

TOÀN CẦU HÓA SỐ VÀ TÁC ĐỘNG ĐẾN BẢO VỆ CHỦ QUYỀN QUỐC GIA CỦA VIỆT NAM TRÊN KHÔNG GIAN MẠNG^(*)

VÕ TƯỜNG HUÂN^(**)
TRẦN THẮNG LONG^(***)

Ngày nhận bài: 30/12/2024 Ngày thẩm định: 05/01/2025 Ngày duyệt đăng: 18/01/2025

Tóm tắt: Việc đánh giá các đặc trưng của toàn cầu hóa số cũng như thành tố của khái niệm chủ quyền số để khẳng định quá trình này vừa tạo ra cơ hội phát triển, vừa đặt ra thách thức đối với khả năng quản lý của nhà nước. Điều đó cho thấy, nhà nước vừa phải thích ứng với đặc điểm của không gian mạng toàn cầu, vừa phải bảo vệ được lợi ích và an ninh quốc gia. Bài viết phân tích mối quan hệ của toàn cầu hóa trên không gian mạng đối với chủ quyền quốc gia, làm rõ những biến đổi vai trò và chức năng của nhà nước trong thời đại mới, từ đó đưa ra các khuyến nghị chính sách nhằm bảo vệ chủ quyền quốc gia, tăng cường năng lực quản trị của nhà nước, đặc biệt nhấn mạnh vai trò của hợp tác quốc tế và phát triển năng lực số nội sinh.

Từ khóa: bảo vệ chủ quyền; không gian mạng; quản trị nhà nước; toàn cầu hóa số; Việt Nam

1. Đặt vấn đề

Trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư và quá trình toàn cầu hóa diễn ra mạnh mẽ, không gian mạng trở thành một phần không thể thiếu trong đời sống kinh tế - xã hội của mỗi quốc gia. Sự phát triển nhanh chóng của công nghệ số và internet đã tạo ra

không gian ảo xuyên biên giới, nơi các hoạt động chính trị, kinh tế, văn hóa và xã hội diễn ra ngày càng sôi động. Theo Báo cáo thường niên WeAreSocial Digital 2024, hiện có hơn 05 tỷ người sử dụng internet, chiếm 63% dân số toàn cầu⁽¹⁾ và con số này vẫn đang tiếp tục tăng lên.

Nếu trước đây toàn cầu hóa chủ yếu thể hiện thông qua việc trao đổi hàng hóa hữu hình xuyên biên giới và sự phát triển của các tập đoàn đa quốc gia, thì ngày nay, làn sóng toàn cầu hóa mới xuất hiện - toàn cầu hóa số. Xu hướng này được thể hiện qua sự dịch chuyển không ngừng của dữ liệu số, thông tin, tri thức, cũng như các sản phẩm và dịch vụ được số hóa, tạo nên một mạng lưới kết nối chặt chẽ giữa các quốc gia,

^(*) Nghiên cứu được tài trợ bởi Đại học Quốc gia Thành phố Hồ Chí Minh trong khuôn khổ Đề tài mã số: B2022-28-24

^(**) TS, Trường Đại học Quốc tế, Đại học Quốc gia Thành phố Hồ Chí Minh

^(***) PGS, TS, Trường Đại học Luật Thành phố Hồ Chí Minh

doanh nghiệp và người dân trên phạm vi toàn cầu⁽²⁾. Toàn cầu hóa nói chung và toàn cầu hóa trên không gian mạng nói riêng mang đến những cơ hội to lớn cho sự phát triển của các quốc gia, đặc biệt là trong việc thúc đẩy kinh tế số, tăng cường kết nối và hợp tác quốc tế. Tuy nhiên, quá trình này cũng đặt ra những thách thức đối với chủ quyền quốc gia.

Đối với Việt Nam, trong quá trình đẩy mạnh chuyển đổi số quốc gia và hội nhập quốc tế, việc bảo vệ chủ quyền trên không gian mạng đang trở thành yêu cầu cấp thiết. Theo Số liệu phát triển lĩnh vực Viễn thông Việt Nam năm 2023, tỷ lệ người dùng internet tại Việt Nam ước đạt 78,59%, tăng 4,09% so với năm 2022, Các phương tiện truyền thông xã hội được sử dụng nhiều nhất theo thứ tự tại Việt Nam là: Facebook, Zalo, Facebook Messenger, Tiktok, Instagram, Twitter, Telegram, Pinterest..., riêng mạng xã hội Facebook có tới 70,4 triệu người sử dụng⁽³⁾. Toàn cầu hóa số đã và đang tác động sâu sắc đến vai trò của Nhà nước trên nhiều phương diện, vừa tạo động lực phát triển, vừa đặt ra những thách thức mới trong việc bảo vệ an ninh quốc gia và lợi ích của người dân trên không gian mạng. Vì vậy, cần nhận diện những tác động của toàn cầu hóa số trong quản lý nhà nước, đặc biệt là việc xây dựng các công cụ và phương thức quản lý phù hợp với môi trường số. Đồng thời, cần tăng cường hợp tác quốc tế trên cơ sở tôn trọng chủ quyền và lợi ích quốc gia để ứng phó hiệu quả với các thách thức này.

