Regulating Cyberspace between *Grotius*, *Lotus* and Strasbourg

Andreas Kulick[*]

I. The Three "De"s 559
II. Four Questions 561
1. Which Actor? 561
2. Who Governs How? 562
3. Which Legal Regime? 564
4. Which Regulatory Paradigm? 565
III. Conclusion 568

In this very short piece, I would like to submit a few preliminary thoughts on the regulatory challenges cyberspace poses to (international) law. These, in turn, touch upon some of the most pivotal concepts of general international law: jurisdiction, international legal personality, responsibility of non-state actors, state responsibility and, of course, above all: sovereignty. In the following, I will seek to lay out a framework for these regulatory challenges that may help not only to systematize and order some of the challenges and potential ways to address them but that also, however more *en passant* than in a targeted manner, may inspire further thinking on how to address questions as to some of the aforesaid pivotal concepts of general international law *vis-à-vis* the challenges of cyberspace.

I. The Three "De"s

To start with the rather obvious, the regulatory challenges cyberspace confronts us with, from the perspective of international law, have a lot to do with three "de"s: de-territorialization, de-centralization and de-etatization. Most obviously, cyberspace transgresses borders. It is, at least to some degree, rather non-spatial in the sense of territory or physicality.[1] Law, by

* Privatdozent (*venia legendi*), Dr., LL.M. (NYU), visiting professor (Lehrstuhlvertreter), Georg-August-Universität Göttingen in the summer semester of 2020.

1 However, see the seminal *J. E. Cohen*, Cyberspace as/and Space, Colum. L. Rev. 107 (2007), 210 et seq., constructing cyberspace as "social space", as "experienced spatiality mediated by embodied human cognition".

contrast, is usually territorially linked.[2] While international law does not always have to be limited to a specific territory, but can have world-wide application – think of custom or the admittedly rather rare occasion of a completely universal treaty – it usually does not: Treaties usually apply only to the territories of the state parties to them,[3] the secondary law of (regional) international organizations also usually only applies to the territories of their member states.[4] This poses challenges not only when the attempt is made to regulate the horizontal relationship between global tech companies such as Google and Facebook and its users, particularly with regard to privacy and data protection, as *Stephan Kolo*ß*a* addresses in his paper.[5] It also pertains to issues such as jurisdiction over global data flows, particularly enforcement jurisdiction.[6]

De-centralization – international law's lack of a central government, i.e., a central legislature, executive and judiciary – amplifies the regulatory challenge posed by de-territorialization: international law is inter-national, not global. Thus, giving an answer to the de-territorial challenge of cyberspace that transgresses the confines of territory is both messy and strenuous. Custom is difficult to form and even more difficult is it to discern what the customary norm actually says, specifically. A treaty of global application needs to be thus: global, i.e., with all 195 states and other semi-independent territories etc. on board, in order to avoid loopholes that would otherwise undermine the entire effort.

However, even if there were customary and treaty norms of global application in place, would this sufficiently address the regulatory challenges of cyberspace? Hardly. This, of course, is because of what I refer to as de-etatization: This trend, particularly prominent (again)[7] after World War II, pertains to the arrival of non-state actors on the international arena. The rise of the individual and thus of human rights immediately comes to mind. However, with regard to cyberspace, the most important aspect of de-etatization is the role multinational corporations, i.e., the global tech companies, play in the regulation of cyberspace. Different to individuals, they

2 As *Stephan Kolo*ß*a* aptly points out in his paper, see 509 et seq.
3 See Art. 29 of the Vienna Convention on the Law of Treaties.
4 See, e.g., Arts. 52 TEU and 355 TFEU.
5 See *S. Kolo*ß*a* (note 2).
6 See only *M. N. Schmitt/L. Vihul* (eds.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 51 et seq.
7 On the role and status of the Trading Companies, particularly the Dutch and the British East India Companies, see *C. Berezwoski*, Les sujets non souverains du droit international, RdC 65 (1938), 1 et seq.; *C. H. Alexandrowicz*, Treaty and Diplomatic Relations between European and South Asian Powers in the Seventeenth and Eighteenth Centuries, RdC 100 (1960), 207 et seq.

become regulatory competitors to states, both on the domestic and the international levels, as they set standards for the users of their platforms, applications or search engines regarding privacy, data protection or freedom of speech for example.[8] So, an effective regulatory framework for cyberspace must take into account that a lot, if not to say most of the rule-making, at least in certain sectors, is done by non-state, i.e., corporate actors. In addition, of course, most of the rule-making pertains to non-state actors: individuals affected by corporate data policies, global tech companies deleting user content for alleged breaches of their terms of use etc.

