



Viola Schmid: „Weltrecht² Entourage Documents“

→ here: A STANDARD FOR A UNIVERSAL (TECHNOLOGY) LAW LECTURE
IN CYBERSPACE AND (TECHNOLOGY) LAW (2018)

PRELIMINARY ANNOTATIONS TO CLUSTER WELTRECHT² & THE CLYAW-REPORT SERIES (STATUS IN NOVEMBER 2022):

“**Weltrecht²**” addresses the process of digitalization and the economization of state and private (information) value chains since the inception of cyberspace as the 5th dimension of being. The designation “Weltrecht²” has been chosen for a [World Congress of Constitutional Law \(WCCL\)](#) with the conference title “Constitutional Transformations” to be held in South Africa, Johannesburg from December 5 to 9, 2022. One workshop topic on the agenda concerns “Constitutional law scholarship and constitutional transformation: actors and influences.” The submission of a 10,000-word paper titled “Weltrecht² - Multidisciplinary constitutional law scholarship from Germany and the EU” is imminent. The present “**Entourage Document**” is meant to complement the paper and will be referenced in it. The present CyLaw Report XXXXI forms part of the cluster Weltrecht² and builds **directly**

- onto [Cylaw Report XXXVI: Der kleinste gemeinsame Nenner - 13 Basics zum Cyberlaw? \(The smallest common denominator – 13 basics for Cyberlaw?\) \[“Cyberlaw All 2 - 2014”\]](#) (2016) in **German Language [GL]**, as well as
- the concomitant publication [Forschungsmatrix für eine globale Cyberlaw-Agenda – „Cyberlaw All 4 – 2016“](#), (research matrix for a global cyberlaw agenda - „Cyberlaw All 4 – 2016) in: Schweighofer et al. (Ed.), Networks – Proceedings of the 19. International Legal Informatics Symposium (IRIS 2016), p. 441 – 448 also in German language [GL].

Content Innovation regarding this Cylaw Report: In this Cylaw Report are published for the first time and in this format

- the draft of a **Teaching Standard (ST)**: „A Universal **STANDARD** for a (Technology) Law Lecture“, which seeks to pave the way to a new scientific discipline – **CYBER-SCIENCE (CySci)**. This “**STANDARD**” was first presented at the Internet Work in Progress conferences in 2017 and 2018. In this way, the cyber(law) scientific research system opens up on the level of teaching **and** learning;
- the **GLOBALMATRIX**;

- the Visual Legal Design of Weltrecht² (GALAXY metaphor) and
- the Weltrecht² TAXONOMY as „Entourage Document“ in preparation of the paper to be submitted for the World Congress of Constitutional Law.
- In addition, several articles published in the course of the past two decades will, for the first time, be presented in form of a „STEP LADDER“ chronology to exhibit the developing work on CYBERSCIENCE (and in Cyberlaw and AILAW) by an author with the veniae legendi (authority) to teach Public, European and Energy law („Her-story“).

Mapping (Cartography) of the Cylaw Report Series: The Cylaw Report I commenced in 2008, discussing the „Evergreen“ topic of the Telecommunication Traffic Data Retention and Usage Law (TTDL) – a challenge for the German and European law that even in 2022 has not yet been overcome (European Court of Justice, Judgement of the court (Grand Chamber), Sept. 20, 2022 – C-793/19, C-794/19 – ECLI:EU:C:2022:702). The challenge has not been met due to the lack of a legitimate and applicable German Telecommunication Traffic Data Retention and Usage Law. The Cylaw Reports I – XXXVI have been continuously dated (time management) and have so far been published in a consistent sequence. However, Cylaw Report XXXXI interrupts this sequence and leaves space for Cylaw Reports XXXVII to XXXX, all of which are under preparation (Nov. 2022).

Table of contents

Part 1: Entourage Documents & „Weltrecht²“	9
A. Title: “Weltrecht ² ”	9
B. First Abstract: Weltrecht ² - as submitted in June 2022 in 500-words.....	9
C. Excerpt from Second Abstract: Weltrecht ² - in November 2022 in 820-words	11
D. Pedigree of (working) documents – especially “Entourage Documents”	15
I. Backbone Documents	15
1. „Cylaw-Report XXXX „Weltrecht ² “ [...] Organisational Chart (Organigram) (2022)“	15
2. TAXONOMY – Visual Legal Design	15
II. This Cylaw-Report XXXXI as „Entourage Document“	17
III. Pedigree: "Cyberlaw All" & "Cyberlaw Special" Publications	17
1. “Cyberlaw All”	17
2. “Cyberlaw Special”	18

E.	Timeline of the “Weltrecht^2” Project: Development Phases & STEP LADDER	18
I.	Different Languages – GL & EL	18
II.	Multimediality and Equivalence of Publications in Prose & PPT forms	19
III.	List of Abbreviations (Acronymology) for the “Herstory Step ladder”	20
IV.	“Weltrecht^2” as Visual Legal Design: Development Phases as a “STEP LADDER”	21
V.	Varying Degrees of Maturity.....	22
F.	Acknowledgments.....	22
G.	A STANDARD FOR A UNIVERSAL (TECHNOLOGY) LAW LECTURE (March 24, 2018)	22
I.	Internet Law Works in Progress Conference	22
II.	Editorial Amendments in 2022 by Viola Schmid	22
III.	Editorial Amendments in 2022 by Georg Gesk.....	23
IV.	Temporal & Local Context.....	23
1.	EL – USA.....	23
2.	GL – BRD	23
V.	Iterations and Self-Critical Concretization.....	24
1.	Trans-, Multi- and Pluri- Disciplinarity.....	24
2.	Feedback.....	24
Part 2:	What (I)? Standardization for Global Cyberteaching in Order to Better the World	24
A.	What, How, Why, Who, Where and Intended Impact as well as SWOT-Analysis ..	24
B.	Draft Status No. 1	26
I.	Multimedia Ambition.....	26
II.	Partial Mono- and Bilingualism with the Aim of Trilingualism	26
III.	Original and Own Terminology for This Project: “Securitization”	26
IV.	Time Management and Living Documents	27
V.	(Legal) Sustainability through the Choice of Challenges and “Shepardizing”	28
VI.	Citation and Detection Strategy – “Blanket Strategy”	29
C.	Global Cyberteaching for a World Connected by the Technology of Cyberspace: Adding a Fifth Dimension of Being	30
I.	“We” all Agree – some Talking Points?	31
II.	“We” – with a Focus on Three Legal Traditions, Systems, and Languages	32

III.	Academic Open Innovation (AOI) as Crowd Sourcing	32
IV.	“Privacy by Design and Default” as a Model for “Legality by Design and Default”	33
Part 3:	Why and for What? The Challenges and Opportunities of a Global Legal Perspective with Ambitions of Standardization: The Road to a Better Future through Competing (Technology) Legislation	34
A.	May the Best Idea Win: How Arguments Compete.....	34
B.	Global Language Diversity as a Barrier to Consensus and a Challenge for Discourse.....	35
I.	Global Quantity of Languages: The United Nations as an Example	35
II.	Loss of Content through Language Diversity.....	35
III.	Loss of Content and Misunderstanding as a Consequence of Multilingualism: For example “Der Kampf ums Recht” (see Abstract)	36
IV.	Strategy: Focus on German, English and Chinese – <i>pars pro toto</i> (a Part for the Whole)	37
C.	“Fighting Words” before “Weaponization” (<i>prima et ultima ratio</i>).....	38
V.	<i>Prima ratio</i>	38
VI.	Should we Revisit Ihering in Cyberspace?	38
C.	A Chance for a Better Future through Comparative Technology Law (“The Quest of Truth” and “Shared Academia”) – Traffic Communication Data Law	39
I.	Chance for a Better Future through Comparative Technology Law (“The Quest of Truth” and “Shared Academia”).....	39
II.	A Quest of Truth, e.g. German-European Telecommunication Traffic Data Retention Law	40
III.	A Quest of Truth, f.ex. United States: The Declassification and Dissemination of Information Following the “Nunes Memo (I)”	41
Part 4:	What (II)? A Universal (Technology) Law Lecture Fulfilling a Global Agenda for Cyberlaw (2015).....	42
A.	Universal.....	42
B.	(Technology) Law and Especially Cyberlaw	43
I.	Technology is the Starting Point and the Starter of the Law Lecture - and not Mankind	43

II.	Cyberlaw as a Proponent of (Technology) Law	44
C.	“Law” in a Questionnaire	44
D.	Lecture – Syllabus and Agenda of Priorities in March and May 2017 (Santa Clara and Darmstadt)	45
E.	The 13 Basics of a (Global) Agenda for Cyberlaw (the Perspective of a European-German Cyberlaw Professor – a Text Dating from 2015, Published in 2016	52
I.	Pioneering in Cyberspace – an Agenda for Cyberlaw	52
II.	13 Basics in a Nutshell.....	53
III.	“Law on Content of Expression” and “Law on Technology of Expression“ in its Haziness in Cyberspace	54
IV.	13 Basics Illustrated (2015) and not Updated as a Way toward Cyberscience (2018)	54
1.	GNC Formula (Global Networking and Competition) on the one Side, Automation and Man-Machine Interaction on the other.....	55
2.	New and/or Other Ideas about Freedom of Expression, Protection of Personality and Privacy and New Conceptions of Truth	57
3.	Imminent “Clash of Civilizations?” (The France: “Charlie Hebdo” and USA: “The Interview/Sony” Scenarios of 2015)	57
4.	The Necessity of Building (Global) Discourse Bridges and the Legal Establishment of (Global) Minimum Standards	57
5.	Only Cyberlaw Makes Cyberspace a Cyberworld.....	58
6.	Analysis: “Securitization” of Cyberspace and the Realworld as Unprecedented Challenges in the History of Humankind	59
a)	Cyberspace Immediately Affects Everyone.....	59
b)	2015 ff.: A Hybrid World Paralleling Cyberspace and the Realworld	59
7.	The Status Quo is the Transition Period.....	60
8.	Malfunction Management (MaMa).....	60
9.	(IT) Security (Law) as an Equivalent to the Rule-of-Law Principle in the Traditional Law of the Realworld, and the Challenges for IT Security	61
a)	No Security without IT Security = (IT) Security.....	61
b)	(IT) Security as a Prerequisite for the Organisation of Cyberspace and the “Principle of IT Security” as a Component of German Constitutional Law	61
c)	(IT) Security Level Must be Determined as an Accessory to the Legal Application – and not (just) Economically.....	62

d)	Cyberattacks as Technological Enforcement Strategies (The Interview/Sony Scenario)	62
10.	Jurisprudential and Legal-Political Strategies (New Efforts are Necessary)	63
a)	New/Old Task for Global Jurisprudence? – The Question of Experts (Art. 38 Para. 1 Lit. d ICJ-Statute).....	63
b)	New Concepts of Protection (for Instance Privacy Impact Assessments (PIA)) – The Question of Methods	64
c)	PII in a Global Perspective – The Question of Definition.....	65
d)	A New Relationship with the Truth? – The Question of Content.....	65
aa)	Statements without (Identifiable) Author According to German Law	65
bb)	“Truth with Expiration Date” According to Union Law and Rights to Ephemerality, Net-Working and De-Networking.....	66
11.	“Legal Information Technology Circular Thought Process”	67
12.	Pilot: (Global) Comparative Technology Law in “E-Justice” – a Temple Architecture for Securitization.....	67
13.	Sustainability through Cyberlaw in 2015 ff. in its Significance for the Cloud with Respect to Content and Technology	70
F.	Standard for a Law Lecture as an Instrument for Fulfilling Basic No. 4.....	71
I.	Navigator: Global Agenda for Cyberlaw	72
II.	Audience and Glossary	72
III.	Hybrid Strategy in the Realworld und Cyberspace	72
IV.	Time frame.....	72
V.	Content (I) – “Survival Guide”, “Basics”, “GoCore! Scenarios“ and “Outcome”	72
VI.	Content (II) – the Modules.....	74
1.	Module: “Survival Guide” – LAW and not Philosophy, Political Science, Sociology, Economics etc.	74
2.	Module “Basics 1” – Robots and Cyborgs and the Right of Humans	74
3.	Module “Basics 2” – Reaching out for a Global and Universal Perspective	75
4.	Module “Basics 3” – Language as a Strategy for a Global Lecture Standardization Effort – here: “Rechtsanwalt”	75
5.	Module “Basics 4” – “Lexonomics” – How do Financial Resources and Efficiency and Efficacy Principles Influence the System.....	76
6.	Module “Basics 5” – National constitutional reserves for (inter)national law in globalized (and digitized) societies	76
7.	Module “Basics 6” – Electricity as the Lifeblood/ Fuel for Cyberspace.....	77

8.	Double-Module “GoCore!” 1 – Telecommunication Traffic Data Retention And Usage Law	77
9.	Module “GoCore! 2” – Ramifications of Virtual Currencies on Governance	77
10.	Module “GoCore! 3” – “Who Owns the Sky?” – Drone Law.....	77
11.	Module “GoCore! 4” – “Interactive Toys”.....	77
12.	Module “GoCore! 5” – Legal Technology, TechJustice and “Technology Transforms Legal Markets” (Own Terminology).....	78
13.	Module – Terroir	78
14.	Module: Outcome and ROI	78
Part 5:	Who? German Initiative	79
A.	Prof. Dr. Viola Schmid LL.M (Harvard)	79
B.	Prof. Dr. (NTU) Georg Gesk – Relation to Chinese Cyberlaw and Development of Curricula	80
C.	Dr. Christoph Merkelbach	81
D.	Crowd Research Sourcing and Funding in Order to Organize International Competence as well as Interdisciplinary Knowledge Management for CYBERSCIENCE.....	81
Part 6:	Reaching out to Europe from Germany – Module “GoCore!” 1.....	82
A.	An Area of Freedom, Security and Justice (Art. 67 TFEU)	82
B.	Supremacy of European Law– 28 Member States and 500 Million People (2018)	83
C.	National Identity Clause in the German Constitution (Art. 23 Abs. 1 S. 3 GG, Art. 73 Abs. 3 GG).....	83
D.	Positive Obligation for Privacy of Telecommunication in German Constitution Law (Art. 10 Basic Law) Pertaining to European Union and International Law.....	85
I.	Precautionary Storage of Telecommunication Traffic Data as a Restriction of Privacy of Telecommunication	85
II.	Positive Obligation of the German Government to Preserve the Constitutional Identity Including the Privacy of (German) Citizens around the World	86

E.	Legal Innovation in German and European Data Protection Law in 2018: New Governance for the Raw Material Data	87
I.	Time & Transition Management: German and European Data Protection Law in Relation to the First Power	88
1.	Terminology: “Deadline” and “Date of Coming into Effect”	88
2.	Deadlines and Dates of Coming into Effect – May 6 and 25, 2018, May 6, 2023, and May 6, 2026.....	88
II.	If You Want Peace, Prepare for War (<i>Qui desiderat pacem, bellum praeparat</i>): The Near Future of a Data Protection Conflict between the EU and the US	89
Part 7:	Reaching out to the US.....	89
Part 8:	Reaching out to China – Georg Gesk und Christoph Merkelbach.....	90
A.	Reaching out to China – Insights by Georg Gesk.....	90
I.	Supremacy of Supra-Individual Actors (Natural paragraph 13, Preamble, Constitution 1982).....	90
II.	Supremacy of Chinese Law – 1.3+ Billion People (2018).....	91
III.	Priority of Public Law vs. Civil Law vs. Industry Self-Regulation	92
IV.	Consequence: Intranet vs. Internet, or: Restrictions of the Chinese Cyberspace ..	94
V.	Right to Privacy vs. Corporate Interest in Big Data vs. State Interest in Big Data ..	95
VI.	Consequence: Corporate Mining and Processing of Big Data as a Common Asset in Public law	100
VII.	Quest of Truth, e.g. PR China: Transparency as Precondition of Responsibility and therefore as Necessary Condition for Truth.....	101
B.	Let’s talk about Cyberlaw – Insights by Christoph Merkelbach.....	103
Part 9:	Summing up	107
Part 10:	Appendix – Further in-depth Information and Citations of International, European Union and German law	108
A.	International Law – Statute of the International Court of Justice.....	109
B.	European Union Law	109
I.	Primary Law – Consolidated Version of the Treaty on European Union	109
II.	Secondary Law	110

1.	General Data Protection Regulation.....	110
2.	Data Protection Directive	111
3.	Regulation on Privacy and Electronic Communications (de lege ferenda).....	112
a)	Council of the European Union – Proposal 12/5/17 – Application Date in Brackets	112
b)	European Commission – Proposal 1/10/17.....	112
C.	German Law	113
I.	Primary Law – Basic Law for the Federal Republic of Germany (German Constitution; Grundgesetz, GG).....	113
II.	Secondary Law	115
1.	Federal Data Protection Act (until 5/25/2018; Bundesdatenschutzgesetz, BDSG)	115
2.	Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG)	116
3.	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU.....	116
4.	Code of Civil Procedure (Zivilprozessordnung, ZPO).....	117
5.	Code of Administrative Court Procedure (Verwaltungsgerichtsordnung, VwGO).118	

Part 1: Entourage Documents & „Weltrecht^2“

A. Title: “Weltrecht^2”

Since June 2022, the work of 20 years of research in and teaching(s) on innovation and innovative law has been subsumed under the title “Weltrecht^2” (Global Law^2). The designation “Weltrecht^2” has been chosen for a World Congress of Constitutional Law (WCCL) with the conference title "Constitutional Transformations" to be held in South Africa, Johannesburg from December 5 to 9, 2022. One topic on the workshop agenda concerns "Constitutional law scholarship and constitutional transformation: actors and influences"¹.

B. First Abstract: Weltrecht^2 - as submitted in June 2022 in 500-words

The project „Weltrecht^2“ was first outlined in an abstract submitted to the WCCL in June 2022 as follows:

¹ Workshop 27, <https://wccl.co.za/workshops/> (last accessed Oct. 20, 2022).

“Weltrecht^2”

Multidisciplinary constitutional law scholarship from Germany and the EU

Cyberspace, which has been in existence for 20 years, offers us undreamed-of opportunities for ubiquity and internationality in addition to real-time and long-distance communication. It deserves the best possible backing in research and teaching. The occasionally inherent non-transparency of technologies across the entire value chain (from programming to usability) of algorithms fundamentally changes science-based constitutional law research and calls for “Weltrecht^2”. “Weltrecht^2” responds to the plenary 3 title “Constitutionalism in the era of [...] the Fourth Industrial Revolution”. It is about strategies of multidisciplinary research and teaching in technology-related (constitutional) law intended to help tackle current challenges regarding electronization, digitalization, automation and autonomization (EDAA). Thus, “Weltrecht^2” realizes a discourse between the legal, engineering and economic sciences (CYBERLEXONOMICS). The German terminology “Weltrecht^2” is a new venue to a “CYBERWORLD”, which suggests

- the world of law (i.e., consisting of at a minimum all legal systems of the members of the United Nations) on the one hand and
- how to draft and/or cover all challenges of a technology-based world that is ready and available anytime and anywhere in a legal science-based (constitutional) manner on the other hand.

In other words, it is about the “world of law” for a “technology-based world” that constitutional law can withstand. “Weltrecht^2” includes:

- an invitation to take a global perspective of law (GLOBAL MATRIX);
- an initial GLOBAL CYBERLAW AGENDA;
- a draft of a TEACHING STANDARD and
- an updating and archiving strategy (Cyberlaw TAXONOMY) for all “materials”.

“Weltrecht^2” aligns with the mission of the conference, “the role of constitution[s] in responding to [...] the challenges of the digital revolution and artificial intelligence”. From a German-European legal perspective, “Weltrecht^2” methodically details how this challenge can be handled analytically, strategically and creatively. Example: It is not limited to a report (public scholarly reviews) on German-European constitutional controversies in the context of telecommunication traffic data retention and usage laws. On the contrary, it addresses this experience with unlawfulness from 2005 to 2022—documented by rulings of German and European courts—within a universal teaching standard for technology-related law.

The objectives of “Weltrecht^2” could not be more ambitious. Even the invitation to the conference emphasizes: In a digitized world, “democratic deficits” and “the expanding power of private corporations” are a reality. Therefore, cyber research and cyber education are the first building blocks for a law and technology-based world firmly entrenched in the “rule of law” and the “principle of IT security”. If Atlas were able to shoulder this load using the “Weltrecht^2” project, then

- better investment decisions* for technology could be made;
- assessment lists** could be created that promote innovation and protect legal interests; and

- opaque technologies could be subjected globally to effectiveness and efficiency tests.

Hence, there is a vital interest in gaining and sharing knowledge and experience globally. With “Weltrecht²”, constitutional law is to become a component of a multidisciplinary cyberscience (based on cyberlaw). Get ready for the already impending fifth industrial revolution^{***}!

References will be provided in the conference paper

*High-Level Expert Group on Artificial Intelligence (AI HLEG), Policy and Investment Recommendations for Trustworthy AI, 26th June 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343 (01.06.2022).

**AI HLEG, The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment, July 17, 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342

***European Commission, Directorate-General for Research and Innovation, Industry 5.0: A Transformative Vision for Europe, ESIR Policy Brief No. 3, 01/2022, <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/38a2fa08-728e-11ec-9136-01aa75ed71a1> (June 1, 2022).

This abstract forms the basis for the submission of a 10,000 word research “paper” and shall be initially published in this context for further clarification:

C. Excerpt from Second Abstract: Weltrecht² - in November 2022 in 820-words

Abstract: “Weltrecht²”

Multidisciplinary constitutional law scholarship from Germany and the EU in 10,000 words in November 2022

There are two (r)evolutions that trigger “Weltrecht²” [GLOBAL LAW²]. On the one hand, the transformation of the REALWORLD into a technology-based HYBRIDWORLD (REALWORLD+CYBERSPACE) preparing us for an AI-enriched CYBERWORLD. On the other hand, the opportunities that such a data-driven world holds for coping, for example, with our common global challenge - climate change adaptation & mitigation (**CCAM**). Thus, technology law should ultimately serve to mitigate the technology-induced perils - climate change - that threaten the survival of humankind. This end should not justify the loss of minimum standards for freedom, security and justice (Art. 67 Treaty on the Functioning of the European Union).

Within Weltrecht² a new scientific value chain has been formed, which will herein be called CYBERSCIENCE [Cyber(rechts)wissenschaft] - and may elsewhere be named “complexity science”. In 2017, **CYBERSCIENCE** was defined as the “process of creating knowledge that is essential in the transition period from the ‘real’ to the ‘digital’ and the ‘digital’ to the ‘real’”. Goal is to preclude any non-transparent and (un)intended ‘value losses’². In 2022, **the**

² “The End of Lawyers“...? presentation at the International Legal Informatics Symposium (IRIS 2017) with the topic „20 years of IRIS – Trends and Communities of Legal Informatics“, Feb. 23 - 25, 2017, University of Salzburg, Austria

above CYBERSCIENCE definition is adjusted to “a new multidisciplinary science originating in law scholarship, utilizing “the world of law” for a “legally coded as well as by lawfulness-driven world” (own terminology). The need to transform in the face of climate and technological change is being increasingly recognized. The German Federal Constitutional Court (GFCC) states: “[...] especially considering that such innovations will have to be introduced on a massive scale in nearly all areas of economic production and in practically every aspect of how people live. Given the extent of the requisite socio-technological transformation [...]”³. How technological (r)evolution may result in the (r)evolution of the legal system is addressed by a 52-member Independent High Level Expert Group for Artificial Intelligence (AI HLEG) set up by the European Commission:

„9. Adopt a risk-based governance approach to AI and ensure an appropriate regulatory framework

Ensuring **Trustworthy AI** requires an **appropriate governance and regulatory framework**. We advocate [...]to safeguard AI that is lawful, ethical and robust, and fully aligned with fundamental rights. **A comprehensive mapping of relevant EU laws** should be undertaken so as to assess the extent **to which these laws are still fit for purpose in an AI-driven world. In addition, new legal measures and governance mechanisms may need to be put in place to ensure adequate protection from adverse impacts as well as enabling proper enforcement and oversight, without stifling beneficial innovation.**”⁴

Likewise, the World Congress of Constitutional Law in 2022 addresses this challenge with its title „Constitutional Transformations“. Concomitantly, “Weltrecht²” explores how and to what extent legal systems can become drivers for a technology-based world in order to master the challenges of such a technology based world. This global perspective is an essential requirement because a technology-based world can only be grasped, shaped and written in such a way. Traditional distinctions of scope and applicability of state law/national law are acknowledged as much as they are rejected for their limiting quality for a science and teaching design in CYBERSCIENCE. This global perspective is visualized and operationalized for research and teaching in the below presented GLOBALMATRIX⁵:

The project with the ambition quest of truth since 1990: Schmid, Werbung, Meinung, Cyberspace – Eine neue Perspektive auf Rechtswissenschaft, <http://www.cyberlexonomics.de/index.php/de/> (October 30, 2022).

³ BVerfG, Order of the First Senate of 24 March 2021 - 1 BvR 2656/18, para. 121, [ECLI:DE:BVerfG:2021:rs20210324.1bvr265618](https://www.bverfg.de/urteilsverzeichnis/2021/18/1803241bvr265618.html).

⁴ AI HLEG (Independent High Level Expert Group for Artificial Intelligence set up by the European Commission), Policy and Investment Recommendations for Trustworthy AI, 26.06.2019, (Acronym: “EGPaIRfTAI-I-2019”), p. 50, https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy_and-investment-recommendations.pdf (last accessed Sept. 28, 2022); citation with emphasis by the author.

⁵ This slide regarding the GLOBALMATRIX has been part of the author’s teachings since 2020. The slide is structured in a traditional manner along the separation of powers.

„Recht in einer Globalmatrix“

Demn., V. Schmid, in „Werbung, Meinung, Cyberspace

– Eine neue Perspektive auf (Rechts)Wissenschaft“, Springer



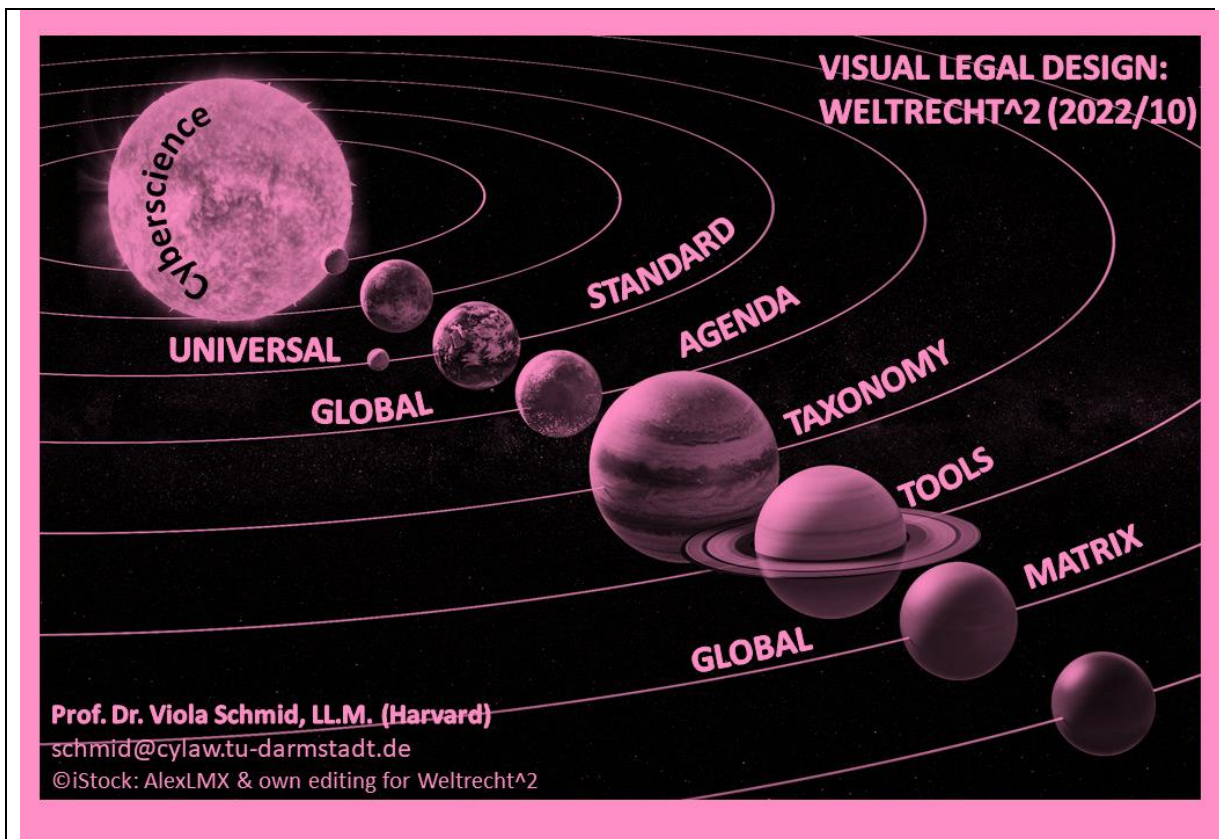
Law of the Federal Republic of Germany		European Union Law		International (Public) Law		Comparative Legal Analysis	
Legislative Power	Primary Law	Legislative Power	Primary Law	Legislative Power	Primary Law	Legislative Power	Primary Law
	Secondary Law		Secondary Law		Secondary Law		Secondary Law
	Tertiary Law		Tertiary Law		Tertiary Law		Tertiary Law
Federal	State						
Executive Power	Federal Level	Executive Power	Primary Level	Executive Power	Primary Level	Executive Power	Federal Level
	State Level		Secondary Level		Secondary Level		State Level
	Communal Level				Communal Level		Communal Level
Judicial Power	Primary Court	Judicial Power	Primary Court	Judicial Power	Primary Court	Judicial Power	Primary Court
	Secondary Court		Secondary Court		Secondary Court		Secondary Court
	Tertiary Court				Tertiary Court		Tertiary Court

27.05.2020 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 2



For this version of Weltrecht² (2022) we will complement the GLOBALMATRIX with the metaphor of a singular „academic galaxy“⁶. The visualization of such galaxy metaphor serves to illustrate the various orbits in “Weltrecht²”.

