

THỰC HIỆN CHÍNH SÁCH PHÁP LUẬT VỀ BẢO VỆ AN NINH THÔNG TIN Ở VIỆT NAM HIỆN NAY: THỰC TRẠNG VÀ GIẢI PHÁP

VŨ THỊ MỸ HẠNH*

Ngày nhận: 09/04/2024

Ngày phản biện: 29/04/2024

Duyệt đăng: 20/5/2024

Tóm tắt: Bài viết đề cập một số văn bản chính sách pháp luật bảo vệ an ninh thông tin ở Việt Nam, khái quát tình hình thực hiện chính sách pháp luật bảo vệ an ninh thông tin; trên cơ sở đó đề xuất một số giải pháp nhằm thực hiện có hiệu quả chính sách pháp luật bảo vệ an ninh thông tin ở Việt Nam trong giai đoạn hiện nay.

Từ khóa: bảo vệ an ninh thông tin; chính sách pháp luật.

Đặt vấn đề

Xuất phát từ tầm quan trọng của an ninh thông tin và bảo vệ an ninh thông tin, Đảng và Nhà nước luôn quan tâm đến chính sách pháp luật bảo vệ an ninh thông tin, từng bước xây dựng, kiện toàn hệ thống chính sách pháp luật bảo vệ an ninh thông tin quốc gia và đã có những tiến bộ trong công tác này, bên cạnh đó vẫn còn một số bất cập cần có những giải pháp khắc phục để bảo đảm việc thực hiện chính sách pháp luật về bảo vệ an ninh thông tin trong tình hình mới có hiệu quả cao hơn.

1. Khái quát về an ninh thông tin và chính sách pháp luật bảo vệ an ninh thông tin

Ở Việt Nam, an ninh thông tin được hiểu là việc bảo đảm thông tin trên mạng, không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân [4]. An ninh thông tin là một bộ phận không thể tách rời của an ninh quốc gia, bảo vệ an ninh thông tin là nhiệm vụ của toàn Đảng, toàn quân và của cả hệ thống chính trị cũng như mỗi người dân Việt Nam.

Chính sách bảo đảm an ninh thông tin là việc thiết lập các chiến lược và trách nhiệm của những cá nhân, tổ chức có liên quan nhằm bảo đảm 3 yêu cầu cơ bản của an ninh thông tin, đó là tính bí mật, tính toàn vẹn và tính sẵn sàng. Trong thời gian gần đây, trước sự phát triển mạnh mẽ của công nghệ, an ninh thông tin còn phải đáp ứng thêm một vài yêu cầu đó là tính chính xác, tính xác thực, tính tiện ích... Trong suốt quá trình lãnh đạo cách mạng giải phóng dân tộc và xây dựng chủ nghĩa xã hội, Đảng Cộng sản Việt Nam luôn quan tâm, chỉ đạo việc xây dựng và thực hiện chính sách pháp luật về an ninh thông tin, coi đây là nhiệm vụ quan trọng góp phần bảo vệ an ninh quốc gia

Về cơ bản, việc thực hiện chính sách bảo vệ an ninh thông tin bao gồm các nội dung: Hướng dẫn thực hiện; Tuyên truyền phổ biến; Đảm bảo các điều kiện cần thiết để thực hiện; Tổ chức, bộ máy, con người thực hiện; Cơ chế phối hợp; Kiểm tra, xử lý vi phạm...

2. Thực trạng việc thực hiện chính sách bảo vệ an ninh thông tin hiện nay

Sau gần 40 năm Đổi mới, hệ thống thông tin của Việt Nam đã có sự phát triển vượt bậc, phục vụ hiệu quả công cuộc lãnh đạo, quản lý, điều

* Trường Đại học Sư phạm Hà Nội.

hành của Đảng và Nhà nước, đáp ứng nhu cầu thông tin của xã hội. Trong Chỉ thị 01/CT-BTTTT ngày 03/01/2020 về định hướng phát triển ngành Thông tin và Truyền thông năm 2020, Bộ trưởng Bộ Thông tin và Truyền thông đã nhấn mạnh: “An toàn, an ninh mạng là điều kiện tiên quyết để phát triển Chính phủ điện tử và chuyển đổi số, do đó phải đi trước một bước.” Theo đó, Việt Nam đã “bước đầu hình thành hệ thống pháp luật và cơ sở vật chất cho việc bảo đảm an ninh mạng, an toàn thông tin quốc gia, không gian mạng quốc gia. Ban hành và thực hiện Chiến lược an ninh mạng quốc gia” [2, tr.68].