II. Four Questions

If we now zoom in closer, I think four questions are particularly instructive in that they may provide a framework, or a matrix if you will, that fosters understanding of the regulatory challenges cyberspace confronts international law with. These four questions are: (1) Which actors are involved? (2) Who governs how? (3) Which legal regime(s) is/are employed in order to address the specific issue? (4) Which regulatory paradigm(s) is/are being adopted? While I do not think that these questions are by any means exhaustive, I submit that they pertain to what arguably are the most pivotal regulatory questions cyberspace poses to international law.

1. Which Actor?

As foreshadowed with respect to the three "de"s, three international actors are of particular importance with respect to the regulatory challenges of cyberspace *vis-à-vis* international law: individuals, states and corporations. Let me call them, with a deliberate tongue-in-cheek naïveté: the good (individuals), the bad (states) and the ugly (corporations). In line with such naïveté we may describe individuals as potential targets in need of protection of human rights violations, traditionally by states, against whom they hold domestic fundamental and international human rights, granted by national constitutions and international (or regional) human rights treaties. Corporations come into the picture because they accumulate considerable power resources that may affect, or even target, individuals as well. But they do not fit into the classical structure of international law, as they are not parties

[8] Such as *Stephan Kolo*ß*a* describes *vis-à-vis* Facebook, see *S. Kolo*ß*a* (note 2).

to the respective human rights treaties and both domestic and international human/fundamental rights up to the present day are usually not regarded as bearing horizontal effects.[9]

Reality, naturally, is much more complex. First off, human/fundamental rights issues are just one aspect of the regulatory challenges of cyberspace.[10] Secondly, the state's role is not limited to being the bad guy. Quite the contrary, it is states' regulatory efforts – domestically, regionally (through regional international organizations such as the European Union [EU]) or internationally – that may contribute to the protection of individual rights. Beyond human rights issues, there are of course vital (national) security interests that make state/international organization cyberspace regulation perfectly legitimate, such as prosecution of and enforcement regarding cybercrimes.[11] Thirdly, as again already pointed at before,[12] it is also more complex than stated above as to who – between the individual, the state and the corporation – sets and influences regulatory standards. This leads directly to the second question regarding who governs and how.

2. Who Governs How?

To start with maybe the least intuitive, individuals can exert considerable influence on the regulation of cyberspace. While they themselves, at least as individuals, cannot set standards – albeit, they can do so as a collective, i.e., as the *demos*, at least indirectly in a representative democracy – individuals influence cyberspace regulation through pursuit of claims and other remedies before domestic, regional and international courts, tribunals or regulatory bodies. They can take the initiative to thwart regulation violative of their rights or even in some instances may successfully demand creation of new rules. Think, e.g., of various examples from the jurisprudence of the Court of Justice of the European Union (CJEU), above all the right to be

[9] For the international level see, e.g., *A. Reinisch*, The Changing International Legal Framework for Dealing with Non-State Actors, in: P. Alston (ed.), Non-State Actors and Human Rights, 2005, 37 (38). For the domestic level see, from a comparative perspective, *S. Gardbaum*, The "Horizontal Effect" of Constitutional Rights, Mich. L. Rev. 102 (2003), 387 et seq.

[10] See, e.g., *J. Daskal*, The Un-Territoriality of Data, Yale L. J. 125 (2015), 326 et seq.

[11] See, e.g., *S. W. Brenner*, Cybercrime: Criminal Threats from Cyberspace, 2010, in particular 139 et seq.

[12] See above I.

forgotten that the Court acknowledged upon a claim introduced by a Spanish national against Google in the *Google Spain* case.[13]

However, yet, individuals themselves usually cannot regulate but need an intermediary. Such intermediary may be the state and its various organs, including courts, as well as – of increasing importance at least in Europe – regional international organizations and their organs, above all the EU (and its courts). States may adopt domestic legislation, such as the German Netzwerkdurchsetzungsgesetz (NetzDG, Network Enforcement Law)[14] or national policies such as the Chinese measures regarding cybersecurity.[15] Regional organizations such as the EU may establish sweeping legal regimes such as the General Data Protection Regulation (GDPR).[16] On the international level, states may, at least theoretically, conclude multi-lateral treaties or contribute to the emergence of international custom. Finally, states regulate cyberspace through executive action, including prosecutorial and enforcement measures.[17]

Nonetheless, because states and regional organizations are territorially bound, their regulatory reach – absent entirely globally applicable rules involving all three types of international actors as identified before – is territorially limited and thus to some degree inadequate to address the borderless challenges of cyberspace and cybersecurity. Here, corporations enter the regulatory stage. Global tech companies conclude individual private law contracts with their users that set certain standards with respect to, among others, nudity, free speech or data protection and portability.[18] Hence, corporations establish private regulatory schemes and standards with often a world-wide reach, which, absent a global public regulatory framework, affect users in a very similar way as and parallelly, additionally and complementarily with domestic or regional public regulation.

