten Beurteilungen und meiner Urteile anhand dessen, was richtig, gut oder sinnvoll wäre, zu tun, sondern auf der Grundlage dessen, was der andere für richtig, gut oder sinnvoll erachtet. In diesem Zusammenhang gilt es als eine grundlegende Bedingung für Autonomie, zu kontrollieren, was andere über mich sagen: Das Privatleben bietet mir einen vor den Blicken meiner Mitmenschen geschützten Raum, in den ich mich zurückziehen kann, um mich den Erwartungen Dritter zu widersetzen. Schliesslich ist das Privatleben grundlegend für die Achtung der Menschenwürde. Stellen wir uns doch das Verschwinden des Privatlebens vor: Wir würden ständig beobachtet, registriert, blossgestellt. Stützt man sich beispielsweise auf die Ausführungen von George Kateb, käme es zu zwei Problemen. Einerseits könnten wir recht einfach beschuldigt bzw. angegriffen werden: «Man gilt als interessant, ja sogar als mutmasslich oder potenziell schuldig, selbst wenn man das Gesetz respektiert». Auf diese Weise würde eine gewöhnliche Form der Menschenwürde im Sinne eines sozialen Status als ehrenhafte Person angegriffen. Andererseits würden wir als Untersuchungsgegenstände behandelt - demnach als Gegenstände: «Man wird einfach wie ein zu beobachtendes zweideutiges oder pathologisches Exemplar behandelt»[26]. Es würde dann also eine philosophischere Form der Menschenwürde, übernommen aus der Kant'schen Tradition, im Sinne eines moralischen Status einer objektivierbaren Person angegriffen. Unter diesem Gesichtspunkt ist die Menschenwürde dieser nicht verhandelbare Wert, den jeder Mensch auf Grund seiner Menschlichkeit besitzt und der verlangt, einen anderen Menschen stets als bewusstes, rationales und freies Subjekt und niemals nur als Objekt zu behandeln, andere Menschen - im Kantschen Vokabular - immer als Zweck an sich selbst und nicht lediglich als Mittel zu einem anderen Zweck zu behandeln[27]. Schliesslich ist das Privatleben von grundlegender Bedeutung für die zwischenmenschliche Intimität. In einem bekannten Artikel stellt der Philosoph Charles Fried die These auf, dass das Privatleben der «notwendige Kontext für Liebe, Freundschaft und Vertrauen» sei[28]. Sein Argument sei einfach und verdiene es, trotz aller Fragen, die es aufwirft, dass Menschen wie Mark Zuckerberg darüber nachdächten. Die zwischenmenschliche Intimität, wie sie sich in der Liebe und in der Freundschaft manifestiert, erfordert eine «spontane Aufgabe» der Barrieren, die uns üblicherweise vor Fremden schützen: Romeo liess, wie einer Redewendung zu entnehmen ist, Julia in seine Intimsphäre eintreten. Intimität, so Fried, ist genauer gesagt das «Teilen einer Information über seine Handlungen, seine Überzeugungen oder seine Emotionen, die man nicht mit jedem teilt und die man nicht mit jedem teilen muss»[29].

Wir stellen demnach fest, dass uns die moralische und politische Philosophie wahrlich gute Gründe liefert, dem Privatleben, trotz der Verkündung seines Endes seitens der Verfechter der kalifornischen Ideologie, einen Wert einzuräumen, der Modeströmungen überdauert.

26 George Kateb, art. cit., S. 271.

27 Für eine tiefergehende Analyse dieser Maxime im Sinne von Kant, siehe Onora O'Neill, «Between Consenting Adults», Philosophy & Public Affairs 14, 1985, S. 252-277.

28 Charles Fried, «Privacy», The Yale Law Journal 77:3, 1968, S. 475-493; hier: S. 478.

29 Ibid., S. 484.

Da dieses Recht existiert, kann man von spontaner Aufgabe sprechen. Und sobald ich (teilweise) die informationelle Barriere aufgebe, die mein Privatleben zu Gunsten jener, die ich mag, schützt, trete ich in eine selektive intime Beziehung. Ohne diese könnten Romeo und Julia keine besondere Beziehung haben. Das Recht auf Privatleben «bildet das moralische Kapital, das wir für Freundschaft und Liebe ausgeben»[30]. Das Verschwinden des Privatlebens würde das Todesurteil wertvollster menschlicher Beziehungen bedeuten.

Wie wir sehen, ist das Recht auf Privatleben nicht nur für «unsoziale» Individuen von Bedeutung. Es existieren ebenfalls Thesen, dass das Privatleben von grundlegender Bedeutung für das Befinden demokratischer Gemeinschaften sei, und es einen kollektiven Wert aufweise. Wie allgemein bekannt, sind demokratische Gesellschaften jedoch, trotz des Ideals der Gleichstellung, das sie beseelt, von Macht- und Herrschaftsverhältnissen durchzogen. Diese asymmetrischen Beziehungen verlangen, wie der Politologe James Scott sehr treffend darlegt, «öffentliche Transkripte»: erwartete Handlungs- und Kommunikationsweisen, die von der Einhaltung geltender sozialer Regeln und ideologischer Fiktionen zeugen, die diese rationalisieren[31]. In diesem Zusammenhang postuliert Scott, dass sich Gesellschaftskritik, Vorstellungskraft politischer Alternativen und Kontestationsdiskurse im Scheinwerferlicht nicht leicht entwickeln: Daher müssen «soziale Kulissenbereiche» existieren, die wie geschützte Labore funktionieren, in denen sich - abseits der Öffentlichkeit und zulässiger Normen der kollektiven Rationalität – Unzufriedene, Dissidenten und Militanten frei fühlen, alternative Modelle zu entwickeln und heterodoxe Standpunkte zu vertreten. Diese knappe Darstellung hätte eine weitergehende Behandlung verdient, reicht jedoch bereits aus, um die kollektive Bedeutung des Rechts auf Privatleben anzudeuten: Letztgenanntes stellt den Bürgern geschützte soziale Kulissen für die freie Entwicklung von Meinungsvielfalt zur Verfügung, ohne die sich die demokratische Meinungsbildung in eine Konsens-Komödie verwandeln würde. In allgemeinen Überwachungsregimen wie PRISM oder im Regime der individuellen Offenlegung nach Zuckerberg würden die geschützten sozialen Bereiche unter der ständigen Beobachtung Dritter zerfallen und die demokratische Meinungsbildung würde massiv beeinträchtigt. Die Bürger würden auf diese Weise durch ein Übermass an Transparenz all diese kleinen Ideenlabors (Think Tanks) verlieren, in denen Gedanken ohne Angst vor unmittelbarer öffentlicher Beurteilung frei ausgetauscht und konkretisiert werden. Votieren ist gut; aber das Votieren für Ideen, die sich in einer ständigen Wiederholung desselben niemals erneuern, bedeutet den Hirntod der Demokratie.

