Bảo đảm an ninh thông tin ở Mỹ, Trung Quốc và khuyến nghị giải pháp cho Việt Nam

Ngô Thị Mai Diên(*)
Nguyễn Thị Lê(**)

Tóm tắt: *Lợi dụng sự tiến bộ, phát triển của khoa học công nghệ trong cuộc Cách mạng Công nghiệp lần thứ tư cùng những biến động phức tạp của tình hình trong nước và thế giới, các thế lực thù địch đang khai thác triệt để các công cụ truyền thông, không gian mạng để tạo ra thông tin, dữ liệu giả, truyền bá các quan điểm xuyên tạc, sai trái, thù địch ở quy mô ngày càng lớn, với thủ đoạn ngày càng tinh vi. Do vậy, công tác bảo đảm an ninh thông tin góp phần bảo vệ nền tảng tư tưởng của Đảng có ý nghĩa cấp thiết. Bài viết đề cập đến một số chính sách, chiến lược bảo đảm an ninh thông tin ở Mỹ và Trung Quốc, từ đó đề xuất một số khuyến nghị cho Việt Nam*.

Từ khóa: An ninh thông tin, Nền tảng tư tưởng, Đảng Cộng sản, Việt Nam, Mỹ, Trung Quốc

Abstract: *Taking advantage of the progress and outstanding development of science and technology in the Fourth Industrial Revolution as well as the complex fluctuations of the domestic and world situation, hostile forces are thoroughly exploiting communication tools and cyberspace to create fake information and data, spreading distorted, false and hostile views on an increasingly large scale and with increasingly sophisticated tricks. Therefore, the work of ensuring information security, contributing to protecting the Vietnamese Communist Party's ideological foundation is of urgent significance. The article mentions a number of policies and strategies to ensure information security in the US and China, thereby proposing some recommendations for Vietnam.*

Keywords: Information Security, Ideological Foundation, Vietnamese Communist Party, US, China

Ngày nhận bài: 23/5/2024; Ngày duyệt đăng: 15/6/2024

1. Mở đầu

Sự phát triển nhanh chóng của Internet, của các nền tảng công nghệ hiện đại, đặc biệt là công nghệ trí tuệ nhân tạo (AI) không chỉ đem lại cơ hội tiếp cận, tương tác thông tin dễ dàng cho từng cá nhân với tốc độ đường truyền nhanh, độ bao phủ rộng và chi phí thấp, mà còn cung cấp các công cụ, phương tiện hiện đại giúp nhanh chóng tạo thành các thông tin giả mạo, sai lệch, xấu độc,… gây ra những hậu quả nghiêm trọng đối với an ninh thông tin (ANTT) -

(*) ThS., NCVC, Viện Thông tin Khoa học xã hội, Viện Hàn lâm Khoa học xã hội Việt Nam;
Email: maidienissi@gmail.com
(**) ThS., NCVC, Viện Thông tin Khoa học xã hội, Viện Hàn lâm Khoa học xã hội Việt Nam;
Email: lenguyen22@gmial.com

thành tố trọng yếu của an ninh quốc gia. Đây là thách thức an ninh phi truyền thống ở phạm vi toàn cầu. Để ứng phó kịp thời, hiệu quả với những diễn biến cấp bách, phức tạp, khó lường của tình hình ANTT hiện nay, Việt Nam có thể tham khảo các chính sách và công nghệ bảo đảm ANTT của Mỹ và Trung Quốc - hai quốc gia có công nghệ chiến lược tiên phong, có năng lực không gian mạng hàng đầu thế giới.

2. Bảo đảm an ninh thông tin ở Mỹ

Mỹ là một trong những quốc gia dẫn đầu thế giới về chiến lược, quy định và triển khai các hoạt động cụ thể trong bảo vệ ANTT cơ sở hạ tầng quan trọng. Sau khi lên nắm quyền, Tổng thống Mỹ Joe Biden đã ban hành Sắc lệnh hành pháp số 14028 về "Cải thiện an ninh mạng quốc gia" (Executive Order 14028: Improving the Nation's Cybersecurity)[1] và "Biên bản ghi nhớ an ninh quốc gia về Cải thiện an ninh mạng cho các hệ thống kiểm soát cơ sở hạ tầng quan trọng" (National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems)[2], làm rõ các mục tiêu và phương hướng trong bảo vệ an ninh cơ sở hạ tầng quan trọng quốc gia. Tháng 3/2022, Tổng thống J. Biden ký ban hành "Đạo luật Báo cáo sự cố mạng cơ sở hạ tầng quan trọng năm 2022" (Cyber Incident Reporting for Critical Infrastructure Act of 2022 Publication)[3] làm rõ thêm các quy tắc về báo cáo sự cố an ninh mạng và chia sẻ thông tin các mối đe dọa. Tháng 3/2023, Nhà Trắng công bố "Chiến lược An ninh mạng quốc gia" (National Cybersecurity Strategy)[4] mới, lần đầu coi việc bảo vệ cơ sở hạ tầng quan trọng là trụ cột đầu tiên của an ninh mạng quốc gia; đồng thời đề xuất "xây dựng các yêu cầu về an ninh mạng, mở rộng hợp tác công - tư, tích hợp các nguồn lực xã hội, cập nhật các kế hoạch và quy trình ứng phó sự cố an ninh mạng, phát triển năng lực an ninh, quốc phòng hiện đại".