Of course, the answer to who governs with regard to a particular issue is not necessarily clear-cut. Think of the aforementioned German Network Enforcement Law, which is an example of what we may call regulated self-

[13] See CJEU Case C-131/12, Judgment of 13.5.2014 – *Google Spain and Google*.

[14] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz, NetzDG), BGBl. 2017 I, 3352 et seq., in force as of 1.10.2017.

[15] See the Chinese Ministry of Public Security ("MPS")'s Guideline for Internet Personal Information Security Protection of 19.4.2019, see <http://beian.gov.cn>.

[16] Regulation 679/2016/EU of the European Parliament and of the Council of 27.4.2016, OJ L 119, 4.5.2016, 1 et seq. (General Data Protection Regulation, GDPR).

[17] On US policy and legislation on the issue, see, e.g., *J. Galbraith*, Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data, AJIL 112 (2018), 486 et seq.

[18] See *Stephan Kolo*ß*a's* examples regarding Facebook, (note 2).

regulation:[19] Legislation sets a framework according to which private social media companies must administer their services. Also, domestic or regional regulatory schemes may be initiated by grassroots movements or individual claims before domestic or regional courts that lead to judgments requiring subsequent legislative or other regulatory action by the domestic or regional authorities.

3. Which Legal Regime?

The aforesaid paves the way to the third question: Which legal regime(s) is/are employed in order to address the specific issue of cyber activities and security at hand? Again, three main regimes may be identified: private, domestic public and public international law. To start with the last one first, issues of cyberspace could be addressed through bi-, pluri- or multi-lateral treaties or even through evolving norms of international custom. While strictly speaking global regulation by way of multi-lateral treaties or rules of customary international law are both absent and unlikely to emerge in the near future, bi- or pluri-lateral treaties that do not include the entire world but significant parts of it seem more realistic. Think for example of the framework developed by the Trans-Pacific Partnership Agreement (TPP),[20] which, however, eventually failed because of United States (US) withdrawal from the ratification process under the Trump administration[21] and has been resuscitated only without the participation of the most important player with regard to issues of cyberspace.[22]

In absence of global or nearly global responses to the de-territorialized challenges of cyberspace, regulatory initiatives from the public sector must remain territorial. They may take the form of domestic or regional laws or regulations requiring public authorities and/or private entities to observe certain rules pertaining to data protection, privacy or else. In addition, states

[19] On this concept see, e.g., *M. Liesching*, Lösungsmodell regulierter Selbstregulierung – Zur Übertragbarkeit der JMStV-Regelungen auf das NetzDG, in: M. Eifert/T. Gostomzyk (eds.), Netzwerkrecht – Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, 2018, 135 et seq.

[20] See in particular Ch. 13, 14 and 18 TPP.

[21] See <https://ustr.gov> (visited 19.3.2020).

[22] See *D. Sherwood/F. Iturrieta*, Asia-Pacific Nations Sign Sweeping Trade Deal Without U.S., Reuters, 8.3.2018, available at <https://www.reuters.com> (visited 19.3.2020).

may regulate cross-border private law relations also through their conflict of law rules.[23]

Most frequent and most adept at the freedom and flexibility that cyberspace offers, however, is regulation by private actors, particularly global tech companies such as Facebook, Alphabet (Google), Microsoft and the like, through private legal arrangements. These, as regards their doctrinal structure, have usually three aspects. First, as mentioned before,[24] they consist of private law contracts between the individual user and the service provider. These contracts are creatures of domestic private law. However, because these contracts usually contain rather lengthy and complex terms of use, i.e., contracts of adhesion (or, in German legal parlance, Allgemeine Geschäftsbedingungen [AGB]), that apply to all users, second, their sum creates a regulatory regime that may include rules on the deletion of content, the freezing, blocking or deletion of accounts[25] or even forms of dispute settlement, including appeals mechanisms.[26] Since content transgresses borders easily and since different users may reside in different countries and again act from the territory of yet other states and since the service providers operate globally, third, these private regulatory (and also potentially adjudicatory) schemes attain a transnational dimension.[27]

