The Rule of Law in Cyberspace: A Hybrid and Networked Concept?

*Nicholas Tsagourias**

I. Introduction

The rule of law is a legal principle which has also become a principle of governance.[1] It is attached to state orders and signifies "law's title to rule"[2] as opposed to rule by political power which is often associated with discretion, arbitrariness, and the instrumental use of the law. It requires that individuals and governing institutions are guided by and respect the law with the ultimate goal of disciplining the exercise of power. *Dicey's* standard-bearer definition of the rule of law as "no man is above the law"[3] expresses this idea.

From a domestic concept conditioning the exercise of state power, the rule of law was also transposed to the international legal order.[4] The international rule of law can be defined in the following terms: "international law should guide the conduct of states: it is the final arbiter of the exercise

* Professor of International Law and Director of the Sheffield Centre for International and European Law, University of Sheffield, <Nicholas.Tsagourias@sheffield.ac.uk>.

1 Report of the Secretary-General on the Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies, UN Doc. S/2004/616, 4.

2 *G. Palombella/N. Walker*, Introduction, in: G. Palombella/N. Walker (eds.), Relocating the Rule of Law, 2009, xi.

3 *A. V. Dicey*, [1885], Introduction to the Study of the Law of the Constitution, 1982, 114, <http://files.libertyfund.org>.

4 Declaration on the Rule of Law at the National and International Levels made at the High-Level Meeting on the Rule of Law at the National and International Levels, A/RES/67/1, 30.11.2012, <https://www.un.org>. *B. Tamanaha*, On the Rule of Law, 2004, 127 et seq.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

of power and states must comply with its provisions".[5] As with the domestic notion of the rule of law, the aim of the international rule of law is to tame the power of the state, encapsulated in the notion of sovereignty. Sovereignty connotes ultimate power and the international rule of law provides a framework according to which sovereign power can be exercised externally and internally under the authority of the law.[6]

Against this backdrop, in this article I will engage in a mapping exercise of how the rule of law as traditionally defined in jurisprudence is experienced and realised in cyberspace which will be used as a springboard to conceptualise its parameters in cyberspace. My main contention is that cyberspace provides an environment where a *hybrid and networked rule of law* concept can emerge, exhibiting some of the traditional attributes of the rule of law but one that is also open and interactive regarding its participants and properties. Such conceptualisation signifies the adaptation of the rule of law for an environment – cyberspace – which has a political, legal, social and technical dimension and is also characterised by the emergence of governance structures outside the state context. In relation to this, it should be noted that the rule of law is a construct which responds to demonstrations of power wherever they take place and in whatever form they manifest themselves and is modelled according to the characteristics of the particular order to which it applies.

II. The Concept of the Rule of Law

Although the rule of law is an important legal-political principle, its content is debated. Central to the debates is the question of whether, in order to achieve its aim of guiding human and institutional action and tame political power, the rule of law should have formal and procedural attributes only or also substantive ones. The former view envisages a thin notion of the rule of law, whereas the latter a thick one.[7]

---

[5] *G. Blum*, Bilateralism, Multilateralism, and the Architecture of International Law, Harv. Int'l L.J. 48 (2008), 323 (331 et seq.); *M. Kumm*, International Law in National Courts: The International Rule of Law and the Limits of the Internationalist Model, Va. J. Int'l L. 44 (2003/04), 19 (22); *W. W. Bishop*, The International Rule of Law, Mich. L. Rev. 59 (1961), 553 (553).

[6] Individual Opinion Judge *Anzilloti*, Customs Regime between Germany and Austria, PCIJ Series A/B, No. 41, 57.

[7] *P. Craig*, Formal and Substantive Conception of the Rule of Law: An Analytical Framework, Public Law (1997), 467; *B. Tamanaha* (note 4), 91 et seq.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

Fuller for example emphasises the formal and procedural aspects of the rule of law which are the following: (i) laws must apply equally to everyone across the area of jurisdiction; (ii) laws must be made public; (iii) laws must be applied retroactively; (iv) laws must be clear enough to be followed; (v) laws must not be contradictory; (vi) laws must be possible to obey; (vii) laws must maintain some consistency over some time; (viii) there must be congruence between an official action and the stated law.[8]

In the same vein, *Raz* posits that the rule of law "means that government in all its actions is bound by rules fixed and announced beforehand – rules which make it possible to foresee with fair certainty how the authority will use its coercive powers in given circumstances, and to plan one's individual affairs on the basis of this knowledge".[9] Since the "basic intuition" from which the rule of law derives is that "the law must be capable of guiding the behavior of its subjects",[10] the rule of law has, according to *Raz*, eight attributes: three formal and five procedural ones. The formal attributes are, first, that "all laws should be prospective, open, and clear"; second, that "laws should be relatively stable"; and third, that "the making of particular laws (particular legal orders) should be guided by open, stable, clear, and general rules".[11] The five procedural attributes refer to the accessibility to law institutions and to law protection and are the following: the independence of the judiciary must be guaranteed; the principles of natural justice must be observed; the courts should have review powers over the implementation of the other principles; the courts should be easily accessible; the discretion of the crime-preventing agencies should not be allowed to pervert the law.[12]

