BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 14, NUMBER 1 (2021)
ISSN 2029-0454

sciendo

Cit.: *Baltic Journal of Law & Politics* 14:1 (2021): 103-123
DOI: 10.2478/bjlp-2021-0005

PANDEMICS IN CYBERSPACE – EMPIRE IN SEARCH OF A SOVEREIGN?

Tomáš Gábriš

Professor
Palacký University Olomouc, Faculty of Law (Czech Republic)

Contact information
Address: Tr. 17. listopadu 8, 771 11 Olomouc, Czech Republic
Phone: +420 585 637 635
E-mail address: tomas.gabris@upol.cz

Ondrej Hamuľák

Senior Researcher
Palacký University Olomouc, Faculty of Law (Czech Republic)

Contact information
Address: Tr. 17. listopadu 8, 771 11 Olomouc, Czech Republic
Phone: +420 585 637 635
E-mail address: ondrej.hamulak@upol.cz

Received: April 26, 2021; reviews: 2; accepted: July 16, 2021.

ABSTRACT

Traditionally, the idea of a sovereign is being connected either with an absolutist ruler (later replaced by "the people") at the national level, or the nation-state at the international level – at least in the conditions of the Westphalian system created in 1648. Today, on the contrary, we are witnessing a "post-" situation in many respects – post-modernism, post-positivism, but also post-statism – basically being a sort of return to the pre-Westphalian system (see Ondrej Hamuľák, "Lessons from the 'Constitutional Mythology' or How to Reconcile the Concept of State Sovereignty with European Integration," *DANUBE: Law, Economics and*

Social Issues Review Vol. 6, No. 2 (2015); or Danuta Kabat-Rudnicka, "Autonomy or Sovereignty: the Case of the European Union," *International and Comparative Law Review* Vol. 20, No. 2 (2020)). However, paternalistic views, prevailing especially in times of crisis and uncertainty, desperately search for a sovereign to lead us from the crises. With regard to cyberattacks and insecurity in the cyberspace this means an effort to subordinate cyberspace to state sovereignty. Still, given the limitations of traditional state-based monopolies of power and legislation, the state as an "analogue sovereign" shrinks in the digital cyberspace rather to a co-sovereign, co-ordinator, or in feudal terms a "senior" vis-à-vis their vassals. The actual ensuring of the tasks of state as a "digital sovereign" is namely often being entrusted to non-state (essentially private-owned) entities, under the threat of legal sanctions. The current situation of constructing "digital sovereignty" of traditional states or of the EU is thus marked by the necessity of cooperation between the state power and those non-state entities which are falling under its analogue jurisdiction.

KEYWORDS

Digital sovereignty, stateless society, cyber-paternalism, shared sovereignty

NOTE

The paper was prepared within the implementation of the project no. 20-27227S "The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union" funded by the Czech Science Foundation (GAČR).

INTRODUCTION

The article offers a parallel between cyberspace and historical stateless society, but also between cyberspace and today's system of international law. Their common element (*tertium comparationis*) is the absence of a supreme sovereign. Traditionally, the idea of a sovereign is thereby being connected either with the absolutist ruler (later replaced by "the people") at the national level, or the nation-state at the international level – at least in the conditions of the Westphalian system created in 1648. Today, on the contrary, we are witnessing a "post-" situation in many respects – post-modernism, post-positivism, but also post-statism – basically being a sort of return to the pre-Westphalian system. But does this diagnosis really hold? Does it apply unconditionally and with no way back to "statism"? And does the same direction of evolution apply to cyberspace?

Today's pandemic namely sometimes reinforces the call for a strong state and the search for a paternalistic state-based and state-enforced legal solutions. These are traditionally being called for and invoked in times of crises or when there are security risks (let us just take the recent example of terrorism at the beginning of the third millennium).

Similarly, in cyberspace, we are currently witnessing numerous cyberattacks, and growing cyber-insecurity can also potentially serve as an argument for state paternalism and more extensive state intervention. Is thus cyberspace looking for its sovereign in a period of "cyber-incident pandemics"? But who is to take over this role? Previously, the role of sovereign was mainly ascribed to nation states internationally, and internally to their "people" and their elected representatives. The idea of the community of cyberspace users as sovereign "people" may certainly be appealing, but so far seems impossible and utopian. On the other hand, states as traditional sovereigns do indeed try to control and protect their "national cyberspace" – but given the nature of cyberspace this in fact means only the control of the assets in their territory and in their jurisdiction in the traditional sense. This strive for "national sovereignty" in cyberspace thus remains largely limited. It is aimed only at some aspects of activities and behaviour in cyberspace, not at "total" and monopolistic control of the "whole cyberspace".

Hence, given the limitations of traditional state-based monopolies of power and legislation, the state as an "analogue sovereign" shrinks in the digital cyberspace rather to a co-sovereign, co-ordinator, or in feudal terms a "senior" vis-à-vis their vassals, since ensuring the tasks of state as a "digital sovereign" is often being entrusted to non-state (essentially private-owned) entities, under the threat of legal sanctions. The current situation of constructing "digital sovereignty" of traditional

states or of the EU is thus marked by the necessity of cooperation between the state and those non-state entities which are falling in its analogue jurisdiction. However, the national digital sovereignty of a state and of its government quickly disappears as soon as the non-state entities escape the "analogue jurisdiction" of traditional state sovereigns, which may be relatively simple to achieve in the case of some entities. But even where the digital sovereignty of a traditional government still applies, this is currently being limited to only a very narrow section of cyberspace – basically only the regulation and protection of particular essential services and interests. Is this actually any sort of sovereignty at all?

