CHỦ QUYỀN KHÔNG GIAN MẠNG: LÝ THUYẾT, THỰC TIỄN THI HÀNH VÀ NHỮNG VẤN ĐỀ PHÁP LÝ ĐẶT RA CHO VIỆT NAM

GS. TS NGUYỄN HỒNG THAO
Trường Đại học Luật TP. Hồ Chí Minh
Ho Chi Minh City University of Law
Email: nhthao@hcmulaw.edu.vn

LÊ SỸ HOÀNG
Học viện Ngoại giao
Diplomatic Academy of Vietnam
Email: hoanglesy003@gmail.com

Tóm tắt

Sự phát triển internet đã tác động mạnh mẽ tới khái niệm chủ quyền quốc gia truyền thống và thúc đẩy xu hướng thực thi chủ quyền không gian mạng trên toàn cầu. Mặc dù kỷ nguyên số thúc đẩy sự phát triển kinh tế - xã hội, những thách thức cũng xuất hiện trong bối cảnh Việt Nam chưa có khung pháp lý về chủ quyền không gian mạng. Bài viết này sẽ phân tích các lý luận và thực tiễn quốc tế về chủ quyền không gian mạng, phân tích tác động của không gian mạng với Việt Nam, từ đó khái quát những vấn đề pháp lý và đưa ra một số gợi mở cho Việt Nam.

Từ khóa: *chủ quyền không gian mạng, không gian mạng, an ninh mạng, internet*

Abstract

The development of internet has had a powerful impact on the traditional concept of national sovereignty and has fueled a global trend toward asserting cyber sovereignty. Although the digital age promotes socio-economic development, challenges also arise in the context that Vietnam have not had a legal framework on cyberspace sovereignty. This article will analyze the theories and international practices related to cyber sovereignty, examine the impact of cyberspace on Vietnam, thereby, outline the legal issues and offer some suggestions for Vietnam.

Keywords: *cyber sovereignty, cyberspace, cybersecurity, internet*
DOI: https://doi.org/10.70236/khplvn.499
Ngày nhận bài: 17/08/2025 **Ngày duyệt đăng: 29/09/2025**

1. Chủ quyền không gian mạng: từ lý thuyết đến thực tiễn áp dụng toàn cầu

Kỷ nguyên internet đã mở ra một không gian mới cho con người, xóa bỏ rào cản địa lý, thay đổi mô hình truyền thông, góp phần xây dựng cộng đồng và nâng cao chất lượng đời sống tinh thần.[1] Tuy nhiên, sự phát triển vượt bậc này cũng đi kèm với các mối đe dọa toàn cầu như khủng bố mạng, tội phạm mạng và chiến tranh mạng, đặt ra yêu cầu phải thiết lập một chế độ quản trị công bằng, có quy tắc, nhằm bảo đảm chủ quyền của quốc gia trên không gian mạng mà vẫn không hạn chế quyền con người, tính mở của Internet và mô hình quản trị đa bên/đa chủ thể. Không gian mạng được xem là không gian thứ năm, bên cạnh lãnh thổ đất liền, vùng trời, vùng biển, đáy biển và lòng đất dưới đáy biển, cần được xác định chủ quyền và điều chỉnh bằng luật quốc tế.[2]

1.1. Nghiên cứu và thảo luận về chủ quyền không gian mạng

Chủ quyền không gian mạng là một vấn đề trọng tâm trong bối cảnh quản trị internet thời hiện đại. Hiện nay, tồn tại hai học thuyết trái ngược: chủ quyền và phi chủ quyền không gian mạng

Đại diện cho học thuyết chủ quyền không gian mạng, học giả Thumfart trong cuốn *The Liberal Internet in the Postliberal Era* đã ủng hộ học thuyết chủ quyền kỹ thuật số *(digital sovereignty)*, cho rằng chủ quyền là cần thiết, thực tiễn và hợp pháp.[3] Chủ quyền

1 Manuel Castells, *The rise of the network society*, Wiley-Blackwell, Vương quốc Anh, 2010, tr. 385-390.
2 Tô Lâm, *Chủ quyền không gian mạng: Yêu cầu thời đại và nghĩa vụ quốc gia*, Nxb. Công an Nhân dân, Hà Nội, 2021, tr. 5.
3 Johannes Thumfart, *The Liberal Internet in the Postliberal Era: Digital Sovereignty, Private Government, and Practices of Neutralization*, Springer Nature Switzerland, 2024, tr. 25-55.

quốc gia là biện pháp cần thiết để kiểm soát luồng dữ liệu, nội dung và ý tưởng,[4] đặc biệt khi các mối đe dọa từ trí tuệ nhân tạo, luồng dữ liệu quốc tế hay các nền tảng số có thể vượt qua biên giới quốc gia. Nhà nước có quyền kiểm soát thông tin độc hại đi vào lãnh thổ có tác động tới công dân, an ninh quốc gia và trật tự xã hội. Chủ quyền không chỉ là quyền kiểm soát mà còn là khả năng đặt ra tiêu chuẩn, quy định để bảo vệ lợi ích quốc gia trong môi trường số khỏi sự lợi dụng của quốc gia khác.

Đại diện cho học thuyết phi chủ quyền không gian mạng, học giả Mueller cho rằng không gian mạng là một không gian chung toàn cầu, tương tự khái niệm về vùng biển quốc tế (*high seas*), nơi chủ quyền quốc gia không nên được áp đặt đầy đủ và nhấn mạnh quyền tự do của các cá nhân, doanh nghiệp cũng như tính không phân mảnh, không biên giới của internet.[5] Phản bác lại quan điểm của Thumfart về chủ quyền không gian mạng, Mueller đưa ra một số phản biện như khái niệm "chủ quyền kỹ thuật số" thường mơ hồ, thiếu định nghĩa rõ ràng hay việc áp đặt chủ quyền theo kiểu lãnh thổ vào không gian ảo có thể gây ra "sự phân mảnh" (*fragmentation*), tạo ra các rào cản thông tin, biên giới kỹ thuật số, các vùng mạng biệt lập, và hạn chế hợp tác quốc tế; hay cơ chế quản trị internet hiện nay, bao gồm các tiêu chuẩn kỹ thuật, các giao thức mở, khối tư nhân và các thể chế xuyên quốc gia, đã hoạt động vượt trội hơn so với khuôn khổ bị kiểm soát nghiêm ngặt bởi Nhà nước[6] và việc thúc đẩy mạnh mẽ chủ quyền không gian mạng có thể làm mất đi các lợi ích quan trọng của thị trường mở, sự sáng tạo xuyên biên giới và tự do trao đổi.