4. Which Regulatory Paradigm?

Most pivotal, however, is the fourth and final question that pertains to the regulatory paradigm entertained in order to address the challenges of cyberspace. From the perspective of international law, I submit, the following three paradigms are the most prevalent as to the regulatory approaches towards the challenges of cyberspace: (1) a *mare liberum* paradigm; (2) a *Lotus*/*Nottebohm* paradigm; or (3) a Strasbourg/human rights paradigm. These paradigms, naturally, should be understood as *Weberian* "ideal

[23] On this see *P. S. Berman*, Global Legal Pluralism: A Jurisprudence of Law Beyond Borders, 2014, 195 et seq., advancing a bold reconception of the matter at 244 et seq.

[24] See above II. 2.

[25] See on this, e.g., *F. Cafaggi*, New Foundations of Transnational Private Regulation, J. L. & Soc. 38 (2011), 20 et seq.

[26] On the latter see Facebook founder and CEO *Mark Zuckerberg's* announcement in an op-ed in the Washington Post of 30.3.2019, *M. Zuckerberg*, The Internet Needs New Rules. Let's Start in These Four Areas, Washington Post, 30.3.2019, available at <https://www.washingtonpost.com> (visited 19.3.2020).

[27] On this matter see, e.g., *L. Viellechner*, Transnationalisierung des Rechts, 2013.

types"[28] that can overlap and aspects of which can be combined with one another.

Mare liberum: Under a *mare liberum* paradigm, the cyberspace is regarded as a space resembling the high seas: no state can claim sovereignty, characterized by freedom of action, dominated by free agents that can navigate as they please and thus are free to impose their own rules on such space beyond the control of particular states. Borrowing from *Grotius*, I think, is particularly adequate considering the parallel that can be drawn from his motivation to write *mare liberum*, as part of his *de jure praede*, following the Santa Catarina incident:[29] The study, published separately in 1609, was intended to serve as a justification for a private company, the Dutch East India Company (VOC),[30] to act freely and beyond the spheres of control of (rival) state governments.

Indeed, there is a considerable amount of *mare liberum* in the aforementioned regulatory approach of self-regulation and standard-setting by the big global tech firms of the present day. Not unlike the Trading Companies of the great naval nations of the 17th and 18th centuries, above all the VOC and the British East India Company,[31] the theory of egalitarian freedom of the high seas/cyberspace in practice transforms into an oligarchy of standard-setting by a few powerful players. Also, not unlike with respect to the Trading Companies that commanded armies and administered territories,[32] the classical late 19th, early 20th century concept of state sovereignty is called into question *vis-à-vis* large multinationals that wield tremendous power over the arguably most valuable resource of the 21st century, i.e., data, and themselves have established global standards on the use of this resource.

Lotus/Nottebohm: Speaking of the classical paradigm of state sovereignty as consolidated in the second half of the 19th and the first half of the 20th century, the dominant thinking here is one of compartmentalization of separate spheres of influence: usually of a territorial nature; focused on states as the only relevant regulatory actors; that exert exclusive regulatory power within their domestic realm; and that coordinate their relationship *vis-à-vis* other states. Thus, in *Wolfgang Friedmann's* words, an order of "co-

[28] *M. Weber*, Wirtschaft und Gesellschaft, 4th ed. 1956, Vol. I, 3 et seq.

[29] See on this *S. Kadelbach*, Recht, Krieg und Frieden bei Hugo Grotius, 2017, 8 et seq.

[30] On the history of the VOC see, e.g., *N. Steensgaard*, The Dutch East India Company as an Institutional Innovation, in: M. Aymard (ed.), Dutch Capitalism and World Capitalism, 1982, 235 et seq.

[31] On the history of the British East India Company see, e.g., *J. Keay*, The Honourable Company: A History of the English East India Company, 1993.

[32] See, e.g., *S. R. Brown*, Merchant Kings: When Companies Ruled the World, 1600-1900, 2010.

existence" or coordination.[33] Internally, this is what several states attempt when regulating issues of cyberspace and cybersecurity within their domestic realm and also jurisdictional measures, including issues of enforcement jurisdiction, may be based on such paradigm. However, the spatial thinking underlying this paradigm, focused on sovereign, separate spheres of influence controlled by individual states, seems a rather futile and at best subsidiary and complementary response to the regulatory challenges of cyberspace, considering its non-spatial character.