2.1. Thành tựu

Thực hiện chủ trương, chính sách của Đảng và Nhà nước, những năm qua, việc thực hiện chính sách pháp luật bảo vệ an ninh thông tin đã đạt được một số kết quả nhất định.

Về hướng dẫn thực hiện và tuyên truyền phổ biến: Cục An toàn thông tin (Bộ Thông tin và Truyền thông) đã đẩy mạnh chiến dịch tuyên truyền trên diện rộng tập trung vào nhóm đối tượng cán bộ, nhân viên các cơ quan, đơn vị nhà nước khu vực công từ Trung ương đến địa phương tại 63 tỉnh thành cả nước để tổ chức tập huấn và hướng dẫn các cán bộ công chức, viên chức. Bên cạnh đó, đã chú trọng giáo dục, bồi dưỡng, phổ biến kiến thức về an ninh thông tin cho cơ quan, tổ chức, cá nhân với mục tiêu tham gia không gian mạng an toàn, lành mạnh, hạn chế tối đa nguy cơ, tác động tiêu cực, phát huy tối đa hiệu quả.

Bảo đảm các điều kiện cần để thực hiện: cơ sở pháp lý cho công tác thực hiện chính sách pháp luật bảo vệ an ninh thông tin được bảo đảm, đã xây dựng và hình thành lực lượng chuyên trách bảo vệ an ninh thông tin đủ khả năng đáp ứng yêu cầu của tình hình thực tế, hiệu quả quản lý nhà nước, đấu tranh phòng, chống tội phạm

trước các diễn biến phức tạp của an ninh thông tin được nâng cao, cụ thể một số chủ trương, chính sách: Luật An toàn thông tin mạng năm 2015; Luật An ninh mạng năm 2018; Nghị quyết số 29-NQ/TW ngày 25/7/2018 về Chiến lược bảo vệ Tổ quốc trên không gian mạng, Nghị quyết số 30-NQ/TW ngày 25/7/2018 về Chiến lược an ninh mạng quốc gia... Đặc biệt, ngày 10/8/2022, Thủ tướng Chính phủ đã ban hành Quyết định số 964/QĐ-TTg phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030. Đây là lần đầu tiên kể từ khi Luật An toàn thông tin mạng và Luật An ninh mạng có hiệu lực thi hành, Chiến lược An toàn, An ninh mạng quốc gia được ban hành. Chiến lược An toàn, An ninh mạng quốc gia đã đề ra 13 mục tiêu cụ thể đến năm 2025 và 8 mục tiêu cụ thể đến năm 2030 để hiện thực hóa tầm nhìn trở thành quốc gia tự chủ về an toàn, an ninh mạng để bảo vệ sự phát triển thịnh vượng của Việt Nam trên không gian mạng. Cùng với đó, Chiến lược cũng đưa ra 12 nhóm nhiệm vụ, giải pháp để triển khai thực hiện. Tiếp đó, một số văn bản quy phạm pháp luật được ban hành trong thời gian gần đây như: Luật Viễn thông ban hành ngày 24/11/2023; Luật giao dịch điện tử (Sửa đổi bổ sung năm 2023); Chính phủ (2023), Nghị định số 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân, ngày 17/04/2023; Chính phủ (2023), Nghị quyết số 175/NQ-CP Về phê duyệt đề án trung tâm dữ liệu quốc gia, ngày 30/10/2023; Bộ Nội vụ (2023), Quy chế bảo đảm an toàn, an ninh thông tin mạng, ngày 21/4/2023...

Tổ chức, bộ máy, con người thực hiện: Nhận thức được tầm quan trọng của việc thực hiện chính sách bảo vệ an ninh thông tin, Đảng và Nhà nước đã quy định trách nhiệm của cơ quan,

tổ chức, cá nhân trong quá trình thực hiện chính sách pháp luật bảo vệ an ninh thông tin, tập trung vào việc xác định trách nhiệm của lực lượng chuyên trách bảo vệ an ninh thông tin được bố trí tại Bộ Công an, Bộ Quốc phòng. Bên cạnh đó, đã ưu tiên đào tạo nguồn nhân lực an ninh thông tin chất lượng cao, tiếp tục bồi dưỡng đội ngũ công chức, viên chức có chuyên môn cao về an toàn, an ninh thông tin.

