International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, 2020
ISSN: 1475-7192

The Sovereignty of Cyberspace

[1]Dr. Omar Mahmoud Omar, [2]Dr. Ma'en Juwaihan

Abstract:

The creation of a virtual world parallel to the material world created a kind of competition for sovereignty, which promoted the idea of a transition to coexistence in these sovereign centers, away from chaos and violence. Recognition of this diversity of sovereignty would lead to the existence of competing forces but in a peaceful and homogeneous manner. The international nature of digital conflicts is certainly a source of difficulty in defining applicable law and jurisdiction. cyberspace has made national boundaries transparent, because inter-network overlaps have made the boundaries intangible. So, it is not surprising that the state loses its legitimacy when it comes to regulatory matters. The contradiction between the geographical and territorial boundaries of national laws and the universality of the Internet led to the loss of the state part of its sovereignty in the area of cyberspace. Limits are not a fixed and unchanging chapter, but they are evolving in place and time and are losing their importance in many areas. Globalization and the existence of a networked world have contributed to building areas where it is difficult to set boundaries accurately.

Key words: *Sovereignty, cyberspace, information sovereignty, virtual sovereignty.*

I. Introduction:

Sovereignty is originally a French idea in emerged in Middle Ages [0], as it was used to indicate to the superiority authority over another, and to define an authority that does not subject to any other authorities and does not acknowledge any superior authority[0]. On other hand, territory represents the space protected and secured by the State. The boundaries were made and defined, in addition to creating territorial space, which the State impose its legislative, executive and judicial authorities, to define the space of State Sovereignty.

The national territory defines the context where the State Law is systematically applicable, the national juridical authorities shall consider all Cybercrimes of this territory, Irrespective of perpetrators of victims. Accordingly, the boundaries are a legal fact that constitutes the borderlines of other competences in which the State practices its jurisdiction.

The uniqueness of Cyberspace [0] is represented in the fact that it cannot contained by any State through imposing its monopoly and sole sovereignty and it became a symbol of exceeding boundaries, which will lead to a path

[1] Faculty of Law, University Of Petra, Jordan
[2] Faculty of Law, University Of Petra, Jordan

Received: 15 Jan 2020 | Revised: 5 Feb 2020| Accepted: 30 Mar 2020

that shall harm humanity. The doubt that surrounds Cyberspace as a mere material space, such as earth, air and sea, led to new disputes over the hegemony and sovereignty of it(). According to the aforementioned, two approaches are presented: The first approach describes the Cyberspace as extrajudicial area. On the other hand, the second approach states otherwise that cyberspace, when it was created, was not subject to law, but currently, its area shall be subject to law.[0].

Ignoring limits by Cyberspace, makes it difficult to impose national legal rules to control it, as a result of the contradiction between geographical boundaries as well as the territoriality of the national laws, and the universality of the Internet. This led the nation to lose part of its sovereignty as the Internet may be considered to be an area without boundaries nor laws().

In the field of Virtual law, the efforts of various States are combined and integrated, which imposes the question about the nature of the relations of those who are involved in the communications community, and this makes it inevitable for States to give up part of its sovereignty in return for who controls servers. Besides the web users, resorting to mere concepts or general principles with unstable content, because it is in constant movement and this is the very evidence for the hierarchical roles played by each user. Through the online world, there are those who claim that the user is the sovereign entity in virtual space, and on the other hand, there are those who claim that the sovereignty is represented in the web itself. As the rate of the web users is estimated at 30-40% of the Earth ().

Currently, the concept of State sovereignty began to be interpreted in the light of relativity. Globalization has reviewed and redefined this concept and other key concepts of political science, international public law, and constitutional law. As the economic and customs boundaries defined by globalization became incompatible with the political borders that the traditional concept of sovereignty is based on. (). In fact, international law evolves correspondingly with States evolution, but it does not keep the same pace with this evolution, for instance States prohibit espionage within their borders under domestic laws, but international law does not prohibit espionage(). Regardless, no one can deny leading role of the State in the field of Information, which is a significant element to operate many of the political activities and practices related to this information. The state is the important pivot in defining the reasonable risks or people identity, the contractual practices and the information flow, but it is unable to impose its unilateral authority on cyberspace.

The State sovereignty over the infrastructure and electronic activities within the cyberspace has two main consequences so that the state may issue and apply its local laws and regulations to its own cyberspace, furthermore, sovereignty gives the State a right under international law to protect cyber-infrastructure and protect cyber-activity presented in its territory or that happens in its.()

This study is divided into two chapters, the first revolves around the Modern Concept of National Sovereignty over Cyberspace, and the second discusses the concept of the multiplicity of sovereignty over Cyberspace.

