DIGITAL SOVEREIGNTY

Stelio Mangiameli[1]

Abstract
The contribution examines the most recent questions that the development of cyberspace has raised regarding the theme of sovereignty. In fact, despite the frequent recriminations regarding an alleged annihilation of the sovereignty of the States, we realize how the Internet – like all other public service networks – is fully subject to state authority and its legislation which preserves the unchanged charisma of legitimacy and satisfies general interests linked to community life. On the other hand, the technical legislation of private operators remains an expression of the core interests of these great powers whose actions never reach the dimension of public power, with the guarantees of rights and democracy, and never match the intervention capabilities of the State. Therefore, to safeguard the fundamental rights of the people of the Internet, a new regulation of cyberspace is needed, which is modeled according to a typically constitutional projection. To do this, however, in addition to the conformation of the State as a constitutional State of law, it is necessary to define an international network regime which, through the signing of a Cyberspace Treaty, recomposes the digital sovereignties of the States and limits virtual conflict.

Keywords
Digital sovereignty, Internet, Private Actors, Internet Bill of Rights, Cyberspace Treaty.

Summary

[1] Full Professor in Constitutional Law, Department of Law, Teramo University – Italy.

1. DIGITAL SOVEREIGNTY AND THE NET

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather". So stated John Perry Barlow, who saw cyberspace as a dimension fully capable of resisting the power of governments, in the name of freedom of thought.

"We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts. We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before"[2].

Never has a vision of the world been so incorrect and misleading, because "sovereignty" is a constitutive element of every order, including the virtual one. And without sovereignty, no order is possible, at least in the world of living persons.

The term "digital sovereignty" is used to indicate the prerogative of national states to impose rules on the activities and economy of the network, even if transnational and global, when they concern their citizens[3].

Today, digital sovereignty has become current, because the public demands a regulation of cyberspace, for multiple reasons: first of all, in online life an existential condition is manifested, characterized by an unclear distinction between the virtual and the real, for which many protection needs of the person, typical of the real world, have also taken on consistency in the virtual world; secondly, the information circulating online is reified (data) and has become goods in the legal sense, that is, "things that can form the object of rights" (art. 810 c.c.) and, as such, the object of economic activity, due to their accessibility, specificity and limited nature; finally, the large

[2] BARLOW 1996.
[3] BERTOLA 2022.

platforms[4] are no longer actors, but directors of the network and, even when they regulate their behavior, in reality, they do not look at the freedom of the people of the network, but exclusively at their interest and their self-representation as standard bearers of freedom and commonwealth is simply instrumental.

Regardless of the demand on behalf of public opinion, which increasingly pushes for a political regulation of the network to safeguard fundamental rights, it is clear that acts of sovereignty over the network have been possible since its creation. It is no coincidence that the beginnings of the internet are military and not civil and there is no military power that does not use instruments of any kind under a sovereign command. Subsequently, the network has enjoyed great freedom, especially in the academic field, giving rise to the dream of a global scientific community, capable of exchanging messages, studies, and discoveries, without any limitations and to the benefit of everyone. Only later came the commercial use of the internet and the creation of the digital market in which the large economic platforms entered. These too have enjoyed and, in part, enjoy great freedom, almost a "state of nature" of the network, without authority and rules.

However, it would be wrong to mistake the phenomenon for the cause. The total freedom we are talking about, the absence of authority, and the lack of rules that seem to characterize cyberspace, are only apparent and not structural of the virtual phenomenon. It is the States and, among them, the most powerful ones that dominate the "large spaces"[5] and represent the "great powers", who have allowed such a development of cyberspace, abstaining from regulating the network. It was a choice to encourage technological development and technological economy, but the internet has always been under the political control of government authorities, and this – as happens with every aspect of societies – is not in itself free of problems.

---

[4] SALVATORI 2023, 369: "in the broadest sense of the term, the platform is a structure capable of managing different contents and making them available to authorized users".

[5] SCHMITT 1941.