⁶ In further research, we will need to explore the existence of further (legal) galaxies. As illustration, see also „Overlapping galaxies VV 191“, NASA, ESA, CSA, Rogier Windhorst (ASU), William Keel (University of Alabama), Stuart Wyithe (University of Melbourne), JWST PEARLS Team, Alyssa Pagan (STScI), https://www.esa.int/ESA_Multimedia/Images/2022/10/Overlapping_galaxies_VV_191_Webb_and_Hubble_composite_image (last accessed Oct. 28, 2022). In clear opposition to a jurisprudential school of thought anchored in the belief: “You are on earth, there is no cure for that” already in Schmid, Veröffentlichung der Vereinigung der Deutschen Staatsrechtslehrer, Grenzüberschreitungen, VVDStRL 76, p.322.



A value chain of research and teaching(s) characterizes the exploration of such a new „science galaxy“ – especially of CYBERSCIENCE. CYBERSCIENCE is the sun around which the planets orbit. In addition to the GLOBALMATRIX, there are – to stay with the galaxy metaphor – four more planets. Within the framework of this contribution, the planets can only be given names and first explorational insights be shared. It initially is a standard of teaching(s), which also includes space law (UNIVERSAL STANDARD). This STANDARD planet was contoured in 2017/2018 and is reproduced in Cylaw-Report XXXXI (2022) → A STANDARD FOR A UNIVERSAL (TECHNOLOGY) LAW LECTURE IN CYBERSPACE AND (TECHNOLOGY) LAW (2018).⁷ The Teaching Standard serves as „proof of concept“ of a herein so-called “GLOBAL AGENDA OF CYBERLAW”, which was developed between 2014 and 2016 and has already been published.⁸ Since 2022, a Weltrecht^2 - TAXONOMY has been providing clarity on the value chain, consisting of research and teaching(s) for CYBERSCIENCE. A document⁹ delineating TOOLS („Essentials for Legal Work”) is currently under preparation and shall allow for international, cross and multidisciplinary collaboration by establishing good scientific practice.

⁷ Part 2 of this “Entourage Document”.

⁸ [GL] [Forschungsmatrix für eine globale Cyberlaw-Agenda – „Cyberlaw All 4 – 2016“](#), in: Schweighofer et al. (Ed.), Networks – Proceedings of the 19. International Legal Informatics Symposium (IRIS 2016), p. 441 – 448 (October 30, 2022); [CyLaw-Report XXXVI: Der kleinste gemeinsame Nenner - 13 Basics zum Cyberlaw? \[“Cyberlaw All 2 - 2014“\]](#), 2016 (November 11, 2022).

⁹ In preparation for publication: [GL] Cylaw-Report XXXVIII: (Qualitäts)Strategien der „akademischen Wertschöpfungskette“ für „WELTRECHT^2“ → TOOLS for Legal Work.

Summing up: “Weltrecht²” is an iterative and dynamic teaching, learning and research concept based on legal realism. “Inventory or stock research” [“Vorratsforschung”] for the legal design¹⁰ of an “AI-driven world”¹¹ is conducted. With the intention that humans, (human) law systems, societies and economies

- are not condemned to be driven by a technological (r)evolution and
- become competent as well as effective and efficient actors in the climate fight.

D. Pedigree of (working) documents – especially “Entourage Documents”

Over a period of 20 years of research and teaching, a wealth of documents has been created. An initial division into two parts is undertaken with the distinction of herewith called „Backbone Documents” and „Entourage Documents“ – or to use a corporeal metaphor the skeleton and the flesh of “Weltrecht²”.

I. Backbone Documents

“Backbone Documents” are such project documents that possess supporting functionality.

1. „Cylaw-Report XXXX „Weltrecht²“ [...] Organisational Chart (Organigram) (2022)“

A „Cylaw-Report XXXX „Weltrecht²“ – “Backbone Documents” → here: Organisational Chart (Organigram) (2022)“, is currently under preparation and will soon be published. This “Organigram” currently has – to stay with the corporeal metaphor skeletal function.

2. TAXONOMY – Visual Legal Design

A further document, created in 2022, concerns the structure of a taxonomy which visualizes the four “Weltrecht²” components: [GA, ST, GM, TOOLS]. This taxonomy is herewith presented for the first time and will be specified in the course of further publications:

¹⁰ [Explanation to the POP-Principle: “The POP principle can be applied to this value chain – the process of \(lifelong\) learning in the organisation \(of the research group\) creates „products“. These „products“ are then fed back into the process in an iterative cycle.”](#)

¹¹ AI HLEG (Independent High Level Expert Group for Artificial Intelligence set up by the European Commission), Policy and Investment Recommendations for Trustworthy AI, 26.06.2019, (Acronym: “EGPaIRfTAI-I-2019”), p. 49 , https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf (last accessed Sept. 28, 2022).

“Weltrecht²-Taxonomy”: “Taxing” “Global Agenda” (GA), “Lecture STANDARD” (ST) & TOOLS

Global Agenda for Cyberlaw– 13 Basics (GA)

- I. Cyberspace as a new Dimension of Being!
- II. Cyberlaw makes Cyberspace a Cyberworld
- III. Status Quo: Transition Period
- IV. Malfunction Management (MaMa)
- V. Global Networking and Competition – the GNC Formula
- VI. Sustainability
- VII. “Legal Information Technology Circular Thought Process”
- VIII. Automation and Human-Machine-Interaction (AILAW)
- IX. (IT) Security (Law) as an Equivalent to the Rule-of-Law Principle (ROBUSTNESS)
- X. New Terminologies and Basics Laws - “Right to Ephemerality”
- XI. New Conceptions of Truth?
- XII. Building (Global) Discourse Bridges and „STANDARD“
- XIII. Temple Architecture for the Challenges regarding an „Agenda of Securitization“ – E-Justice

„Proof of Concept“ of „13 Basics“ in the „STANDARD“

„Right to be forgotten“
Judgment of the Court of Justice of the EU, 13 May 2014, „Google Spain and Google“, C-131/12
Art. 17 EU-GDPR

„ephemerality“ ≠ „to be forgotten“

“SECURITIZATION”



Universal STANDARD for a (Technology) Law Lecture (ST)

15 Modules à 90 Min.

Module	Title	Content
1	“Survival Guide” & Table of Contents	LAW and not Philosophy, Political Science, Sociology, Economics etc. TOOLS: „Essentials for Legal Work“ α „Blank Strategy“ β „GAST-Index“ γ Writing
2	“Basics 1”	Robots and Cyborgs and the Right of Humans
3	“Basics 2”	Reaching out for a Global and Universal Perspective
4	“Basics 3”	Language as a Strategy for a Global Lecture Standardization Effort
5	“Basics 4”	“LEXONOMICS” – Financial Resources, Efficiency and Efficacy Principles
6	“Basics 5”	National Constitutional Reserves for (Inter)National Law in Globalized (and Digitized) Societies
7	“Basics 6”	Electricity as the Lifeblood of/ Fuel for Cyberspace
8	“GoCore! 1”	Telecommunication Traffic Data Retention and Usage Law (TTDL) als “Double Module”
9		
10	“GoCore! 2”	Ramifications of Virtual Currencies on Governance
11	“GoCore! 3”	“Who Owns the Sky?” – Drone Law
12	“GoCore! 4”	“Interactive Toys” – Spyware in Nurseries around the World?
13	“GoCore! 5”	TechJustice and “Technology Transforms Legal Markets”
14	“Terroir”	Burgeoning historical, political, societal etc. specific issues from idiosyncratic national perspectives
15	“Outcome & ROI”	Concerted Pioneering in Cyber- and AILAW with the Ambition of best possible Cyber Governance (without stifling beneficial innovation)

*Submitted by Viola Schmid for „World Congress of Constitutional Law“, Workshop 27: Constitutional law scholarship and constitutional transformation, Johannesburg, South Africa, 5 – 9 December 2022.

II. This Cylaw-Report XXXXI as „Entourage Document“

The “Entourage Documents”, which provide the flesh, are to be distinguished from the “Backbone Documents”, which delineate the skeleton. “Weltrecht¹²” allows for a review of the document “A Standard for a Universal (Technology) Law Lecture in a German Initiative Reaching out to Europe, China and the USA in Cyberspace and (Technology) Law – Draft No. 1“, which was developed between 2017 and 2018, and presented in New York in 2018. In this sense, it is a multi-functional “Entourage Document”:

- On the one hand, it offers complementary background knowledge that is not subject to the limitations of conference presentations and paper publications.
- On the other hand, the publication of older documents serves to prove the sustainability / long-term validity of the research results.
- Furthermore, the „Herstory“¹² allows the comprehensible tracking and conception of the genesis of focal points (Telling history).

III. Pedigree: "Cyberlaw All" & "Cyberlaw Special" Publications

Both the “Backbone Documents” as well as the “Entourage Documents” can in part be thematically grouped into one document pedigree.

1. “Cyberlaw All”

The term "Cyberlaw All" is used to designate documents devoted to cyberspace in its totality. The first example is Cyberlaw All I from 2003 with the title “Cyberlaw – Eine neue Disziplin im Recht?”¹³ [EL: Cyberlaw - A new discipline in law?]. Also this Cylaw report, which deals with a teaching standard (“A Universal Standard for a (Technology) Law Lecture”), is classified as a Cyberlaw All document. Ideally, it outlines a dogmatic, methodological, and content-rich teaching canon for informed cybercitizens. What is distinctive for the STANDARD is that it addresses a technology-based world with a focus on diverse life experiences that range from technology

¹² The term „Herstory“ was also used in German television: Das Erste, Geschichte im Ersten: [HERstory \(1\) – Lebensgefahr](#), (video available until August 16, 2022).

¹³ Cyberlaw – Eine neue Disziplin im Recht? in: Hendlar, Reinhard/Marburger, Peter/Reinhardt, Michael/Schröder, Meinhard, Jahrbuch des Umwelt- und Technikrechts 2003, Erich Schmidt Verlag, 2003, S. 449-480.

in children's nurseries¹⁴, “ramifications of virtual currencies on governance”¹⁵, drone-determined environments¹⁶ [“Drohnenwelt”], to the evolution of humans into transmachines (original terminology) and of machines into AI machines with human similarities (transhuman)¹⁷.

2. “Cyberlaw Special”

Sector-specific publications which focus (only) on technology specific (e.g. RFID law)¹⁸ and/or application specific (e.g. e-Justice)¹⁹ challenges shall be designated as „Cyberlaw Specials“. More recently, these include the law governing aerial drones (UAS law).²⁰

E. Timeline of the “Weltrecht^2” Project: Development Phases & STEP LADDER

As the research and teaching(s) have been ongoing since 2003, several documents that have never been published in the internet exist in various degrees of maturity as well as different languages. In summary: These work outcomes are evidence of an author's research and teaching progress - referred to here as the "Herstory."

I. Different Languages – GL & EL

The author has the German authorization to teach public, European and energy law, and has published generally in her native language. The complexity of translation already into English is considerable – therefore several documents have so far been only available in German.

¹⁴ STANDARD, Modul 12 – „GoCore! 4“: “Interactive Toys” – Spyware in Nurseries around the World?

¹⁵ STANDARD, Modul 10 – „GoCore! 2“: Ramifications of Virtual Currencies on Governance.

¹⁶ STANDARD, Modul 11 – „GoCore! 3“: “Who Owns the Sky?” – Drone Law

¹⁷ STANDARD, Modul 2 – „Basics 1“: Robots and Cyborgs and the Right of Humans

¹⁸ See selected contributions by Schmid reg. Radio-Frequency Identification (RFID): Radio Frequency Identification Law Beyond 2007, in: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma (Eds.), The Internet of Things, First International Conference, IOT 2008, Zurich, Switzerland, March 26-28, 2008, p. 196-213; RFID Legislation in a Global Perspective, in: Hansen/Gillert, RFID for the Optimization of Business Processes, 2008, p. 209-219; Mastering the Legal Challenges, in: Heinrich, RFID and Beyond, 2006, p. 193–207. See also the supervision as „Doktorvater“ for Löw, [RFID-Recht der Zukunft – Brauchen wir in einer ubiquitären Radiofrequenz-Umgebung bereichsspezifische Datenschutzregelungen zur Verhinderung der Erosion der Rechte des Einzelnen?](#), 2013 (last accessed Oct. 28, 2022) und Gerhards, [\(Grund-\)Recht auf Verschlüsselung?](#), series of publications „Der elektronische Rechtsverkehr“, Band 23, 2010 (last accessed Oct. 28, 2022).

¹⁹ See also Schmid [GL] §§ 55a, b und c, in: Sodan/Ziekow (Hrsg.), Kommentar zur Verwaltungsgerichtsordnung, 4th Ed. 2014.

²⁰ Schmid/Toptaner: Integration von „Flugdrohnen“ in das (deutsch-europäische) Rechtssystem – eine Kartographie, p. 469- 514, and Schmid/Kretschmann, Operative Herausforderungen einer Drohnenwelt (Luftverkehrs)-Management inkl. der „Drohnerdetektion“; p.522-553, in Chibanguza et al. (Ed.), Künstliche Intelligenz – Recht und Praxis automatisierter und autonomer Systeme, Nomos 2022.

These partly older documents are shared as part of a Legal Open Source Project on the Internet and rely on the following translation strategies:

- On the one hand, new digital translation programmes allow for initial access to the published information in a variety of languages. The supplementation of the native German text is thus left to the possibilities of technology. The extent to which technological possibilities have advanced is illustrated by the controversy regarding language AI, which allegedly possessed its own consciousness. According to a Google employee and developer, a LaMDA (Language Model for Dialogue Applications) was said to have already had acquired this quality. Corresponding media reports also talked about the suspension of the employee.²¹
- Preferable for the author is the collaborative textual critique at the hand of qualified translators, who will be the source of her English, and in future, Chinese language texts. Due to capacity constraints and in light of the challenge to keep data regarding innovation law current, an adequate translation cannot be provided for all documents in real time. The current focus remains on the German [GL] as well as the English language [EL].
- The “Step-Ladder” chronology of relevant publications also includes references in the German language – titles of original publication in German have not been translated to ensure better accessibility.²²

II. Multimediality and Equivalence of Publications in Prose & PPT forms

The volatility as well as the dynamics of the „digital transformation of the real and the real transformation of the digital“ (original terminology) leads in consequence to a publication strategy that at times selects publication forms other than prose texts in academic journals. This reflects a pragmatic approach, which corresponds to the ambition of achieving a functional and “real time” effectiveness. Therefore, for „Weltrecht²“ not only essays but also video- and audio formats as well as slides are consistently shared.

²¹ <https://www.heise.de/news/Ein-Softwareentwickler-kaempft-fuer-Persoenlichkeitsrechte-eines-Chatbots-7153612.html> (2022.10.16).

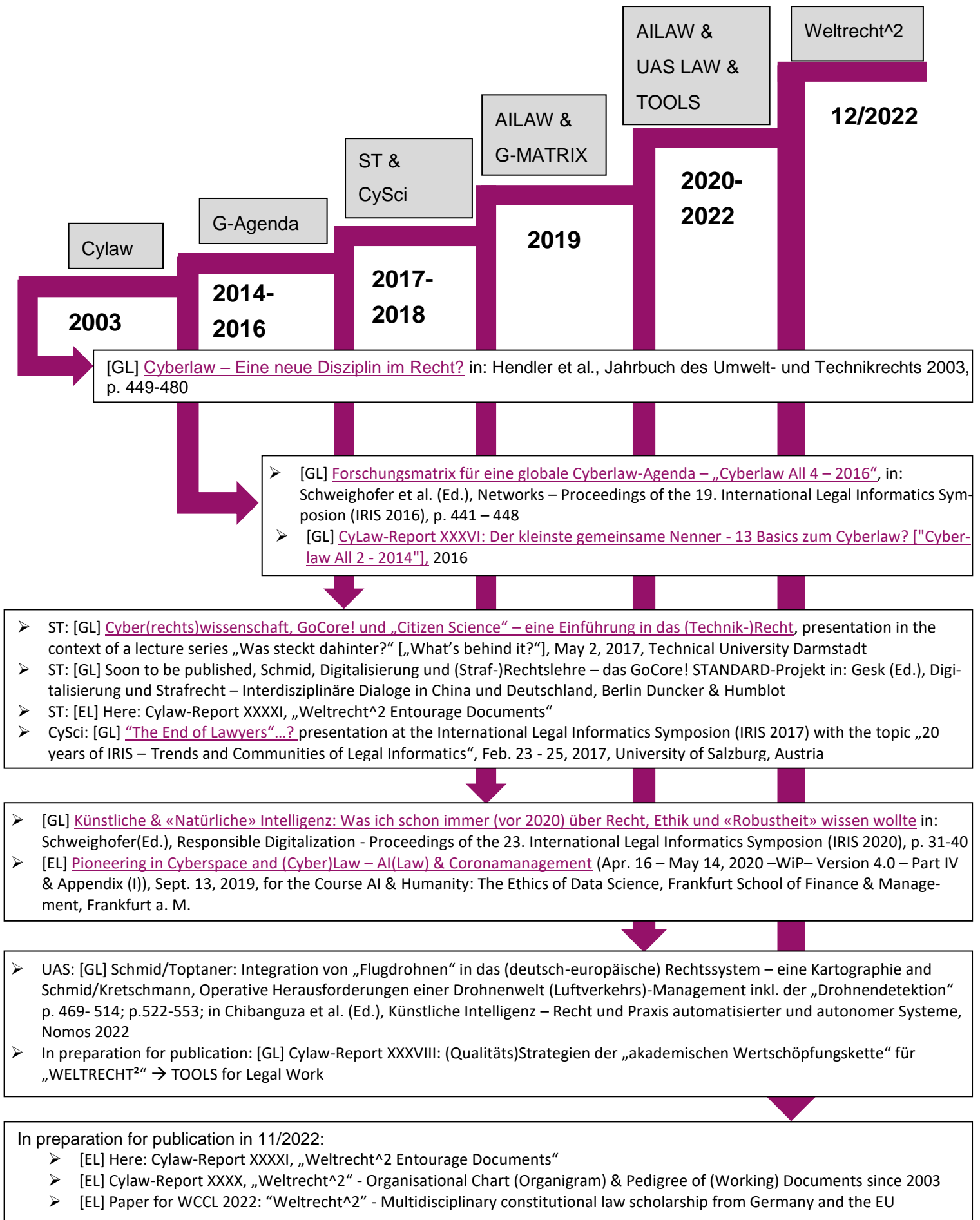
²² Libraries enter book titles into their catalogues with officially published titles. German titles here have been kept in German to allow for better traceability in library catalogues.

III. List of Abbreviations (Acronymology) for the “Herstory Step ladder”

In order to visualize the sequence of phases of academic findings regarding Cyberlaw and AILAW leading up to „Weltrecht^2“ as the goal, it requires the development of an acronymology:

- AILAW – (European) Law Of/On „Artificial Intelligence(s)“
- Cylaw – Cyberlaw
- CySci – Cyberscience (Cyber(rechts)wissenschaft)
- GA – GLOBAL (CYBERLAW) AGENDA
- GM – GLOBALMATRIX
- [EL] – English Language
- [GL] – German Language
- ST – Teaching Standard
- Tools – Tools/Essentials for Legal Work
- Tax – Taxonomy
- UAS – Unmanned aerial systems

IV. "Weltrecht^2" as Visual Legal Design: Development Phases as a "STEP LADDER"



V. Varying Degrees of Maturity

The document that is shared further below in Part 2 originated in 2018 and shall be designated as “Draft No.1”. It is a working document and the pedigree of (working) documents was visualized above.

F. Acknowledgments

My deepest gratitude goes to American cyberlaw pioneers - such as Eric Goldman, Chris Hoofnagle, Barbara Endicott-Popovsky and Scott David - to mention just a few here. Their works have always encouraged me on the long road to “Weltrecht²”, as much as their critique has helped me. I would also like to thank Harvard Law School as well as the Fullbright Grant that in 1990/91 opened up the doors into the international world of law for me.

G. A STANDARD FOR A UNIVERSAL (TECHNOLOGY) LAW LECTURE (March 24, 2018)

I. Internet Law Works in Progress Conference

For the past 10 years, the Internet Law Works in Progress conference has been hosted alternately on the East and West coasts of the United States: „The Santa Clara University School of Law is a co-host: the Innovation Center for Law and Technology at the New York Law School and the High Tech Law Institute at Santa Clara University School of Law host an annual symposium for Internet law scholarship. This conference series provides an opportunity for authors and scholars to improve their papers and projects, regardless of how well-developed or polished their theses or drafts may be. To achieve that goal, all comments to authors are made in the spirit of collaboration.”²³

II. Editorial Amendments in 2022 by Viola Schmid

This text, first presented in 2018, has been reproduced with only slight amendments with re-

²³ https://www.techpolicy.com/Events/2020/03_March/Internet-Law-Works-in-Progress.aspx, 2022-10-16.

gards to grammatical and spelling correctness. In the following, the historical “Entourage Document” has been appended as Part 2-10 to this Cylaw-Reports XXXXI from 2022, in order to illustrate the „flesh“ related element of the „corporeal metaphor“ for „Weltrecht^2”.

III. Editorial Amendments in 2022 by Georg Gesk

Georg Gesk provided some new insights. In Part 8 A. the version of 2018 has been marked in grey and his annotations have been added in a box:

“Reading this agenda, and as a matter of fact actually being involved in reaching out to China, I realize how much things have changed in this relatively short period of time since the agenda was developed. Having left [University of Osnabrück](#) for a few weeks, I’m sitting on the campus of Anhui University, being involved in comparative research concerning legal developments as a reaction to rapid advances in the field of digitalization and AI in China, having vivid discussions with colleagues and students of [Anhui University Law School](#) (and with students and colleagues in other parts of this amazing country), planning for advancing a [common LLM program](#) and other future common [activities](#), I try to pin down just a few major points of changes in the development of digitalization and AI law in China, attempting a dialogue with the text from 2018.”

IV. Temporal & Local Context

1. EL – USA

This Cylaw-Report is concerned with DRAFT No. 1 of the teaching standard, which was first presented in 2017 and 2018 at the “Internet Law Works-in-Progress“ Conferences in Santa Clara und New York.

2. GL – BRD

Also in German, the publication of slides can be found at the Technical University of Darmstadt in 2017²⁴ and in a soon-to-be-published article.

²⁴ [Cyber\(rechts\)wissenschaft, GoCore! und „Citizen Science“ – eine Einführung in das \(Technik-\)Recht](#), presentation in the context of a lecture series „Was steckt dahinter?“ [„What’s behind it?“], May 2, 2017, Technical University Darmstadt.

V. Iterations and Self-Critical Concretization

Concretization of the original (own) terminologies and argumentation are the purpose of the publication and the discourse with the audience.

1. Trans-, Multi- and Pluri- Disciplinarity

DEMONSTRATOR: While the draft document from 2018 still strives for transdisciplinarity, the following concretization has been made in 2022: teaching is oriented in a multi and pluridisciplinary manner, and especially jurisprudential research strives for transdisciplinary competence. The ambition is to research and process the work results of those disciplines that offer the best possible [Governance, Compliance & Regulatory strategies \(GoCore!\)](#). This unbiased exploration as well as processing of work results is herewith referred to as "Pluridisciplinarity".

2. Feedback

The author and initiator of "Weltrecht ^2" remains naturally grateful for any critique and suggestions, and can therefore be contacted at schmid@cylaw.tu-darmstadt.de.

VIOLA SCHMID, GEORG GESK, CHRISTOPH MERKELBACH

A STANDARD FOR A UNIVERSAL (TECHNOLOGY) LAW LECTURE
IN A
GERMAN INITIATIVE REACHING OUT TO EUROPE, CHINA AND THE USA
IN
CYBERSPACE AND (TECHNOLOGY) LAW
– DRAFT No. 1 –

Contribution for the "Internet Law Works-in-Progress" Conference,
March 24, 2018
New York Law School, Innovation Center for Law and Technology, USA

Part 2: What (I)? Standardization for Global Cyberteaching in Order to Better the World

A. What, How, Why, Who, Where and Intended Impact as well as SWOT-Analysis

The United States has been enriching the world for decades through major films, television series and broadcasts. Its citizens are masters in the art of the screenplay and lead the world

of economics. We owe the interrogative pronouns “Who, What, Where, When, Why, and How” as a plotting strategy as well as the concept of SWOT (Strength, Weaknesses, Options, and Threats) analysis to the Anglo-American (management) perspective. This script presupposes these coordinates for a global lecture project, and uses interrogative pronouns as they are embedded in the SWOT analysis to explain which sub-goals have been achieved step by step or where the weaknesses currently lie. SWOT is the matrix that advocates, supporters, and critics of this project should use for further discourse.

One of the strengths of the project is its innovation and the scope of its ambition. A basic lecture for a trans-disciplinary audience that is potentially located in all states/ nations of the world or none is such an ambitious project that the attempt alone can be a strength. These weaknesses are the mirror image of the project’s strength: how can we study from a globalized perspective the rule of law in an interesting and sustainable manner? How can we interest a (previously) unaffiliated audience in the topic?

The options are evident: gaining a wider audience for the project’s importance, improving general understanding of (cyber)law as the basis of peace, security, trade, (inter)national solidarity in the event of a crisis – and last but not least avoiding costly misunderstandings as well as overworked bureaucracies.

The threats include uncontrolled conflict, lack of sustainability, lack of quality in law, and a lack of consensus. Additionally, the dominance of individual legal systems and traditions under a misleading claim that the project is international (and not based on an organization of “representatives/citizens” of individual nation-states) is problematic. This may be a threat for the project as well as a weakness or strength: proselytization is not the strategy, instead the strategy is broadening the horizon by sharing a vision.

These opening comments are necessary in order to introduce a trans-disciplinary project that also has learning potential for “everyday people”²⁵. Thus, the proposed impact of this project is to form an (inter)national coalition of interested persons and groups (coalition of the willing), who seek to use the rule of law as a science and a (teaching) grid.

²⁵ In the sense of „non-academic“, „non-expert“ people. How difficult right wording appears to be can be compared here: BP CEO’s media blurb during the Gulf of Mexico Oil spill (<https://watchingthesweddes.com/2010/06/18/the-little-people/> - (10-04-2022); and the press conference: <https://www.youtube.com/watch?v=th3LtLx0IEM>) – (10-04-2022);

B. Draft Status No. 1

This forward-thinking project, which aims to set **a standard for law schools and law lectures** on (cyber)law, is outlined in this draft at the 2018 “Internet Law Works-in-Progress” Conference. Following an interpretation of the conference title, it is indeed a work-in-progress that is conceived as a “living document”. It is hereby submitted to an academic open innovation (AOI) process addressing the attendees of the conference.

I. Multimedia Ambition

The draft status supports the manuscript to integrate a variety of presentation modes: on the one hand, text and on the other hand, Power Point presentation slides (incorporated in a speech protocol). The inclusion of audio and video sequences is a didactic strategy in another version. In short: The gradual enrichment of the project with additional materials is part of the strategy for longevity.

II. Partial Mono- and Bilingualism with the Aim of Trilingualism

The lecture concept is not only multimedia-based, but – owing to the draft status – partially mono- or bilingual with the aim of trilingualism in the future. This draft version is partly presented only in German (see Christoph Merkelbach in part “reaching out to china” – “let’s talk about cyberlaw”) because the focus of this draft is soliciting critique and feedback for the project’s broader agenda (and not consent to details). Moreover, specific translation in comparative legal analysis is highly controversial. The justification for this project management strategy is exemplified with the abstract. The meaning of the term “rule of law,” for example, is so intricately portrayed in different legal traditions that the work on terminology alone would unduly slow project progress. So, the mono-, bilingual and trilingual parts should be consolidated in the final version. Open-minded management is required: in other words, unresolved definitional and translational challenges should never prevent the search for common solutions.

III. Original and Own Terminology for This Project: “Securitization”

A constructive way not to lose focus in discussions of traditional terminologies in different and fractured disciplines is the use of own terminology. Regularly, such terminology efforts will be exposed to the criticism of misunderstanding (because this term is understood differently in

another language) to incomprehensible (because the project wants to establish a new word with a new meaning). Therefore, caution is required in this respect, but it will be preserved if the new terminology continues to be useful for understanding key issues. An example is the concept of “securitization” that shapes this draft. Securitization has a specific meaning in the German and English financial sector. In a global world, the security level of a nation (or lack thereof) and of the world is so central that it continues to be used here in terms of increasing the level of security at national and worldwide levels. This is so important because with the ubiquitous interconnectedness of cyberspace, there is both the chance to inform multinational public opinion as well as the opportunity to commit worldwide crimes against anyone. The digital identity of every human being can theoretically be violated and manipulated by global perpetrators. In cyberspace, there is a different level of uncertainty than in the physical world (here called realworld). Also, IT-Security Law (“ITS-Law”) becomes the prerequisite of the right to assert legal authority. In summary: Securitization as understood here is the core challenge of cyber governance.