Chiến lược An ninh mạng năm 2023 của Mỹ gồm 02 định hướng xuyên suốt. *Một*, chuyển trọng tâm trách nhiệm bảo vệ an ninh mạng từ người dân, doanh nghiệp nhỏ, chính quyền địa phương sang các doanh nghiệp, tập đoàn công nghệ lớn có đủ tài nguyên và năng lực, chịu trách nhiệm xây dựng, vận hành và bảo trì hệ thống mạng trong nước. *Hai*, các cơ quan chính phủ sẵn sàng đầu tư, can thiệp khi cần thiết để xây dựng một hệ sinh thái số bảo đảm ANTT trong dài hạn. Các doanh nghiệp, tập đoàn buộc phải tuân thủ những yêu cầu, tiêu chuẩn tối thiểu về công nghệ và phải chịu trách nhiệm pháp lý nếu vi phạm.

Kế thừa chiến lược của chính quyền tiền nhiệm, chiến lược này cũng đề cao vai trò của không gian mạng như một bộ phận của sức mạnh quốc gia, phát huy vai trò và trách nhiệm của khu vực tư nhân, tích cực đầu tư vào khoa học, công nghệ, tăng cường hợp tác quốc tế. Điểm mới của

[1] Xem: *Improving the Nation's Cybersecurity*, https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

[2] Xem: *National security memorandum on improving cybersecurity for critical infrastructure control systems*, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[3] Xem: *Cyber incident reporting for critical infrastructure act of 2022*, https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf

[4] Xem: *National Cybersecurity Strategy*, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Chiến lược An ninh mạng năm 2023 là bổ sung cấu phần "an ninh", thể hiện ưu tiên cao của chính quyền đối với yếu tố an ninh quốc gia, đặt nguy cơ tấn công mạng tương đương mối đe dọa an ninh quốc gia, đề cao trách nhiệm của các doanh nghiệp, tập đoàn công nghệ.

Để triển khai hiệu quả Chiến lược, chính quyền Biden chú trọng 05 nhóm giải pháp: (i) Bảo vệ cơ sở hạ tầng trọng yếu, trong đó có thiết lập các yêu cầu, tiêu chuẩn an ninh bắt buộc đối với các ngành, các lĩnh vực thiết yếu; thúc đẩy hợp tác công - tư; hiện đại hóa hệ thống mạng liên bang và cập nhật kế hoạch ứng phó với sự cố mạng liên bang. (ii) Vô hiệu hóa các tác nhân đe dọa an ninh mạng đối với nước Mỹ thông qua việc sử dụng mọi biện pháp, mọi công cụ sức mạnh của quốc gia, như ngoại giao, tình báo, quân sự, tài chính, luật pháp… (iii) Có hình thức khuyến khích (trợ cấp, ưu đãi thuế liên bang) cho các dự án hạ tầng mạng bảo đảm ANTT; quy trách nhiệm pháp lý cho các doanh nghiệp, tập đoàn không quản lý tốt dữ liệu hoặc cung cấp sản phẩm, dịch vụ công nghệ kém an toàn. (iv) Huy động đầu tư từ cả hai khu vực công - tư, tăng ngân sách liên bang cho nghiên cứu và phát triển các công nghệ an ninh mạng thế hệ mới, chú trọng mã hóa lượng tử, phát triển nguồn nhân lực an ninh mạng. (v) Thúc đẩy hợp tác quốc tế theo hướng: tăng cường năng lực cho các đồng minh, đối tác để các quốc gia này có thể tự vệ trước các mối đe dọa trên không gian mạng; hợp tác xử lý các mối đe dọa; phối hợp xây dựng hệ sinh thái số toàn cầu an toàn và bền vững, xây dựng các chuỗi cung "sạch" về 5G và các hạ tầng mạng không dây thế hệ mới (Theo: Nguyễn Hồng Quang, 2024).