As a basis for this alleged "anomia" of cyberspace, a parallel is usually placed between it and the sea, ascribing regulation exclusively to physical spaces, to the land. Thus, with this revival of the Schmittian distinction[6], the network is thought of as the place where "lovers of freedom and self-determination" reject "the authorities of distant, uninformed powers", as the world in which "all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat", as in a new civilization such as the "civilization of the Mind in Cyberspace"[7].

However, anyone who thinks in this way commits two errors: the first is that he does not know, or pretends not to know, what the principle of freedom of the seas was; the second is that the sea is no longer what it used to be.

The vision of the sea as a lawless reality derived from the circumstance that the sea was placed outside the Community of European States (*Comunitas Christianorum*) and its law (*jus publicum europaeum*). In this way, European states have been allowed to commit the worst atrocities, from the slave trade to piracy and private warfare. In this sense, it is correct to state that the fears and dangers of the high seas are the same as those encountered online and that the absence of rules does not mean absolute freedom at all, but rather a de facto condition and precarious.

If we delve deeper into the evolution of technologies, we immediately see that the sea, the airspace, and now also the space outside the Earth's atmosphere have all become spaces regulated and controlled by sovereign powers. The same happens with cyberspace which is itself a technological invention, that of a new space without a physical "where".

For jurists, entering new spaces, as before in the marine and aerial ones and now in the virtual one, constitutes a challenge, since legal science, although

---

[6] SCHMITT 1991, 2002, *passim*.

[7] BARLOW 1996.

created for the juridification of terrestrial relations and relationships, is perfectly capable of bringing the law everywhere, even in virtual spaces, as long as the law itself is supported by a sovereign power.

2. THE NET AS AN INFRASTRUCTURAL ASSET BELONGING TO THE STATES

The expression sovereignty indicates a power that is absolute and perpetual over a human group and over a territory, which lies on the ridge of the *Sein* and the *Sollen* and is in principle unifying. It is an effective power, therefore, which establishes a system and, more specifically, the sources of the law of a specific system, that is, a power that is capable of legitimizing itself on its own (because *superiorem non recognoscens*), of legitimizing every other power and to give validity to every rule. A power not in itself subordinated to respect for the legal system on which it is based and capable of authentically interpreting the law. A power that makes the order, towards the outside, independent and impenetrable. Finally, a power that can only limit itself, but which does not allow external interference or limitations.

What effects does sovereignty with its attributes have on the internet which is a virtual, aspatial reality and whose users do not qualify for their citizenship?

Apparently – as already said – this reality seems to escape the hypothesis that the internet can be traced back to the domain of sovereign subjects, but in reality, it is also the result of their political capacity, as well as of the technology that they are capable of developing.

After all, the Internet, however singular the phenomenon may appear, belongs to the group of "networks" which are technological structures created by States, according to the evolution of human needs and the results of scientific research.

Since its appearance, the State has been busy and concerned with building networks, regulating their use, and placing them under its control, because these networks are an important lever of its domination.

Originally, they were the consular roads, as the Romans taught, which had a precise military function: to keep Rome's enemies divided and intercept any attempt at an alliance between them. Subsequently, with pacification, the roads became a civil instrument of communication, and people and goods traveled on them and other network services developed, the main one being the postal service which allowed correspondence between men from different places. Of course, at the beginning at the speed of the horse, then at that of the internal combustion engine, and, when the mail abandoned the road, at the speed of the train, of ships, and of the plane, today also at that of the internet.

The objection that the Internet is a transnational network built in a decentralized way and by private individuals is not decisive. First of all, internet technologies do not only produce a polycentric system but also give rise to unprecedented forms of centralization, as emerges from the experiences of states that use the internet to implement forms of mass surveillance and distort the truth. It is not without significance, in this regard, to consider the strong presence of the political-military power of the States since its creation.

Secondly, the fact that the Internet is transnational is not a peculiarity that can remove it from the dominion of sovereign subjects, given that it is presided over by a specific international organization (International Telecommunication Union [ITU]), made up of States, within the framework of the United Nations. In this sense, the idea of the internet as a system without a center[8], which would make one think of the Middle Ages[9], rather than of a new world, must deal with unifying tendencies that also operate, and which make a world order possible, the result of international collaboration and characterized by a balance of powers.