1. CYBERSPACE: ANALOGIES TO THE ANALOGUE WORLD

In general, cyberspace may be regulated either by rules of law (regulation) or governed by extra-legal standards (governance), such as e.g. the rules so-called Netiquette. Originally, quite naturally, the extra-legal governance prevailed absolutely. In the meanwhile, though, many countries in the world took notice of the legal importance of cyberspace and started addressing it in their legal systems and legal norms. The states and their laws have thus entered into cyberspace.

Constitutions of some countries explicitly reflect this technological development and the emergence of cyberspace. E.g., Sweden has amended Article 2:1 of its Regeringsform from 1974 in order to make it more technology-neutral, guaranteeing: "The freedom to communicate information and to express ideas opinions and emotions, whether orally, in writing, in pictorial representations, or *in any other way*". On the other hand, Article 5 of the German Grundgesetz and the US freedom of speech provision (1st Amendment to the Constitution) are considered sufficiently abstract to accommodate for new technologies without any need for amendment. Finally, as a third possible approach towards tackling the legal aspects of cyberspace, the French protection of freedom of speech is based rather on lower legislation and on case law, which can take the technological development into account much faster, without the need to amend the Constitution at all. The French Conseil d'État (advisory board to the government) in its 1998 advice even somewhat surprisingly proclaimed that radical changes in legislation as a result of Internet evolution were unnecessary.[1]

Many countries adopted an approach situated somewhere in between the German and French attitude, meaning that the Constitution itself is not an issue as long as it is sufficiently abstract. Constitutional values are important rather in an

[1] Ronald Leenes, Bert Jaap Koops, and Paul De Hert, *Constitutional Rights and New Technologies: A Comparative Study* (The Hague: T.M.C. Asser Press, 2008), 8.

indirect way – the legislation namely further develops and implements constitutional rights. It is therefore mostly up to the legislation (Acts of Parliament and implementing ordinances, decrees etc.) to accommodate for the regulation of modern technologies including cyberspace, or more importantly, to provide for rights, freedoms and their protection even in the cyberspace. The states should namely realize they cannot turn a blind eye to the technological development and their obligations arising from the international law, generally accepted principles of human rights and freedoms, from their EU membership must be fulfilled even with respect to cyberspace.

However, coming back to the nature of rules regulating cyberspace, it is important to emphasize also the role of non-state, non-legal, extra-legal, i.e. social, economic, technological and other types of norms. Originally, it was namely claimed that the cyberspace is rather regulated by a non-legal Netiquette, and that cyberspace is and should be independent and free from any legal regulation. This was the underlying idea in the early beginnings of the Internet, in the period when Barlow openly proclaimed his 1996 Declaration of Independence of Cyberspace:

> Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.[2]

The original idea was hence that the assumption that the existence of law is based on state sovereignty and its monopoly of physical violence (coercion) simply does not work in the cyberspace, also due to the fact that there is no physical presence at all. Thus, the existence of law could allegedly not rely here on traditionally understood state-based norms and state-enforced sanctions.[3]

Indeed, in the period of the early evolution of cyberspace, it resembled a "*stateless society*", as known in Europe in the Middle Ages.[4] In Central and Eastern Europe, this would be mostly the historical period of the 9th to 12th Centuries, representing the founding period of the legal system of the Central European region.

[2] John Perry Barlow, "A Declaration of the Independence of Cyberspace" (May 2021) // https://www.eff.org/cyberspace-independence.
[3] Radim Polčák, "In Law, we Trust: Shortly to Bumblebees and the Normativity of Law in Cyberspace": 6-8; in: Radim Polčák, Martin Škop, and David Šmahel, eds., *Cyberspace 2005* (Brno: Masayrkova Univerzita, 2006).
[4] The same parallel has already been used by Alfred C. Yen, "Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace," *Berkeley Law Journal* 17 (2002): 1207.

In this period, "law" (if one is willing to anachronistically accept its existence in the modern sense of the word) appears as equivalent to a general normative system comprising and consisting of generally accepted ideas of justice, morality, ethics and religion. It was not based on any theoretical scholarship, nor on any legislation, but rather on actual daily experience and practice, on "local customs". This was a system of rules that worked fine without any central legislative authority, being at the same time based only on local enforcement – by the community itself. That is the main reason why cyberspace might have originally indeed resembled a pre-modern society and it still may be considered a living experiment (*in vivo*) of the emergence of customary law, and even of the application of the alleged "natural law" concepts of ownership, liability, and conflict resolution among the Internet users. The scholars of cyberspace hence have a possibility to research similar objects and use similar research methods as legal historians and legal anthropologists do, when studying the origins of legal (regulatory/governance) institutions in pre-modern societies and cultures. where state authorities are absent.[5]

Still, even today, in the "statist" or even "post-statist" era, there are state-less norms outside and without any state backing, and this is true even outside the cyberspace, in the "analogue world". One could mention here e.g. the so-called Sports Law (autonomous rules of international and national sports federations), or the Canon Law of the Roman Catholic Church. However, in contrast to these systems which are often rather pyramidally shaped, in the cyberspace, the immediate supreme authority is lacking to a much greater extent (with certain exceptions, e.g., that of admins in forums). In the cyberspace, therefore, the communities are closer to the state-less system of numerous communities creating their own rules of minimal ethical conduct. The role of users themselves – netizens, is of special importance.

All the provided analogies between cyberspace and historical stateless societies definitely have to do with the lack of centralised supreme regulatory authority in these systems – in contrast to some hierarchical non-state systems such as that of Sports Law or Canon Law. This is thereby the point where we should naturally shift our attention to the similarity between cyberspace and the current system of International law – also lacking a central authority.