Về AI, Ngoại trưởng Mỹ Antony Blinken khẳng định, chống thông tin sai lệch, trong đó có những nội dung do AI tạo ra, là một lợi ích "sống còn" đối với an ninh quốc gia và là ưu tiên ngoại giao của Mỹ. Theo ông Blinken, các công nghệ kỹ thuật số, trong đó có truyền thông xã hội và AI, đã đẩy nhanh đáng kể tốc độ và quy mô lan truyền thông tin sai lệch. Trước đây, các trang mạng tuyên truyền thông tin cần người viết nội dung, thì nay các công cụ AI tạo sinh có thể đảm nhận việc này với chi phí rẻ hơn và tốc độ nhanh hơn trong khi nội dung khó xác minh hơn. Washington đang nỗ lực đẩy lùi vấn nạn này bằng cách tăng cường các biện pháp ngăn chặn hoạt động dùng phần mềm gián điệp để giả danh các nhà báo, nhà hoạt động xã hội; siết chặt trừng phạt, hạn chế xuất khẩu và hạn chế thị thực đối với những sản phẩm, cá nhân và thể chế bị phát hiện sai phạm; chú trọng các biện pháp giúp người dân cảnh giác hơn; và chống lại mọi hình thức thao túng thông tin, như khuyến khích các nền tảng truyền thông xã hội dán nhãn lưu ý các nội dung do AI sáng tạo để người dùng biết rõ hình ảnh và nội dung là thật hay là sản phẩm dàn dựng (Lê Ánh, 2024).

Mới đây nhất, *Báo cáo về Hiện trạng an ninh mạng của Mỹ* công bố vào tháng 5/2024 (2024 Report on the Cybersecurity Posture of the United States)[1] đã thông tin cập nhật về bối cảnh phát triển công nghệ hiện đại, về sự hiện diện của các công nghệ mới, tác động của những mối đe dọa, lỗ hổng an ninh mạng đối với an ninh quốc gia, sự phát triển kinh tế - xã hội và các giá trị dân chủ. Báo cáo nhấn mạnh, khả năng dễ bị tổn thương trước

[1] Xem: *2024 Report on the cybersecurity posture of the United States*, https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

"sự can thiệp" trên không gian mạng là "đặc biệt nghiêm trọng", đòi hỏi phải có những phản ứng mạnh mẽ và kịp thời của tất cả các tổ chức, cá nhân để bảo đảm ANTT trong không gian mạng, trong hệ sinh thái kỹ thuật số.

Báo cáo đã chỉ ra bốn vấn đề nổi bật về an ninh mạng trong năm 2023 là: cơ sở hạ tầng quan trọng phải đối mặt với mức độ rủi ro ngày càng gia tăng; phần mềm tống tiền và phần mềm gián điệp thương mại tiếp tục phát triển các chiến lược tinh vi; chuỗi cung ứng liên kết phức tạp cho phép các tác nhân độc hại xâm phạm trên quy mô lớn; AI phát triển mạnh mẽ đặt ra nhiều thách thức đối với việc quản trị ANTT.

Trước tình trạng này, Mỹ đã nỗ lực: (i) áp dụng nhiều biện pháp để bảo vệ cơ sở hạ tầng quan trọng; (ii) thực hiện quản trị đa bên về ANTT, tăng cường hợp tác giữa các cơ quan, tổ chức trong việc thực thi các giải pháp bảo đảm an ninh mạng, ANTT; (iii) tăng cường chia sẻ thông tin về rủi ro an ninh để tăng cường năng lực ứng phó; (iv) thực hiện nhiều chiến dịch đáp trả các cuộc tấn công mạng độc hại; (v) tiếp tục phát triển công nghệ lượng tử, công nghệ bảo mật đám mây, mô hình bảo mật Zero Trust (hoạt động dựa trên giả định rằng tất cả các mối đe dọa đều có thể xảy ra cho dù đó là nguồn truy cập đáng tin cậy); (vi) tăng cường bảo mật phần mềm để tạo ra các sản phẩm và dịch vụ an toàn hơn; (vii) kích hoạt nền kinh tế kỹ thuật số trao quyền và bảo vệ người tiêu dùng, triển khai chương trình dán nhãn chứng nhận an ninh "Cyber Trust Mark"; (viii) thúc đẩy hệ sinh thái kỹ thuật số mở ra tầm nhìn tích cực về một Internet mở, miễn phí, toàn cầu, có thể tương tác, đáng tin cậy, có thể truy cập và an toàn; (ix) ngăn chặn sự phổ biến và lạm dụng các công nghệ kỹ thuật số như phần mềm gián điệp thương mại; (x) xây dựng liên minh chống lại các cuộc tấn công mạng độc hại, hướng đến "sự đồng thuận về các nguyên tắc chỉ đạo", thúc đẩy "các chuẩn mực toàn cầu" trong việc phát triển và sử dụng công nghệ AI (Xem thêm: Nguyễn Thạc Ngọc, 2023; Nguyễn Anh Tuấn, 2024; Trần Văn Liệu, 2024).

3. Bảo đảm an ninh thông tin ở Trung Quốc

Theo Chủ tịch Tập Cận Bình, Trung Quốc phải xây dựng rào chắn an ninh vững chắc xung quanh Internet của nước này dưới sự giám sát của Bắc Kinh; phải tuân thủ sự quản lý của Đảng Cộng sản Trung Quốc đối với Internet; phải kiên trì quản lý, vận hành và đảm bảo quyền truy cập Internet theo luật pháp; và phải tuân thủ nguyên tắc làm cho Internet hoạt động vì người dân (Dẫn theo: Bình An, 2023).

