Áp dng pháp lut An ninh mng Vit Nam - Lý lun và thc tin: Sách tham kho: Dùng cho ào to trình i hc Cnh sát nhân dân, h Chính quy, các chuyên ngành - Lu hành ni b

Lê Quang Thành; Nguyn Quc Khánh

2025
Trng i hc CSND
https://library.dhcsnd.edu.vn/handle/123456789/58

BỘ CÔNG AN

TRƯỜNG ĐẠI HỌC CẢNH SÁT NHÂN DÂN

SÁCH THAM KHẢO

NHỮNG VẤN ĐỀ LÝ LUẬN VÀ THỰC TIỄN VỀ ÁP DỤNG PHÁP LUẬT AN NINH MẠNG Ở VIỆT NAM

(Dùng cho đào tạo trình độ Đại học CSND, hệ Chính quy, các chuyên ngành)

Lưu hành nội bộ

THÀNH PHỐ HỒ CHÍ MINH - 2025

CHỦ BIÊN
TS, TRUNG TÁ LÊ QUANG THÀNH

SÁCH THAM KHẢO

NHỮNG VẤN ĐỀ LÝ LUẬN VÀ THỰC TIỄN VỀ ÁP DỤNG PHÁP LUẬT AN NINH MẠNG Ở VIỆT NAM

(Dùng cho đào tạo trình độ Đại học CSND, hệ Chính quy, các chuyên ngành)

Lưu hành nội bộ

THÀNH PHỐ HỒ CHÍ MINH – 2025

BAN BIÊN SOẠN

Chủ biên

TS, TRUNG TÁ LÊ QUANG THÀNH – GVC KHOA LUẬT

Tham gia biên soạn

1. TS, Trung tá Lê Quang Thành	GVC Khoa Luật - T05
Biên soạn: Chương 1, Chương 2	
2. ThS Nguyễn Quốc Khánh	P. Trưởng Khoa - T05
Biên soạn: Chương 3	

MỤC LỤC

LỜI NÓI ĐẦU

Trên cơ sở Quyết định số 2404/QĐ-T05, ngày 21/10/2024 về việc giao biên soạn tài liệu dạy học năm học 2024 – 2025, của Hiệu trưởng Trường Đại học CSND, tập thể tác giả đã thực hiện việc biên soạn Sách tham khảo **"Những vấn đề lý luận và thực tiễn về áp dụng pháp luật an ninh mạng ở Việt Nam"**. Đây là một tài liệu cần thiết và có ý nghĩa quan trọng trong công tác giảng dạy và nghiên cứu khoa học tại Trường Đại học CSND, nhất là với đối học viên bắt đầu học tập, nghiên cứu học phần Lý luận Nhà nước và pháp luật trong chương trình đào tạo.

Nội dung của Sách tham khảo phù hợp với mục tiêu, yêu cầu của chương trình đào tạo trình độ Đại học CSND; phù hợp với Đề cương chi tiết học phần Lý luận nhà nước và pháp luật, do Trường Đại học CSND ban hành. Đối tượng thụ hưởng chủ yếu là học viên đang tham gia học tập, nghiên cứu khoa học tại Trường Đại học CSND. Với mục đích trang bị nhiều hơn, bổ sung thêm lượng kiến thức sâu hơn về thực hiện và áp dụng pháp luật, góp phần đánh giá một cách toàn diện hơn các yếu tố tác động đến quá trình thực hiện và áp dụng pháp luật về không gian mạng ở Việt Nam trong bối cảnh hội nhập, toàn cầu hóa, phù hợp với yêu cầu đào tạo lực lượng CSND trong tình hình mới.

Sách tham khảo được biên soạn mới, trên cơ sở kế thừa nhiều nguồn tài liệu như: Giáo trình, sách chuyên khảo, sách tham khảo, các loại tài liệu được sử dụng để giảng dạy và nghiên cứu khoa học của các cơ sở đào tạo trong và ngoài ngành Công an đã được thừa nhận một cách chính thống. Hơn nữa, Sách tham khảo này còn được cập nhật kịp thời quan điểm, chủ trương mới nhất của Đảng, chính sách, pháp luật của Nhà nước, thể hiện trong những Văn kiện của Đảng, các Luật ban hành gần đây.

Sách tham khảo **"Những vấn đề lý luận và thực tiễn về áp dụng pháp luật an ninh mạng ở Việt Nam"**, được kết cấu gồm 2 Chương. Cụ thể như sau:

Chương 1. Những vấn đề lý luận về an ninh mạng và áp dụng pháp luật an ninh mạng

Chương 2. Thực tiễn áp dụng pháp luật về an ninh mạng ở Việt Nam và phương hướng nâng cao hiệu quả

Mặc dù chủ biên và nhóm tác giả tham gia biên soạn đã rất cố gắng, nỗ lực tuy nhiên vẫn sẽ không tránh khỏi những thiếu sót, hạn chế nhất định. Ban biên soạn rất mong nhận được những đóng góp ý kiến quý báu của các nhà khoa học, giảng viên, học viên, những người nghiên cứu, người đọc để Sách tham khảo được hoàn thiện hơn.

Xin trân trọng cảm ơn./.

TRƯỜNG ĐẠI HỌC CSND

Chương 1
NHỮNG VẤN ĐỀ LÝ LUẬN VỀ AN NINH MẠNG VÀ ÁP DỤNG PHÁP LUẬT AN NINH MẠNG

I. NHẬN THỨC CHUNG VỀ AN NINH MẠNG VÀ PHÁP LUẬT AN NINH MẠNG

1. Nhận thức về an ninh mạng

Về mặt thuật ngữ, khái niệm an ninh được các từ điển giải thích có những sự tương đồng. Từ điển tiếng Việt 2010 giải thích "an ninh là tình hình trật tự xã hội bình thường, yên ổn, không có rối loạn"[1]. Theo Đại từ điển Tiếng Việt, "an ninh được hiểu là trật tự xã hội, tình hình chính trị yên ổn, không lộn xộn, không nguy hiểm"[2]. Từ các quan niệm trên cho thấy ở góc độ chung nhất, an ninh là trạng thái xã hội trật tự, yên ổn, chế độ chính trị ổn định.