From the above, it becomes apparent that a thin notion of the rule of law is concerned with the ways law is promulgated and applied in order to maintain its autonomy and, consequently, ability to guide human behaviour and restrain political power. Such a notion can also apply to the international rule of law. For instance, *Stephane Beaulac* posits that the international order is characterised by "(1) the existence of principled normative rules, (2) adequately created and equally applicable to all legal subjects and (3) en-

[8] *L. L. Fuller*, The Morality of Law, rev. ed. 1969, 46 et seq.

[9] *J. Raz*, The Rule of Law and Its Virtue, in: The Authority of Law: Essays on Law and Morality, 1979, 212.

[10] *J. Raz* (note 9), 214.

[11] *J. Raz* (note 9), 214 et seq.

[12] They are "designed to ensure that the legal machinery of enforcing the law should not deprive [the rule of law] of its ability to guide [individual action] through distorted enforcement and that [the rule of law] shall be capable of supervising conformity to the rule of law and provide effective remedies in cases of deviation from it'". *J. Raz* (note 9), 218.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

forced by accessible courts of general jurisdiction".[13] Indeed, there exist in international law primary rules that regulate most areas of international interaction as well as secondary rules of interpretation, adjudication, and enforcement. This finding should however be tempered by certain features of the international order such as the horizontal and decentralised manner in which law is created, interpreted, implemented, applied, and enforced, which can affect the construction and scope of the international rule of law without however denying its existence.[14]

A thick notion of the rule of law maintains that the rule of law, in addition to the attributes of the thin notion, also promotes certain substantive values which, among others, include justice, human rights, democracy, or liberty.[15] When invoking such a notion of the rule of law, one should however make a distinction between those values that are inherent to the rule of law and which are secured by its formal and procedural attributes; and those values that are independent and separate from the rule of law but actively promoted by the rule of law. *Raz* for example argues that the rule of law protects personal freedom and ensures respect of human dignity but these values are innate to the rule of law,[16] whereas *Lord Bingham* contends that human rights are values promoted by the rule of law.[17] It is only in relation to independent values that one can speak of a thick notion of the rule of law. A thick notion can also apply to the international rule of law which can be viewed as instrumental in promoting the values of peace, justice, and "social aims, in such fashion as to preserve and promote the values of freedom and human dignity for individuals".[18]

The debate between the proponents of a thick and the proponents of a thin version of the rule of law is inconclusive. The former criticise the latter for collapsing the rule of law to the notion of "rule by law" which does not necessarily offer protection against arbitrary power. They also question the contention that the formal requirements of the rule of law promote human

[13] *S. Beaulac*, The Rule of Law in International Law Today, in: G. Palombella/N. Walker (note 2), 203 et seq.

[14] *B. Tamanaha* (note 4), 128. For a critical approach see *A. Watts*, The International Rule of Law, GYIL 36 (1993), 15 and *S. Chesterman*, An International Rule of Law?, Am. J. Comp. L. 56 (2008), 331 et seq.

[15] *B. Tamanaha* (note 4), 112 et seq.; *B. Tamanaha*, The Rule of Law for Everyone?, Current Legal Probs. 55 (2002), 97.

[16] *J. Raz* (note 9), 211.

[17] *T. Bingham*, The Rule of Law, 2010; *R. McCorquodale*, Defining the International Rule of Law: Defying Gravity, ICLQ 65 (2016), 277 et seq.; European Commission for Democracy through Law (Venice Commission), Report on the Rule of Law, adopted at its 86th plenary session, Venice, March 2011.

[18] *W. W. Bishop* (note 5), 553.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

dignity and, instead, argue that the rule of law in fact derives from human dignity, a substantive value. The detractors of a thick notion in turn raise questions about the type of human rights that should be included in such a notion and how the rule of law can be distinguished from other concepts such as justice.

The immediate question then is how these constructions of the rule of law map out in cyberspace in light of the latter's particular features of a-territoriality, interconnectedness, instantaneousness, a-materiality, anonymity, as well as the absence of a single and unitary sovereign in cyberspace and the prominence of the private sector.

III. Challenges Facing the Traditional Rule of Law Concept in Cyberspace

On the basis of the preceding discussion it transpires that the thin notion of the rule of law with its attributes of publicity, clarity, certainty, and consistency can be variably challenged in cyberspace.[19] To explain, activities in cyberspace can take place simultaneously across different jurisdictions whose laws may not be known or understood or whose laws may be inconsistent or contradictory.[20] This state of affairs is not confined to domestic laws only but extends to international law as well because states may have different international law obligations. Moreover, to the extent that the international rule of law interacts with the domestic rule of law in order to tame sovereign power internally, the different ways in which domestic orders accept, interpret or refer to the international rule of law is another source of uncertainty. As a result, power may not be constrained whereas individuals may not get clear guidance or may be required to do the impossible.