Modern Concept for National Sovereignty over Cyberspace

The concept of sovereignty and equality between states is one of the basic rules in public international law. The first paragraph of Article Two in United Nations Charter, stipulated that the organization is based on the principle of equal sovereignty of all States.

It is definite that the State authority shall not be marginalized by the other interventions that affect the concept of traditional or symbolic sovereignty, but theoretically, that may seriously undermine its authority by facing a competing sovereignty that claims to be a substitute for its authority in certain territories. The state will face a competition over sovereignty in multiple matters such as international trade and finance; human rights, electronic environments, international trade practices and the acting authority in cyberspace.

This chapter will be divided into two topics in which the first topic discusses the modern approaches for the sovereignty of cyberspace while the second discusses the elaboration of the "Sovereignty of Cyberspace" concept.

1.1 Modern approaches for Sovereignty over Cyberspace

The boundaries lost its significance at the current time as the boundaries are not separated and fixed but rather evolve over time and space. Globalization has contributed to the establishment of a domain linked to the web and the construction of spaces that are difficult to define precisely.

"Cyberspace" has become a space for data exchange and storage, using electronic technologies that include the Internet, communication networks and computer systems that can be accessed everywhere in the world, a symbol of exceeding boundaries(). In fact, if sovereignty concept is limited to specific physical spaces, the Internet, as a virtual space, connects all territories. In addition, the digital technologies are designed by circulating Streaming media and non-physical data. The cyberspace information is in constant motion, while imposing sovereignty of the State requires the existence of clearly defined territorial spaces and therefore, the state can claim sovereignty only if it is able to control all its information activities, within its territory and outside its borders().

The territorial sovereignty cannot be easily applied to the Virtual Globe field. Therefore, it is necessary to give a new concept to this territorial sovereignty by changing the name from "Territorial Sovereignty" to "International, Universal or Digital Information Sovereignty".

The "Universal Information Sovereignty", otherwise "Territorial Sovereignty", means the ability of the State to develop a new system able to deals with virtual activities and able to control virtual liability, which means providing a new virtual sovereignty. It also means the right to limit or subject the virtual activities to some conditions in terms of transmitting and transferring them across other States. Under this sovereignty, the State can claim it, when it has the ability to control the ongoing activities in its territory and abroad, on its claim that these activities affect its interests, this is called the external controller(). This is not unprecedented idea as it is applicable to civil and penal laws, international private law and criminal law. So that the State can, by its information technology, detect the related information which is followed up before transferring it across communication satellites and before breaching the its information space. Therefore, the state could make a virtual wall or filters to defend against all of the above so that the information cannot pass without promoting the access across this filters or wall. This called the "Firewall" in China. ().

According to the nature of cyberspace, the concepts of sovereignty contradict from a State to another, and determining the scope of sovereignty over cyberspace is a political issue rather than a legal issue(). It should be noted that the value of information in the decision-making process is essential for the State, since the information sovereignty is an expression of State central authority. It must control the export of information that appears crucial for discharging its duties of the public authority. Maintaining State control over its information and not exposing it, are within the concept of information sovereignty(). These information is of prominent strategic importance in the implementation of State policies. This control seems unrealistic with regard to the electronic web, such control can be envisaged when main acting authorities are still Limited, for electronic environments, to large multinational companies. However, the concept of information sovereignty seems to be outdated in the light of new electronic environments(). The practice of information sovereignty is not easy, especially with no access and transference of information, besides the encryption and anonymization techniques, above all, the ever-increasing number of the information users by quick ways, practically, they are opposed to any attempt to place them under control(). Practically, in all cases, the State cannot prevent the dissemination of information and data about it. One of the most important characteristics of cyberspace is that it covers all electronic Communications satellite. It cannot be limited by any physical geo-territorial borders, meaning that the nature of virtual space contradicts limiting it within a certain scope of miles or kilometers, such as the borders of territorial or international waters. The state that is a victim of an electronic crime (Often the perpetrator is outside the State or may be inside it but anonymous), When the State claims, under its domestic law, its right after a crime, its claim is shortly considered ineffective. When the information sent from the territory of the State, it cannot impose its control and sovereignty over the sent information through the world wide web which contradicts such territorial sovereignty.

The relationship among the state, citizens, companies and consumers shape a new network of the sovereignty and a new area with indefinite rules. In this environment there are many areas of sovereignty: The first: the personal information which give the citizen the right to provide these information besides having the right to assign it and to entrusted it to other partners() in addition to the information transferred by the citizen to the State and some administrations. The main mission of the first area represented in the State role in protecting the citizens' confidentiality and their information. While the second area involves companies and organizations sovereignty, through data which are the main resource of companies. While the third and the last area, which discusses the sovereignty of the States to face Internet Giants, raises the debate on data protection within territorial organizations, such as European Union to face US domination().

1.2 The elaboration of the "Sovereignty of Cyberspace" concept.

The Territorial Airspace Sovereignty is no longer an effective term due to the breach of boundaries through these signals and radio waves, which necessitated the issuance of international air law for communications in addition to the air navigation lawn, to protect this use by all. Therefore, the concept of human joint liability replaces personal individual liability for either States or normal people.

States has the right to exercise its sovereignty and impose their laws on its own land through its means, but States do not always have the means to guarantee compliance with their own laws within their borders, even when

States require Internet service providers to prevent illegal sites from reaching their lands, and they are ordered to block unwanted sites, as the implementation of such measures is time consuming, expensive and may be ineffective.

Internet sovereignty is related to all competences sectors and fields of the European Union in all its forms: Digital sovereignty, information sovereignty, citizens individual sovereignty, cloud sovereignty... Currently, the features of sovereignty concept tremble due to instability and constant development of the web(). While the European Union works on improving its policy to protect data, another authority write special rules to govern cyberspace. The fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union, and citizens' data protection inside and outside European territories, do not allow the transference of personal data outside the European Union, unless the European Union considers the receiving State is "appropriate" for that(). The United States dominance on the Internet technically, economically, or politically pushes Europe to support its role by defining new skills, privileges and values to face the States and giant companies, which renews the urgent need to establish and define an international framework for sovereignty.

The data continue to evolve, as the new market value for the Internet and the spread of services across the Internet increase the division of the cyberspace, thus raises questions around Internet neutrality(). In contrast, online Economists have a vested interest in maintaining and developing an open and interoperable environment and expanding their business activities. Internet fragmentation as a result of the conflict among the sovereignty aspirations of the States, acting authorities, Corporations and citizens is considered a punishment for all actors. The idea of developing a sovereign operating system is interesting, but it is not viable due to a number of obstacles that await its implementation: Sovereign Encryption tools, that aim to protect citizens' and corporations'' data by encrypting messages and data, and the state is the only owner of it, however, these tools often have harmful effects()

Article 8/3 of the Directive 2001/80/EC of the European Parliament, stated three techniques for the Member States, to act accordingly, to protect their national sites by banning the "Uniform Resource Locator"(URL), "Internet Protocol" (IP) or by blocking the domain name ("Domain Name System" or "DNS")[0].

The law was generally proven insufficient to ensure the nation ability to face attacks and extend the sovereignty of other States because the measures taken against cyberspace is of a technical nature rather than legal. As the States wish to restore its independence and develop its own digital network to ensure a secure information system in the State. China, Russia, and Iran opt for restricted and controlled "Cyberspace", which maps the fragmentation features of cyberspace, hardware, software and information fragmentation into several isolated regions.(). Some opt for the need to implement something similar to a social contract between states regarding the Sovereignty of Cyberspace (). Another opinion objects the expansion in implementing the traditional concept of "Sovereignty of Cyberspace" in a way that oppose the nature of Internet use().

Economic integration, whether it is territorial as in the European Union or the International Free Trade Agreement or North American Countries Free Trade Agreement, cannot reduce the legal intervention of States as in the case of the World Trade Organization. Likewise, the national financial markets which are almost independent, create "external markets" which are places outside the jurisdiction of the States(), where deal emerges outside the

territorial borders, and everything that happens during trade exchanges is only an exchange of authorities. Therefore sovereignty became mobile and no longer have a physical location(). the protection of environment, human rights, indigenous people rights, shared strategies and goals are interstate activities and at the same time, they are considered national for all States.

The possibility of applying national law outside the borders of the state is tantamount to ignoring the sovereignty of other States. Beyond technical difficulties, technical measures and blocking foreign sites on national territory may have an impact on the sovereignty of other States. In the dispute between Germany and the American company "CompuServe"، the judiciary has ordered that forums should not be accessible on German territory based on German law that prohibits its contents.

This decision prevented 4 million CompuServe subscribers from accessing 140 locations in 140 States[0]. In another case, the Court of First Instance in Paris has claimed the American company "Yahoo" to set up a purification system to identify the French Internet users identity to prevent them from access to the sales site by auction of Nazi symbols[0]. Yahoo company, on the other hand, considered that the foreign jurisdiction could not interfere with its servers in the United States, and that forced action against it could not lead to anywhere, because it contradicted the First Amendment to the U.S. Constitution, which guarantees freedom of expression to every citizen. This shows that the application of national law beyond borders and when it applies to all users of the web located in other regions can give the State additional authority in the scope of its sovereignty, which may enter it into competition with the forces of other countries.[0].

There may be other violations of State sovereignty in international criminal investigations. States may generally be claimed to send the login data to determine the perpetrator of an online dispute, related to Internet, within their territory to foreign legal authorities. To access this technical information from ISPs, prior approval shall be provided by the state that maintains the contact information.[0]. According to the ruling of Permanent Court of International Justice in the Lotus case, the ruling stipulated that any exercise of State authority could not be exercised outside its territory unless there is a rule that would otherwise allow, pursuant to customary international law or the Convention[0].

Theoretically, only seven states allow access to contact information to foreign authorities: Finland, Portugal, Poland, Chile, Montenegro, Japan and the United States. On the other hand, unapproved entry is no longer permitted by nine states: Czech Republic, Lithuania, Germany, Sweden, Turkey, Bosnia and Herzegovina, Hungary, Estonia and the Netherlands[0]. In practice, despite the obligation to obtain the consent of the concerned State, foreign authorities often gain access to information stored abroad through cooperation with private companies, without any request for legal aid from the State in which this information is located. The ICC has revealed that many companies are under strong pressure from foreign governments to obtain contact information, while such access is not permitted in their State legislation[0]. Many States undermine the national sovereignty of other States, in the context of international investigations to eliminate computer crimes.

Many of the "Great powers" or "Great States" that dominate the Internet, do not recognize the existence of sovereignty over cyberspace, but in practice most States exercise their sovereignty objectively over cyberspace because it is inconceivable that there is a State that allows its cyberspace without sovereignty.[0].

In fact, it is not possible to talk at this time about the sovereignty of States over cyberspace because some of the main components of the Internet are managed outside the international legal framework by [0](ICANN) and with the authorization of the U.S. government since 1988, and this company has the responsibility of managing and distributing Websites names and domain addresses on the Internet, including "International Numbers", which is a private company subject to California law, and it is known that USA has control over the Internet. Sovereign states should submit their applications to the ICANN in order to participate in creating the internet protocols, which are crucial for the operation of local national networks. For this reason, the World Summit on the Information Society WSIS in Geneva in 2003 and Tunisia in 2005 called for broad participation in internet governance and management. The European Union and China have laid a participation claim to the United States, but this claim has been rejected.

II. The multiplicity of Sovereignty scopes over Cyberspace

The creation of a virtual globe parallel to the physical world created a kind of competition for sovereignty that reinforced the idea led to the study of coexistence in these sovereign centers, away from chaos and violence and the recognition of that sovereignty diversity would create a peaceful and harmonious deployment of competing authorities. The result is a greater democracy; an issue that should not suffer from the claims of the dominant state.

The authority of the State to control its borders and impose its laws on its territory, is diminishing with the emergence of new electronic communication channels. Therefore, the implications of information technology for the national sovereignty concept must be studied. Information technology is a factor among others that explain the slow declination of the national sovereignty concept. Then it will be logically not to talk about sovereignty, but the multiplicity of sovereignty.

This chapter will be studied through two topics, the first studies the hardness of exercising sovereignty over cyberspace by State and the second is studies the shared sovereignty concept.

2.1 The hardness of exercising sovereignty over cyberspace by State

The Concept of Sovereignty is discussed widely, where sovereignty has been defined as the fundamental features of the State that allow it to directly influence the social, economic and cultural policies of a particular group. But in the same time, the State has recognized its sovereignty limits imposed by international law.

Respect the territorial sovereignty for the International Court of Justice is a prerequisite for relations between States and the mere connection of the State infrastructure to the web of Cyberspace, cannot be considered as a waiver of its sovereignty.[0]. States are free to exercise their sovereignty and impose their laws on their national territory, but States do not always have the means to ensure compliance with their own laws within their borders.

The international nature of digital conflicts() is certainly a difficult source in determining applicable law and the competent jurisdiction, but otherwise to control cyberspace, States use national and international law to punish cybercrime perpetrators. As cyberspace defies physical boundaries, its users are real and all are located on state territory. Despite the phenomena of illegal abstraction and porous boundaries generated by the globalization of networks, the territory concept is still a standard in the law. Therefore, It is necessary to take into account not only the conflict parties who are the perpetrator and the target of the attack on the computer or the State representative, but also the location of the conflict on networks whether within and outside the borders of the state().

The ruling of the case on 14 Oct 2011, by the Court of first instance in Paris, Copwatch located in the US, which condemn police violence by posting personal data to them (Names, IP addresses, Phone numbers and photos), was banned by internet service providers(). A year later, a similar copy of Copwatch was posted on Mirror Websites. In a new legal procedure, the court decided to ban it from all sites inside the French country. However, experts said that the necessary time to carry out these technical measures will be from six months to one year and It represents an initial investment of approximately €10 million per operator.

In a resolution issued on 28 November 2013, The Paris Court ordered five Internet service providers to block Allostreaming websites and three search engines (Google, Microsoft, Yahoo) to stop the illegal presentation of films or series for French Internet users(), Here again, Internet service providers have indicated that targeted sites will circumvent these provisions. In this regard, the does not fail but the State does not have the ability to exercise its full sovereignty on its lands and ensure the effectiveness of judicial decisions when servers and data are located abroad().

We should put in mind the fact that Internet "is a web of switching packets, which make it difficult for anyone or even the government to prevent or control the flow of information from users' origin". The Internet is one of the webs that connect millions of users around the world. the decentralized nature of the web is another example of difficulties in controlling the information circulating through it. The technology of "Packet" practically makes it impossible to detect millions of accessible data on networks that may violate national legislations(). AS proxy and VPN allows the access to the Internet and browsing, although these sites are blocked in the user's country.

In the field of Virtual law, the efforts of various States are combined and overlapping, where the need for the question of the relations nature of those who are involved in the communications society, and this makes it imperative for countries to give up part of its sovereignty to who controls links, besides the web users and resorting to concepts or general principles with unstable content, because it is in constant movement which proves the varied role played by each user. Through Internet, there are who claimed that the user is the Sovereign entity in the virtual space () Therefore, the seek to digital sovereignty, represents a joint target for companies and public authorities, Internet users, citizens and consumers().

Indeed, the war on data sovereignty in France has already begun; in 2009, the government funded two sovereign cloud projects. The goal was to provide French companies and management with information technology infrastructure capable of hosting data and applications and access to them remotely securely(). The war on Digital

Received: 15 Jan 2020 | Revised: 5 Feb 2020| Accepted: 30 Mar 2020

sovereignty is also ideological and cultural, as the European Digital Library was created as a reaction to the success of Google Books[0].

In view of the Steadily grow of economic weight of GAFAs (Google, Apple, Facebook, and Amazon), economic dependence and a massive transfer of value are increasing the imbalance that forces public authorities and economic acting authorities to implement regulatory tools compatible and equal to the freedom space provided by Internet[0].

States want to confirm and impose their rules on cyberspace and to have a political, technical, and legal framework. But to what extent national intervention can be Legitimized and excused, driven by recent skepticism about the superiority of the United States on Internet. The ideal situation for free, open and accessible cyberspace is deteriorating, not only because of the political and economic tensions that pass it, but also because of the many regimes that are imposed on it.

The Internet covers a complicated reality and multiple and often contradictory dynamics of fragmentation and openness, which occur at different physical or legal levels of the web. Hence, the difficulty is for the state to impose its sovereignty on political and commercial issues. In the face of distrust between users and consumers, companies are therefore committed to five ethical practices, including implementing datagrams, to meet new requirements for confidentiality, transparency, assistance and security in data processing. This ethical data processing represents the issue of sovereignty that requires the establishment of an appropriate legal framework, as it established through the development of European laws, which are already among the best security laws in the world on these issues[0].

2.2 Joint Sovereignty

The role of the State today is more important than that of sovereignty in feudal eras. Modernity has established long-standing connections and structures that have an impact on making the state an essential component, in many territories, which cannot be avoided. For example, the State competes for sovereignty in areas such as international trade, financing, human rights and electronic environments, among others. However, the state still enjoys sovereignty and the full meaning of this term in various sectors such as defense and foreign affairs, and the conclusion of treaties and conventions.

In these sectors, the States are divided into two groups who are the controller of the system, and in other territories that are beginning to retract their strength, the State can try to intervene directly. But, it will face strong resistance from competing sovereigns, as well as from other states. For example, the state's desire to require everyone to comply with its standards of free expression on the Internet. The Internet is a reflection of these external and multiple goals[0]. However, the Internet can appear as a mirror to these goals because of the unique nature of this medium. Creating a virtual world parallel to the physical world in a cross-border context is a unique phenomenon in which participants have already begun to develop their own rules similar to national legislators[0]. This competition cannot fail to increase freedom for individuals and intermediaries when they share in authority or its spread in many sovereign centers, while acknowledging the importance of the symbol of State sovereignty in an international system that strengthens those who are concerned about the seizure of authority by one party This distribution of authority is a certain democratic safeguard. Another effect of this competition is the acknowledgment of the legitimacy of

international legal pluralism. It has already been proven that the state or states do not have a monopoly alone on setting special standards on cyberspace, which confirms the idea of coexistence of these sovereign centers().

Beyond the chaos and violence often associated with the concept of domination, concurrent authority can be exercised, and it is already exercised practicality through a relative harmony. However, friction points are expected to occur in light of the attempts made by the state to assert its sovereignty over cyberspace().