Luật An ninh quốc gia 2004 quy định: "An ninh quốc gia là sự ổn định, phát triển bền vững của chế độ xã hội chủ nghĩa và Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, sự bất khả xâm phạm độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc"[3]. Đó là sự bảo đảm an ninh trên các lĩnh vực truyền thống như: chính trị, kinh tế, tư tưởng - văn hoá, xã hội, quốc phòng, đối ngoại... Trong bối cảnh mới, không gian mạng (KGM) đã trở thành một miền tác chiến mới, sự xuất hiện và diễn biến của tội phạm phi truyền thống như tội phạm mạng, tội phạm sử dụng công nghệ cao... ngày càng phức tạp, không chỉ ảnh hưởng tiêu cực đến an ninh quốc gia (ANQG), trật tự an toàn xã hội (ATXH) mà còn là một trong những thách thức lớn mang tính toàn cầu. Đảm bảo an ninh mạng (ANM) là một nhiệm vụ trọng yếu trong đảm bảo an ninh quốc gia. Để phục vụ hoạt động xây dựng và hoạch định chính sách, chiến lược ANM, mỗi quốc gia trên thế giới đều có những cách tiếp cận cũng như quan niệm khác nhau về ANM. Tuy nhiên, xét về bản chất, quan điểm về ANM được quyết định bởi quan niệm an ninh. Chính vì lý do đó, khái niệm an ninh mạng xuất hiện đã phản ánh sự thay đổi nhận thức, tư duy của con người về an ninh và là sự mở rộng, nối dài nội hàm của khái niệm an ninh.

[1] Trung tâm từ điển học (2010), *Từ điển tiếng Việt 2010*, Nxb Đà Nẵng, Hà Nội.
[2] Nguyễn Như Ý (1999), *Đại từ điển Tiếng Việt*, Nxb Văn hóa thông tin, Thành phố Hồ Chí Minh.
[3] Xem Khoản 1, Điều 3, Luật An ninh quốc gia 2004

Hiện nay, có nhiều quan niệm khác nhau về nội hàm của các khái niệm chỉ trạng thái đảm bảo an toàn thông tin (ATTT) cho hệ thống mạng như an toàn, an ninh thông tin (information security), an ninh mạng (cyber security/network security), trong đó phổ biến nhận thức là các khái niệm an toàn, ANTT hay ANM đều là sự bảo đảm an toàn mạng và ATTT trong quá trình khởi tạo, truyền đưa và lưu trữ dữ liệu trên máy tính cá nhân, trên mạng và trên điện toán đám mây.

Theo Chương trình Phát kiến quốc gia về sự nghiệp và nghiên cứu an ninh mạng của Mỹ (National Initiative for Cybersecurity Careers and Studies - NICCS, Hoa Kỳ), thuật ngữ an ninh mạng được hiểu là "hoạt động hoặc quá trình, khả năng, hay trạng thái mà theo đó thông tin, hệ thống thông tin liên lạc và thông tin chứa trong đó được bảo vệ khỏi và/hoặc bảo vệ chống lại thiệt hại, việc sử dụng trái phép hoặc sửa đổi, khai thác"[4]. Đạo luật An ninh mạng năm 2015 của Hoa Kỳ quy định mục đích của ANM là nhằm bảo vệ hệ thống thông tin khỏi đe doạ về ANM hoặc tình trạng dễ bị tấn công, bao gồm các giải pháp được thiết kế để bảo vệ người dùng máy tính và các công ty hoạt động trên internet. Thực tế, ANM thuộc nội hàm của khái niệm an ninh thông tin, mục tiêu mà nó hướng đến là bảo vệ thông tin kỹ thuật số khi các hệ thống được kết nối với nhau.

Luật An ninh mạng của Cộng hòa nhân dân Trung Hoa năm 2017 quy định "An ninh mạng chỉ khả năng thông qua việc áp dụng các biện pháp cần thiết để phòng ngừa, ngăn chặn các hành vi tấn công, xâm nhập, can thiệp, phá hoại, sử dụng bất hợp pháp và các sự cố ngoài ý muốn liên quan đến hệ thống mạng để bảo đảm mạng trong trạng thái vận hành ổn định, và bảo đảm tính hoàn chỉnh, tính bảo mật, tính ứng dụng của dữ liệu mạng"[5].

Đạo luật cơ bản về An ninh mạng của Nhật Bản định nghĩa ANM là các biện pháp cần thiết được thực hiện nhằm quản lý thông tin an toàn, phòng chống rò rỉ, mất mát hoặc thiệt hại đối với thông tin được lưu trữ, truyền đưa qua các phương tiện điện tử, từ tính hoặc các phương tiện khác (sau đây gọi là phương tiện điện tử, từ tính) và bảo đảm an toàn, tin cậy của các hệ thống thông tin, mạng viễn thông và thông tin (gồm các biện pháp cần thiết phòng chống hoạt động tấn

[4]National Initiative for Cybersecurity Careers and Studies (2009), *Cybersecurity Glossary*, tại trang https://niccs.cisa.gov/about- niccs/cybersecurity-glossary#C, [ngày 20/2/2024].

[5] Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2018), *Các loại tội phạm công nghệ cao ở Việt Nam, bao gồm tội phạm lạm dụng tình dục trực tuyến và tội phạm liên quan đến tiền mã hóa, các biện pháp phòng ngừa hoạt động tội phạm*, Tài liệu Hội thảo bàn tròn quốc gia về an ninh mạng và tội phạm sử dụng công nghệ cao, do UNODC và Bộ Công an tổ chức ngày 24, 25/9/2018 tại Thành phố Hồ Chí Minh, tr.30.

công mã độc nhằm vào các máy tính điện tử thông qua hệ thống thông tin hoặc phương tiện lưu trữ thông tin tạo ra bởi phương tiện điện tử, từ tính (sau đây gọi là phương tiện lưu trữ điện tử, từ tính)[6]. Luật an ninh mạng của Nhật Bản quy định an ninh mạng chỉ là những biện pháp cần thiết để quản lý thông tin một cách an toàn và đáng tin cậy của hệ thống thông tin và mạng lưới viễn thông.