Cơ chế phân công phối hợp: Việc triển khai thực hiện chính sách bảo vệ an ninh thông tin một cách đồng bộ, thống nhất từ Trung ương tới địa phương, trọng tâm là các cơ quan nhà nước và các tổ chức chính trị, quy định rõ các nội dung triển khai, hoạt động kiểm tra việc thực hiện chính sách bảo vệ an ninh thông tin đối với hệ thống thông tin của các cơ quan, tổ chức này. Kết cấu hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế cũng là một trong những đối tượng được bảo vệ trọng điểm. Các hoạt động nghiên cứu, phát triển an ninh thông tin, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh thông tin, nâng cao năng lực tự chủ về an ninh thông tin đã cũng được quy định chi tiết.

Kiểm tra, xử lý vi phạm: Bộ Thông tin và Truyền thông tăng cường thanh tra, kiểm tra việc tuân thủ quy định của pháp luật về an toàn thông tin tại các cơ quan, tổ chức nhà nước; các doanh nghiệp triển khai nền tảng số phục vụ chuyển đổi số, phát triển Chính phủ điện tử, Chính phủ số, kinh tế số, xã hội số; các doanh nghiệp cung cấp các dịch vụ nền tảng hạ tầng số, dịch vụ viễn thông, Internet và các doanh nghiệp khác có liên quan tại Việt Nam; xử lý nghiêm các cơ quan, tổ chức, doanh nghiệp có hành vi vi phạm pháp luật về an toàn thông tin mạng. Chỉ trong 2 năm (2019 và 2020), Bộ Công an đã phát hiện hàng trăm cá nhân, tổ

chức liên quan bán dữ liệu cá nhân, đồng thời chỉ đạo đơn vị chức năng xác lập chuyên án để tập trung đấu tranh, làm rõ một số đường dây chiếm đoạt, mua bán dữ liệu quy mô lớn tại Việt Nam. Qua đó, phát hiện 1.300GB dữ liệu chứa nhiều thông tin về các cá nhân, tổ chức trên toàn quốc đã sử dụng dịch vụ điện lực của EVN; thông tin phụ huynh, học sinh tại các trường trên cả nước; thông tin khách hàng của các ngân hàng BIDV, Techcombank, VPBank, AgriBank... bị mua bán, trao đổi trái phép; thông tin đăng ký kinh doanh, nhân sự cơ quan nhà nước, bảo hiểm, hộ khẩu; dữ liệu viễn thông, thuê bao điện thoại của các nhà mạng Viettel, Mobiphone, Vinaphone; thông tin khách hàng tại các dự án bất động sản trên toàn quốc; khách hàng điện máy tại 63 tỉnh, thành toàn quốc; thông tin của khách hàng VIP, khách hàng đầu tư tài chính, chứng khoán, khách hàng các ngành Spa, nha khoa, thời trang, thẩm mỹ viện[3]. Trong năm 2019, số cuộc tấn công mạng vào các hệ thống thông tin Việt Nam có chiều hướng giảm (khoảng 45,9%) so với cùng kỳ năm 2018.

2.2. Hạn chế

Bên cạnh những kết quả đạt được, việc thực hiện chính sách pháp luật bảo vệ an ninh thông tin còn bộc lộ một số hạn chế.

Thứ nhất, chưa có khái niệm chính thức về an ninh thông tin, truyền thông và công tác bảo vệ an ninh truyền thông dẫn đến nhận thức về vấn đề này chưa thực sự đầy đủ. Một số cơ quan, tổ chức, cá nhân còn chủ quan, sơ hở trong quản lý thông tin nội bộ, bí mật nhà nước, chưa nhận thức đầy đủ vị trí, tầm quan trọng của công tác bảo đảm an ninh thông tin cũng như tính chất nguy hiểm trong âm mưu, hoạt động của các thế lực thù địch, tội phạm mạng chống phá Đảng và Nhà nước ta trên không gian mạng; tình trạng lộ bí mật nhà nước qua hệ thống thông tin gia tăng đột biến;

hiện tượng khai thác, sử dụng trái phép cơ sở dữ liệu, tài nguyên thông tin quốc gia, dữ liệu cá nhân người dùng diễn biến phức tạp; xuất hiện nhiều dịch vụ mới, hiện đại gây khó khăn cho công tác quản lý, kiểm soát của các cơ quan chức năng.

