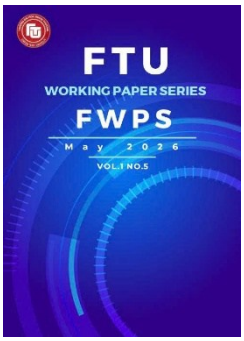

Working Paper 2026.1.5.5
- Vol. 1, No. 5

CHỦ QUYỀN SỐ VÀ AN NINH MẠNG TOÀN CẦU: NHỮNG VẤN ĐỀ ĐẶT RA ĐỐI VỚI BẢO VỆ AN NINH QUỐC GIA

Nguyễn Thị Minh Thư[1]

Sinh viên K62 Luật Thương mại quốc tế - Khoa Luật

Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Nguyễn Ngọc hà

Viện trưởng Viện nghiên cứu Sáng tạo

Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Tóm tắt

Không gian mạng ngày càng trở thành lĩnh vực chiến lược quan trọng, nơi chủ quyền số nổi lên như biểu hiện hiện đại của chủ quyền quốc gia nhằm bảo vệ lợi ích quốc gia trước các mối đe dọa xuyên biên giới. Nghiên cứu phân tích mâu thuẫn giữa nguyên tắc chủ quyền truyền thống dựa trên lãnh thổ và bản chất phi lãnh thổ của Internet, các vấn đề pháp lý thực tiễn trong bảo vệ an ninh quốc gia, cũng như hàm ý pháp lý cho Việt Nam trong việc thực thi chủ quyền số. Qua đó, bài báo đóng góp cơ sở lý luận và định hướng pháp lý cụ thể để hoàn thiện khung pháp luật, tăng cường hợp tác quốc tế và cân bằng giữa an ninh quốc gia với quyền con người, hướng tới xây dựng không gian mạng an toàn, tự chủ cho Việt Nam trong kỷ nguyên số.

Từ khóa: chủ quyền số, an ninh quốc gia, không gian mạng, bảo vệ dữ liệu.

[1] Tác giả liên hệ, email: minhthuvn509@gmail.com

DIGITAL SOVEREIGNTY AND GLOBAL CYBERSECURITY: ISSUES FOR THE PROTECTION OF NATIONAL SECURITY

Abstract

Cyberspace has increasingly become a critical strategic domain, where digital sovereignty emerges as a modern manifestation of national sovereignty, aimed at safeguarding national interests against cross-border threats. This study analyzes the conflict between the traditional principle of territorial-based sovereignty (Westphalian model) and the borderless, non-territorial nature of the Internet, as well as the practical legal issues in protecting national security in cyberspace. It also examines legal implications for Vietnam in implementing digital sovereignty. Through this analysis, the article contributes a theoretical foundation and specific legal orientations to improve the legal framework, strengthen international cooperation, and balance national security with human rights, towards building a safe, autonomous, and secure cyberspace for Vietnam in the digital era.

Keyword: digital sovereignty, national security, cyberspace, data protection.

Mở đầu

Trong những thập niên gần đây, sự phát triển mạnh mẽ của công nghệ thông tin, Internet và các nền tảng số đã làm thay đổi sâu sắc cấu trúc của môi trường an ninh ở cả cấp độ quốc gia và quốc tế. Không gian mạng ngày càng trở thành một hạ tầng thiết yếu của đời sống kinh tế-xã hội, đồng thời là môi trường diễn ra nhiều hoạt động chính trị, kinh tế và xã hội quan trọng. Nếu trước đây Internet chủ yếu được xem như một công cụ phục vụ trao đổi thông tin và kết nối toàn cầu, thì hiện nay không gian mạng đã trở thành một lĩnh vực chiến lược gắn liền với các lợi ích cốt lõi của quốc gia, bao gồm phát triển kinh tế, ổn định chính trị, bảo đảm quốc phòng và an ninh. Cùng với sự mở rộng nhanh chóng của hệ sinh thái số, các nguy cơ an ninh mạng như tấn công mạng, gián điệp mạng, thao túng thông tin, đánh cắp dữ liệu hay phá hoại các hệ thống hạ tầng số quan trọng cũng ngày càng gia tăng cả về quy mô lẫn mức độ tinh vi. Những nguy cơ này khiến an ninh mạng trở thành một trong những thách thức nổi bật của môi trường an ninh toàn cầu trong kỷ nguyên số.