2. Toàn cầu hóa số và chủ quyền quốc gia trên không gian mạng

Một là, toàn cầu hóa số

Toàn cầu hóa số (digital globalisation), hay còn gọi là toàn cầu hóa trên không gian mạng, là khái niệm đa chiều, phản ánh sự hội nhập và kết nối toàn cầu thông qua công nghệ số và internet. Khái niệm này được định nghĩa theo nhiều cách khác

nhau. Ở góc độ công nghệ, khái niệm toàn cầu hóa số nhằm chỉ quá trình liên kết và tích hợp các hệ thống thông tin, mạng lưới kỹ thuật số và kết cấu hạ tầng công nghệ trên phạm vi toàn cầu, tạo nên một không gian mới cho các tương tác xã hội và kinh tế⁽⁴⁾, trong đó nhấn mạnh vai trò của công nghệ thông tin trong việc định hình lại cấu trúc xã hội và kinh tế toàn cầu. Ở khía cạnh kinh tế, đây là xu thế mà các hoạt động kinh doanh, thương mại và tài chính được số hóa và vận hành trên nền tảng internet, giúp doanh nghiệp và người tiêu dùng dễ dàng tham gia vào thị trường toàn cầu⁽⁵⁾. Toàn cầu hóa không gian mạng tạo ra hệ sinh thái số toàn cầu, nơi diễn ra sự tương tác đa chiều giữa các yếu tố công nghệ, kinh tế, chính trị và văn hóa - xã hội⁽⁶⁾. Toàn cầu hóa số góp phần thúc đẩy giao lưu văn hóa, hình thành cộng đồng trực tuyến xuyên quốc gia và tạo ra những hình thái văn hóa mới trong môi trường kỹ thuật số⁽⁷⁾. Hiện tượng này là quá trình mở rộng, đào sâu và tăng tốc độ kết nối toàn cầu trong mọi khía cạnh của đời sống xã hội đương đại thông qua không gian số. Toàn cầu hóa trên không gian mạng làm mờ đi ranh giới địa lý và văn hóa truyền thống⁽⁸⁾.

Toàn cầu hóa số có những đặc trưng riêng so với toàn cầu hóa truyền thống. Đặc trưng quan trọng nhất là khả năng kết nối và tương tác theo thời gian thực trong không gian số. Khác với mô hình toàn cầu hóa truyền thống vốn phụ thuộc chủ yếu vào sự dịch chuyển vật lý của các yếu tố sản xuất và thương mại, toàn cầu hóa số tạo ra hệ sinh thái tương tác đa chiều, ở đó các chủ thể kết nối và giao dịch tức thời mà không phụ thuộc vào khoảng cách địa lý. Bằng chứng cho đặc trưng này là sự phát triển của các hệ thống tài chính toàn cầu và nền tảng giao tiếp đa phương tiện.

Đặc trưng thứ hai là tính phi vật thể và phi địa lý trong không gian mạng. Điều này dẫn đến sự thay đổi trong khái niệm

không gian và lãnh thổ truyền thống. Ranh giới địa lý truyền thống dần mờ nhạt trước sự xuất hiện của “vùng lãnh thổ số” - được hiểu như là không gian ảo, nơi diễn ra các hoạt động kinh tế, văn hóa và chính trị song hành với thế giới vật lý. Hiện tượng này được thể hiện qua sự phát triển của hệ thống lưu trữ đám mây phân tán toàn cầu.

Tính đổi mới liên tục là đặc trưng thứ ba của toàn cầu hóa số. Kết quả của sự phát triển công nghệ số góp phần quan trọng tạo ra những mô hình kinh tế - xã hội hoàn toàn mới. Toàn cầu hóa số tạo ra những mô hình kinh doanh và phương thức tương tác xã hội hoàn toàn mới, như kinh tế chia sẻ (Uber, Airbnb), tiền điện tử (Bitcoin), hay mạng xã hội. Các công nghệ đột phá, như blockchain, trí tuệ nhân tạo và internet vạn vật (IoT), đang định hình lại cách thức vận hành của các thể chế kinh tế và xã hội truyền thống.

Dân chủ hóa thông tin và cơ hội là đặc trưng quan trọng thứ tư. Công nghệ số đã tạo ra cuộc cách mạng trong việc tiếp cận tri thức và cơ hội phát triển. Internet và công nghệ số cho phép mọi người tiếp cận với lượng thông tin khổng lồ và các cơ hội học tập, kinh doanh mà trước đây chỉ dành cho một số ít. Minh chứng cho xu thế này thể hiện qua sự phát triển của các nền tảng giáo dục trực tuyến mở (MOOCs) và thương mại điện tử xuyên biên giới, tạo điều kiện cho việc phân phối lại nguồn lực và cơ hội trên phạm vi toàn cầu.

Đặc trưng thứ năm là tính tương hỗ và phụ thuộc lẫn nhau trong hệ thống số toàn cầu. Trong không gian mạng, các hệ thống số hiện đại tạo thành một mạng lưới phức hợp với độ kết nối cao, nơi biên độ động cục bộ có thể nhanh chóng lan tỏa và tạo ra hiệu ứng domino trên phạm vi toàn cầu. Minh chứng cho hiện tượng này là các cuộc khủng hoảng an ninh mạng và sự cố hệ thống của các nền tảng số lớn.