To elaborate on this analogy in a greater detail, one may start here with an apparent similarity between the nature of the norms and rules in both systems. Currently, there are three basic approaches to the norms and rules of international law, and we suppose the same approaches can be taken for granted as far as the norms and rules of cyberspace are concerned:

[5] Edward E. Evans-Pritchard, *The Nuer: A Description of the Modes of Livelihood and Political Institutions of a Nilotic People* (Oxford: Clarendon Press, 1967).

a) legal idealism (school of natural law),

b) analytic approach, i.e., positivism, and

c) sociological approach, refusing positivism as well as idealism.

In general, the school of natural law recognizes morality as the basic source of law, and the way of getting to know the "true law". On the other hand, the sociological approach does not search for norms which should be applicable, but rather uncovers norms that are in fact being applied in practice as kind of sociological rules. Finally, legal positivism based on the fundaments laid down by H. Kelsen[6] or H.L.A. Hart.[7] Hart namely discerned between the so-called primary law and secondary law. The secondary law sets the rules for what should be accepted as primary law. That is how the current system of modern law works – a legal norm (so-called recognition norm) sets what should be considered law. However, in the other (historical) types of law and in other normative systems, it may be perfectly acceptable not to have any secondary recognition norm, rather only the primary normative system, not specifying what exactly should be considered law. According to Hart, this is the current situation in international law, which lacks a recognition norm and therefore is considered valid only as far as it is accepted in practice notwithstanding any recognition norm.

In the world of cyberspace and its normative system, these approaches can be perfectly united with the Lessig's explanation of the regulatory system of cyberspace – allegedly consisting of four layers: "law", "social norms", "market" and the "code".[8] While law is created under specific rules for the enactment of law (an idea being close to legal positivism), market and social norms are rather sociological (societal and economical) rules, which may at the same time reflect the general notions of natural law and ideas of natural justice. The "Code" should then be understood as a part of the technological "ecosystem" – nature, or reality – giving foundation and framing (but also limiting) the whole system of norms in the cyberspace.

The role of state agencies and of state-based law is hence naturally minor in cyberspace, providing only a part of the applicable norms. Nevertheless, in comparison with the early cyberspace, state agencies interfere with cyberspace to an ever-greater extent nowadays, not being limited only to specific areas such as patrolling for criminal activity (cybercrime) anymore.[9] The states interference into cyberspace is gaining impetus mostly with respect to cyberattacks and other cyber

[6] Hans Kelsen, *General Theory of Norms* (Oxford: Oxford University Press, 1991).
[7] Herbert L. A. Hart, *The Concept of Law* (Oxford: Oxford University Press, 1961).
[8] Lawrence Lessig, *Code V.2* (New York: Basic Books, 2006).
[9] Aleš Završnik, "Cybercrime: (Cyber)Criminological and (Cyber)Victimological Particularities of the 'Information Superhighway'": 161; in: Radim Polčák, Martin Škop, and David Šmahel, eds., *Cyberspace 2005* (Brno: Masayrkova Univerzita, 2006).

incidents, where a traditional sovereign is called to fulfil its role of protecting the rights and freedoms of its citizens.

Thereby, historically speaking, as soon as the central power becomes more intervening, the traditional self-governance gets weakened by the ever-increasing interference of the dominant regulatory authority. That is the point when "state society" emerges and replaces the earlier "stateless society". The absolutist states in Europe started to intervene in the lives of the towns, of the people in the countryside, even churches, whereby this was accepted and confirmed in the Westphalian system of international relations created in 1648 – recognizing sovereign states as being the sole and supreme sovereigns in the territory under their control.

The state-centered monopoly of law-making and law-enforcing emerging between the 17th and 18th centuries, with the peak at the turn of the 19th and 20th centuries, represents also a dramatic change and shift in the understanding of law, influencing our modern perception of law in continental Europe. The original non-state-based normative systems of autonomous corporations and different social groups were replaced by the widely accepted theory of the state-centered legal monopoly.

However, the idea of state-independent rule-making never died away completely even in the 20th century. Santi Romano, Italian lawyer in the 1930s, the forerunner of the modern idea of legal pluralism, was one of those who proposed the idea that law is primarily a social phenomenon, and that every social institution forms its own social norms, thus creating their own "law".[10] Although this simple solution does not necessarily have to convince all opponents, the use of the term "law" to designate non-state-made standards was not at all uncommon in the 20th or 21st centuries: for example, in 1933, a German lawyer Hans Grossmann-Doerth used the phrase "*selbstgeschaffenes Recht der Wirtschaft*" (autonomous law of economy) as a synonym for general contractual terms and conditions; similarly, the label of "*autonomes Recht*", "*private Normenordnungen*", "*autonome Rechtsordnungen*" or "*Privatgesetzgebung*" is still being used nowadays to denote non-state-based normative systems,[11] such as *lex mercatoria*, *lex sportiva*,[12] or *lex constructionis* (the international construction standards),[13] but also the *lex informatica (lex digitalis, lex tecnica)*.