Trong bối cảnh đó, nhiều quốc gia đã ban hành các chiến lược và học thuyết an ninh mạng nhằm bảo vệ lợi ích quốc gia trong không gian số. Có thể kể đến, Hoa Kỳ thúc đẩy cách tiếp cận chủ động trong phòng thủ mạng thông qua học thuyết "tương tác liên tục" (persistent engagement) với mục tiêu duy trì sự hiện diện thường xuyên trong không gian mạng nhằm phát hiện và ngăn chặn sớm các mối đe doạ. Trong khi đó, Trung Quốc và Nga tăng cường xây dựng các khuôn khổ pháp lý và chiến lược quốc gia nhằm kiểm soát hạ tầng thông tin và bảo vệ không gian mạng nội địa. Những động thái này

cho thấy không gian mạng ngày càng trở thành một lĩnh vực cạnh tranh chiến lược giữa các quốc gia, nơi các lợi ích an ninh và quyền lực quốc gia được thể hiện dưới những hình thức mới.

Song song với sự gia tăng của các mối đe dọa mạng là sự nổi lên của khái niệm "chủ quyền số". Khái niệm này phản ánh nỗ lực của các quốc gia nhằm khẳng định quyền kiểm soát đối với hạ tầng số, dữ liệu và các hoạt động diễn ra trong không gian mạng có liên quan đến lợi ích quốc gia. Trong bối cảnh Internet vốn có tính chất xuyên biên giới và phi lãnh thổ, việc thực thi chủ quyền số đặt ra nhiều vấn đề phức tạp cả về pháp lý lẫn chính sách. Tuy nhiên, đối với nhiều quốc gia, chủ quyền số ngày càng được xem là một công cụ quan trọng nhằm bảo vệ an ninh quốc gia, duy trì ổn định xã hội và bảo đảm khả năng tự chủ trong kỷ nguyên số.

1. Khái niệm chủ quyền số và mối quan hệ giữa chủ quyền số và an ninh quốc gia

Khái niệm chủ quyền số (digital sovereignty) ngày càng được nhắc đến nhiều trong các nghiên cứu về quản trị Internet và an ninh mạng, đặc biệt từ thập niên 2010 trở lại đây. Sự xuất hiện của thuật ngữ này phản ánh xu hướng chuyển dịch từ mô hình Internet mở, mang tính toàn cầu cao sang các cách tiếp cận nhấn mạnh vai trò quản lý và kiểm soát của nhà nước nhằm bảo vệ lợi ích chiến lược quốc gia trong môi trường số. Một trong những sự kiện có ảnh hưởng lớn đến nhận thức của các quốc gia về vấn đề này là vụ rò rỉ tài liệu giám sát toàn cầu do Edward Snowden công bố năm 2013, các tài liệu cho thấy mức độ giám sát rộng lớn của cơ quan tình báo Hoa Kỳ đối với dữ liệu và hệ thống thông tin trên phạm vi toàn cầu. Sự kiện này đã thúc đẩy nhiều quốc gia xem xét lại mức độ phụ thuộc của mình vào các hạ tầng và nền tảng công nghệ nước ngoài, từ đó tăng cường xây dựng các chính sách nhằm bảo đảm quyền kiểm soát đối với dữ liệu và hệ thống thông tin quốc gia.

Theo Diễn đàn Kinh tế Thế giới (WEF), chủ quyền số được định nghĩa là khả năng kiểm soát "số phận kỹ thuật số" (digital destiny) của một quốc gia, bao gồm dữ liệu, phần cứng và phần mềm mà quốc gia phụ thuộc và tạo ra. Theo Pohle và Thiel, khái niệm này bao gồm ba lớp cấu trúc chính: lớp hạ tầng vật lý (bao gồm mạng lưới, trung tâm dữ liệu và thiết bị phần cứng); lớp mã và quy tắc (liên quan đến tiêu chuẩn kỹ thuật, giao thức và thiết kế hệ thống); và lớp dữ liệu (liên quan đến tiêu chuẩn kỹ thuật, giao thức và thiết kế hệ thống). Các yếu tố cốt lõi của chủ quyền số bao gồm kiểm soát dữ liệu, kiểm soát hạ tầng số và quản lý hoạt động trên không gian mạng. Theo báo cáo Digital Economy Report 2021 của UNCTAD, nhiều quốc gia đang phát triển đang đối mặt với rủi ro mất chủ quyền số do phụ thuộc lớn vào hạ tầng đám mây và các nền tảng số do các công ty từ Mỹ và Trung Quốc thống trị, dẫn đến sự tập trung quyền lực trong chuỗi giá trị dữ liệu toàn cầu.