IV. Time Management and Living Documents

One author, Viola Schmid, has been a pioneer in German-European cyberlaw for 15 years. Most of her publications are in German and therefore are difficult for a non-German-speaking audience to access. For that reason, manuscripts that appeared a few years ago will be reproduced in this draft. In particular, this is the case for the “Global Agenda for Cyberlaw,” which the author published in 2015.²⁶ This decision was taken because identifying changes over the past three years will become easier when compared to earlier published texts. Cyberlaw in Germany and Europe is currently undergoing significant shifts, including social and economic disruptions, so a lean production strategy promises the greatest efficiency and effectiveness. For the benefit of the reader, as well as for quality assurance and transparency purposes, the date of creation and/or publication is consistently provided.

²⁶ V. Schmid, CyLaw-Report XXXVI / 2016, „Der kleinste gemeinsame Nenner – 13 Basics zum Cyberlaw? [Cyberlaw All 2 – 2014]“, http://tuprints.ulb.tu-darmstadt.de/5323/1/CyLaw-Report%20XXXVI_02_2016.pdf (26.02.2018); V. Schmid, Cyberlaw FORSCHUNGSMATRIX FÜR EINE (GLOBALE) CYBERLAW-AGENDA – «CYBERLAW ALL 4 – 2016», in: Schweighofer/Kummer/Hötzendorfer/Borges (Hrsg.), Netzwerke – Tagungsband des 19. Internationalen Rechtsinformatik Symposiums (IRIS 2016), S. 441 – 448 (in der Printausgabe), http://www.cylaw.tu-darmstadt.de/media/jus4/publikationen/beitraege_in_buechern/2016_02_09_54_IRIS2016_Schmid_FJK.pdf (26.02.2018).

It is to be noted, however, that using older texts in this first draft may demonstrate the validity of such a strategy and tactic. For someone who has been writing in Germany 15 years ago about Cyberlaw as a new discipline of law²⁷ and gave lectures on telecommunication traffic data retention and usage law,²⁸ history is telling today. Written from a global perspective over the last decade and a half - these texts show that the risks of chill, digital identity (theft), anonymity and pseudonymity are as acute today as back then. They are evergreens among the challenges for rule of law in cyberspace.

V. (Legal) Sustainability through the Choice of Challenges and “Shepardizing”

If a lecture script and project seem to be under constant threat of expiration, given the anticipated volatility of technology law (especially cyberlaw), the challenge of updating strategy and tactics will arise. Such a complex pioneering project must be designed in such a way that it is both sustainable and is prepared for inevitable modification. To meet that challenge, we propose to select paradigmatic scenarios and challenges and to alter their content when the law under discussion changes.

For this reason, we plan to carry out a revision at specific intervals and to reserve a unit of current/idiosyncratic questions (an “**terroir and up-to-date**” module, see Part 4 F.VI.13) of the fifteen ninety-minute units.

The tactic chosen is “**Shepardizing**,” which is consistently revisited in cyberspace and cyberlaw. The idea is to describe a paradigmatic scenario in detail with a matrix and then to transfer this matrix structure into other legal systems. Once we have agreed on the matrix, we cannot only access the law but also open it up to timely updates. The traditional “Shepardizing” tactic structuring common law thereby serves for clarity in global (cyber)law.

The leading scenario here is “**telecommunication traffic data retention and usage law**”. Experiences from German and European law in the past twelve years are used and presented. We leave it to the superior knowledge of the American audience to supplement the German/European/Chinese findings with results of the (current) discussions on monitoring of

²⁷ V. Schmid, Cyberlaw – Eine neue Disziplin im Recht? in: Hendlar, Reinhard/Marburger, Peter/Reinhardt, Michael/Schröder, Meinhard, Jahrbuch des Umwelt- und Technikrechts 2003, Erich Schmidt Verlag, 2003, S. 449-480; http://www.cylaw.tu-darmstadt.de/media/jus4/publikationen/beitraege_in_buechern/Schmid_V_Cyber-law_eine_neue_Disziplin_im_Recht.pdf (22.02.2018).

²⁸ V. Schmid, CyLaw-Report I, „Speicherung von IP-Adressen“, „Speicherung von IP-Adressen“ Entscheidung des Amtsgericht Darmstadt vom 30.06.2005 – 300 C 397/04, 02.05.2006; http://tuprints.ulb.tu-darmstadt.de/1099/1/CyLaw_Report_I_060502.pdf (22.02.2018).

American citizens at the time of manuscript submission (such as the very recent discussions in US media following the publication of the Devin Nunes memorandum (I – declassified by order of the president 2/2/2018; “Nunes memo (I)”)²⁹. Thus, in this first draft, the topic of pre-recorded data storage is also proposed as the leading module.

The authors have a strong interest in taking on a major intellectual challenge, and their project should therefore attract global attention as the project progresses. Schmid’s English language publishing strategy, which dealt with RFID-Law, with IT-Security-Law and in 2009 with the “Internet of Things” illustrates her ability to address legal problems as they develop. These examples of transnational publications, including the “Springer Lecture Notes on Computer Science” and the “Dagstuhl” publication series demonstrate the author’s preparedness for the challenges of bilingual citation.

VI. Citation and Detection Strategy – “Blanket Strategy”

Anyone wanting to cite laws and legal literature using a global perspective quickly faces capacity, competence, and language barriers. In addition, we face barriers of financial resources as well as the partial non-disclosure of texts (of the past) on the Internet. Of course, the authors have neither boundless financial resources nor time to find and to process all relevant publications on globalism. Consequently, it is necessary to be selective with sources in literature, jurisprudence, and legislation. A classic German proverb says: “*Aus der Not eine Tugend machen*” (make a virtue of necessity). This strategy of “eclectic yet informed” selection is taken and delineated as a “Blanket Strategy” and consistently includes the courage to revise our thinking and to include more materials in our analysis. **The few citations used as evidence in this draft do not take the place of traditional scientific research with complete sourcing.** This perspective on sourcing is justified by the pioneering character of the course’s design. However, the authors plan to fill existing gaps given their expertise especially on China, Germany and Europe, and their additions will appear in the agenda-setting for the second draft.

²⁹ “Nunes memo (I)” is a four-page memorandum written by Republican staff members of U.S. Representative Devin Nunes declassified by order of the president 2/2/2018; https://en.wikipedia.org/wiki/Nunes_memo, https://en.wikipedia.org/w/index.php?title=File%3ANunes_Memo.pdf&page=1 (22.02.2018).

C. Global Cyberteaching for a World Connected by the Technology of Cyberspace:

Adding a Fifth Dimension of Being

Only the aspiration for a global understanding (of cyberspace) allows global trade and production, thus furthering economic growth, security and welfare. The purpose of standardization is to facilitate a global discourse, to improve understanding of one another, to discover the quality and quantity of the positioning of different people and nations vis-à-vis the challenges of the future—in particular, (living) together with machines. The rule of law, legal traditions and systems (art. 67 para. 1 Treaty on the Functioning of the European Union (TFEU)³⁰ and art. 6 para. 3 Treaty on European Union (TEU), in this respect, establish the potential for a “**global legal grid**” transmitting intellectual energy, like a “power grid”.

Art. 67 TFEU

1. The Union shall constitute an area of freedom, security and justice with respect for fundamental rights and the **different legal systems and traditions** of the Member States. [...]

Art. 6 TEU

[...]3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the **constitutional traditions common to the Member States**, shall constitute general principles of the Union's law. [...]

Global cyberteaching prepares for the interoperability of the different participants and contents administered and sophisticated by this network. In the past, each legal scholar in each country might have assumed a very insular approach for his/her country, its legal system and its tradition. In the future, legal science—even in the USA with its massive size—has to be prepared in such a way that not only national law will be relevant, but that international law will have to be increasingly taken into account for legal analysis. Moreover, supranational entities (for example European Union) will prevail and dominate. Writing from a German perspective: We no longer teach German law; instead, we teach law “coming into effect” within German borders. The old metaphor that by sailing you might discover that earth is not flat and shaped like a disc

³⁰ Consolidated version of the Treaty on the Functioning of the European Union, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> (22.02.2018).

but develop a spherical perspective also applies to global cyberteaching ambitions. And cyberspace with its connectivity principle adds a fifth dimension to all our lives besides the cubic meters of the realworld and the dimension of time.

Cyberspace enables researchers as well as (law school) professors to enter into contact at low financial costs, in a fast manner (nearly real time) and allows scalable communication (individual- and mass communications). Using cyberspace for academic teaching in a global format is the challenge that this project tries to master. In short: in this project, **technology is causa sine qua non for content** (sharing), thus enabling us to explore uncharted territories and hitherto unbeknownst dimensions. Moreover, we may not only analyze that the world is round and not flat, but we have to envision the necessity of sharing place and time with “fellow machine beings.” Digital updates of humans and human updates of machines are on the agenda of AI proponents. The “machinization” (original terminology) of human and animal society as well as the humanization of machines and robots is a world-turning phenomenon. Human-machine interaction is the immediate challenge for justice as well as law in the near future. This change of dimensions is a good reason for such a project. Hence, it is essential to find and/or build common ground in different disciplines as well as nations in order to provide “a bouquet of possibilities” (“a toolbox for legal instruments”) *“ (einen Strauß der Möglichkeiten)*. It is likewise essential to ascertain what we agree and what we disagree on.

I. “We” all Agree – some Talking Points?

- The consequence of the global nature of a “cyber-audience” is the global competition for ideas and the need or wish for protection against manipulation and repression.
- Data is the new oil and the “refining of oil” and trust in the quality and truth of data are vital for future generations.
- New competitive environment for scientists: every day, scientists realize that somewhere in the world, maybe even at some other point in time, another scientist has or has had the same or a better idea. Therefore:
- While we live in fractured societies, our cyberspace horizon enables us – perhaps for so many people for the first time in human history – to enter into contact with so many legal and cultural traditions that a large number of people are technologically empowered to get to know and to analyze our differences. We lived and live in a fractured world – but cyberspace offers us an intimate view of the injuries as well as the remedies in other parts of the world. The selection of glasses and the eyes of the beholder differ, however.

In European Union Law, you find this reflected in art. 67 Treaty on the Functioning of the European Union (TFEU)³¹ and art. 6 para. 3 Treaty on European Union (TEU).

- In a time of competing national, economic and legal systems, such a dream project like GLOBAL CYBERTEACHING requires more capacity, resources and competences than one person in their lifetime can offer and sacrifice. Hence, legal open source projects (data banks) and legal tech/AI provide material support but—nowadays—do not replace the need for human supporters, followers and mentors around the world.

II. “We” – with a Focus on Three Legal Traditions, Systems, and Languages

In early 2018, our standardization project is in its infancy, and our core language, research, and legal competences are anchored in these three legal systems. This strategic focus includes the openness to the acquisition of other sources using additional competences – for example, sources in French or Spanish.

III. Academic Open Innovation (AOI) as Crowd Sourcing

The idea that a lecture is jointly conceived and taught in parallel by scientists from different legal systems and traditions comes from Darmstadt. Our model is the initiative of the Director General of the European Space Agency, Professor Johann-Dietrich Wörner, who oversaw a one-day debate in 9/2016 in which one hundred citizens simultaneously discussed space-related legal and political issues in twenty-two nation-states.³² This establishment of an open platform and standards for addressing cross-cultural and multilingual challenges seems groundbreaking for promoting the idea of a trans-disciplinary, spatially (and space-oriented) informed, law lecture series.

³¹ Consolidated version of the Treaty on the Functioning of the European Union, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> (22.02.2018).

³² The European Space Agency organised the first citizens' consultation about space and outer space treaty law, http://www.citizensdebate.space/en_GB/home (22.02.2018); Discover citizens debate results, <http://www.citizensdebate.space/results> (22.02.2018).

IV. “Privacy by Design and Default” as a Model for “Legality by Design and Default”

Starting on May 25, 2018, the new General Data Protection Regulation³³ becomes applicable in the European Union as well as in Germany. “Data protection” (in the sense of privacy) is embedded in technological environments and dependent on a cost-benefit ratio.

Art. 25 GDPR – Data protection by design and by default

1. Taking into account the state of the art, the **cost of implementation** and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to **integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation** and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, **by default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that **by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.** [...]

From a global perspective, the default and design strategy (**law determines code or law is code**) holds the potential to become the model for embedding law in societies. The cyber-teaching standard could be a step towards reaching the end of this journey. Hence, the project defines the vision of “Legality by Design and Default”. This vision can only materialize if people other than lawyers are entitled to access materials for evaluation, information and research. Furthermore, the acquisition of “knowledge capital” from other legal systems is of vital importance. That vision also includes an aim to avoid the sunk costs, unnecessary expenditures and financial losses from of investing in non-functioning or poorly functioning digitization initiatives (in Germany, the fields of e-health and e-Justice are indisputably included). The vision

³³ REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), <http://eur-lex.europa.eu/eli/reg/2016/679/oj> (17.02.2018).

is to educate citizens on becoming competent cybercitizens, especially regarding security in the realworld and cyberspace. Moreover, if machines implement the rule of law in the future, **their code should reflect the best knowledge as well as practice of law.**

Part 3: Why and for What? The Challenges and Opportunities of a Global Legal Perspective with Ambitions of Standardization: The Road to a Better Future through Competing (Technology) Legislation

A. May the Best Idea Win: How Arguments Compete

A fundamental idea of societies that value the freedom of expression is that allowing for competing arguments in the public space is a promising way to determine common ground. All the more interesting for this project is that differently structured societies mediate and accomplish that task differently. So, from a global perspective, there are divergent views on the legal meanings of freedom of speech and expression.

Even if unanimity in the freedom of expression is affirmed, the existence of cyberspace raises the question of “how” that freedom is legally supported, and what content may be disseminated in cyberspace. A bifurcation of our perspective into law on content of expression (German: Äußerungsinhaltsrecht – whether) and law on technology of expression (German Äußerungstechnologierecht – how) becomes essential with cyberspace. “Whether” and “how” have intersections. Even in societies that support freedom of expression, the content of that expression may be so unlawful that its distribution specifically in cyberspace should be prohibited and suppressed. This is the current legal situation in Germany, which obliges with the law on enforcing the rule of law in social media (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG – 10/1/2017))³⁴ certain providers (f.ex. Facebook) to suppress and remove such “illegal” language.

³⁴ <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> (26.02.2018).

Hence, from a global perspective, the question of “whether” content is (in cyberspace) allowed or prohibited arises for all communication and legal systems. Nevertheless, the project believes that because of the variety of people and legal traditions and systems involved, and in the likely case of confrontation and competition, different and contradictory arguments should be handled following the old motto *fortiter in re, suaviter in modo* (strong in conviction, gentle in approach).

B. Global Language Diversity as a Barrier to Consensus and a Challenge for Discourse

I. Global Quantity of Languages: The United Nations as an Example

The United Nations recognizes 193 members³⁵. It uses six official languages³⁶, which in the bottom-up approach of this teaching project are not sufficient to prepare regulatory and policy documents for people of many nations (and not only members of academia and government). Limited linguistic ability and access is a present weakness of a global project. The challenge becomes even clearer when linguistic research assumes a worldwide quantity of more than seven thousand languages (depending on the classification method). If language provides access to legal cultures and traditions (literal interpretation), then lack of a common language has a core importance. The justification for limiting the project to three languages is due to project management and building on the existing linguistic strengths of the three authors. This strategic decision does not conceal any tactical losses that will likely result.

II. Loss of Content through Language Diversity

It is already clear that the pre-publications of this project written in German or Chinese by the three authors are not accessible to all participants in the conference. Even here, it becomes evident that German or Chinese publications are not easily accessible for the (cyber)law/cyberscience scientific community. In this sense, the lack of a common language is **one aspect of the universal inaccessibility of content**. The phrase “language diversity” describes this

³⁵ Overview United Nations, <http://www.un.org/en/sections/about-un/overview/index.html> (22.02.2018).

³⁶ Official Languages of the United Nations, <http://www.un.org/en/sections/about-un/official-languages/index.html> (22.02.2018).

challenge. In addition (see above under I.), content in other than the three project languages will not be used due to the limits of our own linguistic ability.

The other aspect is evident as well: Even the limitation of three project languages carries the risk of content loss and misunderstandings, which we refer to as the “Multilingualism Challenge.”

III. Loss of Content and Misunderstanding as a Consequence of Multilingualism: For example “Der Kampf ums Recht” (see Abstract)

The abstract for this conference contribution depicts this challenge – “Multilingualism Challenge” – with citing the famous quote from Rudolof v. Ihering in 1872:

„Das Ziel des Rechts ist der Friede, das Mittel dazu der Kampf.“³⁷

John J. Lalor (1915) translates this German sentence as follows: “The end of the law is peace. The means to that end is war.”³⁸ His translation of Kampf as “war” in this first sentence differs from Lalor’s earlier translation of the title of Rudolf v. Ihering’s work. There, he translates Kampf as “struggle” (“Der Kampf ums Recht”–“The Struggle for Law”). “War” and “struggle” differ—consequently one would have expected the following translation: “The end of the law is peace. The means to that end is struggle.” So, even if these famous translated words of Ihering could not be more easily misunderstood—they could not have more relevance today. Yes, in 2018, the world is still threatened by “wars” and has new options for “struggles,” such as communications in social media with a globalized and perhaps compartmentalized audience. Furthermore, in a unique way (“war”–“struggle”³⁹), even Lalor’s “mistranslation” paves the way for the postulate: Military conflict and force (“war”) are ultima ratio and campaigning for ideas, contest of arguments and “struggle” are prima ratio. When seen in the Chinese context, we witness significantly different frictions, since the double meaning of “Recht” as both objective law and subjective right is not translatable into Chinese without choosing different words. Objective law

³⁷ Rudolf v. Ihering, *Der Kampf ums Recht* (1872; Frankfurt: M. Klostermann, 1960), 1.

³⁸ Rudolf v. Ihering, *The Struggle for Law*, trans. John J. Lalor, 2nd edition with an introduction by Albert Kocourek, (Chicago: Callaghan, & Co., 1915), 1 (<https://archive.org/details/cu31924021172832>).

³⁹ David Kennedy also uses “struggle” in his title: *A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy* (Princeton: Princeton University Press, 2016).

is translated as “法,” and subjective law is translated as “权利.” The latter word raises an intriguing linguistic relationship with the homonymous (and in its first half identical) notion of “权力” = power. Therefore, when Chinese sources translate Ihering’s famous title, they limit its inherent meaning to the objective or state-dominated level but miss the subjective or individually dominated level. Therefore, a very different mindset arises out of the “same” text when seen from different cultural and linguistic backgrounds in Europe as well as in China.

IV. Strategy: Focus on German, English and Chinese – *pars pro toto* (a Part for the Whole)

The guiding idea of this project is to make the best use of the experience and abilities of the three authors as pioneers in (cyber)law, linguistics and CYBERSCIENCE. The three selected legal systems and traditions are suitable for generating and representing groundbreaking arguments, such as the project’s use of Academic Open Innovation as a tool. The focus on three working languages in draft no. 1 is intended to make our internal network functional and to prevent additional labor costs for translation. English, Chinese and German are chosen because:

- The US is the cradle of cyberspace and cyberlaw: the opening of access to cyberspace for broad layers of international populations originates there. Hence English is the lingua franca⁴⁰.
- China is a pioneer in a governance doctrine that is transforming the nation-state of the past into the “cyberstate.” This is evident in the digitization of the country’s borders (the electronic frontier) as well as its citizens (digital citizens). China goes so far as to subject citizens to a Key Performance Indicator (KPI) system. This nationalization and utilization of people’s digital identity, according to the traditional three-element doctrine (the state is contoured by territory, citizenship, and power), argues for China’s position as a cyber-state pioneer.

⁴⁰ V. Schmid, *Verwaltungsorganisation und moderne Kommunikationsmittel*, in: Kazushige Asada/Heinz-Dieter Assmann/Zentaro Kitagawa/Junichi Murakami/Martin Nettesheim, *Das Recht vor der Herausforderung neuer Technologien*, Deutsch-japanisches Symposium in Tübingen 12. Bis 18. Juli 2004, S. 71-80 (71).

-
- As a result of its history, legal and otherwise, especially in the 20th century, Germany holds experience as “World Privacy Cop” and as a “Privacy Law Watchdog.” Not surprisingly, this background leads to possible backwardness in the digitization (of the state) as a cutting-edge proponent of privacy protection.

Strategy and tactics prepare for the aim of the project:

C. “Fighting Words” before “Weaponization” (prima et ultima ratio)

It is by no means an undisputed and global reality that opinion, media, and cyberspace freedoms are essential for both states and citizens. (This statement moves beyond the fundamental question of whether there are still any democracies or states without cyberspace in 2018.) One detail is the quality and value of the data in cyberspace – and in the US and Germany in particular, hate speech, “alternative facts,” and personality-distorting statements are significant problems. Despite the potentiality and reality of injury with words, it remains clear that disputes and conflicts using words almost as weapons will continue.

V. Prima ratio

Fighting and struggling with arguments and words, however, is prima ratio; sending missiles and “Weaponizing” soldiers and drones is ultima ratio. Ihering’s sentence from the nineteenth century is evergreen as far as it stresses the peacekeeping function of the rule of law. In the words of contemporary European Union Primary Law:

Art. 67 TFEU

1. The Union shall constitute an **area of freedom, security and justice** with respect for fundamental rights and the different legal systems and traditions of the Member States. [...]

Moreover, in 2018, Ihering provides a truism, preparing us for the conclusion that cyberspace as a space structured and supported by technology and energy might also pose the challenge of “the struggle for law” on an everyday basis.

VI. Should we Revisit Ihering in Cyberspace?

Adapting Ihering, the end of struggle has to be clarified in a globalized and digitized society in

the face of cyberspace—the fifth dimension of being (alongside the familiar metrics of the real-world and time). The means to that end, as suggested here, is the following lecture curriculum that attempts to further understanding and debate among globalized cybercitizens. The curriculum for this (online) law lecture course includes fifteen 90-minute units. It comprises outer space law and some additional core scenarios (nuclear energy, data retention, cyber-toys (e.g. the “My Friend Cayla” doll), and drone law). The timing for such a universal (technology) law lecture is relevant because the European continent will undergo a data protection law innovation on May 25, 2018. Data protection law is one core element of technology law, and the German-European perspective opens and forecloses “markets” having 500 million customers and—still—28 states.

The German rule of law with Germany as a so-called “World Privacy Cop” is complemented with Chinese legal expertise by Georg Gesk.⁴¹ However, this lecture strives for open academic innovation and the solicitation of other perspectives. The principle guiding the innovation process is—again—contained in art. 67 para. 1 TFEU: “respect for fundamental rights and the different legal systems and traditions” of others. Crossing disciplinary boundaries as well as bridging cultural gaps and preventing misunderstandings (along with mistranslations) are the challenges. Furthering peace through struggle, including a war of words instead of waging war with force, is the ultimate end.

C. A Chance for a Better Future through Comparative Technology Law (“The Quest of Truth” and “Shared Academia”) – Traffic Communication Data Law

I. Chance for a Better Future through Comparative Technology Law (“The Quest of Truth” and “Shared Academia”)

Combat and war scenarios should be taken into consideration – even if they should never drive us. Using trust as well in people as in the rule of law, which has to prove itself every day, all the time and everywhere, allows us to look into a (better) future that augments the reality around cyberspace (augmented reality) and uses cyberspace to increase opportunities for justice in realworld (augmented virtuality). The old Kant phrase that the rule of law is a prerequisite

⁴¹ Chair for Chinese Law, Faculty of Law, University of Osnabrück, Germany.

for a livable world („[...] denn wenn die Gerechtigkeit untergeht, so hat es keinen Werth mehr, daß Menschen auf Erden leben.“ – see Part 4.E.IV.5) is the guiding principle. And an economized cyberworld in particular demands the return to, and revaluation of, old virtues such as the quest for truth.

Cyberspace and age provide for the option of a globalized and well-informed public opinion building in multinational and multistate audiences. Freedom of expression, speech, media and opinion are prerequisite especially for democracies. These are – or should be - fundamental requirements for scientific processes. Quest of truth⁴² adds an element of quality to decision-making and (global) governance. Regularly the linkage between the quest for truth and rule of law enables us to engage socially with other humans. CYBERTEACHING and –RESEARCH focusing on comparative analysis of technology law opens up for fact-checking and allows for laboratory strategies (such as one nation acquiring expertise with Telecommunication traffic data retention as well as usage for the sake of terror prevention). Hence, because the technology is applied and marketed globally, the technology law of each nation provides **experimental evidence**. This experimental evidence is the experience capital the project wants to realize: one leading scenario is Telecommunication Traffic Data Retention Law:

II. A Quest of Truth, e.g. German-European Telecommunication Traffic Data Retention Law

The economic potential of this search for common ground becomes clear in a transatlantic perspective on one key issue: namely, the right of storage and use of Telecommunication traffic data without cause. From a German and European perspective, that so-called right is a merger of unlawfulness starting from its illegality under European secondary law, moving to its illegality under German secondary law⁴³, to its illegality under Romanian and British secondary law from 2006 to 2018.⁴⁴ The dissemination of knowledge regarding this singular legal question

⁴² Own terminology: The author is well aware that “quest for truth” is grammatically correct as well as regularly used. The preposition “of” is here used to indicate that there might be an a priori truth (that can be found and is preexisting). Furthermore, the notion of “Wahrheit” might be different than the English “truth” and “quest for truth”.

⁴³ Federal Constitutional Court (Bundesverfassungsgericht (BVerfG)), judgment from 3/2/2010, 1 BvR – 256/08 –, 1 BvR – 263/08 –, 1 BvR – 586/08 –; http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html:jsessionid=7CA1C3B2B2758C7366C26925405FB01E.1_cid383 (26.02.2018).

⁴⁴ See Part 4 D slides and further references in: V. Schmid, Vorratsdaten“organisation“ in der Vergangenheit und Zukunft, soon to be published.

in Europe and Germany should have prepared American (legal) science in an abstract and forward-looking manner for the Snowden scenario in 2013, as well as for the “FISA debates” in 2018 following the publication of the “Nunes memo (I)”. It is a current human question: to what extent is a person’s identity digitized? The possibility of an omnipresent and ubiquitous determination monitoring and surveillance of someone’s communication relationships (with others), mediated through machines, and without (probable) cause is a key issue that seems to be addressed **completely differently** in Chinese law than in German-European or American law. This diversity—analyzed in a multinational perspective—prepares for the gigantic challenges for rule of law in cyberspace. If, from a global perspective, regulation differs so widely, it is foreseeable that citizens’ attitudes in the European Union and in Germany will differ as well. Consequently, “class actions” in Germany and legal activists fought for and succeeded in the annihilation/annulment of German and European law in 2010 ff. In short: This unlawfulness paralleled lawlessness because the courts rendered a core area of cyberlaw unlawful and unconstitutional. This law could neither be enforced nor could it exert a lasting influence on entrepreneurial decisions.

III. A Quest of Truth, f.ex. United States: The Declassification and Dissemination of Information Following the “Nunes Memo (I)”

This supplementary perspective explains why the project is so interested in the Snowden revelations of 2013 ff. as well as in the “Nunes memo (I)” – proceedings. At the core of these matters is Telecommunication traffic data collection, retention, processing, and disclosure by transmission: in short, from a European Union perspective on Data Protection law (art. 4 para. 2 General Data Protection Regulation).

Art. 4 GDPR – Definitions

[...] (2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; [...]

American colleagues are much better informed about “FISA law”–the paradigmatic scenario, however, is evident and comparable. May evidence (illegally or wrongfully?) be generated by cyber surveillance and monitoring be used to obtain a warrant in order to obtain further evidence? It is an educated guess that the transparency of cyber surveillance law and warrants will be of importance for the rule of law, security law, digital forensics and governance in the United States in the future as well. Already now (February 2018), Wikipedia⁴⁵ informs readers about the issue and the debate over the declassification of the memorandum of the Democrats. Furthermore, the announcement of further versions of the “Nunes memo (I)” is part of reporting in American media (Rachel Maddow, Tucker Carlson, Sean Hannity...). That is the reason why the project accords Telecommunication Traffic Data Law the status of one paradigmatic setting as well as a common challenge that unifies (cyber)governance around the world. Trailblazing motivation for this global cyberteaching project is the “sale of experience.” Referring to the experience of a third party enables us to avoid sunken cost as well as loss of trust (“If we could sell you our experience and if experience could be marketed like a product”). **This gain of (truthful and therefore valuable) experimental evidence is the chosen trigger for the project.** This scenario, however, is only one paradigm among a bigger agenda contoured in a German publication in 2015.

Part 4: What (II)? A Universal (Technology) Law Lecture Fulfilling a Global Agenda for Cyberlaw (2015)

Establishing and implementing this agenda – following Part 3 (What (I)) – is among the first prerequisites for promulgation in teaching:

A. Universal

A law lecture has to include outer space law because private entrepreneurs want to exercise personal and economic freedoms in this space. For example, Elon Musk recently succeeded in sending an autonomous car in outer space via “Falcon Heavy”. Moreover, the smarter our environment becomes, the more relevant is the control, functionality and integrity of the infrastructure in outer space (such as satellites) for the realworld on earth.

⁴⁵ https://en.wikipedia.org/wiki/Nunes_memo (Stand: 02/11/2018).

B. (Technology) Law and Especially Cyberlaw

This global (cyber)teaching project is exploring a new form of outreach regarding the legal system: It integrates humans and machines, “human updates of machines,” and “digital updates of humans.” Hence, the content focus is not on law in general (such as international business law or human rights law) but on technology law paving the way for (trans)humanity.

