www.jusletter-it.eu

Robert Briner

Der NSA-Skandal: Etwas für Juristen?

The knowledge about the data interceptions of the American security service NSA (National Security Agency; www.nsa.gov) – transcending even bold visions – is at first sight calling for a detailed legal analysis. Taking one step back, a certain distance discloses a more important context.

Category: Discussions
Field of law: Data Protection; Data Security
Region: Switzerland

Citation: Robert Briner, Der NSA-Skandal: Etwas für Juristen?, in: Jusletter IT 15 May 2014

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1 Ausgangslage
2 Worum es nicht geht
3 Elemente einer Analyse
4 Fragen ohne Antworten
5 Fragen mit Antworten
6 Erkenntnis

1 Ausgangslage

[Rz 1] Offenbar ab Januar 2013[1] kopierte Edward Snowden als damals knapp 30jähriger Informatik-Mitarbeiter einer Firma, welche für die NSA arbeitete, unbemerkt (!) die enorme Menge von 1,7 Mio. – teilweise als «Top Secret» eingestuften – Dateien und lud sie auf einen USB-Stick. Er kontaktierte im Januar 2013 die Filmregisseurin Laura Poitras[2], und im Februar 2013 den Journalisten Glenn Greenwald. Unter einem Vorwand nahm er «für ein paar Wochen» frei und flüchtete am 20. Mai 2013 nach Hongkong, kurze Zeit später nach Russland. Er setzte die amerikanische *Washington Post* und den britischen *Guardian* in Kenntnis und verlangte die vollständige Publikation einer höchst brisanten Powerpoint-Präsentation über das «Prism»-Programm der NSA. Beide Zeitungen lehnten die vollständige Publikation der Präsentation ab, publizierten sie aber am 6. Juni 2013 in Auszügen, die auch so noch brisant genug waren. Eine Quellenangabe unterblieb bewusst, um Edward Snowden zu schützen. Am 9. Juni 2013 erfuhr die Öffentlichkeit auf Wunsch von Edward Snowden, dass er der Informant war, weil er richtigerweise davon ausging, dass der Verdacht bald auf ihn fallen werde. Seit nun über einem Jahr werden laufend neue Einzelheiten über die Internet-Spionage der NSA bekannt. Die NSA verfügt gemäss dem Bericht einer Internet-Zeitung über fünf Trilliarden Bytes Speicherplatz in Utah[3,4]. Gespeichert werden angeblich[5] «nur» die Verbindungsdaten (A hat dem B am Datum DDMMYY zum Zeitpunkt HH:MM:SS ein Mail geschickt), und nicht oder nur in Sonderfällen die Inhalte.

[Rz 2] Nur noch für laue Empörung sorgte die Bestätigung, dass die US-basierten Konzerne wie Microsoft oder Google in Nachachtung amerikanischer Gesetze sogenannte «Trap Doors» (Falltüren) in ihre Software eingebaut haben, welche es der NSA ermöglichen, deren Verschlüsselungen zu umgehen. Das war seit langem vermutet worden. Bekannt war zudem, dass den Unternehmen verboten war, sich dazu zu äussern (sog. «gagging orders»).

---

1 Zum Folgenden (statt vieler): Wikipedia, de.wikipedia.org/wiki/Edward_Snowden(alle Internet-Quellen wurden am 30. April 2014 nochmals überprüft).

2 Eine mehrfach preisgekrönte Dokumentarfilmerin, Initiatorin der *Freedom of the Press Foundation*, siehe z.B. en.wikipedia.org/wiki/Laura_Poitras.

