FORSCHUNGSMATRIX FÜR EINE (GLOBALE) CYBERLAW-AGENDA – «CYBERLAW ALL 4 – 2016»

Viola Schmid

Professorin, Technische Universität Darmstadt, Fachgebiet Öffentliches Recht,
Hochschulstraße 1, 64289 Darmstadt, DE,
schmid@cylaw.tu-darmstadt.de, www.cylaw.tu-darmstadt.de

Schlagworte: ***Ge(recht)igkeit, Mindeststandards, Forschungsmatrix, Cyberlaw-Agenda, (IT-)Sicherheit***

Abstract: *Der Vorschlag einer «Forschungsmatrix» soll die Forschung «durch Netzwerke» fördern und reiht sich so in die IRIS 2016 Agenda – Forschung «über Netzwerke» – ein. Die Kommunikations- und Interaktionsstrategie ist hybrid (Papier- und Cyberspaceveröffentlichungen – «Cyberlaw All 2 – 2014» (www.cylaw.tu-darmstadt.de)). Review und Abstract im Vorfeld der IRIS 2016 dienen als «Pilot» für die Initiative zu einem (inter)nationalen Cyberlawdiskurs. Erster inhaltlicher Schritt ist das Design von «13 Basics». Nächstes Arbeitsergebnis – anschließend an das Feedback wie die Kritik der IRIS – soll die Sophistikation und Veröffentlichung dieser Basics in angelsächsischer Sprache im Cyberspace sein.*

1. Erste «Cyberlaw Crowd Research»: Abstract und Review

1.1. Was bisher geschah

Das obige Abstract ist die Fortschreibung (Sophistikation) *und* Verkürzung des «Einreicherabstract» aus 2015:

«Diesjähriges Thema von IRIS ist die Forschung *über* «Netzwerke». Dieser Beitrag soll die Forschung *durch* «Netzwerke» fördern. Kennzeichnend für diese «Netzwerke» sind Transdisziplinarität, Globalität und Mensch-Maschine-(Inter-)Aktion. Ziel dieser Vernetzung soll der Schutz der informationstechnologischen Lebensgrundlagen auch «in Verantwortung für die künftigen Generationen» (vgl. für die natürlichen Lebensgrundlagen Art. 20a GG) sein.

Dieser Beitrag hat einen Fokussierungsvorschlag zum Gegenstand – nämlich eine Agenda. Überzeugung der Autorin ist, dass erst rechtliche Strukturen der «Cybergovernance» den Cyberspace zur Cyberworld reifen lassen. Insoweit kann auf Kant rekurriert werden, der ein Leben nur mit (Ge)recht(igkeit) für lebenswert erachtet hat. Umgekehrt gilt: Ein Raum ohne Recht bleibt ein (technischer) Raum (Cyberspace) – er hat keine Chance, zur lebenswerten Welt zu erstarken.

Anders vielleicht als das Welt(völker)recht der Realworld und des Traditional Law (eigene Terminologie) zwingt die weitere Dimension des Cyberspace zu einer Internationalisierung der (rechts-)wissenschaftlichen Forschung. Globale Vernetzung wie Konkurrenz auf der einen, ubiquitäre Rechenassistenz auf der anderen Seite, lassen ein weitgehend berührungsloses Nebeneinander nationaler und europäischer (rechts-)wissenschaftlicher Forschung nicht mehr als akzeptabel erscheinen. Technologierechtsvergleichung ist insoweit Qualitätspostulat und nicht -desiderat. Eindrucksvolles Beispiel ist die (vorgebliche) Überraschung der US-amerikanischen Öffentlichkeit wie Rechtswissenschaft über die Daten«organisations»strategien[1]

[1] «Datenorganisation» ist der Oberbegriff der Autorin für das Erheben, Verarbeiten und Nutzen von Daten (§ 3 Abs. 2 bis 5 BDSG); siehe seit 2003 Schmid, Cyberlaw – Eine neue Disziplin im Recht?, in: Hendler/Marburger/Reinhardt/Schröder, Jahrbuch des Umwelt-

US-amerikanischer Nachrichtendienste im Juni 2013 infolge des «Snowden-Szenarios».

Der Blick auf sowie Einblick in die europäische und deutsche Rechtslage hätte auch US-amerikanischen Rechtswissenschaftlern die Frage aufdrängen müssen: Wie werden bei «uns» Daten«organisationen» zur Erfüllung von Sicherheitsaufgaben rechtlich und technologisch eingesetzt (hier sog. Informationstechnologisches Sicherheitsrecht)?