Đối với các nhà chức trách Trung Quốc, virus đe dọa ANTT giống virus sinh học về phương pháp đe dọa, sức tàn phá, tốc độ lan truyền và đối tượng tấn công, nên các biện pháp phòng, chống virus sinh học có ý nghĩa tham khảo quan trọng đối với công tác bảo đảm ANTT, ngăn chặn và loại bỏ virus mạng. Theo đó, cần: (i) nhận biết chính xác, nhạy bén các loại virus đang trong giai đoạn lây truyền bước đầu nhưng tiềm ẩn nguy cơ lớn, cảnh báo sớm các loại virus này làm cơ sở triển khai các biện pháp phòng ngừa, kiểm soát; (ii) xác định, phân loại các máy chủ hoặc nghi nhiễm, hoặc bị nhiễm virus có triệu chứng hoặc không có triệu chứng; (iii) căn cứ các loại máy chủ và tình trạng lây nhiễm để tiến hành các biện pháp xử lý phù hợp như ngắt kết nối, cách ly, cài đặt lại, củng cố hệ thống (Xem: Nguyễn Thị Trường Giang, 2023).

Trung Quốc cũng rất coi trọng việc bảo vệ an ninh cơ sở hạ tầng thông tin

quan trọng, gồm các ngành và lĩnh vực như dịch vụ thông tin và truyền thông công cộng, năng lượng, giao thông vận tải, bảo tồn nguồn nước, tài chính, dịch vụ công, chính phủ điện tử, công nghiệp, công nghệ quốc phòng. Để xây dựng một "pháo đài an ninh" cho cơ sở hạ tầng thông tin quan trọng, Trung Quốc đã: (i) phân định rõ chức năng, nhiệm vụ của bộ phận an ninh công cộng, cơ quan viễn thông và bộ phận bảo vệ an ninh cơ sở hạ tầng thông tin quan trọng; (ii) thực hiện các biện pháp bảo vệ chính yếu cho cơ sở hạ tầng thông tin quan trọng; (iii) xác định kịp thời các mối đe dọa mạng lớn và các nỗ lực tấn công để liên tục cải thiện khả năng phòng thủ chuyên sâu, nâng cao tính chủ động; (iv) tăng cường nghiên cứu và phát triển công nghệ then chốt để hỗ trợ bảo vệ ANTT: công nghệ chủ động phát hiện rủi ro bảo mật dữ liệu, công nghệ bảo vệ dữ liệu kết hợp các thuật toán cường độ cao, công nghệ chia sẻ bảo mật dữ liệu hỗ trợ bảo vệ quyền riêng tư, công nghệ hỗ trợ giám sát an ninh cho các giao dịch dữ liệu (Xem: Nguyễn Thị Trường Giang, 2023).

Luật An ninh Dữ liệu (中华人民共和国数据安全法, Data Security Law - DSL) được Chính phủ Trung Quốc thông qua ngày 10/6/2021 và có hiệu lực từ ngày 01/9/2021. Đạo luật này áp dụng với các tổ chức, cá nhân Trung Quốc hoạt động trong và ngoài nước, cũng như tổ chức, cá nhân nước ngoài hoạt động trên lãnh thổ Trung Quốc. Trước đó, Trung Quốc đã có hai đạo luật liên quan đến bảo vệ dữ liệu và thông tin: Luật An ninh mạng (中华人民共和国网络安全法, Cyber Security Law - CSL) được thực thi từ ngày 01/6/2017; Luật Bảo vệ thông tin cá nhân (中华人民共和国 个人信息保护法, Personal Infomation Protection Law - PIPL) có hiệu lực từ ngày 01/11/2021. Cả ba luật này đều có các điều khoản liên quan đến cơ sở hạ tầng thông tin quan trọng, dữ liệu quan trọng, yêu cầu lưu trữ cục bộ, chuyển giao dữ liệu qua biên giới... giúp tạo thành "cỗ xe tam mã" quản lý không gian mạng, bảo vệ dữ liệu của Trung Quốc.