Cyberspace can also challenge the rule of law's property of generality. Generality is about the application of the law to abstractly defined categories of people or to abstract situations but cyber operations cannot be easily distinguished from one another because their means and methods are indistinguishable. Moreover, individuals or cyber users and operators in general may not be able to control cyber operations because data travel in packets

[19] *H. B. Holland*, The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty, J. Marshall J. Computer & Info. L. 24 (2005), 1 et seq.

[20] See for example in relation to the Digital Millennium Copyright Act ("DMCA") the report "Unintended Consequences: 16 Years under the DMCA", <https://www.eff.org>.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

and can take different paths or because they may not know the architecture of the system and its connections. For example, it is difficult to qualify *ex ante* a cyber operation as cyber espionage, cyber theft, or cyber armed attack because the same means and methods can be used which may produce different effects which can further be direct or indirect. Often it is only *ex post*, when effects occur, that cyber operations can be legally qualified. Yet, law enforcement after the event[21] may be considered to be outside the rule of law because law, in this case, fails to provide guidance prior to the act and does not allow individuals to foresee the consequences of their actions. Post-act enforcement seems to be about the instrumental use of law, which the rule of law tries to prevent.

The rule of law in cyberspace can also be challenged by the normative gaps that exist in international law, the indeterminacy of existing international law rules and the uncertainty that surrounds their application to cyberspace. Although it is accepted that international law applies to cyberspace,[22] how it applies or what is the content and scope of the applicable rules is debated. For example, it is not settled whether espionage is a lawful activity in international law; whether sovereignty is a legal rule; or what constitutes a use of cyber force.

Cyberspace can also challenge values inherent to the rule of law or values promoted by the rule of law in its thick version. Being exposed to multiple rule of laws means that individuals are exposed to arbitrariness, something that can have a negative impact on their dignity as an innate value of the rule of law or as a substantive value promoted and protected by the rule of law in the form of human rights. More critically, cyberspace can provide a facilitative environment that can be exploited by states in order to intrude into and tamper with human rights or democratic values. Incidents of electoral cyber interference reveal how cyberspace can be used for such purposes.

Electoral cyber interference has mainly taken the form of "hack and leak" operations and disinformation operations but other methods include trolling, memes, and deep fakes. Electoral cyber interference can undermine the right to privacy[23] by harvesting, using, and sharing personal and inferred data; the right to freedom of thought and to hold opinions without interfer-

21 *J. Raz* (note 9), 213.

22 UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24.6.2013, 68th Sess., UN Doc. A/68/98; UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22.7.2015, 17th Sess., UN Doc. A/70/174.

23 Art. 12 UDHR; Art. 17 ICCPR.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

ence;[24] the right to freedom of expression;[25] and the right to vote when, for instance, voters are discouraged from voting.[26] Electoral cyber interference can also inverse the democratic process by exerting control over the cognitive environment within which people make decisions in order to influence the outcome of the election and, consequently, influence the government that is elected.[27]

What can also affect the substantive notion of the international rule of law in cyberspace is the manner in which its often competing values are balanced. In the absence of firm institutions to adjudicate between competing values, for example between freedom of expression and security, the opportunities for the arbitrary use of power increase.

In addition to the above, there are further challenges that cyberspace's features of interconnectedness and anonymity pose to the traditional concept of the rule of law. Interconnectedness can undermine the relationship, mediated by law, between individuals and governing institutions (power holders) which is an essential trait of the rule of law. This relationship is diluted when individuals are exposed to multiple laws and to multiple power holders, having no input in the construction of those laws. Anonymisation in turn can negate the rule of law altogether because, in the relationship between power holders and those subject to power which is the basis of the rule of law, the latter is removed from the equation.

Finally, the fact that ownership of and control over cyber infrastructure is exercised by private companies which are also at the forefront of technological innovation, raises questions as to how the rule of law can be maintained in a private-public constellation of power and how the rule of law which, as was said, is also a governance principle will not be circumvented by private companies or by states acting through such companies, an issue I will discuss immediately.

---

[24] Art. 18 UDHR; Art. 19 ICCPR; Art. 18 ECHR.

[25] Art. 19 UDHR; Arts. 19-20 ICCPR.

[26] Art. 21 UDHR; Art. 25 ICCPR.

[27] *N. Tsagourias*, Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace, EJIL: Talk, 26.8.2019, <https://www.ejiltalk.org>. *N. Tsagourias*, Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace, in: D. Broeders/B. van den Berg (eds.), Governing Cyberspace: Behaviour, Power and Diplomacy, 2020, <https://ssrn.com/abstract=3438567>.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

IV. The Rule of Law in Cyberspace and Private Governance

As was said previously, the private sector owns and controls cyber infrastructure and consequently exercises forms of governance over digital platforms, entities, and people by adopting, interpreting, and enforcing norms and standards.[28] The emergence of private governance challenges many of the attributes of the traditional rule of law concept in its thin or thick version but, more critically, it poses a challenge to the rule of law itself.