Summa summarum: Nur eine netzwerkende globale Wissensgemeinschaft (Community) kann die Herausforderungen analysieren und so eine Chance auf deren Bewältigung schaffen. Dieser Beitrag entwirft eine Agenda für den Beitrag des Cyberlaw, die Herausforderungen benennt sowie Szenarien auswählt. Die Auswahl wie die Reihenfolge der «*13 Basics für eine (globale) Cyberlaw-Agenda»* mögen umstritten sein – die Entschlossenheit der Autorin zum Angebot einer «Forschungsmatrix» wie zum Werben um «Schwarmintelligenz» (Cyberlaw-Crowd-Research) ist angekündigt.

Dieses Abstract wurde von einem Rezensenten[2] des Redaktionskomitees der IRIS 2016 positiv bewertet und wie folgt kommentiert (die Einwilligung zur Wiedergabe liegt vor):

«Datenschutz und Datensicherheit spielen eine herausragende Rolle in sich verdichtenden Netzwerken. Für Staat und Verwaltung ist Cybersicherheit genauso zentral, wie für Unternehmen und andere Organisationen. Netzwerksicherheit wird zum Überlebensfaktor, insbesondere dann, wenn nicht nur Datentransport und Vertrieb über das Netz laufen, sondern der gesamte Produktionsprozess (etwa in der Industrie 4.0). Erkennbar wird, was auch für die staatliche Sicherheit gilt: Niemand kann für sich allein Cyber-Sicherheit garantieren. Das erfordert eine globale Debatte über Cyberlaw-Prinzipien in Gemeinschaften. Entscheidend wird sein, welche Prinzipien gelten sollen und in welcher Form sie Eingang ins Recht finden können. Beitrag und Diskussion gehören damit zu den wichtigsten Zukunftsthemen in hochkomplexen Netzwerkstrukturen. Eine Matrix zu finden – die allgemeine Gerechtigkeitserwägungen mit den Entwicklungen der Informationsgesellschaft verbindet – ist ein Interessensprojekt! für eine interdisziplinäre Debatte.»

Diese – ungewöhnliche – Vorgehensweise der Auswahl des ersten Diskurspartners setzt sich bei der Präsentation des Diskursgegenstandes fort:

1.2. Projektmanagement: «Cyberlaw All 1 – 2003» bis «Cyberlaw All 4 – 2016» ...

Die Überführung von Erde wie Weltall in den Cyberspace ist ein kaum fassbares Unterfangen. Die Seitenlimitierung der IRIS motiviert zu einer differenzierten Präsentationsstrategie. Dieser Beitrag soll als erstes Tor dienen, das den Zugang zu Veröffentlichungen über mehr als ein Jahrzehnt wie auch zum Vortrag der Autorin auf der IRIS 2016 erleichtert («Back End-Funktion»).

1.2.1. «Cyberlaw All 1 – 2003» bis «Cyberlaw All 3 – 2015–2016»

Diese Papierveröffentlichung – «*Cyberlaw All 4 – 2016*» – wird deswegen durch mehrere Cyberspaceveröffentlichungen ergänzt. Im Rückblick festzuhalten ist: Grundlegend war 2003 die Veröffentlichung des Beitrags «Cyberlaw – Eine neue Disziplin im Recht?»[3], die das Entstehen wie das Ende einer neuen Disziplin des Rechts voraussah. Bereits 2003 hat also die Autorin einen Beitrag zur rechtswissenschaftlichen Erkundung des Cyberspace angeboten, der in 2016 hiermit als *erster Schritt* mit der Bezeichnung Dokument «*Cyberlaw All 1 –*

und Technikrechts 2003, S. 449 (469).

2 Die Verwendung männlicher Sprache erfolgt im Interesse von Klarheit, Kürze und Einfachheit verbunden mit der Bitte, nicht das grammatische Maskulinum auf das biologische Geschlecht zu reduzieren.

3 Schmid, Cyberlaw – Eine neue Disziplin im Recht?, in: Hendler/Marburger/Reinhardt/Schröder, Jahrbuch des Umwelt- und Technikrechts 2003, S. 449–480; *zum Ende der Disziplin S. 465 f.*

2003»[4] *identifiziert wird.*

Nach Bejahung des «Ob» für eine Wissenschaftsdisziplin «Cyberlaw» in 2003 bis 2016 stellt sich die Frage nach dem «Wie». In Bezug auf das «Wie» erfolgen jetzt und in Zukunft (2016) Veröffentlichungen der Dokumente «Der kleinste gemeinsame Nenner – 13 Basics zum Cyberlaw?» (in deutsch als «*Cyberlaw All 2 – 2014*»)[5] und «The 13 basics of a (global) agenda for cyberlaw – The perspective of a European-German cyberlaw professor («Cyberlaw All 3 – 2015–2016»).[6]

