CYlaw-Report XLIII

TECHNISCHE UNIVERSITÄT DARMSTADT

ISSN: 1867-1969

Viola Schmid in 2023/06: „Weltrecht^2 Backbone Documents“

→ here

“ORAL WCCL - LAUNCH“: “MULTIDISCIPLINARY CONSTITUTIONAL LAW SCHOLARSHIP FROM GERMANY AND THE EU” ON DEC. 7TH 2022

ABSTRACT:

(1) Weltrecht^2 – Backbone & Entourage Documents are milestones in the process of developing a textbook with the title „Weltrecht^2 – a new Perspective on Legal Science [Weltrecht^2 – eine neue Perspektive auf Rechtswissenschaft]“. The project was launched in three continents in December 2022 with the submission of a relevant 10,000-word paper[1]. This Cylaw-Report XLIII provides a reproduction of the **oral presentation**.[2]

(2) During the launch, the oral presentation addressed the below topics:

- A temporally oriented comparative law of TRADITIONAL-, CYBER- and AILAW- (LAW CONE) (own terminology (ot)) and
- Arguments for Weltrecht^2 which also tackle the challenges posed by the workshop chairs (Workshop 27) - „Why the Classic Model of Constitutionalism might not Suffice for the Best Possible Governance (for an AI-Driven World)”.

(3) The presentation was held in English. Further updated information regarding the Weltrecht^2 project will be shared in the immediately published Cylaw-Report XLIV [„Viola Schmid in 2023/06: „Weltrecht^2 Entourage Documents“ → here ZUKUNFT DES DIGITALEN (STAATS-)RECHTS“ [„DLT-Staatsinfrastruktur“, „Plattformmenschen“ and l’origine du monde] on April 24, 2023] (PRESENTATION MANUSCRIPT: „THE FUTURE OF DIGITAL (PUBLIC) LAW [“DLT state infrastructure”, “platform people” and l’origine du monde]).

(4) Reservoir for Global Knowledge: German – European AI-Jurisprudence of 2022 and 2023 (3 Judgments) on „information technology relevant security law”

[1] In the meantime published as Cylaw-Report XXXXII (XLII) „Viola Schmid in 2023/01: „Weltrecht^2 Backbone Documents“.
→here “PAPER“: “MULTIDISCIPLINARY CONSTITUTIONAL LAW SCHOLARSHIP FROM GERMANY AND THE EU”

[2] Regarding the topic cluster Weltrecht^2: This Cylaw-Report builds on the Cylaw-Report XXXXII (s. Chapter 5) and complements the written submission published therein with the documented, oral presentation at the World Congress of Constitutional Law (WCCL) ON DEC. 7TH 2022. It contains information regarding the launch of Weltrecht^2 on three continents. The Cylaw-Report is based on a speech manuscript that was forwarded prior to the conference. For the sake of good order, the enclosed presentation slides will also be reproduced.

(a) This review (Chapter 4) will be complemented with current information regarding a new case law by the Federal Constitutional Court (Bundesverfassungsgericht - BVerfG) on „information technology relevant security law“ of the Federal Republic of Germany. Another judgment of the Court of Justice of the European Union (CJEU) addresses the organization of flight data (Passenger Name Records (PNR)). A further decision regarding the automated utilization of data from information technology systems within the Asylum Act (Asylgesetz) and Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory (Aufenthaltsrecht) of the Federal Administrative Court (Bundesverwaltungsgerichts – BVerwG) is communicated.

(b) At the heart of those three decisions lies an information technology that carries the unwieldy title: „Verarbeitung gespeicherter Datenbestände durch automatisierte Anwendung zur Datenanalyse oder –auswertung.“ As this phrasing originates from German jurisdiction and legislation (§ 25a HSOG), the German terminology will also be retained in the English language publication. At this point, we offer only a possible translation proposal: „processing of stored personal data through automated data analysis (Hesse) or automated data interpretation (Hamburg).“[3]

(c) These recent developments in German-European CYBER- and AILAW are meant as contributions to a global pool of **LEGAL FOREKNOWLEDGE**.

(5) As the individual Cylaw-Reports of the Cylaw-Report series are in principle meant to be self-explanatory, Chapter 5 refers to Cylaw-Report XXXXII (XLII).

PRAGMATIC GUIDELINES FOR THE READER:

In "global" innovation law (i.e., CYBER- and AILAW), the age-old dilemma of having to choose between the devil and the deep blue sea, or in Greek mythology, having to navigate between *Scylla*, the six-headed monster and *Charybdis*, the massive whirlpool, has proven itself to be true. The frequency and speed of publications currently occurring in various contexts (e.g., lecture formats, written publications in several disciplines with various citation styles, etc.) that are not written in the author's native language is *Scylla*. Those authors who try to avoid *Scylla* and instead place the highest value on accounting for every detail (both formally and in terms of content) and then claim that they have thoroughness on their side will, however, not be protected from *Charybdis* either. In the vortex of time, such a publishing strategy will not be able to escape the whirlpool and will invariably become outdated due to impending obsolescence. Therefore, in order to gain an audience for Weltrecht^2 as quickly as possible and to ensure the highest possible quality, the following pragmatic stylistic approach has been adopted for publications:

(1) Formal differentiations are accepted. For example, in the following text, German terms are indicated with [...] but in another text with (...). This is a result of the variation in written contexts – e.g., the Federal Constitutional Court publishes its information in a different style than the author.
(2) Slides: The text formats used here are inserted in frames and titled as slides/transparencies.

[3] Following Federal Constitutional Court: Press Release No. 18/2023 of 16 February 2023 to Judgment of 16th Feb, 2023.

(3) "...": Inverted commas have four possible functions in the author’s (Viola Schmid) work. Firstly, they indicate direct speech. Secondly, they indicate literal or direct quotations. Thirdly, they reflect the author's own terminology (ot) (neologisms). Fourthly, they emphasize the (lack of) unambiguity in terminologies.

(4) '...', '...' and '...': Punctuation intricacies such as the stringent requirements of German, British or US styles of inverted commas are pragmatically dispensed with in this 1.0 version. These punctuation style variations, too, are reserved for further versions in the same way that different text production cultures are recognized.

(5) Citation etiquette: Given the stringent and pragmatic handling of German-English text conventions in legal texts, the following etiquette has been adopted for the present purposes in the translation of relevant documents, i.e., German writing conventions such as the use of “§” and “paragraph” will be retained in English language translations. Equally, the English language equivalent of “section” will be retained for any English legal text translated into German. This etiquette will serve to clarify the differing legal linguistic traditions that have emerged over time in different, country-specific legal contexts.

(6) Bilingualism: For practical reasons, in this publication, several texts which originated in the legal environment of Germany were not translated. Interested readers can avail themselves of any of the available online translation services – at own risk.

Chapter 1: Oral Launch of Weltrecht^2

A. "Weltrecht^2" evolving

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"** held in South Africa, Johannesburg from December 5 to 9, 2022. One topic on the many workshop agendas concerned "Constitutional law scholarship and constitutional transformation: actors and influences"[4].

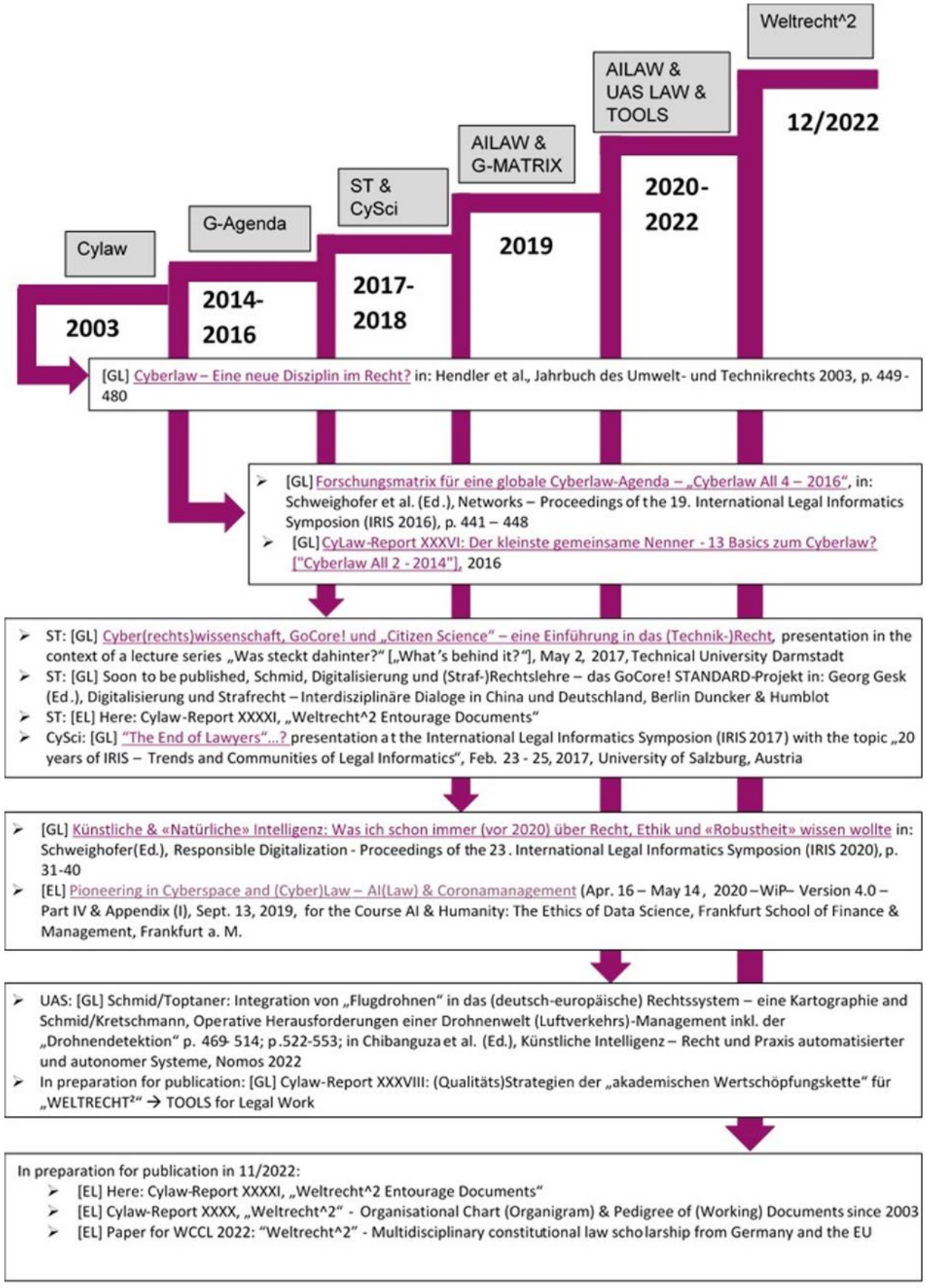
B. Timeline of the "Weltrecht^2" Project: Development Phases & STEP LADDER

This timeline has been first published in the Cylaw-Report XXXXI (XLI). The repeated publication here serves only to meet the requirement of the "self-explanatory" quality of the individual Cylaw-Reports.

SLIDE 1: Screenshot of Website "Chair for Public Law at Technical University, Darmstadt"

[4] Workshop 27, https://wccl.co.za/workshops/ (last accessed Oct. 20, 2022).

SLIDE 2: Step Ladder



C. Two Workshops – one Paper and one Presentation

Given the relevance of two workshop topics, Viola Schmid decided to submit two abstracts and was consequently accepted for both workshops. Subsequently, however, she focused on Workshop 27 which in her view provided the more fertile ground for the development of a new principle of constitutional law – robustness. This new principle of constitutional law was also the content of her second abstract. Consequently, information regarding the second workshop as well as the second abstract will be provided here, in order to

- clarify the context of the oral presentation and the discussions during workshop 27 and
- to present for discussion the consequences for the Constitutional Legal Design of an AI-Driven World as an effect of World Law^2.

I. About Workshop 27: "Constitutional law scholarship and constitutional transformation: actors and influences"

SLIDE 3: Conference-Website of Workshop 27

Cited from the conference-website:

"In this workshop, we inquire how and to what extent constitutional knowledge and actions of constitutional scholars could shape a different world on constitutionalism during crucial moments of constitutional changes, such as constitutional drafting, constitutional amending, transitional periods, and grand transformation. Beyond the Weberian premise that scholarly professionalism is separated from political participation, intellectual constitutional scholars can be political actors when practising their professions with public obligations. Constitutional scholars should be understood broadly in this workshop, including researchers working outside traditional scholarly circles in private structures.

We will also reflect on immigration and transplantation of constitutional knowledge in a historical and comparative perspective. In addition to mapping or restoring the fixed picture of Western constitutional enlightenment, we invite participants to find the national narrative of a country's own (unfinished) path into constitutionalism under the framework of multi-modernity, which would significantly contribute to building up and upholding constitutional faith in different societies throughout time at the level of constitutional theory.

Since this workshop would benefit different areas of studies, interdisciplinary methodologies are highly welcomed.

The sub-themes include:

- various processes and ways, legal and non-legal, through which researchers influence constitutional changes.
- public participation and professional influences of constitutional scholars in spreading ideas of constitutionalism during the transitional period.
- the role of constitutional lawyers in historical moments, such as the founding moment or constitutional drafting.
- how knowledge of modern constitutionalism is translated, taught, and accepted in the successor countries, especially in the transitional and post-communist regimes.
- public scholarly reviews on emerging controversies caused by the ongoing technology revolution.
- academic freedom at universities through the historical developments and its contemporary challenges.
- the democratic legitimacy of researchers' influence on constitutional changes.

WORKSHOP CHAIRS:

Dr Han Zhai
Research Fellow on Special Appointment, School of Law | Vice-dean, Research Institute of Cyberspace Governance, Wuhan University
China

Camille Bordere
PhD Candidate in Comparative Law, Bordeaux University
France

Dr Sacha Sydoryk
Lecturer, Università di Corsica Pasquale Paoli
France”

II. About Workshop 30: The principle of the rule of law in the age of digital constitutionalism

SLIDE 4: Conference-Website of Workshop 30

Cited from the conference-website:

“The rise and consolidation of digital technologies have raised multiple concerns for the principle of the rule of law and the protection of fundamental rights. The rule of law has a direct impact on the life of every citizen: it is a precondition for ensuring equal treatment before the law, protecting fundamental and legal rights, preventing abuse of power by public authorities and holding decision-making bodies accountable.