Wir stellen demnach fest, dass uns die moralische und politische Philosophie wahrlich gute Gründe liefert, dem Privatleben, trotz der Verkündung seines Endes seitens der Verfechter der kalifornischen Ideologie, einen Wert einzuräumen, der Modeströmungen überdauert. Wir können nun untersuchen, wie dieser Wert im US-amerikanischen und Schweizer positiven Recht zum Ausdruck kommt.

30 Ibid., S. 484.

31 James C. Scott, Domination and the Arts of Resistance, Yale University Press, 1990.

3. USA versus Schweizer Eidgenossenschaft: Wie steht es um die Wahrung des Datenschutzes?

Im Gegensatz zu den Vereinigten Staaten, in denen die grössten Online-Speicherdienste ansässig sind, stellt die schweizerische Gesetzgebung auf dem Gebiet des Privatlebens einen wirksamen Schutz der Integrität von Daten in einer Cloud dar. Wie wir noch aufzeigen werden, bietet die Schweiz beim Schutz personenbezogener Informationen einen komparativen gesetzlichen Vorteil, der auf das Cloud Computing[32] Anwendung findet, da diese Art von Daten gegenüber anderen Formen digitaler Informationen nicht Gegenstand einer differenzierten rechtmässigen Verarbeitung sind. Insbesondere Personendaten unterliegen der am Speicherort geltenden Gesetzgebung. Die Ermittlung des Vergleichswertes in Bezug auf den Schutz von Daten aus dem Clouding in den USA und in der Schweiz erfordert daher die Berücksichtigung zweier Dimensionen des rechtlichen Rahmens beider Länder. Die Existenz einer Rechtsgrundlage, welche an sich dem Privatleben und dem Schutz von Personendaten im Bereich des Cloud Computing gewidmet ist, einerseits; und die Qualität des disruptiven rechtlichen Rahmens, d. h. das Mass, in dem die zulässigen Beeinträchtigungen gegenüber dem Grundsatz der Achtung des Privatlebens in Bezug auf das Cloud Computing geregelt sind, andererseits.

Wie wir noch aufzeigen werden, bietet die Schweiz beim Schutz personenbezogener Informationen einen komparativen gesetzlichen Vorteil, der auf das Cloud Computing Anwendung findet

Die Tatsache, dass ein Land von einer Gesetzgebung profitiert, die der Privatsphäre der Person gesetzliche Geltung verleiht, die auf gespeicherte digitale Informationen anwendbar ist, bildet den ersten grundlegenden Punkt, der es ermöglicht, den Vergleichswert, der dem Schutz von Personendaten aus dem Clouding beigemessen wird, zu ermitteln.

Der Grundsatz des disruptiven rechtlichen Rahmens geht seinerseits von einer Prämisse aus, die in direktem Zusammenhang mit den Enthüllungen von Edward Snowden steht. Betrachtet man PRISM als ein Exempel für systematische und massive Verletzung der Privatsphäre durch den Staat, kann man davon ausgehen, dass dieser eine konstante invasive Gefahr für unser Privatleben darstellt. Diese Invasion kann beispielsweise im Rahmen einer Ermittlung auch rechtmässig, ja sogar notwendig sein: Der Zugriff auf persönliche Daten von Personen, die in einen Mordfall verwickelt sind, kann sich für die Durchführung der Ermittlungen als unerlässlich erweisen. Dieser Zugriff hat indessen in einem rechtlichen Rahmen zu erfolgen, es müssen Beschränkungen existieren, um eine Ausweitung in Richtung Freiheitsbedrohung zu verhindern. Dabei geht es um die zweite Dimension, die es ermöglicht, den relativen Wert, der dem Schutz von Personendaten aus dem Clouding eines Landes beigemessen wird, zu bestimmen: das Mass, in dem der Zugriff seitens einer öffentlichen Behörde auf digitale Daten, die von einem beliebigen

32 An dieser Stelle wird lediglich die Gesetzgebung über den Schutz personenbezogener Daten analysiert. Die Integrität der durch juristische Personen gespeicherten Daten wird durch den Know-how-Schutz und den Schutz des Wirtschaftsgeheimnisses sowie durch die Frage (der Wahrung) des Berufsgeheimnisses garantiert (siehe Sylvain Métille, «Le secret professionnel à l'épreuve des mesures de surveillance prévues par le CPP», Medialex, 2011, S. 131-137. Siehe ebenfalls, die Schweiz betreffend, das Bundesgesetz über unlauteren Wettbewerb vom 19. Dezember 1986).

Anbieter für eine Person gespeichert werden, gesetzlich beschränkt und kontrolliert wird. Die vorliegende Analyse besteht daher in einem Vergleich des rechtlichen Rahmens zwischen den Vereinigten Staaten und der Schweiz. Erstgenannte, in ihrer Eigenschaft als Hoster der Clouding-Giganten, Zweitgenannte, als Outsider, mögliches Aufnahmeland von Anbietern, deren Speichermodalitäten einen grösseren Schutz des Privatlebens gewährleisten. Wir beginnen mit den Vereinigten Staaten.