3 Quelle: www.techradar.com/news/internet/cover-your-tracks-beat-the-nsa-and gchq-at-their-own-game-1205096.

4 Eine Trilliarde ist 1021. Eine solche Zahl sprengt das menschliche Vorstellungsvermögen. Die Entfernung zwischen Erde und Sonne beträgt 149.6 Mio km; wäre jedes Byte ein dünnes Blatt Papier (Dicke 0.1mm), ergäbe der Papierstapel 100'000'000 Mio km – gut 65'000 mal soviel wie die Distanz Erde-Sonne. Die Weltmeere haben ein Volumen von rund 1.3 Milliarden km3; da 1 km3 1 Billion (1012) Liter enthält, beträgt das Volumen der Weltmeere 1.3 x 1021 *Liter*– die NSA kann gut 3 mal soviele Bytes speichern. Astronomische Vergleiche kommen am nächsten: man kann gemäss www.astronews.com/frag/antworten/3/frage3209.htmlfür das gesamte Universum (!) vereinfachend von 100 Milliarden Galaxien mit je 100 Milliarden Sternen ausgehen, was 10 Trilliarden Sterne ergibt. Und gemäss derselben Quelle (www.astronews.com/frag/antworten/2/frage 2011.html) hat die Erde eine Masse von knapp 6 x 1021 Tonnen – gerade etwa soviele Bytes kann die NSA speichern.

5 Dass die Geheimdienste selber keine verlässlichen Angaben machen, liegt auf der Hand; dass bzw. ob Edward Snowden verlässliche Angaben macht, und dass die Medien aus seinem Fundus lauter verlässliche Informationen publizieren, sollte auch nicht als gegeben erachtet werden.

[Rz 3] Hingegen sorgte für Empörung, und zwar auch bei den betroffenen amerikanischen Unternehmen, zum Beispiel Google, Apple und Yahoo, dass die NSA «Anzapfstellen» in Datenübermittlungs-Knotenpunkten solcher Unternehmen plazierte, und auch das Untersee-Datenkabel zwischen dem europäischen und dem amerikanischen Kontinent direkt angezapft habe.

[Rz 4] Stückweise bekannt wurde auch die enge Zusammenarbeit der NSA mit ihrem britischen Gegenstück, der GCHQ (Government Communications Headquarter). Weniger bekannt ist, dass auch die Geheimdienste von Australien, Neuseeland und Kanada kooperieren. Diese Allianz ist unter dem Namen «Five Eyes» (Akronym: FVEY) bekannt[6], und operiert unter einem Abkommen namens UKUSA, *United Kingdom – United States of America Agreement*[7]. Mit *Five Eyes* kooperieren unter der Bezeichnung *Nine Eyes* Dänemark, Frankreich, Niederland und Norwegen, und unter der Bezeichnung *Fourteen Eyes* zusätzlich Deutschland, Belgien, Italien, Spanien und Schweden.

2 Worum es nicht geht

[Rz 5] Es ist offensichtlich müssig, als Jurist darüber nachzudenken, ob und in welcher Hinsicht oder in welchen Facetten solche Tätigkeit – und dann noch in solchen Dimensionen – mit den Gesetzen der Schweiz konform sei. Um nur die offensichtlich verletzten Rechtsnormen kurz zu erwähnen: Art. 13 der Bundesverfassung (BV) (Schutz der Privatsphäre; so auch Art. 8 der Europäischen Menschenrechtskonvention [EMRK]), Art. 28 des Zivilgesetzbuches (ZGB), Art. 1 ff. des Datenschutzgesetzes (DSG), Art. 272 ff. des Strafgesetzbuches (StGB), die sogenannten Computerdelikte wie z.B. Art. 144bis StGB[8], und wohl noch viele mehr.

[Rz 6] Ebenso müssig ist ein juristisches Nachdenken darüber, dass und warum Spionage als solche seit Menschengedenken praktiziert wird, woran nicht zu rütteln ist. Man darf in diesem Sinne als Bürger gleich welchen Landes sehr wohl hoffen, dass auch das eigene Land spioniert, und man kann und darf die Augen nicht davor verschliessen, dass geheimdienstliche Zusammenarbeit mit anderen Staaten – auch wenn die Schweiz nicht einmal zu den *Fourteen Eyes* zu gehören scheint – sinnvoll ist.

[Rz 7] Aber warum bleibt beim NSA-Skandal ein derart ungutes Gefühl?

3 Elemente einer Analyse

[Rz 8] Die Spionagetätigkeit der NSA bzw. der *Five Eyes* ist zunächst einmal in dem Sinne anders, als sie nicht gängigen Klischees entspricht: keine harten Männer in unauffälligen Mänteln mit Hut und dunkler Sonnenbrille, auch keine hinreissenden Frauen mit vielfältigen Fähigkeiten. Die Internet-Spione sind Leute «wie Du und ich», der einzige Unterschied sind ihre technischen Fähigkeiten und Hilfsmittel bei der Arbeit. Edward Snowden wäre auf der Strasse niemandem besonders aufgefallen. Das erzeugt Unbehagen.