In the first place, private governance is not designed to protect individuals from the exercise of power which forms the basis of the rule of law but it is business-oriented and, mainly, contractual where the power differentials between companies and individuals are more than striking.

Second, because tech companies have control over the "code",[29] over access to platforms, over published content, and over contracts with users (customers), the potential for unchecked power increases.

Third, private regulation is not "law" but standards which are voluntary, *ad hoc*, often vague, elaborated *in situ* and through on-going discussion with certain stakeholders. This means that they are more prone to discretionary and contextual interpretation and implementation. They are also enforced through private mechanisms whereas such enforcement may be informed by economic interests (for example, revenue from advertisement) or customers' views about norms and expectations. Any internal processes of appeal may also be limited, restrictive, and may lack transparency, whereas external and independent mechanisms of redress against adverse decisions may be few or completely absent. Tech companies thus act at the same time as judge and jury against the rule of law principle of *nemo judex in causa sua*.

Fourth, private governance standards may often be below the formal or substantive rule of law requirements but tech companies may resist requests for more rule of law compliant governance structures and standards. To use again incidents of electoral cyber interference as an example, although tech companies have introduced policies and standards to prevent and suppress such activities, these standards and policies are not always clear, comprehensive, or properly enforced and adjudicated. For example, whereas Twitter

[28] See for example "A Blueprint for Content Governance and Enforcement", 15.11.2018, <https://www.facebook.com>. Private governance is not only about tech companies but also about any other non-state actor regulating aspects of cyberspace such as ICANN although tech companies will be my main focus.

[29] *L. Lessig*, Code and Other Laws of Cyberspace, 1999.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

banned all political ads because, according to its founder and Chief Executive Officer (CEO), "political message reach should be earned and not bought",[30] this is not the case across all providers. Facebook failed to comply fully with the United States (US) Federal Trade Commission (FTC) Consent Decree 2011 which required Facebook to establish a "comprehensive privacy program" to protect users' data and to have independent, third-party audits every two years.[31] Facebook was implicated in electoral interference by allowing its customers' data to be harvested as in the case of Cambridge Analytica. Although it announced measures such as third party fact-checking, labelling of news outlets and launched the Facebook Protect policy to prevent hacking into accounts of political persons, it does very little about fake accounts or political ads. As the United Kingdom (UK) Parliament's Digital, Culture, Media and Sport Committee opined "Facebook seems willing neither to be regulated nor scrutinised".[32] Similarly, the UK Informational Commissioner submitted to the UK Parliament that "unless there is a legal order compelling a change in their business model and their practice, they are not going to do it",[33] whereas in relation to the activities of Cambridge Analytica, the UK Parliament opined that "it was a profound failure of governance within Facebook that its CEO did not know what was going on […] [t]he incident displays the fundamental weakness of Facebook in managing its responsibilities to the people whose data is used for its own commercial interests".[34]

Fifth, the competition for rules[35] that the private sector can create when they apply their own rules does not only fragment the governance of cyberspace but also falls below the rule of law standards because these rules will be contingent on the commercial and financial interests of the private companies, on what values they deem to be worthy of protection, and on the interests of a narrow circle of individuals cum customers who decide on what governance system they prefer according to the values they hold and want to promote or protect. It means, for example, that there will be a market of differing rules on privacy or hate speech and users will choose the

30 <https://twitter.com>.

31 United States of America Trade Federal Commission, in the matter of Facebook Inc., DOCKET NO. C-4365, <https://www.ftc.gov>.

32 House of Commons, The Digital, Culture, Media and Sport Committee Disinformation and "fake news": Final Report HC 1791, Published on 18.2.2019, para. 29, <https://publications.parliament.uk>.

33 House of Commons, para. 58.

34 House of Commons, para. 63.

35 *D. G. Post*, Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace, J. ONLINE L., 1995, Art. 3, para. 42.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

provider who is closer to their values and expectations.[36] However, this is contrary to the rule of law which detaches law from contingent social reality or from particular narrow interests. Even more critically, they may even turn private governance into an anti-rule of law echo chamber if this is what users want.

Sixth, and related to the above, private governance exhibits elements of instrumentalisation in the sense that users have little *direct* input in these governance structures which are mainly informed by the companies' financial or other considerations and by their interpretation of what their customers' expectations are.