In this sense, precisely, the internet is only one of the fruits of interstate collaboration and there are now various transnational networks, just think

[8] CASTELLS 2003.

[9] On this phenomenon RODOTÀ 2010; D'ANDREA 2002; VENANZONI 2020.

of gas and electricity, which obey geopolitical and economic logic. These networks, that is, by interconnecting improve the living and economic standards of the men who use them, but create an interdependence among States, which can be positive, because it induces them to behave peacefully and collaboratively, but also negative, because, regardless of the hypotheses of conflict, can create a dependence of some states on others, affecting their state of equality and independence.

Even in the case of the internet, therefore, there is a structural element that must be taken into account, to clarify the relationships that are established in the network and that branch out from it. As strange as it may seem, the 'virtual network' is equipped with an authentic "physicality", made up of cables that cross oceans, as well as continents, and which carry the signal everywhere, albeit still with large holes. It was the States who implemented this physicality of the network, which implies ownership of it and ownership entails the availability of the good. The network, therefore, belongs to the States, like any public service network, and this is even when private individuals participate in its construction or when prerogatives and privileges are granted to them over the network.

The fact that the Internet is multipolar does not prevent the State from carrying out sovereign acts on the Internet. Indeed, this is precisely one of the main problems to which virtual reality is exposed. Every network, even the most interconnected one, can be segmented, isolating the nodes of interest by an act of the prince and this decision cannot be questioned by anyone. Cases are known in which sites are blocked by governments and it has even happened that entire populations have been deprived of the use of the internet. However execrable such situations may be, due to the violation of the fundamental rights of those populations, all this can happen precisely because of the sovereign dominion over the network.

As for the fact that the network is implemented and updated (also) by private individuals, this method of intersection between public and private is typical of the action of States. Think of the train and the myth of the American frontier, fueled by strong private investments; an example that is also present in the history of other states, including Italy, where the

nationalization of the railways was intended to push private companies to build the electricity grid. Consider, furthermore, the development of radio and television broadcasts and the large global trusts that operate alongside thousands of small televisions (once called 'free'), which nevertheless always depend on the power of the States and are part of it, within the sphere of their dominion. The same goes for the internet, as a physical structure in itself, and for the platforms that operate on the network, just think of all the social media events, from Facebook to Yahoo, to Google, which have occupied tribunals and courts around the world.

Certainly, this digital sovereignty, like any form of power, is not a static fact, but a dynamic and continually evolving dimension that implies (power) struggles and permanent challenges.

3. THE INTERNET GOVERNANCE BETWEEN GENERAL AND PRIVATE INTERESTS

The directions of digital sovereignty do not differ from those of sovereignty *tout court*, as they imply a governance power of the network, on the one hand, over the operators (providers and platform managers) and, on the other, over the users (the people of the network) and, as a matter of principle, this power is not subject to external restrictions; indeed, on acts of internal sovereignty the other subjects who boast the quality of statehood should abstain from any form of interference, and this would allow sovereign power to be configured as absolute.

Actually, in the case of digital sovereignty, the historical reconstruction of state sovereignty does not appear sufficient, not only due to the peculiarities of the network, but above all because sovereignty, as such, no longer corresponds to the Westphalian stereotype; and the main reason for this derives from the emergence of Empires that interact with States, dominating the scenario of globalization and the network and making state

sovereignty porous[10]. In this sense, this would now have a relative and interdependent character and, in the case of the network, it would be forced to seek support from those who are more technologically advanced, hoping that in the meantime a structure could arise, the result of multilateral collaboration and under the international aegis of mutual control, capable of organizing the 'global cyber environment'.

However, this does not mean that the digital sovereignty of states is devoid of content; indeed, it has specific forms of expression and determined contents.

Concerning the forms, how a State exercises its power on the network is eminently given by legislation, which however must achieve specific administrative skills, especially supervision and sanctioning capacity, and justice including punitive power and compensation.

Nowadays, it is known that internet operators tend to dictate regulations that they impose on users to access services; furthermore, they have established their bodies responsible for the application of their regulations, which can sanction the violation of the respective regulations even with the suspension or exclusion of individuals from the network or platform.