[Rz 9] Internet-Spione arbeiten nicht verdeckt und gefährlich im fremden Land, sondern irgendwo auf der Welt, und sitzen vollkommen gefahrlos in einem Büro vor einem Computer. Das Ge-

6 Siehe z.B. en.wikipedia.org/wiki/Five_Eyes.

7 Siehe z.B. en.wikipedia.org/wiki/UKUSA_Agreement.

8 Vgl. z.B. Annina Baltisser, Datenbeschädigung und Malware im Schweizer Strafrecht, Diss Zürich 2013.

fühl sagt, dass die Spionage-Tätigkeit leichter und umfassender ist, obwohl auch ein Internet-Spion aufpassen muss, nicht erwischt zu werden.

[Rz 10] Es werden auch nicht Bunker, Raketenbasen, Waffenlager, Militärspitäler und Codes für den Zugang zu Festungswerken ausspioniert. Es schleicht auch niemand Entscheidungs- und Geheimnisträgern nach. Die Verfolgung geschieht lautlos und unsichtbar. Es braucht nicht einmal Wanzen – fester Bestandteil des Spion-Standard-Werkzeugkastens, um das Mobiltelefon der deutschen Bundeskanzlerin Angela Merkel abzuhören. Die Aufregung, die nach Bekanntwerden entstand, ist eigenartig. Sogenannte Wanzen zum Abhören von Räumen und Telefonen gehörten schon immer zum Standard-Werkzeugkasten eines Spions. Unbehaglich ist, dass es ohne Wanze geht, von irgendwo auf der Welt.

[Rz 11] Einer der offensichtlichen Gründe für die Empörung ist, dass nicht nur klassische Objekte der Spionage wie eben zum Beispiel die deutsche Bundeskanzlerin erfasst werden, sondern auch unverdächtige Bürger, nämlich *schlicht jedermann*, unterschiedslos, und ohne jeglichen Anfangsverdacht oder sonstige Begründung.

[Rz 12] Ein weiterer Angelpunkt ist der Umstand, dass *alles* (vgl. dazu aber oben bei Rz. 3) «mitgehört» und gespeichert wird oder werden kann, *was über das Internet oder über den Äther* läuft, wiederum unterschiedslos. Die NSA stellt sich auf den Standpunkt, sie suche Terroristen, und um die sprichwörtliche Nadel im Heuhaufen zu finden, müsse sie zuerst den Heuhaufen aufbauen[9]. Das ist zwar ein elegantes Bild, aber es sagt natürlich gleichzeitig, dass lauter Heu gesammelt wird, in der Hoffnung, es spüle auch einmal eine Nadel mit.

[Rz 13] Auf eine interessante Spur führt Art. 269 StGB: «Wer in Verletzung des Völkerrechts auf schweizerisches Gebiet eindringt, wird mit Freiheitsstrafe oder Geldstrafe bestraft. Dazu sagt die einhellige Kommentierung[10], dass Schutzobjekt «die Gebietshoheit» der Schweiz ist. Einhelligkeit besteht aber auch darüber, dass sich diese Gebietshoheit auf «Erde, Luft und Wasser» erstreckt. Als «Gebietshoheit» gilt die ausschliessliche Befugnis zur Vornahme von Hoheitsakten in sämtlichen staatlichen Funktionen betreffend Rechtsetzung, Rechtsprechung und Verwaltung auf dem Staatsgebiet[11]. Diese Fixierung auf die Territorialität zeigt sich auch darin, dass die Verletzung des Völkerrechts darin besteht, dass das Einmischungs- und Interventionsverbot von Art. 2 Abs. 4 der UN-Charta verletzt wird. Die Bestimmung lautet wie folgt: «Alle Mitglieder unterlassen in ihren internationalen Beziehungen jede gegen die territoriale Unversehrtheit [...] gerichtete Androhung oder Anwendung von Gewalt». Die dahinter stehende Vorstellung ist kongruent mit dem Datum der Charta, 26. Juni 1945. Aber passt das auch noch im Juni 2013?