Strasbourg/Human Rights: However, there is a third regulatory paradigm that is, like the previous paradigm, primarily driven not by private but by public actors. It nonetheless seeks to transcend the classical *Lotus/Nottebohm* paradigm in two respects (which, however, do not necessarily need to be present cumulatively but also can exist individually from each other). Firstly, it often places individual rights and interests front and center of regulatory efforts. Government policies or regional initiatives such as the General Data Protection Regulation (GDPR), e.g., focus on "data subjects," i.e., usually individual human beings.[34] Even more importantly from a regulatory perspective *vis-à-vis* the challenges of non-spatial cyberspace, secondly, it focuses on the effect on individual or other interests by certain actions under the control or influence of non-individual international actors in cyberspace: it asserts applicability, even extra-territorially, whenever the relevant actor controls any aspect of the activity in question. Or, put differently, from the perspective of states, it focuses on responsibility: i.e., the state's responsibility not to inflict and to protect from harm, both with respect to individuals as well as with respect to an effective system of crime prevention and enforcement etc.

A distinctive innovation of the European Convention on Human Rights (ECHR) and the Strasbourg court's human rights jurisprudence has been the extra-territorial application of the ECHR, according to Article 1 of the Convention, based on the concept of control or responsibility, as expressed in the notion of "jurisdiction": if an ECHR member state controls[35] a certain activity that affects Convention rights, it is responsible for such activity,

[33] See *W. Friedmann*, The Changing Structure of International Law, 1964, 15, 60.

[34] See GDPR (note 16), e.g., Preamble, Recital (1) and Art. 1(1).

[35] As the ECtHR (GC) explains in *Loizidou v. Turkey*, 23.3.1995, Preliminary Objections, App. No. 15318/89, paras. 62 et seq., Art. 1 entertains a concept with regard to "jurisdiction" pursuant to Art. 1 ECHR, which is less strict than the Nicaragua approach (*Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), ICJ Reports 1986, 14, paras. 109-110, 115) prevalent under general public international law, see *J. Crawford*, State Responsibility – The General Part, 2013, 155 et seq.

even if said activity takes place outside its state territory.[36] A similar rationale underlies the GDPR, for example: as soon as a company processes personal data of a data subject of the EU – and thereby asserts control over these data[37] – it falls within the purview of the GDPR and thus has to abide by its rules.[38] In a sort of reverse-type human rights notion, this can also be said of the underlying rationale of the extra-territorial enforcement policies prevailing in current state practice:[39] if the data are being processed, stored etc. by an intermediary service provider that has a link to the enforcing state, the latter enjoys jurisdiction.

III. Conclusion

Hence, counter-intuitively, the contemporaneous hot topic of international law and cyberspace leads us back to age-old, if not to say timeless, questions of public international law: participants in the making of international law, responsibility, jurisdiction, sovereignty. As I have argued in this sketchy account, the challenges of cyberspace – the three "de"s of de-territorialization, de-centralization and de-etatization – crystallize into four interlinked questions: Which actor? Who governs how? Which legal regime? And most importantly: Which regulatory paradigm? As we have seen with respect to the last question, the recent approach of the EU, through the GDPR, appears to offer a new paradigm that promises to combine extra-territorial reach of individual protection with public instead of private

[36] See for the development of the case law *B. Rainey/E. Wicks/C. Ovey*, Jacobs, White, and Ovey: The European Convention on Human Rights, 7th ed. 2018, 89 et seq.

[37] Which thus means a rather wide concept of control in this regard, see Art. 4(2): "[…] 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[38] See Art. 3(2) GDPR: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

[39] See merely *A. Ghappour*, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, Stanford L. Rev. 69 (2017), 1075 et seq. or *A.-M. Osula*, Accessing Extraterritorially Located Data: Options for States, in: CDCCOE – NATO Cooperative Cyber Defence Centre for Excellence (2015), available at <https://ccdcoe.org> (visited 19.3.2020), 17 et seq.

regulation of cyberspace.[40] This is by no means the perfect solution, since such regulatory paradigm threatens to create a pluralism of overlapping spheres and potentially competing extra-territorial jurisdictions. However, as *Nico Krisch* argued forcefully a decade ago,[41] in the postnational era pluralism is not necessarily a bad thing – and even less so in the messy regulatory world of cyberspace. In any case, the regulation of cyberspace needs further thinking beyond the *Lotus* and *Grotius* paradigms.

[40] See above II. 4.

[41] See *N. Krisch*, Beyond Constitutionalism: The Pluralist Structure of Postnational Law, 2010.