Chính vì vậy, cần thảo luận thêm để làm rõ vấn đề chủ quyền không gian mạng. Thứ nhất, việc áp dụng định nghĩa, tiêu chí truyền thống của chủ quyền quốc gia đã được pháp điển trong Công ước Montevideo năm 1933 và được thừa nhận có tính tập quán, bao gồm lãnh thổ xác định, dân cư ổn định, chính quyền hữu hiệu và khả năng tham gia các quan hệ quốc tế cho chủ quyền không gian mạng có khả thi, hay cần sự áp dụng mềm dẻo, mở rộng có tính tới các đặc thù của không gian mạng như luồng dữ liệu, máy chủ hay ứng dụng phân tán vượt ngoài đường biên lãnh thổ. Thứ hai, cần giải quyết vấn đề mức độ khả thi về mặt kỹ thuật và kinh tế của việc áp đặt chủ quyền mạnh mẽ như bắt buộc lưu trữ trong nước, kiểm duyệt và quản lý nội dung mà không gây hại tới tính mở của không gian mạng và quyền tự do người dân. Thứ ba, cần giải quyết mâu thuẫn giữa lợi ích quốc gia gồm các vấn đề an ninh và kiểm soát luồng dữ liệu với việc duy trì internet như một "tài nguyên chung" (*commons*), đem lại lợi ích cho cộng đồng quốc tế, giao lưu học thuật, thương mại và văn hóa số. Cuối cùng, cần xây dựng khái niệm chủ quyền không gian mạng nhằm thúc đẩy hợp tác quốc tế và giải quyết tranh chấp liên quan về sử dụng kỹ thuật số, trong bối cảnh các quốc gia phát triển có lợi thế hơn trong việc đầu tư và áp đặt chủ quyền, trong khi các nước kém phát triển có thể bị cô lập, phụ thuộc hoặc dễ bị tổn thương.

1.2. Thực tiễn áp dụng quyền chủ quyền không gian mạng trên thế giới

Hiện nay, các "luật mềm" về chủ quyền không gian mạng như Tuyên bố tại Hội nghị thượng đỉnh thế giới về xã hội thông tin (WSIS) tại Geneva năm 2003[7] và 2005;[8] các báo cáo của Nhóm chuyên gia chính phủ Liên hợp quốc (*United Nations*

4 Johannes Thumfart, "Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory", *Journal of Global Security Studies*, Vol. 9 (1), 2024.
5 Milton Mueller, "Against Sovereignty in Cyberspace", *International Studies Review*, Vol. 22(4), 2020, tr. 779-801
6 Milton Mueller, "Open Letter to Thumfart", *School of Public Policy – Internet Governance Project*, 2024, https://www.internetgovernance.org/2024/12/31/the-debate-on-sovereignty-in-cyberspace/, truy cập ngày 20/09/2025.
7 WSIS, *Geneva Declaration of Principles Building the Information Society: a global challenge in the new Millennium*, WSIS-03/GENEVA/DOC/4-E. ITU, 2003, tr. 49.
8 WSIS, *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6(Rev. 1)-E. ITU, 2005, đoạn 35.

Groups of Governmental Experts, UNGGE) vào năm 2013,[9] 2015[10] và 2021;[11] Thông cáo Hội nghị Thượng đỉnh G20 năm 2015[12] và 2016;[13] Tuyên bố của Hội nghị Thượng đỉnh (*Brazil, Russia, India, China, South Africa,* BRICS) năm 2016;[14] và Báo cáo tóm tắt của Chủ tịch Nhóm công tác mở (*Open-Ended Working Group,* OEWG) của Liên hợp quốc[15] đã ủng hộ nguyên tắc chủ quyền trong luật quốc tế áp dụng cho không gian mạng. Nguyên tắc cũng được các quốc gia lớn tiếp cận và áp dụng trong chính sách nội bộ quốc gia. Luật Chủ quyền internet của Nga[16], xây dựng khái niệm "chủ quyền không gian mạng" là quyền tối cao của thẩm quyền chính phủ trong một quốc gia và sự độc lập của quốc gia đó trong quan hệ quốc tế.[17] Luật An ninh mạng quốc gia Trung Quốc yêu cầu địa phương hóa dữ liệu,[18] khẳng định quan điểm về "chủ quyền dữ liệu" và được coi là thành tố quan trọng góp phần bảo vệ và gìn giữ chủ quyền không gian mạng. Các quốc gia như Ấn Độ,[19] Áo,[20] Canada,[21] Phần Lan,[22] Đức,[23] hay Nhật Bản[24] cũng ủng hộ nguyên tắc chủ quyền trong luật quốc tế được áp dụng cho không gian mạng. Vương quốc Anh có quan điểm đối lập[25] cho rằng chủ quyền không gian mạng là một nguyên tắc của luật quốc tế có thể hướng dẫn tương tác giữa các quốc gia, nhưng những hoạt động trên không gian mạng không thể vi phạm chủ quyền theo các nguyên tắc của luật quốc tế.

1.3. Yêu cầu thiết lập cơ chế quản trị không gian mạng toàn cầu

Cuộc biểu tình của Gen Z[26] tại Nepal tháng 9/2025 là một tín hiệu cảnh báo rõ ràng về sự cần thiết phải định hình lại quy chế chủ quyền không gian mạng. Để củng cố "lãnh thổ kỹ thuật số", Chính phủ Nepal đã triển khai nhiều chính sách và hành động, như hoàn thiện dự luật quản lý mạng xã hội, thành lập Trung tâm An ninh mạng quốc gia và thực hiện chặn 26 nền tảng mạng xã hội của Mỹ như Facebook, Youtube... do các nền tảng này không tuân thủ quy định đăng ký và thành lập văn phòng đại diện.[27] Các biện pháp kiểm soát này đã gây gián đoạn thông tin và dấy lên lo ngại về kiểm duyệt, dẫn đến phản ứng mạnh mẽ từ Gen Z qua các cuộc biểu tình đường phố, gây bất ổn chính trị và cuối cùng buộc Chính phủ phải dỡ bỏ