3.1. Mục tiêu của CSL là bảo đảm an ninh mạng; bảo vệ chủ quyền không gian mạng, an ninh quốc gia và lợi ích công cộng; bảo vệ quyền lợi hợp pháp của công dân, pháp nhân và các tổ chức khác; thúc đẩy phát triển thông tin hóa kinh tế và xã hội. CSL quy định các nhà cung cấp thông tin, dịch vụ thông tin phải: (i) Thiết lập cấp độ an ninh mạng, hệ thống bảo vệ theo cấp độ - hệ thống đánh giá công đối với cơ cấu quản lý an ninh mạng. (ii) Tuân thủ tiêu chuẩn bắt buộc của quốc gia, không được phép cài đặt các chương trình độc hại. Khi phát hiện sản phẩm hoặc dịch vụ có khiếm khuyết, lỗ hổng bảo mật, hoặc các rủi ro khác, phải ngay lập tức thực hiện các biện pháp cần thiết, thông báo cho người dùng và báo cáo cơ quan quản lý có thẩm quyền. (iii) Yêu cầu đăng ký thông tin thật khi cung cấp các dịch vụ như kết nối mạng, kết nối mạng điện thoại cố định và di động, dịch vụ chia sẻ thông tin, dịch vụ tin nhắn… (iv) Nhà điều hành cơ sở hạ tầng thông tin quan trọng, vận hành mạng lưới thông tin không chỉ cần thực hiện các biện pháp bảo mật, mà còn phải phân loại dữ liệu, bảo vệ dữ liệu quan trọng bằng cách sao lưu và mã hóa, xây dựng kế hoạch ứng phó với sự cố an ninh mạng. (v) Nếu cài đặt chương trình độc hại hoặc không thực hiện biện pháp đối với rủi ro như lỗi sản phẩm, dịch vụ hoặc lỗ hổng bảo mật, người vi phạm sẽ nhận được lệnh sửa chữa, cảnh báo và nộp phạt. Mức phạt sẽ thay đổi tùy theo nội dung vi phạm, có thể bị yêu cầu đóng trang

web, hủy bỏ giấy phép kinh doanh, hoặc tạm dừng hoạt động kinh doanh (Xem: Văn phòng Luật sư Monolith, 2024a).

3.2. Trong bối cảnh nhiều vấn đề phức tạp liên quan đến dữ liệu nảy sinh, đặc biệt khi các nền tảng trực tuyến thu thập dữ liệu cá nhân người dùng một cách quá mức, Chính phủ Trung Quốc đã thông qua, ban hành PIPL gồm 8 chương, 74 điều, được đánh giá là bộ luật bảo vệ thông tin cá nhân toàn diện cấp quốc gia đầu tiên ở Trung Quốc. Nhìn tổng thể, bộ luật bao trùm toàn bộ quá trình xử lý thông tin cá nhân, từ thu thập, lưu trữ đến biên tập, sử dụng, phổ biến, cung cấp, công khai, xóa bỏ… dữ liệu. PIPL "nói không" với việc thu thập quá mức dữ liệu cá nhân, cung cấp cơ sở pháp lý cho hoạt động xử lý thông tin cá nhân, bảo đảm đầy đủ quyền lợi của người dùng trong việc bảo vệ thông tin cá nhân, cung cấp hướng dẫn giúp doanh nghiệp tuân thủ các quy định liên quan (Xem: Chân Hoàn, 2021). Chế tài xử lý đối với hành vi vi phạm quyền dữ liệu cá nhân theo quy định của PIPL rất nghiêm, như bắt buộc khắc phục hậu quả, bồi thường thiệt hại, bị tịch thu thu nhập bất hợp pháp, đình chỉ dịch vụ, thu hồi giấy phép hoạt động hoặc kinh doanh, phạt tiền lên tới 50 triệu Nhân dân tệ hoặc 5% doanh thu năm tài chính trước đó của tổ chức vi phạm. Trường hợp vi phạm nghiêm trọng còn có thể bị xử phạt theo Bộ luật Hình sự Trung Quốc, bị tịch thu tài sản và mức phạt tù cao nhất là chung thân (Xem: Trần Thị Việt Hà, 2024).