Im US-amerikanischen Recht ist der Schutz des Privatlebens auf Verfassungsebene durch den 4th Amendment verankert; er beinhaltet für die Personen «the right to be secure in their persons, houses, papers and effects against unreasonable researches and seizures [...]». Der Schutz von Personendaten, welche solche aus dem Cloud Computing beinhalten, hat seine Wurzeln in der Auslegung dieser Verfassungsbestimmung[33]. Digitale Daten sind indessen in den Vereinigten Staaten Gegenstand einer Taxonomie, die je nach Status differenzierte Möglichkeiten der Beschaffung und Verarbeitung impliziert. Ob es sich um Metadaten, Inhaltsdaten, Übertragungsdaten oder um gespeicherte Daten handelt, die Regeln des Rechts, denen diese digitalen Informationen unterliegen, differieren und machen Eingriffe seitens der Regierung mehr oder weniger einfach. Lediglich die Inhaltsdaten sind vom 4. Zusatz betroffen; Sekundärdaten oder Metadaten, die durch Nutzung eines Dienstes anfallen (IP-Adressen, Zeit der Verbindung, Zugriffsdauer, besuchte Webseiten) sind ihrerseits nicht geschützt. Der Staat benötigt demnach keine gerichtliche Anordnung[34], um sie zu erhalten[35], eine einfache verwaltungsrechtliche Anordnung oder eine Ladung[36] sind ausreichend, um auf Sekundärdaten einer Person zuzugreifen, und dies bereits ab ihrer ersten Verbindung ins World Wide Web. Dies bedeutet, auf unsere Problematik angewendet, dass die Verbindungsdaten, die durch die Nutzung seitens eines Cloud-Dienstes anfallen, für den Staat leicht zugänglich sind. Eine erste Differenzierung zeichnet sich nun zwischen diesen Metadaten oder Sekundärdaten und den sogenannten Inhaltsdaten wie Inhalte von E-Mails, Inhalte von Telefongesprächen oder Dateiinhalte, ab. Lediglich letztgenannte Daten sind durch den 4. Zusatz abgedeckt. Bei den sogenannten Inhaltsdaten gibt es ebenfalls einen Statusunterschied. In der Tat unterscheidet das US-amerikanische Recht mittels des Electronic Communication Privacy Act of 1986 (ECPA) zwischen Übertragungsdaten und gespeicherten Daten. Der ECPA besteht aus dem Pen Register Act, dem Wiretap Act und dem Stored Communication Act (SCA). Diese drei Bestandteile sollen den Rahmen für die verschiedenen Arten der Überwachung bilden, die mit den verschiedenen Arten von Daten verknüpft sind. Elektronische Inhaltsdaten, sogenannte Kommunikationsdaten wie E-Mail-Austausch oder Anrufe, unterliegen dem Wiretap Act und bedürfen einer richterlichen Anordnung[37]. Sie dürfen nur im beschränkten Rahmen im Zusammenhang mit Strafsachen[38] abgefangen werden, und auch nur, wenn die Überwachung durch

33 Siehe: Perrine, 518 F.3d at 1204. United states v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983). Quon v. Arch wireless Operating Co., 529 F.3d 892, 905-06 (9th Cir. 2008).

34 Court warrant: einmalige und zielgerichtete Bewilligung, ausgestellt durch einen Richter oder Magistrat, für die Erfassung von Elementen, die durch den 4. Zusatz für Ermittlungszwecke geschützt sind.

35 Siehe: United States v. Miller, 425 U.S. 435 (1976).

36 U.S.C. § 2703(c) (2) (2012).

37 18 U.S.C. § 2516 (3) (2012).

38 Ibid. § 2515 (3) (2012).

einen «wahrscheinlichen Grund» gerechtfertigt ist, der «den höchsten Standard im amerikanischen Strafrecht» darstellt[39]. Der «wahrscheinliche Grund» impliziert, dass Eingriffe seitens des Staates vorgängig durch gewichtige Verdachtsmomente gerechtfertigt sein müsse; führt objektiv zum Verdacht, dass eine strafbare Handlung begangen wird oder begangen worden ist.[40] Dieser Aspekt des US-amerikanischen Rechts erfordert demnach vor der Überwachung eine Rechtfertigung, die auf Tatsachen basiert, welche als hinreichend für sich selbst sprechend gelten.

Die gespeicherten und mit einem Dritten geteilten elektronischen Daten, wie sie in einer Cloud vorliegen, unterliegen ihrerseits dem Stored Communication Act und geniessen einen Status, durch den ihr Schutz gegenüber invasiven Möglichkeiten seitens des Staates herabgesetzt wird. Der Stored Communication Act gilt «when law enforcement agents obtains email and related electronic informations shared with third party providers»[41] und betrifft «any temporary, intermediate storage that is incidental to the communication and any storage of such communication by an electronic communications service for purpose of backup protection of such communication»[42]. Diese Informationen, die mit einem Dienstanbieter geteilt werden, dürfen im Gegensatz zu den Übertragungsdaten im Rahmen jeder Art von Untersuchung beschafft werden[43]. Zudem sieht das Gesetz eine Differenzierung von Informationen vor, die über einen Electronic Communication Service (ECS) bzw. einen Remote Computing Service (RCS) gespeichert werden. Die erste Kategorie betrifft «any service which provides to users thereof [ECS] the ability to send and receive wire or electronic communication»[44], beispielsweise eine Mailbox, deren Nachrichten vom Nutzer auf seinem Gerät gespeichert werden. Die zweite verweist auf «the provision to the public of computer storage or processing services by means of electronic communication service»[45] – d. h., unter anderem, die von einem Anbieter auf einem externen Server wie im Falle des Cloud Computing gespeicherten Daten. Die ECS-Daten sind durch den 4. Zusatz geschützt und erfordern in den ersten 180 Tagen ihrer Speicherung eine gerichtliche Anordnung; nach Ablauf dieser Frist sind sie auf einfache verwaltungsrechtliche Anordnung – subpoena – , Anordnung einer Grand Jury, durch Gerichtsverfahren oder aufgrund gerichtlicher Verfügung verfügbar[46]. Die RCS-Daten besitzen 181 Tagen denselben Status wie die ECS-Daten, gegenüber staatlichen Eingriffen weisen sie den geringsten gesetzlichen Schutz auf. Eine klassische Anordnung ist somit für den Zugang nicht erforderlich, soweit die Überwachung nicht Gegenstand einer Rechtfertigung nach dem Grundsatz des «wahrscheinlichen Grunds» ist. Die Daten in einer Cloud fallen unter diese Kategorie und sind demnach, vergleichsweise betrachtet, im Rahmen einer Überwachung die zugänglichsten Daten. Der Foreign Intelligence Surveillance Act[47] erlaubt seinerseits die Überwachung mithilfe aller durch den ECPA vorgesehenen Mittel, vorbehalt-

39 Isaak Dore, «La Constitution Des États-Unis et L'accusé», Revue Internationale de Droit Comparé 57: 4, 2005, S. 959-69.