Sämtliche Dokumente – «Cyberlaw All 1 – 2003»[7] bis «Cyberlaw All 3 – 2015–2016» – sind zugänglich bzw. werden als Legal Open Source (LOS) Projekt auf der Homepage des Fachgebiets Öffentliches Recht an der Technischen Universität Darmstadt[8] zugänglich gemacht. Die gesamte CyLaw-Reports Series (über 30 Veröffentlichungen) ist Teil der Projektidee:

«*Pioneering Cyberlaw: Schritte zur recht(swissenschaft)lichen Erkundung einer 5. Dimension des Seins.*»

Erklärungsbedürftig ist die Differenzierung zwischen den Bezeichnungen «Cyberlaw All» und «Cyberlaw Special». Mit der Bezeichnung «Cyberlaw All» werden Dokumente gekennzeichnet, die sich dem Cyberspace in seiner *Totalität* widmen und nicht (nur) *technologiespezifische* (etwa RFID-Recht) und/oder *anwendungsspezifische* (etwa «E-Justice» – E-Justiz») Herausforderungen in den Vordergrund stellen. Mit der Bezeichnung «Cyberlaw-Special» werden «sektorspezifische» Dokumente gekennzeichnet,[9] weil sie sich entweder auf spezielle Anwendungen und/oder Technologien beziehen.

1.2.2. Dieser Beitrag als Vorbereitung von «Cyberlaw All 3 – 2015–2016»

In die Reihe dieser Veröffentlichungen fügt sich 2016 dieses Dokument ein, das konsequenterweise den Untertitel «*Dokument Cyberlaw All 4 – 2016»* trägt. Diese ineinandergreifende, auf einander aufbauende Publikationsstruktur erklärt sich zum einen mit dem Forschungsfortschritt, dem der Cyberspace mit der Möglichkeit dynamischer Veröffentlichungen entspricht, und zum anderen mit der Platzlimitierung dieser Papierveröffentlichung. Deswegen wird für längere Fußnoten in dieser Veröffentlichung etwa auf «Cyberlaw All 2 – 2014» referenziert. «Cyberlaw All 2 – 2014» enthält in deutscher Sprache eine Auswahl von Herausforderungen (die 13 Basics), die auch in Zukunft zu meistern sind. Im Anschluss an die IRIS 2016 ist die Cyberspaceveröffentlichung der Basics für den angelsächsischen Sprachraum projektiert – «*Cyberlaw All 3 – 2015–2016*». Diese (parallele) Arbeit mit «pending documents» ist Ausdruck der Zielorientierung des Besuchs bei der IRIS 2016. Zusammengefasst: «Cyberlaw All 2 – 2014» enthält *(Vorab-)Informationen* zu den inhaltlichen Basics einer Forschungsmatrix. «Cyberlaw All 4 – 2016» (dieser Beitrag) dient der Sophistikation dieser Basics für den angelsächsischen Sprachraum *nach der IRIS 2016* in «Cyberlaw All 3 – 2015–2016». Die hybride Vorgehensweise – papierene Einführung (Realworldveröffentlichung) in Cyberspace-Dokumente wie Vortrag – soll auch das Eingehen auf aktuelle Fragestellungen im Februar 2016 ermöglichen. So wird etwa mitzuteilen sein, dass das neue deutsche «Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für

4 Schmid, Cyberlaw – Eine neue Disziplin im Recht?, in: Hendler/Marburger/Reinhardt/Schröder, Jahrbuch des Umwelt- und Technikrechts 2003, S. 449–480.

5 Veröffentlicht als CyLaw-Report Nr. XXXVI, ISSN: 1867-1969. Abrufbar unter: http://www.cylaw.tu-darmstadt.de/home_2/forschung_4/onlinepublikationencylawreports_1/online_publikationen_cylaw_reports.de.jsp (3. Februar 2016).

6 Nach der IRIS zu veröffentlichen als CyLaw-Report Nr. XXXVII, ISSN: 1867-1969. Abrufbar unter: http://www.cylaw.tu-darmstadt.de/home_2/forschung_4/onlinepublikationencylawreports_1/online_publikationen_cylaw_reports.de.jsp (3. Februar 2016).

7 Eine Wiedergabe von «Cyberlaw All 1 – 2003» erfolgt im Rahmen der Cylaw-Reports auch aus Respekt vor der Papierveröffentlichung nicht – wohl aber die Verlinkung im Dokument «Cyberlaw All 2 – 2014» unter A. III. 3.

8 http://www.cylaw.tu-darmstadt.de.

9 Siehe Dokument «Cyberlaw All 2 – 2014», S. 4.

Verkehrsdaten»[10] bereits vor dem BVerfG angegriffen wird.[11]

Die Frage schließt sich an: Welchen Inhalten, welchen Strategien dient das Projektmanagement?