Bất đối xứng về quyền lực và nguồn lực là đặc trưng thứ sáu của toàn cầu hóa số. Trên thực tế đang diễn ra xu hướng tập trung quyền lực vào một số ít các tập đoàn công nghệ và quốc gia phát triển. Xu hướng này thể hiện qua việc kiểm soát dữ liệu, hạ tầng số và các công nghệ then chốt bởi một số ít các chủ thể có vị thế thống trị. Các công ty công nghệ lớn, như Google, Amazon, Facebook, có thể kiểm soát phần lớn dữ liệu và hạ tầng số toàn cầu.

Hai là, chủ quyền quốc gia trên không gian mạng

Khái niệm “chủ quyền quốc gia” truyền thống xuất hiện từ năm 1648 (còn gọi là chủ quyền Westphalia), nhấn mạnh đến tính toàn vẹn lãnh thổ và quyền tối cao của quốc gia trong phạm vi biên giới quốc gia. Tuy nhiên, cuộc Cách mạng công nghệ lần thứ tư đóng vai trò là nền tảng tạo ra hiện tượng toàn cầu hóa số, kéo theo những tác động sâu sắc đến chủ quyền quốc gia. Hiện tượng này không chỉ thay đổi cách thức các quốc gia thực thi quyền lực của mình, mà còn định hình lại khái niệm về chủ quyền trong kỷ nguyên số, dẫn đến sự xuất hiện của khái niệm mới: “chủ quyền quốc gia trên không gian mạng” hay còn gọi là “chủ quyền số” (digital sovereignty). Khái niệm này không chỉ phản ánh quyền tự chủ của một quốc gia trong môi trường số, mà còn thể hiện năng lực thực tế trong việc kiểm soát và phát triển không gian mạng của mình.

Theo tác giả Floridi, khái niệm “chủ quyền quốc gia trên không gian mạng” được định nghĩa là quyền tự chủ và năng lực kiểm soát của một quốc gia đối với không gian số của mình, bao gồm dữ liệu, cơ sở hạ tầng số và các hoạt động trong môi trường mạng⁽⁹⁾. Đây là khái niệm đa chiều, phản ánh nhiều khía cạnh khác nhau của quyền lực quốc gia trong thời đại số; thể hiện khả năng của một quốc gia trong việc quản lý, bảo vệ và phát

triển tài nguyên số, đồng thời duy trì sự độc lập về công nghệ và an ninh mạng⁽¹⁰⁾.

Một trong những khía cạnh cốt lõi của khái niệm này là chủ quyền dữ liệu (data sovereignty). Khía cạnh này liên quan đến quyền kiểm soát và quản lý dữ liệu quốc gia, bao gồm quyền quyết định về việc lưu trữ và xử lý dữ liệu trong lãnh thổ, khả năng bảo vệ dữ liệu của công dân và tổ chức, cũng như quyền quản lý luồng dữ liệu xuyên biên giới⁽¹¹⁾. Trong thời đại hiện nay, việc kiểm soát và bảo vệ dữ liệu trở nên đặc biệt quan trọng đối với mỗi quốc gia. Các quốc gia ngày càng khẳng định quyền kiểm soát dữ liệu được tạo ra trong phạm vi biên giới của họ, ban hành các quy định về an ninh mạng và bảo vệ dữ liệu người dùng, như Quy định chung về bảo vệ dữ liệu (GDPR) của Liên minh châu Âu hay Luật An ninh mạng của Trung Quốc, ban hành năm 2017, Luật An ninh mạng của Việt Nam, ban hành năm 2018.

Cùng với chủ quyền dữ liệu, độc lập công nghệ cũng là khía cạnh quan trọng không kém. Việc phát triển năng lực công nghệ tự chủ, bao gồm khả năng phát triển và làm chủ công nghệ số cốt lõi là rất quan trọng, giúp giảm sự phụ thuộc vào các nền tảng và giải pháp công nghệ nước ngoài⁽¹²⁾. Việc xây dựng hệ sinh thái công nghệ trong nước vững mạnh không chỉ bảo đảm an ninh quốc gia, mà còn tạo nền tảng cho sự phát triển bền vững của nền kinh tế số của quốc gia đó.

Một thành tố quan trọng khác tạo nên khái niệm chủ quyền quốc gia trong không gian mạng chính là “quản trị số” - liên quan đến khung pháp lý và thể chế để thực thi chủ quyền số. Điều này bao gồm việc xây dựng và thực thi luật pháp về không gian mạng, thiết lập cơ chế quản lý các hoạt động số và tham gia vào các cơ chế quản trị internet toàn cầu. Một hệ thống quản trị số hiệu quả sẽ tạo ra môi

trường thuận lợi cho sự phát triển của không gian mạng quốc gia, đồng thời bảo đảm an ninh và lợi ích quốc gia⁽¹³⁾.