40 E., N. L.»Probable Cause for the Issuance of Search Warrants." University of Pennsylvania Law Review and American Law Register 76, no. 3 (January 1928): 305. doi:10.2307/3307461.

41 Susan Freiwald et Sylvain Métille, «Reforming the Surveillance Law: The Swiss Model» Berkeley Technology Law Journal 28, 2013, S. 1261-1332.

42 18 U.S.C. § 2510 (17).

43 Ibid. § 2703 (d).

44 Ibid.

45 Ibid. § 2711 (2).

46 Administrative subpoena, a grand jury subpoena, a trial subpoena, court order.

47 50 U.S.C. §§ 1801-1862 (2012).

lich des Vorliegens eines wahrscheinlichen Grunds, unter der Voraussetzung, dass der Gegenstand der Aufmerksamkeit entweder eine fremde Macht oder ein Agent einer fremden Macht[48] ist. Die Überwachungsgenehmigungen werden von einem aus 11 Bundesrichtern zusammengesetzten Geheimausschuss erteilt. Dieses Gesetz findet daher a priori angesichts des Wertes des wahrscheinlichen Grunds im US-amerikanischen Recht nur bei starkem Verdacht Anwendung, der durch objektive Anhaltspunkte einer fremden Macht, die Interessen der USA zu beeinträchtigen, untermauert wird. Zielsetzung muss sein, ausschliesslich Informationen über eine fremde Macht zu beschaffen. Der Patriot Act[49] lässt indessen eine radikale Änderung einfliessen, indem die fremde Informationsbeschaffung nicht als einziges Ziel, sondern als das wichtigste Ziel gilt[50]. Die Folgen dieser Änderung sind in Bezug auf den Schutz der Daten, darunter die Daten aus dem Cloud Computing, insofern gewichtig, als jede Person potenziell Zielscheibe einer solchen Überwachung werden kann.

Wenden wir uns nun der Schweiz zu. Die Schweiz ist Unterzeichnerstaat der Europäischen Menschenrechtskonvention, in der in Artikel 8 das «Recht auf Achtung des Privat- und Familienlebens» verankert ist, sowie des Internationalen Pakts über bürgerliche und politische Rechte, in dem die Person durch Artikel 17 vor Eingriffen Dritter in ihr Privatleben geschützt wird[51]. Als Mitglied des Europarates hat die Schweiz das Übereinkommen Nr. 108 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ratifiziert. Artikel 13 der Bundesverfassung besagt, dass jede Person «Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs»[52] und Anspruch «auf Schutz vor Missbrauch ihrer persönlichen Daten» hat[53]. Auf Bundesebene bezweckt das Bundesdatenschutzgesetz (DSG) «den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden»[54]. Sowohl durch Achtung der Grundsätze des jus cogens als auch durch innerstaatliches Recht verankert die Schweiz die Privatsphäre. Im Gegensatz zum US-amerikanischen Recht impliziert der gesetzliche Rahmen in der Schweiz keine für das Cloud Computing nachteilige

Das Nachrichtendienstgesetz

Das Nachrichtendienstgesetz (NDG), welches vom Parlament in der Oktobersession 2015 angenommen wurde, ersetzt fortan das Bundesgesetz über die Massnahmen zur Wahrung der inneren Sicherheit (BWIS). Das Gesetz soll eine neue allgemeine Gesetzesgrundlage für den Nachrichtendienst des Bundes (NDB) schaffen, dessen Kompetenzbereich es erweitert. Das neue Gesetz ermöglicht Hacking und die Nutzung von Spionagesoftware durch die Regierungsbehörde (Art. 25, Abs. 1, Bst. d.). Es erlaubt dem NDB zudem die Sammlung von im Ausland versandten Daten, welche die Schweiz über das Kabelnetz durchqueren. Dies « zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge […]» (Art. 38, Abs. 1).

48 Ibid. 1805 (a).

49 USA PATRIOT Act § 216, 115 Stat. 272, 288-90 (2001).

50 Ibid. 44 S. 1731.

51 «Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen».

52 Verfassung Art. 13 Abs. 1.

53 Ibid. Abs. 2.

54 DSG Art. 1

Taxonomie. Vom Gesichtspunkt der Möglichkeiten staatlicher Eingriffe in individuelle digitale Informationen, die von Dritten verarbeitet und/oder gespeichert werden, finden die gleichen Normen wie für die restlichen personenbezogenen Daten Anwendung. Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) erlaubt derzeit die Beschaffung digitaler privater Informationen, unabhängig davon, ob es sich dabei um Sekundärdaten oder um Inhaltsdaten handelt, nur im Rahmen eines Strafverfahrens oder im Rahmen der Suche und Rettung vermisster Personen[55], falls eine Zustimmung durch die Bundesanwaltschaft vorliegt[56]. Die Zustimmung wird nur bei bestimmten Verstössen[57] erteilt. Darüber hinaus muss die Überwachungsmassnahme als verhältnismässig und erforderlich angesehen werden[58]. Die Daten der Cloud unterliegen hier keiner Ausnahme und profitieren daher - wie auch die Informationen aus Fernmeldeverkehr - von einem umfassenden Schutz. Das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS), das durch das Nachrichtendienstgesetz (NDG) ersetzt werden soll, von dem weiter unten noch die Rede sein wird, erlaubt die präventive Überwachung von verdächtigen Personen nur in beschränktem Umfang[59] und muss sich in Bezug auf die Beschaffung digitaler persönlicher Informationen an das BÜPF halten. Es erlaubt daher keine vereinfachten staatlichen Zugriffe auf die Daten in einer Cloud. Wir stellen daher in Bezug auf die USA fest, dass (1) der Schutz von Metadaten gegenüber staatlichen Eingriffen unangemessen niedrig ist; (2) die verschiedenen Arten von digitalen Personendaten Gegenstand einer differenzierten rechtmässigen Verarbeitung unterzogen werden; und (3) die Daten des Clouding einer ungünstigen Taxonomie zum Opfer fallen.