I. Technology is the Starting Point and the Starter of the Law Lecture - and not Man-kind

This daring scientific presumption is chosen in order to define the common ground and understanding for comparative legal analysis and teaching. The focus on technology is the path to comparability and interoperability. A laptop, a cellphone, e-policing, e-justice, unmanned aerial vehicles, and other technologies provide similar functionalities and options for a world population (digital divide and digital dividend considered) living in widely different legal systems and different cultural traditions and challenges.

Despite these differences in humankind, they are confronted with identical technological challenges – at least in theory. Consequently, challenges such as man-machine-competition and human surrogates as well as “Legal Technology” (legal robots?) promise experimental capital if governance strategies are researched, analyzed and evaluated.

Summing up: If focusing as a starter on human rights discourses and conflicts, it would be evident **that the object of the discourse is identical with the subject**. The living conditions of a world population differing in race, culture, tradition, legal entities and personalities provide different images. Starting with technology promises different mirrors depicting identical technologies—the same image. This **mirror function** of comparative legal analysis and the detection of distortions as well as attractive reflections is our justification for centering on technology. - whereas comparative analyses of technology law may refer to a common basis—for example, surveillance strategies and technologies that are marketed and implemented worldwide. Consequently, in contrast to international human rights research and teaching, comparative legal analysis of technology law has indisputably the same challenge—the challenge posed by identical technologies. Even more so, if humans are “updated” with technology or interact with machines, those actions might be the common denominator in the future. To summarize: comparative technology law does not exhaust itself in governance culture for human behavior.

Different cultural and legal traditions might mirror these technologies differently while they may have the technology in common, they might not have the culture in common.

II. Cyberlaw as a Proponent of (Technology) Law

Constant and round-the-clock networking is a prerequisite for both the dissemination of our teaching standard and technologies of the future. Hence, cyberlaw is an essential element of the lecture syllabus. Before focusing on technology and especially on cyberlaw, the different ideas of (rule of) law have to be explored as well as ascertained. One of the first steps, taken in 2017, was the design and dissemination of a questionnaire. In order to detect the quality of the mirror in the face of the new technologies as well as societal change, the German initiative (Schmid) designed and distributed the following questionnaire, asking Germans

C. “Law” in a Questionnaire

From a global perspective, it is by no means expected that a common understanding of the origin and meaning of law is widespread. In Germany, therefore, Schmid uses a questionnaire that captures the different informational backgrounds of the students (and others who are interested), analyses the difficulties, and develops the first step toward positioning the lecture vis-à-vis its potential audience.

(1) What does “law” mean to you and what do you want to know about “law”?

[Was bedeutet „Recht“ für Sie und was wollen Sie über „Recht“ wissen?]

(2) Against which risks should “law” protect?

[Vor welchen Risiken soll das Recht schützen?]

(3) What contribution can and/or should “law” make (for the dissemination of technology)?

[Welchen Beitrag kann und/oder soll das Recht (für die Verbreitung von Technik) leisten?]

(4) What is the function and the meaning of “law”...

[Wie sehen Sie die Funktion und Bedeutung des Rechts...]

a) for the development of the European Union?

[bei der Europäische Einigung?]

b) for the withdrawal of Member States?

[beim Austritt von Mitgliedstaaten?]

(5) How do you see the development of drones in the future and how can German and European Union Law contribute?

[Wie sehen Sie die künftige Entwicklung von Drohnen und welchen Beitrag kann das deutsche und Europarecht Ihrer Meinung nach hierzu leisten?]

D. Lecture – Syllabus and Agenda of Priorities in March and May 2017 (Santa Clara and Darmstadt)

One first proposal for the lecture project and syllabus was presented at the last Internet Law Works in-Progress conference in March 2017 and in a lecture with a transdisciplinary audience in Darmstadt, Germany, in May 2017. These premieres in the US and Germany assumed a timeframe of fifteen modules with 90 minutes each.

The slides and the text of **the oral presentation in Santa Clara** are part of the step-by-step strategy of the project (anyone interested in the much more elaborate German slides of May 2017 may contact Viola Schmid). Please note that this contribution dates from 2017 and will be updated before further publication and further dissemination.

“Dear ladies and gentlemen,

A. “Time waits for nobody“, Art. 67 TFEU with a content focus on “**securitization**”



Freddy Mercury:

“We've got to build this world together;
Or we'll have no more future at all [...]
You don't need me to tell you what's gone wrong [...]
You know what's going on;
But it seems to me we've not cared enough
Or confided in each other at all [...]
It seems that we've all got our backs against the wall [...]”



Art. 67 Treaty on the Functioning of the European Union (TFEU)

The Union shall constitute an **area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the (VS: 28) Member States**. [...]

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 1 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



Thanks for staying with me late in the afternoon, and thank you Eric Goldman for inviting me to this wonderful conference. Coming from Germany, I am not a native speaker and beg your pardon for sometimes not passing the language barrier very elegantly. Today, I would like to solicit your input for my dream lecture—a universal technology law lecture. As a hymn for this lecture I have chosen Freddy Mercury: ...Perhaps you are familiar with the fact that Germany has special experiences with The Wall (*die Mauer*) separating East and West Germany for 28 years (1961—1989). Perhaps you recall President Reagan (6/12/87) ordering: “Mr. Gorbachev, tear down this wall”.

Living in peace and security without a wall and borders has motivated me to focus on “securitization” for my dream lecture, with the support of art. 67 of the Treaty on the Functioning of the European Union—as an area of freedom, security and justice with respect for fundamental rights and different legal traditions. And “Securitization” (my own terminology) is my choice because I think that we can “fight” each other as competitors competing with our products and services on global markets, but that we need each other in connected worlds to further an area of freedom, security and justice for the sake of humanity.

A. “Time waits for nobody“, Art. 67 TFEU and content focus on “securitization”



→ VS content focus on “Securitization”: In a world of “CAA” (Computing Anywhere Anytime) we might compete with our products and services in (universal) markets, but we have to cooperate – **we need each other** – in order to further an area of freedom, security and justice (for the sake of humanity).

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 2 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



Time waits for no one—I am 56, and I am determined to choose a step-by-step approach for the design of my dream lecture. The third of 19 minutes is already invested, and you see that this is my statistical life expectancy and the time slot for the lecture. The question mark indicates that I need your input. Do you think fifteen modules of 90 minutes each are a good idea? Following the motto: as much law as necessary, as little law as possible?

Time management for the outcome after 19 minutes is your critique in order for me to follow up from this version 0.1 to version 1.0 of the canon.

B. Time for a Canon for a Universal (Technology) Law Lecture - Version 0.1



- (1) **My time (management):** 3rd of 19 minutes / 83 years of life expectancy / 30.514 days / 732.336 hours / 19 minutes are 0,00000044 % of my statistical lifetime
- (2) **Time slot** for the lecture: **15 modules of 90 minutes** following the motto “As much law as necessary- as little law as possible” in order to pave the way for **CYBERSCIENCE** (furthering “securitization”)
- (3) **Time Management** for the **outcome** after 19 minutes: Your feedback and critique for drafting a **Version 1.0** following this presentation

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 3 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



C. Why a universal technology law lecture with a focus on “securitization“?



Universal: My hometown – Darmstadt, Germany, Europe – is home of [European Space Operations Centre](#), hence my universal, transdisciplinary perspective

We need to include International (Space) Law because cyberspace infrastructure (also relevant for the realworld as a consequence of digitalization) is in space (satellites,...).¹

¹ See soon Schmid as a contribution to the discussion in: *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer (VVDStRL), Grenzüberschreitungen (2017)*

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 4 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



What is the reason for my universal perspective?

My hometown is Darmstadt, Germany, and it is the home of the European Space Operation Center. I brought you a photo of Germany from space, and I think we need to include the international space law in the lecture because cyberspace infrastructure is relevant for the realworld as well as for cyberspace: the satellites in space make decisions about the infrastructure on earth. So, we need a new transdisciplinary approach that includes international law and a universal—and not only a global—perspective.

C. Why an universal technology law lecture with a “**securitization**“ focus?



- “**Securitization**“: (IT) Security is not a status but a process, demanding permanent engagement, reflection and readiness for change as well as rebuttal (VS). “**Securitization**“ is a cybernetic approach allowing cross-border analysis of realworld and cyberspace and vice versa. The motto is: There is no Security without IT Security and there is no IT Security without Security.
- “**Herstory**“ (VS): Female pioneer in public law (*veniae legendi* in German Public Law, Energy Law and European Law) – “Staatsrechtslehrerin“ – securitization as governance challenge
- **Historical reasons** (Germany - especially 1933 – 1945: The „PERFECTION OF LAWLESSNESS“ (VS))

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS“ | 5 | “INTERNET LAW Works-in-Progress“ 2017 / 19 minutes



I see securitization as the first priority, and I have chosen a cybernetic approach stating: There is “no security without IT security and no IT security without security”.

For a constitutional law professor (*Staatsrechtslehrerin*) like me, securitization is a challenge for governance and, coming from Germany, our history tells us: security is of utmost importance (remember the Third Reich). Hence, it is not surprising that Germany is a world pioneer in (IT) security law. And, since you now know my personal and historical bias, I want to share another argument with you. It is a new methodology for this lecture—I call it LEXONOMICS, which combines law and economics.

C. Why an universal technology law lecture with a “**securitization**“ focus – LEXONOMICS?



LEXONOMICS (methodology combining law and economics)¹ in order either to teach:

- “bn € scenarios” and/or to find
- national legal cultures (see Art. 67 TFEU) with potential for Creative Destruction² (“Schöpferische Zerstörung”) / Disruptive Innovation

In a nutshell: As little law as possible - what are the financially and/or intellectually challenging scenarios that need to be mastered? VS: **Germany as a world pioneer in (IT) Security Law** – three pilots positioning law against/with economic entrepreneurship

¹ LEXONOMICS in the context of (IT) Security law, see New “E-Justice” Law in Germany since 2013 – A Temple Architecture for an “Agenda of Securitization”, in: [Report from Dagstuhl Seminar 14092 “Digital Evidence and Forensic Readiness”](#), Edited by G. S. Dardick, B. Endicott-Popovsky, P. Gladyshev, T. Kemmerich, and C. Rudolph; S. 163 – 167
² “Creative Destruction” (“Schöpferische Zerstörung”) in the Schumpeter sense, see Schumpeter, “Capitalism, socialism and democracy”, 3 rd. ed., 1950

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS“ | 6 | “INTERNET LAW Works-in-Progress“ 2017 / 19 minutes



So, I have tried to identify and consequently to teach either the “billion Euro scenarios” on the one hand, and/or national legal traditions with the potential for creative destruction and disruptive innovation for law and legal theory on the other hand.

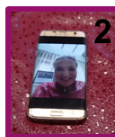
So, one selector is economic importance, and the other selector is the intellectual challenge for comparative legal analysis. What do I—you see the acronym “VS”—have to offer?

I brought with me three pilots (in the sense of paradigmatic scenarios) of German-European securitization law. The idea is to prove to you the quality/value of my selection, as well as to invite you to supplement the structure with input from your own jurisdictions. My scenarios are meant to form the nucleus and format for comparative legal analysis within the framework of this universal law lecture.

D. Nuclear Energy, TDOs and “CAA” child toys prohibited under German law (in the future)?



“Securitization” in German Nuclear Energy Constitutional Law (four Court decisions): As early as the 1970’s, complainants feared that nuclear energy would change society into an Orwellian state



“Securitization” via traffic data organizations (TDO) Decisions by the highest German Court (34.000 complainants) and the European Court of Justice led to a “maximum credible accident” (MCA) for German and European cyberlaw from 2010 to 2016.



“Securitization” in the nursery: “Cayla” is a doll that can access cyberspace anytime anywhere (CAA computing). The administration is trying to prohibit the sale of this “camouflage spyware” (§§ 90, 115 German TKG) [as of 02/17/2017](#)

Image source 1: <http://www.cloud-computing-koeln.de/my-friend-cayla-eltern-muessen-puppen-ihrer-kinder-zerstoeren/>
Image source 3: Photographer: Armin Kübelbeck, CC-BY-SA, Wikimedia Commons

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 7 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes

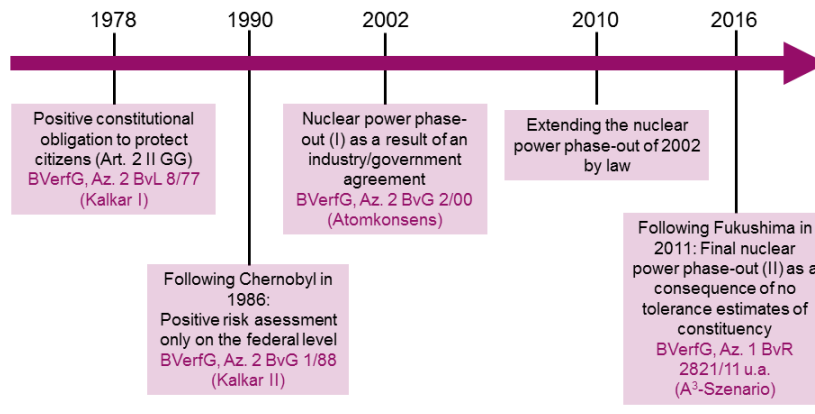


In a nutshell: I would like to share with you that, under German law, we currently have a phase-out in nuclear energy (which entails compensating the nuclear industry, which is at dispute in the “Vattenfall case” at the International Centre for Settlement of Investment Disputes [ICSID]). We have not mastered the “Telecommunication traffic data organization” challenge for German and European law—you recall the “Snowden revelations” from the US perspective and two weeks ago, an interactive children’s doll was banned as camouflage spyware by German Federal authorities (*Bundesnetzagentur*).

I mentioned that Germany is an IT security law pioneer from a global perspective. I do not want to argue for or against this, but I think reporting truthfully is of value in itself. In order to back

up my report with facts, I brought some slides with timelines with me. But I only offer them here at the moment—for the sake of your valued input—for browsing.

D. 1. “Securitization” – Nuclear Energy and four court decisions



03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 1 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



So, in short, regarding nuclear energy constitutional law: as early as 1970, people in Germany feared that nuclear energy would change society into an Orwellian-State. And I would show you, citing the decision of the *Bundesverfassungsgericht* (Federal Constitutional Court) in 2016 that the fear of a lack of support for this high-risk technology in the constituency became a legally accepted argument as part of the proportionality test that the phase-out law had to pass.

D. “Securitization” – “Traffic Data Organizations” and MCA



- “Data” are defined as in Art. 4 Sec. 1 General Data Protection Regulation (EU 2016/679)¹: ‘personal data’ means [...]
- “Traffic data” are defined as in Art. 1 sec. d Cyber Crime Convention: “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.
- “Organization” as a superordinate concept for various strategies and technologies, such as processing, collecting, transmitting, recording, etc. compare Art. 4 para 2 GDPR 2016/679.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

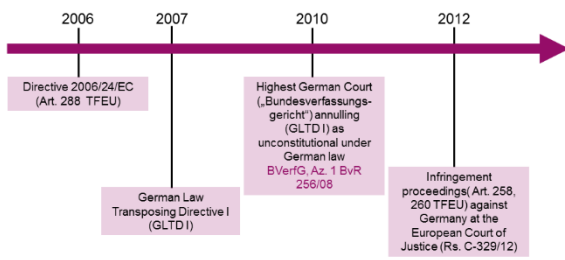
² Convention on Cybercrime, 23.11.2001, CETS No. 185

³ It is noted, however, that Schmid’s data organization terminology differs from the regulation, because “organization” here is the terminology for the superordinate concept, whereas the regulation cites “organization” as a mean of “processing”.

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 2 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



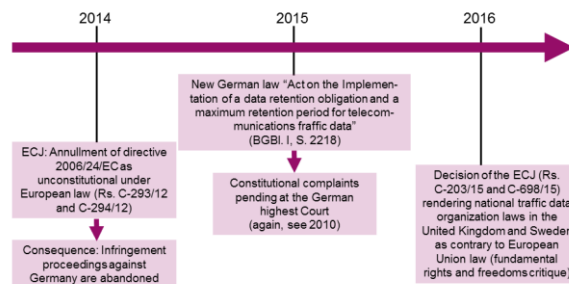
D. “Securitization” – “Traffic Data Organizations” and MCA



03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 3 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



D. “Securitization” – “Traffic Data Organizations” and MCA



03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 4 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



And briefly to traffic data organization law: starting in 2006, and after more than a decade, German and European Union law allows for no legal certainty (*Rechtssicherheit*). Moreover, this cyberspace challenge led to a maximum credible accident experience for me. Not only a European directive, but also German law transposing the directive was rendered invalid by the European Court of Justice in 2014 and the highest German court in 2010. Moreover, Germany subsequently had to face infringement proceedings at the ECJ in 2012.

And briefly to the doll “My friend Cayla” and this idea of prohibiting spyware in nurseries: I do not see that it is feasible for the sale of such a doll to be prohibited elsewhere—or do you see this differently?

D. “Securitization” – “CAA” child toys



A global analysis shows: High risk technologies such as nuclear energy (1) and traffic data organizations with a (purportedly) high potential for enhancing security in cyberspace age (2), and digital natives communicating with “spyware” in their nurseries add as “disruptive innovation” or “creative destruction” the



to the quality of (national) “securitization” LAW (“Wesen des Rechts”).

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 5 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



The idea for comparative legal analysis—nuclear energy plants, traffic data organizations and interactive dolls are scalable and comparable products—reveals the underlying fundamental question: Is it law that decides cyberlaw or “different legal traditions and philosophies?” May I

remind you of article 67 TFEU, “respecting different legal traditions of member states,” and here, the last question is thrust upon us: Is law and are lawyers sufficient, or do we need to pave the way to CYBERSCIENCE by allowing more than pure legal arguments to be taken into account and to open up to other disciplines? I end with my initiative “Go to the core!”⁴⁶ (an acronym for **g**overnance **c**ompliance and **r**egulation) and hope that such a dream lecture will become reality.”

E. Outcome and GoCore!



Your input to:

- time management and
- content management with focus on “securitization” and a universal perspective

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 6 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



E. Governance, Compliance & Regulation¹ ?



Last but not least: Following R. Susskind’s analysis “The End of Lawyers”²: Do you agree that we need this lecture in order to pave the way and bridge gaps between disciplines in order to foster CYBERSCIENCE, allowing (as in this pictogram) considerations of automation, effectiveness and efficiency potentials, law and the balancing of opportunities and risks?



¹ Research initiative „Governance, Compliance & Regulation“ (GoCore!) at Technical University Darmstadt, Germany
² R. Susskind, “The End of Lawyers”, 2008

03/04/2017 | Prof. Dr. Viola Schmid, LL.M. (Harvard) – “VS” | 7 | “INTERNET LAW Works-in-Progress” 2017 / 19 minutes



This presentation in Santa Clara promulgating the idea of global cyberteaching is part of a greater agenda first drafted in February 2015 and published in German in 2016.

E. The 13 Basics of a (Global) Agenda for Cyberlaw (the Perspective of a European-German Cyberlaw Professor – a Text Dating from 2015, Published in 2016

I. Pioneering in Cyberspace – an Agenda for Cyberlaw

Personal motivation and research instruments are justified through results, not only through pronouncements. Therefore, as agenda-setting and prioritizing needs for the execution of research can multiply quickly, we must handle them all with the same level of quality as our previous work, according to the phrase “as soon as possible and as best as possible (ASAP and ABAP).”

⁴⁶ Die Forschungssäule „Governance, Compliance & Regulation“ (GoCore!); <http://www.gocore.wi.tu-darmstadt.de/start/index.de.jsp> (21.02.2018).

“The goal of these basics is to further a consensus among globally engaged scientists about the most fundamental common ground regarding the challenges of cyberspace. Thirteen (13) basic theses should act as bridges for discourse between representatives of various disciplines and members of various nations. Twelve of these theses can be characterized as abstract, top-down questions that can serve as the point of departure for global comparative cyberlaw. One basic assumption (no. 12) supplements the top-down approach with a pilot scenario that depicts the bottom-up approach, with the goal of “glocalisation” from a local perspective. This is a puzzle piece in the e-Governance movement in Germany—namely e-Justice (with legal technology, e-Administration and e-Legislation). The contribution attempts to outline the challenges currently (2015) being discussed in Germany in order to bolster comparative analysis with other legal systems. Both the experience advantage of other legal systems (time management), as well as the awareness that the digitalization of the courts is a core function in the search for justice, are motivation for the selection of this pilot.

The leading bifurcation question will again be:

- How does the technology of cyberspace influence and change our traditional legal ideas and ideals about content?
- To what extent does our traditional view of justice change through digitalization?

II. 13 Basics in a Nutshell

- I. GNC Formula (Global Networking and Competition) on the one side, automation and man-machine interaction on the other
- II. New and/or other ideas about freedom of expression, protection of personality and privacy and new conceptions of truth.
- III. Imminent “Clash of Civilizations”?
- IV. The necessity of building (global) discourse bridges and the legal establishment of (global) minimum standards
- V. Only cyberlaw makes cyberspace a cyberworld
- VI. Analysis: Securitization of cyberspace and the realworld as unprecedented challenges in the history of mankind
- VII. The status quo is the transition period
- VIII. Malfunction Management (MaMa) – an example from European legislation

IX. (IT) Security (law) as an equivalent to the rule-of-law principle in the traditional law of the realworld, and the challenges for IT security

X. Jurisprudential and legal-political strategies (new efforts are necessary)

XI. “Legal information technology circular thought process”

XII. Pilot: (Global) Comparative technology law in “e-Justice” – a template architecture for securitization

XIII. Sustainability through (future) cyberlaw in its significance for the Cloud with respect to content and technology

III. “Law on Content of Expression” and “Law on Technology of Expression“ in its Haziness in Cyberspace

A bifurcation of our perspective into **law on content of expression** (German: *Äußerungsinhaltsrecht*) and **law on technology of expression** (German *Äußerungstechnologierecht*) is essential. It should be highlighted that both the content of cyberspace as well as the technological infrastructure tend toward fuzziness. With regard to content, the distinction between blasphemy and disparagement of government bodies and freedom of expression is difficult—particularly when the law demands global validation (e.g. France: “Charlie Hebdo” and USA: “The Interview/Sony” scenario). With regard to technology, cyberspace, with its tendency toward the Cloud, threatens to withdraw itself from the obligation to state and union compliance with the law. In summary: Not just the content of cyberspace is difficult to manage in its interpretation and legal appraisal, but also the technological structure that tends toward a lack of definability in external appraisal. This haziness—symbolized in a figure through clouds and sun (see under IV, XII and XIII – “E-Justice”)—requires cooperation with representatives of the technological sciences on the one hand, who we have to thank for the framework of cyberspace, and, on the other hand, a new humility in legal sciences, which must incorporate the boundaries of the law (the existence of non-law) into their methodology. This agenda for cyberlaw tries to pave the way to a new discipline of science – cyberscience.

IV. 13 Basics Illustrated (2015) and not Updated as a Way toward Cyberscience (2018)

The goal of this agenda for academic open innovation is and was to further a consensus among

globally engaged scientists about the most fundamental common ground regarding the challenges of cyberspace. **Cyberlaw, as it is understood here, is the law of the distribution of chances and risks, rights and obligations in cyberspace** (and realworld). Cyberspace supplements and partially replaces the realworld previously known to the legal tradition. These legal traditions that have been carried to the old continent since before the Romans will be called “**traditional law**” in the following. From the perspective of a female law professor also trained in European and German (traditional) law, the following thirteen basic challenges exist for local and global (glocal)

- science (and jurisprudence) and
- (legal) policy.

The author is convinced that the law is *conditio sine qua non* for the development of cyberspace into a cyberworld. For this reason, the consensus of a globally thinking jurisprudence on the status analysis and the challenges is a prerogative in order to master the challenges that lie ahead and to protect the world we leave behind (Idea of Sustainability – art. 20a German Basic Law (GG)). The following thirteen basics hopefully serve as a common ground for the first steps. They were first designed in 2015 and are not updated in 2018. The renouncement has two reasons: (1) The date of origin and actuality of this agenda proves the validity of the strategy and (2) Germany and the European Union presently 2/2018 are at the threshold to new data protection law. From a German-European perspective we live in data protection law transition times (see under Part 6 E).

1. GNC Formula (Global Networking and Competition) on the one Side, Automation and Man-Machine Interaction on the other

One of the consequences of technical networking is the almost immediate, international competition for future life prospects, to which nearly all people are subject. In the following, the term “international” will be replaced with “global” (or “glocal” in its local connection, as a portmanteau of “local” and “global”), because, according to current estimates, cyberspace has not just international, but also global potential. However, it is not just people at one production location competing with people at another production location, but rather also manpower competing with “machine power” (automation scenario). Not only incremental pattern recognition, but also opportunities for robotics pose the question: to what extent should a functional caveat

in favor of human activity or passivity be anchored by a society governed by the law (“reservation for human occupation”?). The fact is that **global networking, competition (“GNC Formula”)** and automation have, as their consequences, chances, risks and dangers for the future. Additionally, there is man-machine interaction in the broad sense. As the German Federal Constitutional Court recognized in 1983, machines possess the potential to model and to monitor behavior patterns. This thesis, well known in Germany and Europe, states: [...]

BVerfGE – „Volkszählungsurteil”⁴⁷

“A social order in which individuals can no longer ascertain who knows what about them and when and a legal order that makes this possible would not be compatible with the right to informational self-determination. A person who is uncertain as to whether unusual behavior is being taken note of at all times and if that information is being permanently stored, used or transferred to others will attempt to avoid standing out through such behavior.”

Also, Jaron Lanier emphasized in 2014:

“Without people, computers are space heaters that generate models [...].”⁴⁸

In short: **Model Design, Pattern Recognition & Surveillance** are essentials as well as opportunities in cyberspace (“MDPRS-Formula”).

The challenge from 2015 to the present is: how do we cope in the ubicom world with these traditional law principles? Moreover, these human-machine competition scenarios are not limited to the private sector. Even federal legal systems are increasingly subject to global competition: on the one hand, what will happen if citizens flee from their own legal system and its enforcement (“Avoidance Scenario”—as in the past in tax law)? On the other hand, what if citizens make a (well-informed) choice for another legal system, for example in their commercial activities (“Forum Shopping” in the broader sense)?

The immediate competition of the states with one another should also be highlighted, as their “digital identities” in cyberspace can be more easily valued comparatively (in the representation of the self and others, as well as within inter- and/or supranational institutions).

⁴⁷ BVerfGE 65, 1, 43 – „Volkszählungsurteil”, Az. 1 BvR 209 u.a./83, v. 15.12.1983, Rn. 154; for another inauthentic translation see J. Bröhmer/C. Hill (Eds.), 60 Years German Basic Law: The German Constitution and its Court Landmark Decisions of the Federal Constitutional Court of Germany in the Area of Fundamental Rights (2010).

⁴⁸ J. Lanier, Frankfurter Allgemeine Zeitung (FAZ) v. 13.10.2014, S. 1 (translation by the author).

Despite all the challenges, the goal is always to internalize the advantages of cyberspace. For the first time in the history of humankind, the opportunity exists to enter into (real time) person-to-person communication worldwide and to form international, European, and/or global opinions. Consequently, we also have to deal with new challenges.

2. New and/or Other Ideas about Freedom of Expression, Protection of Personality and Privacy and New Conceptions of Truth

As a rule, the existence of cyberspace requires a bifurcation of the perspective on “freedom of expression” into “the law of content of expression” and “the law of technology of expression.” This situation concerns a still-new technology, and it must focus on the content that is generated and/or disseminated using this technology. Fundamentally, it must be clarified how the traditional freedom of expression of the (paperbound) realworld can develop legally into global electronic cyberspace. Furthermore, it needs to be stated that the participants in cyberspace will be confronted with different freedoms of expression and liberties due to the globality of the medium. It should be assumed that especially the breadth of dissemination allowed for by the technology has the potential in individual cases for conflict over the content.

3. Imminent “Clash of Civilizations?” (The France: “Charlie Hebdo” and USA: “The Interview/Sony” Scenarios of 2015)

Associatively, there may be different concepts of laws of expression, in a global perspective, regarding the caricature and criticism of religious communities and (foreign) ruling bodies. With the emergence of a global cyber-audience (global public opinion), these “legal and religious cultures” compete with one another—perhaps primarily in cyberspace because networking through cyberspace makes the different concepts clear and communicates them to a wide public. The consequences—in the case of “The Interview/Sony” an “information war”; in the case of “Charlie Hebdo” the murder of the authors—are evocative of the literary predictions of the “clash of civilizations.” For this reason, it is strategic to promote

4. The Necessity of Building (Global) Discourse Bridges and the Legal Establishment of (Global) Minimum Standards

The previous basic principles already prepare one for the pioneer challenges of the formative function of law in the cyber-world. At least five bridges should therefore be “built” or extended:

- Bridges across spaces (cyberspace, realworld, cross-border issues)
- Bridges between disciplines (“Law and Techies“)
- Bridges between generations (digital natives and immigrants)
- Bridges between science and practice and
- Bridges between “pro-cyber-protagonists” and “anti-cyber-protagonists”.

In the center are the “Minimum Standards” that offer opportunities as the crucial common ground for the effective and efficient implementation and enforcement of (cyber)law.

The “interoperability” of not just technical systems and legal power (legislative, executive, judiciary), but also the “netizens,” is a prerequisite for the qualitative mastery of the challenges of “securitization.” Securitization (*Versicherheitlichung*) is necessary, because cyberlaw does not have a comparable quality of experience with cyberspace as traditional law has had for thousands of years with the realworld. However, cyberlaw and traditional law have formative potential in common. In particular, the recent history of the European Union has shown that only a legal community is capable of organizing the economic and social coexistence of 28 member states and over 500 million people. What holds for the realworld could or should form the basis for turning cyberspace into a cyberworld.