2. Forschungsmatrix: Ein offener Begriff mit Nachhaltigkeitsziel

Dieser Beitrag kündigt die Initiative für eine «Forschungsmatrix» an. Die weitere Frage, die sich stellt, ist: Was ist eine «Forschungsmatrix»? Die «Antwort» dieses Beitrags (Stand 1/2016) lautet: Hinsichtlich der Inhalte, der Methoden (LEXONOMICS?[12]), der Rechtskreise, der Rechtsordnungen und – last but not least – der Ergebnisse (*Outcome*) handelt es sich um einen Begriff, der einen offenen und dynamischen Prozess konturiert. Nur *ein Ergebnis* wird von der Autorin vorgegeben und ist insoweit «fix»iert. Hierbei handelt es sich um die Notwendigkeit *nachhaltiger rechtlicher Konturierung von Freiheit und Sicherheit* (etwa Art. 67 Abs. 1 AEUV) – und damit *die* Innovationschance dieser Forschungsmatrix. Methodisch setzt sich dieses Dokument die Aufgabe eines ersten Schritts – die Analyse von Gemeinsamkeiten wie Unterschieden in Abstract und Review. Es bietet so einen «Piloten» für das Projekt «Pioneering Cyberlaw» wie auch für die Forschungsmatrix.

3. Forschungsmatrix: «Pilot» mit einer Analyse von Review und Abstract

Essentiell für «Cyberlaw Crowd Research» (Abstract) und «Interessensprojekt» (Review) sind die perspektivischen Gemeinsamkeiten – der *common sense*. Ohne den Review vereinnahmen zu wollen (gekennzeichnet in folgenden Überschriften mit «?»), erfolgen eine Kommentierung der Gemeinsamkeiten und Unterschiede sowie Sophistikationen aus der Perspektive der Autorin.

3.1. Gemeinsamkeiten: Nachhaltige Konturierung von Freiheit und Sicherheit

Zunächst glaubt die Autorin dem Review entnehmen zu können, dass nachhaltige rechtliche Konturierung ebenfalls «nachgefragt» wird. Elementarer Bestandteil dieser Nachhaltigkeit ist die IT-Sicherheit.

3.1.1. Gemeinsamkeiten: IT-Sicherheit als conditio sine qua non (und als Verfassungsprinzip)

Der Review betont, dass *wegen der Vernetzung* IT-Sicherheit(srecht) traditionelle Vorstellungen von der Abgrenzung privater Freiheit und staatlichen Pflichten nicht zugrunde legen kann. Fokussiert zusammengefasst und von der Autorin *weitergedacht*: Eine im Cyberspace vernetzte (globale) Gesellschaft, die etwa von den Angeboten der E-Governance ernsthaft und nachhaltig profitieren will, braucht für das Rechtsstaatsprinzip (Art. 20 Abs. 3; 19 Abs. 4; 28 Abs. 1 S. 1 GG) des Traditional Law ein informationstechnologisches «Update» – ein konstitutionalisiertes (primärrechtliches*) Prinzip der IT-Sicherheit*. Erste Ansätze finden sich in Deutschland auf einfachgesetzlicher Ebene in dem am 25. Juli 2015 in Kraft getretenen «Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)»[13]. Dieses Gesetz verlangt erstmals die Kodifizierung eines Katalogs «kritischer Infrastrukturen» (Art. 1 Nr. 8 IT-Sicherheitsgesetz zu § 10 Abs. 1

[10] Vom 10. Dezember 2015, BGBl. I Nr. 51 vom 17. Oktober 2015, S. 2218.

[11] Forgó/Heermann, Vorratsdatenspeicherung 2015 – Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicher[frist] für Verkehrsdaten, K&R 2015, S. 753 (S. 759). Verfassungsbeschwerde von Tabea Rößner. Abrufbar unter: http://tabea-roessner.de/2016/01/06/verfassungsbeschwerde-gegen-vorratsdatenspeicherung-eingereicht/ (1. Februar 2016).

[12] Schmid, § 55a Rn. 1, 14, 53, 55, 78, 136; § 55c Rn. 2; § 173 Rn. 3, 9, 62, 71 f., in: Sodan/Ziekow (Hrsg.), Kommentar zur Verwaltungsgerichtsordnung, 4. Auflage, 2014 sowie Schmid, New «E-Justice» Law in Germany since 2013 – A Temple Architecture for an «Agenda of Securitization», in: Dardick/Endicott-Popovsky/Gladyshev/Kemmerich/Rudolph (Eds.), Report from Dagstuhl Seminar 14092 «Digital Evidence and Forensic Readiness», p. 163, 166.

[13] BGBl. I Nr. 31 vom 24. Juli 2015 S. 1324.