[10] Santi, Romano, *Die Rechtsordnung (The Legal Order)*, translated by Werner Daum (Berlin: Duncker & Humblot, 1975), 44–45.
[11] Miloš Vec, "Das selbstgeschaffene Recht der Ingenieure. Internationalisierung und Dezentralisierung am Beginn der Industriegesellschaft" (The self-created right of engineers. Internationalisation and decentralisation at the beginning of industrial society): 96-97; in: *European and International Regulation after the Nation State* (Baden-Baden: Nomos, 2004).
[12] Nils Ch. Ipsen, *Private Normenordnungen als Transnationales Recht? (Private Norm Systems as Transnational Law?)* (Berlin: Duncker & Humblot, 2009), 32.
[13] See Stefan Kadelbach, Klaus Günther, "Recht ohne Staat?" (Law without State): 19-21; in: Stefan Kadelbach and Klaus Günther, eds., *Recht ohne Staat? Zur Normativität nichtstaatlicher Rechtssetzung*

One might, however, still be sceptical and believe that all these systems represent only a transitional stage, and in the future they will be subjected to state control and replaced by state-made norms in full.[14] Nevertheless, even then, the normative systems such as international law or European Union law or legal principles introduced by jurisprudence and case law, will probably still be exempt from state control, causing some authors from the opposing camp, supporting the idea of non-state law and legal pluralism,[15] to believe that the state has throughout the 17th to 19th centuries usurped powers which do not necessarily belong to the state, and now is partially withdrawing from the regulatory field, allowing once again for the emergence of the never-completely-forgotten "non-state" law.[16]

How might the situation look like with regard to the regulation of cyberspace, what are the natural limits of state-based regulation in cyberspace and what forms the sovereignty of state might take in cyberspace, will be pondered upon in the following pages.

2. GOVERNANCE OR REGULATION IN THE CYBERSPACE?

In the context of regulation of cyberspace, there are two main lines of thought as to the most appropriate way for the cyberspace to be regulated or governed: the cyber-libertarian approach and the cyber-paternalist approach. The cyber-libertarian approach links the new technology with libertarian ideas such as freedom, society and market, and requests that these liberties should be protected also in cyberspace. The opposite, cyber-paternalist view, requests that a centralised regulatory control is introduced.[17]

So far, none of the two approaches proves valid – the state sovereigns intervene into cyberspace, albeit only to a very limited extent and through very specific regulatory methods. While the cyber-libertarian approach is thus being refused by the state and also by those who call for guarantees for their rights and freedoms (and for protection) even in the cyberspace, the cyber-paternalist approach necessarily fails due to the lack of a dominant position of one supreme digital sovereign. Cyberspace is namely only "softly" (extra-legally) governed by various self-governing bodies – such as the ICANN[18], closely related to the IANA

(Law without State? On the Normativity of Non-State Lawmaking) (Frankfurt am Main: Campus Verlag, 2011).
[14] Nils Ch. Ipsen, *supra* note 12, 246.
[15] Boaventura de Sousa Santos, "Law: A Map of Misreading. Toward a Postmodern Conception of Law," *Journal of Law and Society* 14(3) (1987).
[16] Reinhold Zippelius, *Verhaltenssteuerung durch Recht und kulturelle Leitideen (Behavioural control through law and cultural guiding ideas)* (Berlin: Duncker & Humblot, 2004), 161.
[17] Kevin M. Rogers, *The Internet and the Law* (London: Palgrave Macmillan, 2011), 6.
[18] See ICANN (May 2021) // http://www.icann.org.

organization,[19] a non-binding Internet Governance Forum (IGF), the ISOC – Internet Society and others – mostly from among local authorities, bodies, and self-governing communities, with only partial interference by the state sovereigns and organizations such as the European Union (see infra). So far, the self-governance of the cyberspace thus truly resembles rather an autonomous and diffused community with only minor and limited authorities.

However, what used to be perceived as only a vague patrolling function of states, slowly changes into actual legal interference by traditional sovereigns (EU, states) into some sectors of cyberspace – albeit in a rather limited extent and effect.

From among the tools that states use to enforce their sovereignty in cyberspace and at the same time to delineate their area of competence from that of other states (by as a sort of e-borders), they use legal tools of establishing jurisdiction, determination of applicable law, cooperation in investigation of cybercrime, geo-blocking, censorship, blocking of cross-border online-gambling, the so-called general blocking laws,[20] rules on e-evidence, e-privacy, data protection and cross-border transfer of personal data[21], electronic identity and trustful services, electronic communication, and – last but not least – the most recent efforts for strengthening cyber security, especially in relation to the future extensive use of 5G networks.

The instruments by which states (EU Member States) and the EU itself enforce their sovereignty in cyberspace are primarily legal instruments – the traditional tools of traditional sovereigns. However, the specificity of cyberspace also requires a specific form of legal instruments (besides non-legal, mostly technical instruments that the traditional sovereigns are not accustomed to use).

As the most relevant examples of accommodation of legal rules to the specificities of cyberspace and modern technologies, we can mention here two examples: the requirement or the need for the technological neutrality of law, and the greater use of teleological standards.

To start from the latter, the EU law, not only in the area of efforts to regulate cyberspace, is characterized by an increased rate of the use of so-called teleological, special-purpose rules, which, instead of a specific procedure, set only the desired goal of the legal regulation, leaving the way of achieving it to the relevant addressees of the law, provided they respect the values of constitutionality and legality on their way. This is the case, in particular, with the Directives of the European Union – as one of the basic sources of EU law, besides the directly applicable Regulations. The

[19] Kevin M. Rogers, *supra* note 17, 8.
[20] Erica M. Davila, "International E-Discovery: Navigating the Maze" (May 2021) // https://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/37.
[21] Jozef Andraško, Matúš Mesarčík, and Ondrej Hamuľák, "The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework," *AI & Soc* Vol. 36 (2021) // https://doi.org/10.1007/s00146-020-01125-5.

EU Member States are namely required to implement the targets set by the Directives through their own national legislation, choosing themselves the most appropriate way to achieve the goal.

The objectives set, but yet more the specific procedure for achieving the objectives, must in addition show a quality of being formulated in such terms that the rapidly evolving and varying technological tools will be covered in a neutral manner – this is the need for the formerly mentioned technological neutrality of legislation. Its essence is such a formulation of legal regulations, which as far as possible disregards the specificities of contemporary technological tools, in order to prevent the rapid need for the amendment of legislation. At the same time, according to some opinions, however, law can never be completely technologically neutral, as it in itself predominantly uses a "technologically" written form (in contrast to the historical times of oral and customary law). Nevertheless, where appropriate, efforts should be made to achieve a reasonable degree of neutrality, ensuring that the law will not have various effects depending on the technological processes and equipment used (document, electronic document). This type of neutrality is achieved, for example, by the fact that instead of a "paper form", rather a "written form" will be invoked by law, which naturally includes also electronic writing (electronic communication).