Seventh, states may use private governance to evade the rule of law by treating certain matters such as human rights or consumer protection as private issues or by using private companies as proxies for regulation or enforcement, instead of using public regulation and enforcement.[37] To explain, rule of law abiding governments may "encourage" private companies to act in ways contrary to the rule of law as when they enlist their help to disclose personal data or block certain material but maintain that these practices are private and, therefore, outside the rule of law. At the same time, they can cover such practices with a blanket of secrecy. States with low rule of law standards can instead force private companies to disclose personal information but such conduct can also have collateral rule of law implications beyond the specific geolocation.[38]

Eighth, private companies can evade the rule of law not only by treating all private regulation as being below the rule of law threshold but also by

---

[36] *M. Zuckerberg*, Building Global Community, 18.2.2017, "The guiding principles are that the Community Standards should reflect the cultural norms of our community, that each person should see as little objectionable content as possible, and each person should be able to share what they want while being told they cannot share something as little as possible.", <https://www.facebook.com>.

[37] For a tenuous balance between blocking access to unlawful materials and legitimate access see *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, 27.3.2014; *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, 13.5.2014.

[38] See for example "Turkey Goes Into Battle with Google" 2.7.2010, <https://www.bbc.com>; "Singapore Instructs Facebook to Block Page Access Under Online Falsehoods Law", 17.2.2020, <https://www.zdnet.com>. That does not mean that rule of law states cannot obligate private companies to disclose personal data but such a demand follows rule of law procedures, for example, legislation and possibly adjudication. In relation to searching Apple Iphones see *Apple, Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, & Opposition to Government's Motion to Compel Apple's Assistance, In re the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300*, No. CM 16-10, C.D. Cal., 25.2.2016.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

using their technical knowledge and dark patterns to present activities or content as being outside the rule of law.

Ninth, private companies can also evade the rule of law by complexifying jurisdiction, denying *locus standi* to individuals or by playing rule of law frameworks against each other.[39]

Tenth, private governance can potentially antagonise the traditional statist rule of law concept or try to delegitimise it by misrepresenting its requirements or remedies and, more critically, by promoting private governance as the only credible form of governance. For example, tech companies can prioritise their community standards over state standards (by asking users to comply with their community standards) and they can prioritise their own governance institutions over state ones. Facebook's plan to create an "independent body, whose decisions would be transparent and binding" is a case in point because it antagonises state adjudication mechanisms.[40]

The above set out the challenges posed by private governance to the rule of law, but private governance can also undermine the rule of law concept itself. This is due to the fact that private governance inserts itself between the government and the governed and disrupts the direct link that exists between them, which is the foundation of the rule of law. Yet, tech companies are not direct subjects of the rule of law even if they exercise power and authority over individuals and they are not democratic or transparent. As a result, individuals as the targets of power and authority by the state and/or the private sector may find themselves exposed to arbitrary power. The question then is how to make cyber governance rule of law compliant?

V. A Hybrid and Networked Rule of Law Concept in Cyberspace

Notwithstanding the strains cyberspace places upon the concept of the rule of law, in my opinion, this should not be viewed as detrimental to the operation of the rule of law in cyberspace. If, as I said in the introduction, the rule of law is a construct and, if cyberspace with its particular features and governance layers represents a legal, political, technological, and social reality, the question to ask is how the rule of law should be conceptualised and operationalised in cyberspace. Cyberspace in fact invites us to think of

[39] See in general *E. Cohen*, Information Privacy Litigation as Bellwether for Institutional Change, DePaul Law Review 66 (2017), 535.

[40] *M. Zuckerberg*, A Blueprint for Content Governance and Enforcement, 15.11.2018, <https://www.facebook.com>.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

how the rule of law can be adapted in order to attain its underlying objectives of guiding behaviour and taming power in this novel environment which is both similar but also different from the traditional physical legal-political spaces where the rule of law applies. I therefore contend that, because of its particular features and governance structures, the rule of law in cyberspace should be conceptualised as a *hybrid and networked* concept.

With hybrid I describe a rule of law construct that has layers of the traditional, statist, rule of law paradigm with its underlying attributes and purposes, but also layers of a private rule of law paradigm which may not entirely satisfy the traditional attributes of the rule of law but shares the rule of law aim of providing guidance and constraining power in the particular context of private governance where such power manifests itself.

To explain, the rule of law in cyberspace has a layer of the thick paradigm of the traditional rule of law concept with its values of human rights, justice and human dignity as well as a layer of the formal paradigm with its attributes of stability, predictability, publicity, generality. There is, for example, a good amount of international and national law regulating cyber activities ranging from trade law to human rights, with rules exhibiting certainty, predictability, and stability, notwithstanding any interpretative penumbra which may exist and which is common to any rule of law regime. That law has been promulgated publicly by means of legislation, treaties, or customary law. There are also adjudication or, more generally, dispute settlement mechanisms at the international and national level.