5. Only Cyberlaw Makes Cyberspace a Cyberworld

Cyberspace, as a space created by technology, is the fifth dimension of being, alongside the familiar cubic meters of the realworld and time. Cyberspace opens new opportunities—as well as new risks—for freedom and security. In the past, traditional law has helped shape the realworld.⁴⁹ Living space became a world worth living in. In cyberspace, we possess neither comparable knowledge about the potential for the creation of law, nor do we know the regulatory

⁴⁹ Kant, „[...] denn wenn die Gerechtigkeit untergeht, so hat es keinen Werth mehr, daß Menschen auf Erden leben.“ (Kant, Die Metaphysik der Sitten, Erster Abschnitt „Das Staatsrecht“, E. „Vom Straf- und Begnadigungsrecht“, Zeile 01 – 03, S. 332, Onlinequelle: <http://www.korpora.org/kant/aa06/332.html>, Abruf am 26.02.2018); „Dieser Vernunftidee einer friedlichen, wenn gleich noch nicht freundschaftlichen, durchgängigen Gemeinschaft aller Völker auf Erden, die untereinander in wirksame Verhältnisse kommen könnten, ist nicht etwa philanthropisch (ethisch), sondern ein rechtliches Princip.“ (Kant, Die Metaphysik der Sitten, Dritter Abschnitt „Das Weltbürgerrecht“, § 62, Zeile 06 – 09, S. 352, Onlinequelle: <http://www.korpora.org/kant/aa06/352.html>, Abruf am 26.02.2018); „Also sind es drei verschiedene Gewalten (potestas legislativa, executoria, iudiciaria), wodurch der Staat (civitas) seine Autonomie hat, d. i. sich selbst nach Freiheitsgesetzen bildet und erhält. - In ihrer Vereinigung besteht das Heil des Staats (salus reipublicae suprema lex est); worunter man nicht das Wohl der Staatsbürger und ihre Glückseligkeit

potentials beyond its boundaries (“non-law”). As long as we do not possess this certainty, uncertainty that demands securitization threatens us. Cyberlaw, the law of the distribution of chances and risks, rights and obligations in cyberspace, can offer a contribution toward establishing legal certainty, and shape cyberspace into a cyberworld.

6. Analysis: “Securitization” of Cyberspace and the Realworld as Unprecedented Challenges in the History of Humankind

a) Cyberspace Immediately Affects Everyone

Cyberspace, with its ideal, social and economic potential—such as the creation of cross-border public opinion, establishing and maintaining global contact with others and global invention, sales and marketing of products (goods and services)—seems like the discovery and settlement of a new continent or a new planet. Unlike previous generations of pioneers, nearly everyone is affected by cyberspace, and not just seafarers (Columbus) and astronauts (in the moon landing). These particular directly affected chances for globality differentiate cyberspace from the traditional acquisitions of space. Additionally, the affectedness of so many quantitative components does not solely explain the complexity of cyberspace from a legal perspective. There are also qualitative components, namely the current coexistence between cyberspace and the realworld.

b) 2015 ff.: A Hybrid World Paralleling Cyberspace and the Realworld

Because cyberspace is not connected to the realworld without media discontinuity, chances for efficiency are currently being lost. This is always the case when, in a hybrid view, there are “doublings”—for instance, when documents are transmitted electronically and in hardcopy, or transmitted electronically but printed out by several different people. The coexistence of both spaces may then lead to new, unprecedented redundancies. An example from German e-Administration and e-Justice: The idea of gaining efficiency through cyberspace (paperless

verstehen muß; denn die kann vielleicht (wie auch Rousseau behauptet) im Naturzustande, oder auch unter einer despotischen Regierung viel behaglicher und erwünschter ausfallen: sondern den Zu-stand der größten Übereinstimmung der Verfassung mit Rechtsprincipien versteht, als nach welchem zu streben uns die Vernunft durch einen kategorischen Imperativ verbindlich macht.“ (Kant, Die Meta-physik der Sitten, Erster Abschnitt „Das Staatsrecht“, § 47, Zeile 06 – 14, S. 318, Onlinequelle: <http://www.korpora.org/kant/aa06/318.html> (26.02.2018).

administration) is, at least in Germany, not currently implemented, with the widespread coexistence of paper and electronic administration (hybrid organization). It goes without saying, that, all in all, these redundant hybrid organizations cost more time and money than the two “worlds” alone. For Germany, it should be therefore stated: At present, the paperbound real-world administration has not yet been bid farewell by cyberspace. This process requires a transition period.

7. The Status Quo is the Transition Period

Currently, and in the near future, transfer processes between realworld and cyberspace will occur for the first time in the history of humankind. These transfer processes will lead to a shift and expansion of realworld expressions of freedom in cyberspace. In this transition period, we must accept that pragmatic solutions will be sought but not always found, and therefore, precautionary management is required. For instance, precautionary management of the type that incorporates the temporary failure of information and technical systems in project and application management is included. The strategy recommended here is:

8. Malfunction Management (MaMa)

The digitalization of the realworld is an innovation project that is highly challenging, and of course not just in Germany, because the number of users in the public sector is significantly larger than in the private sector. In addition to this quantitative argument, a different expectation of quality in the public sector in Germany plays a major role. Therefore, largescale information-technological projects in the recent past, such as the electronic healthcare card or the electronic income statement (ELENA) threaten to fail or have failed in Germany. Even if digitalization is successful—when the “if” is overcome—the challenges of a high-quality treatment with the dysfunctions that accompany its application still arise—the “how.”

An example from legislation: For an essential need, such as the publication of legal norms, European and German legislative bodies take precautions should the electronic publication (for technical reasons) not proceed properly. The European Union and German laws consistently include provisions in the case of deficits in electronic publication that allow access to the

paper world (Malfunction Management)⁵⁰. Such a return to traditional forms of communication, which are often paperbound, is called a hybrid strategy here. Basically, such precautionary management should be required without being determined *ex ante*, if it is a hybrid and/or other strategy (such as reinstatement). Even in the aspect of “malfunction management,” the paramount importance of IT security for the (legal) organizations of cyberspace is clear.

9. (IT) Security (Law) as an Equivalent to the Rule-of-Law Principle in the Traditional Law of the Realworld, and the Challenges for IT Security

a) No Security without IT Security = (IT) Security

“IT” is placed in parentheses before “security” to illustrate at all times that, from the perspective of cyberlaw, security without IT security is unthinkable at the beginning of the third millennium, nor can IT security be guaranteed without the presumable integration of the realworld component of human beings (“Snowden scenario,” “Wikileaks,” ...).

b) (IT) Security as a Prerequisite for the Organisation of Cyberspace and the “Principle of IT Security” as a Component of German Constitutional Law

Cyberspace is energy-dependent and prone to attack. IT security (law) is *conditio sine qua non* for freedom, security and justice (Area of freedom, security and justice – art. 67 TFEU) – even in cyberspace. This highlighted importance of technological quality should, in the future, be echoed at least in German law, if not also in constitutional law. Therefore, a “principle of IT security” is proposed *de lege ferenda*—as is known in German law for the rule-of-law principle. Comparable with this principle of clarity of standards and definition of standards in the German constitution in traditional law (Rule of law – art. 20 abs. 1, 3 and art. 28 abs. 1 s. 1 German Basic Law (GG)), (IT) security is the legal constituent of cyberspace—in particular when the three governing authorities largely decide to impart justice to the citizens and demand obligations from the citizens only electronically (e-Governance).⁵¹

⁵⁰ Art. 3 Regulation EU Nr. 216/2013 of council from 7.3.2013 on the electronic publication of the official register of the European Union, OJ L 69/1 from 13.3.2013 or § 8 Publication and Notification Act.

⁵¹ Necessity of information technology in e-Justice – §55d Code of Administrative Court Procedure (VwGO) at the latest until 01.01.2022 – “Informationstechnologiezwang”.

c) (IT) Security Level Must be Determined as an Accessory to the Legal Application – and not (just) Economically

Traditionally, (IT) security in German and European secondary law is located in the context of the protection of

- Personally Identifiable Information (Germany – § 3 Abs. 1 BDSG-2015) and
- with the caveat of an economical cost-benefit evaluation (IT-Security & cost-benefit ratio – Germany – § 9 S. 2 BDSG-2015).

The European Court of Justice Decision from 08.04.2014⁵² and the German Federal Constitutional Court Decision from 02.03.2010⁵³ indicate an abandoning of this caveat of cost effectiveness. Both the decision of the European Court of Justice, as well as the decision of the German Federal Constitutional Court on data retention, require a particularly high IT security standard for certain applications (sector-specific for the organization of telecommunication traffic data). Even the more recent German legislative policies for an “IT security law” are trying to define “minimum standards,” thereby detaching themselves from the idea with the caveat that financing of the IT security level should be by the provider. Traditional, normative cost-benefit models (for instance § 9 S. 2 BDSG) therefore require revision—new research in accordance with legal dogma is being promised, which carries the title LEXONOMICS.

d) Cyberattacks as Technological Enforcement Strategies (The Interview/Sony Scenario)

The significance of (IT) security—or lack of (IT) security—becomes clear in cyberattacks, in which content limitations (law on content of expression) should be enforced and for which legal avenues with this objective are unavailable. It is simply inconceivable that a court outside of North Korea would have banned the distribution of the film “The Interview.” It was evident that the goal of the cyber activists was to discourage the film distribution company from circulating the film through technological leakages. From a legal perspective, it should be noted: The

⁵² Requests for a preliminary ruling concern the validity of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Judgment of the Court of 08.04.2014 in joined cases C-293/12 and C-594/12, Digital Rights Ireland und Seitlinger u. a.

⁵³ Data „retention“ decision – Vorratsdaten,„speicherungs“-Entscheidung vom 02.03.2010, Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 German Federal Constitutional Court.

information technological security breach and the unauthorized publication of foreign content of expression in cyberspace (“The Interview/Sony scenario”: confidential email traffic) is a strategic instrument for attaining outcomes that cannot legally be enforced. In a nutshell: Technology replaces and/or supplements the legal system in enforcement according to the mottos: “No justice without technology” or “Justice through technology.”

From a German perspective, it should be added that both federal level and States want to sanction tax evasion by German citizens using comparable strategies. In this respect, the German States pay people who, for instance, copy data in foreign banks without authorization. The purchase of these data is a prerequisite for the enforcement of tax law—either through self-reporting by tax evaders or for the execution of penal proceedings for tax fraud and other tax offenses. Furthermore, this German strategy is a motivating element for a change in international tax law. The growing chances to enforce laws through cyberspace pose for the legal sciences—possibly sometimes in competition with the technological sciences—unprecedented challenges.

10. Jurisprudential and Legal-Political Strategies (New Efforts are Necessary)

On the basis of a few questions, the following will demonstrate which functions jurisprudence acting with a global perspective can and/or must perceive.

a) New/Old Task for Global Jurisprudence? – The Question of Experts (Art. 38 Para. 1 Lit. d ICJ-Statute)

The aforementioned basics already illustrate the dynamics and the complexity of (global) challenges that affect the realworld with experience in traditional law. It is foreseeable that a legal dogma structured with traditional public law and perceivable political borders, which also domestically builds on federal models for division of power, cannot master these challenges. From a German perspective, it must be noted that the federal division of Germany is constitutionally prescribed for eternity (inviolable core of German constitutional identity – art. 79 abs. 3 German Basic Law (GG)). The German constitutional law has only recently begun to reflect that domestic borders are not good for cyberspace (infra-structure of German federal networks – Art. 91c German Basic Law (GG)).

This description and prediction of the difficulties for legal policy highlights a new—or old —task for legal science across the globe. This is the chance for legal experts to contribute to cyberlaw (traditional law expertise – art. 38 para. 1 lit. d Statute of the International Court of Justice).

Art. 38

1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: [...]

d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law. ...]

b) New Concepts of Protection (for Instance Privacy Impact Assessments (PIA)) –

The Question of Methods

Not just the question of the “authors” of law will be reexamined (see above under a)), but also the organization of legal protection. If traditional law is largely shaped by the reactive sanction system, a global cyberlaw may require bottom-up approaches that proactively and locally implement, for example, Quadriga Legality, (IT) security & privacy by design.

The European RFID law could be groundbreaking, as it aims to use so-called PIAs (Privacy Impact Assessments) since⁵⁴ 2009 in a recommendation. It should be pointed out that this recommendation⁵⁵ should be made applicable using a framework⁵⁶ created by the private sector (several companies). What is clear: Cyberlaw in a global perspective could search for new authors (experts) and put new methods (PIAs) to the test. Additionally, new terminological challenges arise with global demand.

⁵⁴ History: S. Spiekermann, The RFID PIA- Developed by Industry, Endorsed by Regulators, in D. Wright/P. de Hert, Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy”, 2011, S. 323 – 346.

⁵⁵ Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, Bussels 12.5.2009, C(2009) 3200 final. (26.04.2012); Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011 (26.04.2012). Zur deutschen Handhabung: BSI, Technical Guidelines RFID as Templates for the PIA-Framework, 2010. (26.04.2012).

⁵⁶ Mit unterschiedlicher Intensität der Betonung von Privacy, der Voraussetzung von IT-Security und der Konformität mit Recht (Legality): Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011 (26.04.2012), S. 3: “The PIA process is based on a privacy and data protection risk management approach focusing mainly on the implementation of the EU RFID Recommendation and consistent with the EU legal framework and best practices.” und S. 18: IT-Security als “system protection”.

c) PII in a Global Perspective – The Question of Definition

It is foreseeable that a consensus will exist, at least across the Atlantic, that the scope of personality and privacy protection will be triggered with the existence of Personally Identifiable Information (PII). This consensus in the abstract is at odds with differentiation in the concrete. A recent essay⁵⁷ points out that significant differences exist in the identification of PIIs in concrete application and therefore proposes a “PII 2.0” approach. It is foreseeable that the concept of PIIs in a machine-determined space of the ubicom will be questioned fundamentally and globally. Technologies like RFID that make it possible to organize data without contact, therefore making data collection and transmission invisible, will require new designs.⁵⁸

d) A New Relationship with the Truth? – The Question of Content

aa) Statements without (Identifiable) Author According to German Law

It might surprise Americans, but in the German constitution “speech” is not protected, but it is formulated:

Art. 5 GG (German constitution) – Freedom of expression, arts and sciences⁵⁹

English: (1) Every person shall have the right freely to express and disseminate **his opinions** [...]

German: (1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten [...]

The fundamental question is what legal relationship do truth and liability have, when an author who expresses **his opinions** is not identifiable?⁶⁰ This question arose in Germany in light of an alleged unfounded evaluation of the professional activity of a doctor on a review portal in cyberspace. The Federal Court of Justice withheld the identity of the author from the negatively evaluated doctor as a last resort, and thereby supported the provider who pled protection of

⁵⁷ P. M. Schwarz/D. J. Solove, 102 California Law Review, 877.

⁵⁸ Furthermore, de lege ferenda see art. 4 para. 1, 13, 14, 15 und art. 9 para. 1 General Data Protection Regulation.

⁵⁹ https://www.gesetze-im-internet.de/gg/art_5.html (26.02.2018).

⁶⁰ For the German speaking audience: Inwieweit setzt Meinungsfreiheit (Art. 5 Abs. 1 S. 1 Alt. 1 GG) „mein“en voraus? Konsequenz wären Äußerungen, die kein Kommunikator für sich beansprucht (also „mein“t), nicht (in gleichem Maße) meinungsfreiheitlich geschützt wie andere [...].

privacy (“Review Site – John Doe”)⁶¹. In such a case, the liable person in anonymous (unfounded) statements in cyberspace is apt to be “lost”—and perhaps prone to be protected (precautionary management for a Charlie Hebdo scenario?). It is given over to the jurisprudential discussion, to what extent the primacy of privacy protection of the statement-maker is convincing. This is particularly notable when the European Court wants to remove factual statements from cyberspace in its “Google Spain” decision from 2014 (in “Review Site – John Doe” the request for information regarding an alleged unfounded claim was rejected; see also “Review Site – Anti-cyber-protagonist”)⁶².

bb) “Truth with Expiration Date” According to Union Law and Rights to Ephemerality, Net-Working and De-Networking

In principle, the question arises about conflicts of values of national laws on freedom of expression. The famous “Google Spain 2014” scenario⁶³ exemplifies that the globality of cyberspace leads to the fact that conflicting concepts of truth and freedom of information must come together in “coexistence.”

Furthermore, under consideration of the realworld (the so-called hybrid view), the question arises regarding the basis for interpretation for new basic rights—in particular a right to ephemerality, a right to de-network and a right to network.

The “Google Spain Decision” of the European Court of Justice from May 2014 chose the variant of a right to not be indexed by a search engine with one’s real name in connection with a truthful fact(ual report). The decision does not include fundamental statements on the “right to ephemerality” (author’s own terminology). Therefore, it does not give an opinion on the extent to which Google (as a tertiary source) must forget this data (“deleting” the “deletion request file”) or how to handle the primary and secondary sources (media).

Moreover, the questions arise: how can the individual unlink him/herself from cyberspace (de-networking)? Or how can barrier-free access be made possible (networking)? In summary: Only a few central questions are presented here, for which global cyberlaw must find answers. This top-down approach should be expanded in the interest of sustainability with circular thinking.

⁶¹ Federal Court of Justice (Bundesgerichtshof (BGH)), 01.07.2014, Az. VI ZR 345/13, “Review Site – John Doe”.

⁶² Federal Court of Justice (Bundesgerichtshof (BGH)), 23.09.2014, Az. VI ZR 358/13, “Review Site – Anti-cyber-protagonist”.

⁶³ European Court of Justice (Grand Chamber), Judgment of 8.4.2014, C-293/12 and C-594/12.

11. “Legal Information Technology Circular Thought Process”

For realworld products, the “circular economy” thought process has been established in European and German environmental and, in particular, waste legislation. Currently, such strategy perspectives are lacking for “information” – which can be seen in particular with archive legislation (keyword: archival diplomatics). Both with regard to the “if” (which electronic documents), as well as the “how” (time frame and quality of the archiving strategy), legal regulations are lacking in the German legislation that provide orientation certainty in the administrative and jurisdiction sectors.

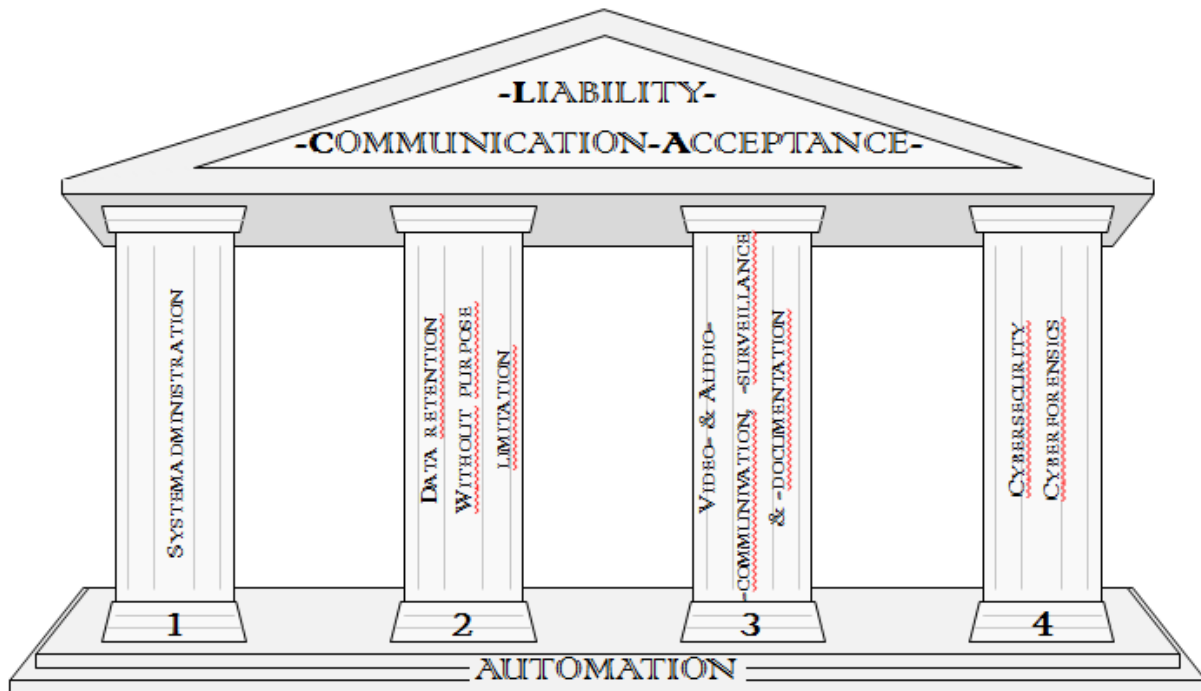
This deficit affects not just electronic information from the cradle to the grave, but also the transfer process of “paper documents” to “electronic documents.” What should be avoided: Replacement through scanning should not be allowed to corrupt the authenticity and integrity of the paper documents that previous generations have left to us.

From a European and German perspective, new and differentiated ideas are needed for rights to information access and subsequent use.⁶⁴ The value and private subsequent use of information that is available at federal locations are only beginning to be taken into consideration. From a global perspective, it should be noted: The more freely available information in federal possession is (for private business), the more chances increase for informed (allocation) decisions.

For a global comparative legal analysis based on technological law and a future-oriented jurisprudence, there is no lack of tasks according to what has been presented above. These abstract, top-down, answerable questions will be supplemented with a concrete pilot in the following, which should be successfully implemented in Germany in the coming years. It is a pilot project that represents a core area of cyberspace and cyberlaw, and already promises the highest level of motivation and interest due to the clientele involved—lawyers, judges and district attorneys.

12. Pilot: (Global) Comparative Technology Law in “E-Justice” – a Temple Architecture for Securitization

⁶⁴ Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information (Text with EEA relevance), OJ L 175, 27.6.2013, p. 1–8; Bundesministerium für Wirtschaft und Energie (BMWi), Entwurf eines Gesetzes über die Weiterverwendung von Informationen öffentlicher Stellen (Stand: 23.05.2014).



It should be stated up front that Germany has had comparably little experience with e-Justice. Therefore, this image of a temple⁶⁵ carries the title “Securitization,” because experiences in Germany rest on paper-based justice. The point of departure for the author is that the digital innovation of the legal profession—here: justice—poses fundamental questions of quality assurance. In light of lacking certainty through experience, the working thesis will not assume the security of the infrastructures and the applications, but rather investigate to what extent the law can make a contribution in this regard (*pro securitate*). From a German perspective, this is a large-scale information technology project that should be partially completed on January 1, 2022. At this time, Germany will know only “electronic legal avenues” (*elektronischer Rechtsweg*) for attorneys. This may be a late “digitalization” of justice in a global comparison. Nevertheless, there are fundamental questions named in the following four pillars:

- **Pillar 1:** Law of “System Administration”
- **Pillar 2:** Law of “Data Retention”
- **Pillar 3:** Law of “Video and Audio Communication, Surveillance and Documentation”

⁶⁵ See also V. Schmid: New “E-Justice” Law in Germany since 2013 – A Temple Architecture for an “Agenda of Securitization”, in: Report from Dagstuhl Seminar 14092 “Digital Evidence and Forensic Readiness”, (13.01.2015) Edited by G. S. Dardick, B. Endicott-Popovsky, P. Gladyshev, T. Kemmerich, and C. Rudolph; S. 163 – 167.

- **Pillar 4:** Law of “Cybersecurity (IT Security) and Cyberforensics”⁶⁶
- These four pillars are already represented in German “e-Justice” jurisprudence and legislation.
- **Pillar 1:** The question of system administration played a role in the so-called “Web Suit” (*Netzklage*).⁶⁷
- **Pillar 2:** The data retention decisions of the German Federal Constitutional Court and the European Court of Justice are legal core elements of every digitalization.
- **Pillar 3:** From a German perspective it should be noted: The question of to what extent court buildings may be protected through video surveillance has already occupied the e-Justice legislators in Hessen.⁶⁸ A lawyer refused to go advocate in a court that was to be protected through video cameras at the entrance. Even in the video communication portion of the pillar, legal procedures are beginning to permit video interrogation of witnesses (§ 102a Code of Administrative Court Procedure (VwGO)). This corresponds with recent legislation of 2013⁶⁹. What has not been definitively clarified, however, is in which judicial interrogations can the simultaneous presence of judge and witnesses/parties be forgone.⁷⁰ In principle, a peculiarity of German legal procedures should be mentioned: The video documentation and transmission of judicial processes continue to be prohibited.⁷¹
- For **Pillar 4—Cyberforensics**—the evidentiary value of electronic documents is of central importance (Evidentiary value of electronic documents – § 371a presently and in future ZPO).

⁶⁶ V. Schmid, contribution to Report from Dagstuhl Seminar Forensic Computing (11401), 3.10.-7.10.2011. „Casebook on Cyber Forensics (CCF) – a proposal for discussion” (10.01.2013); CyLaw-ReportXXXIV: V. Schmid (Hrsg.): “Beweisbare IT-Sicherheit – sichere IT-Beweise? Ein Fallbeispiel aus der Rechtsgeschichte und zur Studienarbeit von cand. Wirtsch. Inf. H. Baur (CyLaw-Report□□XXXIV)” (07.02.2014); CyLaw-Report XXXV: V. Schmid (Hrsg.): „Studienarbeit von cand. Wirtsch. Inf. H. Baur: Zur „Beweiskraft informationstechnischer Expertise““ (07.02.2014).

⁶⁷ Hessisches Dienstgericht für Richter v. 11.7.2008 – 1 DG 5/2007; Hessischer Dienstgerichtshof für Richter Ur. v. 20.4.2010 – DGH 4/08; BGH Ur. v. 6.10.2011 – RiZ(R) 7/10; BVerfG Beschl. (Kammer) v.17.1.2013 – 2 BvR 2576/11, „E-Justiz I“. Diese Bezeichnung wird gewählt, weil weitere Verfahren erwartet werden.

⁶⁸ § 6 (2) no. 2 Act on the Establishment of an Information Technology Agency for the Hessian Justice System (Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten vom 16.12.2011, GVBl I 2011, 778 (JITSTG (Hessen))).

⁶⁹ Gesetz zur Intensivierung des Einsatzes von Videokonferenztechnik in gerichtlichen und staatsanwaltlichen Verfahren vom 25.04.2013, BGBl I, S. 935, mit in Kraft treten zum 01.11.2013, Art. 10 Sec. 1.

⁷⁰ OLG Stuttgart, Beschl. v. 03.05.2012, Az. 4 Ws 66/12; AG Darmstadt, Beschl. v. 12.08.2014, Az. 50 F 1990/13.

⁷¹ Section 169 s. 2 Courts Constitution Act (Gerichtsverfassungsgesetz (GVG)): “Audio and television or radio recordings as well as audio and film recordings intended for public presentation or for publication of their content shall be inadmissible.”

-
- The **roof** that rests upon these pillars is considerations about the realization of information-technological projects using a fundamental consideration of cyberlaw: the “LCA” formula (Liability-Communication-Acceptance (*Haftung-Kommunikation-Akzeptanz* –HKA)).⁷²
 - The **stairs** of this temple are labeled “automation.” To what extent does a person still act autonomously and to what extent is s/he supported by information-technological products and processes? The idea that there could be “robot judges” is certainly still far-fetched. However, a doctoral dissertation with the title “IT Application in Justice” needs just two and a half pages to conclude: “No IT application for the dispensation of justice.”⁷³

In summary: **The author is convinced that for German law, a high-quality digitalization of justice can have a model character for private (high-security) zones, as well as administration.**

The pillar model for the securitization of e-Justice from a global cyberlaw perspective should also be supplemented with the integration of content of expression (law on content of expression) and the evaluation of technologies of expression (law on technology of expression) – here: the Cloud. This addition of the content of expression that is so difficult to evaluate, like the technological Cloud that is so difficult to organize and monitor, are depicted in the following expanded pillar model. It should be highlighted that not just the haziness of the clouds (with respect to technology and the difficulty of legal evaluation and interpretation of the content) should be represented, but also **the sun that shines on the realization of personal and economic freedom through cyberspace.**

13. Sustainability through Cyberlaw in 2015 ff. in its Significance for the Cloud with

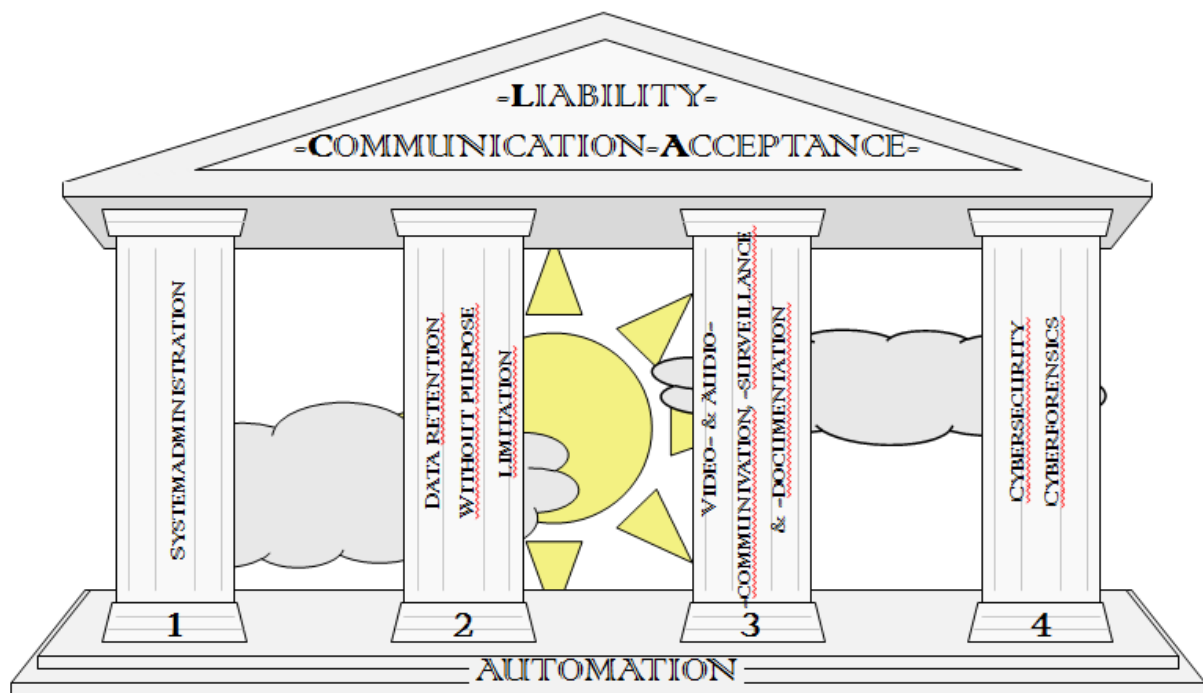
Respect to Content and Technology

Particularly in the current transition period (see above under 7.), this is about the challenge of “generation justness” in the context of cyberlaw (Idea of Sustainability – art. 20a German Basic Law). (Legal) deficient “data organizations” of the present threaten to become eternal hin-

⁷² V. Schmid, Zu den Voraussetzungen für die erfolgreiche Realisierung informationstechnologischer Projekte: die „HKA- Formel“ (Haftung – Kommunikation – Akzeptanz) und andere Herausforderungen, in Anzinger/Hamacher/Katzenbeisser (Hrsg.), *Datenschutz als multidisziplinäre Aufgabe – Herausforderungen durch genetische, medizinische und soziale Daten*, Springer Verlag, 2013, S. 219-237.