BSIG[14]), für die spezielle IT-Sicherheitsstandards gelten (über § 9 BDSG mit Anlage hinaus).[15]

3.1.2. Gemeinsamkeiten: Thesen zur (Äußerungs-)Freiheit

Der Review formuliert «Das erfordert eine globale Debatte über Cyberlaw-Prinzipien in Gemeinschaften. Entscheidend wird sein, welche Prinzipien gelten sollen und in welcher Form sie Eingang ins Recht finden können.» Dieser Beitrag schlägt – inspiriert durch den Review – folgende Grundannahmen/Basics vor.

3.1.2.1. Zur Bedeutung von (nationalstaatlichen) «Rechtstraditionen»

Art. 67 Abs. 1 AEUV verlangt unionsrechtlich zum einen den Respekt vor und die Gewährung von «*Freiheit, Sicherheit und Recht*», zum anderen aber auch die Achtung von «Rechtsordnungen und -*traditionen* der Mitgliedstaaten». Welche Bedeutung diese Traditionen der Mitgliedstaaten bei der rechtlichen Konturierung des Cyberspace haben werden, beginnt sich derzeit erst anzudeuten. So hat beim Äußerungsinhaltsrecht der EGMR einen deutschen Sonderweg bei volksverhetzender Sprache respektiert.[16] Diesen im Traditional Law erkämpften wie verteidigten Status von Äußerungs*freiheit* auf der einen und der hier sog. «negativen Rezipientenfreiheit» auf der anderen Seite gilt es im Cyberspace erneut einer Analyse zuzuführen wie einer Konsensfindung zu unterbreiten. Auch die unterschiedlichen transatlantischen Vorstellungen über «Hate Speech» – deutlich geworden etwa an der Nichtratifikation des Zusatzprotokolls[17] zur «Convention on Cybercrime»[18] durch die USA[19] – bereiten auf traditionelle «Sonderwege» zum «Weltrecht» Cyberlaw vor. Evident ist nach hier vertretener Ansicht, dass der Blick in die *unvernetzte Welt der Vergangenheit (Realworld) wie in ihr maßgebendes Recht* (*Traditional Law*) nicht unmittelbar weiterhilft.

3.1.2.2. Absage an pauschale «Parallelitätsthese»: «Es war schon immer so…»

Vorhersehbar ist: Plumpe Parallelitätsdogmen, die Cyberspace und Realworld als gleichartig begreifen wollen (Motto: «Es war schon immer so und so soll es bleiben»), werden für die globalen Audiences des nichtvergessenden Internets nicht überzeugen können. Insoweit wird – aus Platzgründen – auf die Ausführungen in dem Dokument «*Cyberlaw All 2 – 2014»* mit Beispielen aus dem unionalen Finanzmarktinformationsrecht wie dem deutschen Recht der «Cyber-Hygienepranger» Bezug genommen.[20] Festzuhalten ist: Der Cyberspace als 5. Dimension des Seins bietet so neue Chancen, dass eine parallele Betrachtung von Realworld auf der einen und Cyberspace auf der anderen Seite mit dem *Anspruch identischer Standards wie Ergebnisse* nicht überzeugt. Eine weitere Konsequenz dieser Öffnung rechtswissenschaftlicher Argumentation für innovative Rechts«konzeptionen» (etwa eine Schutzpflicht für die körperliche Unversehrtheit, die mit E-Health-Strategien erfüllt wird [Art. 2 Abs. 2 GG]) ist die Absage an strikte «Trennungsthesen».

---

14 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).

15 Art. 1 Nr. 7 IT-Sicherheitsgesetz zu §§ 8a ff. BSIG; Art. 3 Nr. 1 lit. b IT-Sicherheitsgesetz zu § 11 Abs. 1b und 1c Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG).

16 BVerfG 8. November 2009, 1 BvR 2266/04, nachfolgend EGMR 8. November 2012, 43481/09. Es handelte sich um eine Tierschutzinitiative, deren Werbung in anderen Staaten – insbesondere den USA – rechtlich unbeanstandet geblieben ist. Als Verschlagwortung wird der Titel der Werbekampagne vorgeschlagen: «Der Holocaust auf Ihrem Teller».

17 Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, Straßburg, 28. Januar 2003, SEV Nr. 189.

18 Übereinkommen über Computerkriminalität (Convention on Cybercrime), Budapest, 23. November 2001, SEV Nr. 185.

19 Siehe das Gesamtverzeichnis zum Zeichnungs- und Ratifikationsstand, SEV Nr. 189. Abrufbar unter: http://www.coe.int/de/web/conventions/search-on-treaties/-/conventions/treaty/189/signatures?p_auth=YLVfaZur (13. Januar 2016).