Mối quan hệ giữa chủ quyền số và an ninh quốc gia thể hiện ở việc chủ quyền số tạo ra nền tảng để nhà nước bảo vệ các lợi ích chiến lược trong môi trường số. Trước hết, việc kiểm soát dữ liệu có ý

nghĩa quan trọng đối với bảo vệ các thông tin nhạy cảm liên quan đến kinh tế, chính trị và quốc phòng trước nguy cơ gián điệp hoặc đánh cắp dữ liệu từ bên ngoài. Bên cạnh đó, chủ quyền số cũng gắn với khả năng bảo vệ các hệ thống hạ tầng thông tin quan trọng, chẳng hạn như hệ thống tài chính, năng lượng hoặc giao thông,... trước các cuộc tấn công mạng có thể gây ra hậu quả nghiêm trọng đối với ổn định quốc gia. Ngoài ra, việc quản lý hiệu quả không gian thông tin còn góp phần hạn chế các chiến dịch thao túng dư luận và thông tin sai lệch trên môi trường mạng. Một ví dụ thường được nhắc đến trong các nghiên cứu là các chiến dịch thông tin sai lệch bị cáo buộc có liên quan đến Nga trong cuộc bầu cử tổng thống Hoa Kỳ, cho thấy mức độ ảnh hưởng của các hoạt động thông tin trên không gian mạng đối với đời sống chính trị và xã hội.

Nhìn chung, trong bối cảnh các mối đe dọa mạng ngày càng gia tăng và cạnh tranh chiến lược giữa các quốc gia mở rộng sang môi trường số, chủ quyền số ngày càng được xem là một thành tố quan trọng của an ninh quốc gia. Không chỉ là vấn đề kỹ thuật hay quản lý dữ liệu, chủ quyền số còn gắn với năng lực của nhà nước trong việc bảo đảm quyền kiểm soát đối với các nguồn lực chiến lược trong kỷ nguyên số, qua đó duy trì ổn định và khả năng tự chủ của quốc gia trong môi trường an ninh ngày càng phức tạp.

2. Thách thức xuyên biên giới và sự đa dạng trong cách tiếp cận chủ quyền số

Một trong những trở ngại lớn nhất đối với việc thực thi chủ quyền số là bản chất xuyên biên giới và phi lãnh thổ của không gian mạng. Khác với các lĩnh vực truyền thống vốn gắn chặt với lãnh thổ địa lý, các hoạt động trong không gian mạng thường diễn ra đồng thời trên nhiều hệ thống hạ tầng đặt tại các quốc gia khác nhau. Dữ liệu có thể được thu thập ở một quốc gia, lưu trữ trên máy chủ đặt tại quốc gia khác và được xử lý thông qua các hệ thống điện toán đám mây phân tán trên phạm vi toàn cầu. Tính chất phi lãnh thổ này làm suy giảm hiệu lực của các cơ chế thực thi pháp luật dựa trên nguyên tắc chủ quyền lãnh thổ truyền thống. Trong nhiều trường hợp, việc xác định quốc gia có thẩm quyền tài phán đối với một hoạt động mạng cụ thể trở nên hết sức phức tạp, đặc biệt khi các hành vi vi phạm được thực hiện thông qua nhiều tầng trung gian và các hệ thống kỹ thuật đặt tại nhiều khu vực pháp lý khác nhau.