⁷³ M. Ballhausen, *IT-Einsatz in der Justiz*, 2012, S. 83 ff.

drances on freedom for younger and future generations. In light of the breathtaking opportunities of cyberspace, a (global) cyberlaw dogma and its systematic precautions should ensure that even more generations can operate as cyber-personalities in the fifth dimension of being “in the pursuit of happiness” under legal protection. A first step could be these basics that can lay the foundation for the second step: tackling a global agenda for cyberlaw.



F. Standard for a Law Lecture as an Instrument for Fulfilling Basic No. 4

As one can easily see, the standardization idea is the result of the **agenda setting basic no. 4**. Discourse bridges have to be built and the brick and mortar for these bridges is the “(Cyber)Teaching Standard” proposed in this contribution. As you now know, the first proposal stems from the last Internet Law in Progress Conference (see slide presentation above, Part 4 D: Lecture — Syllabus and Agenda of Priorities in March and May 2017 (Santa Clara and Darmstadt)). This first syllabus and agenda is hereby augmented with this manuscript: Further lecture details, such as the specific language under each heading, will be determined as the project progresses and the results of involvement in academic open innovation (AOI). The following framework and talking points are suggested here.

I. Navigator: Global Agenda for Cyberlaw

The Agenda for Cyberlaw, created in 2015, brings together a total of thirteen basic topics, including an “e-Justice demonstrator,” which serves as a navigator for project progress. It is a reservoir of methods and ideas that can be prioritized differently as needed.

II. Audience and Glossary

It is a transdisciplinary lecture intended to address and motivate citizens as well as members of different academic disciplines. Therefore, the lecture does not require any previous legal knowledge and thus tries to counteract prejudices against the law strategically. The consequence of this renunciation of prior knowledge is that related legal terms must be included in a glossary for the project of a definition. An example can be found above in “Securization” (Part 2 B III). The multilingual complexity, such as the necessity of forming one's own terminology, has already been demonstrated in the module on language using the example of the German term “lawyer” (“Rechtsanwalt”).

III. Hybrid Strategy in the Realworld und Cyberspace

This innovative project requires a debate—and the culture of debate that offers content and criticism (academic and practical crowd sourcing with impact and ambition) should be organized in the realworld in an organized manner. This strategy corresponds to the ideas of citizen science and citizen debates (as in the 22 European Space Agency states). For this reason, it is planned that the online modules will be tested and evaluated during the lecture courses.

IV. Time frame

As already proposed in Santa Clara in 2017, fifteen modules of ninety minutes each will be created. The aim of this draft is to outline a concrete overall structure and specify details of the content.

V. Content (I) – “Survival Guide”, “Basics”, “GoCore! Scenarios“ and “Outcome”

The 15 moduls are as follows:

- 1 Module with a **Survival Guide for the Lecture**

- 6 Modules with **Basics of (Global)Law**
- 6 Modules with **GoCore! Scenarios**, identifying paradigmatic scenarios for pressing challenges for Governance (Law). In this draft, one double module is designed. GoCore!⁷⁴ is a movement with a point of origin at the faculty of law and economics at the Technical University Darmstadt, Germany in 2015 (led by Viola Schmid).

“GoCore!” is an acronym for the three terms Governance, Compliance & Regulation. It is about the core challenge of a new academic discipline – cyberscience. The goal and agenda of cyberscience is the analysis of chances and risks, rights and obligations, as well as the consequences of a new fifth dimension of being (in addition to space and time) – namely the Cyberspace as a “space” created by technology.

More than a decade ago, the coordinator of the pillar of research “CoCoRe” began establishing a new jurisprudential discipline in Germany–Cyberlaw. The research portal “GoCoRe” has opened up the legal perspective for the input of other sciences. Due to the fact that the “GoCoRe” pillar of research originated in a department of Law and Economics, the need for economic findings and outcomes is self-evident. Expert input from the technological sciences is also mandatory, because the “Intelligence” of the future will also be „Artificial Intelligence“ (AI). In this regard, “GoCoRe” has a special “anchor” to its home university – Technische Universität Darmstadt. Moreover, “GoCoRe” strives for a “Glocal”-perspective. Issues that will be analyzed and answered regionally in collaboration with the Johannes Gutenberg-Universität Mainz can be shared with the world in a bottom-up and top-down framework within the Jean Monnet-Centre of European Excellence. The previous coordinator and the current coordinator are members of the Jean Monnet-Centre of European Excellence that was granted on 07/31/2015 with the task “EU in Global Dialogue” (CEDI).⁷⁵

The current status of “GoCoRe” (10/2015) is aligned not only with its goals but also its methodology. The goals are laid out by the “RPF formula” that incorporates the three elements of defense rights (“Respect”), intellectual property rights (“Protect” – positive obligations) and the enforcement level (= “Enforcement” + “Compliance” = “Fulfill”). Its mission is about the analysis of physical states in real-world and Cyberspace and the compliance with legal guarantees which are defined by this trinity: “Respect”, “Protect”, and “Fulfill”.

⁷⁴ <http://www.gocore.wi.tu-darmstadt.de/start/index.en.jsp> (22.02.2018).

⁷⁵ About CEDI – The Jean Monnet Centre of Excellence “EU in Global Dialogue” (CEDI) was designated in July 2015 by the European Commission to support an ambitious programme of research, teaching and outreach activities. The Jean Monnet Centre of Excellence is a focal point of competence and knowledge on European Union issues; <https://www.eu-global-dialogue.eu/> (22.02.2018).

This respect for the freedoms also of others, this protection for the necessities of the claimants (Protect), as well as the implementation and enforcement of these legal guarantees are the core of a model that is anchored in European Union Law – a space of freedom, security and justice (art. 67 para. 1 TFEU).

- 1 Module: **Terroir**: This module encourages every participating legal system to choose one paradigmatic scenario along the three criteria: (1) National idiosyncrasy of the legal system and tradition and/or (2) billion euro/dollar scenarios and/or (3) up-to-date importance. The denomination “terroir” is meant to underline the respect for every participating legal system, acknowledging, as in winemaking, the importance of the “soil and the climate where the grapes grow.”
- 1 Module: **Summing up**: The success and return on investment (ROI) of the lecture for the students and contributors in different legal systems and traditions.

The module titles are working (not final) titles. At this stage of the project, only keywords are presented because we assume that every academic participating in the project knows the details. Module 1 to 7 may be criticized as topics as derived from legal philosophy. However, the impact of these theoretical foundations will be exemplified with the following scenarios (Modules 8 – 13). The selection strategy follows GoCoRe principles (acronym for Governance Compliance and Regulation) focusing on the heart of people as well on the core of a subject. The leading question concerning the challenges for law in the future will be: Where are the unicorn questions (in German: *milliardenschwere Fragen*) and where are—regarding cultural identity and legal traditions—the idiosyncratic scenarios?

VI. Content (II) – the Modules

1. Module: “Survival Guide” – LAW and not Philosophy, Political Science, Sociology, Economics etc.

Keywords: Analyzing the “unique selling proposition (USP)” of LAW, the chance of enforcement, admissibility (court systems), being based on merit decisions, etc.

2. Module “Basics 1” – Robots and Cyborgs and the Right of Humans

Law, including robots and cyborgs, governing human and machine interaction, are covered in this module. It also includes technical determinism, disruption theory, “algocracy”, accountability, liability and responsibility in “autonomous environments,” etc. Summing up: This module opens up a legal perspective on “transhumanity”.

3. Module “Basics 2” – Reaching out for a Global and Universal Perspective

Law in globalized and digitized societies has to include energy and outer space law in order to deal with (critical) infrastructure (challenges). Another argument for including space law in this lecture is that satellites are now determining how smart our cities can function with cybergovernance. And: These infrastructures are threatened by perpetrators acting globally and universally. Hence the **theoretical concepts of international law and multilayer systems (e.g. European Union Law)** have to be shared in this basics module to arrive at a deeper understanding for GoCore! scenario 3.

4. Module “Basics 3” – Language as a Strategy for a Global Lecture Standardization

Effort – here: “Rechtsanwalt”

Christoph Merkelbach comments on different terminologies for lawyers (German: *Rechtsanwalt*):⁷⁶

“Communicating across languages and national cultures always includes a cross-cultural mediating process. In the case of this proposed project, three languages are involved: Chinese, English and German (in alphabetical order). We define culture as a repertoire of behavior and communication patterns that distinguish one group of people from another (e.g. Thomas 2003: 380; Weidemann & Strauß 2000: 835). In the case of our project, this does not only have an implication on the discourse between the members of different national cultures (China, Germany, US) but also has an impact on the scholarly discourse between members of different legal traditions or legal systems and its linguistic codification. In order to bridge this gap between at least three different national and legal traditions, we propose English as a lingua

⁷⁶ Literature for this contribution listed as follows: Fisher, G. (1980) *International Negotiation: A Cross-Cultural Perspective*. Yarmouth, ME. Schneider, S. C. & Barsous, J.-L. (2003) *Managing across Cultures*. (2nd Edition. Harlow, England. Thomas, A. (1992/2003) „Psychologie interkulturellen Lernens und Handelns.“ In: Alexander Thomas (Hrsg.) *Kulturvergleichende Psychologie*, Göttingen, 377–420. Weidemann, D. & Straub, J. (2000). „Psychologie interkulturellen Handelns.“ In: Jürgen Straub, Alexander Kochinka & Hans Werbik (Hrsg.), *Psychologie in der Praxis. Anwendungs- und Berufsfelder einer modernen Wissenschaft*, München, 830–55.

franca (or bridge language) to ensure that the discourse can proceed smoothly. This meta-function of English (in this case American English + World English) does not exclude the presence of English as a legal language, as it excludes neither Chinese nor German.

Even a seemingly global legal German term like *Rechtsanwalt* translates into several English terms (*advocate, lawyer, jurist, attorney-at-law, counselor-at law, barrister, legal practitioner, or solicitor*) and only one Chinese term (律师). The English terms may include the German

Notar which in Chinese often is translated as 法官 or as 公证人 and may be used (according to the task being performed) as *solicitor* or *notary public*. Since the underlying thoughts and ideas in legal discourse influence its epistemology, which in turn is greatly defined by language, language as a cultural determined system itself is a subject of specific attention in this project. Language awareness turns out to be a central and essential point of our work.

A linguistic lecture about speech act theory, different grammar theories, and the function of legal language for specific purposes will ensure this project's success by developing an English meta-language in which all partners can communicate about the issue at hand in order to ensure a smooth discourse without losing important information. It will also keep all members of the project involved on the same hierarchical level (e.g. Fisher 1980: 62; Schneider & Barsous 2003: 195)."

The German *Rechtsanwalt* example is paradigmatic for the glossary challenges we have to face. Hence, we need and have someone with theoretical and methodological input like Merkelbach.

5. Module “Basics 4” – “Lexonomics” – How do Financial Resources and Efficiency and Efficacy Principles Influence the System

In the European Union data protection law, cost-benefit ratios are vital for the application and enforcement of law. Viola Schmid foresaw this in the context of IT-security law as early as 2015 this methodology was named “Lexonomics”.

6. Module “Basics 5” – National constitutional reserves for (inter)national law in globalized (and digitized) societies

See under Part 6 C regarding German constitutional identity principles. Where are the (national) legal “No Go’s” for internationalization and international rule of law?

7. Module “Basics 6” – Electricity as the Lifblood/ Fuel for Cyberspace

This module is about realworld infrastructure of cyberspace analyzing and determining how much energy and electricity every cybercitizen needs? Is it necessary in order to mine virtual currencies, or in order to encrypt location and communication? Consequently, energy law is groundbreaking for this law lecture. And it will be interesting to monitor whether China indeed restricts the use of energy for currency miners.⁷⁷

8. Double-Module “GoCore!” 1 – Telecommunication Traffic Data Retention And Usage Law

This double-module provides an original analysis of the legal perceptions of digital and real identities of humans and machines in different nations and different systems as well as in various legal traditions. From a German-European perspective this challenge has, since 2006, not been solved.

9. Module “GoCore! 2” – Ramifications of Virtual Currencies on Governance

How do different legal systems acknowledge virtual currencies (bitcoin, ethereum, ripple, bitcoin cash etc.), and what consequences do they have for national and global economies?

10. Module “GoCore! 3” – “Who Owns the Sky?” – Drone Law

Unmanned aerial vehicles (drones) are a challenge for economies and legal systems worldwide. Using space in order to fly drones or air taxis becomes of everyday importance for everyone—especially for those whose pictures are taken by surveillance drones.

11. Module “GoCore! 4” – “Interactive Toys”

Future generations will consist of persons who are digital natives—and not like nowadays in transitional times between realworld and cyberspace “digital immigrants.” Hence, these questions are essential to how we bring up future generations—for example, do we allow companionship with robots and spyware in nurseries? The paradigmatic scenario in a transatlantic

⁷⁷ FAZ, Ankenbrand/Nestler/Plickert/Welter, China kappt den Digitalwährungen den Strom, 12.01.2018, S. 18.

perspective is the toy “my friend Cayla,” which was prohibited in Germany as spyware and also criticized in the United States (see above Part 4 D slides).

12. Module “GoCore! 5” – Legal Technology, TechJustice and “Technology Transforms Legal Markets” (Own Terminology)

The global agenda chooses as a demonstrator (point 12) the influence and disruption in legal science and practice through technology.

13. Module – Terroir

It is reserved for burgeoning issues from different national perspectives. In 2018 the American contribution could focus on the technological and legal ramifications for (e)voting, social media governance and manipulation in the context of (presidential) elections (key phrase: the Russia probe).

14. Module: Outcome and ROI

Return on Investment – be it time, be it money, be it commitment – is the defining maxim of many people, especially in such a complex project. For this reason, it has to be clarified in Module 14 what return the audience of the lecture can expect, which (not) to expect and how their knowledge will improve.

The ideas of the author are not yet herein presented conclusively, but her determination should be clear: her commitment is to the advance of pure knowledge in the academic–scientific environment. In this Draft No. 1, module 14 is provided only as a placeholder after the development of modules 1 to 13, because the ambitions of this lecture will be presented clearly therein. The quantity and quality of truly global academic open innovation in this series—for the time being, only by tricontinental—does not yet permit further explication.

However, some aspects of module 14 can already be highlighted: cyberspace, with its ubiquitous and all-round networking, presents us with unknown challenges that cannot be answered by a single nation with its legal system and its legal tradition in a scientific perspective. Therefore, there is no alternative but to establish a platform for international crowdsourcing to present a range of experiences, knowledge, strategies, and tactics. The decisive factor should be

that the “forgotten men and women”—people left behind in the digital divide—are integrated in a timely manner into the design of law in our global analysis.

Moreover, this module will be about positioning ourselves against technical determinism. Technical determinism could occur when technology quickly creates the interfaces for global and universal connectivity and cannot keep up with (other) (legal) scientific structures. The experiences and opportunities of governance—traditional ideals of the past—should not be sacrificed unreflectively for progress that ends up in regression. Some parts of the past are so “retro” that they can end up have future meaning after our present is over.

Part 5: Who? German Initiative

Three authors have contributed to this project: Viola Schmid, Georg Gesk and Christoph Merkelbach. Georg Gesk’s and Christoph Merkelbach’s contributions are specified in the text. Georg Gesk is the specialist for Chinese (cyber)law and legal education and Christoph Merkelbach is the specialist for linguistic and intercultural competences in general. Viola Schmid is the project designer and is responsible for all parts of the draft that are not otherwise specially identified.

A. Prof. Dr. Viola Schmid LL.M (Harvard)

Schmid is a German professor of public law focusing on cyber governance with a background (*veniae legendi*) in German and European Union law; her expertise is the design of this lecture. She advocates the necessity of an international multigenerational and multidisciplinary debate about the essential (legal) requirements for the organization of cyberspace. It is her belief that only law—the so-called cyberlaw—has the potential to render cyberspace into a cyberworld, just as the law of foregone decades and centuries (traditional law) was a prerequisite for a livable environment (the realworld). It goes without saying that the fifth dimension of being, which has been managed thus far without traditional political borders, poses new and unprecedented challenges for an area of freedom, security and justice (art. 67 para. 3 TFEU, art. 3 para. 2 TEU). Schmid believes that a trans-disciplinary and trans-national approach promises the highest potential for mastering these challenges. 15 years after she advocated for a new discipline of law (cyberlaw) she now argues for a new discipline of science – she calls it CYBERSCIENCE. This lecture concept is a tool for the construction of a CYBERSCIENCES grid.

B. Prof. Dr. (NTU) Georg Gesk – Relation to Chinese Cyberlaw and Development of Curricula

Prof. Dr. (NTU) Georg Gesk shows proficiency in both, the field of Chinese cyberlaw and the task of planning of (intercultural)l curricula. Some publications Publications and Lectures Related to (Chinese) Cyberlaw are shared:

- Censorship in China – Public Opinion as a Political Means (Zensur in China – Meinung als politisches Instrument), in: Bösling et al. (ed.) *Censorship does (not) happen (Eine Zensur findet (nicht) statt)*, Osnabrück: VHS/OS, Remarque Gesellschaft, 2018, in print.
- Meta-Study Programm – the Example of CRiOS ‘Chinese Law in Osnabrück’ (Meta-Studiengänge – das Beispiel CRiOS ‚Chinesisches Recht in Osnabrück‘), *10th German-Sino Symposium on Applied University Education – Enhancing Startups & Entrepreneurship in the Realm of Universities*, Osnabrück: University of Applied Sciences (HZC), 03.11.2017.
- Georg Gesk, Yimeng Feng, Trans-border e-Commerce with Relation to China (Grenzüberschreitender E-Commerce mit Bezug zu China), Lecture, Osnabrück: IHK, 16.08.2017.
- Protection of Intellectual Property and Choice of Legal Procedure (德国知识产权保护与诉讼选择), School of Law, Anhui University, 24.03.2017.
- New Reforms of the Crime of Market Manipulation (关于市场操纵的最新法律发展), Dt.-Chin. Rechtswissenschaftliches Institut, Nanjing University, 21.03.2017.
- Market Behavior without Contractual Basis? Blockchain Transactions und IoT in Taiwan and China, International Conference *Contract Compliance and Market Behavior*, Osnabrück, 25.11.2016.
- Regulation of Online Platforms in China, International Conference *Digital Economy and the Law: Asian and European Perspectives*, Osnabrück, 20.8.2016.
- Development Trends of German Universities (德國大學的發展導向), *2014 Conference on Teaching and Applied Research in Teaching in the Digital Age (2014 數位學習時代教學實務研究暨教學研討會)*, Hsinchu: Hsuan Chuang University, 30.4.2014.

-
- Structural Changes of the Internet and their Consequences for Criminal Law (Strukturelle Veränderungen des Internet und dessen Herausforderungen an das Strafrecht), *Cyber-crime in Germany, Japan, and Korea (Cybercrime in Deutschland, Japan und Korea)*, Osnabrück: Universität Osnabrück, 01.-05.09.2013.

C. Dr. Christoph Merkelbach

Merkelbach, with his linguistic, intercultural and didactic competence, enables the initiators to prevent translation errors or ambiguities as demonstrated above. Furthermore, he is director of the Center of Intercultural Competence at the Technical University of Darmstadt. He is in many ways the link between academia and students, between disciplines, Asia, and Germany. His support as well as critique is the backbone of the project providing outreach to interested potential audiences among his wide network of colleagues. He is leading an initiative to teach refugee students the necessary German language skills to succeed at university. He is currently writing a habilitation thesis on developing pedagogical skills for instructors of refugee students. He publishes widely on issues related to multilingualism and the politics of linguistic diversity at the university level.

D. Crowd Research Sourcing and Funding in Order to Organize International Competence as well as Interdisciplinary Knowledge Management for CYBERSCIENCE

Not only do we need a global (cyber)law competence organized as scientific crowd sourcing and content funding. Our ubiquitous interconnectedness with each other in/and with cyberspace also requires transdisciplinary efforts. Cyberspace is constructed, defined and designed by technology and its (non-)governance, its freedom as well as its virtue and righteousness. Its functions and its potential to better the world depends on supplementary competences such as computer science and economics. Schmid's terminology for this new discipline is "CYBERSCIENCE". Knowing the law does not suffice if you do not know the technological strength, weaknesses, options and threats. The principle of IT Security as the sophisticated development of the traditional rule of law in cyberspace is the paradigmatic argument. Moreover, new

transdisciplinary methods such as LEXONOMICS, incorporating costs and benefits in legal analysis, are of vital importance.⁷⁸

This is a project bigger than a person and a discipline, showing the necessity of (inter)national and transdisciplinary crowd research as funding. In this draft status the acquisition of financial means was postponed in order to first work for the quality of the product. That is also the reason, why supporters and mentors at this stage are not named.

Part 6: Reaching out to Europe from Germany – Module “GoCore!” 1

The German initiative offers some background information concerning the impact of international law on national (constitutional) law for the module “GoCore!” 1 – Telecommunication Traffic Data Retention and Usage Law.

A. An Area of Freedom, Security and Justice (Art. 67 TFEU)

(In)Security in times of digital transformation is of vital importance. But as European Union Primary Law stresses, there is no freedom without security and no security without justice. In European Union Law, you find this reflected in art. 67 Treaty on the Functioning of the European Union (TFEU)⁷⁹.

Article 67 TFEU

1. The Union shall constitute an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States. [...]

⁷⁸ In the following publication V. Schmid presented this connectivity between law and economics for the first time in the context of IT–Security: New “E-Justice” Law in Germany since 2013 – A Temple Architecture for an “Agenda of Securitization”, in: Report from Dagstuhl Seminar 14092 “Digital Evidence and Forensic Readiness”, (13.01.2015) Edited by G. S. Dardick, B. Endicott-Popovsky, P. Gladyshev, T. Kemmerich, and C. Rudolph; p. 163–167; http://drops.dagstuhl.de/opus/volltexte/2014/4549/pdf/dagrep_v004_i002_p150_s14092.pdf (22.02.2018).

⁷⁹ Consolidated version of the Treaty on the Functioning of the European Union, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> (22.02.2018).

B. Supremacy of European Law– 28 Member States and 500 Million People (2018)

To clarify for a global perspective: The origin of this initiative is in Germany (with its approximately 82 million inhabitants). Two of the authors work at the Technical University Darmstadt (Schmid, Merkelbach). The standardization idea is a contribution of Viola Schmid to the CEDI⁸⁰ that is situated at the Technical University Darmstadt^{81 82}.

Legal design—here in the form of designing a law lecture—thus is of importance for Germany and the European Union to open up for global dialogue. Not only is this initiative backed and supported by the Centre (the lecture project was the agenda of the 2nd annual Jean Monnet Center of European Excellence conference in July 2017); moreover European Union law claims supremacy over German law.

This principle has one exception: European Union law may never encroach upon the “**constitutional identity of the Federal Republic of Germany**”.

C. National Identity Clause in the German Constitution (Art. 23 Abs. 1 S. 3 GG, Art. 73 Abs. 3 GG)

The German constitution (Basic Law [*Grundgesetz* – GG]) dates back to 1949. The experience with the Third Reich induced the authors of the constitution to implement a “**constitutional identity retention principle**”. Consequently, this German constitutional identity is untouchable—and cannot be modified by future lawmakers and majorities in parliament. The relevant provisions are cited here:

Art. 79 Basic Law – Amendment of the Basic Law

[...] (3) Amendments to this Basic Law affecting the division of the Federation into Länder, their participation on principle in the legislative process, or the principles laid down in **Articles 1 and 20 shall be inadmissible.**

⁸⁰ About CEDI – The Jean Monnet Centre of Excellence “EU in Global Dialogue” (CEDI) was designated in July 2015 by the European Commission to support an ambitious programme of research, teaching and outreach activities. The Jean Monnet Centre of Excellence is a focal point of competence and knowledge on European Union issues; <https://www.eu-global-dialogue.eu/> (22.02.2018).

⁸¹ Technischen Universität Darmstadt; <https://www.tu-darmstadt.de/> (22.02.2018).

⁸² & Johannes Gutenberg-Universität Mainz; <http://www.uni-mainz.de/> (22.02.2018).

Art. 1 – Human dignity – Human rights – Legally binding force of basic rights

- (1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.
- (2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world.
- (3) The following basic rights shall bind the legislature, the executive and the judiciary as directly applicable law.

Art. 20 Basic Law – Constitutional principles – Right of resistance

- (1) The Federal Republic of Germany is a democratic and social federal state.
- (2) All state authority is derived from the people. It shall be exercised by the people through elections and other votes and through specific legislative, executive and judicial bodies.
- (3) The legislature shall be bound by the constitutional order, the executive and the judiciary by law and justice.
- (4) All Germans shall have the right to resist any person seeking to abolish this constitutional order, if no other remedy is available.

Art. 23 Basic Law – European Union – Protection of basic rights – Principle of subsidiarity

- (1) With a view to establishing a united Europe, the Federal Republic of Germany shall participate in the development of the European Union that is committed to democratic, social and federal principles, to the rule of law, and to the principle of subsidiarity, and that guarantees a level of protection of basic rights essentially comparable to that afforded by this Basic Law. To this end the Federation may transfer sovereign powers by a law with the consent of the Bundesrat. The establishment of the European Union, as well as changes in its treaty foundations and comparable regulations that amend or supplement this Basic Law, or make such amendments or supplements possible, shall be subject to paragraphs (2) and (3) of Article 79. [...]

Art. 28 Basic Law - Land constitutions – Autonomy of municipalities

- (1) The constitutional order in the Länder must conform to the principles of a republican, democratic and social state governed by the rule of law, within the meaning of this Basic Law. In each Land, county and municipality the people shall be represented by a body chosen in general, direct, free, equal and secret elections. In county and municipal elections, persons who possess citizenship in any member state of the European Community are also eligible to vote and to be elected in accord with European Community law. In municipalities a local assembly may take the place of an elected body.

(2) Municipalities must be guaranteed the right to regulate all local affairs on their own responsibility, within the limits prescribed by the laws. Within the limits of their functions designated by a law, associations of municipalities shall also have the right of self-government according to the laws. The guarantee of self-government shall extend to the bases of financial autonomy; these bases shall include the right of municipalities to a source of tax revenues based upon economic ability and the right to establish the rates at which these sources shall be taxed.

(3) The Federation shall guarantee that the constitutional order of the Länder conforms to the basic rights and to the provisions of paragraphs (1) and (2) of this Article.

D. Positive Obligation for Privacy of Telecommunication in German Constitution Law

(Art. 10 Basic Law) Pertaining to European Union and International Law

In its landmark judgment of March 2, 2010, the German Federal Constitution Court (*Bundesverfassungsgericht – BVerfG*) established the legal basis for “Precautionary storage of Telecommunication traffic data without cause”.⁸³ First, it awarded the highest constitutional protection to privacy law so far by qualifying this information technology, as well as surveillance strategy, as intrusive to the German constitutional identity. Second, the court established a positive obligation for the Federal Republic of Germany to preserve this data sovereignty of its citizens in Europe as well as the world. The following paragraphs cite the court:

I. Precautionary Storage of Telecommunication Traffic Data as a Restriction of Privacy of Telecommunication

Article 10 Basic Law - Privacy of correspondence, posts and Telecommunication

(1) The privacy of correspondence, posts and Telecommunication shall be inviolable.

(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

“ [...] The challenged provisions encroach upon Article 10.1 GG.

⁸³ BVerfG, Judgment of 02 March 2010 - 1 BvR 256/08, Headnote no. 1.