Trong khi đó, qua việc khảo cứu một số tài liệu khác, chúng tôi nhận thấy rằng, ANM là sự phòng tránh xâm nhập có hại hoặc những truy cập sai mục đích dẫn đến tình trạng an ninh, bảo mật thông tin gặp rất nhiều các vấn đề. Phần lớn các tài liệu kỹ thuật và từ điển quốc tế cho rằng, khái niệm "an ninh mạng" (cyber security) được hiểu là các biện pháp và hành động nhằm bảo vệ máy tính, máy chủ, các thiết bị di động, hệ thống điện tử, mạng và dữ liệu khỏi những tấn công độc hại.

Các tiếp cận trên đây tuy diễn đạt khác nhau, nhưng đều có điểm chung về ANM, đó là sự bảo đảm trạng thái hoạt động yên ổn của mạng lưới có kết nối internet khỏi sự tấn công từ bên ngoài gây ảnh hưởng hoặc làm gián đoạn hoạt động của hệ thống mạng. Như vậy, các quốc gia trên có điểm chung là đều giới hạn phạm vi điều chỉnh về ANM ở các biện pháp kỹ thuật nhằm ngăn chặn và đối phó với những hoạt động truy cập trái phép vào hệ thống mạng và phòng ngừa các cuộc tấn công trên KGM.

Thuật ngữ An ninh mạng còn được một số tổ chức, nhà nghiên cứu tiếp cận, định nghĩa và sử dụng trong các bối cảnh, lĩnh vực cụ thể. Ví dụ, Ngân hàng Nhà nước quy định: an ninh mạng là sự bảo vệ hệ thống công nghệ thông tin và thông tin truyền đưa trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính toàn vẹn, tính bảo mật và tính sẵn sàng của thông tin[7].

Nghị định về quản lý, cung cấp, sử dụng dịch vụ interrnet và thông tin trên mạng tiếp cận hai khái niệm ATTT và an ninh thông tin như sau: an toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. Còn An ninh thông tin là việc bảo

[6] Bùi Thị Long, *Thực hiện pháp luật về An ninh mạng ở Việt Nam,* Xnb Tư pháp, Hà Nội 2023

[7] Ngân hàng Nhà nước Việt Nam (2015), *Thông tư 31/2015/TT-NHNN ngày 28/12/2015 của Ngân hàng Nhà nước Việt Nam quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng,* Hà Nội.

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[8]. Luật An toàn thông tin mạng năm 2015 quy định ATTT mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin[9]. Như vậy, an ninh thông tin chú trọng bảo đảm thông tin trên không gian mạng, liên quan đến việc bảo vệ an ninh quốc gia, trật tự an toàn xã hội, còn ATTT mạng chú trọng đảm bảo các thuộc tính của thông tin gồm tính sẵn sàng, tính toàn vẹn và tính bí mật.

Bên cạnh đó, cũng cần làm rõ một khái niệm tương đối gần với khái niệm ANM là "tội phạm có sử dụng công nghệ cao" trong bối cảnh phát triển của khoa học công nghệ như hiện nay. "Tội phạm có sử dụng công nghệ cao" là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự có sử dụng công nghệ cao; "vi phạm pháp luật khác có sử dụng công nghệ cao" là hành vi vi phạm pháp luật có sử dụng công nghệ cao nhưng chưa đến mức truy cứu trách nhiệm hình sự[10]. Như vậy, về cơ bản, theo cách hiểu chung nhất, khái niệm "tội phạm có sử dụng công nghệ cao" tương đương với khái niệm "tội phạm mạng", nhưng có nội hàm rộng hơn vì "tội phạm có sử dụng công nghệ cao" còn bao hàm một số loại tội phạm không chỉ sử dụng phương thức tấn công, truy cập trái phép mạng máy tính để gây án mà còn sử dụng mạng điện thoại để thực hiện hành vi lừa đảo, buôn bán ma túy, đánh bạc, truyền bá văn hóa đồi trụy... đặc biệt là các thủ đoạn lừa đảo trong giao dịch thương mại điện tử.

Ngoài ra, về mặt học thuật theo khảo cứu của chúng tôi, ANM còn được nghiên cứu, tiếp cận theo hai góc độ.

Theo nghĩa rộng, ANM được hiểu theo nghĩa là ANM quốc gia, là khả năng đảm bảo thông tin, hệ thống thông tin và hoạt động của con người trên KGM mà không gây phương hại đến chủ quyền, lợi ích, 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.

Theo nghĩa hẹp, ANM hay ANM máy tính là khả năng đảm bảo an toàn cho hoạt động của hệ thống mạng máy tính và thông tin trên mạng máy tính, không

[8] Chính phủ (2013), *Khoản 23, 24 Điều 3 Nghị định 72/2013/NĐ-CQ ngày 15/7/2013 của Chính phủ quy định về quản lý, cung cấp, sử dụng dịch vụ interrnet và thông tin trên mạng*, Hà Nội
[9] Quốc hội (2015), *Luật An toàn thông tin mạng năm 2015*, Hà Nội.
[10] Chính phủ (2014), *Nghị định số 25/2014/NĐ-CP ngày 07/4/2014 của Chính phủ quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao*, Hà Nội.

gây phương hại đến hoạt động bình thường của các tổ chức, cá nhân sở hữu và sử dụng mạng máy tính đó. Ở đây, mạng máy tính được hiểu theo nghĩa rộng gồm mạng máy tính và thông tin được lưu trữ, truyền tải và xử lý trên mạng máy tính đó. Khái niệm ANM ở đây hàm chứa cả an toàn mạng, không chỉ mạng đó được đảm bảo an toàn mà mạng đó không được là nguồn gốc phát sinh ảnh hưởng đến các đối tượng khác (tổ chức, cá nhân sở hữu hay sử dụng mạng đó). ANM là một hệ thống các kỹ thuật, thủ tục và biện pháp được thiết kế nhằm bảo vệ sự toàn vẹn của mạng, máy tính, chương trình và dữ liệu trước các cuộc tấn công, phá hoại hoặc xâm nhập trái phép.