20 Siehe im Dokument «Cyberlaw All 2 – 2014» unter A. III. 5 d) und 6.

3.1.2.3. Absage an strikte «Trennungsthesen»

Ein Beispiel für den Versuch beide Räume getrennt rechtlich regeln zu wollen, ist der jüngste Vorschlag des deutschen Bundesministers der Justiz und für Verbraucherschutz Maas für «Unsere digitalen Grundrechte».[21] Gegen eine Trennung von Cyber- und Realworldlaw sprechen die Vielzahl von cross-border Sachverhalten (eigene Terminologie) und die Prozesse *digitaler Transformation des Realen und realer Transformation des Digitalen* (Beispiele werden für den IRIS-Vortrag angeboten). Von zentraler Bedeutung ist das Additions- und/oder Substraktionsergebnis der Verwirklichung von Rechten auf Freiheit wie Schutz in beiden Räumen – das ***Outcome***. Nach den (hier unterstellten) Gemeinsamkeiten sollen auch Unterschiede zur Diskussion gestellt werden.

3.2. Unterschiede von Review und Abstract – we agree to (dis)agree

Credo ist das alte Motto «fortiter in re, suaviter in modo, constanter in se»[22] mit dem auch die Unterschiede Inspirations- und Sophistikationspotenzial haben.

3.2.1. Ge(recht)igkeit und die Konzentration auf das (Recht-)«Staats»prinzip

Der Cyberspace bietet erstmals den Raum und die Chance für die Bildung einer globalen/internationalen öffentlichen Meinung wie auch der Entwicklung globaler/internationaler digitaler Persönlichkeiten. Der Blick zurück vor allem auf traditionelle Printmedien (Parallelitätsthese), wie auch die pauschale Zugrundelegung einer *einzigen* Rechtsordnung wie -tradition sind evident nicht zielführend. Vorhersehbar ist, dass sich Gerechtigkeitsvorstellungen aus vergangenen Zeiten wie einzelner Nationen einer so nie gekannten «globalen Konkurrenz» ausgesetzt sehen. Damit reduziert sich das «*Projektmanagement der Forschungsmatrix»* in Abweichung zum Review auf die Aufgabe «Recht» – bisweilen als Verkürzung von Ge(recht)igkeit. Und es gibt eine Vielzahl von Argumenten, die gegenwärtig (2016) für eine Konzentration auf rechts«staatliche» *Mindeststandards* streiten. Innovativ werden diese neuen Perspektiven für ein «altes» Prinzip in «...» gesetzt, um zum Ausdruck zu bringen, dass die Rechtsstaatsidee historisch und gegenwärtig zunächst durch Staaten entwickelt und verwirklicht wurde (anders als auf supranationaler Ebene mit Rechtspersönlichkeit ohne Staatscharakter). Ein Beispiel für die Herausforderungen bereits der Wahrung rechtsstaatlicher *Mindeststandards wie im Cyberspace komplementärer IT-Sicherheitsstandards* ist das Vorratsdaten«speicherungs»recht[23]. Dieses Szenario wird hier als Lernkapital für zukünftige Forschungen geschildert – aus deutscher Sicht als *eine in Qualität und Quantität bisher ungekannte Erfahrung mit (inter)nationaler Rechtswidrigkeit:*

3.2.2. Herausforderung der Einhaltung rechtsstaatlicher «Mindeststandards» im Cyberlaw

Die Trias «Freiheit, Sicherheit und Recht» ist uns auch aus dem Unionsrecht bekannt (Art. 67 Abs. 1 AEUV, Art. 6 EU-Grundrechtecharta). Zur Gestaltungsaufgabe für und Bedeutung von Recht für Freiheit und Sicherheit rekurriert das Abstract auf Kant[24] statt – insbesondere in einer globalen Betrachtung – auf eine unvorstellbare Vielzahl von Rechtsquellen. In Bezug auf ein Kernthema des Cyberlaw – das Vorratsdaten«speiche-

---

21 Maas, Unsere digitalen Grundrechte, DIE ZEIT Nr. 50 vom 10. Dezember 2015, S. 9.

22 Siehe etwa der deutsche Philologenverband in einem Nachruf. Abrufbar unter: http://www.dphv.de/aktuell/archiv/news-archiv-liste/article/dphv-ehrenvorsitzender-bernhard-fluck-ueberraschend-verstorben.html (19. Januar 2016).

23 «Speicherung» wird deshalb in «…» gesetzt, weil es sich um die Erhebung, Speicherung, Übermittlung und ggf. Nutzung («ESÜN») von Telekommunikationsverbindungsdaten handelt (vgl. auch § 3 Abs. 3 ff. BDSG); Schmid, Die Vorratsdatenspeicherungsentscheidung des Bundesverfassungsgerichts – Eckpfeiler für eine Charta des (internationalen) (IT-)Sicherheitsrechts?», Vortrag im Rahmen der 2. SIRA Conference Series, München, 26.–27. Mai 2011 im Rahmen des BMBF-geförderten Projekts «Sicherheit im öffentlichen Raum – SIRA», Folie 14, unter http://www.cylaw.tu-darmstadt.de/media/jus4/publikationen/vortraege/2SIRA_Conference_Series_2011_05_25_EI_SO_VS_Version_28112012.pdf (19. Januar 2016).