Một thách thức quan trọng khác liên quan đến vấn đề quy trách nhiệm trong các sự cố và tấn công mạng xuyên biên giới. Các cuộc tấn công mạng thường được thực hiện thông qua các mạng lưới máy tính trung gian, các hạ tầng ẩn danh, khiến việc truy vết nguồn gốc thực sự của cuộc tấn công trở nên khó khăn. Điều này gây trở ngại đáng kể cho việc áp dụng các quy tắc trách nhiệm quốc gia trong luật quốc tế, đồng thời làm hạn chế khả năng phản ứng pháp lý hoặc chính sách của các quốc gia bị ảnh hưởng. Thực tiễn cho thấy nhiều vụ tấn công mạng quy mô lớn nhằm vào cơ sở hạ tầng quan trọng, hệ

thống tài chính hoặc các cơ quan nhà nước đã gây ra thiệt hại đáng kể nhưng vẫn khó xác định rõ chủ thể chịu trách nhiệm.

Bên cạnh các thách thức kỹ thuật và pháp lý, sự khác biệt trong cách tiếp cận quản trị không gian mạng giữa các quốc gia cũng làm gia tăng mức độ phức tạp của vấn đề chủ quyền số. Một số quốc gia ưu tiên bảo đảm dòng chảy dữ liệu xuyên biên giới và duy trì tính mở của Internet, đồng thời phát triển các cơ chế hợp tác quốc tế nhằm thúc đẩy quản trị mạng đa bên. Tuy nhiên, ngay cả trong những trường hợp này, các quốc gia vẫn áp dụng những biện pháp pháp lý nhằm bảo vệ lợi ích an ninh và dữ liệu của mình. Chẳng hạn có thể kể đến, Hoa Kỳ ban hành Clarifying Lawful Overseas Use of Data Act cho phép cơ quan thực thi pháp luật yêu cầu các doanh nghiệp công nghệ cung cấp dữ liệu được lưu trữ ở nước ngoài trong một số trường hợp nhất định, qua đó làm dấy lên nhiều tranh luận về phạm vi quyền tài phán và chủ quyền dữ liệu của các quốc gia khác.

Trong khi đó, Liên minh châu Âu phát triển cách tiếp cận chủ quyền số gắn với bảo vệ quyền riêng tư và quyền con người trong môi trường số. Các khuôn khổ pháp lý như General Data Protection Regulation đặt ra các tiêu chuẩn nghiêm ngặt đối với việc thu thập, xử lý và chuyển giao dữ liệu cá nhân, đồng thời áp dụng nguyên tắc hiệu lực ngoài lãnh thổ đối với các doanh nghiệp cung cấp dịch vụ cho công dân EU. Cách tiếp cận này góp phần nâng cao mức độ bảo vệ dữ liệu nhưng cũng tạo ra những thách thức nhất định đối với các doanh nghiệp và quốc gia khác trong việc tuân thủ các quy định pháp lý phức tạp.

Trái lại, một số quốc gia áp dụng mô hình nhấn mạnh quyền kiểm soát mạnh mẽ của nhà nước đối với hạ tầng thông tin và dữ liệu trong phạm vi lãnh thổ. Trung Quốc xây dựng khuôn khổ quản trị mạng tương đối tập trung thông qua Cybersecurity Law of the People's Republic of China, yêu cầu lưu trữ dữ liệu quan trọng trong lãnh thổ và tăng cường kiểm soát đối với các nền tảng trực tuyến. Nga cũng phát triển các chính sách nhằm tăng cường khả năng kiểm soát và vận hành độc lập của Internet trong nước thông qua các chiến lược bảo đảm "chủ quyền Internet". Những cách tiếp cận này giúp tăng cường khả năng kiểm soát hạ tầng số và dữ liệu trong nước, nhưng đồng thời có thể làm gia tăng nguy cơ phân mảnh Internet toàn cầu.