Từ nhận thức ANM là một bộ phận không thể tách rời của an ninh quốc gia, trên cơ sở các văn bản quy phạm pháp luật điều chỉnh các vấn đề có liên quan đến ANM được ban hành, trên cơ sở hệ thống hóa, nghiên cứu tài liệu, chúng tôi xin được tiếp cận khái niệm ANM thống nhất với quy định của Luật An ninh mạng Việt Nam năm 2018, theo đó: An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân[11].

Có thể khẳng định rằng khái niệm ANM do Luật An ninh mạng 2018 đưa ra đã bao quát được các đối tượng bảo vệ của ANM gồm: chế độ chính trị và Nhà nước Cộng hòa XHCN Việt Nam; KGM quốc gia và cơ sở hạ tầng KGM quốc gia; hệ thống thông tin quan trọng về an ninh quốc gia; hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị ở Trung ương và địa phương; tổ chức, cá nhân tham gia hoạt động trên KGM. Khách thể bảo vệ mà ANM hướng đến bao gồm: độc lập, thống nhất, toàn vẹn lãnh thổ của Tổ quốc; chế độ chính trị, chế độ kinh tế, nền văn hóa; quốc phòng, an ninh, trật tự an toàn xã hội; bí mật nhà nước; tính mạng, sức khỏe, danh dự, nhân phẩm của con người; quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Tại Việt Nam, đến nay một số cơ sở giáo dục, đào tạo đã thực hiện nghiên cứu, đào tạo chuyên ngành an toàn, an ninh thông tin, an toàn không gian mạng, không gian số. Về chuyên ngành An ninh mạng hiện nay được nghiên cứu, giảng dạy tại một số trường đào tạo chuyên về an ninh hay công nghệ thông tin... như Đại học Quốc gia Hà Nội; Học viện An ninh nhân dân; Học viện Bưu chính Viễn thông…Mặc dù vậy, lý luận về ANM cho đến nay vẫn là lĩnh vực tương đối mới

[11] Quốc hội (2018), *Luật An ninh mạng năm 2018*, Nxb Lao động, Hà Nội.

mẻ. Do đó, trong quá trình nghiên cứu, tổng hợp, đánh giá và xây dựng lý luận về ANM cần tiếp tục tăng cường đầu tư thời gian, công sức, kinh phí với sự tham gia của nhiều cơ quan, tổ chức và đặc biệt là đội ngũ chuyên gia.

2. Pháp luật về an ninh mạng ở Việt Nam

a. Quy định của pháp luật về an ninh mạng trước khi ban hành Luật An ninh mạng 2018

Những quy định đầu tiên trực tiếp ghi nhận và bảo vệ ANM ở Việt Nam là Nghị định số 21/NĐ-CP ngày 05/3/1997 của Chính phủ về việc ban hành Quy chế tạm thời về quản lý, thiết lập, sử dụng mạng internet. Theo tinh thần của Nghị định này, trách nhiệm quản lý nhà nước, cung cấp và sử dụng dịch vụ mạng internet được xác lập và do Chính phủ thống nhất quản lý. Bất cứ thông tin đưa vào, truyền đi và nhận đến mạng internet qua cửa đi quốc tế tại Việt Nam phải tuân thủ quy định tại Điều 3 của Nghị định này, với những quy định như sau: (i) Không được kích động chống Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, phá hoại khối đoàn kết toàn dân; (ii) Không được kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, truyền bá tư tưởng, văn hoá phản động, lối sống dâm ô, truỵ lạc, các hành vi tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục; (iii) Không được tiết lộ bí mật của Đảng, Nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại, bí mật đời tư của công dân và bí mật khác do pháp luật quy định; (iv) Không được thông tin sai sự thật, xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, xúc phạm vĩ nhân, anh hùng dân tộc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của công dân[12].

Ngày 19/11/1997, Việt Nam đã chính thức khai trương dịch vụ internet. Sự kiện này có thể được xem là mốc lịch sử quan trọng trong quá trình hội nhập về công nghệ thông tin của Việt Nam với thế giới. Sau đó, năm 2001, Chính phủ ban hành Nghị định 55/NĐ-CP ngày 23/8/2001 để điều chỉnh việc quản lý, cung cấp và sử dụng dịch vụ internet. Nghị định đã có những quy định nghiêm cấm các hành vi gây rối, phá hoại hệ thống thiết bị và cản trở việc cung cấp, sử dụng các dịch vụ internet; đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã và thông tin riêng trên internet của các tổ chức, cá nhân; lợi dụng internet để chống lại nhà

[12] Chính phủ (1997), *Nghị định số 21/NĐ-CP ngày 05/3/1997 của Chính phủ về việc ban hành Quy chế tạm thời về quản lý, thiết lập, sử dụng mạng internet ở Việt Nam*, Hà Nội.

nước Cộng hoà xã hội chủ nghĩa Việt Nam; gây rối loạn an ninh, trật tự; vi phạm đạo đức, thuần phong, mỹ tục và các vi phạm pháp luật khác[13].