What differentiates State legislation and its supervision and sanctioning activity from the regulation, supervision, and sanctioning of private actors in the network?

The most evident feature is given by the circumstance that only the legislation of the State is characterized by the chrism of legitimacy, while every other regulation is a *de facto* discipline and follows the form of private law unless it operates in a manner derived from the authority of the State (public concession).

There is, then, a difference in content between the legislation of the State and that of the private actors of the network. The virtual space was immediately filled with state legislation, with the existing legislation, which

[10] For a more accurate analysis of the pluralism of large spaces and new forms of politics, MANGIAMELI 2022.

has been interpretatively adapted to the network, or also referred to it, and with that, which the States have launched specifically for the network (think of the computer crimes or cyberbullying[11]). In any case, State legislation satisfies general interests linked to community life. Differently, the regulations of private operators who invest in the network mainly tend to preserve their economic position and their interests which may also have a political, as well as economic, character.
Finally, only public rules can guarantee rights to users, while private ones, culminating in the stipulation of a contract with a strong contractor, can easily sacrifice the rights of individuals in the name of the contractual code.

4. FORMS AND LIMITS OF THE TECHNICAL LEGISLATION OF PRIVATE NETWORK OPERATORS

Even the so-called technical legislation[12] which regulates access to the network and the carrying out of activities by private operators, in so far as it can be considered real legislation, as there are a series of agreements and international agencies which have linked the technical profiles of the global network and, in this context, states come before the various stakeholders. Over time there have also been changes that may suggest the opposite, such as the privatization of some government agencies (this is the case of the succession between IANA and ICAAN), but this never excludes the primacy of public power over private power.
Furthermore, the entire technological architecture that substantiates the '*lex* informatica' does not have a neutral character and this is why it always requires the protection of a political power that guarantees its role and function. In this, moreover, there is a perfect similarity with the '*lex*

[11] On the phenomenon of cyberbullying and its regulation see LODEVOLE 2023, 88 ss.
[12] For a broader reflection on the ability of platforms to regulate the architecture of the network see SANTANIELLO 2021.

mercatoria', which – using the internet itself – poses as an economic power that regulates legal relationships with consumers on its own. In truth, however, this capacity of the '*lex* mercatoria' still presupposes the protection of a political power that protects it, without which it would be torn to pieces as soon as the first consumer turns to his domestic judge.

It is also true that the relationships between public power and network actors[13], especially with providers and platforms, are extremely complicated by the circumstance that they would like to simulate, in the virtual world, forms and structures that are specific to state reality and this cannot be ruled out moreover, that their actions may have a political character; in this regard, it is sufficient to recall the alleged ethical character of their regulations and their supervision, or even their declarations of safeguarding human rights and democracy.

Yet in reality, it is precisely these who behave in violation of rights with forms of censorship towards ideas that do not conform to the so-called political correctness and of suspension or expulsion of individuals from the network, whose absolute freedom has always been proclaimed.

In this regard, Elon Musk's change of attitude, before and after the purchase of Twitter, is symptomatic. When negotiations were still underway, his statements were in favor of "absolute freedom of speech" as the "basis of the functioning of a democracy", asserting that the platform would be "the digital square in which vital issues are discussed for the future of humanity". However, immediately after the purchase, in order not to worry advertisers, Musk himself immediately changed his tone by declaring that the social network "cannot become a hellish landscape where you can say anything without consequences". Hence, the probable establishment of a system for reviewing 'tweets', to avoid hate speech and misinformation.

In short, we cannot forget that we are faced with economic operators of global importance, capable of having financial resources superior to those of many medium-sized states, who have accumulated an unimaginable

[13] For an analysis of which see more recently BETZU 2021.

quantity of information and data, through hidden profiling and forms of discreet surveillance, which allows them to exercise an influence on the needs and desires of individuals and their inclinations (including political ones)[14].

Now, that these great private powers pose themselves as defenders of human rights and democracy, requalifying themselves as great philanthropists, also guarantors of the environment, despite their servers being among the largest sources of pollution, appears to be a sort of an attitude that is in line with the "representation of organized interests"[15] and is, in this sense, something already known, even if the scale is now global.