1. Article 10.1 GG guarantees the secrecy of Telecommunication, which protects the incorporeal transmission of information to individual recipients with the aid of Telecommunication traffic (see BVerfGE 106, 28 (35-36); 120, 274 (306–307)) against the taking of notice by state authority (see BVerfGE 100, 313 (358); 106, 28 (37)). In this connection, this protection does not only relate to the contents of the communication. On the contrary, the protection also covers the confidentiality of the immediate circumstances of the process of communication, which include in particular whether, when and how often Telecommunication traffic occurred or was attempted between what persons or Telecommunication equipment (see BVerfGE 67, 157 (172); 85, 386 (396); 100, 313 (358); 107, 299 (312–313)); 115, 166 (183); 120, 274 (307)). The protection of Article 10.1 GG applies not only to the first access by which state authority takes notice of Telecommunication events and contents. Its protective effect also extends to the information and data processing procedures that follow the taking of notice of protected communications events, and to the use that is made of the knowledge obtained (see BVerfGE 100, 313 (359)). An encroachment upon fundamental rights includes every taking of notice, recording and evaluation of communications data, and every analysis of their contents or other use by state authority (see BVerfGE 85, 386 (398); 100, 313 (366); 110, 33 (52–53)). The recording of Telecommunication data, their storage, their comparison with other data, their evaluation, their selection for further use or their transmission to third parties are therefore each an individual encroachment upon the secrecy of Telecommunication (see BVerfGE 100, 313 (366–367)). Consequently, an order to communications enterprises to collect and store Telecommunication data and to transmit them to state agencies is in each case an encroachment upon Article 10.1 GG (see BVerfGE 107, 299 (313)).”⁸⁴

II. Positive Obligation of the German Government to Preserve the Constitutional Identity Including the Privacy of (German) Citizens around the World

“[...] Regardless of the structure of the provisions on use, such legislation would from the outset be incompatible with the constitution. For precautionary storage of Telecommunication traffic data without cause to be constitutionally unobjectionable, this procedure must, instead, remain an exception to the rule. [...] The introduction of the storage of Telecommunication traffic data may therefore not serve as a model for the precautionary creation without cause of further data

⁸⁴ BVerfG, Judgment of 02 March 2010 - 1 BvR 256/08, no. 188 – 190.

pools, but forces the legislature to exercise greater restraint in considering new duties or authorizations of storage with regard to the totality of the various data pools already in existence. **It is part of the constitutional identity of the Federal Republic of Germany that the exercise of freedom of its citizens may not be totally be recorded and registered (on the constitutional identity retention principle, see BVerfG, judgment of the Second Senate of 30 June 2009 – 2 BvE 2/08 and others –, juris, marginal no. 240), and the Federal Republic of Germany must endeavor to preserve this in European and international contexts.** Precautionary storage of Telecommunication traffic data also considerably reduces the latitude for further data pools created without cause, including collections by way of European Union law.”⁸⁵

E. Legal Innovation in German and European Data Protection Law in 2018: New Governance for the Raw Material Data

If it has not yet become clear how important this pioneering project is, then another argument remains: current and future rights and obligations in German and European data protection law. In May 2018, this law will fundamentally change, and data governance will largely affect global and bi-and multinational discourse, including business opportunities. Still further: Ignorance of legal language and systems could be used for foreclosure against foreign competition. Pioneering theory in cyberlaw faces the challenge of constant openness to innovation and revision. This openness, combined with the renunciation of legal certainty, is a prerequisite for the chance of legal sustainability in teaching.

At the European level, the General Data Protection Regulation comes into force in May 2018 with the complementary German „*Datenschutz-Anpassungs- und -Umsetzungsgesetz* EU (DSAnpUG-EU)”. Schmid uses the term “*lex futura*” to describe them. In addition, the Federal Data Protection Act⁸⁶ (*Bundesdatenschutzgesetz*, BDSG) ceases to apply at the German federal level. At the European level, the Regulation on Privacy and Electronic Communications is in the legislative process and at German state level, the “*Hessisches Datenschutzgesetz*” is in the advisory process. These areas are traditionally outlined as “*de lege ferenda*” in legal time

⁸⁵ BVerfG, Judgment of 02 March 2010 - 1 BvR 256/08, no. 218.

⁸⁶ Translations of German statutes are – if available – provided by the German Federal Ministry of Justice and Consumer Protection; https://www.gesetze-im-internet.de/Teilliste_translations.html (14.02.2018).

management. Therefore, time management, transition management and openness to change must be communicated and implemented in this draft no. 1.

I. Time & Transition Management: German and European Data Protection Law in Relation to the First Power

1. Terminology: “Deadline” and “Date of Coming into Effect”

There are rules about “deadlines” on the one hand, and “dates of coming into effect” on the other.

- “Deadline” encompasses, for example, the deadlines for the transposition of German law into European law (Article 288 (1) and (3) TFEU) and for the expiry of law in general.
- “Date of Coming into Effect” is Schmid’s own terminology, which she uses as an umbrella for three German terms: namely the application of the law, the validity of the law and the date of a law coming into effect.

This differentiation is already necessary in a bilingual perspective, because the authentic version of the new European data protection law differs in English and German versions. This differentiation becomes relevant because the legal obligations of the debtors and the legal claims of the creditors cannot be contoured differently in time. One example is the European General Data Protection Regulation (GDPR), which was established two years before it came into effect.

Art. 99 GDPR – Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union [24 May 2016].
2. It shall apply from 25 May 2018.

2. Deadlines and Dates of Coming into Effect – May 6 and 25, 2018, May 6, 2023, and May 6, 2026

The currently known relevant dates on the German and European level are May 6 and 25, 2018, May 6, 2023, and May 6, 2026. More reliable information for the legislative process at

the German state level and the European Regulation on Privacy and Electronic Communications is not available as of this writing (February 5, 2018). Further information is available at request.

II. If You Want Peace, Prepare for War (*Qui desiderat pacem, bellum praeparat*): The Near Future of a Data Protection Conflict between the EU and the US

In the European Union, and thus Germany, there is a need for a data protection law turnaround. It is foreseeable, as outlined in the highly respected *Frankfurter Allgemeine Zeitung*, that this new European and German governance system for the extraction of “raw data” and its “refining” causes a (data) trade conflict with the US. The European Court of Justice (ECJ) in Luxembourg has already declared that international agreements on transatlantic data transfer and use are unlawful.

If you want to solve a conflict, then it is a good idea to search for other opinions at eye level. Therefore, it is important to analyze the status and the pros and cons of US and Chinese data protection law as well as to do additional research. Otherwise, the heterogeneity of these legal systems threatens to call into question the character of “law” (in the sense of enforceability) in a global perspective. Otherwise, if a company operates in multiple jurisdictions, illegality seems inevitable, at least in one system. And the potential ignorance of the legal system of another nation denies lawmakers the chance to share experience and sometimes even the knowledge of an improved state of the art.

Part 7: Reaching out to the US

However, this ambitious endeavor takes time, demands a stepwise approach and needs nurturing. In 2017, this dream lecture concept had its American premiere at Santa Clara University in the legal design section. The project began in Germany at the second annual conference (July 6–7, 2017) of the Jean Monnet Center of European Excellence “EU in Global Dialogue” (CEDI).⁸⁷ Today, this competence cluster is reaching out to the United States for guidance as well as critique: Are the topics of the lecture of universal concern, and does teaching about

⁸⁷ Jean Monnet Centre of Excellence: EU in Global Dialogue, “CEDI,” <https://www.eu-global-dialogue.eu/> (viewed 22.11.2017).

them fulfill (US-American) efficacy standards? This mission and vision shows the potential of a standard for a universal (technology) law lecture. A presentation in New York—by now a paper-in-progress—shall serve the acquisition of US-American intelligence for this German-European-Chinese project of a “dream lecture on (technology) law.”

Part 8: Reaching out to China – Georg Gesk und Christoph Merkelbach

The concept of the law lecture is supported by Georg Gesk and Christoph Merkelbach. For this draft no. 1, their endorsement and promise to promulgate the innovation in the linguistic discipline (Christoph Merkelbach) and at Chinese universities and law faculties (Georg Gesk) can be shared. Some milestones—partly in German—should be incorporated in the following. The strategy has to be developed before the standard is carved out in detail. The excuse for not delivering all slides in English is that the project with this competence trial in cyberlaw, linguistics and Chinese legal science started only in 2017.

A. Reaching out to China – Insights by Georg Gesk

I. Supremacy of Supra-Individual Actors (Natural paragraph 13, Preamble, Constitution 1982)

According to the preamble of the Chinese Constitution (1982), the main responsibility of implementing and maintaining basic social order is not seen as a collective responsibility of individuals, but as a task that has to be obeyed by supra-individual actors as diverse as ethnicities, state institutions and armed forces, political parties, enterprises and other entities (natural paragraph 13, Preamble, Constitution (1982)). Any obligation of the citizen to obey the constitution and the laws (Sec. 33 IV) is only derived at a later point and thus seen as structurally (and practically) of lesser importance.⁸⁸

⁸⁸ Concerning the role of the preamble as constitutional core within the Chinese Constitution (1982), see Georg Gesk, Lee Bing-Nan, Chen Hsian-Wu, *The Chinese Constitution of 1982 Revisited: Between Law and Politics*, Research Paper, Taipei: NTU, 2009, p. 27.

Natural paragraph 13, Preamble, Constitution 1982

This Constitution, in legal form, affirms the achievements of the struggles of the Chinese people of all nationalities and defines the basic system and basic tasks of the State; it is the fundamental law of the State and has supreme legal authority. The people of all nationalities, all State organs, the armed forces, all political parties and public organizations and all enterprises and institutions in the country must take the Constitution as the basic standard of conduct, and they have the duty to uphold the dignity of the Constitution and ensure its implementation.

Sec. 33 IV, Chap. 2, Constitution 1982

Every citizen is entitled to the rights and at the same time must perform the duties prescribed by the Constitution and other laws.

II. Supremacy of Chinese Law – 1.3+ Billion People (2018)

China suffered under semi-colonial oppression beginning in the mid-nineteenth century and lasting until the mid-twentieth century. One of the most visible signs of imperialist powers carving into Chinese sovereignty was the so-called consular jurisdiction, which is the refusal of imperialist powers to accept Chinese laws and court rulings. As a consequence, China is very weary when it comes to international affairs. With only a very few exceptions, any case that has to be decided by Chinese courts is obliged to adhere to Chinese law. The possibility of international arbitration or of both parties agreeing upon application of foreign law to a given contract is very limited and depends upon

- the existence of a legal norm that entitles both parties to do so;
- a clear and written agreement of both parties to make use of the possibilities they are entitled to.

Although China is a party to the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards⁸⁹, both parties to any given contract have to agree upon an arbitration regime before any outcome of said arbitration may gain enforceability. Cyberspace might undermine such a principle. But as a matter of fact, most Chinese will not be able to enter any server that is not subject to Chinese laws and even the VPN-technique is more and more restricted. Therefore national law is clearly dominant.

⁸⁹ China signed the Convention on 22 January 1987, ratification was on 22 April 1987.

III. Priority of Public Law vs. Civil Law vs. Industry Self-Regulation

Although the Chinese internet started out as a rather unregulated cyber space, things gradually changed and Chinese cyber space is now regulated by a variety of different laws and regulations.

In a first wave, cyberspace tried to achieve some kind of order by introducing industry self-regulation. In other words, it was not the cyber citizen that introduced some form of responsibility scheme into cyberspace, but industrial players. As early as 2005, the Chinese E-Commerce Association promulgated the service rules for Internet trading platforms (SRITP, 网络交易平台服务规范). Within SRITP, platform providers even assumed responsibilities that are most often related to public law. According to SRTIP Sec. 7 IV, any platform provider has to notify state institutions of any illegal activities that make use of a respective platform. Since search engines are defined as providers of search results and therefore qualify as platform providers, any company that enters the Chinese realm of cyber space will have to comply with such active reporting practices even under industry self-regulation.

It therefore is no wonder when we see most laws governing cyberspace implementing similar reporting schemes. This diminishes control tasks for state agencies on one hand and increases the responsibility of the platform provider on the other hand. No provider of information, services, or goods can deny the fact of being obliged to flag illegal behavior and to pass relevant data to state agencies. Otherwise, the platform provider itself will be recognized as supporting illegal acts.

The Chinese Internet regulator even took this logic in order to ask platform providers to guarantee in advance that they do not sell fake products. However, with the industry being already a financial heavyweight and politically very well connected, Alibaba and so on had—at least for the time being—succeeded in persuading relevant institutions to limit any responsibility for fake goods.

However, the tendency to “outsource” the obligation of public institutions for monitoring public space and—if needed—to control, prevent, or repress any kind of illegal behavior is a characteristic of the Chinese cyber sphere. The Chinese Internet Security Law (CISL, 中华人民共和国网络安全法) Sec. 21 (3) asks any service provider to proactively store any contact data for at least six months. This is significantly less than the three-year storage requirement of all

relative transaction information we find in SRITP Sec. 16. However, it is still not the state and its agencies that store data, but the service provider, thus turning the responsibilities of monitoring, reporting, and retaining of evidence and thus of a public law obligation into an obligation of (private) service providers.

Hence, we can see public law dominating both, other fields of law (civil/economic law) and industry self-regulation. Ironically it is able to do so, since it only had to enforce structures that industry put into place prior to any regulatory effort by state legislation.

Chinese Internet Security Law (CISL, 中华人民共和国网络安全法) Sec. 21 (3)

The state introduces a graded protection system for internet security. In accordance with this graded protection system for Internet safety, the Internet provider shall fulfil the following Internet protection obligations, guarantee that the Internet is not interrupted, crippled, or visited unauthorized; he shall prevent internet data from being leaked or from being stolen or altered:

...

(3) measuring and recording the action status of the Internet, technical measures for Internet safety, and save Internet protocols in accordance with regulations for at least six months;

...

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

...

(三) 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

...

Service Rules for Internet Trading Platforms (SRITP, 网络交易平台服务规范) Sec. 7 IV

The Internet trading platform provider shall pay attention to security aspects and take realistic and applicable measures in order to guarantee the safety of trade; this includes technical, administrative, and legal measures. In case it notices illegal actions on his trading platform, it shall take adequate measures for timely ending those and report them immediately to respective state institutions.

网络交易平台提供商应高度重视交易的安全性，采取合理可行的措施保障交易的安全，包括技术措施、管理措施和法律措施。在发现其交易平台上存在违法行为时，应采取适当措施及时制止并及时向有关部门反映。

Service Rules for Internet Trading Platforms (SRITP, 网络交易平台服务规范) Sec. 16

Internet trading platform providers have to diligently preserve information, records, and material concerning the Internet exchange happening on their platform in a complete and correct manner in order to be able to retrieve said information etc. as evidence; such information etc. shall be saved for a period of at least three years, beginning with the day the exchange was finalized. The Internet trading platform provider ought to keep digital backup, restore facilities in case of a breakdown in order to safeguard the completeness and correctness of the internet trade data.

网络交易平台提供商应尽谨慎义务保存在其平台上发生的网络交易的相关信息、记录或资料，确保资料的完整性和准确性并使其日后可以调取查用，且保存时间不得少于3年，自交易完成之日起计算。网络交易平台提供商应当采取数据备份、故障恢复等技术手段确保网络交易数据和资料的完整性和安全性。

IV. Consequence: Intranet vs. Internet, or: Restrictions of the Chinese Cyberspace

The above insistence upon application of Chinese public law to any transaction or communication that happens within the Chinese realm of the Internet is cause for conflict with many international service providers, mainly with big international corporations based in the US. In order to enter the Chinese realm of cyberspace, they have to comply with Chinese rules and therefore have to provide transaction protocols and proactively report on cybercrime as defined by Chinese legislation. In all cases where Chinese regulations are more restrictive than in Europe or in the US, this means corporations have to either block some of their content for

Chinese cyberspace, or they are seen as collaborating with instigating violence, advocating for secession, or insulting certain persons or institutions. We have seen in the past that many large providers of either services or of content did draw the consequence and refused to give access to Chinese authorities to enter their servers or to comply in other ways, i.e. they refused to repress content. However, the structural problem that is behind all of these struggles is not solved. As long as one part of cyberspace tries to link applicable laws to the place they provide a server, and other parts of cyberspace insist upon implementing their legal standard to the place where action in cyberspace takes place in terms of individual actors, we have a conflict of laws that is hard to overcome. One way out might be a common cyber agenda with all major players agreeing upon a common framework and common ethical principles.

Still such a quest for an ethical imperative for cyberspace is not easy to achieve. In order to reach this state of affairs, we must combine cyber citizens, service providers, and representatives of political entities (EU, US, China, India, Russia...) and then progress to a common standard. For the time being, this seems out of reach. The clash between political, financial, and public interests seems to prevent us from reaching common ground.⁹⁰ Another way to aim for a common ethical framework might be a general standard put forward by cyber citizens alone. However, when looking at examples of new services that are basically ignoring concerns for responsibilities and aim at minors,⁹¹ we can hardly maintain the fiction that cyber citizens are all mature and therefore might select their cyber actions in accordance with rational choices.

V. Right to Privacy vs. Corporate Interest in Big Data vs. State Interest in Big Data

Although the Chinese Constitution (1982) does not specifically mention a right to privacy, it guarantees freedom and privacy of correspondence (art. 40), allowing for meddling with freedom of correspondence only in case of criminal investigation. However, the right to privacy is guaranteed via ordinary laws, most recently⁹² by the General Principles of Civil Law (GPCL, 民法总则) Sec. 109-111. However, as noted in GPCL Sec. 111, protection of personal data will depend upon legal regulation and further regulation is rather sparsely. As Sec. 111 Sentence 2 formulates, only illegal forms of processing personal data that are legally obtained is

⁹⁰ See i.e. <http://www.bbc.com/news/technology-43070555>, last visited on 16 February 2018.

⁹¹ See i.e. <https://www.nytimes.com/2018/01/30/technology/messenger-kids-facebook-letter.html>, last visited on 16.2.2018.

⁹² The GPCL was promulgated on 15.3.2017 and gained legal effect on 1 October 2017.

forbidden. Therefore, it is totally legal to process data, i.e. within the “wechat” system and combining or pooling information in order to create highly valuable sets of big data.

Annotations to the marked text by Georg Gesk in November 2022

Since legislation of the Chinese Civil Law (CCL) on 28.05.2020, the Chinese Internet presumes a differentiation of personal data in three different clusters: first, there are “private“ (隐私) data that are not supposed to be used in an economic setting, any economic usage of those private data is facing strict normative hurdles (sec. 1032 f. CCL); second, there are personal data that can be handed in for economic purposes by individuals (for a distinction between private and personal data, see sec. § 1034 CCL); third, there are personal data that are shared freely in the virtual realm, therefore allowing for unhindered economic use. This normative settlement aligns in a certain aspect with the argumentation of the German Federal Constitutional Court (Bundesverfassungsgericht), with the latter claiming that a “core area” (Kernbereich) of human rights enjoys “absolute” protection. Since personality rights are accepted as a human right, they share this notion of an absolute protected core area. In Chinese terms, sec. 132 II CCL tries to define this as aspects of personal life such as “private spaces, private actions, and private information, [a person] does not want others to know” (不愿为他人知晓的私密空间、私密活动、私密信息). Since the term that’s being used here is partially different from the term used in right to privacy (隐私), it may well be translated as “intimate” (私密), thus showing even more the parallel line of thought when compared to relevant rulings of the German Constitutional Court (compare BVerfG 1 BvR 472/14, 24.02.2015). Therefore, when others are prohibited from encroaching into the “right to privacy” (隐私权), they are explicitly prohibited from “harming the right to privacy of others by exploring, disturbing, leaking, or making public” (以刺探、侵扰、泄露、公开等方式侵害他人的隐私权) any of the related informations, and thus largely preempting any economic use of privateintimate personal data in China.

The question as to whether personal data can be passed on to third parties is answered in twofold: as long as personal data are anonymous, they can be freely shared, and as long as personal data can be individually identified passing on has to be authorized by relevant individuals. This means, that using personal data to pool big data is possible as long as personal data are anonymous (sec. 1038 CCL); however, the problem of re-individualization of data is not addressed. As long as the big data pool is large enough, almost every personal data can be re-individualized, therefore creating the need for further legislative action.

This tri-partite differentiation of data is not limited to the CCL. The new Chinese Data Protection Law (CDPL, 20.08.2021) makes a similar distinction. However, § 28 CDPL does not mention the term private data, but creates the notion of “sensitive personal data” (敏感个人信息) instead. The iteration of examples of sensitive data in sec. 28 CDPL is focusing on concrete phenomena such as biometrical data, religious belief, special status, medical records etc. (包括生物识别、宗教信仰、特定身份、医疗健康...) instead of referring to privacy in a rather abstract way; therefore, it is only partially congruent with similar norms of the CCL. However, the main aims of both laws are the same: they want to balance a sphere of protection of the individual personality on one hand and corporate interests on the other

hand. Therefore, they create two opposing notions and an intermediate zone in between those two.

One consequence of this attempt at limiting corporate use of personal data via functional and individual protection is a basic shift in public perception. Both, CCL and CDPL have shown, that it is possible to protect personality rights vs. corporate (economic) interests, and have to question whether state authority and its actors are free to use personal data in any way they want. In other words, state authority finds itself in a position where it has to explain and to justify its use of personal data. When state employees in Henan province used the local health app as a tool to stop healthy people from gathering for protests, they provoked a stunned and furious response from the public. Although there was no indictment in criminal law (illegal restriction of personal freedom, falsifying of public records, forging of documents), but responsible persons had to endure disciplinary action, some even losing their job.

This shows how the setting of legal norms in one area of society causes repercussions for other fields: the creation of norms in the field of civil and economic law influences discussion and adjudication in the realm of public law, thus diminishing instances of arbitrariness of executing state power. This shows how the common Western notion of an omnipotent Chinese state, ruthlessly pressing for its paternalistic agenda against its own citizens, does not necessarily add up to facts in real life. On the contrary, society puts up structures that bind all actors – citizens as well as state and party – in a system of responsibility. Therefore “transparency” (see below) is not only a transparency based upon content, but it is more and more gaining aspects of procedural transparency as well.

Since “wechat” integrates functions from messaging to facilitating third-party services or consuming on internet platforms, it gives an opportunity for integrating data on almost every aspect of life without any legal boundaries.

The possibilities for cyber citizens to refuse participating in these data processing clusters are close to non-existent. When analyzing provisions of the Chinese Consumer Protection Law (CPL, 中华人民共和国消费者保护法) under this aspect, we see the problem of unified forms of contract (or the possibility of a cyber consumer to escape pre-formulated contract clauses) addressed in rather mediocre ways. The main focus of legal norms is tied to restrictions of responsibility (CPL Sec. 44 I) without any clause to mention processing of obtained consumption patterns or making further use of information that might be seen as covered by privacy rights. In other words, there is no clause that prevents the platform provider from processing personal data, and there is almost no way for a consumer to preclude such behavior via altering any formalized contracts. To the contrary, if the platform provider argues that processing of data helps to shield the consumer from rogue traders, there might even be a case to construct an obligation for the platform provider to engage in big data mining and processing in order to

guarantee safe transactions. The problem of dual use—protecting the consumer and exposing him/her to more aggressive marketing tactics—is not addressed at all.

Chinese Constitution (1982) Art. 40

Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens' freedom and privacy of correspondence, except in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law.

中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。

Chinese Civil Law (中华人民共和国民法总则) Sec. 109-110

§ 109

Personal freedom and personal dignity of natural persons are protected by the law.

第一百零九条 自然人的人身自由、人格尊严受法律保护。

§ 110

Natural persons enjoy the rights to life, body, health, name, their own picture, credit, honour, privacy, and autonomous decision concerning marriage.

Judicial persons and non-judicial organizations enjoy the right to name, credit, and honour.

第一百一十条 自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。

法人、非法人组织享有名称权、名誉权、荣誉权等权利。

§ 111

Personal data of private persons are protected by the law. In case any organization is in need of obtaining personal data of others, they have to obtain it in accordance with the law and protect the safety of information; illegal selling, using, processing, forwarding of personal information or any publishing of personal information is not allowed.

第一百一十一条 自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

Chinese Law on Consumer Rights (中华人民共和国消费者权益保护法) Sec. 44

A consumer that buys goods or obtains services from an Internet trading platform and whose legal rights and interests are harmed may ask the seller or the provider of services to reimburse damages. In case the Internet trading platform provider is unable to give the consumer the real name, address, and effective contact data of the seller or service provider, the consumer may ask the Internet trading platform provider to reimburse damages occurred; in case the Internet trading platform provider made an even more favorable commitment towards the consumer, the platform provider must come up for fulfillment. After reimbursing the consumer for damages, the Internet trading platform provider can ask the seller or the service provider for reimbursement.

In case an Internet trading platform provider clearly knows or ought to know that a seller or service provider uses the platform to harm legal rights and interests of consumers and did not take necessary action [against such behavior], he shall share common liability together with the seller or service provider.

消费者通过网络交易平台购买商品或者接受服务，其合法权益受到损害的，可以向销售者或者服务者要求赔偿。网络交易平台提供者不能提供销售者或者服务者的真实名称、地址和有效联系方式的，消费者也可以向网络交易平台提供者要求赔偿；网络交易平台提供者作出更有利于消费者的承诺的，应当履行承诺。网络交易平台提供者赔偿后，有权向销售者或者服务者追偿。

网络交易平台提供者明知或者应知销售者或者服务者利用其平台侵害消费者合法权益，未采取必要措施的，依法与该销售者或者服务者承担连带责任。

VI. Consequence: Corporate Mining and Processing of Big Data as a Common Asset in Public law

As we have seen above, big Internet service providers are virtually (and practically) free for mining and processing private information that is obtained in their “corporate” realm of cyberspace. This leads to huge volumes of big data being created and commercially used.

However, the state is stepping into these corporate assets and asks corporations to make these data sets available to common interests. Without this precondition, the newly established concept of the “social credit system”⁹³ would not be viable.

Annotations to the marked text by Georg Gesk in November 2022

This seems to be a misconception: as far as the author can see, most data sets that are incorporated into different subsystems of what is called “Social Credit System” (there is no single SCS, but it is a set of at least 8 different systems) are derived from public data collections. Therefore, the number of data sets integrated into various SCSs differs between each province. (To give only one example: within the evaluation sheet concerning the performance of government employees that are involved with the setup of the local SCS, there are only references to data that are readily available within public administration, no reference to any data of private enterprises is made; see 2018 年江汉区社会信用体系建设工作目标考核计分办法, last visited on 5.12.2019.

The author has no knowledge about evidence that the whole data pool of Tencent (the parent company of WeChat) was integrated into any one of the SCS. The picture appears different when we focus on state security, since any corporate actor has an obligation to report suspicious cases.

As to whether this social credit system with rewards for “positive” behavior in the cyber and the realworld and “negative sanctioning” of “negative” behavior is going to change the whole perception of what it means to “adhere to the laws,” we cannot know now. However, it might be that at one point, legal norms might be perceived as inferior because adhering to norms is most of the time not so easy to control and therefore in its scope much more vague. If this gives rise to a social system that is close to any Orwellian dystopia, or will open up for the utopia of much smarter and less invasive means of social control, we cannot know in advance.

⁹³ See <https://futurism.com/china-social-credit-system-rate-human-value/>, last visited on 16 February 2018.

VII. Quest of Truth, e.g. PR China: Transparency as Precondition of Responsibility and therefore as Necessary Condition for Truth

China perceives cyberspace as a public place. This place is easy to reach for the majority of citizens and allows for decentralized transmission and processing of information. Since both the state and citizens are concerned with “fake news,” i.e. misleading and/or wrongful information, both sides perceive an unregulated cyberspace as high risk. Therefore, many citizens agree upon the need for regulation of cyberspace and the Internet.

This means that Chinese cyberspace relies less upon the maturity of usage by citizens and tends to make use of a more or less paternalistic model of state regulation. This logic leads to a semi-public list of selectors⁹⁴ that try to prevent users from generating texts concerning sensitive topics on one hand and to guarantee publicity and transparency of any message published on the Internet on the other.⁹⁵ The fact that lists of selectors are semi-public leads to an interaction with cybercitizens: on one hand, allowing the creative circumvention of restrictions and on the other hand, leading to the need for an extensive institutional structure of state-run monitoring systems in order to “upgrade” relevant lists of selectors.⁹⁶ Although there is a semi-public interaction concerning lists of selectors, the power to decide upon what notions are introduced into these lists clearly remain with state-run agencies; the reasons for doing so remain opaque.⁹⁷ Still, the fact that at least parts of selector lists are partly public allows cybercitizens to engage in a “concealed informed choice.” “Truth” in cyberspace is therefore a function constructed by pluralistic reporting of events and selective authoritative interpretation of events.⁹⁸

⁹⁴ See i.e. <http://cj.sina.com.cn/article/detail/1480190601/462756>, last visited on 13 February 2018, news from March 2017.

⁹⁵ The mere fact that lists of “forbidden expressions” are published and discussed in mass media is proof of the fact that these lists show ways to steer clear of unwanted censorship or other repercussions. In parts, this is expressly stated as intent in related discussions, see http://www.sohu.com/a/158448364_570250, last visited on 13.2.2018.

⁹⁶ See <https://www.reuters.com/article/us-china-internet/chinas-internet-police-open-a-window-on-web-censorship-idUSKBN0OH17N20150601>, last visited on 13 February 2018.

⁹⁷ The existence of a hotline for reporting cyberspace crimes (and for tracking reported cases) shows that any list of selectors is at least in part a reflection of concrete experiences of cyber citizens. However, the criteria for developing selectors are nonetheless not publicly available: see <http://www.cyberpolice.cn/wfjb/>, last visited on 13 February 2018.