24 Aus Platzsparsamkeit wird für Zitate auf das Dokument «Cyberlaw All 2 – 2014», dortige Fn. 27 verwiesen.

rungs»recht – ist freilich in Rückblick auf 2006 festzuhalten: Fast ein Jahrzehnt seit Erlass der europäischen Richtlinie[25] ist vergangen; die BRD konnte die Richtlinie im ersten Anlauf nicht nachhaltig umsetzen (Nichtigerklärung durch das BVerfG in 2010), die Richtlinie selbst, die in allen anderen Mitgliedstaaten umgesetzt wurde, ist vom EuGH in 2014 für ungültig erklärt worden.[26] Damit ist zur Kenntnis zu nehmen, dass nicht nur 27 Mitgliedstaaten eine rechtswidrige Richtlinie umgesetzt haben bzw. umzusetzen suchten, sondern auch die Kommission den letzten säumigen Mitgliedstaat (die BRD) mit einem Vertragsverletzungsverfahren (Art. 258 ff. AEUV) zur Umsetzung einer (später vom EuGH für rechtswidrig erachteten) Richtlinie verpflichten wollte. Dieser «rechtsrealistische» Befund zum Cyberlaw aus deutscher Perspektive (in 2016) motiviert zu selektiver Demut: falls es dem Recht gelingen sollte, den Cyberspace zu einer lebenswerten Cyberworld zu machen, erfolgt dies *mit der Beschränkung auf Mindeststandards und dem Eingeständnis von Selektion statt Universalität.* Und: Diese neue Qualität an internationaler («Umsetzung» in den Mitgliedstaaten) und europäischer Rechtswidrigkeit (der Richtlinie) widerspricht dem Qualitätsmerkmal «Nachhaltigkeit».

Art. 20a GG betont für den Umweltschutz die Idee der Nachhaltigkeit («in Verantwortung für die künftigen Generationen»). Rechtswidrige Daten«organisationen» bergen auch dann Risiken für nachfolgende Generationen, wenn die Löschung gerichtlich angeordnet wurde.[27] Gerade in der Gegenwart geht es im Kontext von Informationstechnologierecht um die Herausforderung der «(*Generationen*-)ge(*recht*)igk(*e)*it»[28] – Rechtsgedanke von Art. 20a GG. (Rechtlich) Defizitäre «Datenorganisationen» der Gegenwart drohen zu ewigen Freiheitsnachteilen für jüngere und nachfolgende Generationen zu werden («These data keep on giving» – eigenes Motto].[29] Mit dieser Schilderung eines «Lernkapitals» aus negativen Erfahrungen will sich der Beitrag indes nicht begnügen, sondern 13 Kernherausforderungen des Cyberlaw benennen.

4. Forschungsmatrix: Vorschlag von «13 Basics»

Grundsätzlich ist festzuhalten, dass in der Vergangenheit wie in der Gegenwart, in der Rechtswissenschaft wie in der politischen Praxis, die Idee verbreitet war, Agenden für das Cyberlaw vorzuschlagen. Ein Beispiel aus der Vergangenheit sind die «Sieben Goldene[n] Regeln des Datenschutzes» von Bizer[30]. Ein Beispiel aus der Gegenwart (Ende 2015) ist der – ebenfalls 13 Artikel umfassende – Katalog «digitaler Grundrechte» des Bundesministers der Justiz und für Verbraucherschutz Maas.[31] Auch der noch nicht abgeschlossene Prozess einer unionsrechtlichen Datenschutzgrundverordnung auf der einen und einer sektorspezifischen Datenschutzrichtlinie[32] auf der anderen Seite setzt eine ((rechts)wissenschaftliche) Agenda für grundsätzliche

[25] RL 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 2006/105, 54.

[26] Aus Platzsparsamkeit wird für Rechtsprechungsnachweise auf das Dokument «Cyberlaw All 2 – 2014», dortige Fn. 16 verwiesen.

[27] BVerfG 2. März 2010, 1 BvR 256/08 u.a. Urteilstenor zu 3.: «[…] gespeicherten Telekommunikationsverkehrsdaten sind unverzüglich zu löschen. Sie dürfen nicht an die ersuchenden Stellen übermittelt werden.»