[Rz 14] Der NSA-Skandal hat im Bewusstsein der Weltöffentlichkeit aus dem «frei» und «anonym» geglaubten Internet eine offen daliegende Fundgrube gemacht. Selbsternannte Propheten einer freien Welt dank Internet sind aus grosser Höhe auf den Boden der Realität gefallen[12]. Der berühmte Cartoon mit zwei Hunden vor einem Computerbildschirm und dem Text «In the internet nobody knows you are a dog» ist widerlegt.

---

9 So die NZZ vom 8. Februar 2014, S. 6 («Überwachung mit Lücken»), unter Berufung auf einen Artikel in der Washington Post vom 7. Februar 2014, der seinerseits auf eine Aussage eines hohen US-Beamten gegenüber dem amerikanischen Kongress verwies.

10 Statt vieler: Praxiskommentar StGB, Stefan Trechsel et al. (Dike, Zürich/St. Gallen 2008); Kommentar StGB (Hrsg. Andreas Donatsch), 18. Auflage, Orell Füssli, Zürich 2010.

11 Praxiskommentar StGB (Fn. 10), N 4 zu Art. 269 StGB.

12 Zum Beispiel Sascha Lobo, cf. NZZ vom 4. Februar 2014 S. 41 («Das Netz wird euch frei machen»).

[Rz 15] Die positiven gesellschaftlichen Auswirkungen des Internet, nämlich der einfache, leichte und schnelle Informationsaustausch, sind nur die eine Seite der Medaille. Wer glaubte, repressive Staaten würden nur Internetverbindungen kappen oder zensurieren, sieht sich eines besseren belehrt: Die Surfer werden belauscht. Das Belauschen, durch's Schlüsselloch gucken, in diesen Dimensionen verletzt auch das Anstandsgefühl – dahingestellt, ob es auf dem internationalen Parkett eine Bedeutung hat – und riecht nach ungehemmtem Voyeurismus. Es gehörte schon immer zum Repertoire der Spione, Peinlichkeiten zu sammeln und bei Bedarf nötigend einzusetzen: welch' ungeheurer Fundus über die gesamte Weltbevölkerung im Internet!

[Rz 16] Die Welt hat sich in den knapp 70 Jahren seit dem Ende des Zweiten Weltkriegs verändert. Bezogen auf die Thematik des NSA-Skandals beruht die Welt vielfach auf beherrschender US-Technologie (das Internet, Microsoft, Google, Apple, GPS), was dem amerikanischen Gesetzgeber erlaubt, auf diesem indirekten Weg eine Machtposition zu erlangen und auszubauen. Hinzu kommt, dass nicht einmal Berufsleute, geschweige denn der Konsument, wirklich wissen, was in ihren digitalen Geräten passiert, und dass sie es selbst dann nicht herausfinden könnten, wenn sie wollten. Wer weiss schon, was sein Smartphone so alles tut? Wer weiss schon, was mit einer E-Mail alles passiert, bis sie beim Empfänger ankommt? Wer weiss schon, dass die vielgepriesene «SSL-Verschlüsselung» (Websites mit «https://...») unsicher ist, nicht nur weil die NSA sie knacken kann, sondern weil die Sicherheit nicht durchgängig ist, zumal offenbar die Versionen 9 und 10 von Microsoft's Internet Explorer einen wesentlichen Sicherheitsmechanismus nicht unterstützen[13]? Wer wusste schon, dass die meisten Telekomunternehmen eine völlig veraltete, leicht zu entschlüsselnde Technik einsetzen[14]?

4 Fragen ohne Antworten

[Rz 17] Die vorstehenden Bemerkungen zeigen, dass das Schweizer Datenschutzgesetz zwar Schweizer schützt, aber nicht vor amerikanischen Mitarbeitern eines NSA-Subcontractors schützen kann, der wie Edward Snowden in Hawaii zum Beispiel über ein angezapftes Unterseekabel mithört. Sie zeigen auch, dass das StGB das Hoheitsgebiet schützt, das aber rein territorial verstanden wird, wie das die Staatengemeinschaft bei Niederlegung der UN-Charta sah. Last but not least: Es zeigt sich und rächt sich, dass wir nicht mehr Herr der Technik sind, die wir alltäglich nutzen und von der wir in hohem Masse abhängig sind.