⁹⁸ Concerning the latter, we find a positive and a negative list of either policy aims or of actions and outcomes to be avoided in Law on Internet Security (LIS, 中华人民共和国网络安全法) Sec. 12. Any list of restrictive selectors ought to be (and as far as published is) in line with this passage.

In case any discourse between cyber citizens or instances of single statements in cyberspace create danger or harm despite all precautionary measures, state institutions monitoring the Internet insist upon the principle of individual responsibility of the user.⁹⁹

Annotations to the marked text by Georg Gesk in November 2022

This account does not recognize the different “ranking” of individuals, being translated into different spheres of movement of individuals at different ranks. What is the personalized internet experience of Western consumers (and potential buyers) translates into a personalized freedom to access and exchange of information of individuals and institutions alike. How strict any restriction to access and exchange information is, depends in part upon personal criteria (trusted entity) that can change over time, leading – on the negative end – to individuals being completely or partially blocked from accessing or exchanging comments on different levels, either outside of China or inside of China or both. The paternalistic control of digital content is therefore not a simple and categorical division into a pure yes/no-dichotomy, but is much smarter, leading to personalized content availability that is as intriguingly differentiated as in Western systems. Only the parameters to personalize content seems to be different, since Chinese granularity of access is – at least in part – aligned to the criteria trusted/non-trusted with all shades in between.

However, in order to make such a principle operable, the state insists upon the possibilities of retaining proof and of making any statement in cyberspace traceable throughout an extended period of time.¹⁰⁰ The idea of doing so is positive prevention. Since individual participants have no possibility of enforcing sanctions on rogue users, any sanctioning scheme must come from supra-individual actors.¹⁰¹ Within the multitude of supra-individual actors, the principle of state sovereignty prevents state agencies from relinquishing this power to private companies or other collective entities. It is therefore a task to be fulfilled by state agencies to regulate (and sanction) cyberspace. Within this context, privacy concerns¹⁰² are only of limited concern and in part precluded by the presumption of notions of “public space”¹⁰³ and “publicity.”

⁹⁹ We see therefore a process similar to what Foucault described as ‘raréfaction’ of ‘discourse’ itself or of individual instances of ‘énoncé’ within a given discourse through application of power, Concerning possibilities for a système d’exclusion or the systematic curtailment of a given discourse, see in general Michel Foucault, *L’Ordre du Discours*, Paris: Gallimard, 1971, p. 21; concerning the functioning of raréfaction, see *ibid.* p. 54f.

¹⁰⁰ Communication protocols have to be kept for at least six months in accordance with LIS Sec. 21 No 3.

¹⁰¹ In this respect, see Qi Xiong, *Massenmedien und Strafrecht*, Berlin: Duncker & Humblot, 2012.

¹⁰² Regulations for the Protection of Personal Information of Telecommunication and Internet Users (电信和互联网用户个人信息保护规定).

¹⁰³ Public in this sense means a space that allows only for limited privacy, as any participant has to be able to provide real data concerning his or her identity at any time: according to LIS Sec. 24 I, any participant on the internet is obliged to provide personal data such as name, ID-Nr. etc. This principle is enforced by the possibility of sanctioning service providers in case they do not enforce authentication rules, see LIS Sec. 61.

As a consequence of this regulatory approach, cyberspace is perceived as a transparent space that has to maintain individualized “real name” participants, traceability of content after publication in order to achieve responsibility, and thus aims at achieving transparency. State actors assume that this approach is necessary in order to guarantee a publicly acceptable minimum of truth.

Questions concerning potential conflicts between the assumptions of truth, responsibility, and transparency are suppressed in order to maintain the above-stated monitoring structure.

B. Let's talk about Cyberlaw – Insights by Christoph Merkelbach

Georg Gesk's insights are the only means of access if the standard does not provide for a strategy regarding how to communicate with other Chinese knowledge bearers. Christoph Merkelbach – the linguist – focused on this challenge with the oral presentation at the second annual conference of the 2017 Jean Monnet Centre of Excellence EU in global dialogue: “Let's Talk about Cyberlaw!” (“Lasst uns über Cyberlaw reden!”)


Lasst uns über Cyberlaw reden!
Eine fremdsprachendidaktische Perspektive
am Beispiel des Sprachenpaares Deutsch/Chinesisch



22.02.2018 | Sprachenzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 1

ZIKK

Gliederung des Vortrags




- Ausgangslage
- Besonderheiten der Fachsprache Jura (FsJ)
 - textstrukturelle Besonderheiten
 - syntaktische / grammatische Besonderheiten
 - lexikalische Besonderheiten
- Konsequenzen

22.02.2018 | Sprachenzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 2

ZIKK

Besonderheiten der FsJ




- Juristischen Probleme beziehen sich immer auf einen empirischen überprüfbareren Sachverhalt
- FsJ ist keine technisch-naturwissenschaftliche FS
- FsJ ist Produkt eines argumentativen Diskurses
- Termini sind schwer zu erkennen und zu semantisieren
- FsJ verwendet (i.d.R.) keine Symbole
- Verhältnis Satzlänge/Termini ist unterschiedlich zu anderen FS

22.02.2018 | Sprachenzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 3

ZIKK

Unterschied FsJ und technische Fachsprachen



„Verglichen mit den technisch-naturwissenschaftlichen Fachsprachen unterliegt die Rechtssprache einer geringen Beeinflussung durch moderne Fremdsprachen [...] Während in den [anderen] Fachsprachen neue Benennungen als notwendige Folge des technischen Fortschritts gebildet werden, entscheiden Juristen selbst darüber, ob ein juristischer Ausdruck durch einen neuen zu ersetzen ist.“

Znamenáková, Katherina. 2007. "Fachsprachliche Wortgruppen in Textsorten des deutschen Zivilrechts." In: Gejek, Barbara (Hg.) *Rechtssprache Beiträge zur deutschen Sprach- und Literaturwissenschaft*. Frankfurt am Main, 29.

22.02.2018 | Sprachenzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 4

ZIKK

Textstrukturelle Besonderheiten



- Eine linguistisch begründete, quantitativ und qualitativ abgesicherte Differenzierung von juristischen Fachtextsorten gibt es noch nicht.
- Fachtexte werden nach Sprachfunktionen untersucht: deskriptive, instruktive, direktive Funktion
- Juristische Textsorten enthalten unterschiedliche Sprechakte (z.B. Verordnungen, Gesetzeskommentar)
- Eine linguistische Beschreibung von juristischen Textsorten muss systematisch, funktional, kontextuell und nach Ebenen abgegrenzt werden
- Vorrangig noch eine hermeneutische Klassifikation

22.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 5



Textstrukturelle Besonderheiten



- Kohärenzprinzipien
- formale Textorganisation
- Themenentfaltung
- textkonstitutive Sprachhandlungsmuster

22.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 6



Kulturspezifik von Texten



„Die Rahmenbedingungen, unter denen Texte entstehen, werden im weiteren Sinne durch den Kulturraum geprägt, zu dem ein Autor gehört bzw. für den er schreibt, sowie durch die Kontakte, d.h. den sozialgesellschaftlichen Bereich, im bzw. für den ein Text produziert wird.“

Jakobs, Eva-Maria (1997): Textproduktion als domänen- und kulturspezifisches Handeln. Diskutiert am Beispiel wissenschaftlichen Schreibens. In: Adamić, Kirzen/ Ancoz, Gerid/ Jakobs, Eva-Maria (Hrsg.): Domänen- und kulturspezifisches Schreiben. Frankfurt/ M.: Peter Lang, 10.

22.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 7



Kulturspezifik von Texten



Studien bewiesen, „dass ein kultureller Hintergrund in der Textorganisation zu finden ist und daß die dadurch entstandenen Textmerkmale keinen strikten linguistischen Ursprung haben, sondern sie entsprechen [...] kulturspezifischen Denkstrukturen – ‚kulturelle Imperative‘ [...] - die durch Bildungsinstitutionen und Erziehung vermittelt werden.“

Francois, A. (2004) Wissenschaftliches Schreiben in der Fremdsprache Deutsch am Beispiel von Abschlussarbeiten französischer Studierender. Dissertationsschrift: Universität Siegen, 41.

22.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 8



Kulturspezifik von Texten



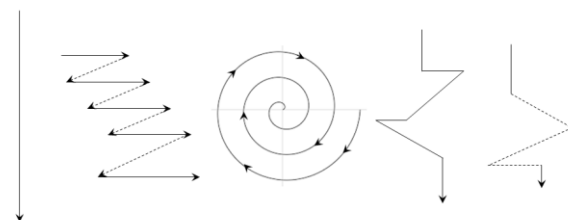
„Wenn jemand Englisch als Fremdsprache spricht, besteht die Tendenz, die subjektiven Bedeutungen der Muttersprache beizubehalten [...] Es besteht daher eine erhöhte Chance, dass Leute nicht mit der gleichen Bedeutung sprechen, selbst wenn sie die selbe Sprache verwenden.“

Fisher, G. (1980) International Negotiation: A Cross-Cultural Perspective. Chicago: Intercultural Press, 62.

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 9



English Semitic Oriental Romance Russian



Kaplan, Robert (1966) Cultural Thought Patterns in Intercultural Education. Language Learning 16 (1-2), 1-20

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 10



deutsch		mexikanisch*
Information über einen objektiven Sachverhalt	Textfunktion	Information über einen objektiven Sachverhalt und eine subjektive Einstellung
komplexe, abstrakte, (neg.) kritische Theoriedarstellung mit wenig Praxis	Textinhalt	eingegrenzte, konkrete Praxisdarstellung mit wenig Theorie
stark argumentativ und subordinierende Themenentfaltung	Textstruktur	stark deskriptiv mit koordinierter Themenentfaltung
unpersönlich, nicht leserbezogen, begrifflich	Textstil	persönlich, leserbezogen, begrifflich + ästhetisch

*Anmerkung: Grundlagenforschung zu Chinesisch fehlen hier. Mexikanisch wird zur Illustration der Problematik herangezogen.

Esse, Ruth (1997): "Etwas ist mir geheim geblieben am deutschen Referat." Kulturelle Geprägtheit wissenschaftlicher Textproduktion und ihre Konsequenzen für den universitären Unterricht von Deutsch als Fremdsprache. München: iudicum, 10

Komprimierung:

- Substantivierung
- Erweiterte Nominalphrasen:
 - a) Satzglieder anstelle von Gliedsätzen
 - b) Adjektiv-, Partizipial-, Präpositionalgruppen und andere Attribute.

Allgemeingültigkeit/Objektivität:

- Passivischen Formen in der 3. Person Singular im Präsens
- Funktionsverbgefüge

Notwendigkeiten/zwingende Anordnungen:

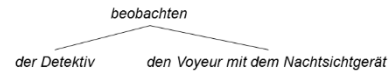
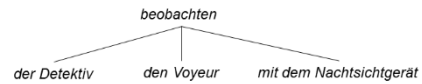
- Modale Infinitivkonstruktionen
- Konditionale Konjunktionen

Beispielsatz

Der Detektiv beobachtete den Voyeur mit dem Nachtsichtgerät.

Beispielanalyse: Valenz-/Dependenzgrammatik

Der Detektiv beobachtete den Voyeur mit dem Nachtsichtgerät.

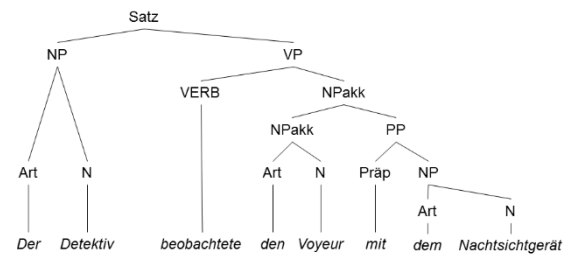
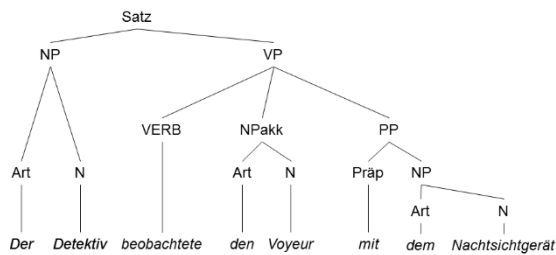


Beispielanalyse: KS-Grammatik

Der Detektiv beobachtete den Voyeur mit dem Nachtsichtgerät.

Beispielanalyse: KS-Grammatik

Der Detektiv beobachtete den Voyeur mit dem Nachtsichtgerät.



Lexikalische Kennzeichen der juristischen Fachsprachen



1. Terminologisierung (Person, 力能任責),
2. Wortzusammensetzung (Eigentumsvorbehalt, 留保權有所),
3. Derivation (**un**lauter, vermeid**bar**, 任責失過**無**, 制產財妻**夫**),
4. Konversion (Verweisen, 託委政**行**),
5. Entlehnung (Factoring, 分處假, 院法法憲)
6. Kürzungsverfahren (EU-Vertrag, 0,5-Promille-Grenze, 效失, 世入),
7. seltener durch Neubildungen.

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 17



Bsp. Drohne deutsch/chinesisch



1. 雄蜂 [Drohne als zoologischer Begriff]
2. * 雄蜂机 [Drohne als zoologischer Begriff+ Maschine]
3. 无人机 [ohne Mensch Maschine]
oder
4. 无人驾驶机 [ohne Mensch Fahrer Maschine]

Die Übersetzung des englischen Begriffs *drone* ins Chinesische wurde zunächst über den biologischen Begriff mit dem Zusatz *Maschine* vor allem in der Umgangssprache geleistet. Dieser hat sich jedoch nicht durchgesetzt. Die Begriffe in den Zeilen 3. und 4. haben sich heute allgemein durchgesetzt, im übertragenen Sinne als *unbemannter Maschine*. Aus dem Chinesischen geht nicht eindeutig hervor, dass die Maschine auch fliegt. Dies kann man nur aus dem Kontext erschließen.

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 18



Fachsprache ist mehr als Fachterminologie



Eine Fachsprache ist „Mittel einer optimalen Verständigung über ein Fachgebiet unter Fachleuten; sie ist gekennzeichnet durch einen spezifischen Fachwortschatz und spezielle Normen für die Auswahl, Verwendung und Frequenz gemeinsprachlicher lexikalischer und grammatischer Mittel; sie existiert nicht als selbständige Erscheinungsform der Sprache, sondern wird in Fachtexten aktualisiert, die außer der fachsprachlichen Schicht immer gemeinsprachliche Elemente enthalten“

Schmidt, Wilhelm. 1969. "Charakter und gesellschaftliche Bedeutung der Fachsprachen." In: Sprachpflege 18 (6.A.), 10-20

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 19



Fachsprache ist mehr als Fachterminologie



- Fachsprache als präzises und differenziertes Verständigungsmittel ist als eine Gesamtheit aller sprachlichen Mittel anzusehen
- Fachsprache wird in einem fachlich begrenzten Kommunikationsbereich verwendet
- Fachsprachen sind keine selbständigen, geschlossenen Sprachsysteme, sondern besitzen vielfältige Beziehung zur Gesamtsprache.
- Die Grenze zwischen Fachsprache und Gemeinsprache liegt in der Sprachverwendung und -funktion.
- Fachsprachen verfügen über keine autonomen phonologischen, lexikalischen oder syntaktischen Ebenen

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 20



Fachsprache ist mehr als Fachterminologie



- Wenn sich also juristisch etwas verändert, ist dies eine Neuerung, die innerhalb der Gesellschaft bereits vollzogen oder als relevantes Problem allgemein erkannt ist
- die Rechtswissenschaft greift auf die Sprache des Gemeinwesens zurück.

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 21



Fachsprache ist mehr als Fachterminologie



- Für die juristischen Fachsprachen des Chinesischen: der Bruch in der chinesischen Rechtstradition, welcher von Staats wegen Ende des 19., Anfang des 20. Jahrhunderts vollzogen wurde, brachte ein legislatives Muster der voreilenden Gesetzgebung hervor = westliche Handlungsmuster werden normiert, denen zum Zeitpunkt der Gesetzgebung keine innergesellschaftlichen Handlungsmuster entsprach.
- Gesetzgeber setzt durch den legislativen Akt Begriffe fest, welche erst in der Folge Eingang in den Sprachschatz der Gemeinsprache finden.

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 22



Konsequenzen für den Fachsprachenunterricht



- die lexikalische Differenzierung der dogmatischen und normativen Ebene nur dem Fachmann ersichtlich
- Fachdenken ohne Fachsprache nicht möglich ist, aber auch Fachsprache nicht ohne Fachdenken

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 23



中华人民共和国网络安全法



Article 1: This law is formulated so as to ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social informatization. *

第一条 为了保障网络安全, 维护网络空间主权和国家安全、社会公共利益, 保护公民、法人和其他组织的合法权益, 促进经济社会信息化健康发展, 制定本法。*

di yī tiáo wéi le bǎo zhàng wǎng lù ān quán, wéi hù wǎng lù kōng jiān zhǔ quán hé guó jiā ān quán、shè huì gōng gòng lì yì, bǎo hù gōng mín、fǎ rén hé qì tā zú zhǐ dí hé fá quán yì, cù jìn jīng jì shè huì xī huà jiàn kāng fā zhǎn, zhì dìng běn fǎ。

Artikel 1 Um die Netzwerksicherheit zu gewährleisten, Cyberspace Souveränität und nationale Sicherheit, das öffentliche Interessen, Schutz der legitimen Rechte und Interessen der Bürger, juristischen Personen und anderen Organisationen zu sichern, um die gesunde Entwicklung der wirtschaftlichen und sozialen Informationen zu fördern, wird dieses Gesetz in Kraft gesetzt.

- <http://www.chinalawtranslate.com/cybersecuritylaw/2angwen>
- http://www.npc.gov.cn/npc/zwjw/2016-11/07/content_2081605.htm

26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 24



Dr. Christoph Merkelbach
Technische Universität Darmstadt
Sprachzentrum / Zentrum für Interkulturelle Kompetenz
Hochschulstraße 1
S1|03 R 314c
64289 Darmstadt
cmerkelbach@spz.tu-darmstadt.de



26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 25



26.02.2018 | Sprachzentrum | Zentrum für Interkulturelle Kompetenz | Dr. Christoph Merkelbach | 26



Part 9: Summing up

The motivation for this project is threefold:

- Avoiding the use of force and weapons,
- furthering harmony or organizing opposition and dissent among citizens of the globe in their united quest of truth (truth being perhaps a timeless ideal in a transnational and transdisciplinary perspective) and
- generating knowledge capital concerning success and failure in cybergovernance.

It should be emphasized that the bullet points are interdependent: The competition of arguments requires the integration of different and contradictory actors, strategies and activists. The challenge is not the closed discourse of mobocracy or “algocracy”, not the paternalistic exposition of the consensus, but the organization and tolerance of dissent. This project is a

first step along the way to find common ground between such different systems as Germany-Europe, China and the US.

Viola Schmid is supported by the following institutions:



Part 10: Appendix – Further in-depth Information and Citations of International, European Union and German law

The appendix contains further information regarding the statutes in this contribution. From a European-German perspective, we are used to thinking in a multilevel jurisdiction model integrating International Law, European Union Law and German Law (State and Federal Law). Within these jurisdictions, we differentiate between Primary and Secondary Law – e.g. Constitutional and Statutory Law (in Germany). The statutes are shortened, which is denoted with [...]. The emphases stem from the author. Translations of German statutes are – if available – provided by the German Federal Ministry

of Justice and Consumer Protection with the following note: “Translations of these materials into languages other than German are intended solely as a convenience to the non-German-reading public. Any discrepancies or differences that may arise in translations of the official German versions of these materials are not binding and have no legal effect for compliance or enforcement purposes.”¹⁰⁴ Also not every reference (in footnotes) is translated. If readers are interested in further information in English, please feel free to contact the author (schmid@cylaw.tu-darmstadt.de).

A. International Law – Statute of the International Court of Justice¹⁰⁵

Art. 38

1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: [...]
- d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.
[...]

B. European Union Law

I. Primary Law – Consolidated Version of the Treaty on European Union¹⁰⁶

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on the Functioning of the European Union - Protocols - Annexes - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 - Tables of equivalences

¹⁰⁴ https://www.gesetze-im-internet.de/Teilliste_translations.html (14.02.2018).

¹⁰⁵ <http://www.icj-cij.org/en/statute> (14.02.2018).

¹⁰⁶ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT> (14.02.2018).

Art. 6

[...]3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law. [...]

Art. 67

1. The Union shall constitute an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States. [...]

II. Secondary Law

1. General Data Protection Regulation¹⁰⁷

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Art. 4 – Definitions

- (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; [...]
- (13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that

¹⁰⁷ <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679> (14.02.2018).

natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- (14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- (15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status; [...]

Art. 9 – Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. [...]

Art. 35 – Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. [...]

Art. 99 – Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from 25 May 2018.

2. Data Protection Directive¹⁰⁸

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for

¹⁰⁸ <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016L0680> (14.02.2018).

the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Art. 63 – Transposition

1. Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. [...]
2. [...] where it involves **disproportionate effort** [...] by 6 May 2023.
3. [...] in **exceptional circumstances** [...] 6 May 2026.

3. Regulation on Privacy and Electronic Communications (de lege ferenda)

a) Council of the European Union – Proposal 12/5/17¹⁰⁹ – Application Date in Brackets

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Art. 29 – Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from [25 May 2018].

b) European Commission – Proposal 1/10/17¹¹⁰

Art. 29 – Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from 25 May 2018.

¹⁰⁹ http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15333_2017_INIT&from=EN (Stand: 01.02.2018).

¹¹⁰ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010> (Stand: 01.02.2018).

C. German Law

I. Primary Law – Basic Law for the Federal Republic of Germany (German Constitution; Grundgesetz, GG)¹¹¹

Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by Article 1 of the Act of 23 December 2014 (Federal Law Gazette I p. 2438)

Art. 1 – Human dignity – Human rights – Legally binding force of basic rights

- (1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.
- (2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world.
- (3) The following basic rights shall bind the legislature, the executive and the judiciary as directly applicable law.

Art. 2 – Personal freedoms

- (1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.
- (2) Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant to a law.

Art. 5 – Freedom of expression, arts and sciences

- (1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures [...]

Art. 20 – Constitutional principles – Right of resistance

- (1) The Federal Republic of Germany is a democratic and social federal state. [...]
- (3) The legislature shall be bound by the constitutional order, the executive and the judiciary by law and justice.

¹¹¹ http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html (14.02.2018).

Art. 20a – Protection of the natural foundations of life and animals

Mindful also of its responsibility toward future generations, the state shall protect the natural foundations of life and animals by legislation and, in accordance with law and justice, by executive and judicial action, all within the framework of the constitutional order.

Art. 28 – Land constitutions – Autonomy of municipalities

(1) The constitutional order in the Länder must conform to the principles of a republican, democratic and social state governed by the rule of law, within the meaning of this Basic Law. [...]

(3) The Federation shall guarantee that the constitutional order of the Länder conforms to the basic rights and to the provisions of paragraphs (1) and (2) of this Article.

Art. 79 – Amendment of the Basic Law

[...] (3) Amendments to this Basic Law affecting the division of the Federation into Länder, their participation on principle in the legislative process, or the principles laid down in Articles 1 and 20 shall be inadmissible.

Art. 91c – Information technology systems

(1) The Federation and the Länder may cooperate in planning, constructing, and operating information technology systems needed to discharge their responsibilities.

(2) The Federation and the Länder may agree to specify the standards and security requirements necessary for exchanges between their information technology systems. Agreements regarding the bases of cooperation under the first sentence may provide, for individual responsibilities determined by their content and scope, that detailed regulations be enacted with the consent of a qualified majority of the Federation and the Länder as laid down in the agreements. They require the consent of the Bundestag and the legislatures of the participating Länder; the right to withdraw from these agreements cannot be precluded. The agreements shall also regulate the sharing of costs.

(3) The Länder may also agree on the joint operation of information technology systems along with the establishment of installations for that purpose.

(4) For linking the information networks of the Federation and the Länder, the Federation shall establish a connecting network. Details regarding the establishment and the operation of the connecting network shall be regulated by a federal law with the consent of the Bundesrat.

II. Secondary Law

1. Federal Data Protection Act (until 5/25/2018; Bundesdatenschutzgesetz, BDSG)¹¹²

Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814)

Section 3 – Further definitions

(1) “Personal data” means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject). [...]

Section 9 – Technical and organizational measures

[...] Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection.

Annex (to the first sentence of Section 9 of this Act)

Where personal data are processed or used automatically, the internal organization of authorities or enterprises is to be arranged in such a way that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or data categories to be protected shall be taken,

1. to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used (access control),
2. to prevent data processing systems from being used without authorization (access control),
3. to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage (access control),
4. to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (transmission control),

¹¹² http://www.gesetze-im-internet.de/englisch_bdsch/englisch_bdsch.html (14.02.2018).

5. to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed (input control),
 6. to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (job control),
 7. to ensure that personal data are protected from accidental destruction or loss (availability control),
 8. to ensure that data collected for different purposes can be processed separately.
- One measure in accordance with the second sentence Nos. 2 to 4 is in particular the use of the latest encryption procedures.

2. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG)¹¹³

Das G wurde als Art. 1 des G v. 1.9.2017 I 3352 vom Bundestag beschlossen. Es ist gem. Art. 3 dieses G am 1.10.2017 in Kraft getreten.

§ 3 – Umgang mit Beschwerden über rechtswidrige Inhalte

- (1) Der Anbieter eines sozialen Netzwerks muss ein wirksames und transparentes Verfahren [...] für den Umgang mit Beschwerden über rechtswidrige Inhalte vorhalten [...]
- (2) Das Verfahren muss gewährleisten, dass der Anbieter des sozialen Netzwerks
 1. unverzüglich von der Beschwerde Kenntnis nimmt und prüft, ob der in der Beschwerde gemeldete Inhalt rechtswidrig und zu entfernen oder der Zugang zu ihm zu sperren ist [...]

3. Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU¹¹⁴

Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) [...] ausgegeben zu Bonn am 5. Juli 2017

¹¹³ <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> (14.02.2018).

¹¹⁴ https://www.bgbl.de/xa-ver/bgbl/start.xav?start=%2F%2F%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#_bgbl_%2F%2F%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D_1518625425768 (14.02.2018).

Art. 8 – Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am 25. Mai 2018 in Kraft. Gleichzeitig tritt das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 7 dieses Gesetzes geändert worden ist, außer Kraft.

(2) Artikel 7 tritt am Tag nach der Verkündung in Kraft.

4. Code of Civil Procedure (Zivilprozessordnung, ZPO)¹¹⁵

Code of Civil Procedure as promulgated on 5 December 2005 (Bundesgesetzblatt (BGBl., Federal Law Gazette) I page 3202; 2006 I page 431; 2007 I page 1781), last amended by Article 1 of the Act dated 10 October 2013 (Federal Law Gazette I page 3786)

Section 371a – Evidentiary value of electronic documents

(1) The rules concerning the evidentiary value of private records and documents shall be applied mutatis mutandis to private electronic documents bearing a qualified electronic signature. The appearance of authenticity of a declaration available in electronic form, as obtained from reviewing it pursuant to the Electronic Signature Act (Signaturgesetz), can be cast into doubt only by facts giving rise to serious doubts as to the declaration having been made by the holder of the signature key.

(2) Where an individual has registered securely for a “De-Mail” account that is assigned solely to that individual (section 4 (1), second sentence, of the Act on De-Mail (De-Mail Gesetz)), the appearance of authenticity attendant on an electronic message sent from this De-Mail account, as resulting from the verification of the sender authentication pursuant to section 5 (5) of the Act on De-Mail, will be called into question only by facts giving rise to serious doubts as to the message with that content having been sent by that person.

(3) The rules concerning the evidentiary value of public records and documents shall be applied mutatis mutandis to electronic documents created, in accordance with the requirements as to form (public electronic documents), by a public authority within the purview of its official responsibilities, or by a person or entity vested with public trust within the sphere of business assigned to him or it. Where the document bears a qualified electronic signature of the public authority that has created it, or of the person or entity vested with public trust, section 437 shall apply mutatis mutandis. The same shall apply if an accredited service provider furnishes the document, on behalf of the public authority that has created such document, or on behalf of the person or entity vested with public trust that has created such document, with his qualified electronic signature pursuant to section 5 (5) of the Act on

¹¹⁵ http://www.gesetze-im-internet.de/englisch_zpo/englisch_zpo.html (14.02.2018).

De-Mail and the sender authentication identifies the public authority that has created such document, or the person or entity vested with public trust, as the user of the De-Mail account, or the person or entity vested with public trust.

5. Code of Administrative Court Procedure (Verwaltungsgerichtsordnung, VwGO)¹¹⁶

Code of Administrative Court Procedure in the version of the promulgation of 19 March 1991 (Federal Law Gazette I page 686), most recently amended by Article 5 of the Act of 10 October 2013 (Federal Law Gazette I page 3786)

Section 102a

(1) The court may permit those concerned, their proxy-holders and counsel, on request or ex officio, to be in another place during an oral hearing and to implement procedural acts there. The hearing shall be transmitted simultaneously in image and sound form to this place and to the courtroom.

(2) The court may permit on request that a witness, an expert or a concerned party is in another place during questioning. The questioning shall be transmitted simultaneously in image and sound form to this place and to the courtroom. If those concerned, proxy-holders and counsel have been permitted in accordance with subsection 1, first sentence, to be in another place, the questioning shall also be transmitted to that place. [...]

Published under CC-BY 4.0 International (<https://creativecommons.org/licenses/by/4.0>)

¹¹⁶ http://www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.html (14.02.2018).