Im Falle der Schweiz stellen wir fest, dass (1) eine klare Rechtsgrundlage existiert, die den Schutz digitaler Daten gegenüber staatlichen Eingriffen verankert; (2) Daten aus dem Clouding derzeit von einem Schutz profitieren, der dem anderer Arten von Personendaten entspricht; und (3) für Metadaten keine gesetzlichen Ausnahmen gelten. Diese Gegensätze sind in der nachstehenden Tabelle zusammengefasst:

(1) eine klare Rechtsgrundlage existiert, die den Schutz digitaler Daten gegenüber staatlichen Eingriffen verankert; (2) Daten aus dem Clouding derzeit von einem Schutz profitieren, der dem anderer Arten von Personendaten entspricht; und (3) für Metadaten keine gesetzlichen Ausnahmen gelten.

55 BÜPF Art. 1

56 StPO Art. 269 StPO Art. 273

57 StPO Art. 269 Abs. 2.

58 Ibid. Abs. 1.

59 BWIS Art. 14

	Vereinigte Staaten	Schweiz
Verbindungsdaten/Metadaten (IP-Adresse, Verbindungszeiten usw.)	• Nicht geschützt durch den 4. Zusatz • Ohne Anordnung auf einfache verwaltungsrechtliche Anordnung oder Ladung zugänglich	• Europäische Menschenrechtskonvention, Art. 8 • Internationaler Pakt über bürgerliche und politische Rechte, Art. 17 • Bundesverfassung, Art. 13 & DSG • BÜPF & NDG • Nur im Rahmen einer strafrechtlichen Ermittlung oder der Suche vermisster Personen zugänglich • Zustimmung durch die Bundesanwaltschaft • Bei bestimmten Arten von Vergehen zugänglich • Verhältnismässigkeit und Notwendigkeit
Inhaltsdaten Kommunikationsdaten (Inhalt der Kommunikation)	• Geschützt durch den 4. Zusatz • Unterliegen dem Wiretap Act • Auf richterliche Anordnung hin zugänglich • Nur im Rahmen einer strafrechtlichen Ermittlung zugänglich • Erfordert Klausel des «wahrscheinlichen Grunds»	
Über einen Electronic Communication Service gespeicherte Inhaltsdaten (auf dem eigenen Rechner über den Dienstanbieter gespeicherte Daten)	• Geschützt durch den 4. Zusatz • Unterliegen dem Stored Communication Act • Anordnung bis 180 Tage • Ohne gerichtliche Anordnung nach 180 Tagen auf einfache Anordnung oder Ladung zugänglich • Kein «wahrscheinlicher Grund»	
Über einen Remote Computing Service gespeicherte Inhaltsdaten (Daten, die vollständig durch einen Dienstanbieter gespeichert werden. Umfasst die Daten der Cloud)	• «Gleicher Status wie die ECS nach 181 Tagen»	

Angesichts der obigen Elemente können wir den Schluss ziehen, (1) dass das US-amerikanische Recht an sich in Bezug auf den Schutz von digitalen Daten, die in den Vereinigten Staaten elektronisch gespeichert werden, wie im Fall des Clouding , lückenhaft ist; und (2) dass die Schweiz die Privatsphäre in Bezug auf die digitalen Daten vergleichsweise stärker schützt. Die Eidgenossenschaft ist demnach geneigter als die Vereinigten Staaten, die Integrität der in der Schweiz im Rahmen des Clouding gespeicherten Daten zu gewährleisten.

4. Schlussfolgerung

Die Schweiz befindet sich demnach in einer seltenen Lage, die es ihr ermöglichen dürfte, die Verteidigung einer Grundfreiheit und Wirtschaftswachstum miteinander zu vereinen. Denn zusätzlich zu ihrem rechtlichen Status eines «sicheren Gebiets» vereint die Schweiz drei zusätzliche komparative Vorteile. Ersten, wie dies Mateo Meier, CEO von Artmotion, anmerkt, ist die Schweiz, da sie kein Mitglied der Europäischen Union ist, «[...] nicht durch gesamteuropäische Abkommen über den Datenaustausch zwischen Mitgliedstaaten gebunden»[60]. Zweitens geniesst sie den Ruf eines gesicherten Safes und kann so das Vertrauen in das Bankgeheimnis relativ leicht wiederherstellen, was einige schweizerische Anbieter von Cloud Computing, darunter MyKolab.com, bereits tun. Auf der Startseite prangt neben einem Wappen in Nationalfarben das Label Your Swiss «Data Bank». Drittens profitiert die Schweiz ebenfalls von ihrem Status als Alpenfestung; sie ist durch ihre Neutralität, ihre politische Stabilität und ihre militärischen Festungen im Herzen der Gebirge vor den Verwerfungen der Weltpolitik geschützt. MyKolab und Artmotion nehmen daher explizit die Errichtung ihrer data centers in ehemaligen inneralpinen Militärfestungen in Anspruch. Fast zu schön, um wahr zu sein. Denn wir leben in Zeiten einer globalisierten terroristischen Bedrohung; und die öffentliche Sicherheit verlangt vielleicht gerade, dass wir beim Datenschutz wie auch bei den bürgerlichen Freiheiten gewisse Kompromisse eingehen. Es ist ein klassisches Sicherheitsargument: Wie Präsident Obama am 7. Juni 2013 während der Snowden-Affaire sagte: «Man kann nicht 100 Prozent Sicherheit und 100 Prozent Privatsphäre [...] haben»[61]. Dem liegt der Gedanke zugrunde, dass Freiheit und Sicherheit wie zwei Schalen einer Waage sind: Wiegt die Sicherheit schwerer, wiegt die Freiheit weniger. Vieles liesse sich noch sagen zum Thema der Waage - Freiheit vs. Sicherheit - was wiegt schwerer?[62]. Lassen Sie uns an dieser Stelle nur zwei Schwächen dieses Modells aufzeigen. Zunächst ist zu sagen, dass sich das Bild der Waage auf einen strikten Gegensatz zwischen Freiheit und Sicherheit stützt. Dieser Antagonismus ist jedoch illusorisch: Es gibt keinen Gegensatz zwischen Freiheit und Sicherheit, weil die Freiheit eine Form der Sicherheit ist. Es ist diese Form der Sicherheit, die uns gegenüber dem Staat schützt. Die Freiheit, wie es Benjamin Constant ausgedrückt hat, bedeutet «die Vorsichtsmassnahmen der Regierten gegenüber den Regierenden»[63]. Würde man der Sicherheit die Freiheit entgegen setzen, würde dies unter diesem Gesichtspunkt bedeuten, die Sicherheit der Sicherheit entgegen zu setzen. Und Freiheit zu beschränken würde bedeuten, Staaten mehr Macht zu geben,