In addition to this, the rule of law in cyberspace has a layer of guidelines, principles and standards produced and implemented by the private sector through its own mechanisms which interacts with and complements the traditional rule of law. This is inevitable in a complex regulatory environment such as cyberspace which, in addition to its political, legal, and social layer, also has a technical layer which is developed by the private sector and is controlled by it due to the technical specialisation that is needed. In view of the character of these actors, the type of relations they regulate, and the spaces over which they exercise power, certain of the formal traits of the rule of law such as generality, publicity, or prospectivity may not be attained to the degree the traditional rule of law concept, at least in its ideal version, may want, nonetheless this layer provides a normative framework within which the power exercised by private entities can be disciplined.[41]

From the above, the other trait of the rule of law in cyberspace is revealed, namely, its networked character. As noted above, technological spe-

[41] The question of whether it is effective is different although it should be admitted that an ineffective rule of law system signifies the absence of the rule of law.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

cialisation and the complexity of the cyber environment led to a power shift. As a result, there are two poles of governance in cyberspace: one public, represented by the state, its institutions and its notion of the rule of law, whereas the other site is private, represented by the tech companies which lay down their own normative and regulatory standards and which, even if not legally binding, produce normative effects. These two poles coexist and interact with each other in many ways.

Firstly, the private layer of governance can fill the regulatory gaps that can emerge due to varied reasons: the fact that the state cannot regulate the code-based dimension of cyberspace; the private sector's ownership over cyber infrastructure; the specialised knowledge required for regulation;[42] the territorial discontinuity of the traditional rule of law regime in cyberspace; the blurring of different rule of laws in cyberspace due to its interconnectedness; and the break-down of the traditional distinction between the governors and the governed in cyberspace.

Secondly, state regulation and enforcement in cyberspace needs to be deliberated, negotiated and effectuated in conjunction with the private sector which owns and controls cyber infrastructure and has the technical know-how, even if in principle governments retain their regulatory and adjudicatory primacy.

Thirdly, due to the territorial transience of cyberspace, there should also be networking between different territorially defined rule of laws and their institutions such as governments and courts.

It can thus be said that public and private governance mutually condition the rule of law in cyberspace.

Having conceptualised the rule of law in cyberspace as a *hybrid and networked* construct, the immediate question is how such a construct can respond to the challenges discussed previously in order to attain the rule of law objective of providing guidance and disciplining power.

In order for this construction of the rule of law to attain the rule of law objectives in cyberspace, a number of more specific actions are required. First, states should close the regulatory gaps that exist and agree on how existing rules apply to cyberspace. As was said, States have confirmed the application of the rule of law in cyberspace[43] and are working individually

[42] *L. Lessig* (note 29).

[43] In relation to the UK see "Cyber and International Law in the 21st Century", speech by the *Attorney General Jeremy Wright QC*, <https://www.gov.uk>; in relation to the Netherlands see "International Law In Cyberspace: Appendix to the Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace", <https://www.government.nl>; in relation to France see "International Law Applied to Operations in Cyberspace", <https://www.defense.gouv.fr>;

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

or collectively to identify applicable rules and to clarify their application to cyberspace. I will not mention here each and every initiative but the United Nations (UN) Group of Governmental Experts (GGE) and Open-Ended Working group (OEWG) processes are worth mentioning.[44] However, although these processes reveal states' desire to populate cyberspace with norms, they also reveal the serious divisions and disagreements that exist which leave this area in a state of normative uncertainty. Likewise, whereas states frown upon "bad" behaviour in cyberspace by taking measures of retorsion or by imposing sanctions on individuals, entities, or states, they have not, as of yet, used the whole panoply of international law enforcement tools or remedies.[45] One can thus say that, at the moment, states appear to be programmatically attached to the international rule of law but quite reluctant to operationalise it either by legislating or by clarifying the content of existing rules, which means that normative consolidation remains a weak spot of the rule of law in cyberspace.

Such reticence at the international level is however compensated by more concrete initiatives in norm consolidation at the national or regional level. I will mention in this regard the Network Enforcement Act (NetzDG) passed in Germany in 2018,[46] the French law to combat information manipulation[47] or the European Union's (EU's) general data protection regulation.[48] One can thus say that there is intensification and thickening of the rule of law at national or regional level (at least in certain regions).

Second, states should ensure that domestic legislative action complies with the international rule of law, for example with human rights. Although

in relation to Australia see "2019 International Law Supplement to Australia's International Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace", <https://dfat.gov.au>.

44 See above note 20.

45 Recommendations to the President on Protecting American Cyber Interests through International Engagement, Office of the Coordinator for Cyber Issues, 31.5.2018, Prepared pursuant to Executive Order 13800, Section 3(c), <https://www.state.gov>. See also the EU Cyber Diplomacy Toolbox, General Secretariat of the Council, "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox)", 19.6.2017, Doc. 10474/17, <http://data.consilium.europa.eu> and <https://www.enisa.europa.eu>; Council Decision (CFSP) 2019/797 of 17.5.2019 Concerning Restrictive Measures Against Cyber Attacks Threatening the Union or Its Member States, OJ L129I/13 (2019).

46 <https://germanlawarchive.iuscomp.org>.