The primary challenges are particularly related to the troubling legal uncertainty deriving from the exercise of powers through the implementation of unaccountable technologies. It is not by chance that constitutional democracies have tried to address this issue as shown by the EU proposal for the Artificial Intelligence Act. Therefore, this workshop aims to address the challenges for the principle of the rule of law in the digital age, particularly focusing on the use of technology by public authorities, the delegation of public functions and enforcement as well as an alternative model for enforcing technological standards.

This panel which is hosted by the IACL Research Group “Algorithmic State, Market and Society” will address digital constitutionalism in a plural way by looking at the challenges for the rule of law in the digital age.

WORKSHOP CHAIRS:

Prof Erik Longo
Associate Professor of Constitutional Law, University of Florence
Italy

Prof Oreste Pollicino
Professor of Constitutional Law, Bocconi University
Italy

Prof Amnon Reichman
Full Professor of Law, University of Haifa and Berkley Law School
Israel”

D. A tricontinental launch – Republic of South Africa, European Union, People’s Republic of China (RSA, EU & PRC)

Despite “load shedding challenges”. the university of Johannesburg made possible the presentation’s life transmission to the People’s Republic of China and to Europe/Germany via internet. It can therefore be considered a hybrid presentation. As Georg Gesk[5] stipulated:

[5] Der deutsche Text ist eine Übersetzung aus dem Chinesischen und wird deswegen nach dem Prinzip der Dreisprachlichkeit im Folgenden wiedergegeben: „Die Übermittlung an die Volksrepublik China erfolgte als Beteiligung von Viola Schmid an einem Foreign-Expert-Program (Programmleiter auf europäischer Seite ist Prof. Dr. Georg Gesk (Professur für Chinesisches Recht, Universität Osnabrück), der seit 2021 gemeinsam mit chinesischen Kolleginnen und Kollegen an der Universität Anhui an dem Projekt „数字资源法律保护协同创新 “ (Der Ausgleich von rechtlichem Schutz und kreativen Neuentwicklungen im Bereich digitaler Ressourcen)), das in seinem Kernbereich als bikontinentaler akademischer Diskurs (China – D/EU) Fragen im Raum von Digitalisierung, Cyberspace und Recht erörtert; so etwa das Spannungsfeld zwischen Digitalisierung des Rechts und dem Recht der Digitalisierung oder die rechtliche Ausgestaltung des Cyberspace vs. die Auswirkungen der Entwicklung des Cyberspace auf das Recht. Unmittelbar beteiligt waren Prof. Dr. Zhu Qing und Dr. Wang Na auf Seiten der juristischen Fakultät der Universität Anhui in der VR China.“

„The transmission to the People’s Republic of China took place as part of Viola Schmid’s participation in a Foreign Expert Program[6] (program lead for the European side is Prof. Dr. Georg Gesk (Professor for Chinese Law, University of Osnabrück), who has been working on the project „数字资源法律保护协同创新” (Balancing legal protection and creative innovation in the area of digital resources) since 2021 together with Chinese colleagues at the University of Anhui). Having bicontinental (China – G/EU) academic discourse at its core, the program discusses issues in the realm of digitization, cyberspace and law; for example the tensions between the digitization of law versus the law of digitization, or the legal design of cyberspace versus the impact of the development of cyberspace on the law. On the Chinese side, Prof. Dr. Zhu Qing and Dr. Wang Na of the Faculty of Legal Sciences at Anhui University were directly involved.“

E. „Mission“ & „Challenge“

I. Technological Challenges and Interoperability of different systems in two continents

Several photos from Anhui illustrate how the linking from South Africa by means of various digital systems onto a screen at the University of Anhui in the city of Hefei passed the practical test even under Corona conditions – all under the aegis of Prof. Dr. Georg Gesk.

SLIDE 5: Technical (De-)coupling & Pairing

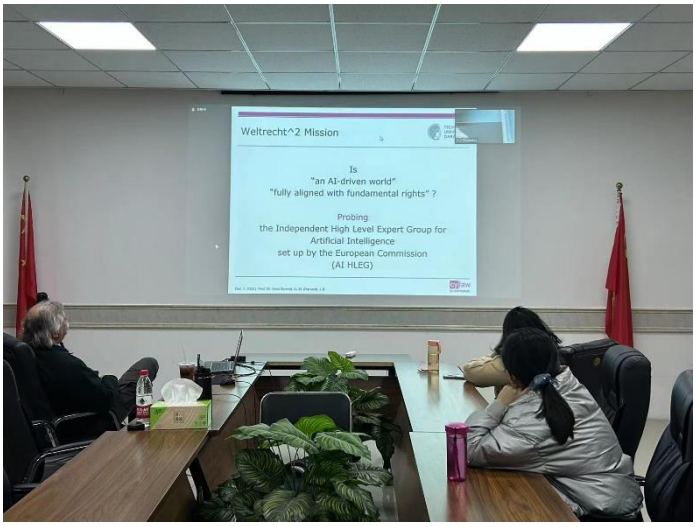
[6] See previously in 2021: „THE (EUROPEAN) ARTIFICIAL INTELLIGENCE (R)EVOLUTION: ARE TRUSTWORTHINESS, LAW, ETHICS, AND ROBUSTNESS ENOUGH FOR (RE)LIABILITY?“.

II. Proof of concept for shared content!

In addition, on the content level it becomes obvious that two core aspects of paper and presentation were understood in their significance on both continents. Especially these two photos, taken by the Chinese colleagues and in particular one colleague in China (Prof. Dr. Georg Gesk), serve to confirm this:

1. **“Probing” the High Level Expert Group (HLEG): Is “an AI-Driven world” fully aligned with fundamental rights?”**

SLIDE 6: PRC Audience I



2. **Rebuttal: Why the Classic Model of Constitutionalism Might not Suffice”**

SLIDE 7: PRC Audience II

Chapter 2: Manuscript

This speech manuscript supplements the conference contribution as well as the footnote document[7]. The speaking time available was 15 minutes.

A. Pre-conference submission of the presentation manuscript

The manuscript was sent with a requirement for confidentiality to the workshop chairs and the conference organizers (Prof. David Bilchitz) for the chair's preparation.

SLIDE 8: Header of Preliminary Information for Chairs
VIOLA SCHMID, FIRST (CONFIDENTIAL) PRESENTATION MANUSCRIPT OF WELTRECHT^2: MULTIDISCIPLINARY CONSTITUTIONAL LAW SCHOLARSHIP FROM GERMANY AND THE EU Dec. 07th 2022 05:27 a.m.

The version published here has slight editorial amendments.

SLIDE 9: Opening **T**ransparency **o**f **P**resentation (**ToP**)
Chair for Public Law Prof. Dr. Viola Schmid, LL.M. (Harvard) TECHNISCHE UNIVERSITÄT DARMSTADT **"WELTRECHT^2":** MULTIDISCIPLINARY CONSTITUTIONAL LAW SCHOLARSHIP FROM GERMANY AND THE EU World Congress of Constitutional Law: TRANSFORMATION S Workshop 27: CONSTITUTIONAL LAW SCHOLARSHIP Johannesburg, South Africa, Dec. 5 - 9, 2022 Dec. 7, 2022 | schmid@cylaw.tu -darmstadt.de | 1 cylaw tu-darmstadt

[7] Weltrecht^2 – Paper - Versatile Footnote Document (ot)": "Multidisciplinary Constitutional Law Scholarship from Germany and the EU", Feb. 07th 2023.

SLIDE 10: **T**ransparency **o**f **P**resentation (**ToP**) - 2

You all read my „paper" ☺

TECHNISCHE UNIVERSITÄT DARMSTADT

In 2022:

- "Weltrecht^2": Multidisciplinary Constitutional Law Scholarship from Germany and the EU, WCCL Workshop 27, Constitutional Law Scholarship And Constitutional Transformation, Johannesburg, South Africa, 2022

Entourage Documents:

- [EL] CyLaw-Report XXXXI: „Weltrecht^2 Entourage Documents (2022)" - A Standard for a Universal (Technology) Law Lecture in Cyberspace and (Technology) Law (2018), 2022
  DOI: 10.26083/tuprints-00022879

- If not – ask me (later on)

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 2

cylaw tu-darmstadt

Ladies & Gentlemen,
I am Viola from Germany and today is a very special day in my life! This is my first stay in (South) Africa and there is a "herstory", which I would like to share with you. Those who know me, know that I am a woman of principles. Those of you who have read my paper now know the origin of my design for constitutional principles of "robustness" and "ephemerality. [see under Chapter 3]

SLIDE 11: **ToP - 3**

„HERstory" – not history

TECHNISCHE UNIVERSITÄT DARMSTADT

Thank you for having me ?

My first stay in South Africa with Weltrecht^2!

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 3

cylaw tu-darmstadt

Surprise not at all, I was raised by a “man of principles” – my venerated father Gottfried Schmid. In the 1980ies, he raved about the mindblowing nature of South Africa for a European citizen, and his family principle was: Sharing. So, he wanted to share this experience with his family and particularly with his daughter. Consequently, he invited the law student Viola to travel to South Africa. With Nelson Mandela still imprisoned back in those days, I refused his invitation. I argued that as long as Nelson Mandela were in prison, Viola would not spend holidays in South Africa. Today it is with strong emotions and deep gratitude to life and my father that I want to share Weltrecht^2 with you.

SLIDE 12: **ToP - 4**

„Weltrecht^2“=“Welt des Rechts”x“Rechtswelt”

TECHNISCHE UNIVERSITÄT DARMSTADT

- “Welt des Rechts“ [“world of law”]:
  consist of all legal systems of the193 members of the United Nations
- “Rechtswelt”:
  legally coded as well as by lawfulnessdriven world

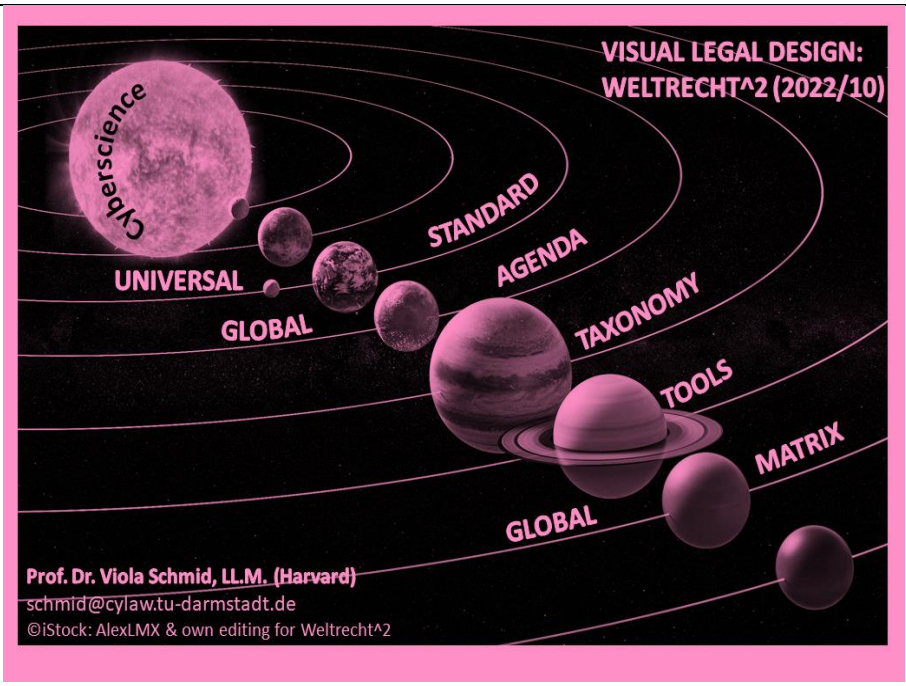
Welt des Rechts” x “Rechtswelt”= „Weltrecht^2“

German terminology–
please help me being understood instead of misunderstood

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 4

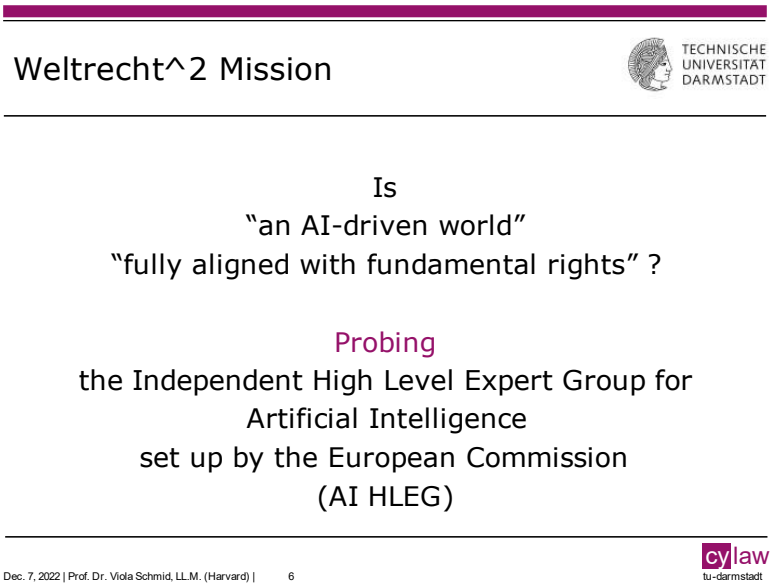
cylaw tu-darmstadt

SLIDE 13: **ToP - 5**



It’s a German terminology describing a CYBERSCIENCE Galaxy with five planets. And the terminology Weltrecht^2 is an equation of “Welt des Rechts” or “world of law” consisting of all legal systems of the 193 members of the United Nations. And “Rechtswelt” – a legally coded as well as by lawfulness-driven world. I know my roots and my roots are German. Therefore, certain German terminologies, for which I was not able to find an equivalent in English, will be maintained. Yet, I ask you to help me - a none-native English speaker - to be understood instead of misunderstood. And correct me whenever you think it necessary.