Sự tồn tại đồng thời của nhiều mô hình quản trị khác nhau đang khiến không gian mạng toàn cầu trở nên ngày càng phân tán. Khi mỗi quốc gia tìm cách củng cố chủ quyền số theo những ưu tiên và lợi ích riêng, môi trường pháp lý quốc tế trở nên phức tạp hơn, trong khi các cơ chế hợp tác đa phương vẫn chưa theo kịp tốc độ phát triển của công nghệ. Điều này tạo ra một nghịch lý: trong khi các mối đe dọa mạng mang tính toàn cầu và đòi hỏi sự hợp tác quốc tế chặt chẽ, sự khác biệt về chính sách và lợi ích giữa các quốc gia lại có xu hướng làm suy yếu khả năng phối hợp đó. Vì vậy, việc bảo vệ an ninh quốc

gia trong không gian mạng không chỉ phụ thuộc vào năng lực công nghệ và khung pháp lý của từng quốc gia, mà còn chịu ảnh hưởng sâu sắc từ cấu trúc quản trị toàn cầu của Internet và mức độ hợp tác quốc tế trong lĩnh vực an ninh mạng.

3. Những vấn đề pháp lý thực tiễn đối với việc bảo vệ an ninh quốc gia trong không gian mạng

Bên cạnh các thách thức kỹ thuật và quản trị, việc bảo vệ an ninh quốc gia trong không gian mạng còn đặt ra nhiều vấn đề pháp lý thực tiễn đối với các quốc gia. Những vấn đề này chủ yếu xuất phát từ sự không tương thích giữa các nguyên tắc pháp lý truyền thống, cái vốn được xây dựng trên cơ sở lãnh thổ và quyền tài phán quốc gia với đặc điểm phi lãnh thổ và xuyên biên giới của không gian mạng. Trong môi trường số, các hành vi xâm phạm an ninh có thể được thực hiện từ bên ngoài lãnh thổ, thông qua các hạ tầng công nghệ đặt tại nhiều quốc gia khác nhau, khiến việc áp dụng và thực thi pháp luật quốc gia trở nên phức tạp hơn nhiều so với các lĩnh vực truyền thống.

Một trong những vấn đề pháp lý nổi bật là khó khăn trong việc thực thi quyền tài phán đối với các hoạt động mạng có yếu tố nước ngoài. Pháp luật của nhiều quốc gia, trong đó có Việt Nam, chủ yếu được xây dựng dựa trên nguyên tắc lãnh thổ. Luật An ninh mạng 2018 quy định trách nhiệm của các tổ chức, cá nhân trong việc bảo vệ an ninh mạng và yêu cầu các doanh nghiệp cung cấp dịch vụ trên không gian mạng phải phối hợp với cơ quan chức năng khi có yêu cầu hợp pháp. Tuy nhiên, trên thực tế, nhiều nền tảng dịch vụ số cung cấp cho người dùng tại Việt Nam lại được vận hành bởi các doanh nghiệp đặt trụ sở ở nước ngoài, với hệ thống máy chủ và cơ sở dữ liệu phân tán trên phạm vi toàn cầu. Trong những trường hợp này, việc yêu cầu cung cấp dữ liệu phục vụ điều tra, xử lý vi phạm hoặc ngăn chặn các hành vi xâm phạm an ninh quốc gia thường phụ thuộc vào mức độ hợp tác của doanh nghiệp cũng như cơ chế pháp lý của quốc gia nơi doanh nghiệp đặt trụ sở.

Một vấn đề pháp lý khác liên quan đến sự xung đột giữa các hệ thống pháp luật quốc gia trong quản lý dữ liệu và hạ tầng số. Các quốc gia ngày càng ban hành nhiều quy định nhằm bảo vệ dữ liệu và tăng cường quyền kiểm soát đối với thông tin số, nhưng những quy định này đôi khi có phạm vi áp dụng vượt ra ngoài lãnh thổ và có thể xung đột với pháp luật của các quốc gia khác. Ví dụ, Clarifying Lawful Overseas Use of Data Act như đã đề cập ở bên trên. Sự khác biệt giữa các mô hình pháp lý càng làm gia tăng nguy cơ xung đột pháp luật trong quản trị dữ liệu xuyên biên giới. Đối với Việt Nam, việc bảo vệ dữ liệu và quản lý các hoạt động xử lý dữ liệu trong môi trường số cũng đang được tăng cường thông qua các quy định pháp lý mới. Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân đặt ra các nguyên tắc và nghĩa vụ đối với tổ chức, cá nhân khi thu thập và xử lý dữ liệu cá nhân, đồng thời quy định các điều kiện đối với việc chuyển dữ liệu ra nước ngoài. Tuy nhiên, trong bối cảnh các nền tảng

số toàn cầu đóng vai trò ngày càng lớn trong hệ sinh thái Internet, việc kiểm soát và thực thi các quy định này trên thực tế vẫn gặp nhiều khó khăn. Khi dữ liệu của công dân hoặc tổ chức Việt Nam được lưu trữ và xử lý trên các hệ thống đặt ngoài lãnh thổ, khả năng áp dụng và cưỡng chế pháp luật quốc gia có thể bị hạn chế đáng kể.

