

MỘT SỐ VẤN ĐỀ PHÁP LÝ ĐẶT RA ĐỐI VỚI VIỆT NAM VỀ CHỦ QUYỀN QUỐC GIA TRONG BẢO ĐẢM AN NINH MẠNG

● ĐỖ QUÍ HOÀNG - LÊ THỊ MAI

TÓM TẮT:

Bảo vệ chủ quyền quốc gia trên không gian mạng là vấn đề mới, đối tượng hoạt động trên không gian mạng phức tạp, gắn với phương tiện và trình độ công nghệ cao. Bên cạnh đó, lực lượng nòng cốt bảo vệ chủ quyền trên không gian mạng của Việt Nam mới thành lập, trình độ và phương tiện chưa phát triển đã nảy sinh nhiều thách thức về bảo vệ chủ quyền quốc gia trên không gian mạng. Nhận thức được đầy đủ các thách thức để có giải pháp đối phó phù hợp, hiệu quả là vấn đề quan trọng, cần thiết. Để góp phần bảo vệ chủ quyền quốc gia trên không gian mạng, bảo vệ vững chắc chủ quyền quốc gia trong tình hình mới, tác giả nghiên cứu một số vấn đề pháp lý đặt ra đối với Việt Nam về chủ quyền quốc gia trong bảo đảm an ninh mạng.

Từ khóa: pháp lý, chủ quyền quốc gia, bảo vệ chủ quyền, an ninh mạng, không gian mạng, Việt Nam.

1. Đặt vấn đề

Chiến lược phát triển kinh tế - xã hội 10 năm 2021 - 2030 trong Văn kiện Đại hội Đại biểu toàn quốc lần thứ XIII của Đảng Cộng sản Việt Nam khẳng định: *“Tích cực, chủ động xây dựng kế hoạch, phương án tác chiến, nâng cao trình độ, khả năng sẵn sàng chiến đấu bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ và giữ vững ổn định chính trị, an ninh quốc gia, trật tự, an toàn xã hội, giữ chủ quyền số quốc gia trên không gian mạng trong mọi tình huống”*¹. Đây là quan điểm mới về bảo vệ chủ quyền quốc gia phù hợp với xu thế chung của khu vực, thế giới, thực

trạng phát triển không gian mạng Việt Nam và sự tác động của Cách mạng công nghiệp lần thứ tư.

Đảng, Nhà nước ta đã sớm nhận thức được bảo vệ chủ quyền quốc gia trên không gian mạng và chủ quyền quốc gia trong bảo đảm an ninh mạng là những vấn đề quan trọng, cần có nhiều chủ trương, chính sách để triển khai thực hiện. Song, đây cũng là những vấn đề mới, phức tạp, khó khăn với những đối tượng đa dạng, khó xác định. Trong khi lực lượng nòng cốt bảo vệ chủ quyền quốc gia, bảo đảm an ninh mạng ở nước ta vẫn chưa thực sự phát triển về cả trình độ lẫn phương tiện thực hiện. Do vậy, bảo vệ chủ quyền quốc gia trên

không gian mạng, chủ quyền quốc gia trong bảo đảm an ninh mạng tại Việt Nam trong giai đoạn hiện nay càng đặt ra nhiều thách thức, khó khăn.

2. Những thách thức về mặt pháp lý và thực tiễn áp dụng pháp luật về chủ quyền quốc gia trong bảo đảm an ninh mạng hiện nay