Thứ hai, các yếu tố đe dọa an ninh phi truyền thống và các giải pháp ứng phó, giải quyết các vấn đề an ninh phi truyền thống trên lĩnh vực thông tin, truyền thông chưa được định hình rõ, chưa được tổng kết, đánh giá một cách toàn diện. Trong khi đó, các mối đe dọa an ninh phi truyền thống trên lĩnh vực thông tin, truyền thông có sự giao thoa, đan xen, pha trộn, chuyển hoá với các yếu tố an ninh truyền thống trên lĩnh vực này, nếu không có sự nhận thức thống nhất, đầy đủ sẽ làm hạn chế đến hiệu quả công tác bảo vệ an ninh thông tin, truyền thông.

Thứ ba, tình hình mất an toàn thông tin mạng còn diễn biến phức tạp; công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng còn hạn chế [2, tr.87-88]. Theo thống kê, từ năm 2010 đến năm 2019 đã có 53.744 lượt cổng thông tin, trang tin điện tử có tên miền “.vn” bị tấn công, trong đó có 2.393 lượt cổng thông tin, trang tin điện tử của các cơ quan Đảng, Nhà nước “.gov.vn”, xuất hiện nhiều cuộc tấn công mang màu sắc chính trị, gây ra những hậu quả nghiêm trọng [5]. Năm 2022 có 180.000 máy tính trong các cơ quan, tổ chức Việt Nam bị nhiễm mã độc APT; 14.500 máy chủ nhiễm ransomware [6] Việt Nam nằm trong nhóm các quốc gia bị tấn công mạng nhiều nhất và là quốc gia có tỷ lệ gặp phải mã độc tống tiền cao nhất tại khu vực châu Á - Thái Bình Dương [1].

2. Một số giải pháp nâng cao hiệu quả thực hiện chính sách pháp luật về an ninh thông tin giai đoạn hiện nay

Để nâng cao hiệu quả công tác thực hiện chính sách pháp luật bảo vệ an ninh thông tin ở

Việt Nam cần quan tâm thực hiện đồng bộ một số giải pháp sau:

Thứ nhất, tiếp tục nâng cao nhận thức pháp luật về an ninh thông tin và bảo vệ an ninh thông tin.

Cần nhận thức rõ, an ninh thông tin là độc lập, chủ quyền, lợi ích quốc gia trên không gian thông tin, sự an toàn, phát triển ổn định, vững mạnh của lĩnh vực thông tin, hệ thống thông tin quốc gia. An ninh thông tin là nội dung trọng tâm của an ninh quốc gia trong điều kiện mới, có mối quan hệ chặt chẽ với các vấn đề an ninh truyền thống khác như an ninh chính trị nội bộ, an ninh quân sự, an ninh văn hóa tư tưởng, an ninh kinh tế, an ninh xã hội. Nguy cơ gây mất an ninh thông tin là mối đe dọa lớn và ngày càng gia tăng đối với an ninh quốc gia, an ninh quốc tế. Chính vì vậy, bảo vệ an ninh thông tin là nhiệm vụ trọng yếu, thường xuyên của toàn Đảng, toàn dân, của cả hệ thống chính trị trong đó lực lượng Công an nhân dân là nòng cốt. Bảo vệ an ninh thông tin cần coi trọng và sử dụng đồng bộ các biện pháp chính trị, pháp luật, khoa học kỹ thuật, tuyên truyền - giáo dục, tổ chức - hành chính, kinh tế, ngoại giao và nghiệp vụ chuyên môn. Các cơ quan chức năng cần tăng cường giáo dục, bồi dưỡng, nâng cao ý thức của cán bộ, đảng viên và quần chúng nhân dân; chú trọng tuyên truyền chính sách pháp luật về bảo vệ an ninh thông tin, phổ biến cho học sinh, sinh viên về các nguy cơ, các yếu tố gây mất an ninh, đe dọa gây mất an ninh thông tin. Từ đó, nâng cao ý thức trong sử dụng các dịch vụ thông tin, nhất là dịch vụ do nước ngoài cung cấp; nâng cao bản lĩnh chính trị, khả năng nhận biết, tiếp nhận thông tin, khả năng tự vệ, “miễn dịch” trước những thông tin giả, thông tin xấu, độc hại.

Thứ hai, tiếp tục hoàn thiện cơ chế chính sách để tạo cơ sở cho thực hiện chính sách pháp luật bảo vệ an ninh thông tin.