However, the law should also avoid the fixation of specific technological procedures and equipment available at the time of drafting the regulation, for which there may be a presumption of rapid obsolescence – e.g. with regard to e-government rules. On the other hand, sometimes technological neutrality leads to so much abstract and generally formulated norms that the addressees of law cannot unambiguously interpret and implement the legal norm. It is therefore clear that a reasonable compromise is necessary between the specificity and abstractness of the legislation.

Moreover, there are also critical voices that reject (technological) neutrality in certain respects, for example in relation to the monitoring of the population, when, on the contrary, the specification of technological procedures available to the state or other monitoring entities (secret service) should actually guarantee limits and prevent abuse of monitoring beyond what the respect for fundamental human rights and freedoms allows.[22]

Cyberspace and modern technology in general hence represent another new factor which shapes and influences both the content as well as the shape and form of legal norms used by the traditional sovereigns – the states. Within a kind of "legal

[22] Paul Ohm, "The Argument Against Technology-Neutral Surveillance Laws," *Texas Law Review* 88 (2010): 1685 *et seq*.

futurology", we can offer here briefly an image of two possible variants predicting contrasting future developments of the legal regulation of cyberspace.

The first option would be the use of special forms of law regulating cyberspace. The second may be a sort of autonomous law, as a compromise between governance and regulation – maybe in the technological form of the so-called smart, self-enforcing law.

The first indicated alternative is a path inspired by political science and the science of administration (administrative science) and their theory of the so-called "New governance". This, in contrast to the state administration, means administration by means of "social coordination", i.e., some form of democratic (self)administration.[23] The authority of central, state-made bureaucratic law is being questioned here; the law must be decentralized. Its source should thus again be the society, and the citizen should have the right to become an active participant in the administration of society, which itself should take on the form of a "network" instead of a hierarchical pyramidal structure.

We are indeed already witnessing some initial attempts at such a form of governance, especially in areas where the need for regulation (or governance) is newly emerging in conjunction with the latest trends in hitherto unregulated areas. E.g., the fight against obesity includes proposals for taxes on sugars and fats, to which, however, the producers of the respective products react immediately, trying to avoid the introduction of tough regulation by their own autonomous measures, such as the removal of snacks from primary schools. In this way, in some US states, the sector really managed to prevent "state" interference in this area of business. A rapid autonomous action thus might fulfil the aim and prevent the introduction of a new "state-made" legal rule.

A similar feature can be encountered in the regulation of personal data protection at the EU level – the EU General Data Protection Regulation (GDPR), for example, also leaves it to the actors – controllers and processors of personal data – to come up with specific solutions to achieve the purpose of the regulation. It is within their internal decision-making that they should determine first to what extent the regulation applies to their business, to what extent in what ways and for what purpose they process personal data, whether their interest in the processing of personal data is genuinely legitimate and to what extent their interest is in balance with the interests of the persons concerned (data subjects), etc. These evaluations in writing, archived and constantly updated by individual entities (addressees of the Regulation), will only be assessed upon inspection by the competent personal data

[23] Myungsuk Lee, "Conceptualizing the New Governance: A New Institution of Social Coordination" (May 2021) // https://pdfs.semanticscholar.org/71ec/0b861a6dad2d93b56ab5f8c6b77bfa415a48.pdf.

protection authority in the light of how the addressees themselves assessed and argued for their possibility to process personal data.

The same approach is currently being promoted and adopted in relation to cybersecurity at both the EU and Member States level, since cybersecurity objectives are to be ensured by the essential service operators or digital service providers themselves (being operators and providers of the most important, essential and sensitive services). The state (and the EU) only generally set goals of security to be achieved here, while the very technical and procedural way of achieving these must be chosen by the addressees of the rules themselves. Polčák speaks here of so-called performative rules as rules that rely on "defining authorities" to fulfil the rules themselves.[24]

Indeed, these are all manifestations of delegated "self-governance", a sort of "new governance" that manifests itself mostly in new areas of regulation, where there is no tradition of strict central, bureaucratic state-made regulation, which moreover might not even bring any results and expected effect, only bring about high costs for both the state and the taxpayers. This type of approach of the state is sometimes also called an "activating state" (*aktivierender Staat*), drawing thereby on the experience with the stimulation of the labour market in Germany.[25]

However, there may not be only positive sides present regarding this possible future of law in the cyberspace. It is especially clear that such a development places much more emphasis on individual responsibility (*vigilantibus iura*), or even emphasis on the importance of lawyers onto whom the responsibility for compliance with the law is to be entrusted. Moreover, according to some opinions, this approach may also cause blurring of the borderlines between norm-making, implementation and the application of law – the existing theory of law would thus need to be completely rebuilt.[26]

On the other hand, we have also foreshadowed the second possible way of development – namely the "smart regulation",[27] mostly in the form of self-enforceable "legal" norms, programmed in the particular device. Such an arrangement is currently proposed, for example, in conjunction with the use of blockchain technologies, which make it possible to pre-set the rules so as to eliminate the need for an intermediary, independent third party, depositary, dispute resolution body or enforcement body. An example is the programmed transfer of funds from