[28] Mit dieser sehr ungewöhnlichen Klammergliederung des Begriffs «Generationengerechtigkeit» soll auf eine der in den Basics geforderte Nachhaltigkeitsanforderung aufmerksam gemacht werden. Im Cyberlaw wird es nicht «nur» um die Diskussion von Staatszielen im Interesse zukünftiger Generationen gehen, sondern um deren Rechte. Beispiele sind etwa Gen-Daten«organisationen», die die Menschenwürde und Unversehrtheit (E-Health-Anwendungen) zukünftiger Menschen unmittelbar berühren.

[29] Siehe im Dokument «Cyberlaw All 2 – 2014».

[30] DuD 5/2007, S. 350–356. Siehe auch zur «Digitalen Agenda der EU» unter http://ec.europa.eu/digital-agenda/en (5. Februar 2016).

[31] Siehe Fn. 21.

[32] Die europäische Datenschutzreform besteht im Wesentlichen aus der Grundverordnung und einer Richtlinie. Seit Dezember 2015 ist der «Trilog» zwischen Europäischem Parlament, Ministerrat und Europäischer Kommission abgeschlossen; mit der Verabschiedung wird für das erste Halbjahr 2016 gerechnet, siehe Pressemitteilung des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE) vom 15. Dezember 2015: «Data protection package: «Parliament and Council now close to a deal». Abrufbar unter: http://www.europarl.europa.eu/news/de/news-room/20151215IPR07597/Data-protection-package-Parliament-and-Council-now-close-to-a-deal (13. Januar 2016). Siehe zudem die LIBE-Pressemitteilungen vom 17. Dezember2015 zur «Datenschutzgrundverordnung»: «EU-Datenschutzreform: Mehr Rechte für Europas Internetnutzer». Abrufbar unter http://www.europarl.

Positionierungen nach dem Motto «be prepared» voraus. Die Idee ist, dass eine vernetzte Forschungs- und Erfahrungsaudience – hier die IRIS 2016 – Perspektiven entwickeln, Analysen erstellen, Technologierechtsvergleiche durchführen, die Voraussagen für die Zukunft wie Positionierungsangebote gegenüber zukünftigen Herausforderungen enthalten und so ein «Forschungsdesign» entwickeln kann. Im Traditional Law ist diese Bedeutung der Rechtswissenschaftler etwa in Art. 38 Abs. 1 lit. d) IGH-Statut[33] in retrospektiver – und gerade nicht wie hier vorgeschlagen *in proaktiver – Funktion* erwähnt. Ein erster – und hoffentlich nicht der letzte – Schritt sind 13 Basics, die in dieser Papierveröffentlichung nur genannt und in «Cyberlaw All 2 – 2014» erläutert werden:

13 Basics

I. Cyberspace als neue Dimension des Seins
II. Cyberlaw macht den Cyberspace zur Cyberworld
III. Status Quo: Übergangszeit (Transition Period)
IV. Malfunction Management (MaMa)
V. GVK-Formel (Globale Vernetzung und Konkurrenz)
VI. Nachhaltigkeit
VII. «Informationstechnologierechtlicher Kreislaufgedanke»
VIII. Automatisierung und Mensch-Maschine-Interaktion
IX. IT-Sicherheit(srecht) als Äquivalent zum Rechtsstaatsprinzip im Traditional Law der Realworld
X. Neue Terminologieanstrengungen und neue Grundrechte – zum Recht auf «Flüchtigkeit»
XI. Neue Wahrheitsideen?
XII. Diskursbrücken
XIII. Tempelarchitektur für die Herausforderungen der Versicherheitlichung

Der Diskurs über die Reihenfolge, «Vollständigkeit» wie die Wertung der Herausforderungen ist Grund, zur IRIS 2016 zu kommen.

europa.eu/news/de/news-room/20151217IPR08112/EU-Datenschutzreform-Mehr-Rechte-f%C3%BCr-Europas-Internetnutzer (13. Januar 2016) sowie zur «Datenschutzrichtlinie für Polizei und Justiz»: «New data protection standards to ensure smooth police co-operation in the EU». Abrufbar unter http://www.europarl.europa.eu/news/de/news-room/20151217IPR08122/New-data-protection-standards-to-ensure-smooth-police-cooperation-in-the-EU (13. Januar 2016).

33 «Der Gerichtshof, dessen Aufgabe es ist, die ihm unterbreiteten Streitigkeiten nach dem Völkerrecht zu entscheiden, wendet an […] richterliche Entscheidungen *und die Lehrmeinung der fähigsten Völkerrechtler der verschiedenen Nationen* als Hilfsmittel zur Feststellung von Rechtsnormen.» Statut des Internationalen Gerichtshofs vom 26. Juni 1945, BGBl. 1973 II S. 505 (Hervorhebung der Autorin).