An ninh mạng được xác định là trụ cột không thể thiếu của chủ quyền số. Khía cạnh này bao gồm năng lực phòng ngừa và ứng phó với các mối đe dọa mạng, bảo vệ cơ sở hạ tầng thông tin quan trọng và bảo đảm an toàn thông tin cho người dân và tổ chức⁽¹⁴⁾. Trong bối cảnh các cuộc tấn công mạng ngày càng tinh vi và phức tạp, việc xây dựng năng lực an ninh mạng vững mạnh trở thành yêu cầu cấp thiết đối với mọi quốc gia⁽¹⁵⁾. Theo Trung tướng, PGS, TS. Phan Xuân Tuy - Giám đốc Học viện Chính trị Công an nhân dân, sự phát triển của công nghệ thông tin, mạng internet và các mạng xã hội tạo ra không gian chiến lược mới - “không gian mạng” mang lại nhiều cơ hội và thách thức cho tất cả các quốc gia trên thế giới, bao gồm Việt Nam⁽¹⁶⁾.

Đảng Cộng sản Việt Nam xác định, không gian mạng hiện đang là vùng lãnh thổ mới rất cần được coi trọng. Theo Tổng Bí thư Tô Lâm, không gian mạng là “không gian thứ năm, chiến trường thứ năm, miền thứ năm của quốc gia, bên cạnh vùng đất, vùng trời, vùng biển và không gian vũ trụ”⁽¹⁷⁾. Đảng và Nhà nước đã sớm nhận thức rõ chủ quyền không gian mạng là bộ phận có tầm quan trọng đặc biệt của chủ quyền quốc gia⁽¹⁸⁾. Tại Việt Nam, chủ quyền quốc gia trên không gian mạng là quyền tối cao, tuyệt đối, đầy đủ và riêng biệt của quốc gia đối với các vùng dữ liệu, thông tin trên không gian mạng do Nhà nước quản lý, kiểm soát trực tiếp hoặc gián tiếp bằng hệ thống chính sách, pháp luật và các công nghệ phù hợp với luật pháp quốc tế. Các quốc gia có quyền tối cao, tuyệt đối với phạm vi không gian mạng thuộc quyền kiểm soát của mình, nghĩa là có chủ quyền quốc gia riêng trên không gian mạng.

3. Tác động của toàn cầu hóa số đến bảo vệ chủ quyền quốc gia trên không gian mạng

Một là, tác động đến khả năng kiểm soát thông tin và dữ liệu

Toàn cầu hóa số đã tạo ra những thách thức đáng kể trong việc kiểm soát thông tin và dữ liệu quốc gia. Hầu hết lưu lượng thông tin số của Việt Nam hiện đang được lưu trữ và xử lý tại các trung tâm dữ liệu ở nước ngoài. Trong khi đó, Việt Nam mới chỉ có khoảng 30 trung tâm dữ liệu, chiếm chưa đến 01% số lượng trung tâm dữ liệu toàn cầu⁽¹⁹⁾. Sự phát triển của các nền tảng số xuyên quốc gia làm suy giảm khả năng kiểm soát luồng thông tin xuyên biên giới của Nhà nước. Điều này không chỉ ảnh hưởng đến công tác quản lý thông tin, mà còn tác động trực tiếp đến an ninh quốc gia. Việc thiếu khả năng kiểm soát dữ liệu làm suy giảm hiệu quả trong hoạch định và thực thi chính sách của Nhà nước. Trong thời đại số, việc coi dữ liệu là tài nguyên chiến lược có thể ảnh hưởng nghiêm trọng đến sức mạnh quốc gia.

Hai là, tác động đến năng lực quản lý và điều tiết kinh tế

Sự phát triển của nền kinh tế số đã tạo ra những thách thức mới trong công tác quản lý kinh tế, cụ thể nhất là trong lĩnh vực thuế và quản lý doanh nghiệp kinh doanh trên không gian mạng. Mỗi năm, Việt Nam đối mặt với sự thất thu hàng tỷ USD từ các giao dịch thương mại điện tử xuyên biên giới⁽²⁰⁾. Dưới tác động của công nghệ tài chính mới, việc quản lý nhà nước đối với các hoạt động tài chính gặp phải những thách thức không nhỏ. Theo báo cáo gần đây của Crypto Crunch App, Việt Nam xếp thứ ba trong bảng xếp hạng về lượng người nắm giữ tiền ảo trên thế giới, với hơn 1/4 dân số sở hữu tiền ảo⁽²¹⁾. Sự phát triển của tiền điện tử và blockchain đã làm suy giảm hiệu lực của các công cụ chính sách tiền tệ truyền thống, qua đó

hạn chế đi khả năng điều tiết nền kinh tế bằng các công cụ, chính sách này.

Ba là, tác động đến khả năng thực thi pháp luật

Toàn cầu hóa số đã tạo ra những thách thức mới trong việc thực thi pháp luật của Nhà nước. Tính xuyên biên giới của không gian mạng đã làm giảm hiệu quả của các công cụ thực thi pháp luật truyền thống. Các mối đe dọa an ninh mạng đã cho thấy giới hạn của quyền lực chủ quyền truyền thống. Các tác nhân nhà nước và phi nhà nước có thể phát động các cuộc tấn công mạng từ bất kỳ đâu, khiến các cơ chế phòng thủ lãnh thổ truyền thống trở nên mất hiệu lực đáng kể.