9 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*, UN Doc A/68/98, 2013, đoạn 20.
10 UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/70/174, 2015, đoạn 27, 28(b).
11 United Nations General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc A /76/135, 2021, đoạn 70, 71(b).
12 G20 Leaders' Communiqué Antalya Summit on 15-16/ 11/2015, 2025, đoạn. 26.
13 G20 Digital Economy Development and Cooperation Initiative 2016 Hangzhou Summit, 2016, đoạn. 5.
14 8th BRICS Summit: Goa Declaration, Ấn Độ, 2016, đoạn 64.
15 UNGA *Chair's Summary, Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/AC.290/2021/CRP.3, 2021, đoạn 11, 20, 21 và Phụ lục.
16 Закон о «суверенном интернете» (Luật Chủ quyền Internet Liên bang Nga).
17 Katri Pynnöniemi & Martti J. Kari, "Russia's New Information Security Doctrine", *FIIA Comment, FIIA Publications*, 2016, https://fiia.fi/en/publication/russias-new-information-security-doctrine, truy cập ngày 20/09/2025.
18 Luật An ninh mạng của Cộng hòa Nhân dân Trung Hoa, ngày 07/11/2016, Điều 37.
19 Karthuka Rajmohan, "Data Localization: India's Tryst with Data Sovereignty", *Tech Policy Press,* 2025, https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/, truy cập ngày 02/10/2025.
20 Austria, Pre-Draft Report of the OEWG - ICT: Comments by Austria, Front UN, 2021.
21 Government of Canada, "International Law applicable in cyberspace", https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, truy cập ngày 02/10/2025.
22 Finland Ministry of Foreign Affairs, International law and cyberspace: Finland's national positions, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727, truy cập ngày 02/10/2025.
23 Germany, On the Application of International Law in Cyberspace: Position Paper, 2021.
24 Ministry of Foreign Affairs of Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 2021.
25 UK Government, *Cyber and International Law in the 21st Century*, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, truy cập ngày 02/10/2025.
26 Gen Z (Generation Z) hay Thế hệ Z là thế hệ sinh từ khoảng 1997 đến 2012, là thế hệ đầu tiên lớn lên với sự tiếp cận Internet cùng các thiết bị kỹ thuật số và điện tử từ nhỏ, còn được mệnh danh là những "công dân thời đại kĩ thuật".
27 Reuters, "Nepal to block some social media including Facebook", https://www.reuters.com/article/nepal-social-media-ban-2025-09-04/, truy cập ngày 21/09/2025.

lệnh cấm. Qua đây, có thể thấy việc thiết lập chủ quyền không gian mạng phải cân bằng mối quan hệ giữa nhà nước, công dân và cộng đồng quốc tế, đồng thời phải xây dựng khung pháp luật rõ ràng kết hợp với hệ thống thực thi pháp luật minh bạch.

Nhằm thiết lập quy chế chủ quyền không gian mạng, các học giả Trung Quốc đưa ra lý thuyết bốn cấp độ quản trị như một giải pháp mềm dẻo cân bằng hai học thuyết phi chủ quyền và chủ quyền không gian mạng. Theo các tác giả, khái niệm chủ quyền mạng được định nghĩa là mở rộng của chủ quyền quốc gia sang môi trường mạng, với quyền nội bộ (*internal supremacy*) và độc lập bên ngoài (*external independence*) đối với hạ tầng, các thực thể, hành vi mạng, dữ liệu, thông tin nằm trong lãnh thổ quốc gia. Chủ quyền trên không gian mạng sẽ bao gồm các quyền lập pháp, hành chính, tư pháp để điều tiết và bảo vệ trong không gian mạng. Khi thực thi chủ quyền trên không gian mạng, quốc gia không chỉ có quyền mà còn có nghĩa vụ không xâm phạm chủ quyền của nước khác, không can thiệp vào công việc nội bộ của quốc gia khác qua mạng, và có nghĩa vụ thực hành quản trị không gian mạng với mức độ phù hợp.[28] Các nguyên tắc căn bản cho chủ quyền trên không gian mạng cũng là các nguyên tắc cơ bản của luật quốc tế quy định trong Hiến chương Liên hợp quốc được áp dụng trong hoàn cảnh đặc thù của không gian mạng như bình đẳng giữa các quốc gia; công bằng, bảo vệ lợi ích của các nước đang phát triển; hợp tác giữa các quốc gia; hòa bình, không sử dụng công nghệ thông tin để gây bất ổn, tránh chạy đua vũ khí mạng, ưu tiên giải quyết tranh chấp qua biện pháp hòa bình; và pháp trị, xây dựng luật pháp trong nước và thúc đẩy pháp trị trong quản trị không gian mạng toàn cầu, tôn trọng luật quốc tế và phản đối tiêu chuẩn kép.

Từ đó, việc quản trị chủ quyền không gian mạng có thể chia thành bốn tầng, bao gồm:[29] (i) Tầng hạ tầng vật lý (*physical infrastructure*), gồm các đường mạng và hạ tầng kỹ thuật số trong lãnh thổ quốc gia; (ii) Tầng tiêu chuẩn đảm bảo tương thích (*logic layer*), liên quan đến các giao thức mạng, tiêu chuẩn kỹ thuật và mã hóa, cho phép quốc gia ban hành quy định riêng không mâu thuẫn với nghĩa vụ quốc tế; (iii) Tầng ứng dụng (*application layer*), gồm phần mềm, nền tảng, nội dung, và dữ liệu, tập trung vào việc kiểm soát nội dung, bảo vệ dữ liệu và quy định hoạt động của các nền tảng xuyên biên giới; và (iv) Tầng xã hội (*social layer*), liên quan đến người dùng, văn hóa trực tuyến, trách nhiệm xã hội và việc định hình nhận thức cộng đồng, cũng như đảm bảo quyền lợi của công dân trên mạng.

Theo quan điểm của nhóm tác giả, mô hình này là một giải pháp tối ưu để thực hiện quản trị không gian mạng khi đã dung hòa giữa nhu cầu duy trì chủ quyền, trật tự xã hội của nhà nước với một môi trường mở cần thiết cho hoạt động kinh tế, giao tiếp và xã hội của người dân và doanh nghiệp. Đồng thời mô hình quản trị này cũng gợi mở các biện pháp chiến lược như phát triển khung hợp tác quốc tế dựa trên tôn trọng chủ quyền, xây dựng chuẩn mực quốc tế mạnh mẽ để điều tiết các hoạt động mạng xuyên biên giới, tăng cường khả năng kỹ thuật và pháp lý của các quốc gia đang phát triển, đồng thời khuyến khích kinh tế số nội địa nhưng vẫn đảm bảo mở cửa.

2. Thực tiễn quyền chủ quyền không gian mạng tại Việt Nam

2.1. Những thành tựu về xây dựng chủ quyền không gian mạng tại Việt Nam

Với những tiến bộ của công nghệ thông tin, không gian mạng hiện nay đang phát triển với tốc độ chưa từng thấy, với 5,56 tỷ người dùng internet và số lượng

28 World Internet Conference, Sovereignty in Cyberspace: Theory and Practice (Version 4.0), 2024
29 *Như trên*.

người dùng tăng trưởng là 2,5% mỗi năm.[30] Hiện nay, Việt Nam có 79,8 triệu người có kết nối internet, trong đó có 76,2 triệu người sử dụng mạng xã hội, tương đương 75,2% tổng dân số.[31] Trong những năm gần đây, Việt Nam đã có nhiều nỗ lực và đạt được những kết quả quan trọng trong việc củng cố chủ quyền quốc gia trên không gian mạng.