47 LOI No. 2018-1202 du 22.12.2018 relative à la lutte contre la manipulation de l'information <https://www.dropbox.com>.

48 Regulation 679/2016/EU of the European Parliament and of the Council of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

some differentiation may be inevitable in this regard because there is always room for flexibility and diversity when the international rule of law meets the national rule of law, it is important to stress that national legislation should be compatible with the international rule of law. For example, the German Network Enforcement Act has given rise to human rights concerns particularly in relation to the freedom of expression.[49]

Third, states should treat private governance as a modality of governance to be embedded within a rule of law framework.[50] As was said, private governance is a site of power and indeed one that affects real, not disembodied, people in all dimensions of their existence and not just in contractual terms; it affects their lives, dignity, the conditions of participation in society, professions, commerce, education, communication, and politics. Individuals are hugely dependent on private governance to exercise their private rights. For this reason, the state should ensure that the rule of law standards that inform public institutions and public life should extend to private governance and its institutions. This means that states, instead of deferring to private governance as a separate and autonomous form of governance, they should lay down the legislative framework within which tech companies should operate and exercise their power but also provide more clarity regarding its content, scope, and enforcement. For example, the German Network Enforcement Act tries to ensure that platforms delete or block illegal content within seven days after being reported or within twenty four hours if it concerns "manifestly unlawful" posts. It also imposes an obligation to publish a report every six months which would include, among other, information as to how it dealt with notifications of criminal activity and the mechanisms in place, the number of complaints and the number of deleted complaints. Companies that fall below the requirements of the Act are facing stiff fines. However, the lack of definition of what constitutes "manifestly unlawful" content in the German Network Enforcement Act can lead to underreaction or overreaction. To mention another example, the French law on the manipulation of information imposes a transparency obligation in

[49] Art. 19, Germany: The Act to Improve Enforcement of the Law in Social Networks, August 2017, <https://www.article19.org>.

[50] As was said "An untrammeled cyberspace would ultimately be inimical to liberal democratic principles. It would free majorities to trample upon minorities and would serve as a breeding ground for invidious status discrimination, narrowcasting and mainstreaming content selection, systematic invasions of privacy, and gross inequalities in the distribution of basic requisites for netizenship and citizenship in the information age. It is thus incumbent upon the liberal state selectively to regulate cyberspace." *N. W. Netanel*, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, Cal. L. Rev. 88 (2000), 395, 498.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

particular during elections and a duty of cooperation to combat disinformation. It also provides for injunctions to stop the circulation of inaccurate and misleading information and increases the supervisory role of the Conseil Supérieur de l'Audiovisuel (CSA). Another example is the "Online Harm" White Paper[51] proposed by the UK government which introduces a duty of care which involves the application and enforcement of certain standards by private companies to enhance users' safety and security online, for example from hateful content or sexual exploitation and abuse. That having been said, it raises questions as to how the formal and/or substantive rule of law requirements can be maintained if, for example, one type of harm against which tech companies have a duty of care is information "undermining our respect and tolerance for each other and confusing our understanding of what is happening in the wider world".[52] Unless the content of this provision and the action it requires are clarified, the possibilities for abuse increase because, in an effort to maximise their rule of law compliance, companies may introduce stringent requirements which can impact negatively on other rule of law attributes such as the freedom of expression or they may introduce more lax standards undermining the rule of law.

Fourth, states should enforce the rule of law when formal or substantive rule of law attributes are breached by tech companies. This is something that states have already done by taking legal action against them or by imposing fines for breaching regulations or guidelines.[53] For example, Facebook was fined in July 2019 for failing to meet the Network Enforcement Act's transparency requirements.[54] State enforcement action can strengthen the rule of law internally and internationally but also in relation to private governance because tech companies will be required to improve their governance standards and structures.

Fifth, states should introduce review and accountability mechanisms which can operate in tandem with existing state-based adjudicatory or conflict resolution mechanisms or similar mechanisms provided by tech companies, in order to ensure that laws and standards are interpreted, implemented, applied, and enforced in a rule of law compliant manner by state authorities or by private actors. For example and in relation to the "Online

51 See for example the UK government's Online Harms White Paper (April 2019) for a duty of care by tech companies, <https://assets.publishing.service.gov.uk>.

52 Online Harms White Paper (note 51), para. 7.25.

53 See for example the UK's Information Commissioner's Office, Investigation Into the Use of Data Analytics In Political Campaigns; A Report to Parliament, 6.11.2018, <https://ico.org.uk>.

54 <https://perma.cc/9G3V-SJRN>. The Federal Office of Justice imposed a 2 Mill. Euro fine. Facebook appealed against the fine.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

Harm" initiative, it has been proposed that Ofcom (Office of Communications) the UK's regulatory and competition authority for the broadcasting and telecommunications industries should become the regulator because of its expertise, experience and credibility.