[24] Radim Polčák, *et al*., *Právo informačních technologií (IT Law)* (Praha: Wolters Kluwer, 2018).
[25] Stephan Bandemer, *et al*., "Staatsaufgaben – Von der 'schleichenden' Privatisierung zum 'aktivierenden Staat'" (The role of states – from 'creeping' privatisation to the 'activating state'"); in: Fritz Behrens, ed., *Den Staat neu denken. Reformperspektiven für die Landesverwaltung (Rethinking the state. Reform perspectives for the state administration)* (Berlin: Sigma, 1995).
[26] Jason M. Solomon, "New Governance, Preemptive Self-Regulation, and the Blurring of Boundaries in Regulatory Theory and Practice" (May 2021) // https://scholarship.law.wm.edu/facpubs/680/.
[27] Radim Polčák, *et al*., *supra* note 24.

one account to another, provided that certain conditions reflected in the program are met. Similarly, it can be used for the automatic distribution of inheritance (e.g. money in bank accounts) to heirs according to a will or law (programmed in a device controlling the handling of the funds of the deceased), similarly for payment of taxes, of insurance premiums and other fees, directly from the account of tax subjects or insured persons, etc.[28]

However, the question that one may pose here is whether this would not mean moving to an extreme "technological positivism", where all the "gains" of humanistic legal post-positivism emphasizing principles and values of good and justice would be abandoned by a return to the technological formalism of software rules – albeit ultimately independent from the state, being thus excluded both from the analogue as well as from the digital world.

3. IN SEARCH OF A SOVEREIGN

As already mentioned, it is not only the state who wish to become a sovereign in the cyberspace. Its role as a sovereign is sometimes called for even by the citizens, Internet users (netizens) themselves. Understandably, it is mostly if there is a problem, when they call for guarantees for their rights and freedoms (and for protection) in the cyberspace. Something similar materialized in the analogue world with respect to a general cry for state help, including EU aid, during the coronavirus COVID-19 pandemic taking place throughout the year 2020.

In general, crisis and imminent danger often leads to seeking protection from a stronger authority. Disregarding here the theories on the abuse of danger in order to strengthen the position of a sovereign (so-called securitization[29]), a similar development can be observed nowadays with regard to cyberspace. It was precisely in the field of cybercrime that cyberspace users themselves called for the first time for the legal regulation of cyberspace – however, up to now, only imperfect and often unenforceable regulation has been achieved.

Similarly, it is in the times of COVID-19 pandemics and the related general shift to digital services, that the need for a safe cyberspace has become even more imminent. The European Union can thus certainly find more support than ever to continue with its efforts for the creation of a true digital sovereignty of the EU,

[28] Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (May 2021) // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.
[29] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Publishers, 1998).

controlling the digital "European Public Sphere",[30] based on the self-proclaimed European values such as transparency, openness and privacy protection.[31]

Still, the gradually growing dependence of EU industry and of the whole "public sphere" on technology and on cyberspace (specifically with regard to the future use of 5G networks and Internet of Things) at the same time calls for precautionary measures to be thought of already at this point, so as to ensure the future security of interests of the EU and its Member States.

This becomes even more important with respect to the fact that most European data is stored either outside Europe or, if stored in Europe, on servers belonging to non-EU companies. That is the point where the notion of "digital sovereignty" of the EU comes into play, meaning foremost the supreme regulatory powers of the EU and its Member States aimed at the protection of the EU citizens, assets and interests, in spite of the enduring absence of a unified European cyberspace and cyber politics.

The first steps towards the idea of a digital sovereignty of the EU had to do already with the goal of creating a Digital Single Market, being a natural aim of economic cooperation among the EU Member States. However, since then, emphasis was also placed on data protection, regulation of electronic communications, cybersecurity, and most recently independent and protected European Cloud Initiative, or the so-called GAIA-X project.

The striving for the digital sovereignty of the EU is thereby clearly here to stay, albeit it certainly means to re-assess the proper notion of sovereignty itself. It is namely for sure that a sovereign control of the whole cyberspace is impossible given the current situation and technology, and also a creation of an "EU cyberspace" or various "national cyberspaces" seems precluded by the proper nature of the cyberspace as such.

The EU and any other sovereign can thus construct its "digital sovereignty" only with respect to specific assets and subjects (entities) in its direct scope of control (jurisdiction). This is in line with the notion of a "layered sovereignty", coined by Przemysław Roguski – meaning a distinction between the physical layer of cyberspace, the logical and social layers.[32] Roguski argues that while the physical layer is covered by state sovereignty by virtue of the principle of territoriality, the logical and social layers of cyberspace may be open to the exercise of state authority

[30] Henning Kagermann and Ulrich Wilhelm, eds., "European Public Sphere: Towards Digital Sovereignty for Europe," *The acatech IMPULSE series* (May 2020) // https://www.acatech.de/publikation/european-public-sphere/download-pdf?lang=en.
[31] *Ibid*.
[32] Przemysław Roguski, "Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment"; in: Tomáš Minárik, *et al*., eds., *11th International Conference on Cyber Conflict: Silent Battle* (Tallinn: NATO CCD COE Publications, 2019) // https://ccdcoe.org/uploads/2019/06/Art_19_Layered-Sovereignty.pdf.

based on a criterion of proximity, i.e. whenever the State can establish a genuine link with the digital objects or online personae over which authority is to be asserted.

In other words, this means that sovereigns are controlling entities that fall in their competence in the analogue world, i.e. outside the cyberspace – being their citizens and legal persons registered or providing services in their territory. Of course, this does not mean direct control of all such entities with regard to all their activities in the cyberspace, but only of those that provide services which are perceived as "essential" or "critical" for the security and interests of the sovereign. These are usually entities that provide access points to the cyberspace, or entities that need state licenses or permits in order to be allowed to provide their specific services in the territory controlled by the traditional sovereign (EU, state), or – in other terms – entities that can be effectively "tamed" by sanctions imposed by the sovereign. This solution thus represents a relatively simple way how to control the provision of essential services in the cyberspace still within the scope of the competences of a traditional sovereign.