Đồng thời, với việc gia tăng tương tác trên không gian mạng, nguy cơ xâm phạm thông tin và các hành vi trái phép cũng tăng theo, trong đó không chỉ nhắm vào các cá nhân, mà còn là các doanh nghiệp. Theo Thống kê của Cybersecurity Ventures, riêng trong năm 2023, thiệt hại bởi các vụ tấn công mạng trên toàn thế giới là khoảng 08 nghìn tỷ USD (tương đương gần 196 triệu tỷ VNĐ)⁽²²⁾. Tại Việt Nam, có tới 46,15% cơ quan, doanh nghiệp bị tấn công mạng trong năm 2024; số vụ tấn công mạng ước tính lên tới hơn 659.000 vụ⁽²³⁾. Theo thống kê của Trung tâm Viễn thông Công viên Phần mềm Quang Trung (QTSC), trong nửa đầu năm 2024, có hơn 5.000 vụ tấn công mạng nhằm vào các hệ thống tại Việt Nam, tăng khoảng 40% so với cùng kỳ năm 2023⁽²⁴⁾. Tỷ lệ phá án đối với các vụ án về an ninh mạng còn thấp. Theo Bộ Công an, giai đoạn 2019 - 2022, cơ quan điều tra các cấp Công an tỉnh đã khởi tố 52 vụ án liên quan đến an ninh mạng và công nghệ cao (chiếm 1,62% tổng số vụ án khởi tố). Năm 2023, khởi tố 38 vụ tội phạm liên quan đến không gian mạng và sử dụng công nghệ cao (chiếm 5,66% tổng số vụ án đã khởi tố). Năm 2024, khởi tố 66 vụ án liên quan đến tội

phạm sử dụng công nghệ cao (chiếm 9,7% số vụ đã khởi tố)⁽²⁵⁾. Việc xử lý các vi phạm xuyên biên giới gặp nhiều khó khăn do sự khác biệt về hệ thống pháp luật giữa các quốc gia. Theo báo cáo của Cơ quan phòng, chống ma túy và tội phạm của Liên hợp quốc (UNODC), chỉ có khoảng 35% các yêu cầu hợp tác quốc tế trong xử lý vi phạm trên không gian mạng được đáp ứng đầy đủ và kịp thời⁽²⁶⁾. Những thách thức trong việc phối hợp thực thi pháp luật xuyên quốc gia còn bao gồm thời gian phản hồi và tính hiệu quả của quy trình tương trợ tư pháp truyền thống⁽²⁷⁾.

Bốn là, tác động đến vai trò hoạch định chính sách

Trong bối cảnh toàn cầu hóa số, vai trò hoạch định chính sách của Nhà nước cũng phải đổi mới với nhiều thách thức mới. Tốc độ phát triển nhanh chóng của công nghệ số tạo ra khoảng cách giữa chính sách và thực tiễn. Chẳng hạn, trung bình mất khoảng 2 - 3 năm để một chính sách mới trong lĩnh vực công nghệ số được ban hành và có hiệu lực, trong khi công nghệ có thể thay đổi nhanh chóng chỉ trong vài tháng. Bên cạnh đó, sự phụ thuộc vào công nghệ nước ngoài cũng ảnh hưởng đến tính độc lập trong hoạch định chính sách của Nhà nước. Việc phân lớn hạ tầng số quốc gia phụ thuộc vào công nghệ nước ngoài đã hạn chế khả năng ra quyết định độc lập của Nhà nước trong nhiều lĩnh vực quan trọng.

Năm là, tác động đến cung cấp dịch vụ công

Toàn cầu hóa số cũng tác động mạnh mẽ đến phương thức cung cấp dịch vụ công của Nhà nước. Chuyển đổi số trong khu vực công vừa tạo cơ hội nâng cao hiệu quả phục vụ người dân, vừa đặt ra thách thức về bảo mật thông tin và an toàn dữ liệu. Từ năm 2022 đến nay, tỷ lệ dịch vụ công trực tuyến đã đạt được những tiến bộ đáng kể⁽²⁸⁾. Đồng thời, theo báo

cáo của Cục An toàn thông tin, Bộ Thông tin và Truyền thông (năm 2023), các sự cố an ninh mạng nhắm vào hệ thống dịch vụ công trực tuyến có xu hướng gia tăng trong những năm gần đây⁽²⁹⁾.