SLIDE 14: **ToP - 6**

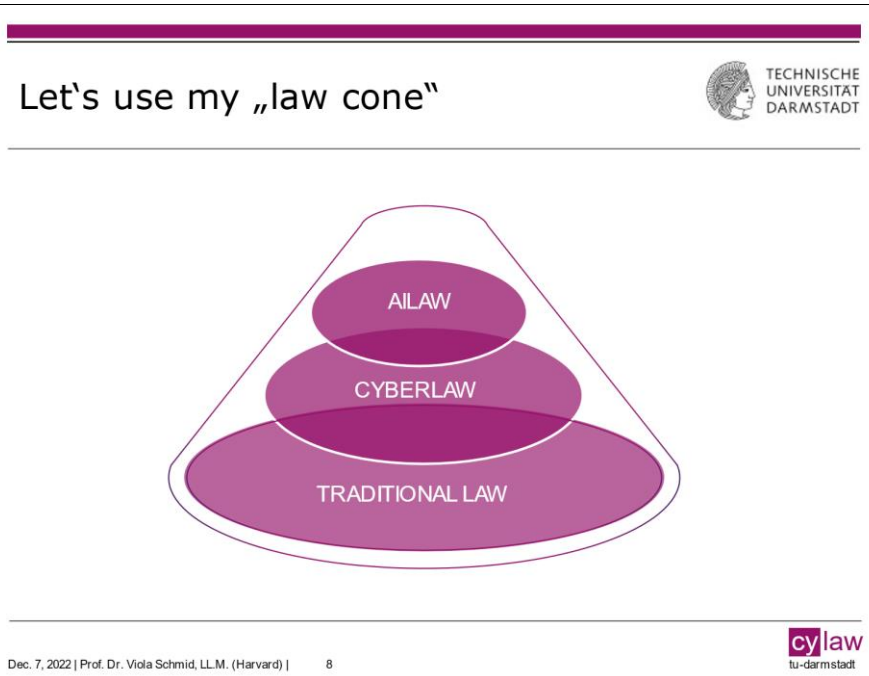


What is the mission of Weltrecht^2? It is the probing of a claim by the independent High-Level Expert Group for Artificial Intelligence, set up by the EU Commission in 2019. They claimed that an AI-driven world is fully aligned with fundamental rights.

SLIDE 15: **ToP - 7**

This slide shows the original text of their argumentation which I would like to quote in part: to “ …ensure an appropriate governance and regulatory framework. We advocate to safeguard AI that is lawful, ethical and robust and fully aligned with fundamental rights in an AI-driven world […], without stifling beneficial innovation.” Let’s probe this argument. To this end, I have developed a law cone depicting the three different categories of law. I call them TRADITIONAL LAW, CYBERLAW and AILAW.

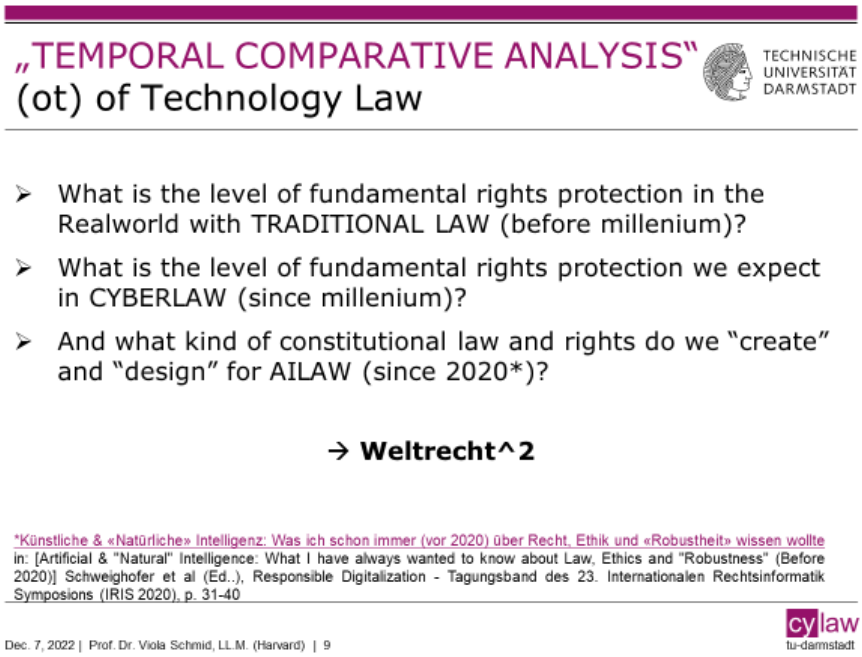
SLIDE 16: **ToP - 8**



Probing the AI-HLEG, I used for Weltrecht^2 a temporal comparative analysis of technology law (ot), focusing on three issues:

- What is the level of fundamental rights protection in the REALWORLD with TRADITIONAL LAW before the turn of the millennium?
- What is the level of fundamental rights protection we expect in CYBERLAW since the turn of the millennium?
- And what kind of constitutional law and rights do we create and design for AI-LAW starting from 2020?

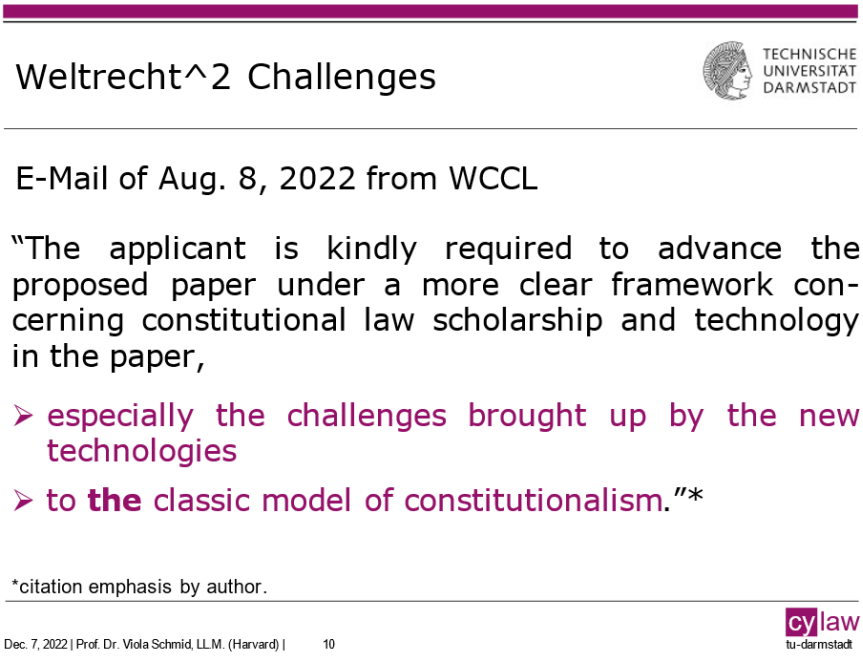
SLIDE 17: **ToP - 9**



The mission of Weltrecht^2 was challenged in an email by the esteemed colleagues chairing this workshop about constitutional law scholarship in Johannesburg. "The applicant is kindly required to advance the proposed paper under a clearer framework concerning constitutional law scholarship and technology, especially the challenges brought up by the new technologies for the classic model of constitutionalism."

And in my "paper" I promised some arguments:

SLIDE 18: **ToP - 10**



SLIDE 19: **ToP - 11**

See PART 4: Why “the Classic Model of Constitutionalism” … (p. 37)

TECHNISCHE UNIVERSITÄT DARMSTADT

FACHGEBIET ÖFFENTLICHES RECHT
PROF. DR. VIOLA SCHMID, LL.M. (HARVARD)

TECHNISCHE UNIVERSITÄT DARMSTADT

WCCL WORKSHOP 27:
CONSTITUTIONAL LAW SCHOLARSHIP AND CONSTITUTIONAL TRANSFORMATION

“WELTRECHT^2”:
MULTIDISCIPLINARY CONSTITUTIONAL LAW SCHOLARSHIP
FROM GERMANY AND THE EU IN 10.000 WORDS IN NOVEMBER 2022

ABSTRACT

There are two (r)evolutions that trigger “Weltrecht^2” [GLOBAL LAW^2]. On the one hand, the transformation of the REALWORLD into a technology-based HYBRIDWORLD (REAL-WORLD+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

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 11

cylaw tu-darmstadt

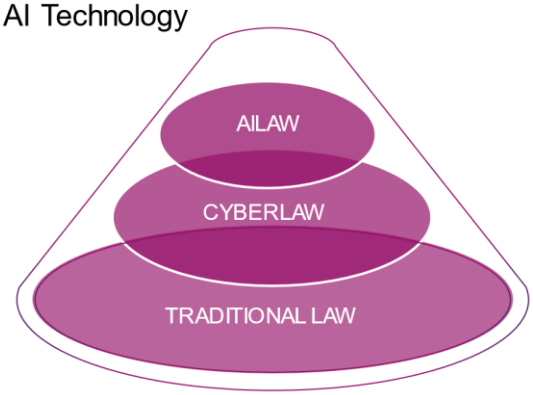
Firstly, there are evidently for me two technological challenges for the classic model of constitutionalism: CYBER- and AI- technology.

SLIDE 20: **ToP - 12**

➢Two Technological Challenges for „the Classic Model of Constitutionalism*“

TECHNISCHE UNIVERSITÄT DARMSTADT

Cyber- & AI Technology

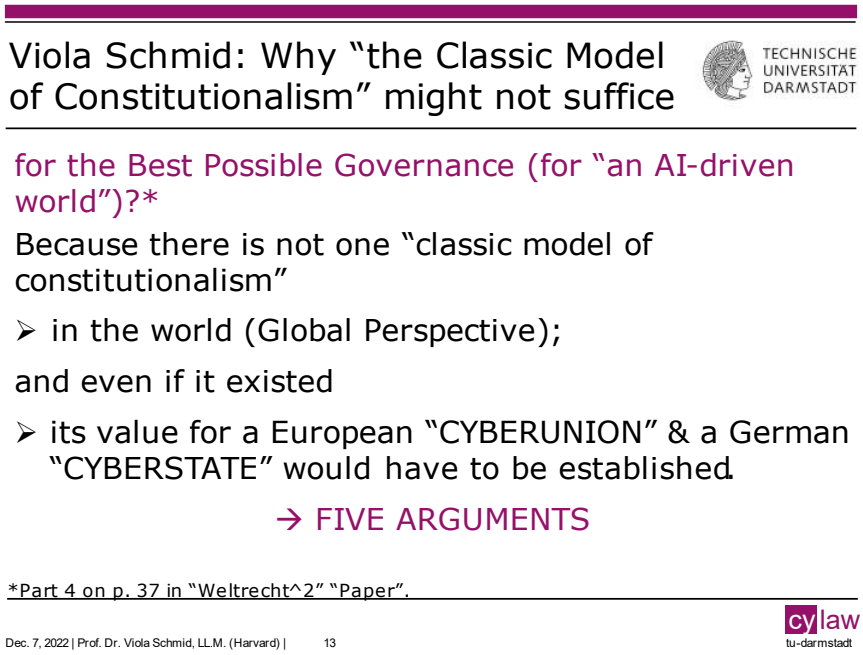


*E-Mail from Aug. 8, 2022.

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 12

cylaw tu-darmstadt

SLIDE 21: **ToP - 13**



And the second challenge concerns the question why the "classic model of constitutionalism" (their terminology) may not suffice as best possible governance for the European High-Level European Expert Group on an AI-driven world. My answer is: Exactly because there is

- neither **one** classic model of constitutionalism in the world,
- not even in TRADITIONAL LAW,
- or from a global perspective in CYBER- & AILAW.

And even if one existed, I believe its value for a European CYBERUNION or a German CYBERSTATE would have to be established - **instead of a priori assumed**. So, I would like to come back to you with five arguments why CYBER- and AILAW are "game changers". They feature:

- activist courts, new fundamental rights and obligations and, consequently, democratic deficits,
- From a EU-German perspective, we have had to deal with CYBERLAWLESSness for over a decade now. Consider the discrepancy of the legislative and judiciary powers in the context of TTDL which is short for Telecommunication Traffic Data Retention and Usage Law.
- The third argument I would like to highlight follows the European High-Level Expert Group on AI law's argument that law alone is NOT enough. The lawful, ethical and robust formula of the AI HLEG is exactly a counterargument against THE classical model of constitutional law scholarship.
- Fourth, I think that CYBERLAW and AILAW" are characterized by a technological abolition of the separation of state, economy, society and citizen.
- And my fifth point concerns two books I would like to recommend. I don't know the authors personally, I will not obtain any commission or revenue from promoting the books. I believe that those who insist on the classical model of constitutional law scholarship should perhaps take into account their content. I am holding them up into the camera so you can see them.

SLIDE 21: **ToP - 14**

Five Arguments

TECHNISCHE UNIVERSITÄT DARMSTADT

(1) Activist Courts, New Fundamental Rights and Obligations & "Democratic Deficits"?

(2) CYBERLAWlessness– Discrepancy of Legislative and Judiciary Power in the context of TTDL?

(3) Law Alone is NOT Enough!– The LER-Formula (lawful, ethical and robust) of the AI HLEG

(4) Technological Abolition of the Separation of State, Economy, Society & Citizen

(5) Personalized Law? Suum cuique?

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 14

cylaw tu-darmstadt

Given that I only have 15 minutes, I can only present a brief outline of the five arguments. Let me now attempt to back these arguments with some sources.
Weltrecht^2 is a German-European endeavour, hence you will not be surprised that I used German or European Union law as a resource. In 1983, the German Federal Constitutional Court [BVerfG] created a right for informational self-determination and modern data processing. In 2008, the same court created a fundamental right on the protection of the confidentiality and integrity of information technology systems. What is the consequence of these new fundamental rights by case law?

SLIDE 22: **ToP - 15**

(1) Activist Courts, New Fundamental Rights and Obligations & "Democratic Deficits"?

TECHNISCHE UNIVERSITÄT DARMSTADT

New Fundamental Rights: Federal Constitutional Court

(1) Right to „informational self-determination and modern data processing"(1983, Volkszählungsurteil - BVerfGE 65,1)*

(2) Fundamental right to protection of the confidentiality and integrity of information technology systems (2008, "Online-Durchsuchung", BVerfGE 120, 274)**

* Decisions of the Federal Constitutional Court, Federal Constitutional Court (Ed.), Vol. 6: General right of personality, Nomos 2022, p. 41-68.
** Ibid. p. 534-564 („Remote Searches – covert searches of private computers").

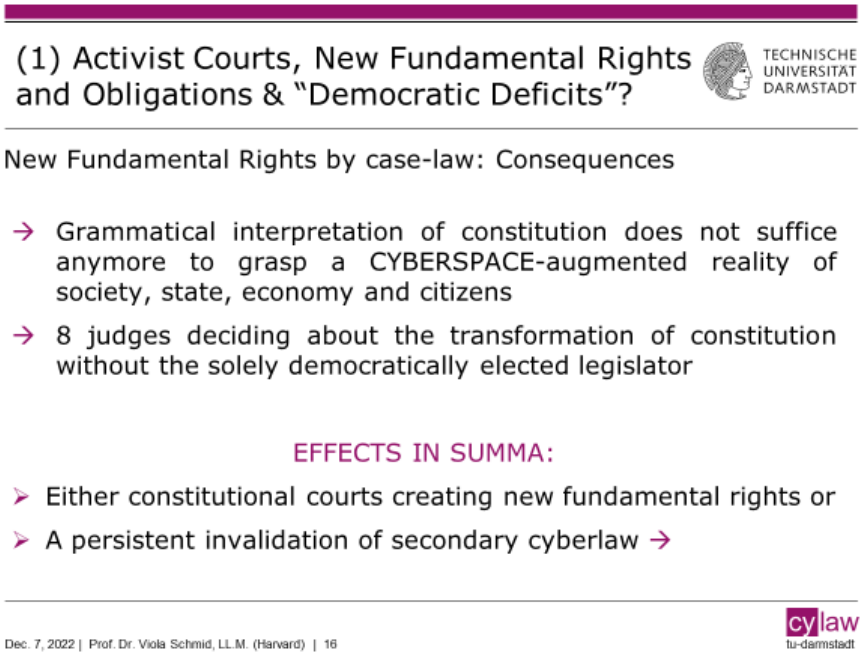
Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 15

cylaw tu-darmstadt

In a grammatical (syntactical) interpretation of the constitution, the CYBERSPACE augmented reality of society, state, economy and citizens cannot be grasped. And eight judges decide on the transformation of the constitution without consulting the sole democratically elected legislative.