Thứ nhất, hiện nay chưa có một điều ước quốc tế toàn cầu, cũng như các cơ chế, thiết chế hợp tác quốc tế để bảo vệ chủ quyền quốc gia trên không gian mạng. Sự phát triển bùng nổ của các công nghệ kỹ thuật số trên khắp thế giới đang mở ra các lĩnh vực tiềm năng mới cho xung đột và khả năng của cả các chủ thể Nhà nước và phi Nhà nước thực hiện các cuộc tấn công xuyên biên giới quốc tế.² Năm 2011, Nga đưa ra sáng kiến về việc Liên Hợp quốc nên xây dựng công ước về bảo đảm an ninh thông tin quốc tế, trong đó đề cập đến các tiêu chuẩn điều phối hoạt động trên internet, như các hoạt động liên quan đến chủ nghĩa khủng bố, hình sự, chính trị và quân sự. Tuy nhiên, sáng kiến này của Nga không được các quốc gia chấp thuận. Đến năm 2015, một nỗ lực để đạt được các thỏa thuận quốc tế nhằm xây dựng bộ quy tắc ứng xử trên không gian mạng tiếp tục được đưa ra. Các chuyên gia của Liên Hợp quốc đã đi đến một thỏa thuận với 4 nguyên tắc nhằm bảo đảm hòa bình trong không gian mạng. Hay gần đây, ngày 7/3/2023, Nga đã đệ trình tầm nhìn của mình về Công ước của Liên hợp quốc về Đảm bảo an ninh thông tin quốc tế cho Nhóm công tác mở của Liên hợp quốc về bảo mật và sử dụng công nghệ thông tin và truyền thông (OEWG). OEWG là một diễn đàn hỗ trợ các cuộc thảo luận về an ninh mạng quốc tế dưới sự bảo trợ của Ủy ban đầu tiên của Đại hội đồng Liên hợp quốc. Trong suốt OEWG, Nga đã nhiều lần kêu gọi thiết lập một hiệp ước. Trong các đoạn mở đầu, Nga cho rằng cần có một hiệp ước ràng buộc về mặt pháp lý vì có những lỗ hổng trong luật pháp quốc tế hiện hành. Nhưng nhiều quốc gia (ví dụ: Thụy Điển, Hàn Quốc, Colombia, Áo và Hoa Kỳ) đồng ý rằng không có khoảng cách nào như vậy và chỉ cần làm rõ thêm luật pháp quốc tế hiện hành. Ví dụ, tất cả các quốc gia đã đồng ý với khả năng áp dụng Hiến chương Liên

Hợp quốc (một hiệp ước pháp lý ràng buộc) đối với không gian mạng.³

Đến nay, ở phạm vi toàn cầu mới chỉ có một điều ước quốc tế điều chỉnh loại tội phạm này là Công ước về tội phạm mạng của Ủy hội châu Âu năm 2001. Với điều khoản cho phép các quốc gia không phải thành viên Ủy hội châu Âu tham gia Công ước, Công ước đã chính thức trở thành một khuôn khổ pháp lý hợp tác quốc tế toàn cầu giữa các quốc gia trong phòng chống tội phạm công nghệ cao với 75 thành viên, trong đó có sự tham gia của 28 quốc gia không phải thành viên của Ủy hội châu Âu.⁴

Hiện nay, công ước đã được đàm phán và mở rộng cho các quốc gia thành viên ở châu Á như: Nhật Bản, Philippines. Tuy nhiên, Nga, Trung Quốc và Brasil lại cho rằng, để công ước này trở thành công ước chung cho toàn thế giới cần phải đàm phán để xây dựng lại công ước bởi bản thân công ước được xây dựng dựa trên những đặc thù của khu vực nên không phản ánh hết các điều kiện và nhu cầu của tất cả các quốc gia trên thế giới.⁵

Thứ hai, liên quan đến năng lực thực thi của các quốc gia. Việc triển khai những hoạt động phòng ngừa và ngăn chặn các vụ tấn công trên không gian mạng nhằm ngăn ngừa hacker hay tội phạm công nghệ cao thường vấp phải các hạn chế liên quan về ngân sách và khả năng triển khai của các cơ quan nhà nước và giới hạn về hệ thống cơ sở hạ tầng công nghệ thông tin. Pháp luật của các quốc gia dường như không bắt kịp với tốc độ gia tăng và biến đổi nhanh của những hoạt động tội phạm dựa trên công nghệ số. Chính vì vậy, nhiều quốc gia ngoài Trung Quốc đã xây dựng không gian mạng riêng biệt phục vụ việc dùng mạng của người dân nước mình. Tại Việt Nam, mọi người cũng đưa ra câu hỏi: vậy Việt Nam có cần xây dựng một hệ thống mạng riêng biệt cho người Việt tương tự với các điều mà Trung Quốc đang làm? Tuy nhiên cần phải thấy rằng, việc làm này đi ngược lại với tinh thần và nền tảng của cuộc cách mạng công nghệ số là kết nối vạn vật, không giới hạn không gian và thời gian.⁶ Điều đó cũng thể hiện sự hạn chế hay sự yếu kém của chính phủ

đối với việc quản lý những hoạt động trên không gian mạng. Do đó, mỗi quốc gia cần thiết phải đưa ra những cách thức tối ưu hơn nữa đối với việc kiểm soát và giám sát những hoạt động trên không gian mạng để bảo đảm an ninh và trật tự, đồng thời bảo vệ những quyền lợi căn bản của người dân mà không để mất những tính năng siêu việt của công nghệ thông tin là kết nối vạn vật.