4. Quan điểm, giải pháp bảo vệ chủ quyền quốc gia của Việt Nam trên không gian mạng trong bối cảnh toàn cầu hóa số

Những năm gần đây, Đảng và Nhà nước Việt Nam đã thể hiện sự quan tâm sâu sắc trong việc thiết lập và bảo vệ chủ quyền quốc gia trên không gian mạng thông qua việc ban hành nhiều nghị quyết và chỉ thị quan trọng. Một dấu mốc đáng chú ý là Bộ Chính trị khóa XII ban hành Nghị quyết số 29-NQ/TW ngày 25/7/2018 “về Chiến lược bảo vệ Tổ quốc trên không gian mạng”. Nghị quyết này có vai trò then chốt, phản ánh tầm nhìn chiến lược của Đảng trong việc bảo vệ không gian mạng - một “lãnh thổ đặc biệt” của quốc gia, đồng thời hoàn thiện hệ thống bảo vệ Tổ quốc trong bối cảnh hiện đại. Cùng với đó là, Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị “về Chiến lược an ninh mạng quốc gia”. Các văn kiện này đã xác định bảo vệ Tổ quốc trong không gian mạng. Đảng xác định đây là trách nhiệm quan trọng, liên tục của toàn thể nhân dân, quân đội, Đảng và hệ thống chính trị⁽³⁰⁾. Bảo đảm an toàn, an ninh mạng đã được xác định là một trong ba nội dung quan trọng trong mục tiêu của Chiến lược bảo vệ Tổ quốc trong tình hình mới đó là: bảo vệ an ninh quốc gia, an ninh con người, an ninh kinh tế, an ninh mạng⁽³¹⁾ Luật An ninh mạng năm 2018 đã xác định những nguyên tắc bảo vệ an ninh mạng, trong đó nhấn mạnh nguyên tắc chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của

cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng và triển khai hoạt động bảo vệ an ninh mạng đối với kết cấu hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia⁽³²⁾.

Các văn kiện của Đảng đã xác định rõ những quan điểm chỉ đạo về bảo vệ chủ quyền quốc gia trong không gian mạng. Theo đó, vấn đề bảo vệ chủ quyền quốc gia cần được xây dựng trên cơ sở các nguyên tắc cơ bản về chủ quyền quốc gia, phù hợp với đặc thù của môi trường số. Cụ thể, cần phải nhận thức rõ ràng rằng, các quốc gia không tách biệt hoàn toàn khỏi môi trường số toàn cầu, mà cần có chiến lược phù hợp để bảo vệ lợi ích quốc gia trong quá trình hội nhập. Để bảo vệ chủ quyền, cần bảo đảm hài hòa giữa việc tham gia sâu rộng vào không gian mạng toàn cầu và duy trì khả năng tự chủ về công nghệ và hạ tầng số. Chiến lược phát triển kinh tế số cần được xây dựng trên nền tảng bảo đảm an toàn và chủ quyền trong không gian mạng và việc xây dựng và hoàn thiện khung pháp lý về chủ quyền số là nhiệm vụ ưu tiên hàng đầu. Tiếp đó, phát triển năng lực số quốc gia là nhiệm vụ quan trọng lâu dài, trong đó, phát triển ba thành tố chính: hạ tầng số, nhân lực số và năng lực đổi mới sáng tạo trong lĩnh vực công nghệ số.

Đảng xác định, bảo vệ Tổ quốc trong không gian mạng cần được thực hiện đồng bộ, toàn diện với các chiến lược khác: “Chiến lược bảo vệ Tổ quốc, Chiến lược quốc phòng, Chiến lược quân sự, Chiến lược bảo vệ an ninh quốc gia, Chiến lược bảo vệ biên giới quốc gia, Chiến lược bảo vệ Tổ quốc trên không gian mạng, Chiến lược an ninh mạng quốc gia và các chiến lược quốc phòng, an ninh chuyên ngành khác”⁽³³⁾. Quan điểm về kiên quyết khẳng định và bảo vệ chủ quyền quốc gia về an

ninh mạng được khẳng định trong trong định hướng phát triển đất nước giai đoạn 2021 - 2030 theo Nghị quyết Đại hội lần thứ XIII của Đảng⁽³⁴⁾.

Quan triệt quan điểm của Đảng, để bảo vệ chủ quyền quốc gia trên không gian mạng trong bối cảnh toàn cầu hòa số, ***cần thực hiện các giải pháp cụ thể*** sau:

Một là, hoàn thiện khung pháp lý về chủ quyền số, khung pháp lý này cần bao quát đầy đủ các khía cạnh của chủ quyền quốc gia trong không gian mạng, từ bảo vệ dữ liệu đến an ninh mạng và quản lý thông tin xuyên biên giới. Các văn bản pháp luật về chủ quyền số cần bảo đảm tính đồng bộ và thống nhất, tránh tình trạng chồng chéo hoặc mâu thuẫn. Đồng thời, khung pháp lý này cũng cần có tính linh hoạt để có thể điều chỉnh kịp thời trước những thay đổi nhanh chóng của công nghệ và môi trường số. Cần rà soát, cập nhật và bổ sung các văn bản pháp luật để đáp ứng những thách thức mới trong không gian mạng.

Cụ thể, cần tập trung vào các nội dung: (1) Hoàn thiện khung pháp lý về an ninh mạng, trong đó, chú trọng các quy định chặt chẽ nhằm bảo vệ hạ tầng số thiết yếu, quản lý dữ liệu xuyên biên giới và ứng phó với các mối đe dọa mới; cần có quy định rõ ràng về tiêu chuẩn an toàn cho các hệ thống hạ tầng quan trọng, như mạng viễn thông, hệ thống ngân hàng, cơ sở dữ liệu quốc gia, xác định trách nhiệm cụ thể của các cơ quan, tổ chức trong việc bảo vệ hạ tầng số, các biện pháp giám sát, cảnh báo sớm và phương án ứng phó khi xảy ra sự cố, quy định chặt chẽ việc lưu trữ, xử lý và chuyển giao dữ liệu ra nước ngoài (bao gồm các loại dữ liệu cần được bảo vệ đặc biệt và không được phép chuyển ra nước ngoài), thiết lập cơ chế giám sát hoạt động của các doanh nghiệp nước ngoài khi thu thập, sử dụng dữ liệu của người Việt Nam; (2) Xây dựng cơ chế

phối hợp liên ngành hiệu quả, cụ thể là thành lập cơ quan điều phối quốc gia về an ninh mạng, có thẩm quyền và nguồn lực phù hợp để điều phối các hoạt động bảo vệ chủ quyền số.