3.3. DSL gồm 7 chương, 55 điều, nhằm 5 mục tiêu: quy định hoạt động xử lý dữ liệu; bảo đảm an ninh dữ liệu; khuyến khích phát triển và sử dụng dữ liệu; bảo vệ quyền và lợi ích hợp pháp của cá nhân và tổ chức; bảo vệ chủ quyền, an ninh và lợi ích phát triển của quốc gia. DSL quy định: (i) Dữ liệu phải được phân loại và xếp hạng dựa trên mức độ tổn thất mà nó có thể gây ra hoặc do hậu quả của việc hủy hoại, rò rỉ dữ liệu. (ii) Cơ quan quản lý Trung ương về An ninh quốc gia chịu trách nhiệm ra quyết định chính, cân nhắc và điều phối nhiệm vụ bảo vệ dữ liệu của quốc gia; nghiên cứu, soạn thảo và hướng dẫn triển khai chiến lược bảo vệ dữ liệu quốc gia và các chỉ thị, chính sách lớn có liên quan; lập kế hoạch, điều phối, thiết lập cơ chế phối hợp cho công tác bảo vệ dữ liệu quốc gia. (iii) Các cơ quan có thẩm quyền về công nghiệp, viễn thông, giao thông vận tải, tài chính, tài nguyên thiên nhiên, y tế, giáo dục và công nghệ có trách nhiệm giám sát bảo mật dữ liệu trong các ngành và lĩnh vực tương ứng. (iv) Nhà nước thiết lập một cơ chế tập trung, hiệu quả và có thẩm quyền để giám sát, đánh giá, báo cáo, chia sẻ thông tin, cảnh báo rủi ro về bảo vệ dữ liệu. Cơ chế điều phối công tác bảo vệ dữ liệu quốc gia sẽ phối hợp với các bộ phận liên quan để tăng cường các hoạt động về thu thập, phân tích, xác định và cảnh báo thông tin rủi ro an toàn dữ liệu. (v) Nhà nước tích cực trao đổi, hợp tác quốc tế trong các lĩnh vực như quản trị an ninh dữ liệu, khai thác và sử dụng dữ liệu, tham gia vào việc biên soạn các quy tắc và tiêu chuẩn quốc tế về bảo vệ dữ liệu, thúc đẩy an ninh xuyên biên giới của dòng chảy dữ liệu. (vi) Các đơn vị thực hiện hoạt động xử lý dữ liệu phải thiết lập, áp dụng các biện pháp bảo vệ an toàn dữ liệu; tăng cường giám sát rủi ro, ứng phó hiệu quả với các rủi ro lỗi hoặc rò rỉ bảo mật dữ liệu (Xem: Nguyễn Quốc Toàn, Đặng Vũ Trung, 2021; Nguyễn Hồng Hải Đăng, 2022; Văn phòng Luật sư Monolith, 2024b; Nguyễn Đức Cường, Lê Trí Thành, Mai Văn Chuẩn, 2024).

Có thể nói, 3 đạo luật liên quan đến an ninh mạng, ANTT của Trung Quốc có những điểm khác biệt nhưng đều nhằm mục đích bảo đảm ANTT, phòng tránh, ngăn chặn việc thông tin, dữ liệu có thể bị xâm hại, bị thu thập, lưu trữ, mua bán và sử dụng trái phép, bị lợi dụng, xuyên tạc để truyền bá với các động cơ chống phá, gây tác động tiêu cực… Đặc biệt, DSL quy định rằng, Chính phủ sẽ thiết lập một cơ chế phân loại dữ liệu theo thứ bậc, theo đó các loại dữ liệu được ma trận hóa căn cứ vào mức độ quan trọng đối với sự phát triển kinh tế - xã hội, an ninh quốc gia, lợi ích công cộng, hoặc quyền và lợi ích hợp pháp của từng tổ chức, cá nhân. Dữ liệu quan trọng và dữ liệu cốt lõi được quản lý ở cấp độ nghiêm ngặt hơn và được ưu tiên bảo vệ; điều này đánh dấu việc dữ liệu được nhìn nhận như là loại hình tài sản/tài nguyên; giá trị trao đổi của dữ liệu vừa được tối ưu hóa, vừa trở nên chính thống và được công nhận rộng rãi thông qua công tác làm luật (Xem: Nguyễn Hồng Hải Đăng, 2022).

4. Một số khuyến nghị cho Việt Nam

Trên cơ sở những nội dung vừa trình bày ở trên, nhóm tác giả đề xuất một số khuyến nghị cho Việt Nam như sau[1]:

(i) Nêu cao quyết tâm chính trị, tiếp tục chủ động triển khai, thực hiện có hiệu quả chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước về vấn đề ANTT, phòng chống tin giả, tin xấu độc.

(ii) Tiếp tục cập nhật, thể chế hóa một cách đầy đủ, toàn diện hơn các đường lối, chủ trương và định hướng chính sách của Đảng, tạo khung khổ pháp lý minh bạch, chuyên nghiệp và hiệu quả hơn để bảo đảm ANTT.

(iii) Tăng cường kiểm soát, xử lý các lỗi vi phạm; đồng thời, hợp tác chặt chẽ với các tổ chức, cơ quan liên quan trong việc ngăn chặn, gỡ bỏ tin giả, tin xấu độc… đối với các ứng dụng truyền thông xã hội xuyên biên giới như Facebook, Google, Youtube, Tiktok, Telegram, Instagram, Zalo, Twitter, WhatsApp…

(iv) Chú trọng công tác tuyên truyền, nâng cao nhận thức: từ nhận thức rõ hiện trạng ANTT đến hiện thực hóa hành động; triển khai đấu tranh, phản bác nghiêm túc, hiệu quả các quan điểm sai trái, thù địch theo tinh thần Nghị quyết số 35-NQ/TW ngày 22/10/2018 của Bộ Chính trị khóa XII về Tăng cường bảo vệ nền tảng tư tưởng của Đảng.

(v) Trong thời gian tới, cần chú ý nghiên cứu, tiến hành sửa đổi, bổ sung Luật An ninh mạng năm 2018 theo hướng có quy định cụ thể, rõ ràng. Mỗi cơ quan, tổ chức cần xây dựng những bộ quy tắc, quy định về thông tin nội bộ, bảo mật dữ liệu của đơn vị mình.