Về xây dựng và hoàn thiện khung pháp lý, Việt Nam đã ban hành nhiều văn bản quan trọng tạo cơ sở pháp lý vững chắc cho việc quản lý không gian mạng. Luật An ninh mạng năm 2018 là văn bản luật đầu tiên điều chỉnh toàn diện vấn đề an ninh mạng quốc gia và lần đầu đưa ra định nghĩa không gian mạng.[32] Bên cạnh đó, Việt Nam còn ban hành Luật An toàn thông tin mạng năm 2015 (được hoàn thiện thêm vào năm 2018), Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân 2025 và văn bản dưới luật như Nghị định 142/2016/NĐ-CP về ngăn chặn xung đột thông tin trên mạng, Nghị định 91/2020/NĐ-CP về chống thư rác, tin nhắn rác, Nghị định 53/2022/NĐ-CP hướng dẫn Luật An ninh mạng yêu cầu về lưu trữ dữ liệu trong nước, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (được thay thế bởi Nghị định 356/2025/NĐ-CP hướng dẫn Luật Bảo vệ dữ liệu cá nhân) hay Nghị định 147/2024/NĐ-CP quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng. Nhìn chung, các quy định này thể hiện xu thế áp dụng các biện pháp quản trị theo mô hình bốn tầng được nêu trên, tạo hành lang pháp lý cơ bản, giúp Nhà nước thực thi chủ quyền không gian mạng một cách chủ động và chặt chẽ.

Về phát triển hạ tầng và năng lực kỹ thuật, Việt Nam đã đầu tư đáng kể vào hạ tầng viễn thông và công nghệ thông tin, với mạng lưới internet băng thông rộng phủ khắp và các trung tâm dữ liệu quy mô lớn đã được thiết lập. Các đơn vị chuyên trách về an ninh mạng được thành lập và củng cố như có Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an giữ vai trò nòng cốt bảo vệ an ninh mạng quốc gia và Bộ Tư lệnh tác chiến không gian mạng thuộc Bộ Quốc phòng làm nhiệm vụ tác chiến bảo vệ tổ quốc trên không gian mạng. Nhờ những nỗ lực này, năng lực ứng phó và phòng thủ không gian mạng của Việt Nam đã được nâng cao đáng kể, thể hiện qua việc phát hiện và ngăn chặn nhiều cuộc tấn công vào hệ thống thông tin quan trọng mỗi năm.

Về hợp tác quốc tế, Việt Nam tích cực tham gia các diễn đàn và sáng kiến quốc tế về an ninh mạng nhằm vừa học hỏi kinh nghiệm, vừa đóng góp vào nỗ lực chung bảo vệ không gian mạng, tiêu biểu như việc hợp tác với các nước ASEAN để chủ động phòng, chống tội phạm mạng xuyên quốc gia.[33] Việt Nam đăng cai Lễ mở ký Công ước "Hà Nội" của Liên hợp quốc về chống tội phạm mạng vào tháng 10 năm 2025,[34] khẳng định vai trò định hình khung pháp lý không gian mạng toàn cầu và đánh dấu lần đầu tiên có một điều ước quốc tế mang tên Việt Nam.

2.2. Tác động của những thách thức toàn cầu của sự phát triển không gian mạng tới Việt Nam

Tuy Việt Nam có nhiều thành tựu trong xây dựng chủ quyền không gian mạng, song thực tiễn đảm bảo chủ quyền không gian mạng trên thế giới và trong nước vẫn đứng trước nhiều thách thức phức tạp.

30 DataReportal, "Global digital overview", https://datareportal.com/global-digital-overview, truy cập ngày 23/09/2025.
31 Simon Kemp, "Digital 2025: Vietnam", *DataReportal*, 2025.
32 Luật số 24/2018/QH14 ngày 12/06/2018 về an ninh mạng, khoản 3 Điều 2.
33 Nguyễn Việt Lâm, *Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam*, Nxb Chính trị quốc gia Sự thật, Hà Nội, 2019, tr. 190-194.
34 Hanoi Convention, Model Conference of the Parties to the United Nations Convention against Cybercrime, 2025.

2.2.1. Những thách thức toàn cầu

Về mặt chính trị và an ninh, xung đột và gián điệp trên không gian mạng đang leo thang với mức độ tinh vi cao, đe dọa an ninh quốc gia. Với những tính chất đặc biệt, như hoạt động quy mô lớn, chi phí thấp và khó bị phát hiện,[35] gián điệp và chiến tranh mạng không chỉ là một mặt trận chiến lược mà còn là một yếu tố quyết định trong chiến tranh hiện đại. Đơn cử là việc Trung Quốc sử dụng "Tam chủng chiến pháp" (*China's three warfares*) để lèo lái dư luận quốc tế[36] hay việc sử dụng mạng xã hội trong các phong trào chính trị như "Mùa xuân Ả Rập" trong việc tổ chức biểu tình và thay đổi chính quyền.[37] Không gian mạng đang được sử dụng như công cụ chủ chốt trong việc chuyển hóa chế độ chính trị và can thiệp vào bầu cử thông qua thao túng thông tin trên mạng, tác động mạnh mẽ đến tâm lý xã hội, ảnh hưởng trực tiếp đến tính minh bạch và ổn định chính trị của nhiều quốc gia.

Về kinh tế - xã hội, sự phân mảnh của internet do các quốc gia áp dụng chủ quyền không gian mạng có nguy cơ phá vỡ tính thống nhất của hệ sinh thái số toàn cầu, khi các "tường lửa kỹ thuật số" và cơ chế kiểm soát dữ liệu quốc gia gây trở ngại cho dòng chảy thông tin, giao thương số và ảnh hưởng trực tiếp đến nền kinh tế số.[38] Việc thiết lập chủ quyền không gian mạng đặt ra những thách thức nghiêm trọng đối với quyền con người, đặc biệt là quyền riêng tư, làm suy giảm quyền truy cập thông tin và tạo ra nguy cơ vi phạm nếu không có những quy định cụ thể.[39]. Ngoài ra, những rào cản về kỹ thuật và hạ tầng công nghệ thông tin (ICT) ngày càng trở nên phức tạp, đặc biệt là vấn đề không tương thích trong tiêu chuẩn kỹ thuật và quản trị dữ liệu xuyên biên giới.[40] Bên cạnh đó, cuộc cạnh tranh về kỹ thuật bán dẫn và viễn thông giữa Mỹ và Trung Quốc có thể dẫn đến hai hệ thống tiêu chuẩn kỹ thuật mạng khác biệt, buộc các quốc gia phải "chọn phe" và làm trầm trọng thêm sự bất bình đẳng trong nền kinh tế số.[41]

2.2.2. Những tác động tiêu cực đến Việt Nam

Tại Việt Nam, việc đảm bảo chủ quyền không gian mạng cũng đối mặt với những thách thức đặc thù.