Ngoài ra, một thách thức pháp lý quan trọng khác là việc cân bằng giữa yêu cầu bảo vệ an ninh quốc gia và bảo đảm các quyền cơ bản của con người trong môi trường số. Các biện pháp tăng cường kiểm soát thông tin, giám sát hoạt động mạng hoặc yêu cầu lưu trữ dữ liệu phục vụ mục tiêu an ninh có thể làm dấy lên những tranh luận gay gắt liên quan đến quyền riêng tư, quyền tự do biểu đạt và quyền tiếp cận thông tin. Quyền tiếp cận thông tin cũng có thể bị hạn chế khi các biện pháp chặn truy cập được sử dụng để bảo vệ an ninh. Vì vậy, việc xây dựng và thực thi các quy định pháp luật về an ninh mạng cần bảo đảm nguyên tắc cân bằng, minh bạch và phù hợp với các cam kết quốc tế về quyền con người mà quốc gia đã tham gia. Nguyên tắc "tỷ lệ" (proportionality) và "cần thiết" (necessity) phải được áp dụng nghiêm ngặt: mọi biện pháp hạn chế quyền con người chỉ được chấp nhận khi thực sự cần thiết, phù hợp với mục tiêu an ninh và ít can thiệp nhất có thể. Việc thiếu cơ chế giám sát độc lập và khiếu nại hiệu quả càng làm tăng nguy cơ lạm dụng quyền lực nhà nước, dẫn đến mất lòng tin của xã hội và giảm hiệu quả lâu dài của các biện pháp bảo vệ an ninh mạng.

Những vấn đề pháp lý phát sinh từ đặc điểm xuyên biên giới của không gian mạng, sự khác biệt giữa các hệ thống pháp luật quốc gia và yêu cầu cân bằng giữa an ninh và quyền con người đang đặt ra nhiều thách thức đối với việc bảo vệ an ninh quốc gia trong kỷ nguyên số. Điều này cho thấy nhu cầu tiếp tục hoàn thiện khung pháp lý quốc gia, đồng thời thúc đẩy hợp tác quốc tế nhằm xây dựng các cơ chế quản trị hiệu quả hơn đối với các hoạt động trong không gian mạng.

4. Hàm ý pháp lý cho Việt Nam trong việc thực thi chủ quyền số gắn với an ninh quốc gia

Trong bối cảnh không gian mạng ngày càng trở thành một lĩnh vực cạnh tranh chiến lược giữa các quốc gia, việc bảo vệ chủ quyền số cần được xem là một phần quan trọng của chiến lược bảo vệ an ninh quốc gia. Đối với Việt Nam, quá trình này đòi hỏi sự hoàn thiện và vận hành hiệu quả khung pháp lý hiện hành, đồng thời xây dựng các cơ chế quản trị phù hợp với đặc điểm xuyên biên giới của môi trường số.

Trước hết, cần tiếp tục hoàn thiện và bảo đảm tính đồng bộ của hệ thống pháp luật liên quan đến an ninh mạng và bảo vệ dữ liệu. Trong những năm gần đây, Việt Nam đã xây dựng nền tảng pháp lý quan trọng thông qua Luật An ninh mạng 2018 và các văn bản hướng dẫn thi hành như Nghị định 53/2022/NĐ-CP, quy định trách nhiệm của các tổ chức, doanh nghiệp trong việc bảo vệ hệ thống thông tin và phối hợp với cơ quan nhà nước khi có yêu cầu bảo đảm an ninh quốc gia. Bên cạnh đó, Nghị định

13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân đã bước đầu thiết lập khuôn khổ pháp lý cho việc thu thập, xử lý và chuyển giao dữ liệu cá nhân. Tuy nhiên, để các quy định này phát huy hiệu quả trong thực tiễn, cần tiếp tục cụ thể hóa các cơ chế thực thi như đánh giá tác động xử lý dữ liệu, nghĩa vụ thông báo vi phạm dữ liệu và quy trình kiểm soát chuyển dữ liệu ra nước ngoài. Việc hoàn thiện các quy định chi tiết sẽ giúp nâng cao khả năng bảo vệ dữ liệu và giảm thiểu các rủi ro an ninh trong môi trường số.