Die Schweiz befindet sich demnach in einer seltenen Lage, die es ihr ermöglichen dürfte, die Verteidigung einer Grundfreiheit und Wirtschaftswachstum miteinander zu vereinen.

60 Zitiert in Laura Secorun Palet, art. cit.

61 Siehe z. B. Huffington Post [http://www.huffingtonpost.com/2013/06/07/obama-defends-nsa_n_3406448.html]

62 Für hervorragende kritische Analysen, siehe Stephen Holmes, «In Case of Emergency: Misunderstanding Tradeoffs in the War on Terror», California Law Review 97:2, 2009, S. 301-355; Rahul Sagar, «Who Holds the Balance? A Missing Detail in the Debate over Balancing Security and Liberty», Polity 41:2, 2009, S. 166-188; Jeremy Waldron, «Security and Liberty: The Image of Balance», The Journal of Political Philosophy 11:2, 2003, S. 191-210; Lucia Zedner, «Liberty in the Face of Terror: Reflections From Criminal Justice», Journal of Law and Society 32:4, 205, S. 507-533.

63 Benjamin Constant, Principes de politique (1810) éd. E. Hofmann, Hachette, 1997, S. 388.

ihre Bürger zu bedrohen[64]. Das ist ein riskantes Vorhaben, auf das man es ankommen lassen kann, oder auch nicht. Eines Umstands sollten wir uns jedoch zumindest bewusst sein: Datenschutz und Recht auf Privatleben sind, von dieser Warte aus betrachtet, Bestandteile der allgemeinen Sicherheit. Zweitens, die Neugewichtung der bürgerlichen Freiheiten zu Gunsten der Sicherheit wird häufig durch die Unmittelbarkeit der Gefährdungslage gerechtfertigt. Dies ist schliesslich eine plausible These: Sind wir mit einer Situation konfrontiert, in der wir der «Gefahr eines grossen Schadens» ausgesetzt sind und in der wir «entschlossen oder sofort handeln müssen, um Verluste zu verhindern oder zu minimieren», kann es gerechtfertigt sein, gegen die allgemeinen Grundsätze der herkömmlichen Sittlichkeit zu verstossen[65]. Unter diesem Gesichtspunkt kann eine Neugewichtung zu Gunsten der Sicherheit in der Tat als eine «entschlossene Handlung» angesehen werden, die darauf ausgerichtet ist, eine grosse Bedrohung zu bekämpfen, indem die durch konventionelle öffentliche Ethik liberaler Demokratien geschützten Freiheiten abgeschwächt werden. Es handelt sich in der Tat jedoch um eine Illusion auf der Grundlage einer erheblichen Begriffsverwirrung. Denn die Waage von Sicherheit und Freiheit wird herangezogen, um Änderungen einer Rechtsordnung zu rechtfertigen: Es geht darum, die Gesetze zu ändern. Nun ist das Tempus der rechtlichen Veränderungen jenes der Dauer. Aber die Moral der Dringlichkeit und die Empfindungen, aus denen der Anschein des Natürlichen hervorgeht, hat als Zeitform die Unmittelbarkeit der punktuellen Handlung: Eine dringende Abweichung kann nicht dauern. Und die Gefahren im Zusammenhang mit dem Bild der Waage treten nun vollständig zu Tage: Aufbauend auf einer Logik vorübergehender Reaktionen möchte es die Ausnahme in der stabilen Zeitdauer der Rechtsvorschriften einbauen. Die Schweiz hat daher gute ethische und ökonomische Gründe, Daten von Personen und Unternehmen zu hosten, die Angst vor dem Hunger auf private Daten seitens der Regierung haben. Ein solcher komparativer Vorteil ist jedoch vergänglich: So verlassen beispielsweise in Frankreich einige Hosting-Unternehmen[66] das Staatsgebiet als Reaktion auf die Modalitäten für die Überwachung von Daten in der Cloud, die das von der Nationalversammlung am 5. Mai 2015 angenommene neue Nachrichtendienstgesetz impliziert. Wenn die Eidgenossenschaft, ihre Bevölkerung und ihre Unternehmen Nutzen aus dieser günstigen Dynamik ziehen möchten, müssen sich die Entscheidungsträger bei der aktuellen und künftigen Politik hinsichtlich digitaler Daten der Tatsache bewusst sein, dass die gegenwärtigen Chancen der Schweiz extrem fragil sind. Drei Punkte scheinen im Hinblick auf die Aufnahme und Erhaltung eines positiven Kreislaufs, bei dem das Recht auf Privatleben und ökonomische Chancen zusammen existieren können, von grundlegender Bedeutung zu sein. 1) Sicherheitseinbehalt. Die Schweiz muss sich nicht, wie dies die Vereinigten Staaten oder Frankreich praktizieren, auf Rechtsvorschriften

Es besteht die Notwendigkeit einer durch eine unabhängige Stelle durchgeführten Überwachung von staatlichen Eingriffen in Bezug auf Daten in einer Cloud.

64 Für eine umfassende Darlegung dieser These, siehe Nicolas Tavaglione, Gare au gorille. Plaidoyer pour l'Etat de droit, Labor & Fides, 2010.