3. Giải pháp hoàn thiện chính sách, pháp luật nhằm bảo vệ vững chắc chủ quyền quốc gia trong bảo đảm an ninh mạng

Thứ nhất, bổ sung và hoàn thiện hệ thống pháp luật, chính sách về hợp tác quốc tế trong bảo vệ chủ quyền quốc gia trên không gian mạng và chủ quyền quốc gia trong bảo đảm an ninh mạng. Hoàn thiện khung pháp luật quốc gia, ban hành cơ chế, chính sách phù hợp với các quy định của pháp luật quốc tế xuất phát từ nhận thức an ninh mạng là bộ phận cấu thành của an ninh quốc gia, là nội dung chủ yếu để bảo vệ chủ quyền quốc gia trên không gian mạng; bảo đảm an toàn, an ninh mạng là một trong những động lực quan trọng phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh, nâng cao vị thế đất nước trong quá trình hội nhập, do đó, cần chú trọng hợp tác quốc tế, phát triển khoa học công nghệ, năng lực kỹ thuật, biện pháp bảo vệ tương xứng để hướng đến làm chủ các phần cứng, phần mềm ứng dụng; từng bước hình thành không gian mạng sạch, tạo điều kiện an toàn cho việc lưu trữ cơ sở dữ liệu; hợp tác trong đầu tư nghiên cứu, ứng dụng công nghệ, mã hóa thông tin đối với hệ thống thông tin quan trọng về an ninh quốc gia bảo đảm an ninh mạng, phòng, chống các vi phạm và tội phạm mạng.

Thứ hai, đưa nội dung chủ quyền quốc gia không gian mạng trong các chiến lược phát triển của đất nước; tiến hành trao đổi hợp tác với các đối tác chiến lược toàn diện/đối tác chiến lược/đối tác toàn diện về an ninh mạng, an toàn, an ninh thông tin. Xây dựng và ban hành văn bản của Nhà nước về quy định quản lý dữ liệu trên cơ sở tham khảo kinh nghiệm, hệ thống quy định của quốc tế và các nước; trong đó có nội dung về chủ quyền dữ liệu phù hợp với luật pháp quốc tế, Hiến chương Liên

hợp quốc và các thỏa thuận, hiệp định thương mại thế hệ mới, quy định của WTO, các nghĩa vụ quốc tế mà Việt Nam tham gia ký kết, làm cơ sở cho việc phát triển, mở rộng nội hàm về chủ quyền không gian mạng. Thúc đẩy nghiên cứu tác động của việc thực hiện chủ quyền số trong không gian mạng đối với an ninh, phát triển và vị thế của Việt Nam, trong bối cảnh hội nhập quốc tế ngày càng sâu rộng và toàn diện, cũng như đề xuất các hướng giải quyết. Nghiên cứu, xây dựng nội hàm về chủ quyền không gian mạng của Việt Nam⁷, từ đó có những điều chỉnh, bổ sung kịp thời trong xây dựng và triển khai chính sách đối ngoại của Việt Nam.

Thứ ba, ban hành các chính sách trong đó kết hợp chặt chẽ, có hiệu quả công tác bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng với việc thực hiện các nhiệm vụ phát triển kinh tế, văn hóa, xã hội, quốc phòng, an ninh, đối ngoại và nhiệm vụ xây dựng, chỉnh đốn Đảng. Công tác bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng phải trực tiếp phục vụ việc triển khai thực hiện có hiệu quả các mục tiêu, chỉ tiêu, nhiệm vụ, giải pháp của Đại hội lần thứ XIII đề ra. Theo đó, trong Văn kiện Đại hội XIII, Đảng ta nêu rõ: “Tích cực, chủ động... giữ vững chủ quyền số quốc gia trên không gian mạng trong mọi tình huống”. Đây là một nội dung lần đầu tiên được ghi trong một Văn kiện Đại hội, phản ánh sự nhận thức sâu sắc của Đảng ta về tính chất của thời đại dưới góc độ khoa học - công nghệ, bởi cuộc cách mạng công nghiệp lần thứ tư sẽ chuyển dịch toàn bộ thế giới từ thế giới thực sang thế giới số.

Thứ tư, hoàn thiện khung chính sách, pháp luật về công tác quản lý nhà nước về an toàn thông tin, an ninh mạng, sẵn sàng ứng phó với các thách thức an ninh mạng, đặc biệt là tội phạm mạng nhằm bảo vệ tốt hơn quyền, lợi ích hợp pháp của các tổ chức, cá nhân và bảo vệ vững chắc chủ quyền quốc gia. Với mỗi chính sách, văn bản pháp luật cần phải xác định rõ trách nhiệm của các tổ chức, cá nhân khi tham gia hoạt động trên môi trường mạng và nhiệm vụ của các chủ thể đó trong việc bảo vệ chủ quyền quốc gia trên không gian mạng ■

Bài viết trong khuôn khổ Đề tài nghiên cứu khoa học cấp trường: “Chủ quyền quốc gia trong bảo đảm an ninh mạng - Những vấn đề pháp lý đặt ra đối với Việt Nam”, do TS. Đỗ Quý Hoàng chủ nhiệm, Trường Đại học Luật Hà Nội, năm 2023.