The action of private powers has given rise to important services and continues to realize benefits for human groups or individuals. However, in actuality they have become the main problem that requires legislative intervention by the States, at least to make them pay taxes proportionate to the accumulated profits. Indeed, then, it can be said that their actions never reach the dimension proper to the guarantees of rights and democracy of public power and do not have the same capacity for intervention as the latter. The recent crises, the economic-financial one and the pandemic one, and now also the energy crisis, clearly show this difference; and it is also for this reason that, after years of glory, globalization itself has entered into crisis (there is now talk of deglobalization and selective re-globalization), and with it its instruments such as the *'lex* informatica' and the *'lex* mercatoria'.

5. THE GUARANTEE OF FUNDAMENTAL RIGHTS BETWEEN PUBLIC AND PRIVATE POWERS.

[14] On this topic see MICHETTI 2023.
[15] KAISER 1993, *passim*.

The legislation that network users invoke from public power is therefore based on this dominant position of private operators and the insufficiencies of their regulatory and governance claims. Technological development or the technological economy is no longer at stake in the network; the first is the almost exclusive prerogative of some great powers, such as China and the United States, and the second has consolidated great power at the head of small groups, placed at the top of the economic structures, ensuring them an unprecedented concentration of capital and strong control of the electronic market. Furthermore, fundamental rights and democracy are at stake in the network, so it cannot be accepted that the political structures at the top of governments have a position of power that threatens fundamental rights and allows the manipulation of democratic consensus, through the processing and monitoring of information, the orientation of the debate and, to a certain extent, the definition of the truth.

Hence the unavoidable request from the people of the internet, towards private operators and governments, for a new regulation of cyberspace according to a typically constitutional projection, that is, with reference to the protection of fundamental rights and democracy, as well as other European values (art. 2 TEU), which requires the free exercise of freedoms, the prohibition of manipulation of the truth, the overcoming of the state of surveillance and accumulation of data by private operators and governments and, above all, the prohibition of political use of data.

Can digital sovereignty achieve all this?

Respect for democratic rights and principles could certainly be implemented through multilevel legislation and/or multilateral agreements. In this way, we could formalize, if not a (global) Internet constitution, at least an Internet Bill of Rights[16], which, contrary to some claims, would not overwhelm the

[16] RODOTÀ 2010, 343: "The choice of the ancient formula of the Bill of Rights has symbolic strength, it highlights that we do not want to limit freedom online but, on the contrary, maintain the conditions so that it can continue to flourish. This is why «constitutional» guarantees are needed".

last trenches of state sovereignty, if ever it needed this to come true. However, the action of a single State can also be considered decisive for realizing internet rights.

In this sense, a projection of constitutionalism onto the internet poses, first of all, a question of regulation that moves entirely in the effectiveness of rights towards third parties (*Drittwirchung*)[17]; and such a request can be accepted, in the still absence of a 'global constitutionalism', only if the sovereignty that guides the state system is effectively permeated by the principles of the *rule of law*, in the most current and complete meaning of the term, for which the public apparatuses themselves are subject to respect for fundamental rights and these are constitutionally conformed in such a way as to be an instrument of protection against public power (*Abwehrrechte*).

In the States that accept these principles, legislation has very often given rise to 'digital citizenship', even if the set of faculties and claims that this expression can encompass is not always completely clear, but the right of access to the internet, the right to digital education, the right to electronic democratic participation, etc., would fit in.

It is obvious that, where the State does not follow the form of the *rule of law* and does not recognize fundamental rights, this will lead to the development of a form of 'cyber dominion', concerning the network, both in the relationship between the user and private powers and in that between citizen and state. In the first case the intervention of the political power towards the private operators of the network can always be given, but not to defend the rights of users, but above all to exercise greater control over the network and the private operators themselves through a state censorship, imposed in the name of 'national security' (in this regard, one can recall the conflict between Google and the Republic of China in 2010).

As for the relationship between citizen and state, if this is not based on the principles of constitutionalism, it takes on an authoritarian character in

[17] On the horizontal effectiveness of rights, see the careful study LOMBARDI 1970, *passim*.

which the network can be subjected as a means of domination and social control.