Mặc dù những quy định pháp luật đầu tiên về bảo đảm ANM được xây dựng từ cuối những năm 1990, nhưng do điều kiện kinh tế, xã hội, khoa học công nghệ, pháp luật về ANM gần đây mới được chú trọng hoàn thiện. Trong khoảng một thập niên trở lại đây, KGM được đề cập đến với tư cách là miền lãnh thổ mới được hình thành từ sự tiến bộ của khoa học công nghệ trong thế kỷ XIX. Vấn đề ANM tại Việt Nam được quy định rải rác trong nhiều văn bản quy phạm pháp luật như: Luật Giao dịch điện tử năm 2005, Luật Công nghệ thông tin năm 2006, Luật Viễn thông năm 2009, Bộ Luật hình sự năm 2015, Luật An toàn thông tin mạng năm 2015, một số nghị định,…

Pháp luật về ANM thời gian này đã nghiêm cấm các hành vi lợi dụng internet nhằm mục đích: chống nhà nước Cộng hoà XHCN Việt Nam; gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong, mỹ tục của dân tộc; làm lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định; đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức; danh dự, nhân phẩm của công dân; lợi dụng mạng internet để quảng cáo, tuyên truyền, mua bán hàng hoá, dịch vụ thuộc danh mục cấm theo quy định của pháp luật[14]. Ngoài ra, các hành vi gây rối, phá hoại hệ thống thiết bị và cản trở trái pháp luật việc quản lý, cung cấp, sử dụng các dịch vụ internet và thông tin điện tử trên internet; đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã và thông tin riêng của các tổ chức, cá nhân trên internet; tạo ra và cài đặt các chương trình virus máy tính, phần mềm gây hại cũng bị nghiêm cấm triệt để.

Pháp lệnh bảo vệ bí mật nhà nước năm 2001 là văn bản pháp luật đầu tiên xác định mức độ mật của thông tin bí mật nhà nước, nay là Luật Bảo vệ bí mật nhà nước năm 2018. Bí mật nhà nước là thông tin có nội dung quan trọng do người đứng đầu cơ quan, tổ chức có thẩm quyền xác định căn cứ quy định của Luật Bảo

[13] Chính phủ (2001), *Nghị định số 55/NĐ-CP ngày 23/8/2001 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ internet*, Hà Nội.
[14] Chính phủ (2008), *Nghị định số 97/NĐ-CP ngày 28/8/2008 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ internet và thông tin điện tử trên internet*, Hà Nội.

vệ bí mật nhà nước năm 2018, chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc. Nội dung bí mật nhà nước phải được mã hóa theo quy định của pháp luật về cơ yếu khi truyền đưa bằng phương tiện viễn thông và mạng máy tính. Do tính chất đặc biệt, Nhà nước nghiêm cấm mọi hành vi xâm phạm (như thu thập, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy trái phép) bí mật nhà nước, đồng thời quy định chặt chẽ việc tiếp xúc, bảo quản và xử lý bí mật nhà nước.

Luật Giao dịch điện tử năm 2005 có nhiều quy định bảo đảm an ninh, an toàn cho giao dịch điện tử, bảo vệ quyền và lợi ích hợp pháp của các bên trong giao dịch điện tử. Đây là văn bản luật đầu tiên nhấn mạnh khái niệm bảo đảm an ninh, an toàn và bảo mật thông tin. Luật công nhận giá trị pháp lý của thông điệp dữ liệu, chữ ký điện tử là một hình thức thể hiện mới của giao dịch bên cạnh hình thức văn bản, lời nói như quy định của Bộ Luật dân sự[15]. Luật quy định trách nhiệm bảo vệ dữ liệu, bảo mật thông tin của các tổ chức, cá nhân và xử phạt đối với những hành vi sử dụng, cung cấp, tiết lộ thông tin bí mật nhà nước, thông tin cá nhân trong quá trình giao dịch. Đây là căn cứ pháp lý tin cậy để các bên tham gia giao dịch điện tử. Phạm vi điều chỉnh của Luật giới hạn ở các giao dịch điện tử. Hình thức xử phạt vi phạm của Luật chưa được quy định rõ ràng.

Luật Công nghệ thông tin năm 2006 quy định về hoạt động ứng dụng và phát triển công nghệ thông tin, đồng thời xác định quyền và nghĩa vụ của các cơ quan, tổ chức, cá nhân tham gia vào các hoạt động này. Một trong những nội dung quan trọng của Luật là các quy định về an toàn và an ninh thông tin trên mạng, với các hành vi vi phạm pháp luật được phân chia thành ba nhóm chủ yếu:

+ Nhóm hành vi xâm phạm tài sản của tổ chức và cá nhân: Luật cấm các hành vi như can thiệp trái phép vào hoạt động của hệ thống máy chủ, tên miền quốc gia, phá hoại cơ sở hạ tầng thông tin và làm tổn hại thông tin trong môi trường mạng nhằm xâm hại tài sản.

+ Nhóm hành vi vi phạm có tính chất chống loài người: Cấm hành vi cung cấp, trao đổi, truyền tải, lưu trữ và sử dụng thông tin số nhằm kích động bạo lực, tuyên truyền chiến tranh xâm lược, gieo rắc hận thù giữa các dân tộc, kích động đồi trụy, tội ác, mê tín dị đoan và phá hoại thuần phong mỹ tục.

[15] Quốc hội (2005), *Luật Giao dịch điện tử năm 2005*, Hà Nội.

+ Nhóm hành vi vi phạm chống Chính phủ: Cấm hành vi cung cấp, truyền tải, lưu trữ, sử dụng thông tin số với mục đích chống lại Nhà nước Việt Nam, phá hoại khối đoàn kết toàn dân, tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế và các bí mật khác.

Ngoài ra, Luật cũng nghiêm cấm các hành vi xâm nhập, sửa đổi, xóa bỏ thông tin của cá nhân, tổ chức khác trên môi trường mạng; cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy cập thông tin của cá nhân, tổ chức khác; bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng[16].

Luật Công nghệ cao năm 2008 quy định một trong số các hành vi bị nghiêm cấm là Lợi dụng hoạt động công nghệ cao gây phương hại đến lợi ích quốc gia, quốc phòng, an ninh, quyền và lợi ích hợp pháp của tổ chức, cá nhân. Tất cả các hành vi lợi dụng công nghệ cao như sản xuất vũ khí sinh học, vũ khí hạt nhân, sử dụng trí tuệ nhân tạo để khủng bố, v.v. làm phương hại đến lợi ích an ninh quốc gia trên KGM, gây mất trật tự an toàn xã hội, xâm phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân đều bị nghiêm cấm.

Khoản 1 Điều 6 Nghị định 97/NĐ-CP của Chính phủ ban hành ngày 28/8/2008 quy định về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin điện tử trên internet nghiêm cấm các hành vi lợi dụng internet nhằm mục đích: (a) Chống lại nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong, mỹ tục của dân tộc; (b) Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định; (c) Đưa các thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức; danh dự, nhân phẩm của công dân; (d) Lợi dụng internet để quảng cáo, tuyên truyền, mua bán hàng hoá, dịch vụ thuộc danh mục cấm theo quy định của pháp luật[17].

Năm 2009, Luật Viễn thông được ban hành, trong đó xác định khái niệm cơ sở hạ tầng viễn thông, mạng internet. Luật có quy định về trách nhiệm bảo đảm

[16] Quốc hội (2006), *Luật Công nghệ thông tin năm 2006*, Hà Nội.
[17] Chính phủ (2008), *Nghị định số 97/NĐ-CP ngày 28/8/2008 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ internet và thông tin điện tử trên internet*, Hà Nội.

an toàn cơ sở hạ tầng viễn thông và an ninh thông tin của các chủ thể, trong đó đặc biệt chú ý đến trách nhiệm thực hiện yêu cầu của cơ quan nhà nước có thẩm quyền của chủ thể là các doanh nghiệp viễn thông phải tiến hành ngăn chặn khẩn cấp và ngừng cung cấp dịch vụ viễn thông đối với trường hợp bạo động, bạo loạn, sử dụng dịch vụ viễn thông xâm phạm an ninh quốc gia, chống lại Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam[18].

Luật Cơ yếu năm 2011 quy định rõ các nguyên tắc tổ chức và hoạt động của lực lượng cơ yếu; quyền nghĩa vụ trách nhiệm của cơ quan, tổ chức, cá nhân liên quan đến hoạt động cơ yếu. Đặc biệt, Luật đã quy định chính sách mã hóa áp dụng đối với thông tin bí mật nhà nước được lưu trữ, truyền đưa trên các phương tiện điện tử, mạng viễn thông.

Năm 2013, Hiến pháp nước Cộng hòa XHCN Việt Nam được ban hành. Tuy nhiên, toàn bộ nội dung của Hiến pháp năm 2013 chưa có bất cứ quy định nào về an ninh mạng. Song, có thể coi quy định mọi hành vi chống lại độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ, chống lại sự nghiệp xây dựng và bảo vệ Tổ quốc đều bị nghiêm trị bao gồm cả không gian mạng, bộ phận lãnh thổ mới và không tách rời của Tổ quốc Việt Nam.

Luật An toàn thông tin mạng năm 2015 là văn bản quy phạm pháp luật đầu tiên quy định tương đối tường minh về an toàn thông tin (ATTT) mạng. Luật quy định rõ các hành vi bị nghiêm cấm như hành vi ngăn chặn truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật. Hoạt động bảo đảm ATTT mạng được thực hiện liên tục, kịp thời và theo nguyên tắc: cơ quan, tổ chức, cá nhân hoạt động đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội và quan trọng hơn hết là phải có trách nhiệm bảo đảm ATTT mạng. Các tổ chức, cá nhân không được xâm phạm ATTT mạng của các tổ chức, cá nhân khác. Việc xử lý sự cố ATTT mạng phải đảm bảo quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đời sống riêng tư, bí mật cá nhân, bí mật gia đình cá nhân, thông tin riêng của tổ chức.

Luật tập trung quy định các biện pháp nhằm đảm bảo ba thuộc tính của thông tin là tính bí mật, tính nguyên vẹn và tính khả dụng. Luật cũng quy định rõ

[18] Quốc hội (2009), *Luật Viễn thông năm 2009*, Hà Nội.

việc chú trọng đào tạo, phát triển nguồn nhân lực và xây dựng cơ sở hạ tầng, kỹ thuật ATTT mạng đáp ứng yêu cầu ổn định chính trị, phát triển kinh tế - xã hội,... Đáng chú ý là các quy định cụ thể về bảo vệ thông tin cá nhân như thu thập, sử dụng, cập nhật, sửa đổi, hủy bỏ và bảo đảm ATTT cá nhân trên mạng cũng như trách nhiệm của các cơ quan quản lý nhà nước phải thiết lập kênh thông tin trực tuyến để tiếp nhận kiến nghị, phản ánh của tổ chức, cá nhân trong việc ngăn chặn giả mạo, lợi dụng điểm yếu, lỗ hổng nhằm phát tán phần mềm độc lại, tấn công mạng làm ảnh hưởng đến thông tin và hệ thống thông tin[19]. Tuy nhiên, Luật An toàn thông tin mạng năm 2015 mới điều chỉnh một lĩnh vực do Bộ Thông tin và Truyền thông quản lý, ATTT mạng chỉ là một điều kiện của ANM. Thông tin và hệ thống thông tin, đối tượng tác động chính của ATTT mạng cũng là một trong những đối tượng tác động của ANM.