Finally, states should reinforce existing conflict of laws rules and mechanisms or introduce new ones suited to cyberspace in order to address conflicts between different rule of law regimes. This is crucial because the existing jurisdictional meandering can lead to denial of the rule of law.[55]

As far as private governance is concerned, it was said above that it should be treated as a modality of governance embedded within the hybrid and networked rule of law construct. In fact it should be treated as another pathway to achieve the rule of law aims of providing guidance and of taming power, albeit within its own context of power constellations. Otherwise private governance may turn into raw and instrumental use of power in view also of the power differentials that exist between individuals and tech companies. This does not mean however that self-regulation should necessarily be rejected or that private entities should become a direct source of the rule of law or that their normative output should have the quality of law.[56] What it means instead is that private (tech) companies should recognise the fact that they are not actors in a virtual and lawless environment and that they are not neutral intermediaries between the governed and the government but serve the public good and exercise power producing direct and real consequences on individuals. Consequently, they should protect the public good and the public values which they serve and, they often do so. For example, in relation to the COVID-19 pandemic, Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter, and YouTube issued a joint statement pledging to fight fraud and misinformation.[57] Tech companies from around the world have also signed the Cybersecurity Tech Accord where they pledge to protect all customers and use from cyberattacks, oppose cyberattacks on innocent citizens and enterprises from anywhere, empower users and customers and partner with each other to strengthen cybersecurity.[58]

---

55 For a recent case see the referral by the Court of Appeal of Brussels to the CJEU for a preliminary ruling in the case of the *Belgian Data Protection Authority v. Facebook*, <https://www.dataprotectionauthority.be>.

56 It has been argued that tech companies' role resembles that of sovereign states. See *J. Cohen*, Law of the Platform Economy, U.C.D.L. Rev. 51 (2017), 133, 199 et seq. Accepting that view would however require a radical revision of our concept of international law and of sovereignty.

57 <https://twitter.com>.

58 <https://cybertechaccord.org>.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

The crux of the matter however is for tech companies that exercise governance functions to apply rule of law standards.

In order to do this, the standards and guidelines promulgated by the private sector should be as far as possible general, clear, stable, and predictable. That said, it is true that technical developments and new social conditions may necessitate *ex post* reaction, whereas anticipated security threats may require *ex ante* regulation but such *ex post* or *ex ante* regulation can be accepted only if it is consonant with the public good and the rule of law requirements of predictability based on reasoned decisions, where the uncertainty and the underlying assumptions behind such regulations are explained.

They should also establish review, scrutiny, accountability, and enforcement mechanisms to discipline their power internally but also subscribe to external supervision and oversight. These mechanisms should be independent, regular, and impartial, ascribing to the rule of law requirements when making determinations as to whether private governance standards have been breached or when enforcing penalties.

Their governance standards and structures should also be subjected to public debate. This is important because, as was said, these companies serve the public good and, for this reason, their governance standards and structures should be removed from the private realm of contracts and private interests and be openly scrutinised by those subject to them. Even if this process would not be equivalent to the social contract process between government and governed that underpins the traditional rule of law concept, at least, these standards and structures will be the subject of some form of debate and consensus about the public good and will not be top-down.[59] As was said in relation to states but can apply equally to private governance "the legality of a person's treatment, at the hand of the state depends on its being shown it serves a defensible view of the common good".[60] Another consequence of forming standards through open debates is that private contracts between companies and their customers (users) will also be informed by such standards and will not reinforce the power differentials that exist between companies and their customers cum governed.

---

[59] *Mark Zuckerberg* of Facebook envisages "creating a large-scale democratic process to determine standards with AI to help enforce them", *M. Zuckerberg* (note 36), however previous attempts were not successful. *A. Robertson*, Mark Zuckerberg Wants to Democratize Facebook – Here's What Happened When He Tried, VERGE, 5.4.2018, <https://www.theverge.com>.

[60] *T. R. S. Allan*, Constitutional Justice: A Liberal Theory of the Rule of Law, 2001, 2.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

VI. Conclusion

In this article I presented the challenges cyberspace poses to the traditional rule of law concept and then presented a rule of law concept constructed around the legal, political, technological, and social reality that cyberspace represents with its particular governance layers, structures, and participants. It is a *hybrid and networked* rule of law construct which combines aspects of the traditional rule of law based on public governance and aspects of the rule of law based on private governance. I then explained how this rule of law construct can be operationalised in cyberspace in order to guide behaviour and contain power and what steps states and private companies should take in this regard. In my opinion, this construct can effectively address the governance relations between states, companies, and individuals in cyberspace. Although aspects of this rule of law construct may require further elaboration, the main objective of this article was to instigate a conceptual shift in the way we approach the rule of law in cyberspace and invite further discussion as to how the aims of the rule of law can be attained in cyberspace through a rule of law concept which is reflective of and responsive to the environment to which it applies.

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht

http://www.zaoerv.de
© 2017, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht