

DOI: 10.47743/jss-2021-67-4-19

## Suveranitatea digitală – viitorul spațiului virtual?

### Is Cybersovereignty the Future of Cyberspace?

Carmen Moldovan<sup>1</sup>

**Rezumat:** Conceptul de suveranitate digitală a fost promovat intens de către China și Federația Rusă și se dorește a fi o transpunere în mediul virtual a principiului suveranității din dreptul internațional public. De esența sa este opoziția față de ideea libertății internetului în lipsa reglementărilor din partea statelor. Prezenta lucrare își propune să exploreze, dintr-o perspectivă critică, principalele trăsături și implicații ale suveranității digitale, prin trimitere la principiile dreptului internațional. Până în prezent, la nivelul ONU s-a cristalizat concluzia aplicabilității principiilor dreptului internațional în *Cyberspace* (inclusiv a principiului suveranității), însă nu este clar dacă aplicarea acestora se realizează în aceeași parametri și având același sens ca în spațiul fizic.

**Cuvinte-cheie:** principii; ONU; reglementare; suveranitate; aplicare teritorială

**Abstract:** Cybersovereignty is a concept highly supported by China and the Russian Federation, considering it as an application of the principle of state sovereignty. In essence, it is opposed to the idea of an open Internet outside State regulations. The aim of this paper is to critically explore the main features and implications of the concept of Cybersovereignty by reference to the basic principle of sovereignty in International Law. At this date, within the United Nations the conclusion of specialized working groups is that principles and norms of International Law are applicable in Cyberspace. However, it is far from clear if the same parameters and meaning as in the physical space are applicable.

**Keywords:** principles; UN; regulation; sovereignty; territorial application

### *Introducere*

Dezvoltarea internetului a avut un efect omniprezent asupra comunicațiilor și tehnologiei, afectând și dezvoltând multe niveluri de activitate umană și creând spațiul cibernetic ca mediu global care nu poate exista în absența lui.

Statele și dreptul internațional nu au putut să se adapteze cu ușurință la evoluția dinamică a tehnologiei și să reacționeze prin reglementarea tuturor problemelor legate de utilizarea și mijloacele de comunicare ale acesteia. În acest sens, reacția companiilor private, direct implicate și interesate de acest domeniu și adesea în afara contribuției și sprijinului statelor a fost mai promptă în așa fel încât

---

<sup>1</sup> Lector univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: carmen.moldovan@uaic.ro

paradigma normativă în reglementarea acestui mediu a trecut de la controlul exclusiv al statelor pentru a deveni un interesul mai multor părți interesate.

Totuși, scopul de a asigura aplicarea efectivă a normelor de drept internațional în spațiul cibernetic și, în același timp, securitatea utilizatorilor acestuia se poate dovedi necesar în anumite contexte, dar nu poate justifica mijloace autoritare.

Prezenta lucrare își propune să analizeze dintr-o perspectivă critică, teoretică și practică, ideea de suveranitate cibernetică (*cybersovereignty*). Spre deosebire de alte domenii ale dreptului internațional, operațiunile ciberneticе reprezintă o formă relativ nouă de relații ale statelor, iar spațiul cibernetic este considerat o zonă „gri” a dreptului internațional, aparent în mare măsură neexploatăă de state, din care dreptul internațional nu poate fi exclus, însă se impune luarea în considerare a regulilor și principiilor acestuia raportat la caracteristicile *Cyberspace* (denumire ce va fi folosită în cuprinsul prezentei lucrări pentru a desemna spațiul cibernetic).

Evoluțiile recente de la nivelul Națiunilor Unite constând în raporturile grupurilor de lucru special create – UN Group of Experts și UN Open-ended Working Group – pe tema aplicării dreptului internațional în *Cyberspace* au subliniat că dreptul internațional este aplicabil fără a furniza detalii și fără a preciza care sunt consecințele juridice ale acestei constatări. În scopul acestei lucrări, termenul de suveranitate cibernetică se referă la aplicarea principiului suveranității statului în spațiul cibernetic.

Există o asimetrie între crearea și dinamica constantă a evoluției *Cyberspace* și dezvoltarea unor reguli specifice drept internațional în acest domeniu. Lacunele normative pot părea semnificative, iar necesitatea de a le acoperi este una reală și poate avea consecințe inclusiv asupra instituției răspunderii statului pentru fapte ilicite. Obiectivul prezentei lucrări este de a demonstra că aplicarea sensului teritorial clasic al suveranității în *Cyberspace* este incompatibilă cu trăsăturile spațiului cibernetic ca mediu global și cele două concepte pot fi reconciliate doar dacă statele acceptă o interpretare evolutivă a aplicării suveranității în acest mediu.

### **1. *Cybersovereignty* – concept și implicații**

Ideea de suveranitate cibernetică ce presupune crearea și controlul asupra unui „ciberspațiu național”<sup>2</sup>, reglementat de legile interne ale unui stat este o manifestare a autoritarismului ce urmărește justificarea preluării controlului deplin asupra acestui mediu și asupra internetului și separarea acestora de rețeaua globală, ceea ce este contrar înseși esenței lor. O astfel de abordare este prezentată ca o

---

<sup>2</sup> M. Mueller, *Sovereignty and Cyberspace: Institutions and Internet governance*, Essay presented at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3rd 2018, [Online] la <http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10410/5th-Ostrom-lecture-DLC.pdf?sequence=1&isAllowed=y>, accesat 10.10.2021.

alternativă la hegemonia Statelor Unite în *Cyberspace* ca spațiu global<sup>3</sup> și ca mijloc de a asigura principiul egalității între state ținând cont de faptul că există diferențe semnificative în ceea ce privește accesul real la *Cyberspace* din cauza nivelului tehnologic de dezvoltare inegal, rezultatul fiind un mediu fragmentat.

Această afirmație nu poate fi privită ca un argument pertinent având în vedere exact gradul de dezvoltare tehnologică, este puțin probabil ca țările mai puțin dezvoltate să poată asigura efectiv securitatea rețelei lor cibernetice național, invocarea unor astfel de motive subliniază că problema reglementărilor în mediul *Cyberspace* este un instrument al rivalității geopolitice<sup>4</sup>.

*Cyberspace* este caracterizat uneori ca haotic, anarhic<sup>5</sup> și asimetric în raport cu resursele și capacitățile celor care participă la diferite operațiuni<sup>6</sup> pentru a justifica ideea unei suveranități cibernetice a statului care își protejează interesele în raport cu alte state, însă afirmarea acestui principiu nu rezolvă toate problemele ulterioare: răspunderea statului, consecințe asupra intereselor și drepturilor persoanelor private și a actorilor nestatali.

Oricât de neclară ar fi la acest moment întinderea și conținutul principiilor aplicabile în acest mediu, caracterizarea ca anarhică nu este una satisfăcătoare. Caracteristici precum complexitatea, diversitatea utilizatorilor (state, actori nestatali, companii private, persoane private) au determinat crearea mai multor niveluri și diferite tipuri de relații între utilizatorii săi, în funcție de calitatea acestora și de natura raporturilor create. Este întemeiată opinia potrivit căreia poate fi, din punct de vedere tehnic și juridic, secționat în mai multe părți: rețele publice accesibile tuturor și nelimitate de frontiere interne, cu acces liber; rețele teritoriale precum intranet-uri militare sau rețele guvernamentale cu acces limitat; rețele exclusive – pentru servicii de e-guvernare, afaceri, finanțe – accesul este limitat la persoanele autorizate<sup>7</sup>. Conceptul *cybersovereignty* nu ia în considerare aceste aspecte. Din aceste motive, termenul poate fi considerat inexact sau greșit pentru că principiul suveranității, care este piatra de temelie a dreptului internațional, nu poate fi transferat pe deplin în *Cyberspace*. Noțiunea de suveranitate teritorială în spațiul cibernetic trebuie aplicată în mod restrictiv, doar în raport cu elementele infrastructurii IT&C de pe teritoriul statului. Totodată, interpretarea

---

<sup>3</sup> Y. Shen, *Cyber Sovereignty and the Governance of Global Cyberspace*, Chin. Polit. Sci. Rev. (2016) 1:81–93, p. 82.

<sup>4</sup> H. Moynihan, *Power Politics Could Impede Progress on Responsible Regulation of Cyberspace*, 3 December 2019, [Online] la <https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace>, accesat 20.10.2021.

<sup>5</sup> S. Arsène, *Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?* in China Perspectives 2016/2 | 2016 What Kind of International Order Does China Want, p. 28, <https://doi.org/10.4000/chinaperspectives.6973>.

<sup>6</sup> Y. Shen, *op. cit.*, p. 84.

<sup>7</sup> J. Zeng, T. Stevens, Y. Chen, *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'*, Politics & Policy, Volume 45, No. 3, 2017, pp. 432-464, 451, <https://doi.org/10.1111/polp.12202>.

domeniului de aplicare a acestui principiu ar trebui făcută ținând cont de evoluția termenilor și a relațiilor reglementate de dreptul internațional public pentru a acoperi decalajul în reglementarea comportamentului statelor în acest mediu.

## **2. Implicații ale caracterului sui generis al Cyberspace**

Nu există consens între state cu privire la reglementarea *Cyberspace* sau chiar cu privire la înțelegerea funcționării acestuia în acest mediu complex, a cărui definire și caracteristici provin din literatura science-fiction, din *Neuromantul* scris de Wiliam Gibson. Aceste aspecte nu vor fi abordate în cuprinsul prezentei lucrări deoarece au făcut obiectul unor alte studii și articole<sup>8</sup>. O definiție standard sau obiectivă a acestui mediu lipsește<sup>9</sup> astfel că termenul este utilizat în general în privința oricăror aspecte ale utilizării rețelelor de computere și internet și pentru a descrie legăturile cu rețelele și computerele<sup>10</sup> mai ales în domeniul securității<sup>11</sup>. Lipsa unei definiții unice nu este însă de natură a împiedica aplicarea regulilor și principiilor dreptului internațional în acest mediu și în privința conduitei statelor<sup>12</sup>.

Spre deosebire de teritoriul statului, care are o dimensiune fizică și materială unde este aplicabil principiul suveranității, *Cyberspace* este în întregime creația omului<sup>13</sup> și constituie o rețea globală complexă, un spațiu logic, nelimitat, imperceptibil, nematerializat, dependent de timp<sup>14</sup>, în continuă schimbare, un

---

<sup>8</sup> C. Moldovan, *Blurred lines in defining the conduct of States in Cyberspace. A critical analysis on the cyber sovereignty and impact over free access to information*, presented at European Society of International Law Kraków-Leiden Online Symposium on 'Exploring the Frontiers of International Law in Cyberspace', 4 December 2020; C. Moldovan, *Limits of International Law in a limitless Cyberspace. Challenges and uncertainties*, în *Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași*, Tomul LXVI/Supliment, Științe juridice, 2020, pp. 315-326, [Online] la [http://pub.law.uaic.ro/files/articole/2020/2020\\_i\\_bis/21\\_moldovan\\_dip\\_cyberspace.pdf](http://pub.law.uaic.ro/files/articole/2020/2020_i_bis/21_moldovan_dip_cyberspace.pdf), accesat 20.10.2021; C. Moldovan, *Are there any limits to the rights of States in Cyberspace? An analysis from the perspective of International Law*, presented at the 13th Biennial International Conference organised by the Faculty of Law of the West University of Timișoara, 6-7 November 2020.

<sup>9</sup> R. Ottis, P. Lorents, *Cyberspace: Definition and Implications*, in Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April 2010, [Online] la <https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/>, accesat 20.10.2021.

<sup>10</sup> *Ibidem*.

<sup>11</sup> E. Donahoe, *The Need for a Paradigm Shift on Digital Security*, eds. Fen Osler Hampson and Michael Sulmeyer, *Getting beyond Norms New Approaches to International Cyber Security Challenges* Special Report, Centre for International Governance Innovation, 2017, p. 31

<sup>12</sup> C. Moldovan, *op. cit.*, *Limits ....* 2020, p. 318-319.

<sup>13</sup> M. Baezner, P. Robin, *Trend Analysis: Cyber Sovereignty*, Risk and Resilience Team Center for Security Studies (CSS) ETH Zürich, 2018, p. 8.

<sup>14</sup> R. Ottis, P. Lorents, *op. cit.*

sistem informațional interconectat creat de actori nestatali, fără frontiere<sup>15</sup>, ce este legat de teritoriul fizic prin infrastructură fără de care nu poate exista<sup>16</sup>.

Toate aceste elemente descriu un fenomen *sui generis*<sup>17</sup>, probabil una dintre cele mai mari creații ale umanității din prezent, un spațiu civil și militar deopotrivă ce nu poate fi e supus controlului exclusiv al statelor, deoarece nu poate fi plasat sub suveranitatea statului<sup>18</sup>.

Caracteristicile speciale aseamănă acest mediu cu cele în care statele nu își exercită jurisdicția exclusivă sau se bucură de prerogative speciale, cum ar fi marea liberă sau spațiul cosmic ce au regim juridic special.

Complexitatea Cyberspace și trăsăturile sale explică motivele furnizării unei definiții general acceptate sau incluse în cuprinsul unui tratat internațional. O astfel de sarcină se poate dovedi nu doar dificilă, ci și imposibilă (sens în care amintim lipsa reglementărilor cu caracter obligatoriu în acest domeniu, cu excepția *Convenției de la Budapesta privind criminalitatea informatică*<sup>19</sup>, adoptată în cadrul Consiliului Europei). În acest context, crearea la nivelul Națiunilor Unite a grupurilor de lucru specializate – UNGGE (*the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*) și OEWG (*Open-ended working group on developments in the field of information and telecommunications in the context of international security*)<sup>20</sup> – reprezintă o încercare de a clarifica aplicabilitatea regulilor dreptului internațional public. Începând cu anul 2013<sup>21</sup> până în prezent, concluziilor ambele

---

<sup>15</sup> K. Nyman Metcalf, *Legal View on Outer Space and Cyberspace: Similarities and Differences*, Tallinn Paper No. 10, 2018, p. 2, [Online] la [https://ccdcoe.org/uploads/2018/10/Tallinn-Paper\\_10\\_2018.pdf](https://ccdcoe.org/uploads/2018/10/Tallinn-Paper_10_2018.pdf), accesat 12.10.2021.

<sup>16</sup> Y. Shen, *op. cit.*, p. 83.

<sup>17</sup> D. Broeders, L. Adamson, R. Creemers, *Coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, in The Hague Program For Cyber Norms Policy Brief. November 2019, p. 2, [Online] la [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3493600](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3493600), accesat 29.11.2021.

<sup>18</sup> W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, in 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), NATO CCDCOE Publications, 2012, p. 8.

<sup>19</sup> Council of Europe, *Convention on Cybercrime*, 23.XI.2001, ETS No.185.

<sup>20</sup> UNODA, *Fact Sheet - Developments in the field of information and telecommunications in the context of International Security*, 2019, [Online] la <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf>, accesat 21.10.2021.

<sup>21</sup> United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, para. 19, U.N. Doc. A/68/98, June 24, 2013, [Online] la <http://undocs.org/A/68/98>, accesat 21.10.2021; United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 2015, [Online] la <https://undocs.org/A/70/174>, accesat 21.10.2021; United Nations General Assembly (2018), *Resolution adopted by the General Assembly on 22 December 2018 on "Advancing responsible State behaviour in Cyberspace in the context of international security"*, UN Doc A/RES/73/266, [Online] la

grupuri au fost în sensul aplicării dreptului internațional pentru conduita statelor în acest mediu, însă un rol esențial în lămurirea efectelor acestora revine statelor, care au exprimat oficial puncte de vedere fie în cadrul grupurilor de lucru, fie prin declarații speciale în această privință.

Normele privind comportamentul responsabil al statelor în *Cyberspace*, identificate prin documentele celor două grupuri de lucru, au fost considerate norme acceptate voluntar de către state (*voluntary norms*)<sup>22</sup>, exprimare ce este ambiguă și conturează lipsa forței juridice obligatorii și creează incertitudine inclusiv în ceea ce privește aplicarea principiului suveranității în acest mediu.

Concluzii din luna iulie 2020 ale OEWG subliniază rolul esențial al Raportului din 2015 adoptat în cadrul UNGGE, care susține necesitatea implementării normelor voluntare identificate pentru a asigura caracterul public al internetului, prin raportare la obligația de respectare a drepturilor fundamentale<sup>23</sup>. Un alt document, din octombrie 2020, denumit *The future of discussions on ICTs and Cyberspace at the UN*<sup>24</sup> propune stabilirea unui *Program de acțiune pentru promovarea comportamentului responsabil al statului în spațiul cybernetic (Programme of Action for advancing responsible State behaviour in Cyberspace)*, în vederea încetării discuțiilor în două niveluri (GGE și OEWG) și a stabilirii unui forum permanent în cadrul Națiunilor Unite pentru analiza utilizării tehnologiilor de informații și comunicare de către state în contextul securității internaționale, luând în considerare constatările făcute de cele două grupuri de lucru.

### 3. Caracteristicile principiului suveranității statului

Pentru a justifica ideea de suveranitate a statului în *Cyberspace*, se folosește principiul suveranității teritoriale. Deși principiul a fost consacrat cu multă vreme în urmă, dreptul internațional nu conține o definiție exhaustivă a acestuia, astfel încât identificarea elementelor și semnificației acesteia este relevantă pentru

---

<https://undocs.org/en/A/RES/73/266>, accesat 21.10.2021; United Nations General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, 10 March 2021, *Final Substantive Report*, A/AC.290/2021/CRP.2, [Online] la <https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>, accesat 21.10.2021.

<sup>22</sup> E. Tikk, M. Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, in Cyber Policy Institute, 2017, p. 14.

<sup>23</sup> Statements by the Republic of Finland Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Virtual Informal Consultations 19 June and 2 July 2020, Statement 2 delivered 2 July 2020, [Online] la <https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-finland-19-june-and-2-july-2020.pdf>, accesat 10.09.2021.

<sup>24</sup> OEWG, *The future of discussions on ICTs and Cyberspace at the UN*, [Online] la <https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf>, accesat 10.10.2021.

analiza aplicabilității acestuia în mediul analizat și pentru identificarea limitelor sale, cum sunt jurisdicția și imunitățile statului. Complexitatea conceptului este amplificată de faptul că sensul modern al suveranității se referă la popoarele din cadrul statului, nu exclusiv la statul însuși ca entitate juridică<sup>25</sup>.

Suveranitatea ca principiu datează din secolul al XVI-lea și este unul dintre conceptele dezvoltate după Pacea de la Westfalia din 1648<sup>26</sup>. Sistemul Westfalian considera că statele dețin suveranitate asupra teritoriilor și afacerilor interne ale acestora fără intervenția altor state.

Principiul suveranității statului este unul dintre principiile fundamentale ale dreptului internațional, consacrat în articolul 2 paragraful 1 din Carta Națiunilor Unite<sup>27</sup> și instrumentele juridice ulterioare (*Declarația privind principiile dreptului internațional, relațiile de prietenie și cooperarea între state în conformitate cu Carta Națiunilor Unite*<sup>28</sup>, *Actul Final Helsinki*<sup>29</sup>, *Carta de la Paris pentru o nouă Europă*<sup>30</sup>) au menționat, de asemenea, acest principiu și valoarea sa ridicată pentru dreptul internațional și au stabilit legături între acesta și alte principii fundamentale precum neintervenția, autodeterminarea, integritatea teritorială și soluționarea pașnică a diferendelor<sup>31</sup>.

Dintr-o perspectivă teritorială, suveranitatea statului și alte principii fundamentale ale dreptului internațional se aplică tuturor componentelor teritoriului unui stat aflat în interiorul granițelor sale (terestre, maritime, aeriene) în care acesta se bucură de o exclusivitate incontestabilă și plenitudine de competență. Toate elementele suveranității statului se referă și sunt analizate în legătură cu teritoriul fizic al statului în funcție de stadiul de evoluție al regulilor și conceptelor de drept internațional. Suveranitatea, atribut esențial al statului atât la nivel internațional cât și intern<sup>32</sup>, descrie competențele statelor și prezintă de fapt sensuri

<sup>25</sup> S. Besson, *Sovereignty, International Law and Democracy*, in *The European Journal of International Law*, Vol. 22 no. 2, 2011, p. 383, <https://doi.org/10.1093/ejil/chr029>.

<sup>26</sup> A. Osiander, *Sovereignty, International Relations, and the Westphalian Myth*, in *International Organization*, vol. 55, no. 2, 2001, pp. 251–287, DOI: <https://doi.org/10.1162/00208180151140577>.

<sup>27</sup> Articolul 2 paragraful 1 al cartei Națiunilor Unite prevede: „1. Organizația este întemeiată pe principiul egalității suverane a tuturor Membrilor ei”.

<sup>28</sup> United Nations General Assembly Resolution 2625 (XXV), adopted on 24 October 1970, A/RES/26/25 (XXV), *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (24 October 1970)*.

<sup>29</sup> Organization for Security and Co-operation in Europe, Helsinki Final Act, August 1975, [Online] la <https://www.osce.org/helsinki-final-act>, accesat 12.10.2021.

<sup>30</sup> Organization for Security and Co-operation in Europe, Charter of Paris for a New Europe, 21 November 1990, [Online] la <https://www.osce.org/mc/39516>, accesat 12.10.2021.

<sup>31</sup> H. Steinberger, “Sovereignty”, în *Encyclopedia of Public International Law*, Volume four, North-Holland, Elsevier, 2000, p. 513.

<sup>32</sup> J. Combacau, S. Sur, *Droit international public*, 12<sup>e</sup> edition, LGDJ 2016, p. 238; M. Bennouna, *Le droit international entre la lettre et l'esprit. Cours général de droit international public*, (Collected Courses of the Hague Academy of International Law, Tome 383, Brill /Nijhoff), 2016, p. 42.

multiple, este indivizibilă, exclusivă, inalienabilă și reprezintă o garanție a derulării relațiilor dintre state<sup>33</sup>, bazate pe independență și lipsa de subordonare a unui stat față de celelalte<sup>34</sup>.

În analiza conținutului și a implicațiilor principiului suveranității, multe lucrări academice au ca reper concluziile din cauza *Insula Palmas*<sup>35</sup>, ce a analizat dimensiunea teritorială a suveranității astfel:

„*Suveranitatea teritorială (...), implică dreptul exclusiv al unui stat a-și face publice activitățile. Acest drept are corolar o îndatorire: obligația de a proteja în interiorul teritoriului drepturile altor state, în special dreptul lor la integritate și inviolabilitate în timp de pace și război, împreună cu drepturile pe care fiecare stat le poate pretinde pentru cetățenii săi pe teritoriul străin*”<sup>36</sup>. În același timp, trebuie subliniat că hotărârea arbitrală a avut în vedere natura dinamică a conceptului de suveranitate, și a menționat:

„*Manifestările de suveranitate teritorială îmbracă, este adevărat, forme diferite, în funcție de condițiile de timp și de loc*”<sup>37</sup>.

Această concluzie poate fi folosită pentru a justifica interpretarea restrictivă a suveranității statului în *Cyberspace*.

Suveranitatea se bazează pe ideea exercitării controlului sau a unei manifestări de autoritate pe un anumit teritoriu<sup>38</sup> al statului și a altor spații cu statut juridic special și include controlul asupra tuturor persoanelor de pe teritoriu<sup>39</sup>, care are semnificația exercitării competenței (competență prescriptivă, competență de a judeca, competență de executare). Sensul principiului suveranității este rezultatul evoluției și are o semnificație diferită de cea pe care a prezentat-o în secolele al XVI-lea și al XVII-lea când a apărut ca urmare a intenției monarhiilor europene de a-și consolida poziția în raport cu biserica<sup>40</sup>.

Transpunerea în *Cyberspace* a ideii de suveranitate având conținutul anterior descris, are ca efect exercitarea controlului în acest mediu asupra elementelor care susțin suveranitatea. În acest sens, lucrările grupurilor din cadrul Națiunilor Unite - GGE și OEWG nu se referă la o idee abstractă de suveranitate, ci se raportează la infrastructura IT & C aparținând statului sau situată pe teritoriul acestuia, abordare pe deplin compatibilă cu caracteristicile și elementele suveranității.

---

<sup>33</sup> C. Moldovan, *Drept internațional public. Principii și instituții fundamentale*, Ediția a II-a, Editura Universul Juridic, București, 2019, p. 140.

<sup>34</sup> J. Crawford, *Brownlie's Principles of Public International Law*, Eighth Edition, Oxford University Press, 2012, p. 447.

<sup>35</sup> PCA, *Island of Palmas Case* (or Miangas), United States of America v. The Netherlands, Award of the Tribunal, 4 April 1928, [Online] la <https://pcacases.com/web/sendAttach/714>, accesat 20.10.2021.

<sup>36</sup> *Idem*, p. 9.

<sup>37</sup> *Ibidem*.

<sup>38</sup> ICJ, *Territorial and Maritime Dispute* (Nicaragua v. Colombia) Judgment of 19 November 2012.

<sup>39</sup> A. Cassese, *International Law*, Second Edition, Oxford University Press, 2005, p. 49.

<sup>40</sup> M. Bennouna, *op. cit.*, p. 41.



#### 4. Divergențe și confluențe asupra suveranității cibernetice

Conceptul de suveranitate cibernetică a fost folosit pentru prima dată promovat intens de China și include mai multe prerogative ale statului, conform legislației naționale, de a reglementa conduita persoanelor private în legătură cu folosirea internetului și a datelor cu caracter personal pe teritoriul său, ca mijloc de protejare a spațiului informațional, în conformitate cu politica generală privind controlul internetului și fluxul de date<sup>41</sup>. Statul chinez a inițiat proiectul numit *The Golden Shield*, în 1996 și l-a implementat în 2008<sup>42</sup>. Acesta este exemplul perfect, deoarece stabilește controlul deplin al statului asupra informațiilor și accesului la informații.

Același tip de abordare este reflectată și extinsă de legislația internă a Federației Ruse care a adoptat în 2019 „*Legea suverană a internetului*”<sup>43</sup> ce stabilește cadrul legal pentru controlul asupra internetului între frontierele acesteia<sup>44</sup>. Federația Rusă a susținut crearea unei rețele naționale proprii pentru care a fost deja făcute teste și utilizatorii nu au întâmpinat probleme sau nici măcar nu și-au dat seama că au intervenit schimbări. Anterior, în decembrie 2016, Președintele Federației Ruse a aprobat *doctrina securității informaționale* care presupune crearea internetului și mediului cibernetic național, precum și separarea acestuia de spațiul cibernetic internațional<sup>45</sup>.

Justificarea dată de președintele rus este că aceasta reprezintă o măsură de securitate pentru protejarea statului în cazul unei „urgente sau amenințări străine precum un atac cibernetic”<sup>46</sup>. Potrivit legii, statul are prerogativa de a controla internetul prin infrastructura instituită în Rusia și de a crea un sistem propriu de nume pentru domeniile de internet. Din perspectiva consecințelor sale, o astfel de măsură constituie deconectarea rețelei de infrastructură rusă de la rețeaua globală și în mod practic, constituie instaurarea cenzurii pentru utilizatorii săi.

O astfel de posibilitate tehnică poate fi pusă în practică fără mare dificultate și ar putea fi văzută ca o manifestare a jurisdicției teritoriale<sup>47</sup>. Totuși, situația în care toate statele, în numele suveranității cibernetice, și-ar crea și izola rețeaua

---

<sup>41</sup> D. Broeders, L. Adamson, R. Creemers, *op. cit.*, p. 2.

<sup>42</sup> S. Chandel, Z. Jingji, Y. Yunnan, S. Jingyao, Z. Zhipeng, *The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall*, în 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, p. 111-119, DOI: <https://doi.org/10.1109/CyberC.2019.00027>.

<sup>43</sup> A. Epifanova, *Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet*, German Council on Foreign Relations DGAP Analysis, No 2 January 2020, [Online] la [https://dgap.org/sites/default/files/article\\_pdfs/dgap-analyse\\_2-2020\\_epifanova\\_0.pdf](https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf), accesat 12.10.2021.

<sup>44</sup> *Ibidem*.

<sup>45</sup> [Online] la <https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html>, accesat 10.11.2021.

<sup>46</sup> [Online] la <https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html>, accesat 10.11.2021.

<sup>47</sup> W.H. Heintschel von Heinegg, *op. cit.*, p. 9.

națională, nu ar mai corespunde ideii de rețea internațională globală așa cum o cunoaștem și o folosim astăzi și ar sacrifica cu siguranță internetul<sup>48</sup>. Ar fi doar o extindere a teritoriului național, controlat în întregime de stat, inclusiv controlul asupra datelor, fluxului de date, utilizatorilor, parametrilor tehnici și caracteristicile generale ale acestui spațiu.

La polul opus, o abordare diferită, mult mai temperată calitativ și cantitativ aparține Franței și a fost exprimată în *Cartea Albă a Apărării și Securității Naționale* din 2013<sup>49</sup>, care se concentrează asupra necesității de a proteja integritatea statului și a infrastructurii în anumite cazuri care ar echivala cu un atac armat. Această viziune a fost extinsă în acte ulterioare precum *Strategia internațională* din 2017<sup>50</sup> și *Analiza strategică* din 2018 *a apărării cibernetice*<sup>51</sup>. Aceasta din urmă afirmă că:

„(...) principiul suveranității se aplică spațiului cibernetic. În acest sens, Franța își reafirmă suveranitatea asupra infrastructurii tehnologiilor informației și comunicațiilor, a persoanelor și a activităților cibernetice situate pe teritoriul său, sub rezerva obligațiilor sale legale internaționale”.

Franța a dezvoltat un sistem național de definire și calificare a acțiunilor care constituie un incident de securitate cibernetică. În stabilirea pragului unei încălcări de suveranitate, abordarea franceză se concentrează pe comportamentul în sine reprezentând pătrunderea sistemului IT&C, nu pe consecințele produse.

Un alt exemplu de abordare globală asupra *Cyberspace* este reprezentat de Statele Unite ale Americii, care propune *Strategia națională cibernetică* din 2018<sup>52</sup>, axată pe ideea de mediu global și deschis ce promovează:

„un cadru pentru comportamentul responsabil al statului în *Cyberspace* construit pe dreptul internațional, aderarea la normele voluntare neobligatorii de comportament responsabil al statului, care se aplică în timp de pace și luarea în considerare a măsurilor practice de consolidare a încrederii pentru a reduce

---

<sup>48</sup> M. Mueller, *op. cit.*, p. 5.

<sup>49</sup> Direction générale des relations internationales et de la stratégie (DGRIS)/Directorate General for International Relations and Strategy, *White Paper on Defence and National Security 2013*, [Online] la <https://www.defense.gouv.fr/english/dgris/defence-policy/white-paper-2013/white-paper-2013>, accesat 20.11.2021.

<sup>50</sup> French Foreign Policy, *Stratégie internationale de la France pour le numérique*, [Online] la <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/https://www.ife.ee/en/international-strategy-for-digital/>, accesat 20.11.2021.

<sup>51</sup> Secretary general on Defense and National Security (France), *Strategic review of cyber defence*, February 2018, [Online] la <http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf>, accesat 20.11.2021; F. Delerue, A. Géry, *France's Cyberdefense Strategic Review and International Law*, March 23, 2018, [Online] la <https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law>, accesat 20.11.2021.

<sup>52</sup> The White House, *National Cyber Strategy of the United States of America*, September 2018, p. 20, [Online] la <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>, accesat 20.11.2021.

*riscul de conflict care decurge din activitatea cibernetică rău intenționată. Aceste principii ar trebui să formeze o bază pentru cooperarea statelor în scopul contracarării acțiunilor care nu sunt conforme cu acest cadru.”*

În 2021, a fost emis un Ordin executiv pentru îmbunătățirea securității cibernetice naționale, care se axează pe adoptarea de măsuri pentru protejarea mediului cibernetic, supus unor numeroase atacuri<sup>53</sup>.

Regatul Unit a dezvoltat de asemenea, o strategie națională de securitate cibernetică<sup>54</sup>, a creat un centru național pentru securitate cibernetică<sup>55</sup> și susține aplicabilitatea suveranității ca principiu, considerând că nu există o regulă a suveranității în Cyberspace<sup>56</sup>. Din punct de vedere teoretic și practic, diferențele dintre cele două abordări ale suveranității: ca principiu și ca regulă, nu sunt de fapt foarte clare și eficacitatea lor poate să nu fie semnificativă, deoarece în fiecare caz există obligații internaționale pentru state.

Pozițiile exprimate public de state cu privire la suveranitatea în Cyberspace pot fi foarte diferite în practică, ceea ce face dificilă argumentarea existenței unei *opinio iuris* asupra modului în care aceasta se aplică, însă această situație nu înseamnă în mod necesar existența unui vid normativ<sup>57</sup>.

Nu toate statele au exprimat puncte de vedere detaliate<sup>58</sup> cu privire la modalitatea în care dreptul internațional se aplică în *Cyberspace*, însă tăcerea statelor sau poziția lor ambiguă poate fi cea mai bună modalitate de a asigura aplicarea dreptului internațional în spațiul cibernetic.

## Concluzii

Noțiunea de „suveranitate digitală” este una ambiguă, în ciuda eforturilor de a clarifica implicațiile acesteia în *Cyberspace* făcute la nivelul Națiunilor Unite. Sunt

---

<sup>53</sup> The White House, *Executive Order On Improving the Nations` s Cybersecurity*, May 12, 2021, [Online] la <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>, accesat 20.11.2021.

<sup>54</sup> Cabinet Office and National Security and Intelligence, *National Cyber Security Strategy 2016 to 2021: progress so far*, [Online] la <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021-progress-so-far>, accesat 20.11.2021.

<sup>55</sup> National Cyber Security Centre, [Online] la <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>, accesat 20.11.2021.

<sup>56</sup> UK Attorney General Jeremy Wright Speech, *Cyber and International Law in the 21st Century*, 23 May 2018, [Online] la <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, accesat 21.11.2021.

<sup>57</sup> M. Tolppa *Overview of the UN OEWG developments: continuation of discussions on how International Law applies in cyberspace*, 2020, [Online] la <https://ccdcoe.org/library/publications/overview-of-un-oewg-developments-continuation-of-discussions-on-how-international-law-applies-in-cyberspace/>, accesat 21.11.2021.

<sup>58</sup> O prezentare a pozițiilor statelor în cadrul sesiunilor OEWG poate fi consultată [Online] la <https://www.un.org/disarmament/open-ended-working-group/>, accesat 20.11.2021.

necesare eforturi suplimentare din partea statelor și a organismelor internaționale pentru a defini această noțiune și a stabili conținutul și limitele sale, prin referire la principiul fundamental al suveranității statului.

Faptul că grupurile de lucru special create în cadrul Națiunilor Unite nu au reușit să dezvolte norme de drept internațional prin mijloace și canale diplomatice subliniază această necesitate. Deși activitatea și constatările sale au fost incomplete și uneori criticate, Națiunile Unite rămâne cel mai potrivit și legitim forum deschis tuturor statelor pentru a discuta toate tipurile de probleme legate de acest mediu, iar dezbaterile din Adunarea Generală pot oferi premisele *opinio juris* asupra comportamentului statelor și a unei guvernări globale în Cyberspace.

Conceptul de „suveranitate cibernetică” se opune ideii de guvernanță globală și nu ține cont de interesele tuturor părților interesate (*mutistakeholders*), cum ar fi companiile private și persoanele private. Exercițarea suveranității statului în acest mediu este limitată și nu are aceeași sferă ca și teritoriul fizic al statului. O abordare echilibrată în această privință ar fi luarea în considerare a unei semnificații diferite, raportat la elementele infrastructurii fizice de care depinde existența *Cyberspace*, urmând a fi clarificate noțiuni precum jurisdicția statului, efectele extrateritoriale ori încălcarea suveranității în spațiul virtual.

### Referințe

- Arsène S., *Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?* in China Perspectives 2016/2 | 2016 What Kind of International Order Does China Want, p. 28, <https://doi.org/10.4000/chinaperspectives.6973>
- Baezner M., Robin P., *Trend Analysis: Cyber Sovereignty*, Risk and Resilience Team Center for Security Studies (CSS) ETH Zürich, 2018
- Bennouna M., *Le droit international entre la lettre et l'esprit. Cours général de droit international public*, (Collected Courses of the Hague Academy of International Law, Tome 383, Brill /Nijhoff), 2016
- Besson S., *Sovereignty, International Law and Democracy*, in The European Journal of International Law Vol. 22 no. 2, 2011, <https://doi.org/10.1093/ejil/chr029>.
- Broeders D., Adamson L., Creemers R., *Coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, in The Hague Program For Cyber Norms Policy Brief, November 2019
- Cabinet Office and National Security and Intelligence, *National Cyber Security Strategy 2016 to 2021: progress so far*, 2021
- Cassese A., *International Law*, Second Edition, Oxford University Press, 2005
- Chandel S., Jingji Z., Yunnan Y., Jingyao S., Zhipeng Z., *The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall*, in 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, <https://doi.org/10.1109/CyberC.2019.00027>
- Combacau J., Sur S., *Droit international public*, 12<sup>e</sup> edition, LGDJ, 2016
- Council of Europe, *Convention on Cybercrime*, 23.XI.2001, ETS No.185
- Crawford J., *Brownlie's Principles of Public International Law*, Eighth Edition, Oxford University Press, 2012
- Delerue F., Géry A., *France's Cyberdefense Strategic Review and International Law*, March 23, 2018

- Direction générale des relations internationales et de la stratégie (DGRIS)/Directorate General for International Relations and Strategy, *White Paper on Defence and National Security*, 2013
- Donahoe E., *The Need for a Paradigm Shift on Digital Security*, eds. Fen Osler Hampson and Michael Sulmeyer, *Getting beyond Norms New Approaches to International Cyber Security Challenges* Special Report, Centre for International Governance Innovation, 2017
- Epifanova A., *Deciphering Russia's „Sovereign Internet Law” Tightening Control and Accelerating the Splinternet*, German Council on Foreign Relations DGAP Analysis, no 2/2020
- Heintschel von Heinegg W., *Legal Implications of Territorial Sovereignty in Cyberspace*, in 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), NATO CCDCOE Publications, 2012
- Moldovan C., *Drept internațional public. Principii și instituții fundamentale*, Ediția a II-a, Editura Universul Juridic, București, 2019
- Moldovan C., *Blurred lines in defining the conduct of States in Cyberspace. A critical analysis on the cyber sovereignty and impact over free access to information*, presented at European Society of International Law Kraków-Leiden Online Symposium on 'Exploring the Frontiers of International Law in Cyberspace', 4 December 2020
- Moldovan C., *Limits of International Law in a limitless Cyberspace. Challenges and uncertainties*, în *Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași*, Tomul LXVI/Supliment, Științe juridice, 2020
- Moldovan C., *Are there any limits to the rights of States in Cyberspace? An analysis from the perspective of International Law*, presented at the 13th Biennial International Conference organised by the Faculty of Law of the West University of Timișoara, 6-7 November 2020
- Moynihan H., *Power Politics Could Impede Progress on Responsible Regulation of Cyberspace*, December 3<sup>rd</sup> 2019
- Mueller M., *Sovereignty and Cyberspace: Institutions and Internet governance*, Essay presented at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3<sup>rd</sup> 2018
- Nyman Metcalf K., *Legal View on Outer Space and Cyberspace: Similarities and Difference*, Tallinn Paper, no. 10/2018
- Ottis R., Lorents P., *Cyberspace: Definition and Implications*, in Proceedings of the 5<sup>th</sup> International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April 2010
- OEWG, *The future of discussions on ICTs and Cyberspace at the UN*, on-line.
- Organization for Security and Co-operation in Europe, Helsinki Final Act, August 1975, on-line
- Osiander A., *Sovereignty, International Relations, and the Westphalian Myth*, in International Organization, vol. 55, no. 2, 2001, DOI: <https://doi.org/10.1162/00208180151140577>
- PCA, *Island of Palmas Case (or Miangas)*, United States of America v. The Netherlands, Award of the Tribunal, 4 April 1928
- Shen Y., *Cyber Sovereignty and the Governance of Global Cyberspace*, Chin. Polit. Sci. Rev. 1/2016, pp. 81–93
- Steinberger H., "Sovereignty", in *Encyclopedia of Public International Law* (Volume four, North-Holland, Elsevier, 2000
- Tikk E., Kerttunen M., *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, in Cyber Policy Institute, 2017

- Tolppa M., *Overview of the UN OEWG developments: continuation of discussions on how International Law applies in cyberspace*, 2020, on-line
- United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, para. 19, U.N. Doc. A/68/98, June 24<sup>th</sup>, 2013
- United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 2015
- United Nations General Assembly, "Resolution adopted by the General Assembly on 22 December 2018 on „Advancing responsible State behaviour in Cyberspace in the context of international security”, UN Doc A/RES/73/266, 2018
- United Nations General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, *Final Substantive Report*, A/AC.290/2021/CRP, 2021
- United Nations General Assembly Resolution 2625 (XXV), adopted on 24 October 1970, A/RES/26/25 (XXV), *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 1970
- UNODA, *Fact Sheet - Developments in the field of information and telecommunications in the context of International Security*, 2019, on-line
- The White House, *National Cyber Strategy of the United States of America*, September 2018
- The White House, *Executive Order On Improving the Nations` s Cybersecurity*, May 12, 2021, on-line
- UK Attorney General Jeremy Wright Speech, *Cyber and International Law in the 21<sup>st</sup> Century*, 23 May 2018
- Zeng J., Stevens T., Chen Y., *China`s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of `Internet Sovereignty`*, *Politics & Policy*, Volume 45, no. 3/2017, <https://doi.org/10.1111/polp.12202>.