The effects in sum create a dilemma: Either, constitutional courts create these fundamental rights, because the legislative does not do it, AND/ OR secondary CYBERLAW will be persistently invalidated. To this point, the Telecommunication Traffic Data Retention and Usage Law serves as my DEMONSTRATOR:

SLIDE 23: **ToP - 16**



I would have never expected that this “maximum credible accident” (ot) of lawlessness in a core area of CYBERLAW would persist for over a decade in Germany and Europe. I am backing this up with a number of decisions here on the slide: by the German Federal Constitutional Court in 2008, by the decision in 2014 of the Court of European Union Court of Justice, invalidating the TTDL directive, and the decision of the same court in 2022 on new German Telecommunication law.

SLIDE 24: **ToP - 17**

→ (2) CYBERLAWlessness – Discrepancy of Legislative and Judiciary Power in the context of TTDL?

TECHNISCHE UNIVERSITÄT DARMSTADT

A persistent invalidation of secondary cyberlaw: DEMONSTRATOR since 2010 until 2022

- German-European Telecommunication Traffic Data Retention & Usage Law (TTDL)
- "Maximum Credible Accident of Lawlessness" (ot)
- German Federal Constitutional Court (2008) invalidation of German telecommunication law
- Court of Justice of the European Union (2014) invalidation of TTDL directive (2006/24/EC)
- Court of Justice of the European Union (2022) on new German telecommunication law (of 2015) : German law is unlawful→ prevailing opinion

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 17

cylaw tu-darmstadt

SLIDE 25: **ToP - 18**

(3) Law Alone is NOT Enough! – The LER-Formula (lawful, ethical and robust) of the AI HLEG

TECHNISCHE UNIVERSITÄT DARMSTADT

EFFECTS IN SUMMA SO FAR:

- New fundamental rights by jurisprudence;
- A constantly by jurisprudence corrected legislator on TTDL
- And starting in 2019: According to the AI HLEG* – law alone is insufficient for "an AI-driven world"

* AI HLEG (Independent High Level Expert Group for Artificial Intelligence set up by the European Commission), Ethics Guidelines for Trustworthy Artificial Intelligence (AI), Apr. 8, 2019, (Acronym: "EGEGfTAI-I-2019"), https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html, (last accessed Nov. 28, 2022).

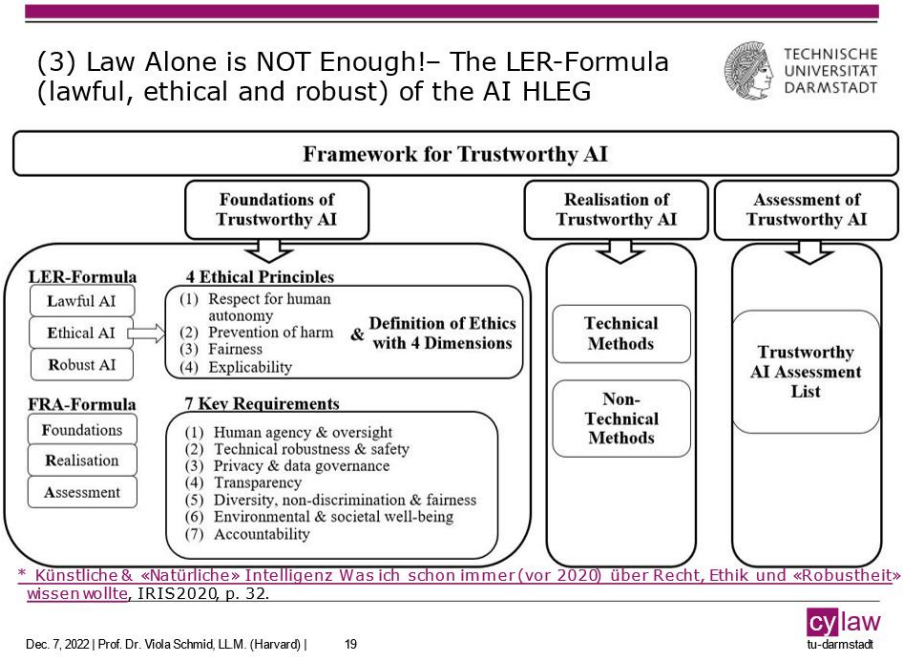
Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 18

cylaw tu-darmstadt

Let me reiterate the effects so far:

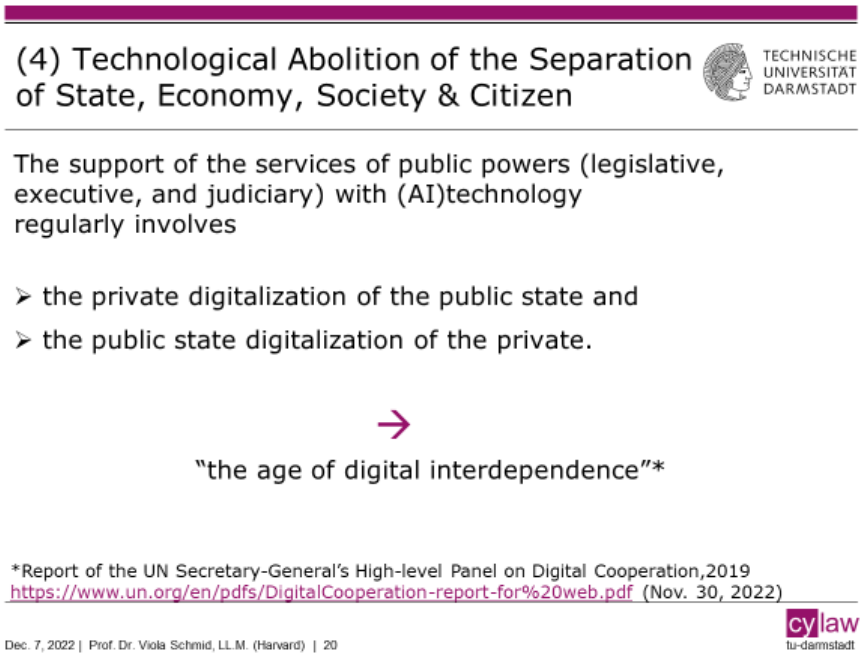
- New fundamental rights are created by jurisprudence for CYBERLAW and future AILAW
- In the case of TTDL, a German and European Union legislator is constantly corrected by jurisprudence
- And moreover, starting in 2019, according to the AI High-Level Expert Group, law alone is insufficient for an AI-driven world

SLIDE 26: **ToP - 19**

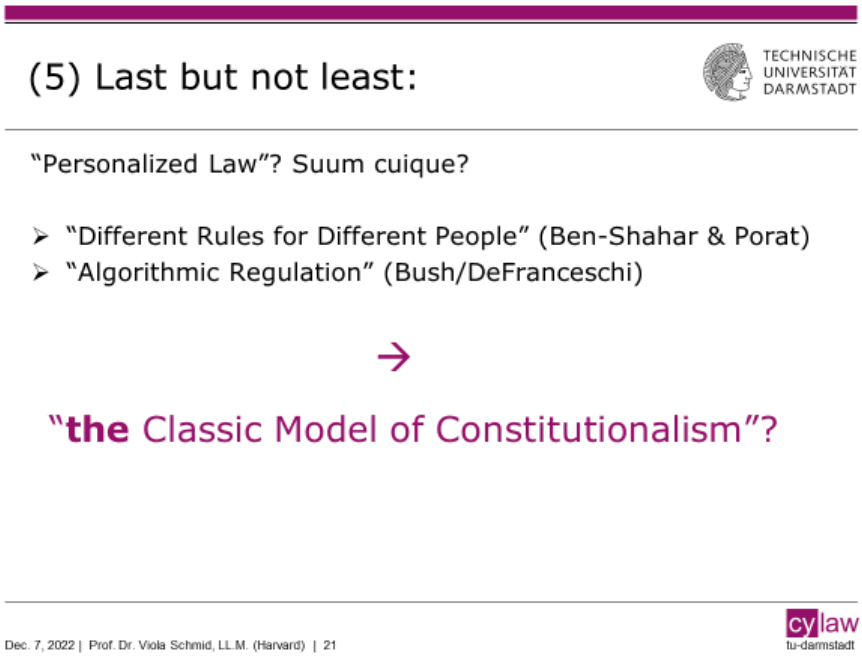


Regarding the latter point, I published in 2020 a framework to enable analysis, which you see here as shown above. I won’t expand on it due to time reasons and because I think you are knowledgeable enough. Please ask me about it later on. As to point four, I would argue that CYBER and AILAW are characterized by the private digitalization of the public state, and the public state digitalization of the private. A report for the United Nations called it the age of digital interdependence. Thus, autonomy and independence were characteristics of classical constitutional law of the past, but do not seem to serve as blueprint for the future.

SLIDE 27: **ToP - 20**

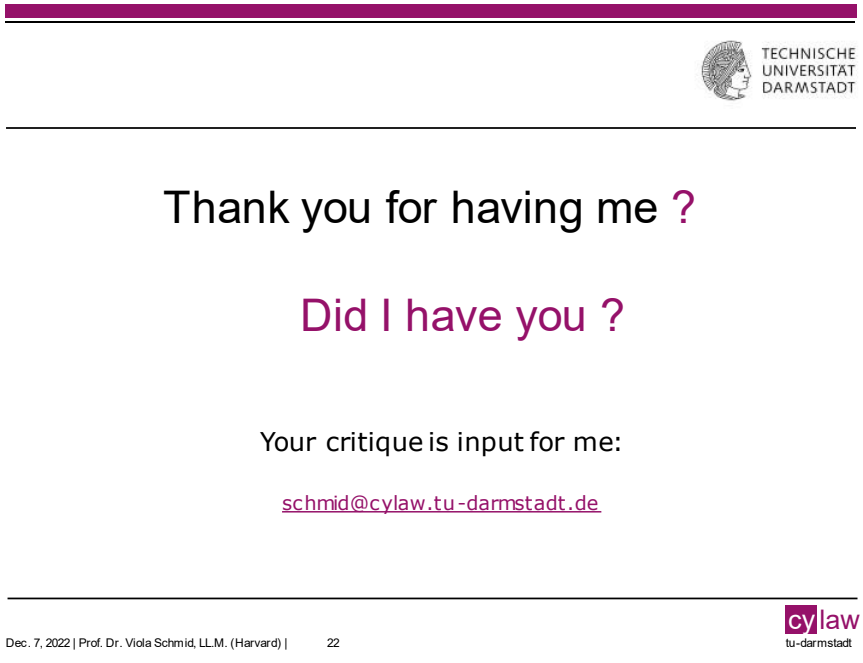


SLIDE 28: **ToP - 21**



And last but not at all least, the question of “personalized law” “Suum cuique tribuendi” - different rules for different people and algorithmic regulation – they defy the classic model of constitutionalism. Finally, the question I would put forward, is following: did you like having me, did I have you? And in any case, your critique is input for me. Thank you for having me.

SLIDE 29: **ToP - 22**



B. ANNEX SLIDES

In addition, the Annex slides prepared for the discussion are being shared below:

SLIDE 30: Weltrecht^2 – Taxonomy

"Weltrecht^2*-Taxonomy": "Taxing" "Global Agenda" (GA), "Lecture STANDARD" (ST) & TOOLS

Global Agenda for Cyberlaw– 13 Basics (GA)

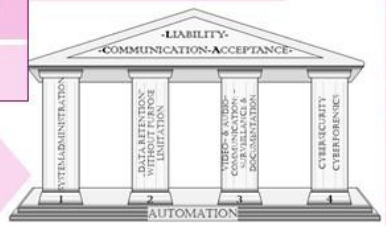
I. Cyberspace as a new Dimension of Being!
II. Cyberlaw makes Cyberspace a Cyberworld
III. Status Quo: Transition Period
IV. Malfunction Management (MaMa)
V. Global Networking and Competition – the GNC Formula
VI. Sustainability
VII. "Legal Information Technology Circular Thought Process"
VIII. Automation 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 9	"**GoCore! 1**"	Telecommunication Traffic Data Retention and Usage Law (TTDL) als "Double Module"
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.

SLIDE 31: Weltrecht^2 - GLOBALMATRIX

GLOBALMATRIX

TECHNISCHE UNIVERSITÄT DARMSTADT

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
Federal	State	Tertiary Law		Tertiary Law		Tertiary Law		Tertiary Law
Executive Power		Federal Level	Executive Power	Primary Level	Executive Power	Primary Level	Executive Power	Federal Level
		State Level		Secondary Level				State 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

cylaw tu-darmstadt

SLIDE 32: Weltrecht^2 – GLOBAL AGENDA

GLOBAL AGENDA

TECHNISCHE UNIVERSITÄT DARMSTADT

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

cylaw tu-darmstadt

cylaw tu-darmstadt

SLIDE 33: Weltrecht^2 - STANDARD

STANDARD

TECHNISCHE UNIVERSITÄT DARMSTADT

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

Module	Title	Content
1	"**Survival Guide**" & Table of Contents	LAW and not Philosophy, Political Science, Sociology, Economics etc.
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 9	"**GoCore! 1**"	Telecommunication Traffic Data Retention and Usage Law (TTDL) als "Double Module"
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)

SLIDE 34: Weltrecht^2 – Time Management & Progress as Step Back?

„HERstory" – The past is the present?

TECHNISCHE UNIVERSITÄT DARMSTADT

"an AI-driven world" that is "fully aligned with fundamental rights"

„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." *

*AI HLEG (Independent High Level Expert Group for Artificial Intelligence set up by the European Commission), Policy and Investment Recommendations for Trustworthy AI, June 26, 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 Nov. 23, 2022); citation with emphasis by the author.