Realizing this diversity in sovereignty, it is now necessary to seek to devise models for the peaceful and harmonious deployment of competing authorities. The result is a greater democracy; an issue that should not suffer from the claims of the dominant state. This greatest freedom definitely has a price: That is represented in a less security into cyberspace and the user does not benefit from the citizens' similar protection. Absolutely, there is a priority to protect the State, public order, and competing interests against freedom of expression, in addition, all the values that, sometimes, the State desperately defends, may prevail in the physical world. Therefore, this security appears to be fundamentally ethical: Protecting an individual against a specific content is considered offensive by a particular community().

In cyberspace, there is no place for prohibitions of a mandatory nature found in national laws or even in international conventions. It is important to replace this security model with another type of model. The only way is to use countermeasures for drastic approaches, as military ones or other divisive approaches to ensure a plurality of opinions for Internet users(). The freedom of this competition can be beneficial because it allows the individual to know pluralism without having to submit to the policies of an only normative authority because it is no longer possible to limit the concept of sovereignty by a purely spatial perspective().

Regarding national sovereignty, it is important to note that the new electronic communication channels are just one of the many stress factors. Because electronic communication networks do not care about the traditional national borders, and do not fit in with them.

Finally, if sovereignty is understood as the right to exercise, or exclude any other state, or its privileges over its territory, then it implies a duty to protect the territory of other states by virtue of the principle of equality, and respect for the principle of state sovereignty set out in article 2\1 of the Charter of the United Nations.

In international law, "no State has the right to use or permit the use of its territory in such a manner as to cause harm in or to the territory of another State"(). In the Corfu Channel case, the International Court of Justice stated that every State has an obligation "Not to allow its territory to be used for acts incompatible with the rights of other States"(). According to the Tallinn Manual, there is an obligation of the State which is the responsibility to prevent illegal acts in the cyberspace in its territory, and that cause severe damage to people or property, whether on its territory or any territory of another State(). However, the application of the duty of prevention in cyberspace must take into account the true ability of States to control the infrastructure that is located in their territory. But these businesses are often run by private companies, which are not always under the control of the States.

Received: 15 Jan 2020 | Revised: 5 Feb 2020| Accepted: 30 Mar 2020

III. Conclusion

Nowadays, the concept of traditional sovereignty is no longer valid with regard to controlling cyberspace, and today, it is time to realize the multiplicity of sovereignty. In this regard, Internet expands this phenomenon due to the virtual world that it supports as a world that is different, complicated, and distinguished from the real world. As there are cases that are get out of the national control or even the international control resulting from user actions. which requires the division of authority regarding cyberspace and introducing the concept of "Multiplicity of Sovereignty" and relationships among these different and competing authorities.

Digital sovereignty must be understood in a different sense than actual sovereignty, which refers to the ability of a particular entity, state, company or individual to control the digital features of this new and virtual space (data, information and knowledge...etc.) The principles that apply to space should be a barrier to prevent dangers that might contribute to the risk of a State claiming the sovereignty through using it.

It is certain that the state will not simply disappear, but we should realize that some sectors of human activity have got out of the government control. It is ludicrous to think that the emergence of the Internet, has denied the ability of states to intervene in electronic activities. There are almost daily examples of States having a great deal of control over online activities. But the role of the state and its nature and scope, depends on the mechanism of co-existence with the interventions of competing authorities.

Recommendations:

- The territorial sovereignty of States over cyberspace should be regarded as a joint liability or a joint heritage of whole humanity. The organization of these activities must reflect global solidarity that goes beyond the framework of State sovereignty, not limited to its inventor or funder.
- Working on Strengthening international solidarity instead of the national solidarity, and the use of such space, should be in the interest of everyone.
- Setting new concepts for principle of the sovereignty for the reconsideration of territorial and physical space standards as the concept pivots of national sovereignty.
- The Arab States should work as soon as possible to conclude a special convention for the protection of cyberspace which has currently become one of the most important pillars of the establishment and provision of the proper conditions for comprehensive development based on safe circulation and Provide useful information using cyberspace and information technology as crossing point, a means and a porter for this vast amount of information.

REFERENCES

1. Al-Essa, Talal, (2010) Sovereignty between its traditional and contemporary concept, "A study of the internationalization of sovereignty in the contemporary era" Al Syada bayn Mafhomha Al Taqlidy Wal

Mo'sir "Drasa fi Mada Tadweel Alsyada fi Al A'sr Alhader", Damascus University Journal of Economic and Legal Sciences, 26 (1), p. 54.