Furthermore, phenomena of this kind, that is, of 'cyber dominion', have also occurred in Western democracies. Think of Edward Snowden's denunciation of mass surveillance and compromise by the NSA in 2013 in a context in which the fight against terrorism and the preservation of national security could not justify these illicit activities, toward American citizens and, equally, towards Allied states. In this case, the existence of free information (online and otherwise) and of a structured civil society with a strong presence of associations acting in defense of rights have brought the violation of fundamental rights by of the US government to the attention of public opinion. This makes us understand how powerful digital sovereignty is and, how even in the otherness between rulers and governed democracies, the desire to privatize public power can lurk.

6. CYBERSECURITY AS THE FIRST CONSTITUENT ELEMENT OF DIGITAL SOVEREIGNTY

"Cyberspace has become strategically indispensable"[18] and states cannot give it up. States have understood that they cannot fail to master network technologies in one way or another if they still want to retain the definition of state authorities.

Consequently, the first element of digital sovereignty is given by the ability to organize cyberattacks and defend oneself from these, knowing full well that aggressive activities through the network, capable of threatening and destroying the infrastructures of a community (think of the Stuxnet case towards Iran), have on their side both the technical anonymity[19] of such actions and the lack of an international sanctioning system.

[18] KISSINGER 2015.

[19] On this topic CIPOLLONI 2023.

The need for a public cybersecurity function[20] arises from the need to protect the digital activities that now innervate every State, in civil policies as well as in those of a military nature, to ensure its institutional functioning and, at the same time, safeguard data, protection-sensitive citizens.

Security presupposes the State's technological development, capable of freeing it from international conditioning that can derive from both political and private external forces.

This substantiates a further task of true digital sovereignty which necessarily requires, within the State budget, a substantial investment of public resources in digital infrastructures, to protect the State itself understood as an 'independent platform' at the service of its community that collects the 'digital identities' of its citizens. In this sense, the State should go as far as to build a 'national and sovereign cloud', capable of requiring the payment of all information concerning its citizens even if allocated on foreign servers, and of imposing public control on the platforms[21].

7. ON THE NEED FOR INTERNATIONAL REGULATION OF THE INTERNET THROUGH A CYBERSPACE TREATY

[20] SARACENI 2023, 98: "Cybersecurity can be considered as the clearest and at the same time problematic aspect of the era in which we are living; due to the widespread diffusion of the web, computers, and smart mobs, we find ourselves immersed in a dense information network daily; we entrust IT tools (...) with our sensitive data, our investments, our savings, our secrets".

[21] COSTANZO 2021 adds: "In short, it is necessary, for its stability, that the State also becomes a protagonist in cyberspace, not only from a legal point of view but also from a technical one, if necessary, through powerful investments in the creation of infrastructures digital services at the service of its functions, to achieve its goals and for its conservation (the establishment of the National Cybersecurity Agency a few days ago seems to be going in this latter direction)".

The sovereignties, in the historical conception of their plurality, all lived within a general framework given by the Community and international law, but each one was very distinct from the others, thanks to territorial borders and the principle of non-interference in 'internal affairs'. Even before the advent of the internet, this was no longer the case. Not only has international trade conveyed a strong interdependence between states, and increasingly internal affairs have taken on international importance, so that domestic law and international law increasingly appear to be two aspects of a single normative problem, going beyond the line of what is internal and what is external.

In the case of the network and digital sovereignty, this condition has an even more evident projection due to the interdependencies that technology has imposed. States use the internet to carry out new forms of economic, political, and military espionage, and to carry out actual attacks on their adversaries. The statement that "the next war will begin in cyberspace"[22] is not without foundation and in any case, technology certainly already now allows for cyber warfare which has an important role alongside conventional weapons, with the advantage that it is not easy to implement forms of retaliation against cyberattacks.

Cyberwarfare proves to be a threat perhaps no greater than the deterrence of nuclear weapons, which is however capable of giving rise to an equally dangerous escalation of geopolitical tensions, to the point of arriving at a situation of continuous conflict that threatens the lives of individuals and forms in their governments a combination of permanent insecurity and intentions to assert themselves, to ensure supremacy in cyberspace.