Từ thực tiễn công tác phòng ngừa, đấu tranh, chống các tội phạm nguy hiểm cho xã hội trong bối cảnh khoa học công nghệ phát triển thần tốc, Bộ luật Hình sự năm 2015, sửa đổi bổ sung năm 2017 đã đánh dấu bước tiến mới, bước hoàn thiện các quy định pháp luật hình sự để đấu tranh hiệu quả hơn với loại tội phạm mạng khi dành cả một mục riêng quy định về tội phạm trong lĩnh vực công nghệ thông tin và mạng viễn thông. Luật bổ sung mới 05 tội danh về Tội phạm trong lĩnh vực công nghệ thông tin và mạng viễn thông bao gồm: Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (Điều 285); Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291); Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông (Điều 292); Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh (Điều 293); Tội cố ý gây nhiễu có hại (Điều 294)[20]. Những tội danh mới bổ sung này được quy định cụ thể về dấu hiệu hành vi, hậu quả thiệt hại cũng như chế tài xử lý tương xứng với tính chất và hậu quả gây thiệt hại của người phạm tội. Điều đó cho thấy, để thực hiện hành vi phạm tội, thủ phạm sử dụng công cụ là các thiết bị kỹ thuật số và mạng máy tính để xâm phạm lợi ích chính đáng của các tổ chức, cá nhân, làm ảnh hưởng đến trật tự, an toàn xã hội. Loại tội phạm này sử dụng khoa học công nghệ để thực hiện hành vi phạm tội, có

[19] Quốc hội (2015), *Luật An toàn thông tin mạng năm 2015*, Hà Nội.
[20] Quốc hội (2015), *Bộ Luật hình sự năm 2015*, Hà Nội.

thể có tính chất không biên giới vì thủ phạm ở quốc gia này có hành vi xâm hại tổ chức, cá nhân ở quốc gia khác. Nhóm khách thể bị xâm hại được quy định từ Điều 285 đến Điều 294 (11 tội danh) trong Bộ Luật Hình sự năm 2015 được hiểu theo nghĩa rộng, từ việc sản xuất, phát tán, buôn bán mã độc, làm hỏng hệ thống, thiết bị, lấy cắp, phá hoại, mã hóa, sửa chữa, làm sai lệch dữ liệu, gây rối loạn chức năng hoạt động của phần mềm máy tính, mạng máy tính và các thiết bị liên quan, xâm phạm đến lợi ích chính đáng của tổ chức, cá nhân, ảnh hưởng đến an ninh quốc gia và trật tự, an toàn xã hội.

BLHS 2015 đã cụ thể hóa các dấu hiệu định tính như "gây hậu quả nghiêm trọng, rất nghiêm trọng, đặc biệt nghiêm trọng" bằng các tình tiết cụ thể dấu hiệu hành vi và tính toán cụ thể hậu quả thiệt hại cụ thể (bằng số phút, số giờ; số tiền cụ thể…) giúp cho công tác phát hiện, điều tra, truy tố, xét xử được tiến hành kịp thời và chính xác. Ngoài ra, BLHS 2015 đã mở rộng áp dụng chế tài phạt tiền là hình phạt chính áp dụng đối với nhóm tội phạm trong lĩnh vực công nghệ thông tin và mạng viễn thông thuộc trường hợp phạm tội ít nghiêm trọng (khung hình phạt đến 3 năm tù) hoặc nghiêm trọng (khung hình phạt từ trên 03 năm đến 07 năm tù) với mức phạt tiền từ 20 triệu đồng đến 1,5 tỷ đồng.

Để tương thích với những quy định về tội phạm trong lĩnh vực công nghệ thông tin và mạng viễn thông trong BLHS 2015, lần đầu tiên khái niệm dữ liệu điện tử được đưa vào Bộ luật Tố tụng hình sự năm 2015. Mặc dù vậy, do chưa có quy định riêng về chứng cứ điện tử, nên trong thực tiễn cơ sở vật chất phục vụ công tác thu thập chứng cứ điện tử làm cơ sở chứng minh tội phạm từ các phương tiện điện tử, mạng viễn thông, mạng máy tính và các nguồn điện tử khác còn không ít khó khăn, vướng mắc.

b. Pháp luật về an ninh mạng ở Việt Nam từ khi ban hành Luật An ninh mạng 2018 đến nay

Tính đến năm 2015, Nhà nước đã ban hành nhiều văn bản quy phạm pháp luật liên quan đến lĩnh vực công nghệ thông tin, viễn thông, và Internet, nhưng vẫn thiếu một văn bản quy phạm pháp luật quy định cụ thể về an ninh mạng. Điều này dẫn đến việc các hành vi vi phạm pháp luật trên KGM chưa được ngăn chặn một cách hiệu quả, và công tác ADPL về an ninh mạng chưa đáp ứng đầy đủ yêu cầu thực tiễn trong bối cảnh mới. Tình trạng này gây khó khăn trong việc triển khai các phương án bảo đảm an ninh mạng, cũng như trong công tác phòng ngừa

và đấu tranh chống lại các hoạt động xâm phạm an ninh quốc gia và trật tự an toàn xã hội trên không gian mạng. Nhận thức rõ vấn đề này, ngày 12/6/2018, Quốc hội nước Cộng hòa XHCN Việt Nam khóa XIV đã thông qua Luật An ninh mạng. Đây là dấu mốc quan trọng đưa pháp luật về ANM lên một bước phát triển mới. Luật An ninh mạng năm 2018 gồm 07 chương, 43 điều. Đây là văn bản quy phạm pháp luật chuyên ngành có giá trị pháp lý cao nhất về bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, một nội dung đặc biệt quan trọng trong lĩnh vực ANM, các biện pháp phòng ngừa, xử lý hành vi xâm phạm ANM, trách nhiệm của các cơ quan, tổ chức, cá nhân trong bảo vệ ANM. Đúng như tên gọi, sự xuất hiện của Luật An ninh mạng năm 2018 khẳng định ANM hiện đã trở thành vấn đề mang tầm chiến lược quốc gia, không bị giới hạn ở một lĩnh vực riêng biệt nào, cần có hành lang pháp lý áp dụng các biện pháp bảo vệ tương xứng. Các chủ thể trong đó có các cơ quan quản lý nhà nước chủ động phòng ngừa, ngăn chặn, loại trừ các tác nhân có thể xâm phạm an ninh, an toàn hệ thống, lợi dụng để xâm phạm an ninh quốc gia, trật tự an toàn xã hội, đồng thời khắc phục sự bất cập trong công tác quản lý, dẫn đến tình trạng bị tấn công, xâm nhập liên tục dai dẳng mà không có biện pháp xử lý triệt để.