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 28

cylaw tu-darmstadt

SLIDE 35: AILAW & "Trustworthy AI"

Regulatory Framework for "Trustworthy AI" – AI HLEG

TECHNISCHE UNIVERSITÄT DARMSTADT

"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."** *

*AI HLEG (Independent High Level Expert Group for Artificial Intelligence set up by the European Commission), Policy and Investment Recommendations for Trustworthy AI, June 26, 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 Nov. 23, 2022); citation with emphasis by the author.

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 29

cylaw tu-darmstadt

SLIDE 36: Weltrecht^2 - Terminology

Terminology

TECHNISCHE UNIVERSITÄT DARMSTADT

➢ **"TRADITIONAL LAW" (ot*):**

The end of TRADITIONAL LAW only is roughly dated for the turn of the millennium. "TRADITIONAL LAW" is understood here as traditional dogmatics and methodology of the legal science within the German constitutional state [Rechtsstaat] and the European legal union [Rechtsunion]. The distinguishing feature of TRADITIONAL LAW is the (experiential) knowledge accumulated in millennia.

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 30

cylaw tu-darmstadt

SLIDE 37: Weltrecht^2 - Terminology

Terminology

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Cyberlaw:**
  The law of distribution of chances and risks, rights and duties in CYBERSPACE as well as the HYBRIDWORLD, consisting of REALWORD and CYBYERSPACE

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 31

cylaw tu-darmstadt

SLIDE 38: Weltrecht^2 - Terminology

Terminology

TECHNISCHE UNIVERSITÄT DARMSTADT

Cyberscience Definition (ot)

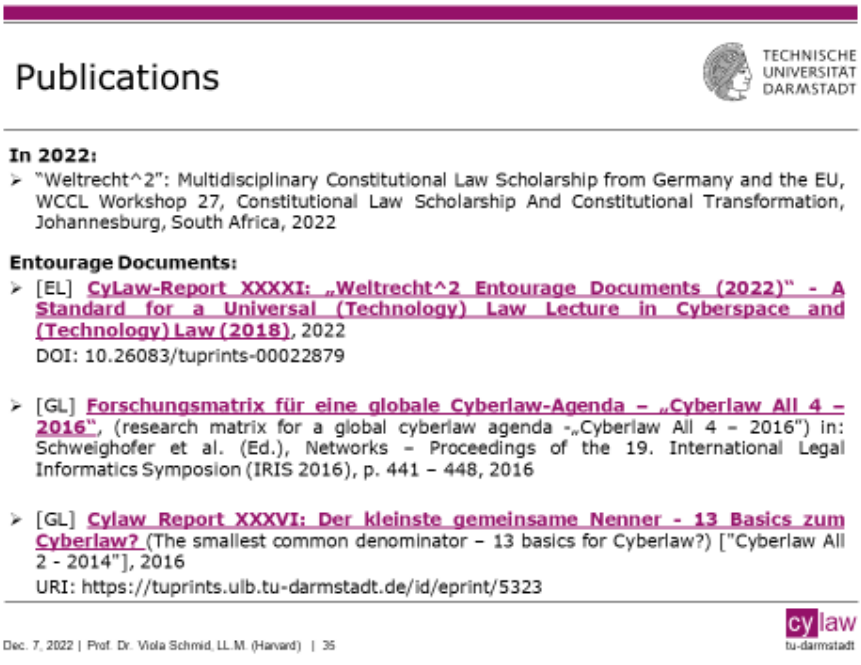
“a new multidisciplinary science originating in law scholarship, utilizing “the world of law” for a “legally coded as well as by lawfulness-driven world” (ot)

Dec. 7, 2022 | Prof. Dr. Viola Schmid, LL.M. (Harvard) | 33

cylaw tu-darmstadt

SLIDE 39: „EU in Global Dialogue“[8]

SLIDE 40: Weltrecht^2 – Backbone & Entourage Documents



[8] About CEDI (Centre of Excellence “EU in Global Dialogue”): CEDI Team - eu-global-dialogues Webseite!; About CEDI - eu-global-dialogues Webseite!

Chapter 3: Abstracts

For complementation as well as convenience purpose both abstracts are reproduced here again to provide context information (limited to roughly 500 words) (s. also Cylaw-Report XXXXII(XLII)). Slight editorial amendments have been made (Version 2.0 – concept of "living document").

A. Workshop 27: "Weltrecht^2" Multidisciplinary constitutional law scholarship from Germany and the EU (Version 2.0)

SLIDE 41: Abstract for Workshop 27
"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. Hence the here so called "Rechtswelt" will be „legally coded and by lawfullness driven" [law is code and not "code is law"].[9] 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 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 communication traffic data retention and usage laws. However, it addresses this experience with unlawfulness from 2005 to 2022 as documented by rulings of German and European courts, within a universal teaching standard for technology-related law.

[9] Lessig, Lawrence: Code and other laws of cyberspace, 1999 S.6, 7; Code 2.0, 2006, S. 5.

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 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[10] for technology could be made;
- assessment lists[11] 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 "Weltrecht^2", constitutional law is to become a component of a multidisciplinary cyberscience (based on cyberlaw). Get ready for the already impending fifth industrial revolution[12]!

References will be provided in the conference paper."

B. Workshop 30: "Artificial Intelligence Constitutionalism" and the "Principle of Robustness"

SLIDE 42: Abstract for Workshop 30

"The German rule of law establishes core elements such as the principles of clarity and certainty of norms, the primacy of the legislature in essential decisions, its democratic legitimacy, the prohibition of retroactivity and the separation of powers. Above all, an independent judiciary exists, to which the path may not be cut off (guarantee of legal recourse). The European rule of law (Art. 67 Treaty on the Functioning of the European Union (TFEU)) establishes a single space - "an area of freedom, security and justice". However, the REALWORLD (author's terminology), which is not entirely technology-based and which created and lived by these rules of law, has been supplemented for about 20 years by a technology-based cyberspace. Constitutionalism must therefore clarify whether Art. 67 TFEU is sufficient for a hybrid world consisting of an autonomy-capable REALWORLD and a technology-based cyberspace. Is "an area" interpretable in such a way that it applies to both?

Moreover, the "(cyber) area" entails different phases of digitalization, automation and autonomization (from digital documents to autonomously flying drones). Therefore, an undifferentiated "digital constitutionalism" perspective is technologically and legally insufficient: There is a need for an "AI Constitutionalism" if the European Union wants to pursue and legislate AI policies (see "Artificial Intelligence Act" of 21st April 2021). Furthermore, Art. 67 TFEU requires "respect for fundamental rights and the different legal systems and traditions of the Member States". If it applies, it requires an "AI-Law analysis" of these different legal systems and traditions. This is precisely the notion of an "AI constitutionalism" that asks: Does cyberspace also need a special rule of technology for freedom and security? A rule of technology that complements the rule of law. And if, which core elements (see above on the rule of law) configure this rule of technology? I suggest the adherence to the principle of robustness.

[10] 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).

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

[12] 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 01,.2022).

For an "AI-driven world", the European Commission has set up a 52-member High-Level Expert Group to develop this "principle of robustness" (in their Assessment List [Annotation 1]). This "principle of robustness" comprises core elements such as security, safety, accuracy, reliability, fall-back plans and reproducibility. One could object that the expert group has not dealt with constitutionalism at all. Instead, it has produced a "framework" for an "AI-driven world" that establishes a triad of lawfulness, ethic conformity and robustness (LER formula). For the first time it equates the "principle of robustness" as a "rule of/for technology" with traditional legal and ethical conformity – the pillars of traditional constitutionalism. Thus, in a transdisciplinary interpretation "robustness" is inevitably linked to "Artificial Intelligence Constitutionalism" from the perspective of a German-European constitutional law scholar. Whether this "principle of robustness" will be the result of an evolutionary legislation or could be the result of a revolutionary jurisprudence, especially in Germany, will be examined in the conference contribution. It is about Legal Design for the Cyberworld.

Annotation 1: AI HLEG, The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment, 17th July 2020,https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342 (09.06.2022)."

Chapter 4: Reservoir for Global Knowledge: German – European AI-Jurisprudence of 2022 and 2023 (3 Judgments)

As a contribution to global research on the „world of law" three court decisions shall be communicated in this publication of May 2023 for an international audience. All three judgments are pioneering decisions informing the emerging AILAW.

A. Terminology: information technology relevant security law [„informationstechnologisches Sicherheitsrecht"]

In terms of topic these judgments concern a matter that Viola Schmid already in 2013 called the **„information technology relevant security law" [„informationstechnologisches Sicherheitsrecht"** [13] **]** [14]. This is not „information technology security law" [Sicherheitsrecht für Informationstechnologie] in the sense of the" Second act on increasing the security of IT systems (German IT Security Act 2.0)".[15] It is not (only) about "New IT security […] for state-of-the-art cybersecurity".[16] Moreover it is about using digitization with "state-of-the-art cybersecurity" to achieve and strive for better (REALWORLD-)SECURITY [sichere Informationstechnologie für Sicherheitsrecht]. This goal – preventing harm – with new safe and secure technologies (such as Digitalization, Automation and Autonomization"[17]) is at the core of **„information technology relevant security law".** The potentially (predictive) wisdom of these AI-Technologies is the center of the debate of the following three court decisions.

[13] Schmid, final report of the BMBF project: „Sicherheit im öffentlichen Raum – SIRA" vom 13.09.2013; 778149676.pdf (tib.eu).

[14] See also "informationstechnische Straßeninfrakstruktur" [informationtechnology relevant road infrastructure] in § 63e section 1 Road Traffic Act.

[15] Federal Office for Information Security: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig_2-0.html (2023/05/17).

[16] Federal Office for Information Security: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig_2-0.html (2023/05/17).

[17] Schmid in 2023/01 Cylaw-Report XLII: Weltrecht^2 Backbone Documents" → here "PAPER": "MULTIDISCIPLINARY ONSTITUTIONAL LAW SCHOLARSHIP FROM GERMANY AND THE EU" SUBMITTED TO WORLD CONGRESS OF CONSTITUTIONAL LAW IN DEC. 2022, p. 14.

B. Federal Constitutional Court in the information technology relevant security law

For decades now, the Federal Constitutional Court has consistently claimed its role as CYBERLAW determinant in the German legal system.[18] With this decision rendered in 2023 it becomes also an agent of the legal design of AILAW.

I. Review & Retrospective: Telecommunication Traffic Data Retention and Usage Law (TTDL) Jurisprudence of the German Federal Constitutional Court (2010) – the path towards IT-Security Law

1. Judgment of the First Senate of 2 March 2010

The headnotes of this judgment of 2010 can be shared here: Judgment of the First Senate of 2 March 2010

Headnotes

to the Judgment of the First Senate of 2 March 2010

1BvR 256, 263, 586/08

1. The precautionary retention of telecommunications traffic data by private service providers without specific grounds, for a period of six months, as provided for under Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 (OJ L 105 of 13 April 2006, p. 54; hereinafter: Directive 2006/24/EC), is not per se incompatible with Art. 10 of the Basic Law; there is thus no need to decide on the possible precedence of the directive over domestic law.

2. The principle of proportionality requires that the statutory framework governing such data retention be designed so as to adequately reflect the particular weight of the resulting fundamental rights interference. This requires sufficiently stringent and clear statutory provisions regarding data security, data use, transparency and legal protection.

3. Under Art. 73(1) no. 7 of the Basic Law, it is incumbent upon the federal legislator to enact provisions ensuring data security and to subject possible data use to a clear purpose limitation, as these elements are inseparable from the statutory provisions imposing obligations to retain data. By contrast, the legislative competence for enacting provisions governing requests for access to the retained data by the authorities, and for specifying the applicable transparency and legal protection regime, lies with the legislator that is competent to legislate on the respective underlying subject matter.

4. With regard to data security, the legislator must lay down particularly high standards in clear and binding provisions. These provisions must ensure that, in principle, the required level of data security is informed by the current state of expertise and incorporates, on an ongoing basis, new

[18] Schmid, Viola: Schlussbericht des„BMBF-Projekt: „Sicherheit im öffentlichen Raum – SIRA, Teilprojekt 5 des Verbundvorhabens: SIRA-Recht (SIRAR) vom 13.09.2013, S.4. „In grundlegenden Fragen dieses „informationstechnologischen Sicherheitsrechts“ scheiterte der Bundes- oder Landesgesetzgeber (beim ersten Versuch), Informationstechnologien in den Dienst der Versicherheitlichung zu stellen: Akustische Wohnraumüberwachung (BVerfG, Urteil v. 03.03.2004; 1 BvR 2378/98, 1 BvR 1084/99), Rasterfahndung (BVerfG Beschluss vom 04.04.2006, 1 BvR 518/02), polizeirechtliche Telekommunikationsüberwachung (BVerfG, Urteil vom 27.07.2005; 1 BvR 668/04), Onlinedurchsuchung (BVerfG Urteil vom 27.02.2008, 1 BvR 370/07, 1 BvR 595/07), Kennzeichenscanning (BVerfG, Urteil vom 11.03.2008; 1 BvR 2074/05, 1 BvR 1254/07) und Vorratsdatenspeicherung (BVerfG, Urteil vom 02.03.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.“

research and advances in this field. It must also be ensured that data security may not be freely weighed against general business considerations.

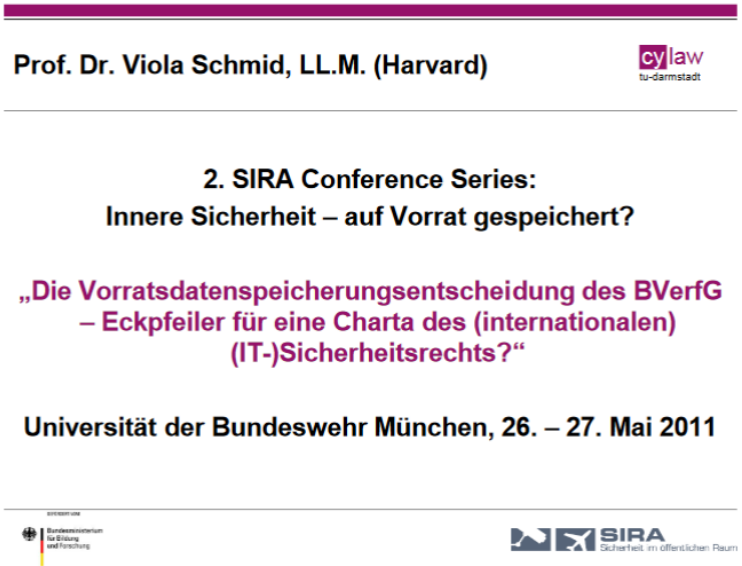
5. Requests for access to and the direct use of retained data are only proportionate if they serve to protect exceptionally significant legal interests. In the domain of law enforcement, this requires that specific facts give rise to the suspicion of serious criminal acts. In the domain of public security and the tasks of the intelligence services, requests for data access and use of the data may only be authorised if there are factual indications of a specific danger to life, limb or liberty of the person or to the existence or security of the Federation or a Land , or of a danger to the general public.