2. Draft Arab Convention for the Protection of Cyber Space between Reality and Ambition"Mashroo'a Al Itifaqiya Al Arabiya lihimayt Al Fadaa Al sybrani bayn Al waq'a wal tomoh", The Arab Center for Legal and Judicial Research, Council of Arab Justice Ministers, League of Arab States, Beirut, 23-25 July
3. Musa, Talib Hasan, Omar, Omar Mahmoud, (2016) The Internet in Law "Internet Qanoonan", Journal of Sharia and Law, United Arab Emirates University, (27), 333-388 p. 339.
4. Naous, Mustafa, (2012) State Sovereignty in Cyberspace "Siadet Al Dawla fi Al fadaa Al electrony", Journal of Sharia and Law, College of Law, United Arab Emirates University, Issue 51.
5. Affaire Du Détroit De Corfou (Royaume-Uni C Albanie), CIJ Recueil 1949, 4, 35
6. Affaire Du Lotus (France C/Turquie ° CPIJ Série A, N°10, P.18 (1927).
7. Affaire Fonderie De Trail (United States V Canada) Recueil Des Sentences Arbitrales Internationales, Vol III Pp 1905-1982, 1965 (1941)
8. Affaire Ministère Public De Munich Allemagne Contre Compuserve, Jugement Du 28 Mai 1998 – 8340, Ds 465
9. Arlene H. RINALDI, A., (1995) The Net: User Guidelines And Netiquette, Disponible À L'adresse Suivante: Tim NORTH, « The Internet And Usenet Global Computer Networks: An Investigation Of Their Culture And Its Effects On New Users », < Disponible À Http: Foo.Curtin.Edu.Au/Thesis/Defautt, Html>.
10. Bacot, G. (1985), Carré De Malberg Et L'origine De La Distinction Entre Souveraineté Du Peuple Et Souveraineté Nationale, Paris, Éd. Du C.N.R.S, P. 9.
11. Bellanger, P., De La Souveraineté En Général Et De La Souveraineté Numérique En Particulier, *Les Échos*, 30 Août 2011 (Archives.Lesechos.Fr/Archives/Cercle/2011/08/30/Cercle_37239.Htm).
12. Benyekhlef, K. & Guy Lefebvre, G., (1993) L'internationalisation Du Droit Et L'affirmation De La Souveraineté: Réflexions Théoriques Et Pratiques, **Dans Souveraineté Et Intégration**, Montréal, Éd. Thémis..
13. Benyekhlef, K., (2002) L'Internet: Un Reflet De La Concurence Des Souverainetés Lex Electronica, Vol. 8, N°1, Automne 2002, P.6. Http://Www.Lex-Electronica.Org/Articles/V8-1/Benyekhlef.Htm
14. Bouchera, L. (1996) " La Souveraineté Informationnelle: Entre Utopie Et Projet " **Le Monde** 1er Février 1996
15. Cassini, S., Cloud Souverain, Un Gâchis À La Française, Lesechos.Fr, 24 Février 2015 (Www.Lesechos.Fr/24/02/2015/Lesechos/21884-030-ECH_Cloud-Souverain--Un-Gachis-A-La-Francaise.Htm

16. Colin, N., And Verdier, H., (2014) « Souveraineté Numérique: La Piste Industrielle », Paristechreview.Com, 30 Juin 2014 (Www.Paristechreview. Com/2014/06/30/Souverainete-Numerique).

17. Corn, G. P., & Taylor, R. (2017). Concluding Observations On Sovereignty in Cyberspace. **American Journal of International Law Unbound**, 111, 282–283. Doi:10.1017/Aju.2017.77

18. Corn, G., & Taylor, R. (2017). Sovereignty in The Age of Cyber**. American Journal of International Law Unbound**, 111, 207-212. Doi:10.1017/Aju.2017.57

19. Cubertafond, B., (1989), Souverainetés En Crise? **Revue De Droit Public Et De Sciences Politiques**,

20. Débat Entourant L'adoption Par Le Législateur Américain Du Communications Decency Act of 1996, Codified at 47 U.S.C., Section 223(A) To (H).

21. Détroit De Corfou, Fond, Arrêt, C.I.J. Recueil 1949,

22. Doutriaux, M. Frontières, 2015, Légales Et Souveraineté Dans Le Cyberespace? ***Chaire Cyber-Défense Et Cyber-Sécurité***.

23. Étienne, J., « Google Health, Un Carnet De Santé Personnel En Ligne », Futura-Sciences.Com, 22 Mai 2008 (Www.Futura-Sciences.Com/Sante/Cvactualites/Medecine-Google-Health-Carnet-Sante-Personnelligne-15600/).

24. Fang, B. (2018) Objective Existence Of Cyberspace Sovereignty In Countries' Affairs. In: **Cyberspace Sovereignty**. Springer, Singapore,

25. Ganascia, J., Germain, E., & Kirchner, C., (2018) La Souveraineté À L'ère Du Numérique. Rester Maîtres De Nos Choix Et De Nos Valeurs. CERNA. 2018.