[Rz 18] Welche Bedeutung kann der Begriff «Hoheitsgebiet» im Kontext des NSA-Skandals noch haben? Wie soll der Bürger entscheiden, wann er entweder auf E-Mail verzichten oder in Kauf nehmen muss, dass die NSA mithört? Wie kann der Konsument «nach angemessener Information freiwillig» (Art. 4 Abs. 5 DSG) darüber entscheiden, ob seine via Smartphone versandte E-Mail in die USA über das Unterseekabel läuft, wenn er keine angemessene Information erhält, sie mutmasslich jedenfalls technisch gar nicht verstünde, und keine praktikable Alternative hat? Wie soll das technologische Umfeld des berufstätigen Europäers aussehen, wenn er keine kompromittierten amerikanischen Produkte verwendet? Und: Was veranlasst den Konsumenten zur Erwartung, China tue nicht dasselbe, und sämtliche technologischen Produkte *Made in China* seien nicht

[13] Zu diesem Resultat kommt eine Studie vom November 2012: www.heise.de/ix/meldung/Studie-Informationen-trotz-SSL-Verschluesselung-nicht-sicher-1742426.html.

[14] NZZ vom 16. Dezember 2013, S. 3 («NSA-Enthüllung wirft schiefes Licht auf Telekom-Unternehmen»).

ebenso kompromittiert? Und welche Bedeutung hat es, dass die UNO eine Resolution verabschiedet, die das «Right to Privacy in the Digital Age» deklamiert[15]?

5 Fragen mit Antworten

[Rz 19] Stellen wir also Fragen, auf die es Antworten gibt!

[Rz 20] Frage: Kann man die Tätigkeit der NSA verhindern? Die Antwort ist ein schlichtes Nein.

[Rz 21] Frage: Kann man die Tätigkeit der NSA behindern? Da fällt die Antwort anders aus: Ja, man kann, und zwar auch als einfacher Bürger. Man kann weniger Information über sich selber ins Internet stellen. Man kann nicht-triviale Information verschlüsseln und als verschlüsseltes Attachment per E-Mail versenden.

[Rz 22] Frage: Kann man verhindern, dass die NSA Kontaktdaten sammelt (A hat dem B am DDMMYYYY um HH:MM:SS ein Mail geschickt)? Das kann «man» wohl üblicherweise nicht, weil «man» die technischen Kenntnisse nicht hat, aber Spezialisten sehen da durchaus Möglichkeiten. So hat Edward Snowden Maildienste benutzt, die das verhindern können. Es kann niemanden überraschen, dass diese US-basierten Maildienste umgehend von der NSA angegangen wurden und ihren Dienst einstellten, um nicht Trapdoors einbauen zu müssen, und dass sie ihre Server physisch vernichteten, um den Zugriff der NSA auf die Maildaten zu verhindern[16].

[Rz 23] Frage: Kann der Staat – die Schweiz – etwas tun? Antwort: Ja, der Staat hat die Mittel und Möglichkeiten, ein eigenes, proprietäres und sicheres Netz aufzubauen. Es ist kein Zufall, dass der Bundesrat das gemäss Pressemitteilung vom 3. Dezember 2013 in der Tat plant[17]; gemäss der Pressemitteilung ist ein solches Netz primär für die Armee gedacht, soll aber auch den Kantonen und den Rettungsdiensten zur Verfügung stehen. Damit steht der Bundesrat nicht allein da. In der NZZ vom 10. Februar 2014 (S. 5, «Mehr Mittel für Cyberkriege») war zu lesen, dass Frankreich punkto «Cybersicherheit» aufrüste und dem Schutz staatlicher Einrichtungen und der Privatwirtschaft Priorität einräume. Das ist eine elegante Formulierung dafür, dass man die Tätigkeit der NSA eindämmen wolle.

[Rz 24] Frage: Sieht die NSA dem tatenlos zu? Antwort: Nein. Soweit das nicht bereits der Fall ist, kommt es auch bezüglich der Internet-Spionage zum *Wettrüsten* zwischen denjenigen, die Spionage verhindern oder wenigstens behindern wollen, und der NSA und anderen Geheimdienstorganisationen.

[Rz 25] Frage: Kann man die NSA-Tätigkeit denn nicht einfach international ächten? Antwort: Nein. Die Resolution der UNO wird – pardon für den offenen Zynismus – wirkungslos verpuffen.