(vi) Xúc tiến việc xây dựng cơ chế, hoạch định chính sách để kịp thời hỗ trợ các cơ quan thông tấn báo chí, các tổ chức, đơn vị tạo lập thông tin, truyền thông, các doanh nghiệp cung cấp dịch vụ Internet, tạo động lực sản xuất, đăng tải nội dung số trung thực, chính xác; xây dựng các ứng dụng truyền thông xã hội đủ mạnh để đáp ứng nhu cầu người dùng, nâng cao khả năng cạnh tranh, giảm sự phụ thuộc vào các phương tiện truyền thông xã hội nước ngoài.

(vii) Nâng cao năng lực, trình độ, bản lĩnh cho đội ngũ cán bộ làm công tác bảo đảm ANTT; đồng thời phải đầu tư trang thiết bị, công nghệ hiện đại nhằm phát hiện, ngăn chặn, cảnh báo và xử lý kịp thời các vấn đề, tình huống nảy sinh trong quá trình bảo đảm ANTT.

[1] Xem thêm: Phạm Thị Hoa, 2024; Nguyễn Đức Cường, Lê Trí Thành, Mai Văn Chuẩn, 2024.

(viii) Triển khai đồng bộ, hiệu quả các biện pháp nghiệp vụ trong bảo đảm an ninh mạng, ANTT; quản lý hiệu quả các trang web, tài khoản xã hội, có các biện pháp đấu tranh, triệt phá, xử lý tài khoản, bài viết cung cấp tin giả, tin xấu độc.

(ix) Có cơ chế khuyến khích, biểu dương, khen thưởng các tổ chức và cá nhân có đóng góp thiết thực vào công cuộc bảo đảm ANTT; đồng thời có chế tài xử phạt cương quyết, nghiêm minh đối với các tổ chức, cá nhân mạo danh, vi phạm các quy định về truyền thông, thông tin, truyền bá các quan điểm, tư tưởng phản động, luận điểm sai trái, xuyên tạc, lôi kéo, kích động lật đổ chính quyền, chống phá Nhà nước.

(x) Nghiên cứu kỹ lưỡng và thấu đáo các chính sách, chiến lược và chương trình hành động bảo đảm ANTT của các nước trên thế giới, trong đó có Mỹ và Trung Quốc, để ban hành luật định, hoàn thiện các quy định của pháp luật hài hòa với thông lệ, quy định quốc tế.

5. Kết luận

Hoàn thiện cơ chế, chính sách, pháp luật để bảo đảm ANTT, góp phần bảo vệ nền tảng tư tưởng của Đảng trên cơ sở nghiên cứu, tham khảo kinh nghiệm quốc tế là việc làm cần thiết. Luật An ninh mạng, Luật Bảo vệ thông tin cá nhân và Luật An ninh dữ liệu của Trung Quốc, các sắc lệnh, chiến lược, chương trình hành động của Mỹ và thực tế triển khai việc bảo đảm ANTT ở hai quốc gia này là những mẫu hình lý thuyết và thực tiễn để Việt Nam có thể xem xét tham khảo, trong quá trình nâng cấp khuôn khổ quản trị thông tin, dữ liệu, hình thành môi trường thông tin lành mạnh, tích cực, trở thành một trong những trụ cột phát triển kinh tế - xã hội quan trọng của đất nước trong kỷ nguyên số ❑

Tài liệu tham khảo

1. Bình An (2023), "Ông Tập yêu cầu 'quây rào kỹ' cho Internet ở Trung Quốc", Báo *Tuổi trẻ Online* ngày 05/7/2023, https://tuoitre.vn/ong-tap-yeu-cau-quay-rao-ky-cho-internet-o-trung-quoc-20230715201959904.htm
2. Lê Ánh (2024), "Mỹ: Công nghệ kỹ thuật số đẩy nhanh đáng kể tốc độ lan truyền tin sai lệch", Trang thông tin điện tử *VietnamPlus* ngày 18/3/2024, https://www.vietnamplus.vn/my-cong-nghe-ky-thuat-so-day-nhanh-dang-ke-toc-do-lan-truyen-tin-sai-lech-post935222.vnp
3. Nguyễn Đức Cường, Lê Trí Thành, Mai Văn Chuẩn (2024), "Pháp luật của một số quốc gia về bảo vệ dữ liệu cá nhân trên không gian mạng: Gợi mở hướng hoàn thiện pháp luật cho Việt Nam", Tạp chí *Giáo dục & Xã hội* ngày 17/3/2024, https://giaoducvaxahoi.vn/tin-phap-luat/phap-lu-t-c-a-m-t-s-qu-c-gia-v-b-o-v-d-li-u-ca-nhan-tren-khong-gian-m-ng-g-i-m-hu-ng-hoan-thi-n-phap-lu-t-cho-vi-t-nam.html
4. Nguyễn Thị Trường Giang (2023), "Một số kinh nghiệm giải quyết vấn đề an ninh mạng của Trung Quốc hiện nay", *Tạp chí Lý luận chính trị và Truyền thông* ngày 12/11/2023, https://lyluanchinhtrivatruyenthong.vn/mot-so-kinh-nghiem-giai-quyet-van-de-an-ninh-mang-cua-trung-quoc-hien-nay-p28047.html
5. Trần Thị Việt Hà (2024), "Pháp luật quốc tế về bảo vệ dữ liệu cá nhân và gợi mở cho Việt Nam", Tạp chí *Thế giới và Việt Nam* ngày 21/4/2024, https://baoquocte.vn/phap-luat-quoc-te-ve-bao-ve-du-lieu-ca-nhan-va-goi-mo-cho-viet-nam-268402.html#google_vignette