26. GOTLIEB, A., DALFEN, C., & KATZ K., (1974) « The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles », **American Journal of International Law.**

27. GUEHAM F., Vers La Souverinete Numerique: Pour Une Nouvelle Gouvernance De L'Internet, 2017, P. 10: Www.Fondapol.Org ›

28. ICC Policy Statement: Cross-Border Law Enforcement Access To Company Data – Current Issues Under Data Protection And Privacy Law » (Février 2012)

29. Institut De La Souveraineté Numérique, « Les Nouveaux Enjeux Européens De La Souveraineté Numérique », *Cahiers De La Souveraineté Numérique*, N° 1, 2015 (Www.Souverainetenumerique.Fr/Sites/Default/Files/Cahiers-De-La-Souverainetenumeriquen1.Pdf).

30. Jacques, L., (1996) Cyberspace Et Droit International: Pour UN Nouveau Jus Communications, **Revue De La Recherche Juridique–Droit Prospectif**, P. 830-832

31. Khanna P. (2018) State Sovereignty And Self-Defence In Cyberspace. **Brics Law Journal**, 5(4): Pp.139-154. Https://Doi.Org/10.21684/2412-2343-2018-5-4-139-154

32. Kilovaty, I. (2019). The Elephant in The Room: Coercion. **American Journal of International Law Unbound**, 113, 87-91. Doi:10.1017/Aju.2019.10

33. Kittichaisaree, K., (2017) Public International Law of Cyberspace, Law, Governance and Technology, Series 32.

34. La Convention De Budapest Du 23 Novembre 2001.

35. La Recherche Juridique- Droit Prospectif, 573; Guy ROCHER, « Pour Une Sociologie Des Ordres Juridiques

36. Les Contours De La Neutralité Du Net En Europe Se Précisent, Lemonde.Fr, 31 Août 2016 (Www.Lemonde.Fr/ Pixels/Article/2016/08/31/Les-Contours-De-La-Neutralite-Du-Net-En-Europe-Se-Precisent_4990450_4408996. Html).

37. Les Nouvelles Règles De L'ue Sur La Protection Des Données Placent Les Citoyens Aux Commandes », Actualité Du Parlement Européen, Europarl.Europa.Eu, 1er Juin 2016: (Www.Europarl.Europa.Eu/News/Fr/Newsroom/20160413BKG22980/Nouvelle-Législation-Européenne-Sur-La-Protection-Des-Données).

38. LIPSCHUTZ, R. Reconstructing World Politics: The Emergence of Global Civil Society, (1992) 21 Millenium. Journal of International Studies, Note 31, 391.

39. MACDONALD, R., (1986), Pour La Reconnaissance D'une Normativité Juridique Implicite Et «Inférentielle », 28(1) Sociologie Et Sociétés, 47.

40. Melzer, N., (2011) Cyberware Fare and International Law, **UNIDIR, Ressources,** P.4

41. POST, D., (1995) Anarchy, State, And The Internet: An Essay On Law-Making In Cyberspace, J. Online L. Art.3, Disponible Également À: <Http://Www.Law.Cornell.Edu/Jol/Post.Html>. L'auteur Y Développe La Théorie De L'exit: (Paragr. 39 Et 40).

42. RUGGIE, J. « Territoriality and Beyond: Problematizing Modernity in International

43. Shen, Y. (2016). Cyber Sovereignty and The Governance of Global Cyberspace. **Chinese Political Science Review**, 1(1),

44. TGI Paris, Ordonnance Du Référé Du 20 Novembre 2000, Http://Www.Juriscom.Net/Txt/Jurisfr/Cti/Tgiparis20001120.Htm

45. Tribunal De Grande Instance De Paris Ordonnance De Référé 10 Février 2012, Http://Www.Legalis.Net/Spip.Php?

46. Tribunal De Grande Instance De Paris Ordonnance De Référé 28 Novembre 2013,

47. Tsagourias, N., (2018) Law, Borders and The Territorialisation of Cyberspace. **Forthcoming, Indonesian Journal of International Law**, 2018. Http://Dx.Doi.Org/10.2139/Ssrn.3213511

48. VANDERLINDEN, J., (1993) Vers Une Nouvelle Conception Du Pluralisme Juridique, 2

49. Voir « Les Géants Du Web Menacent-Ils La Souveraineté Des États? », Vidéo Du Forum « Qui Gouverne Internet? », Organisé Par Libération Le 21 Mai 216 (Www.Liberation.Fr/Evenements-Libe/2016/05/21/Les-Geants-Du-Web-Menacent-T-Ils-La-Souverainete-Des-Etats_1454219).

50. Voy: Politique De Sécurité Des Systèmes D'information De l'État-ANSSI Du 17 Juillet 2014