The use of technologies in relations between states therefore raises the problem of international relations in the digital age. The ambivalence of the network is also projected into relations between states: it can act as a vehicle to undermine and even overthrow authoritarian governments, and demand rights and more democracy, but it can open up unprecedented repressive

[22] HUGHES 2010.

possibilities, its use in itself does not ensure that the values of a free, orderly and truth-based coexistence prevail.

In the so-called digital diplomacy, what is felt is the lack of limits to which states, including great powers, abide, to create a shared balance without giving in to the temptation to act to test the limits themselves.

Various attempts have been made to promote international regulation of the Internet, some coming from the States themselves and looking to the United Nations. Precisely on the initiative of the Secretary-General, based on point 72 of the Tunis Agenda, in 2006, the call came to establish the Internet Governance Forum as a global multi-stakeholder platform that facilitates the discussion of public policy issues relating to the Internet, but without decision-making powers.

In 2019, the *Contract for the Web* was formulated, with nine principles addressed to governments, companies, and individuals, by the Web Foundation and in which some governments were interested (in addition to that of the United States, France, and Germany), important trusts such as Pango (Anchor Free), Microsoft and Google and several civil society associations.

All this is still too little. To define an international internet regime that has a binding character, a Cyberspace Treaty appears necessary, which recomposes the digital sovereignties of the States, limits virtual conflict, and allows them to manage the internet together, in a transparent way and according to a shared discipline.

REFERENCES

BARLOW, John P., *A Declaration of the Independence of Cyberspace*, Davos, 1996.

BERTOLA, Vittorio, *La sovranità digitale e il futuro di Internet*, 39-47, in *Riv. it. inf. dir.*, 1/2022.

CASTELLS, Manuel, *Volgere di millennio*, trad. it. , Milan 2003.

CIPOLLONI, Claudia, *The right to anonymity. Overview of the institute and analysis of its evolution in the age of the web revolution*, in *Human(ties) and Rights*, 5, 3/2023.

COSTANZO, Pasquale, *Lo "Stato digitale": considerazioni introduttive*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Genova, 2021 (https://www.gruppodipisa.it/images/convegni/2021_Convegno_Genova/Pasquale_Costanzo_-_Relazione_introduttiva.pdf).

D'ANDREA, Dimitri, *Oltre la sovranità. Lo spazio politico europeo tra post-modernità e nuovo medioevo*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, 31, 1/2002.

HUGHES, Rex, *A Treaty for cyberspace*, 523-541, in *International Affairs*, 2/2010.

KAISER, Joseph H., *La rappresentanza degli interessi organizzati*, trad. it., Milan, 1993.

KISSINGER, Henry, *Ordine mondiale*, Milan, 2015.

LODEVOLE, Luisa, *Cyberbullismo* (entry), in AMATO MANGIAMELI, Agata Cecilia, SARACENI, Guido, *Cento e una voce di informatica giuridica*, Turin, 2023.

MANGIAMELI, Stelio, *Empires and States and the new International Relations*, in *Humanities and Rights global network journal,* 4, 2/2022.

MICHETTI, Michela, *Surveillance and technological (R)evolution. implications and repercussions on human rights*, in *Human(ties) and Rights*, 5, 3/2023.

RODOTÀ, Stefano, *Una Costituzione per Internet?*, 337-351, in *Politica del diritto*, 3/2010.

SALVATORI, Roberto, *Piattaforma* (entry), in AMATO MANGIAMELI, Agata Cecilia, SARACENI, Guido, *Cento e una voce di informatica giuridica*, Turin, 2023.

SARACENI, Guido, *Cybersecurity* (entry), in AMATO MANGIAMELI, Agata Cecilia, SARACENI, Guido, *Cento e una voce di informatica giuridica*, Turin, 2023.

SCHMITT, Carl, *L'ordinamento dei grandi spazi*, trad. it., 101-198, in *Stato Grande Spazio Nomos*, Milan, 2015.

– *Il Nomos della Terra*, trad. it., Milan, 1991.

– *Terra e mare. Una riflessione sulla storia del mondo,* trad. it., Milan, 2002.

VENANZONI, Andrea, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in *media Laws*, 3/2020.