Thứ hai, cần tăng cường các cơ chế pháp lý nhằm bảo đảm quyền kiểm soát của nhà nước đối với hạ tầng số quan trọng và dữ liệu có ý nghĩa chiến lược. Trong bối cảnh nhiều dịch vụ số thiết yếu đang phụ thuộc vào các nền tảng công nghệ xuyên quốc gia, việc xác định và bảo vệ các hệ thống thông tin quan trọng có ý nghĩa đặc biệt đối với an ninh quốc gia. Pháp luật hiện hành đã bước đầu đề cập đến nội dung này thông qua quy định về hệ thống thông tin quan trọng trong Luật An ninh mạng 2018, tuy nhiên cần tiếp tục hoàn thiện các tiêu chí xác định, cơ chế giám sát và biện pháp bảo vệ đối với các hạ tầng số trọng yếu. Đồng thời, việc khuyến khích phát triển các nền tảng công nghệ và dịch vụ điện toán đám mây trong nước cũng là một hướng đi quan trọng nhằm giảm thiểu sự phụ thuộc vào hạ tầng công nghệ nước ngoài và tăng cường khả năng tự chủ trong không gian mạng.

Thứ ba, cần thúc đẩy hợp tác quốc tế trong quản trị và bảo đảm an ninh mạng. Do đặc điểm xuyên biên giới của các hoạt động mạng, nhiều hành vi xâm phạm an ninh quốc gia có thể được thực hiện từ ngoài lãnh thổ, khiến việc xử lý bằng các công cụ pháp luật quốc gia đơn thuần gặp nhiều hạn chế. Vì vậy, Việt Nam cần tăng cường tham gia các cơ chế hợp tác song phương và đa phương về an ninh mạng, bao gồm trao đổi thông tin, phối hợp ứng phó sự cố và hỗ trợ điều tra các hành vi vi phạm trên không gian mạng. Việc thúc đẩy hợp tác trong khuôn khổ các tổ chức và diễn đàn khu vực, có thể góp phần xây dựng các cơ chế phối hợp hiệu quả hơn trong việc xử lý các thách thức an ninh mạng xuyên biên giới.

Cuối cùng, trong quá trình xây dựng và thực thi các chính sách liên quan đến chủ quyền số, cần bảo đảm sự cân bằng hợp lý giữa mục tiêu bảo vệ an ninh quốc gia và việc tôn trọng các quyền cơ bản của con người trong môi trường số. Các biện pháp kiểm soát thông tin và bảo vệ an ninh mạng cần được thiết kế trên cơ sở nguyên tắc cần thiết, tương xứng và minh bạch, đồng thời phải phù hợp với các quy định của Hiến pháp và các cam kết quốc tế mà Việt Nam tham gia. Việc tăng cường cơ chế minh bạch, trách nhiệm giải trình và bảo vệ quyền lợi hợp pháp của cá nhân, tổ chức trong không gian mạng sẽ góp phần nâng cao tính chính danh và hiệu quả của các chính sách bảo vệ chủ quyền số.

Nhìn chung, việc thực thi chủ quyền số trong bối cảnh an ninh mạng toàn cầu đòi hỏi Việt Nam phải kết hợp giữa hoàn thiện khung pháp lý trong nước, nâng cao năng lực quản trị và thúc đẩy hợp tác quốc tế. Những định hướng này không chỉ góp phần tăng cường khả năng bảo vệ an ninh quốc gia trong môi trường số mà còn tạo nền tảng cho sự phát triển bền vững của hệ sinh thái số quốc gia trong dài hạn.