Thứ nhất, thách thức từ dòng chảy dữ liệu xuyên biên giới. Trước năm 2022, phần lớn dữ liệu cá nhân người Việt được lưu trữ và xử lý trên máy chủ nước ngoài, khiến cơ quan chức năng Việt Nam khó kiểm soát và phải phụ thuộc vào thiện chí hợp tác hoặc cơ chế tương trợ tư pháp quốc tế phức tạp khi xảy ra vi phạm. Luật An ninh mạng năm 2018 và Nghị định 53/2022 yêu cầu các công ty nước ngoài phải đặt máy chủ trong nước,[42] song việc thực thi gặp thách thức do các tập đoàn công nghệ lo ngại chi phí lớn và xung đột với chính sách bảo mật dữ liệu nước họ.[43] Bên cạnh đó, vấn đề tội phạm mạng cũng là một vấn đề

35 Lu Chuanying, "Bullying Empire: US promotes 'digital colonialism' to maintain hegemony, exposes American democracy hypocrisy" *Global Times*, 2023 https://www.globaltimes.cn/page/202306/1293413.shtml, truy cập ngày 20/09/2025.

36 Peter Mattis, "China's 'Three Warfares' in Perspective", *War on the rock*, 2018

37 Radsch, C., "Digital Dissidence and Political Change: Cyberactivism and Citizen Journalism in Egypt", *American University, School of International Service*, 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379913; Ryan, Y., "Tunisia's bitter cyberwar", *Al Jazeera,* 2011, http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html, truy cập ngày 19/09/2025.

38 Milton L. Mueller, "Will the Internet fragment? Sovereignty, globalization and cyberspace", *Cambridge: Polity Press*, Vương quốc Anh, 2017, tr. 45-60.

39 Adrian Shahbaz, Allie Funk, Andrea Hackl, "User Privacy or Cyber Sovereignty?", *Freedom House*, 2020.

40 Nguyễn Việt Lâm, "Chủ quyền không gian mạng: Lý thuyết, thực tiễn trong quan hệ quốc tế và những vấn đề đặt ra hiện nay", *Tạp chí Cộng sản,* 2021.

41 Helen Dixon, "Regulate to Liberate Can Europe Save the Internet", *Foreign Affair*, Vol. 97 (5), 2018, tr. 28.

42 Luật An ninh mạng số 24/2018/QH14, ngày 12/06/2019, Điều 26.3; và Nghị định 53/2022/NĐ-CP hướng dẫn Luật An ninh mạng, ngày 15/08/2022.

43 James Fox,"How Are Foreign Investors Responding to Vietnam's New Data Localization Regulation", *Vietnam Briefing,* 2022; Francesco Guarascio, Phuong Nguyen,"US tech firms warn Vietnam's planned law to hamper data

xã hội nhức nhối khi thông tin cá nhân bị đánh cắp, tiết lộ trái phép, trở thành tài sản bị mua bán tràn lan, với tổng thiệt hại do lừa đảo trực tuyến ước tính lên tới 8.000-10.000 tỷ đồng.[44] Các sự cố lớn gần đây như cuộc tấn công *ransomware* vào Công ty Chứng khoán VNDirect hay sự cố đánh cắp dữ liệu cá nhân tại Trung tâm Thông tin tín dụng quốc gia[45] cho thấy sự dễ tổn thương của các hệ thống lưu trữ dữ liệu, tiềm ẩn nguy cơ gây mất ổn định xã hội và kinh tế vĩ mô.

Thứ hai, nguy cơ từ các cuộc tấn công mạng và gián điệp mạng ngày càng gia tăng. Chỉ trong Quý I năm 2025, Việt Nam đã ghi nhận hơn 257.000 cuộc tấn công từ chối dịch vụ (DDoS), phát hiện 36 lỗ hổng bảo mật nghiêm trọng và hơn 4,5 triệu thông tin tài khoản bị đánh cắp, chiếm khoảng 12,9% tổng số tài khoản bị lộ toàn cầu.[46] Những con số này cho thấy Việt Nam nằm trong nhóm mục tiêu hàng đầu của tội phạm mạng quốc tế, đặt ra yêu cầu cấp bách phải nâng cao hơn nữa năng lực phòng thủ. Ngoài ra, tình trạng phát tán thông tin bịa đặt, xuyên tạc đường lối, chủ trương, chính sách của Đảng và Nhà nước, công kích chế độ, kích động, chia rẽ khối đại đoàn kết dân tộc của các tổ chức phản động ở nước ngoài diễn ra phức tạp, khiến dư luận hoang mang, tác động tiêu cực đến trật tự, an ninh xã hội và làm suy giảm niềm tin của người dân vào các cơ quan chức năng.[47]

Cuối cùng là sự chi phối lớn của các công ty công nghệ toàn cầu đối với không gian mạng Việt Nam, khi hầu hết người dân sử dụng các nền tảng và dịch vụ nước ngoài như Facebook, YouTube, Google, TikTok. Sự phụ thuộc vào các nền tảng này tạo ra điểm yếu về chủ quyền nội dung và dữ liệu khi đây là những kênh truyền bá nhanh chóng các thông tin xấu độc, tin giả, nội dung vi phạm pháp luật Việt Nam. Chính phủ đã nhiều lần yêu cầu các nền tảng này gỡ bỏ thông tin xuyên tạc, chống phá Đảng và Nhà nước, hoặc các video độc hại, với gần 16.000 nội dung vi phạm pháp luật tại Việt Nam được gỡ bỏ trong năm 2024.[48] Bên cạnh vấn đề nội dung, cạnh tranh kinh tế số cũng là thách thức khi các doanh nghiệp số Việt Nam khó cạnh tranh với "gã khổng lồ" toàn cầu ngay tại thị trường nội địa, tiêu biểu với việc ra mắt mạng xã hội Lotus năm 2019, với vốn đầu tư 1.200 tỷ đồng cùng tham vọng cạnh tranh và thay thế Facebook, song dự án "Made in Vietnam" này vẫn thất bại trong việc thay đổi thói quen người dùng.[49] Việc cân bằng giữa tận dụng lợi ích từ dịch vụ xuyên biên giới và kiểm soát ảnh hưởng của chúng là bài toán nan giải trong thực thi chủ quyền không gian mạng tại Việt Nam.

3. Những vấn đề pháp lý đặt ra và giải pháp cho Việt Nam

3.1. Vấn đề định nghĩa và phạm vi chủ quyền không gian mạng

Tuy Việt Nam đã xây dựng khung pháp lý cho việc quản lý không gian mạng, các văn bản này lại thể hiện tính phân mảnh khi các nội dung về quản lý dữ liệu, hạ tầng, nội dung và an ninh mạng nằm rải rác ở nhiều luật và nghị định khác nhau,

centres, social media", *Reuters,* 2024.

44 Huyền Trang, Thu Thuỷ, "Ngăn chặn tình trạng lừa đảo qua không gian mạng", *Báo Quân đội Nhân dân*, 2024, https://www.qdnd.vn/phap-luat/cac-van-de/ngan-chan-tinh-trang-lua-dao-qua-khong-gian-mang-bai-1-mu-on-kieu-lua-dao-802621, truy cập ngày 21/09/2025.