65 Tom Sorrell, «Morality and Emergency», Proceedings of the Aristotelian Society 103, 2003, S. 21-37; hier: S. 22.

66 http://www.nextinpact.com/news/93871-loi-renseignement-eu-org-et-altern-org-plient-bagage-gandiexplique.htm [konsultiert am 05.05.2105]

stürzen, die den Schutz digitaler Personendaten auf dem Altar der Sicherheit opfern. In diesem Zusammenhang ist das neue Nachrichtendienstgesetzes (NDG), das das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) ersetzen soll, besorgniserregend. So ist in Artikel 25 des Entwurfs der Einsatz von Spionage-Software, GovWare, durch die Schweizer Geheimdienste verankert; Artikel 38, Kabelaufklärung, ermöglicht das Scannen grenzüberschreitender Datenströme (Inhaltsdaten)[67]. Diese beiden Möglichkeiten staatlicher Eingriffe erfordern eine Bewilligung[68], ihre Durchführung muss beim Bundesverwaltungsgericht als unabhängige Instanz beantragt werden. Es bleibt zu klären, nach welchen Modalitäten dieses über die Bewilligung entscheidet und welche Transparenz im Zusammenhang mit dem Entscheid herrscht.

2) Unabhängige Überwachung. Es besteht die Notwendigkeit einer durch eine unabhängige Stelle durchgeführten Überwachung von staatlichen Eingriffen in Bezug auf Daten in einer Cloud. Sollten sich Eingriffe als notwendig erweisen, müssen die Achtung des Grundsatzes der Verhältnismässigkeit und die strikte Beschränkung der Datenbeschaffung auf die als notwendig definierten Elemente sowie die Einhaltung der Speicherdauer durch eine unabhängige Behörde sichergestellt werden. Somit scheint die Stärkung der Rolle von Datenschutzbeauftragten eine Notwendigkeit darzustellen: Es ist daher wünschenswert, die institutionelle Unabhängigkeit der Datenschutzbeauftragten zu fördern, indem man ihnen ausreichende Handlungsmöglichkeiten garantiert und ihnen eine institutionelle Position einräumt, durch die sie vor dem Druck seitens der Exekutive geschützt sind. In der Romandie sind in den vergangenen Monaten mehrere kantonale Datenschutzbeauftragte (Genf, Wallis) aus ihren Ämtern ausgeschieden, weil man ihnen einen unzureichenden finanziellen und politischen Handlungsspielraum gewährte. Es besteht daher Grund zur Annahme, dass die politisch Verantwortlichen das Ausmass dieser Herausforderungen nicht erfasst haben. Getreu der freiheitlichen Tradition des Prinzips des Checks and Balances sollte die Schweiz sicherlich darüber nachdenken, den Status der Datenschutzbeauftragten zu «verrechtlichen».

Den Hosting-Unternehmen kommt ebenfalls eine Rolle zu, um die Schaffung eines Schweizer Informationsparadieses zu initiieren.

3) Verantwortung des Privatsektors Den Hosting-Unternehmen kommt ebenfalls eine Rolle zu, um die Schaffung eines Schweizer Informationsparadieses zu initiieren. Vom Gesichtspunkt der Wahrung des Datenschutzes in Bezug auf die Cloud müssen die Nutzer sich nicht nur auf die Behörden, sondern auch auf die Dienstanbieter verlassen können. Letztgenannte müssen demnach über zuverlässige Mittel verfügen, um eine gewisse Transparenz in Bezug auf die Art und Weise, wie sie die ihnen anvertrauten Daten verwalten, gewährleisten zu können[69]. Auch hier könnte sich eine unabhängige Stelle im Rahmen einer Evaluation zur Achtung des Privatlebens seitens der Hosting-Unternehmen äussern. Die Initiative wurde bereits durch TG-CSR (cloud - society and responsability) ergriffen. Ziel

67 Mit grenzüberschreitenden Daten sind sowohl Informationen, die vom Ausland in die Schweiz übertragen werden, als auch solche, die von der Schweiz ins Ausland übertragen werden, gemeint. Gegenüber Schweizer Staatsangehörigen und juristischen Personen ist die Überwachung nicht möglich. Sie ist bei Datenströmen innerhalb des Staatsgebietes nicht möglich.