[Rz 26] Frage: Man kann doch auch ohne Internet auskommen? Antwort: Nein. Es wird soviel ferngesteuert, und die Fernsteuersignale laufen fast unfehlbar übers Internet, unsere Welt sähe anders aus. Was immer ferngesteuert wird, nutzt die Mobil-Technologie und/oder das Internet, und ist damit verwundbar. Staudämme, internationale Stromleitungen, Videoüberwachungen, Zugsicherungssysteme, «einfach alles». Als anfangs Jahr in den USA 40 Millionen Kreditkarten-

15 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

16 So beispielsweise die Lavabit (www.lavabit.com), die anfangs August 2013 den Betrieb schloss und ihren Kunden auf ihrer Website unter anderem mitteilt, sie dürfe nicht sagen, weshalb – obwohl das mittlerweile jedermann wusste.

17 http://www.parlament.ch/d/mm/2013/seiten/mm-sik-s-2013-10-25.aspx.

daten von Kunden gestohlen wurden, da schlich auch niemand nächstens in die Serverräume; die Diebe verschafften sich elektronischen Zugang über eine Einrichtung, welche die Fernsteuerung der Temperatur in den Läden erlaubte[18]. Und mit dem hochgeschätzten «Internet der Dinge» geht das weiter: Der vielgepriesene Kühlschrank, der automatisch Milch nachbestellt, und das Baby-Watch-Gerät im Kinderzimmer stehen auch der NSA zur freien Verfügung.

[Rz 27] Frage: Und im eigenen Land, wie sieht es da aus? Antwort: Seien wir froh, dass wir wachsame Datenschutzbeauftragte haben! Zwei Beispiele. Radio SRF schickte am 7. Januar 2014 einen Beitrag über den Äther, wonach Ladengeschäfte zunehmend Videokameras einsetzen, welche die Bewegungen der Kunden überwachen und analysieren, um die Verkäufe zu optimieren. In der NZZ vom 4. Februar 2014 wurde darüber berichtet, dass im Kanton Zug Automobilisten bei der Ortseinfahrt nach Cham mit einer Videokamera registriert werden sollen, und bei der Ausfahrt ebenso – und wenn sie zu wenig lang in Cham waren und daher verbotenerweise einfach durch Cham hindurchgefahren sind (Nebenfrage: Wo im Strassenverkehrsgesetz (SVG) mag stehen, dass man das verbieten kann?), dank der Videoaufnahmen überführt und gebüsst werden. Für ein «Wehret den Anfängen» ist es längst zu spät. Wir sind mittendrin.

6 Erkenntnis

[Rz 28] Neue Gesetze? Eine Verfassungsänderung? Ein Sondergerichtsstand für Klagen gegen die NSA? Eine parlamentarische Untersuchungskommission? Ein Sonderstaatsanwalt? Die vorstehenden Fragen, auf die es sinnvolle Antworten gibt, zeigen die äusserst beschränkte Reichweite und Relevanz juristischer Überlegungen und juristischer Antworten.

[Rz 29] Ist der NSA-Skandal etwas für Juristen? Nein. Die Spionage und Überwachung wird innerstaatlich durch Gesetzgebung legitimiert, nicht anders als *Big Brother*. Dieser Teil der NSA-Geschichte – es ist der kleinste Teil, die Gesetzgebung dafür benötigt vielleicht maximal ein Megabyte, nicht 5 Trilliarden Bytes – mag etwas für Juristen sein. Aber der ganze Rest, der Skandal-Teil, nicht. Es gibt sie noch, die Bereiche, wo Juristen zwar reden können, aber nichts zu sagen haben.

Dr. iur. Robert G. Briner, Rechtsanwalt, ist Partner bei CMS von Erlach Poncet AG in Zürich. Er leitet dort die Gruppe Immaterialgüter- und Technologierecht. Er hat Lehraufträge an der Universität Zürich und an der Fachhochschule St. Gallen, Autor zahlreicher Fachartikel, Vorsitzender der Rechtskommission von SwissICT, und Vorstandsmitglied der Deutschen Gesellschaft für Recht und Informatik DGRI.

[18] NZZ vom 10. Februar 2014, S. 2 («Der Traum von der segensreichen Erfindung»).