Still, this is clearly the point where the traditional idea of sovereignty possibly turns into a new concept of sovereignty, similar to the new type of sovereignty allegedly shared between the EU and Member States. This time, however, the sovereignty seems to be shared between the state (or EU) authorities and non-state authorities, which are being entrusted with the tasks falling within their scope of activities, such as data processors in the case of data protection, and the operators of essential services and important digital service providers in the case of the legal regulation of cybersecurity. Tropina and Callan in this respect speak of co-regulation,[33] which can be situated on a continuum between the state-controlled regulation and self-governance. The two authors namely claim that "The decentralised architecture of the Internet is eroding old paradigms of the division of responsibilities between government, private sector and civil society, also because in general, the concept of Internet governance has been largely dominated by the idea of a multi-stakeholder model."[34] And they conclude: "Nowadays, self- and co-regulatory approaches exist in many areas of fighting cybercrime both on national and international levels."[35]

Hence, it seems that the state which acts as an actual traditional sovereign with regard to objects and persons falling into the scope of its jurisdiction, is largely relying on the cooperation with specific entities, that are actually being delegated the task to fulfil the day-to-day management of EU (or State) digital sovereignty. Their

[33] Tatiana Tropina and Cormac Callanan, *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security* (Cham: Springer, 2015).
[34] *Ibid*., 12.
[35] *Ibid*., 13.

cooperation (or co-regulation) under the supreme control of the traditional sovereign to whom they are responsible in the analogue world, is the necessary precondition in order to materialize the actual digital sovereignty and protection of interests of the EU and its Member States. Without this sort of cooperation and co-regulation, the analogue sovereign might in fact completely fail to assert its digital sovereignty in the cyberspace. To return back to the medieval analogies, to a great extent the digital sovereign in Europe is actually dependent on its vassals.

CONCLUSIONS

To what extent does cyberspace pose a challenge to the traditional concept of state sovereignty and to the concept of state-based and state-enforced legal regulation? There is no doubt that paternalistic views, prevailing especially in times of crisis and uncertainty, operate in an effort to subordinate cyberspace to state sovereignty, which can be seen in the efforts at the "juridification" of cyberspace or – in other words – the advancing regulation of some aspects of cyberspace by national legal systems. Numerous efforts to create "borders" of national cyberspace over which digital sovereignty could be asserted, are manifested for example in the form of rules for determining the applicable law, jurisdiction, geo-blocking and other blocking laws, censorship on the Internet, rules for electronic communication providers, protection of personal data and, last but not least, efforts to ensure national cyber security.[36] Still, in spite of this, cyberspace remains primarily a borderless area, since all technological as well as legislative tools aimed at erecting e-borders in cyberspace have failed so far, or at least they were not able to create truly impermeable boundaries. In their current form, they do not represent real state borders in the traditional sense, and instead of creating national cyberspace, their aim is actually rather to ensure the exercise of (national) state sovereignty (control) in the cyberspace over the objects and person that traditionally fall into the scope of jurisdiction of the respective sovereign states. This is made possible mainly through the control of access points to the cyberspace or through the control of providers of the respective services to be controlled.

In the case of the EU, where the actors in cyberspace are mostly private entities, the attempts at their control and at their use to assert digital sovereignty of EU over the cyberspace necessarily requires cooperation between the EU (its Member States) and the respective entities. For both objective and subjective reasons, neither the Member States nor the EU can currently take over the role of sole digital

[36] See Ondrej Hamuľák, Lilla N. Kiss, Tomáš Gábriš, and Hovsep Kocharyan, "This Content is not Available in your Country. A General Summary on Geo-Blocking in and Outside the European Union," *International and Comparative Law Review* Vol. 21, No. 1 (2021) // https://doi.org/10.2478/iclr-2021-0006.

sovereign in cyberspace on its own, without an active participation of the private entities under the control of the sovereign, who are being entrusted with numerous tasks so as to ensure at least a partial digital control by the EU (and its Member States) over some sectors of cyberspace. In order to assert this sovereignty, the EU and its Member States must in fact cooperate, coordinate and co-regulate the cyberspace together with the essential service operators and other digital service providers, doing this in a mutually advantageous relationship – the EU needs them to control cyberspace and to protect and secure the EU interests in the cyberspace, while the providers and operators fall into the jurisdiction of the respective sovereign in the analogue world (EU, Member State) and have the interest in providing services within its jurisdiction (possibly even with a special license or permit). Nevertheless, this means that these entities actually "share the digital sovereignty" – in cyberspace, the traditional analogue sovereign in international relations (the state) shares the sovereignty with its "people" (the domestic, internal sovereign) – albeit so far only with the "aristocracy" (vassals) as the most powerful entities entrusted and made co-responsible for the administration and management of cyberspace on behalf of the alleged digital sovereign.

BIBLIOGRAPHY

1. Andraško, Jozef, Matúš Mesarčík, and Ondrej Hamuľák. "The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework." *AI & Soc* Vol. 36 (2021): 623–636 // https://doi.org/10.1007/s00146-020-01125-5.
2. Bandemer, Stephan, *et al*. "Staatsaufgaben – Von der 'schleichenden' Privatisierung zum 'aktivierenden Staat'" (The role of states – from 'creeping' privatisation to the 'activating state'): 41–60. In: Fritz Behrens, ed. *Den Staat neu denken. Reformperspektiven für die Landesverwaltung (Rethinking the state. Reform perspectives for the state administration)*. Berlin: Sigma, 1995.
3. Barlow, John Perry. "A Declaration of the Independence of Cyberspace" (May 2021) // https://www.eff.org/cyberspace-independence.
4. Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.
5. Davila, Erica M. "International E-Discovery: Navigating the Maze" (May 2021) // https://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/37.