Kết luận

Sự phát triển nhanh chóng của công nghệ số và Internet đã khiến không gian mạng trở thành một lĩnh vực có ý nghĩa chiến lược đối với an ninh quốc gia. hủ quyền số ngày càng được xem là một yếu tố quan trọng nhằm bảo vệ lợi ích quốc gia, đặc biệt trong việc kiểm soát dữ liệu, hạ tầng số và các hoạt động thông tin trên không gian mạng. Đối với Việt Nam, việc tăng cường thực thi chủ quyền số cần gắn với quá trình hoàn thiện khung pháp lý về an ninh mạng và bảo vệ dữ liệu, nâng cao năng lực quản lý hạ tầng số, đồng thời thúc đẩy hợp tác quốc tế trong xử lý các thách thức an ninh mạng xuyên biên giới. Đây là những điều kiện quan trọng để bảo vệ an ninh quốc gia và bảo đảm sự phát triển bền vững trong kỷ nguyên số.

TÀI LIỆU THAM KHẢO

Ban Chấp hành Trung ương Đảng Cộng sản Việt Nam. *Nghị quyết số 57-NQ/TW về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia*. Hà Nội.

Chính phủ. (2022). *Nghị định số 53/2022/NĐ-CP quy định chi tiết một số điều của Luật An ninh mạng*. Hà Nội.

Chính phủ. (2023). *Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân*. Hà Nội.

Cục An toàn thông tin. (2021). *Bản tin an toàn thông tin quý I/2021 - Chủ quyền số quốc gia trên không gian mạng*. Truy cập tại: https://attt.mae.gov.vn/pages/ban-tin-an-toan-thong-tin-quy-i2021---chu-quyen-so-quoc-gia-tren-khong-gian-mang.aspx

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Brussels.

European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Brussels.

Freedom House. (2025). *Freedom on the net 2025: The repression of online freedom worldwide*. Freedom House.

Hwang, J. Y. (2025). Digital sovereignty in an era of cyber threats and global connectivity. *International Journal of Multidisciplinary Research Updates, Vol 9* No 2, p.12–23.

International Telecommunication Union. (2024). *Global cybersecurity index 2024*. ITU.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.

Mueller, M. L. (2017). *Will the internet fragment? Sovereignty, globalization and cyberspace*. Polity Press.

Nguyễn, V. L. (2021). 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*. Truy cập tại: https://www.tapchicongsan.org.vn/web/guest/the-gioi-van-de-su-kien/-/2018/823954/chu-quyen-khong-gian-mang%E2%80%93ly-thuyet%2C-thuc-tien-trong-quan-he-quoc-te-va-nhung-van-de-dat-ra-hien-nay.aspx

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1532

Quốc hội. (2015). *Luật An toàn thông tin mạng*. Hà Nội.

Quốc hội. (2018). *Luật An ninh mạng*. Hà Nội.

Trần, P. S. N. (2023). Chủ quyền quốc gia trong không gian mạng: Thực tiễn quốc tế và Việt Nam. *Tạp chí Khoa học Trường Đại học Sư phạm TP. Hồ Chí Minh, Vol 20* no 12, p.2173–2184.

United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development – For whom the data flow*. United Nations.

United States. (2018). *Clarifying lawful overseas use of data act (CLOUD Act)*. Washington, DC.

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. World Economic Forum.

Lynch, T. F. (2024). Cyberspace: Great power competition in a fragmenting domain. *Orbis, Vol 68* No 4, p.607–623

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, Vol 41* No 3, p.44–71.

Bộ Khoa học và Công nghệ. (2023, May 20). *Không gian mạng và chiến lược bảo vệ chủ quyền "vùng lãnh thổ đặc biệt" của quốc gia*. Truy cập tại: https://mst.gov.vn/khong-gian-mang-va-chien-luoc-bao-ve-chu-quyen-vung-lanh-tho-dac-biet-cua-quoc-gia-197158520.htm

Nguyễn, T., Quang, T., Trần, T., & Mai, A. (2024, June 14). Pháp luật về chủ quyền quốc gia trên không gian mạng. *Đại biểu Nhân dân*. Truy cập tại: https://daibieunhandan.vn/phap-luat-ve-chu-quyen-quoc-gia-tren-khong-gian-mang-post375605.html