Hai là, phát triển hạ tầng số quốc gia an toàn, bảo mật là nền tảng quan trọng. Cần tăng cường đầu tư xây dựng hạ tầng số hiện đại, tập trung vào hai yếu tố: an toàn và bảo mật, đảm bảo tính hiện đại và đồng bộ; tập trung vào các công nghệ then chốt, như 5G, điện toán đám mây và trí tuệ nhân tạo, chú trọng phát triển các giải pháp về công nghệ và an ninh do Việt Nam phát triển, làm chủ công nghệ lõi để bảo vệ hệ thống hạ tầng số quan trọng. Phát triển các giải pháp an ninh mạng nội địa. Việt Nam cần làm chủ công nghệ lõi trong bảo vệ hạ tầng số thiết yếu, giảm phụ thuộc vào các giải pháp nước ngoài thông qua việc đẩy mạnh nghiên cứu và phát triển hệ sinh thái công nghệ nội địa mạnh, đồng bộ.

Ba là, phát triển nguồn nhân lực chất lượng cao về công nghệ số. Đây được coi là yếu tố quyết định. Việt Nam cần đào tạo đội ngũ chuyên gia an ninh mạng, có kiến thức sâu về các công nghệ mới, như AI, Machine Learning, Blockchain, IoT, có khả năng phân tích và xử lý dữ liệu lớn (Big Data), trong đó, chú trọng đổi mới chương trình đào tạo, thu hút và phát triển nhân tài, bao gồm cơ chế đãi ngộ đặc thù cho chuyên gia an ninh mạng, kết hợp với việc tạo môi trường làm việc chuyên nghiệp.

Bốn là, Việt Nam cần tăng cường hợp tác quốc tế và chủ động tham gia các diễn đàn đa phương về an ninh mạng. Thông qua đó, tích cực góp phần xây dựng các quy tắc ứng xử trong không gian mạng quốc tế, đồng thời thúc đẩy hợp tác song phương với các đối tác chiến lược nhằm tăng cường hợp tác kỹ thuật trong lĩnh vực an ninh mạng, chia sẻ thông tin về các

mối đe dọa an ninh mạng. Hợp tác quốc tế không chỉ giúp Việt Nam có cơ hội học hỏi kinh nghiệm quốc tế trong việc xây dựng chính sách và giải pháp kỹ thuật, mà còn cập nhật xu hướng phát triển công nghệ và an ninh mạng toàn cầu, tăng cường vị thế của Việt Nam trong cộng đồng quốc tế về an ninh mạng. Công ước Liên hợp quốc về Tội phạm mạng mới được Đại hội đồng Liên hợp quốc thông qua, sẽ được mở ký tại Thủ đô Hà Nội trong năm 2025 và có tên gọi là “Công ước Hà Nội” ghi dấu mốc quan trọng trong nỗ lực chung của cộng đồng quốc tế nhằm ứng phó với những mối đe dọa ngày càng tăng trên không gian mạng, đồng thời phản ánh vị thế, uy tín quốc tế ngày càng cao của đất nước, cũng như sự tham gia đóng góp tích cực, trách nhiệm và thực chất của Việt Nam trong toàn bộ quá trình đàm phán Công ước.

Năm là, nâng cao nhận thức của toàn xã hội về bảo vệ chủ quyền số. Triển khai kịp thời và hiệu quả Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị “về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia”, trong đó, cần đẩy mạnh công tác tuyên truyền, giáo dục như việc tích hợp nội dung an toàn thông tin vào chương trình giáo dục các cấp, kết hợp với truyền thông đại chúng. Phát huy vai trò của doanh nghiệp, có cơ chế khuyến khích doanh nghiệp đầu tư cho an ninh mạng và tham gia vào công tác bảo vệ chủ quyền số.

5. Kết luận

Toàn cầu hóa số đã và đang tạo ra những tác động sâu rộng đến chủ quyền quốc gia, đặt ra những thách thức mới đòi hỏi cách tiếp cận toàn diện và đồng bộ trong việc bảo vệ lợi ích quốc gia trên không gian mạng. Trong bối cảnh này, việc bảo vệ chủ quyền quốc gia của Việt Nam trên không gian mạng không chỉ là nhiệm vụ của các cơ quan chức năng, mà còn đòi

hỏi sự tham gia tích cực của toàn xã hội. Để triển khai hiệu quả các giải pháp đề xuất, cần có sự quyết tâm chính trị mạnh mẽ, sự đầu tư nguồn lực thỏa đáng, đặc biệt là sự đồng thuận, ủng hộ của toàn xã hội. Việc xây dựng một không gian mạng an toàn, lành mạnh, đáp ứng yêu cầu phát triển bền vững của đất nước trong kỷ nguyên số là mục tiêu quan trọng cần được ưu tiên trong giai đoạn hiện nay □