45 Ngày 24/03/2024, Công ty Chứng khoán VNDirect tại Việt Nam bị tấn công bởi mã độc tống tiền (ransomware) và phải ngừng hoạt động nhiều ngày; Ngày 10/09/2025, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) nhận được báo cáo sự cố an ninh mạng và dấu hiệu vi phạm dữ liệu cá nhân xảy ra tại Trung tâm Thông tin tín dụng quốc gia (CIC).

46 Ngọc Diệp, "Những xu hướng tấn công mạng mới và chiến lược ứng phó", *Tạp chí Khoa học & Công Nghệ,* 2025.

47 Hoàng Quốc Cảnh, Nguyễn Hương Hạnh, Đỗ Thị Mỹ Dung, "Vạch trần phương thức, thủ đoạn lợi dụng mạng xã hội Facebook để xuyên tạc, chống phá Đảng và Nhà nước Việt Nam", *Tạp chí Cộng sản,* 2024.

48 Lê Mỹ, "Gần 16.000 nội dung vi phạm đã được gỡ bỏ trên các nền tảng xuyên biên giới", *Báo điện tử Vietnamnet,* 2025, https://vietnamnet.vn/gan-16-000-noi-dung-vi-pham-da-duoc-go-bo-tren-cac-nen-tang-xuyen-bien-gioi-2359105.html, truy cập ngày 21/09/2025.

49 Phương Linh, "Được đầu tư 1.200 tỷ đồng, mạng xã hội Lotus giờ ra sao?", *Tạp chí điện tử Nhà đầu tư,* 2021.

gây khó khăn trong việc xác lập thẩm quyền và xử lý vi phạm. Hơn nữa, dù đã có các chủ trương chính sách về bảo vệ an ninh và xây dựng không gian mạng quốc gia, vẫn chưa có văn bản quy phạm nào trực tiếp xác định đầy đủ và rõ ràng các yếu tố cấu thành chủ quyền không gian mạng quốc gia. Định nghĩa về chủ quyền không gian mạng mới chỉ được giải thích lần đầu là "tất cả các quyền của nhà nước đối với không gian mạng, phù hợp với quy định của luật pháp quốc tế".[50] Khi các khái niệm và phạm vi chưa rõ ràng, chế tài xử lý hành vi vi phạm hoặc tranh chấp phát sinh còn nhiều trở ngại.

Trong bối cảnh đó, thể chế, pháp luật chuyên sâu, toàn diện về chủ quyền không gian mạng là vấn đề ưu tiên, nhằm tạo nền tảng pháp lý vững chắc và thống nhất cho mọi hoạt động quản lý nhà nước. Việt Nam cần sớm ban hành khung pháp lý chuyên biệt nhằm định nghĩa rõ khái niệm chủ quyền không gian mạng, xác lập các nguyên tắc bảo vệ chủ quyền quốc gia trên không gian mạng, quy định các biện pháp kỹ thuật, hành chính và hình sự để ngăn chặn, xử lý các hành vi vi phạm. Bên cạnh đó, cần làm rõ hơn các thành tố cấu thành chủ quyền không gian mạng như kỹ thuật, dữ liệu hay nội dung và mối quan hệ, ranh giới giữa chúng, nhằm xác định trách nhiệm của Nhà nước, doanh nghiệp và công dân. Ví dụ, pháp luật cần quy định cụ thể trách nhiệm của doanh nghiệp trong nước và nước ngoài về đảm bảo an ninh cho hệ thống hạ tầng do họ vận hành; hay quyền và trách nhiệm của người dùng trong việc sử dụng không gian mạng an toàn, tuân thủ pháp luật. Việc xây dựng khung pháp lý vững chắc sẽ tạo nền tảng thuận lợi để triển khai các chính sách phát triển kinh tế và xã hội trong môi trường số.

3.2. Vấn đề thẩm quyền tài phán trong không gian mạng

Không gian mạng có tính xuyên biên giới, phi vật thể, nên việc áp dụng các nguyên tắc thẩm quyền truyền thống của luật pháp quốc tế gặp nhiều khó khăn. Pháp luật Việt Nam đang đối diện với vấn đề xác định thẩm quyền của tòa án hoặc cơ quan chức năng để xử lý các hành vi vi phạm pháp luật trên không gian mạng, đặc biệt nếu hành vi đó liên quan tới nhiều quốc gia. Bộ luật Hình sự Việt Nam năm 2015 đã có điều khoản về tội phạm sử dụng mạng máy tính, mạng viễn thông[51] và nguyên tắc hình phạt áp dụng ngoài lãnh thổ đối với tội xâm phạm an ninh quốc gia hoặc các tội mà Việt Nam theo điều ước quốc tế có nghĩa vụ tài phán. Tuy nhiên, trong thực tiễn điều tra, truy tố các vụ án trên không gian mạng phức tạp liên quan yếu tố nước ngoài, các cơ quan chức năng gặp không ít trở ngại, chủ yếu do khó khăn trong thu thập chứng cứ điện tử quốc tế thông qua ủy thác tư pháp và dẫn độ bị can phụ thuộc vào hiệp định quốc tế. Hiện nay đã có những quốc gia trước đây chưa từng dẫn độ tội phạm cho nước khác nhưng gần đây phải hợp tác với Việt Nam để đưa tội phạm lừa đảo xuyên biên giới ra chịu trách nhiệm.[52]

Để ứng phó hiệu quả với tội phạm mạng quốc tế, Việt Nam cần xây dựng một khuôn khổ pháp lý linh hoạt hơn cho hoạt động điều tra và xét xử. Trước hết, pháp luật trong nước nên quy định rõ thẩm quyền mở rộng của tòa án Việt Nam đối với các hành vi trên không gian mạng gây hậu quả tại lãnh thổ Việt Nam hoặc đối với công dân Việt Nam, kể cả khi đối tượng phạm tội cư trú ở nước ngoài. Đồng thời, cần thiết lập cơ chế pháp lý cho phép truy vết và chia sẻ dữ liệu nhanh chóng, hiệu quả giữa các cơ quan thực thi pháp luật trong nước và đối tác quốc tế, đặc biệt trong các tình huống khẩn cấp Việt Nam có thể tham khảo các kinh nghiệm quốc

50 Nghị định 142/2016/NĐ-CP ngày 14/10/2016 về ngăn chặn xung đột thông tin trên mạng, khoản 6 Điều 3.
51 Luật số 100/2015/QH13 ngày 27/11/2015 Bộ luật Hình sự (Bộ luật Hình sự), Điều 290.
52 Phương Thuỷ, "Có những nước chưa bao giờ dẫn độ tội phạm sang nước khác nhưng đã hợp tác với Việt Nam", *Công an Nhân dân*, 2024.

tế, như Trung Quốc yêu cầu các nhà cung cấp dịch vụ hợp tác với cơ quan chức năng trong điều tra tội phạm, cho phép truy cập dữ liệu và cung cấp hỗ trợ kỹ thuật khi có yêu cầu chính thức.[53] Mặt khác, Việt Nam cũng nên chủ động tham gia các điều ước quốc tế về hỗ trợ tư pháp và dẫn độ trong lĩnh vực tội phạm công nghệ cao như Công ước Hà Nội nhằm hình thành cơ sở pháp lý vững chắc cho hợp tác tài phán về tội phạm mạng.