6. De Sousa Santos, Boaventura. "Law: A Map of Misreading. Toward a Postmodern Conception of Law." *Journal of Law and Society* 14(3) (1987): 279–302.
7. Evans-Pritchard, Edward E. *The Nuer: A Description of the Modes of Livelihood and Political Institutions of a Nilotic People*. Oxford: Clarendon Press, 1967.
8. Hamuľák, Ondrej. "Lessons from the 'Constitutional Mythology' or How to Reconcile the Concept of State Sovereignty with European Integration." *DANUBE: Law, Economics and Social Issues Review* Vol. 6, No. 2 (2015): 75–90 // https://doi.org/10.1515/danb-2015-0005.
9. Hamuľák, Ondrej, Lilla N. Kiss, Tomáš Gábriš, and Hovsep Kocharyan. "This Content is not Available in your Country. A General Summary on Geo-Blocking in and Outside the European Union." *International and Comparative Law Review* Vol. 21, No. 1 (2021): 153–183 // https://doi.org/10.2478/iclr-2021-0006.
10. Hart, Herbert L. A. *The Concept of Law*. Oxford: Oxford University Press, 1961.
11. Ipsen, Nils Ch. *Private Normenordnungen als Transnationales Recht? (Private Norm Systems as Transnational Law?)*. Berlin: Duncker & Humblot, 2009.
12. Kabat-Rudnicka, Danuta. "Autonomy or Sovereignty: The Case of the European Union." *International and Comparative Law Review* Vol. 20, No. 2 (2020): 73–92 // https://doi.org/10.2478/iclr-2020-0018.
13. Kadelbach, Stefan, and Klaus Günther. "Recht ohne Staat?" (Law without State): 9–48. In: Stefan Kadelbach and Klaus Günther, eds. *Recht ohne Staat? Zur Normativität nichtstaatlicher Rechtssetzung (Law without State? On the Normativity of Non-State Law-making)*. Frankfurt am Main: Campus Verlag, 2011.
14. Kagermann, Henning, and Ulrich Wilhelm, eds. "European Public Sphere: Towards Digital Sovereignty for Europe." *The acatech IMPULSE series* (May 2020) // https://www.acatech.de/publikation/european-public-sphere/download-pdf?lang=en.
15. Kelsen, Hans. *General Theory of Norms*. Oxford: Oxford University Press, 1991.
16. Lee, Myungsuk. "Conceptualizing the New Governance: A New Institution of Social Coordination" (May 2021) // https://pdfs.semanticscholar.org/71ec/0b861a6dad2d93b56ab5f8c6b77bfa415a48.pdf.

17. Leenes, Ronald, Bert Jaa Koops, and Paul De Hert. *Constitutional Rights and New Technologies: A Comparative Study*. The Hague: T.M.C. Asser Press, 2008.
18. Lessig, Lawrence. *Code V.2.* New York: Basic Books, 2006.
19. Ohm, Paul. "The Argument Against Technology-Neutral Surveillance Laws." *Texas Law Review* 88 (2010): 1685–1714.
20. Polčák, Radim, *et al*. *Právo informačních technologií (IT Law)*. Praha: Wolters Kluwer, 2018.
21. Polčák, Radim. "In Law, we Trust: Shortly to Bumblebees and the Normativity of Law in Cyberspace": 3–10. In: Radim Polčák, Martin Škop, and David Šmahel, eds. *Cyberspace 2005*. Brno: Masayrkova Univerzita, 2006
22. Rogers, Kevin M. *The Internet and the Law.* London: Palgrave Macmillan, 2011.
23. Roguski, Przemysław. "Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment": 1–13. In: Tomáš Minárik *et al*., eds. *11th International Conference on Cyber Conflict: Silent Battle*. Tallinn: NATO CCD COE Publications, 2019 // https://ccdcoe.org/uploads/2019/06/Art_19_Layered-Sovereignty.pdf.
24. Romano, Santi. *Die Rechtsordnung (The Legal Order)*. Translated by Werner Daum. Berlin: Duncker & Humblot, 1975.
25. Solomon. Jason M. "New Governance, Preemptive Self-Regulation, and the Blurring of Boundaries in Regulatory Theory and Practice" (May 2021) // https://scholarship.law.wm.edu/facpubs/680/.
26. Tropina, Tatiana, and Cormac Callanan. *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*. Cham: Springer, 2015.
27. Vec, Miloš. "Das selbstgeschaffene Recht der Ingenieure. Internationalisierung und Dezentralisierung am Beginn der Industriegesellschaft" (The self-created right of engineers. Internationalisation and decentralisation at the beginning of industrial society): 96–97. In: *European and International Regulation after the Nation State*. Baden-Baden: Nomos, 2004.
28. Wright, Aaron, and Primavera De Filippi. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (May 2021) // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.
29. Yen, Alfred C. "Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace." *Berkeley Law Journal* 17 (2002): 1207–1264.
30. Završnik, Aleš. "Cybercrime: (Cyber)Criminological and (Cyber)Victimological Particularities of the 'Information Superhighway'": 157–174. In: Radim Polčák, Martin Škop, and David Šmahel, eds. *Cyberspace 2005.* Brno: Masayrkova Univerzita, 2006.

31. Zippelius, Reinhold. *Verhaltenssteuerung durch Recht und kulturelle Leitideen*. *(Behavioural control through law and cultural guiding ideas)*. Berlin: Duncker & Humblot, 2004.