68 NDG Art. 25.

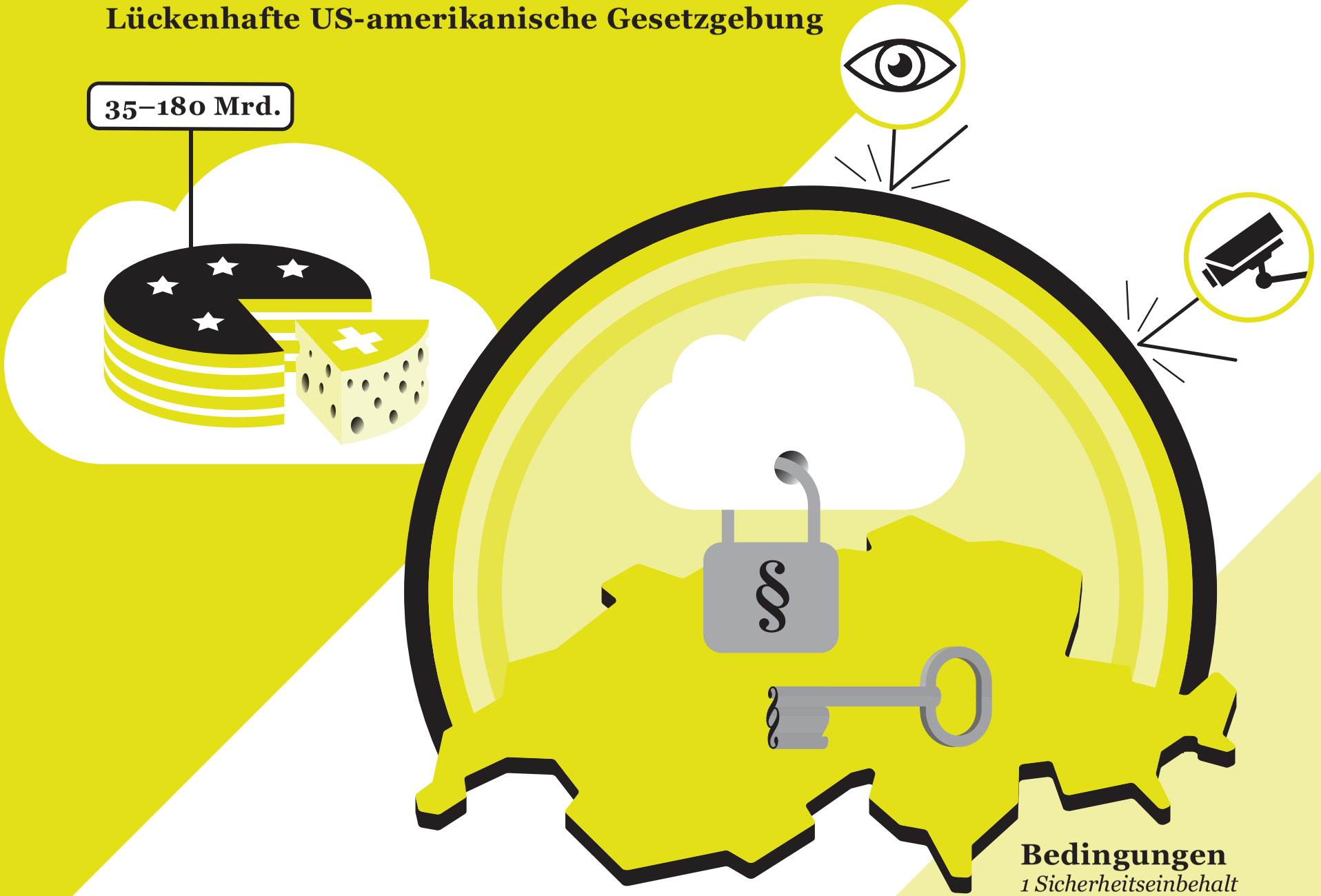
69 Für eine Problemanalyse zum Thema «Digitales Vertrauen» siehe Jean-Henry Morin, La responsabilité numérique, FYP éditions, 2014.

ist es unter anderem, eine Bewertungsskala in Bezug auf die Wahrung des Datenschutzes durch Unternehmen im Bereich des Clouding anzubieten.

Abschliessend lässt sich sagen, dass sich der Schweiz eine äusserst seltene Gelegenheit eröffnet, zwei Fliegen auf einen Schlag zu treffen: Förderung des Privatlebens durch Kultivieren von Wachstum und Förderung des Wachstums durch Kultivieren des Privatlebens. Wirtschaftskreise und zahlreiche Verfechter von bürgerlichen Freiheiten haben allen Grund, in diesem Zusammenhang Hand in Hand zu arbeiten. Aber sie kennen seit langem die Devise «Lachen und Weinen zugleich»: In einem Kontext, der so vertraut ist, dass es beinahe natürlich scheint, dürfte das Ende des Bankgeheimnisses Erstgenannten Kummer bereiten und Letztgenannten Grund zur Freude sein. Die digitale Wirtschaft in der Post-Snowden-Ära setzt sich auf recht aussergewöhnliche Weise für eine neuartige Verbindung ein: Die Unternehmer im digitalen Umfeld haben ein Interesse daran, philosophische Erwägungen in ihr Business Model zu integrieren; und Verfechter des Privatlebens haben ein Interesse daran, von der Schlagkraft der Wirtschaftskreise zu profitieren. Auf diese Weise entsteht ein positiver Kreislauf. In der Post-Snowden-Ära kann die Schweiz wirtschaftliche Gelegenheiten in einer Grössenordnung von Milliarden Dollar wahrnehmen, die nicht nur einen monetären, sondern ebenfalls einen ethischen Wert aufweisen, der eine willkommene Gelegenheit bietet, das Steuerparadies in ein digitales Paradies zu verwandeln. Warum solch eine gute Gelegenheit verpassen? **Das Steuerparadies ist tot; lang lebe das digitale Paradies!**

Lückenhafte US-amerikanische Gesetzgebung

35–180 Mrd.



Bedingungen

1 Sicherheitseinbehalt
2 Unabhängige Überwachung
3 Verantwortung des Privatsektors

Geht es in Richtung Datenparadies?

Bei *foraus* aktiv werden

als Mitglied
Eine Mitgliedschaft in unserem einzigartigen Netzwerk und ein ehrenamtliches Engagement bei *foraus* steht jeder und jedem offen. Wir bieten Dir Zugang zu einem hochkarätigen Netzwerk, spannenden Persönlichkeiten der Schweizer Aussenpolitik und der Möglichkeit, Dein wissenschaftliches Know-How in die öffentliche Debatte zu tragen.

als Autor
foraus ermöglicht es Dir, Herausforderungen der Schweizer Aussenpolitik konkret anzupacken und bietet Dir eine Plattform, Deine innovativen Ideen für die Schweizer Aussenpolitik im Rahmen eines Diskussionspapieres oder einer Kurzanalyse zu publizieren.

als Gönner
Unser Gönnerverein «Cercle des Donateurs» trägt zur Verbreiterung der Trägerschaft bei und bietet interessierten Persönlichkeiten die Möglichkeit, *foraus* nachhaltig zu unterstützen und zu fördern.

Neuste Publikationen

foraus Diskussionspapier 25
Migration aufgrund von Umweltveränderungen und die Rolle der Schweiz: Eine wachsende Herausforderung wirft grundlegende Fragen zur Zukunft des Migrationsrechts auf

foraus Diskussionspapier 24
Suisse-UE: les 50 qui comptent en 2015

foraus Diskussionspapier 23
Gefangen im Nullsummenspiel: Eine Bewertung der MEI-Umsetzungsvorschläge

www.foraus.ch

Zürich | *foraus* - Forum Aussenpolitik | Kurzgasse 4 | 8004 Zürich
office@foraus.ch | +41 77 462 33 08

Geneve | *foraus* - Forum de politique étrangère | c/o IHEID | CP 136 | 1211 Genève 21
bureau_romandie@foraus.ch | +41 22 908 44 56

PC-Konto: 60-176892-9