3.3. Vấn đề chủ quyền dữ liệu

Dữ liệu được ví như "tài nguyên" của mỗi quốc gia trong kỷ nguyên số.[54] Việc kiểm soát dữ liệu, đặc biệt là dữ liệu cá nhân và dữ liệu quan trọng liên quan đến an ninh quốc gia, là một nội dung cốt lõi của chủ quyền không gian mạng. Pháp luật Việt Nam đang trong quá trình định hình cơ chế pháp lý về chủ quyền dữ liệu, bao gồm hai khía cạnh: bảo vệ dữ liệu cá nhân và nội địa hóa dữ liệu. Việt Nam đã bước đầu xây dựng khung pháp lý về bảo vệ dữ liệu cá nhân, đáp ứng các yêu cầu bảo vệ quyền riêng tư và ngăn chặn các hành vi xâm phạm dữ liệu cá nhân, gây ảnh hưởng đến quyền và lợi ích của công dân Việt Nam. Tuy nhiên, khái niệm về chủ quyền dữ liệu quốc gia, tức quyền của Nhà nước trong việc quản lý dữ liệu do tổ chức, cá nhân Việt Nam tạo ra lại chưa được luật hóa cụ thể và việc hài hòa yêu cầu chủ quyền dữ liệu của Việt Nam với mô hình kinh doanh toàn cầu của các doanh nghiệp nước ngoài cũng là một thách thức. Việc yêu cầu lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam chỉ áp dụng khi doanh nghiệp vi phạm hoặc không hợp tác xử lý vi phạm.[55]

Việt Nam có thể học hỏi kinh nghiệm từ các quốc gia khác như Trung Quốc, yêu cầu thiết lập hệ thống quản lý an ninh nội bộ, áp dụng các biện pháp kỹ thuật nhằm ngăn chặn tấn công mạng[56] và yêu cầu không được chuyển dữ liệu quan trọng ra nước ngoài.[57] Việc địa phương hóa dữ liệu (*data localisation*) khẳng định quan điểm về "chủ quyền dữ liệu" và được coi là thành tố quan trọng góp phần bảo vệ và gìn giữ chủ quyền không gian mạng của quốc gia.[58] Việc xây dựng cơ chế pháp lý rõ ràng, bình đẳng sẽ cân bằng việc bảo vệ được dữ liệu người Việt và không tạo gánh nặng cho doanh nghiệp quốc tế.

3.4. Vấn đề quản lý nội dung trên không gian mạng

Như đã phân tích ở trên, sự lan truyền của nhiều loại nội dung vi phạm pháp luật trên không gian mạng là một trong những thách thức lớn hiện nay. Từ những bài học của Bangladesh, Indonesia, Nepal gần đây, để kiểm soát rủi ro "cách mạng màu" và bảo đảm chủ quyền không gian mạng,[59]–Việt Nam cần thiết lập một cơ chế pháp lý rõ ràng và linh hoạt trong quản lý nội dung trực tuyến. Pháp luật hiện hành đã quy định thời hạn 24 giờ và các biện pháp cưỡng chế như khóa tài khoản, kênh vi phạm đối với các nền tảng mạng xã hội quốc tế khi có yêu cầu từ phía Việt

53 Wagner, J., "China's Cybersecurity Law: What You Need to Know", *The Diplomat,* 2017.

54 Nghị quyết 57-NQ/TW về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia ngày 22/12/2024.

55 Nghị định 53/2022, khoản 3 Điều 26.

56 Luật An ninh mạng của Cộng hòa Nhân dân Trung Hoa, Điều 21.

57 *Như trên*, Điều 37.

58 Nguyễn Việt Lâm, *tlđd*.

59 Tại Bangladesh (2024), phong trào khởi nguồn từ sự phẫn nộ đối với hệ thống quota công chức bất công thông qua các cuộc tuần hành, tọa kháng và tuyên truyền trên mạng xã hội mang khẩu hiệu "No Quota, Only Merit" ("Không đặc quyền, chỉ năng lực"), sau đó leo thang thành cuộc nổi dậy toàn dân lật đổ Thủ tướng Sheikh Hasina sau 15 năm cầm quyền; Tại Indonesia, làn sóng biểu tình và bạo loạn bùng phát từ sự phẫn nộ trước chính sách tăng đặc quyền cho giới nghị sĩ trong bối cảnh kinh tế khó khăn, mà ngòi nổ trực tiếp là những hình ảnh bạo lực về cái chết của một tài xế trẻ do cảnh sát gây ra được lan truyền chóng mặt trên mạng xã hội; Tại Nepal (2025), Discord, Telegram và các nhóm mã hóa trở thành kênh huy động và điều phối biểu tình, thay thế hoàn toàn cho mạng xã hội bị phong tỏa bởi lệnh cấm, đã châm ngòi cho làn sóng biểu tình bạo động khiến Thủ tướng KP Sharma Oli phải từ chức. Các sự kiện đều cho thấy một kịch bản chung: thế hệ trẻ đã sử dụng mạng xã hội và các công cụ vượt rào cản internet như "hạ tầng chính trị" để điều phối, lan tỏa thông điệp và lật đổ chính quyền.

Nam,[60] đồng thời có những chế tài trong xử lý việc tuyên truyền chống phá Nhà nước hoặc lợi dụng quyền tự do dân chủ xâm phạm lợi ích Nhà nước.[61] Tuy nhiên, pháp luật cần có chế tài nghiêm khắc nếu các nền tảng không tuân thủ yêu cầu. Đồng thời, quy trình quản lý nội dung phải minh bạch, khách quan để tránh lạm dụng và xâm phạm quyền tự do ngôn luận chính đáng của người dân.