6. The mere indirect use of the data by telecommunications service providers to provide information to the authorities on the subscribers of Internet Protocol addresses is permissible for the purposes of law enforcement, public security and the tasks of the intelligence services, even where this is not subject to a narrowly-defined statutory catalogue of criminal offences or protected legal interests. For prosecuting administrative offences [as a law enforcement purpose], such information may only be provided to the authorities in cases of particular weight on grounds expressly set out in the law.

2. Scientific World Potential

Already as early as 2011 did Viola Schmid consider this court decision by the German Federal Constitutional Court to have scientific world potential[19]:

SLIDE 43: TTDL Jurisprudence in a Presentation for SIRA[20] [Security in public spaces]



[19] Schmid, Viola: Die Vorratsdatenspeicherungsentscheidung des Bundesverfassungsgerichts – Eckpfeiler für eine Charta des (internationalen) (IT-)Sicherheitsrechts? Presentation within the framework of the 2. SIRA Conference Series, 26.-27.05.2011 in Munich, as part of a BMBF sponsored project „Sicherheit im öffentlichen Raum – SIRA“ (Security in the public realm)

[20] SIRA (SIRA: Sicherheit im öffentlichen Raum - BMBF-Sicherheitsforschung (sifo.de).

3. CJEU: Invalidating European Secondary Law in 2014 and "invalidating" German secondary Law in 2022

A publication concerning the legal history (starting in 2005) of the German-European Telecommunication Traffic Data Retention and Usage Law is in preparation – providing further references. Here two judgments have to be shared:

- The voiding of the directive "TTDL DIRECTIVE 2006/24/EC" in 2014 by the CJEU.[21] After the European directive was declared null and void by the Court of Justice of the European Union infringement proceedings (Art. 258 TFEU) were discontinued in 2014.
- The judgment addressing new German telecommunication law (of 2015) of Sept. 2022[22]

4. FCC: Proceedings with TTDL Constitutional Complaints (Status after February 2023)

In the meantime - after 2010 - the Federal Constitutional Court is again dealing with this new German data retention and usage law of 2015 and 2021. Following the 2022-decision of the CJEU, the FCC denied in February 2023 admissibility to three constitutional complaints (addressing the German TTDL of 2015).[23] According to media sources three constitutional complaints are still pending.[24] In summa: TTDL is a DEMONSTRATOR for a Maximum Credible Accident (MCA) of lawmakers from Germany and Europe concerning a core area of Cyberlaw (first branch of government). TTDL is also a DEMONSTRATOR for the dominant role of the third branch of government in the Legal Design for a technology based law. Do you recall Slide 24: **ToP** – 17?

II. 2023: "Processing of stored personal data by means of automated data analysis or evaluation applications" in "information technology relevant security law"

For the latter, Viola Schmid predicts a more recent decision of the Federal Constitutional Court to have a similar quality to the TTDL decision of 2010. It concerns a 59-page long court decision in German language (BVerfG Urteil vom 16.02.2023 1 BvR 1547/19, 1 BvR 2634/20) about the processing of stored personal data by means of automated data analysis and evaluation applications. It is about legal history of AILAW in the Federal Republic of Germany. It is about Hessian state law – and from a global perspective, the state of Hesse is probably a historical pioneer in the world of data protection law. And: It is about a worldwide operating player, because the system HessenData a.o. is evidently[25]

---

[21] Judgment of the Court of Justice of the European Union (CJEU) from April 8,2014, C-293/12, C-594/12, ECLI:EU:C:2014:238.

[22] Judgment of the Court of Justice of the European Union (CJEU) from Sept. 20, 2022 C-793/19 and C-794/19

[23] Order of the Federal Constitutional Court [BverfG] from Feb. 14 and 15. 2023 - 1 BvR 141/16, 1 BvR 2683/16, 1 BvR 2845/16; See also press release from 30.03.2023: [Bundesverfassungsgericht - Presse - Verfassungsbeschwerden gegen die anlasslose Vorratsdatenspeicherung erfolglos.]

[24] Article from LTO.de: "Alles gesagt in Sachen Vorratsdatenspeicherung?" from March 30, 2023: „Nach Auskunft des Gerichtssprechers sind noch drei weitere Verfassungsbeschwerden gegen die Vorratsdatenspeicherung im zuständigen Dezernat anhängig. Zum Verfahrensstand äußerte er sich nicht." (June 16,2023)

[25] s. Wissenschaftlicher Dienst Deutscher Bundestag (WD 3 - 3000 - 018/20):„Datenbank-Analysen durch die Polizei": „Das Bundesland Hessen hat 2017 eine Software von der US-Firma Palantir erworben, die nach Anpassungen unter dem Namen „Hessendata" bekannt wurde.", S: 4; siehe auch BVerfG: Rn. 7 „Bereits 2017 hatte Hessen das Programm „Gotham" vom Software-Unternehmen Palantir erworben und unter dem Namen „hessenDATA" eingesetzt" und Rn. 15 „Die Freie und Hansestadt Hamburg hat bislang nach eigenem Bekunden keine Versuche unternommen, eine hessenDATA vergleichbare Plattform zu errichten (Hamburgische Bürgerschaft Drucks 22/1758, S. 1 f.). Auch nach Abschluss eines Rahmenvertrags zwischen dem Freistaat Bayern und dem Unternehmen Palantir, der es anderen Ländern erlaubt, das ausgewählte Produkt, eine verfahrensübergreifende Recherche- und Analyseplattform (VeRA), ohne Vergabeverfahren selbstständig abzurufen, hat Hamburg über deren Einführung bislang keine Entscheidung getroffen (Hamburgische Bürgerschaft Drucks 22/7701, S.

provided by Palantir[26]. Thus, the potential for a world-spanning research approach of the judgment is justified.

1. Press release of the Federal Constitutional Court in English

Press Release No. 18/2023 of 16 February 2023 to Judgment of the Federal Constitutional Court from Feb.16, 2023, 1 BvR 1547/19, 1 BvR 2634/20

SLIDE 44: “Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional”
[…] Press Release No. 18/2023 of 16 February 2023 Judgment of 16 February 2023 Automated data analysis In a judgment pronounced today, the First Senate of the Federal Constitutional Court held that § 25a(1) first alternative of the Security and Public Order Act for the Land Hesse (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung – HSOG) and § 49(1) first alternative of the Act on Data Processing by the Police for the Land Hamburg (Hamburgisches Gesetz über die Datenverarbeitung der Polizei – HmbPolDVG) are unconstitutional. These provisions authorise the police to process stored personal data through automated data analysis (Hesse) or automated data interpretation (Hamburg). The provisions violate the general right of personality (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law, Grundgesetz – GG) in its manifestation as the right to informational self-determination, because they do not contain sufficient thresholds for interference. They allow the further processing of stored data by means of automated data analysis or interpretation in certain cases, subject to a case-by-case assessment, when necessary as a precautionary measure to prevent specific criminal acts. Given the particularly broad wording of the powers, in terms of both the data and the methods concerned, the grounds for interference fall far short of the constitutionally required threshold of an identifiable danger (konkretisierte Gefahr). § 25a(1) first alternative of the Hesse Security and Public Order Act will continue to apply, subject to the restrictions set out below, until new provisions have been enacted, and in any case no later than

1 f.“ See also the Hesse parlamentary debate regarding the application of Palantir products: Hessischer Landtag - Plenarprotokoll vom 20.06.2018, 19/142, S.10271.

[26] In order to better decribe the agent „Palantir“ the following research was conducted: (1) Wikipedia on rhe search term Palantir Technologies: „Palantir Technologies, Inc. ist ein US-amerikanischer Anbieter von Software und Dienstleistungen, der auf die Analyse großer Datenmengen (Big Data) spezialisiert ist. […]“ (last accessed May 12 2023); (2) Media articles on the link between the State of Hesse with Palantir and regarding the founding history of Palantir: (2a) Spiegel vom 06.04.2018, „Hessens Polizei kauft Software von umstrittener US-Firma“: „Palantir wurde 2004 von dem Facebook-Investor und PayPal-Erfinder Peter Thiel mithilfe von In-Q-Tel gegründet, dem Risikoinvestment-Arm des US-Geheimdienstes CIA.“ (last accessed May 12, 2023); see also (2b) Zeit Online of September 30, 2020: „Die geheimnisvollen Datensortierer“: „125 Kunden arbeiten mit Palantir zusammen, darunter sollen Berichten zufolge schon die NSA, FBI und die CIA gewesen sein, aber auch Privatunternehmen wie zum Beispiel der deutsche Dax-Konzern Merck.“ (last accessed May 12,2023); (3) According to Palantir’s own publication ((https://blog.palantir.com/palantir-and-gaia-x-85ab9845144d)) the company appears to be a member of Gaia-X: (3a) Why Palantir joined Europe's GAIA-X | Palantir Blog und (3b) PalantirTech on Jan. 4th, 2021 via Twitter: “What can a company founded in Silicon Valley bring to Europe's sovereign data ecosystem, #GAIAX? Click to learn how #Palantir hopes to contribute as a Day 1 member https://twitter.com/PalantirTech/status/1346063913390108673. (last accessed May 12, 2023).

30 September 2023. § 49(1) first alternative of the Hamburg Act on Data Processing by the Police is void.

Facts of the case:

§ 25a(1) of the Hesse Act and § 49(1) first alternative of the Hamburg Act, which have essentially the same wording, provide a specific statutory basis for linking previously unconnected automated databases and data sources in analysis platforms and permitting systematic access of data across sources through searches. The provisions authorise the police to process stored personal data through automated data analysis (Hesse) or automated data interpretation (Hamburg), subject to a case-by-case assessment, in order to prevent serious criminal acts within the meaning of § 100a(2) of the Code of Criminal Procedure (Strafprozessordnung – StPO) (first alternative) or to avert dangers to certain legal interests (second alternative). Section (2) of both provisions provides that relationships or connections between persons, groups of persons, institutions, organisations, objects or matters can thereby be established, insignificant information and intelligence can be filtered out, insights generated can be matched to known facts and stored data can be analysed.

In Hesse, the police have employed the powers granted by § 25a of the Security and Public Order Act thousands of times each year via the platform ‘hessenDATA’. In Hamburg, § 49 of the Act on Data Processing by the Police has not yet been put to use.

Key considerations of the Senate:

A. The constitutional complaints are only admissible to the extent that they are directed against the threshold for interference laid down in § 25a(1)first alternative of the Hesse Act and in § 49(1) first alternative of the Hamburg Act (data analysis or interpretation for the prevention of criminal acts). For the rest, they are inadmissible.

B. To the extent that the constitutional complaints are admissible, they are well-founded.

I. When stored data is processed by means of automated data analysis or interpretation, this constitutes an interference with the informational self-determination of all persons whose personal data is used in such processing. It is not just the further use of previously unconnected data that amounts to an interference with fundamental rights – the new intelligence that can be obtained through automated data analysis or interpretation can also affect fundamental rights.

II. Automated data analysis or interpretation requires justification under constitutional law. In principle, it can be justified. Compatibility with the principle of proportionality is of particular importance, the specific requirements of which depend on the reach of the powers in question. The challenged provisions serve the legitimate purpose of increasing the effectiveness of the prevention of serious criminal acts, in view of the development of information technology, in that they enable the discovery of indications of imminent serious criminal acts that might otherwise remain undetected in the police data. In the present proceedings, the Land governments demonstrated that, due to the increasing use of digital media and means of communication, particularly in the areas of terrorist and extremist violence and organised and serious crime, the police authorities are faced with ever larger data streams that are increasingly heterogeneous in terms of their quality and format. According to the Land governments, automated data analysis is essential for successful police action, since information on these crimes is difficult to obtain through a conventional search of police data records, let alone under time constraints. The provisions are suitable under constitutional law for increasing the effectiveness of the prevention of crime. They are also necessary, given that automated data analysis

or interpretation can generate relevant intelligence for the prevention of crime that could not be generated equally effectively by other, less intrusive means.

III. Special requirements for the justification of the interference with fundamental rights here arise from the principle of proportionality in the strict sense. How stringent these requirements are in each case depends on the severity of interference resulting from the measure in question.

1. The severity of interference resulting from automated data analysis or interpretation is first of all determined by the severity of the interferences that resulted from the previous data collection; in this respect, the principles of purpose limitation and change in purpose that have been previously fleshed out in the judgment on the Federal Criminal Police Office Act apply.

Accordingly, the legislator may permit the use of data beyond the specific investigation that initially prompted the data collection measure if the contemplated use is still in line with the purpose for which the data was originally collected (further use in line with original purpose). Further use of data that serves the purpose for which the data was originally collected is only permissible to the extent that the data is used by the same authority in relation to the same task and for the protection of the same legal interests as was the case with regard to the collection of the data. In principle, the data may then be used as leads for further investigation.

Moreover, the legislator may allow the further use of data for purposes other than those for which the data was originally collected (further use with change in purpose). In this case, the principle of a hypothetical recollection of the data is the applicable standard for the proportionality review. According to this principle, the legislator may in principle allow for a change in purpose if the data of the police authorities concerns information that results, in an individual case, in a specific basis for further investigations aimed at detecting comparably serious criminal acts or averting impending dangers that, at least in the medium term, threaten weighty legal interests that are comparable to the legal interests whose protection justified the collection of the data in question.

In both cases, stricter requirements apply to the further use of data obtained through the surveillance of private homes or remote searches of IT systems.

Pursuant to § 25a of the Hesse Act and § 49 of the Hamburg Act, personal data can be subjected to further processing that is in line with the original purpose as well as processing with a change in purpose. Both provisions allow for the processing of large amounts of data, essentially without differentiation as to the source of the data or the original purpose of its collection. Adherence to the constitutional requirements arising from the principle of purpose limitation would therefore require sufficiently clear provisions to ensure compliance with the principle of purpose limitation, both in legal terms and in practical application.