TÀI LIỆU TRÍCH DẪN:

¹ Đảng Cộng sản Việt Nam (2021), Văn kiện Đại hội Đại biểu toàn quốc lần thứ XIII, NXB. Chính trị quốc gia Sự thật, Hà Nội, tập I, tr.277.

²Security Council (2021), Explosive Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats, SC/14563, 29 June 2021, xem tại: <https://press.un.org/en/2021/sc14563.doc.htm>.

³Valentin Weber (2023). The Dangers of a New Russian Proposal for a UN Convention on International Information Security. Net Politics & Digital and Cyberspace Policy Program, <https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security>.

⁴Xem chi tiết các quốc gia thành viên của Công ước về tội phạm mạng của Ủy hội châu Âu tại https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cLFJd5.ffffu-Y.

⁵Nguyễn Việt Lâm (2019), 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.

⁶Hao Yeli (2017), A Three-Perspective Theory of Cyber Sovereignty, The Journal of Complex Operations, PRISM Volume 7, No 2, xem tại: <https://cco.ndu.edu/PRISM-7-2/article/1401954/a-three-perspective-theory-of-cyber-sovereignty/>.

⁷Nội hàm về chủ quyền không gian mạng có thể bao gồm các nội dung chính, như: phạm vi mở rộng chủ quyền quốc gia trong không gian mạng, quyền độc lập trong việc lựa chọn con đường phát triển trong không gian mạng, phòng thủ không gian mạng và quyền bình đẳng trong tham gia quản trị toàn cầu không gian mạng, các nguyên tắc liên quan trong Hiến chương Liên hợp quốc áp dụng trong không gian mạng.

TÀI LIỆU THAM KHẢO:

1. Đảng Cộng sản Việt Nam (2021), Văn kiện Đại hội Đại biểu toàn quốc lần thứ XIII, NXB Chính trị Quốc gia Sự thật, Hà Nội.

2. Oren Upton (2003), Thesis: “Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection”, Naval Postgraduate School, Monterey, California.

3. Security Council (2021), Explosive Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats, SC/14563, 29 June 2021, xem tại: <https://press.un.org/en/2021/sc14563.doc.htm>

4. Valentin Weber (2023). The Dangers of a New Russian Proposal for a UN Convention on International Information Security. Net Politics & Digital and Cyberspace Policy Program, <https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security>.

5. Nguyễn Việt Lâm (2019), 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.

6. Hao Yeli (2017), A Three-Perspective Theory of Cyber Sovereignty, The Journal of Complex Operations, PRISM Volume 7, No 2, xem tại: <https://cco.ndu.edu/PRISM-7-2/article/1401954/a-three-perspective-theory-of-cyber-sovereignty/>

7. Hui Li & Xin Yang (2021), Co-governed Sovereignty Network: Legal Basis and Its Prototype & Applications with MIN Architecture, <https://link.springer.com/book/10.1007/978-981-16-2670-8>.

Ngày nhận bài: 3/5/2023

Ngày phản biện đánh giá và sửa chữa: 16/5/2023

Ngày chấp nhận đăng bài: 5/6/2023

Thông tin tác giả:

1. TS. ĐỖ QUÍ HOÀNG

Giảng viên Trường Đại học Luật Hà Nội

2. LÊ THỊ MAI

Học viên cao học Trường Đại học Luật Hà Nội

SOME LEGAL CHALLENGES IN PROTECTING VIETNAM'S NATIONAL SOVEREIGNTY IN CYBERSPACE

● Ph.D **DO QUI HOANG**¹

● **LE THI MAI**²

¹Lecturer, Hanoi Law University

²Master's student, Hanoi Law University

ABSTRACT:

Protecting national sovereignty in cyberspace is a new issue, with complex cyberspace activities associated with high-tech means and levels. The core force protecting Vietnam's national sovereignty in cyberspace has just been established, and this force's level and means have not yet developed. They have faced many challenges in protecting Vietnam's national sovereignty in cyberspace. It is important and necessary to be fully aware of these challenges in order to have appropriate and effective countermeasures, contributing to protecting Vietnam's national sovereignty in cyberspace and firmly protecting national sovereignty in the new situation.

Keywords: law, national sovereignty, national sovereignty protection, cybersecurity, cyberspace, Vietnam.