Trước sự phát triển nhanh chóng của công nghệ và thông tin trên mạng xã hội tràn lan, cần hoàn thiện hơn nữa cơ chế chính sách để tạo hành lang pháp lý cho an ninh thông tin. Theo đó, cần hoàn thiện hơn nữa chính sách, pháp luật về bảo vệ dữ liệu quốc gia, nâng cấp chính sách bảo vệ dữ liệu cá nhân, quy định hoạt động thu thập, lưu trữ, xử lý dữ liệu công dân Việt Nam và trách nhiệm của các tổ chức, doanh nghiệp trong và ngoài nước trong bảo vệ chủ quyền, an ninh thông tin quốc gia Việt Nam. Đồng thời, cần hoàn thiện các văn bản hướng dẫn thi hành Luật An ninh mạng, các văn bản quy phạm pháp luật về điều kiện kinh doanh các sản phẩm, dịch vụ an ninh mạng, nhất là các sản phẩm, dịch vụ sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin của cơ quan nhà nước.

Thứ ba, cần có chế tài đủ sức răn đe cho những hành vi vi phạm chính sách pháp luật bảo vệ an ninh thông tin

Thực hiện nghiêm quy định về chế tài hình sự liên quan tới vi phạm quy định về bảo vệ an ninh thông tin và cần phải có mức xử phạt vi phạm hành chính đủ sức răn đe cho các hành vi vi phạm chính sách bảo vệ an ninh thông tin. Rà soát các quy định hiện hành về xử phạt vi phạm hành chính thì mức phạt tiền trung bình trong các lĩnh vực được áp dụng đối với các hành vi vi phạm liên quan đến xâm phạm các quy định về chính sách bảo vệ an ninh thông tin.

Tài liệu tham khảo:

- [1] Phan Anh (2023), *Việt Nam đứng thứ 49 thế giới về số lượng tấn công trực tuyến*, <https://vneconomy.vn/>
- [2] Đảng Cộng sản Việt Nam (2021), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, tập I, Nxb. Chính trị quốc gia Sự thật, Hà Nội.
- [3] Nguyễn Ngọc Cương, Nguyễn Ngọc Quỳnh (2021), *"Chế tài xử lý các hành vi vi phạm quy định bảo vệ dữ liệu cá nhân"*; <https://antoanhtongtin.vn>
- [4] Quốc hội (2015), *"Luật an toàn thông tin mạng"*, Hà Nội.
- [5] Lê Văn Thắng: *An ninh thông tin ở Việt Nam trong điều kiện hiện nay - Vấn đề đặt ra và giải pháp*, <https://moj.gov.vn/>
- [6] *Tổng kết an ninh mạng năm 2022 và dự báo năm 2023*, <https://www.bkav.com.vn>.

Thứ tư, kiện toàn tổ chức bộ máy, phát triển nguồn nhân lực về an ninh mạng, an ninh thông tin

Cần xây dựng lực lượng an ninh thông tin đủ mạnh, dưới sự chỉ đạo trực tiếp từ cơ quan có thẩm quyền, có trách nhiệm chủ động thực hiện và sẵn sàng ứng phó với các nguy cơ đến từ không gian mạng; xây dựng các cơ chế, chính sách, quy chế phối hợp giữa các cơ quan, tổ chức đang thực hiện nhiệm vụ bảo đảm an ninh mạng, an ninh thông tin, như Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, Bộ Tư lệnh 86 (Bộ Quốc phòng), Cục An toàn thông tin và An ninh mạng (Bộ Công an); xây dựng cơ chế, chiến lược và kế hoạch đào tạo nguồn nhân lực chất lượng cao về an ninh mạng, an ninh thông tin; xây dựng đội ngũ cán bộ và cơ chế kiểm tra độ an toàn, bảo mật của thiết bị, chương trình nhập khẩu sử dụng trong hệ thống thông tin quan trọng quốc gia.

Kết luận

Trong thời đại Cách mạng công nghiệp 4.0, an ninh thông tin ngày càng trở thành một nội dung quan trọng của an ninh quốc gia. Trong những năm qua, Việt Nam đã thực hiện có hiệu quả việc thực hiện chính sách pháp luật bảo vệ an ninh thông tin. Mặc dù còn một số bất cập, hạn chế nhưng tin là với những giải pháp được thực hiện đồng bộ sẽ góp phần bảo vệ an ninh thông tin quốc gia Việt Nam trong giai đoạn hiện nay. □