2. Moreover, automated data analysis and interpretation amounts to a separate interference, because the further processing of data that has been collected and stored can result in new detrimental effects, which might be more onerous than the severity of interference of the original data collection; in this respect, the principle of proportionality in the strict sense requires additional justification.

a) Automated data analysis or interpretation is directed at generating new intelligence. The authorities involved here can generate far-reaching intelligence from available data through the use of practically all of the existing IT methods and also deduce new connections by way of data analysis. It is not unusual in and of itself that the police will make further use of the intelligence they have obtained as leads or grounds for further lines of inquiry, either by themselves or in conjunction with other available

information, as jumping-off points for additional investigation. Yet automated data analysis and interpretation goes even further because it allows for the processing of large amounts of complex information. Depending on the method of analysis used, integrating existing data can generate new information affecting the personality of those concerned that would not be accessible otherwise. The measures in question thus result in a more intensive generation of information from the data. This process does not just yield intelligence on the persons concerned that is present in the data, but as yet undiscovered due to lack of connections, it can also come close to developing a full profile. This is because the software can open up new possibilities of filling in the available information on a person by factoring in data and algorithmic assumptions about relationships and connections surrounding the person concerned. The principle of purpose limitation by itself could then be inadequate in relation to the severity of interference.

b) The constitutional requirements for the justification of automated data analysis or interpretation vary, given that its severity of interference may differ substantially depending on the design of the statutory framework.

aa) In general, the severity of interference with the right to informational self-determination primarily depends on the type, scope and possible uses of the data, as well as the risks of abuse. Moreover, the permitted method of data analysis or interpretation has an impact on the severity of interference. The use of complex forms of data cross-checking can be particularly intrusive. In general, the intrusion by methods of automated data analysis or interpretation becomes greater the broader and deeper the intelligence that can thereby be obtained , the higher the margin of error and likelihood of discrimination, and the more difficult it is to retrace the links generated by the software.

bb) The legislator can thus determine the severity of interference by providing for rules regarding the type and scope of the data to be used and by limiting the permissible methods of analysis. The constitutional requirements regarding the prerequisites for interference correspond to the respective severity of interference of the measure in question. The requirements arising from the principle of proportionality in the strict sense for a particular measure depend on both the legal interest to be protected and by the threshold for interference, that is, the grounds for carrying out the measure.

If automated methods give rise to serious interferences with the right to informational self-determination of affected persons, such interferences can only be justified subject to the strict requirements that apply to intrusive and covert surveillance measures generally. The use of such methods is only permissible to protect particularly weighty legal interests – such as life, limb or liberty of the person. The threshold for interference that is required here is that of a sufficiently identifiable danger (hinreichend konkretisierte Gefahr).

By contrast, less severe interferences may be justified if they serve to protect legal interests of at least considerable weight, such as the prevention of criminal acts that are at least considerable – provided that an identifiable danger exists. In turn, if a measure serves to protect high-ranking, exceptionally significant or particularly weighty legal interests, a threshold that is less stringent than an identifiable danger may be sufficient.

If the type and scope of the data to be included are limited by the law and the possible methods of analysis or interpretation are restricted to such a degree that a measure carried out on the basis of the power in question will not lead to more extensive insights into the life of affected persons than what could realistically be obtained by the authority, albeit more slowly and laboriously, without automation, or if the power is from the outset only aimed at identifying dangerous or sensitive locations,

without generating personal information, then adherence to the principle of purpose limitation alone may be sufficient for justifying automated data processing.

cc) The threshold of an at least identifiable danger to particularly weighty legal interests can only be constitutionally dispensed with if the statutory framework, in a clear and sufficiently specific manner, limits the permissible options of analysis and interpretation so narrowly that the severity of interference resulting from the measures is substantially lower. In principle, the legislator can divide the task of setting out such rules, laying down some elements itself while allowing other rules to be determined by administrative authorities. However, the legislator must ensure that the rules limiting the type and scope of data that may be used and restricting permissible methods of data processing are sufficient in all situations and adhere to the requirement that interferences must be based on statutory provisions. An authorising statute can be considered for the determination of aspects that do not have to be set out by the legislator. Moreover, the legislator can require administrative authorities to further specify the abstract and general determinations set out in the law or in ordinances. That said, specification by way of administrative rules in any case requires a statutory basis. In this statutory basis, the legislator must ensure that the authorities comprehensibly document and publish the specifying and standardising determinations that will ultimately govern the application of the provisions in the individual case.

c) Based on the general standards set out above, the specific severity of interference of the – broadly worded – powers to carry out data analysis or interpretation pursuant to § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act is potentially great; constitutional law therefore requires that these provisions satisfy strict prerequisites for interference. The powers in question allow the automated processing of unlimited amounts of data by means of methods that are not circumscribed by law. They thus allow the police, with just one click, to create comprehensive profiles of persons, groups and circles. They may also subject many persons who are legally innocent to further police measures, if their data was collected in some context and the automated evaluation of this data leads the police to wrongly identify them as suspects. Therefore, the threshold of an identifiable danger to particularly weighty legal interests applies.

aa) Both provisions have virtually no restrictions on the type and amount of the data that can be used for data analysis or interpretation. They do not set out what types of data and what data records may be used for automated analysis or interpretation. In particular, the provisions do not differentiate between persons for which there are reasonable grounds to assume that they could commit a criminal act or those that have a particular connection to such persons, and others as to which no such grounds exist. They allow the far-reaching inclusion of the data of third parties, who as a result may be subject to police investigations.

bb) Based on their wording, the provisions moreover permit the use of very far-reaching methods of automated data analysis and interpretation. The legislator did not limit the permissible methods of analysis and interpretation. The challenged provisions also provide the basis for data mining, including the use of self-learning systems (AI), and permit open searches. Data analysis or interpretation can be conducted with the aim of detecting mere statistical anomalies, from which further conclusions can then be drawn, potentially with the help of other automated applications. The provisions do not impose any limits on the search results that can be obtained. Based on their wording, the search results could consist of machine evaluations – including prognoses of the potential for danger from certain persons by means of ‘predictive policing’.Thus, the data analysis or interpretation can generate new information affecting the personality of the persons concerned that would otherwise not be accessible to the police. These potentially broad new insights are not accompanied by rules regarding their use that could lower the severity of interference.

In Hamburg, the legislator tried to exclude such far-reaching applications by using the term ‘data interpretation’ instead of ‘data analysis’. However, this failed to clarify, in a constitutionally sufficient manner, that the automated application would be limited to showing matches on the basis of specific search criteria as opposed to replacing analysis and evaluation of the data carried out by the police.

cc) The challenged powers are also not sufficiently circumscribed by the fact that the technology for unlimited data analysis is not currently available. Even if expanded features can only be used following future technological developments, the constitutional requirements must in principle be based on the interferences that are legally possible.

IV. Based on these standards, § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act do not satisfy the requirements arising from the principle of proportionality in the strict sense, given that they do not contain sufficient thresholds for interference.

1. Insofar as the challenged provisions authorise data analysis or interpretation in order to prevent the criminal offences listed in § 100a(2) of the Code of Criminal Procedure, the grounds for interference are disproportionately expansive in light of the severity of interference and the provisions are thus unconstitutional. The additional prerequisite of a case-by-case assessment contained in both provisions does not contain any more detailed specifications. In the oral hearing, a somewhat narrower concept of how the case-by-case assessment is understood and applied by the police in Hesse was described: data analysis is always linked to a criminal act that has already been committed or, at a minimum, to a suspicion that a criminal act has been committed. A prognosis for the future is then made on this basis. In order to carry out automated data analysis under this concept, the following two assumptions must be possible: first, that one of the criminal offences listed in § 100a(2) of the Code of Criminal Procedure was committed in the past and, second, that on this basis, similar criminal offences are to be expected in the future.

Despite the detailed design of this police practice in Hesse, the constitutional requirements are not met because this concept, from the outset, fails to target at least an identifiable danger and the data suitable for averting such a danger. This is necessary given the broad wording of the powers contained in § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act.

Moreover, the challenged provisions do not set out a sufficient threshold given that the catalogue of offences in § 100a(2) of the Code of Criminal Procedure also contains mere threats in the form of preparatory criminal acts. Under constitutional law, the legislator is not precluded from tying the prerequisites for interference to a danger that preparatory acts will be committed. However, the legislator must then ensure that, in each individual situation, the requisite specific danger or identifiable danger to the legal interests protected by the referenced offences actually exists. Such safeguards are lacking in this case.

2. According to the statutory definitions, the prevention of criminal acts within the meaning of § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act does not just encompass the deterrence of crime, but also preliminary measures for the prosecution of future crimes. Under these provisions, police data is to be used by means of automated data analysis in order to gain insights for future intelligence work and police investigations. From this, it cannot be inferred that a specific danger or an identifiable danger would be required for such automated analysis to be permissible. Thus, in this regard too, the grounds for interference are not restricted in any way.

C. § 25a(1) first alternative of the Hesse Security and Public Order Act continues to apply until new provisions have been enacted, but in any event no longer than 30 September 2023. Given the significance that the legislator may accord to the powers in question for the exercise of state functions and for police work in Hesse, a temporary application of the provision is preferable to a declaration of voidness.

However, in ordering the continued applicability of the provision, it is necessary to impose certain restrictions to protect the affected fundamental rights. These, however, do not predetermine the new provisions to be enacted by the legislator. Based on the concept used by the police in Hesse, police officers in Hesse may only make use of the power contained in § 25a(1) first alternative of the Hesse Act subject to the following conditions: sufficiently specific facts must give rise to the suspicion that a particularly serious criminal offence within the meaning of § 100b(2) of the Code of Criminal Procedure has been committed and it is expected, given the particular circumstances of the suspicion in the individual case, that similar criminal offences will be committed that will jeopardise the life and limb of the person or the existence or security of the Federation or a Land. Furthermore, the existence of these requirements and the specific suitability of the data used to prevent the expected criminal offence must be confirmed in a written explanation in each individual case; it must also be ensured that no information is used that was obtained through the surveillance of private homes, remote searches, telecommunications surveillance, traffic data retrieval, longer-term observations, the use of undercover investigators or confidential informants or through similarly serious interferences with the right to informational self-determination.

§ 49(1) first alternative of the Hamburg Act on Data Processing by the Police is void. There are no ascertainable circumstances that would make a temporary order of continued application necessary and could justify such an order.”

2. Hessian Secondary Law as Basis for Authorization

The Hessian secondary law was challenged. An amendment of the legislative process stipulates: „In light of the expanded technical possibilities to use information technology also in police work, §25a HSOG (Hessisches Gesetz für Sicherheit und Ordnung - Security and Public Order Act for the Land Hesse) creates a special legal basis to allow the linking of previously unconnected, automated data files and sources in analysis platforms and to thus systematically open up existing data stocks by means of search functions in order to facilitate and improve the performance of police tasks.“[27] „In the process, data stocks that the Hessian police authorities have already lawfully obtained and stored on the basis of other legal provisions shall thus be connected and processed further.[28]

SLIDE 45: § 25a Security and Public Order Act for the Land Hesse
§ 25a HSOG[29]
Automatisierte Anwendung zur Datenanalyse

[27] BVerfG decision of February 16, 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 2 with reference to HessLTDrucks 19/6502, S. 41.

[28] Applications for amendment submitted by the parliamentary groups of CDU and BÜNDNIS 90/DIE GRÜNEN […] regarding a law on the reorientation of the protection of the constitution in Hessen Drucksache 19/5412Hesse Parliament: HessLT-Drucks 19/6502, S. 41.

[29] Bürgerservice Hessenrecht, Gliederungs-Nr. 310-63, HSOG, last accessed May 12,2023.

(1) Die Polizeibehörden können in begründeten Einzelfällen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten zur vorbeugenden Bekämpfung von in § 100a Abs. 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind.

(2) Im Rahmen der Weiterverarbeitung nach Abs. 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

[…]

3. Prevention of Criminal Offences and Dangers as a Police Function

In the court proceedings before the Federal Constitutional Court, the state argued that the evaluation of data held by the police would offer so far unprecedented opportunities for prevention.[30]

4. Appraisal by the Court

The Federal Constitutional Court affirmed that „an encroachment on fundamental rights through automated data analysis or evaluation by the police authorities [is] in principle constitutionally justifiable. The constitutional requirements for the justification of an automated data analysis or evaluation depend on the concrete scope of the authority and are accordingly variable; here [with respect to § 25a HSOG as amended on June 25, 2018] they are strict in view of the design of the challenged provisions.".[31]

a) Terminology „Artificial Intelligence “

This terminology occurs in three places in the judgments. It should be emphasized that the court shows clear restraint with regard to both the terminology “artificial intelligence” and „self-learning systems “(3 mentions).

b) The Added Value of Predictive Policing?

Because the court in principle recognizes a potential added value of an (AI-supported) information technology relevant security law, it refrained from a directly effective prohibition - a nullification of §25a HSOG.

Citation from the judgment:

[30] HessLTDrucks 19/6502, S. 41: „Die Polizei kann dadurch über die bisherigen Erkenntnismöglichkeiten hinaus Zusammenhänge sowie Handlungsmuster und so auch künftiges strafbares oder gefährliches Verhalten
von Personen erkennen und geeignete präventive Maßnahmen treffen.“

[31] BVerfG decision of February 16, 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 49.

“(e) Depending on the type of operation, the use of adaptive systems, i.e. artificial intelligence (AI), **can have a special interference impact**. Their **added value,** but also their specific dangers, lie in the fact that not only criminological based patterns detected by individual police officers are applied, but such patterns are automatically developed further or generated in the first place and then further linked in advanced analysis stages. By means of an automated application and using **complex algorithms** for the identification of relationships or connections, further independent statements in the sense of "predictive policing" could be made.”[32]

Rather, the court has set a deadline until September 30, 2023 for the legislation by which time an amendment to state law will have to be made.[33]

C. Court of Justice of the European Union: Passenger Name Records (PNR) Jurisprudence & Relation to the Federal Constitutional Court Decision

In the context of flight passenger data – so essential for global mobility - the Court of Justice of the European Union decided that further processing of stored personal data by means of automated applications (for data analysis or evaluation) was **generally prohibited** (Judgment of the Court, C-817/19, from June, 21st 2022, ECLI:EU:C:2022:491). The CJEU appears thus to hold a more deprecating stance towards „self-learning systems such as AI“ than the FCC.

I. Abridged Press release

The Press Release No 105/22. Luxembourg, 21 June 2022. Judgment of the Court in Case C-817/19 in excerpts selected by the author:

SLIDE 46: Flight Data – here: PNR

Judgment of the Court in Case C-817/19 | Ligue des droits humains

The Court considers that respect for fundamental rights requires that the powers provided for by the PNR Directive be limited to what is strictly necessary:

In the absence of a genuine and present or foreseeable terrorist threat to a Member State, EU law precludes national legislation providing for the transfer and processing of the PNR data of intra-EU flights and transport operations carried out by other means within the European Union.