Để giải quyết vấn đề này, việc quản lý nội dung đòi hỏi pháp luật phải cân bằng giữa hiệu quả quản lý và quyền tự do thông tin, đồng thời cần có cơ chế giám sát độc lập và trách nhiệm giải trình từ phía cơ quan thực thi để tránh lạm quyền. Việt Nam cần thiết lập một nhóm công tác gồm các chuyên gia pháp lý và truyền thông để tư vấn cho cơ quan quản lý về việc đánh giá nội dung nhạy cảm. Khi áp dụng các biện pháp kỹ thuật như lọc hoặc chặn website, cần có quy định đảm bảo việc này không gây ảnh hưởng đến hoạt động kinh tế - xã hội trên mạng. Bên cạnh đó, Việt Nam cũng cần chú trọng đào tạo và nâng cao nhận thức người dân trong cách xử lý và phản ứng một cách phù hợp trước các nội dung trên mạng, nhằm tăng cường kỹ năng số và khả năng tự bảo vệ trước các tác động tiêu cực từ môi trường trực tuyến.

3.5. Vấn đề áp dụng luật quốc tế trong không gian mạng

Hiện tại, chưa có một khung pháp lý quốc tế thống nhất để điều chỉnh chủ quyền không gian mạng, dẫn đến nhiều thách thức trong quản lý, bảo vệ an ninh và giải quyết tranh chấp giữa các quốc gia trên không gian này. Điều này tạo cơ hội cho các hành vi vi phạm luật pháp quốc tế gia tăng và đe dọa sự ổn định của trật tự toàn cầu. Việc lợi dụng không gian mạng để truyền bá các tư tưởng chính trị phản động không chỉ làm gia tăng nguy cơ bất ổn, mà còn có thể dẫn đến các cuộc "cách mạng màu" như ở Ukraine năm 2014, "cách mạng hoa hướng dương" ở Đài Loan, Trung Quốc, "cách mạng nghệ tây" ở Myanmar năm 2007, "cách mạng xanh" ở Iran năm 2009[62] và cách mạng "Gen Z" tại Nepal năm 2025. Không những vậy, việc thực thi chủ quyền không gian mạng tiềm ẩn nguy cơ làm gia tăng sự bất đồng, tranh chấp và thậm chí xung đột, làm gia tăng căng thẳng giữa các quốc gia, có thể làm thay đổi cấu trúc quyền lực toàn cầu và đặt ra thách thức nghiêm trọng đối với hệ thống luật quốc tế hiện hành.

Trong bối cảnh đó, Việt Nam cần chủ động tham gia trao đổi, thảo luận, đàm phán và đề xuất các nguyên tắc pháp lý về quyền tài phán trên không gian mạng, an ninh mạng và xử lý vi phạm chủ quyền không gian mạng. Việt Nam có thể tận dụng các diễn đàn quốc tế để thể hiện lập trường quốc gia về bảo vệ chủ quyền, lợi ích quốc gia - dân tộc trên không gian mạng, qua đó góp phần đóng góp vào quá trình nghiên cứu, xây dựng và củng cố nội hàm về chủ quyền không gian mạng. Bên cạnh đó, Việt Nam cũng cần tích cực tham gia vào quá trình xây dựng, soạn thảo và ủng hộ sự phát triển các điều ước quốc tế về hoạt động tội phạm mạng gây đe dọa đến an ninh và chủ quyền quốc gia.[63] Việc chủ động đóng góp vào quá trình xây dựng cơ chế pháp lý toàn cầu giúp củng cố vị thế quốc gia trong thời đại chuyển đổi số toàn cầu và tạo điều kiện thuận lợi để Việt Nam bảo vệ chủ quyền và an ninh không gian mạng một cách chủ động và phù hợp với luật pháp quốc tế.

60 Nghị định 147/2024/NĐ-CP ngày 09/11/2024 quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng, Điều 23.5(b).
61 Bộ luật Hình sự, Điều 117 và Điều 331.
62 Ministry of Public Security of Peoples's Republic of China, Exclusive: New Report Unveils How CIA Scheme Color Revolutions Around the World, 2023.
63 Nguyễn Việt Lâm, *tlđd*, 2021.

Kết luận

Chủ quyền không gian mạng là yếu tố then chốt để đảm bảo an ninh quốc gia và thúc đẩy phát triển bền vững của Việt Nam trong kỷ nguyên số. Tuy Việt Nam đã đạt được một số thành tựu quan trọng trong xây dựng khung pháp lý, củng cố hạ tầng kỹ thuật và mở rộng hợp tác quốc tế, những thách thức và đe dọa từ không gian mạng vẫn ngày càng phát triển. Để củng cố chủ quyền không gian mạng, Việt Nam cần triển khai một cách toàn diện và linh hoạt các chính sách pháp luật, các giải pháp kỹ thuật, và tăng cường hợp tác quốc tế. Đặc biệt, phải luôn đảm bảo hài hòa giữa yêu cầu bảo vệ chủ quyền, an ninh với việc tôn trọng các quyền, lợi ích hợp pháp của người dân và doanh nghiệp, tạo sự đồng thuận trong xã hội. Với cách tiếp cận phù hợp, Việt Nam sẽ giữ vững chủ quyền quốc gia trước những biến động khó lường của thời đại số, đồng thời tận dụng được tối đa cơ hội mà chuyển đổi số và kinh tế số mang lại cho sự phát triển của đất nước. ●

Tài liệu tham khảo

[1] Tô Lâm, *Chủ quyền không gian mạng: Yêu cầu thời đại và nghĩa vụ quốc gia*, Nxb. Công an Nhân dân, Hà Nội, 2021 [trans: To Lam, *Sovereignty in cyberspace: Contemporary requirements and national obligations,* People's Public Security Publishing House, Hanoi, 2021]

[2] Nguyễn Việt Lâm, *Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2019 [trans: Nguyen Viet Lam, *Cybersecurity policy in contemporary international relations and Vietnam's responses,* National Political Publishing House – Truth, Hanoi, 2019]

[3] Nguyễn Việt Lâm, "Chủ quyền không gian mạng: Lý thuyết, thực tiễn trong quan hệ quốc tế và những vấn đề đặt ra hiện nay", *Tạp chí Cộng sản*, 2021 [trans: Nguyen Viet Lam, "Sovereignty in cyberspace: Theory and practice in international relations and contemporary challenges", *Communism Journal,* 2021]

[4] Manuel Castells, *The rise of the network society,* Wiley-Blackwell, Vương quốc Anh, 2010

[5] Johannes Thumfart, *The Liberal Internet in the Postliberal Era: Digital Sovereignty, Private Government, and Practices of Neutralization*, Springer Naure Switzerland, Thuỵ Sỹ, 2024

[6] Johannes Thumfart, "Digital rights and the state of exception. internet shutdowns from the perspective of just securitization theory", *Journal of Global Security Studies,* Vol. 09(01), 2024

[7] Milton L. Mueller, "Against sovereignty in cyberspace", *International Studies Review*, Vol. 22(04), 2020

[8] Milton L. Mueller, "Will the Internet fragment? Sovereignty, globalization and cyberspace", *Cambridge: Polity Press*, Vương quốc Anh, 2017

[9] Helen Dixon, "Regulate to liberate can europe save the internet", *Foreign Affair,* Vol. 97(05), 2018