6. Phạm Thị Hoa (2024), "Nâng cao chất lượng, hiệu quả cơ chế kiểm soát và xử lý tin giả ở Việt Nam hiện nay dưới góc nhìn từ cách tiếp cận thể chế", *Tạp chí Cộng sản* ngày 13/4/2024, https://www.tapchicongsan.org.vn/web/guest/nghien-cu/-/2018/911902/nang-cao-chat-luong%2C-hieu-qua-co-che-kiem-soat-va-xu-ly-tin-gia-o-viet-nam-hien-nay-duoi-goc-nhin-tu-cach-tiep-can-the-che.aspx#
7. Chân Hoàn (2021), "Luật Bảo vệ thông tin cá nhân của Trung Quốc chính thức có hiệu lực", Tạp chí *Công nghệ & Đời sống* ngày 02/11/2021, https://congnghevadoisong.vn/luat-bao-ve-thong-tin-ca-nhan-cua-trung-quoc-chinh-thuc-co-hieu-luc-d45744.html
8. Trần Văn Liệu (2024), "Bảo đảm an ninh thông tin cơ sở hạ tầng quan trọng của Hoa Kỳ", Tạp chí *An toàn thông tin* ngày 11/1/2024, https://antoanthongtin.vn/chinh-sach---chien-luoc/bao-dam-an-ninh-thong-tin-co-so-ha-tang-quan-trong-cua-hoa-ky-109651.
9. Nguyễn Thạc Ngọc (2023), "Chính sách và công nghệ bảo đảm an ninh thông tin của một số nước trên thế giới và kinh nghiệm đối với Việt Nam", *Tạp chí Thông tin đối ngoại và khoa học* ngày 25/11/2023, https://vietnamhoinhap.vn/vi/chinh-sach-va-cong-nghe-bao-dam-an-ninh-thong-tin-cua-mot-so-nuoc-tren-the-gioi-va-kinh-nghiem-doi-voi-viet-nam-45930.htm
10. Nguyễn Hồng Quang (2024), "Đôi nét về Chiến lược an ninh mạng của Mỹ", Tạp chí *Quốc phòng toàn dân* ngày 25/3/2024, http://tapchiqptd.vn/vi/quoc-phong-quan-su-nuoc-ngoai/doi-net-ve-chien-luoc-an-ninh-mang-cua-my/21651.html
11. Nguyễn Quốc Toàn, Đặng Vũ Trung (2021), "Tìm hiểu Luật An toàn dữ liệu của Chính phủ Trung Quốc và khuyến nghị đối với Việt Nam trong tình hình mới", Tạp chí *An toàn thông tin* ngày 04/11/2021, https://antoanthongtin.vn/chinh-sach---chien-luoc/tim-hieu-luat-an-toan-du-lieu-cua-chinh-phu-trung-quoc-va-khuyen-nghi-doi-voi-viet-nam-trong-tinh-hi-107560
12. Nguyễn Anh Tuấn (2024), "CISA cung cấp dịch vụ an ninh mạng cho các tổ chức trọng yếu không thuộc chính quyền", Tạp chí *An toàn thông tin* ngày 21/12/2023, https://m.antoanthongtin.vn/ca-cong-cong/cisa-cung-cap-dich-vu-an-ninh-mang-cho-cac-to-chuc-trong-yeu-khong-thuoc-chinh-quyen-109623
13. Văn phòng Luật sư Monolith (2024a), *Luật An ninh mạng của Trung Quốc là gì? Giải thích các điểm cần tuân thủ*, https://monolith.law/vi/general-corporate/china-cyber-security-law#Tong_quan_ve_Luat_An_ninh_mang_Trung_Quoc, ngày 03/4/2024
14. Văn phòng Luật sư Monolith (2024b), *Luật An ninh Dữ liệu Trung Quốc là gì? Giải thích các biện pháp mà doanh nghiệp Nhật Bản nên áp dụng*, https://monolith.law/vi/general-corporate/china-data-security-law, ngày 03/4/2024.