The PNR Directive* requires the systematic processing of a significant amount of PNR (Passenger Name Record) data relating to air passengers on extra-EU flights entering and leaving the European Union, for the purposes of combating terrorist offences and serious crime. In addition, Article 2 of that directive provides Member States with the possibility to apply the directive to intra-EU flights also.

[…]

In October 2019, the Belgian Constitutional Court referred ten questions to the Court of Justice for a preliminary ruling on, among other things, the validity of the PNR Directive and the compatibility of the Law of 25 December 2016 with EU law.

[32] BVerfG decision of February 16, 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

[33] BVerfG decision of February 16, 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 175.

In its judgment delivered today, the Court held, first, that since the interpretation given by the Court to the provisions of the PNR Directive in the light of the fundamental rights guaranteed by Articles 7, 8 and 21 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’) ensures that that directive is consistent with those articles, the examination of the questions referred has revealed nothing capable of affecting the

[…]

The Court states that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, inter alia, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services. It notes that the question whether the Member States may justify that interference must be assessed by measuring its seriousness and by verifying that the importance of the objective of general interest pursued is proportionate to that seriousness.

[…]

- For the purposes of the advance assessment of PNR data, the objective of which is to identify persons who require further examination before their arrival or departure and which is initially carried out by means of automated processing, the passenger information unit (PIU) may compare those data only against the databases on persons or objects sought or under alert. Those databases must be non-discriminatory and must be used by the competent authorities in the context of their mission to combat terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. As regards, moreover, the advance assessment in the light of the pre-determined criteria, the PIU may not use artificial intelligence technology in self-learning systems (‘machine learning’), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria. Those criteria must be defined in such a way that their application targets, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime and to take into consideration both ‘incriminating’ as well as ‘exonerating’ evidence, and, in so doing, must not give rise to direct or indirect discrimination.
- Given the margin of error inherent in such automated processing of PNR data and the fairly substantial number of ‘false positives’ obtained as a result of their application in 2018 and 2019, the appropriateness of the system established by the PNR Directive to achieve the objectives pursued depends essentially on the proper functioning of the verification of the positive results obtained under those processing operations carried out by the PIU, as a second step, by non-automated means. In that regard, Member States must lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the PIU agents in charge of that individual review for the purposes of ensuring full respect for the fundamental rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination. In particular, they must ensure that the PIU establishes objective review criteria enabling its agents to verify, on the one hand, whether and to what extent a positive match (‘hit’) concerns effectively an individual who may be involved in the terrorist offences or serious crime, as well as, on the other hand, the non-discriminatory nature of the automated processing operations. In that context, the Court also stresses that the competent authorities must ensure that the person concerned can understand the operation of the pre-determined assessment criteria and programs applying those criteria, so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to judicial redress. Similarly, in the context of such an action, the court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to

State security, the persons concerned themselves must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken, including the pre-determined assessment criteria and the operation of the programs applying those criteria.

[…]

Unofficial document for media use, not binding on the Court of Justice.

The full text and résumé of the judgment are published on the CURIA website on the day of delivery.

[…]

*Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132).”

II. Comparable Quality of Information Technology in the FCC and the CJEU case?

At least as far as the quality of the information technology is concerned, the information technology systems could be identical. It always concerns “processing of stored personal data by means of automated applications (for data analysis and evaluation).“

III. Different data quality and quantity

The quality of the (automatedly) evaluated data differs:

- In the German case, the data is already held by and available to the police.
- In the case of the European Union, it concerns mobility data of the global population. Contact with security authorities is not necessarily given in the European Union case.

D. Federal Administrative Court: “Mobile phone reading executive“ to establish identity and determine Right of Unlimited Residence

The court decision of February 16, 2023, currently only available in German and accessible since Mai 3, 2023 with reasons for the decision, implicates a global challenge. How can a state establish which foreign citizen can claim a right of residence for it? How can it ensure the knowledge as well as truthfulness of the identity information provided by the applicant?

I. German Secondary Law – §15a Abs. 1 S. 1 u. 2 AsylG i.V.m. §48 Abs. 3a S. 2 ff. AufenthG))

SLIDE 47: Basis for Authorization - § 15a AsylG

Asylum Act (Asylgesetz)

§ 15a Auswertung von Datenträgern

(1) Die Auswertung von Datenträgern ist nur zulässig, soweit dies für die Feststellung der Identität und Staatsangehörigkeit des Ausländers nach § 15 Absatz 2 Nummer 6 erforderlich ist und der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann. § 48 Absatz 3a Satz 2 bis 7 und § 48a des Aufenthaltsgesetzes gelten entsprechend.

(2) Für die in Absatz 1 genannten Maßnahmen ist das Bundesamt zuständig.

SLIDE 48: Basis for Authorization - § 48 Abs. 3a AufenthG

Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory[34]
(Aufenthaltsgesetz)

Section 48

Collection of access data

[…]

(3a) Analysis of data carriers is permissible only as far as necessary to establish the foreigner’s identity and nationality and to establish and enforce the possibility of removing him or her to another state in accordance with subsection (3) and the purpose of the measure cannot be achieved by more lenient means. Where there is reason to believe that analysing data carriers would provide only insights into the core area of private life, the measure is not permissible. The foreigner must provide the access data required for the permissible analysis of data carriers. The data carriers may be analysed only by employees who are qualified to hold judicial office. Insights into the core area of private life which are acquired in the course of analysing data carriers may not be utilised. Records thereof are to be deleted immediately. A written record is to be made of the fact of their acquisition and deletion.

[…]

II. Administrative Court Berlin

An Afghan applicant was forced to surrender her information technology systems to the authorities.

1. Comparable Quality of Information Technology with the FCC and CJEU case?

Subsequently, a „processing of stored personal data by means of automated applications for data analysis and evaluation“ took place.

2. Quality and Quantity of Data

Different to the two previously mentioned decisions, the use of automated technology concerned the personal data organized in the devices of the applicant.

a) Data under the Power of Disposition of the Applicant’s Information Technology System

Citation from the Judgment: “The federal agency connected the plaintiff’s unlocked mobile phone in her presence to a special computer („M Kiosk“) which read the plaintiff’s data, then processed it automatedly into a findings report which in turn was stored in a data safe. The findings report contains information regarding countries to which the plaintiff most frequently made phone calls and sent messages (SMS/MMS/Chat), or from which countries she most frequently received calls and messages, which language was used to communicate and in which countries the established contacts were located. After the readout from 9:38 hrs until 10:14 hrs the federal agency returned the mobile phone to the plaintiff.”[35]

[34] The following translation originates from the cyber presence of the Federal Office of Justice (existing translation).

[35] Decision by the Administrative Court of June 1, 2021 – VG 9 K 135/20 A, BeckRS 2021, 14390,Rn. 3.

b) „Absolutely Protected Core of Private Life" (Absolut geschützter Kernbereich privater Lebensgestaltung) (Art. 1 Basic law)

It should be noted in advance that in Germany the legislative and the judicial terminologies differ. The Act on the Residence (Aufenthaltsgesetz) refers to the „core of private life" (Kernbereich privater Lebensgestaltung), while the Federal Constitutional Court has formulated in its path breaking decision about acoustic surveillance: „Absolutely protected core of private life"[36] (absolut geschützter Kernbereich privater Lebensgestaltung)[37]

The Federal Administrative Court assumed that the data stored on a mobile phone potentially belongs to this intimate sphere of the applicant. Different to the other two court decisions regarding police and mobility data, this must be regularly assumed in this case.

3. Illegality of the Data Organization – "What are the Consequences?"

The Administrative Court Berlin denied the strict necessity for this severe interference into the applicant's personal privacy. Accordingly, the data organisation was found to be unlawful. Assuming a multidisciplinary perspective, the finding of unlawfulness has to be routinely followed up by an analysis of the consequences. Or, put bluntly: „Unlawfulness – so what?"[38]

4. Inadmissibility of Evidence [Beweisverwertungsverbot]

As a consequence of the unlawful data organisation, the Administrative Court Berlin also assumes in its reasoning the inadmissibility of evidence (Beweisverwertungsverbot) regarding the findings report of the data organisation.

Citation from the Judgment:
"It is established that the Federal Agency for Migration and Refugees was not authorized to read the data of the plaintiff's mobile phone and to analyse it by means of a software, to store the findings report generated based on the analysis of the plaintiff's mobile phone, to release the findings report for use in the plaintiff's asylum procedure and to base on it the decision on her application for asylum."[39]

Citation from the Judgment:
"The Federal Agency was ultimately not entitled to subsequently use the unlawfully collected and stored data, i.e. by releasing the findings report on May 28, 2019 for the plaintiff's asylum procedure and to base the decision on her application for asylum on it, since no weighty reasons existed to justify such encroachment on the fundamental rights by using the unlawfully obtained data."[40]

[36] See Federal Constitutional Court, Order of the First Senate of 3 March 2004 - 1 BvR 1084/99 -, Headnotes.

[37] Decision of the BVerfG of March 03, 2004, 1 BvR 2378/98, Leitsätze.

[38] Schmid, See also the already existing seminar tradition at the Chair of Public Law at the Technical University in 2015.

[39] VG Berlin decision of June 1, 2021 – VG 9 K 135/20 A, BeckRS 2021, 14390, Tenor.

[40] VG Berlin decision of June 1 2021 – VG 9 K 135/20 A, BeckRS 2021, 14390 Rn. 35.

III. Federal Administrative Court (Bundesverwaltungsgericht)

The Federal Administrative Court (FAC) upheld in essence in its 14-page decision the judgment of the Administrative Court Berlin. From a GLOBAL PERSPECTIVE, a special German path has to be noted: only in very exceptional cases are applicants forced to hand over their information technology systems in the context of establishing their identity and their right-of-abode procedure.

These three decisions originating from a German-European law context prepare for the research perspective which Weltrecht^2 assumes. Which is the research and analysis of different legal cultures in the context of innovation law and innovative law – here the **information technology relevant security law**. Therefore, in Chapter 5 recourse is made to the Backbone Document.

Chapter 5: Reference To Cylaw-Report XLII: Weltrecht^2 Backbone Documents"

Dynamic publication etiquette: the Cylaw-Reports shall be self-explanatory on the one hand; on the other hand, they shall reflect the author's best possible level of knowledge at the time of publication. Therefore, 'malfunction management' (MaMa)[41] is at times mandatory. Below, the preliminary annotations to Weltrecht^2 from January 2023 shall be published with the following editorial amendments: The Latin XXXX shall be replaced by XL. In all other respects, it remains in citation mode.

REFERENCE TO "Cylaw-Report XXXXII (XLII): Weltrecht^2 Backbone Documents" - here "Paper": "Multidisciplinary Constitutional Law Scholarship from Germany and the EU" submitted to World Congress of Constitutional Law in Dec. 2022"

PRELIMINARY ANNOTATIONS TO WELTRECHT^2 & THE CLYAW-REPORT SERIES (STATUS IN JANUARY 2023):

"Weltrecht^2" 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 "Weltrecht^2" has been chosen for a World Congress of Constitutional Law (WCCL) with the conference title "Constitutional Transformations" 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." This **"Backbone Document"** presents the 10,000-word 'paper' titled "Weltrecht^2 - Multidisciplinary constitutional law scholarship from Germany and the EU". This Cylaw Report XXXXII forms part of the "Weltrecht^2-Series" and builds **directly**

[41] MaMa" ist ein Neologismus der Autorin, der angesichts der Herausforderungen der digitalen Transformation für die deutsche Rechtsprechung – von der Justiz zur E-Justiz – 2014 konturiert wurde. Auch rückblickend lässt sich festhalten: Die Forderung nach Malfunction-Management als Rechtsprinzip wie – Anspruch hat den test of time („tot") bestanden. So war etwa das deutsche Bundesverwaltungsgericht im April 2023 für mehrere Tage nicht mit dem elektronischen Gerichts- und Verordnungspostfach (EGVP) erreichbar. Siehe für Zukunfts(rechts)wissenschaftliches Legal Design in 2014: Schmid zu § 55a und § 173 VwGO in: Sodan/Ziekow (Hrsg.), Kommentar zur Verwaltungsgerichtsordnung, 4. Auflage 2014, § 55a Rn. 26, 38, 39, 64, 87,121; § 173 Rn. 19 Fn. 44.

- onto Cylaw Report XXXXIII (XLIII): Viola Schmid in 2023/02 → here "ORAL "WCCL - LAUNCH ": "MULTIDISCIPLINARY CONSTITUTIONAL LAW SCHOLARSHIP FROM GERMANY AND THE EU" ON DEC. 7TH 2022– [soon to be published]
- onto Cylaw Report XXXXI (XLI): Viola Schmid in 2023/01: „Weltrecht^2 Entourage Documents", (Version 2) → here: A STANDARD FOR A UNIVERSAL (TECHNOLOGY) LAW LECTURE (2018)
- 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 **G**erman **L**anguage [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 Symposion (IRIS 2016), p. 441 – 448 also in German language [GL].

FORMAT: The following "backbone document" reproduces ASAP (as soon as possible) the submission to the conference in South Africa, held December 5 to 7, 2022. It is therefore acknowledged and accepted that the formatting may not be ABAP (as best as possible – own terminology). Rather, we have set store by keeping the documents in their original format (with only slight editing) – and as originally submitted (confidentially) -, in order to make them available to the interested audience in an immediate and multinational manner to facilitate and promote a [broad] discourse on Weltrecht^2. "Pedigree information": the submission format in November 2022 was Google Drive, following the choice of the conference chair.

VERSATILE FOOTNOTE DOCUMENT (own terminology (ot)): Weltrecht^2 announced this versatile footnote strategy: "Multinational additions of footnotes remain reserved for the Weltrecht^2 Agenda and future publications. A publication in Zenodo (https://about.zenodo.org/) will follow. The term 'Zenodo' is derived from Zenodotus, the first librarian of the Ancient Library of Alexandria and father of the first recorded use of metadata, a landmark in library history.'" German titles and terminologies cited here have been kept in German to allow for better traceability in e.g. library catalogues and/or legal databases. 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. If readers are interested in further information in English, please feel free to contact the author (schmid@cylaw.tu-darmstadt.de).

The author would like to express her deep gratitude to Nitharshini Santhakumar, LL.M., for her support in formatting the article as well as providing first-audience critique as part of an academic writing lab. In addition, she would like to thank Dr. Christoph Merkelbach and Annette Wiedenbach - also but not only - for their language support. The author retains responsibility for any errors and remains thankful for any further critique at schmid@cylaw.tu-darmstadt.de.