- (1) Phong Vân, *Thế giới có 5 tỉ người dùng mạng xã hội*, <https://thanhnien.vn>, ngày 06/02/2024
- (2) Lê Thiên Hương, *Toàn cầu hóa số: tương lai nào cho chúng ta?*, <https://thesaigontimes.vn>, ngày 20/01/2023
- (3) Bộ Thông tin và Truyền thông, *Số liệu phát triển lĩnh vực Viễn thông năm 2023*, <https://mic.gov.vn>, ngày 10/01/2024
- (4) Castells, M, *The Rise of the Network Society*. Wiley-Blackwell, 2010
- (5) Friedman, T. L, *The World Is Flat: A Brief History of the Twenty-first Century*. Farrar, Straus and Giroux, 2005
- (6) Cheng, Y., et al, *Cyber Globalization: Theories, Trends and Challenges*. Journal of Global Information Technology Management, 22(4), 232-249, 2019
- (7) Jenkins, H, *Convergence Culture: Where Old and New Media Collide*. NYU Press, 2006
- (8) Held, D, & McGrew, A, *Globalization/Anti-Globalization: Beyond the Great Divide*. Polity, 2007
- (9) Floridi, L, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*. Philosophy & Technology, 33(3), 369-378, 2020
- (10) Couture, S., & Toupin, S, *What does the notion of "sovereignty" mean when referring to the digital?* New Media & Society, 21(10), 2305-2322. <https://doi.org/10.1177/1461444819865984>, 2019
- (11) và (13) Pohle, J., & Thiel, T, *Digital sovereignty*. Internet Policy Review, 9(4), 1-19 và 1-19, 2020
- (12) Creemers, R, *China's approach to cyber sovereignty*. Policy and Society, 39(3), 416-432, 2020

- (14) DeNardis, L. (2020), *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press
- (15) Nye, J. S, *Cyber Power and State Security*. International Security, 42(3), 44-83, 2018
- (16) và (18) Huyền Thanh, *Một công trình khoa học mạng tầm chiến lược về chủ quyền không gian mạng*, <https://cand.com.vn>, ngày 02/12/2022
- (17) Đại tướng, GS, TS. Tô Lâm, *Chủ quyền không gian mạng: Yêu cầu thời đại và nghĩa vụ quốc gia*, Nxb Công an nhân dân, Hà Nội, 2021, Lời mở đầu
- (19) Thủy Diệu, *Thị trường IDC rất nhiều tiềm năng*, <https://vneconomy.vn>, ngày 07/11/2023
- (20) Nguyễn Giang, *Thu thuế thương mại điện tử xuyên biên giới - Bài 1: Những con số "biết nói"*, <https://dien-dandoanhnghiep.vn>, ngày 16/6/2023
- (21) Trần Mạnh, *Tiền ảo tăng nóng, cấp thiết hoàn thiện khung pháp lý*, <https://baodautu.vn>, ngày 01/3/2024
- (22) Thủy Diệu, *Thế giới mất 8.000 tỷ USD vì tấn công mạng*, <https://vneconomy.vn>, ngày 29/02/2024
- (23) Mai Tấn, *Tấn công mạng tăng mạnh về quy mô và số lượng*, <https://thoibaotaichinhvietnam.vn>, ngày 23/12/2024
- (24) Minh Sơn, *Hơn 5.000 vụ tấn công mạng nhằm vào các hệ thống tại Việt Nam trong 6 tháng*, <https://www.vietnamplus.vn>, ngày 11/11/2024
- (25) Quang Cường, *Nhận diện xu hướng vi phạm pháp luật về an ninh, trật tự trên không gian mạng*, <https://baotintuc.vn>, ngày 24/12/2024
- (26) UNODC, *Challenges and Good Practices in International Cooperation in Cybercrime Investigations*, 2022
- (27) Europol (2023), *Internet Organised Crime Threat Assessment (IOCTA)*
- (28) Bộ Thông tin và Truyền thông, *Sách trắng Công nghệ thông tin và Truyền thông Việt Nam 2023*, <https://mic.mediacd.vn/639352410187198464/2024/4/26/sach-trang-2023-tv-ok-17141213611582082749916.pdf>
- (29) Bộ Thông tin và Truyền thông, Cục An toàn thông tin, *Báo cáo An toàn thông tin Việt Nam 2023*
- (30) Nghị quyết số 29-NQ/TW ngày 25/7/2018 của Bộ Chính trị "về Chiến lược bảo vệ Tổ quốc trên không gian mạng", Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị "về Chiến lược an ninh mạng quốc gia"
- (31) Nghị quyết số 44-NQ/TW ngày 24/11/2023 của Ban Chấp hành Trung ương Đảng khóa XIII "về Chiến lược bảo vệ Tổ quốc trong tình hình mới"
- (32) Điều 4 Luật An ninh mạng năm 2018
- (33) và (34) Đảng Cộng sản Việt Nam, *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, t.I, Nxb Chính trị quốc gia Sự thật, Hà Nội, 2021, tr.160 và 155-161