Luật An ninh mạng xác định *Tội phạm mạng* là hành vi sử dụng KGM, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự. Bên cạnh đó, Luật cũng quy định rõ *Tấn công mạng* là hành vi sử dụng KGM, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; *Khủng bố mạng* là việc sử dụng KGM, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố. Có thể khẳng định, số lượng tội phạm đang dịch chuyển từ thế giới thực sang thế giới ảo là KGM ngày càng gia tăng.

Một trong các loại tội phạm phức tạp nhất trên KGM là *Gián điệp mạng* với ba nhóm hành vi gồm nhóm hành vi cố ý, bất chấp để tấn công, chiếm quyền truy cập, kiểm soát tài nguyên thông tin, hệ thống thông tin quan trọng về an ninh quốc gia; nhóm hành vi chiếm đoạt, thu thập trái phép tài nguyên thông tin trên KGM; nhóm hành vi phá hoại thông tin, tài nguyên thông tin, hệ thống thông tin

quan trọng về an ninh quốc gia trên không gian mạng[21].

Bên cạnh đó, Luật Công an nhân dân năm 2018 quy định nhiệm vụ của lực lượng công an nhân dân tại Khoản 6 và Khoản 12 Điều 16 như sau: thực hiện quản lý về ANM, bảo vệ ANM và phòng, chống tội phạm mạng theo quy định của pháp luật; làm nòng cốt xây dựng nền an ninh nhân dân và thế trận an ninh nhân dân, xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc; hướng dẫn các cơ quan, tổ chức thực hiện công tác bảo vệ an ninh chính trị nội bộ, an ninh kinh tế, an ninh tư tưởng - văn hóa, ANM, an ninh thông tin, truyền thông, an ninh xã hội, an ninh môi trường[22].

Luật Quốc phòng năm 2018 cũng có những quy định hoạt động cơ bản của quốc phòng tại điểm 3 Khoản 2 Điều 7: xây dựng và tổ chức thực hiện kế hoạch, biện pháp về chiến tranh thông tin, chiến tranh không gian mạng.

Bên cạnh đó Chính phủ cũng đã ban hành những văn bản pháp quy để cụ thể hóa Luật, điều chỉnh các nhóm quan hệ xã hội phát sinh trong lĩnh vực KGM, chẳng hạn như: Nghị định số 15/2020/NĐ-CP, ngày 15/04/2020 quy định về xử phạt vi phạm hành chính trong lĩnh vực bưu chính viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử; Nghị định số 53/2022/NĐ-CP, ngày 18/08/2022 quy định chi tiết một số điều của Luật An ninh mạng; Nghị định số 13/2023/NĐ-CP, ngày 17/04/2023 về bảo vệ dữ liệu cá nhân.

Đặc biệt, gần đây nhất, ngày 24/12/2024, Đại hội đồng Liên hợp quốc đã thông qua bằng đồng thuận Công ước Liên hợp quốc về Tội phạm mạng. Theo quy định tại Điều 64 của Công ước, văn kiện này sẽ được mở ký tại Thủ đô Hà Nội trong năm 2025. Theo đó, Công ước có tên gọi là "Công ước Hà Nội". Công ước Hà Nội tạo khuôn khổ pháp lý đầu tiên ở cấp độ toàn cầu cho không gian mạng, khẳng định yêu cầu phải có sự tham gia của tất cả các quốc gia trong phòng, chống tội phạm mạng, góp phần thu hẹp những khác biệt giữa pháp luật các nước, thiết lập cơ chế hợp tác chuyên trách 24/7, qua đó thúc đẩy hợp tác phòng chống tội phạm xuyên biên giới hiệu quả hơn, đồng thời tạo điều kiện cho nỗ lực chuyển đổi số của các quốc gia.

Từ những phân tích nêu trên, có thể khẳng định rằng, ở Việt Nam, hệ thống văn bản luật, văn bản quy phạm pháp luật về ANM đã và đang là hành lang pháp

[21] Trần Mạnh Hùng (2020), *Gián điệp mạng từ góc nhìn mối đe dọa an ninh toàn cầu*, Nxb Công an nhân dân, Hà Nội.
[22] Quốc hội (2018), *Luật Công an nhân dân năm 2018*, Hà Nội.

lý vững chắc để mỗi cơ quan, tổ chức, cá nhân người dân yên tâm khi làm việc và hoạt động trên KGM, đáp ứng yêu cầu khách quan về sự thay đổi nhanh chóng của bối cảnh kinh tế - xã hội Việt Nam, cũng như yêu cầu hoàn thiện khung pháp lý trong bối cảnh hội nhập quốc tế. Tính đến thời điểm này, Việt Nam đã có một hệ thống văn bản quy phạm pháp luật điều chỉnh các quan hệ xã hội phát sinh trong lĩnh vực ANM tương đối đầy đủ và cơ bản đã đáp ứng tốt những đòi hỏi khách quan, từ thực tiễn.

c. Phạm vi điều chỉnh của pháp luật an ninh mạng Việt Nam

Trong điều kiện xây dựng, hoàn thiện nhà nước pháp quyền XHCN ở Việt Nam, pháp luật ngày càng thể hiện vai trò quan trọng trong đời sống xã hội. Từ phương diện lý luận truyền thống, theo quan điểm của chủ nghĩa Mác - Lênin, "pháp luật là hệ thống các quy tắc xử sự, có tính bắt buộc chung, do nhà nước ban hành (hoặc thừa nhận), thể hiện ý chí và bảo vệ lợi ích của giai cấp thống trị và được nhà nước bảo đảm thực hiện bằng sức mạnh cưỡng chế; là công cụ có hiệu lực nhất để điều chỉnh các quan hệ xã hội cơ bản phù hợp với ý chí và lợi ích của giai cấp thống trị trong xã hội có giai cấp"[23]. Pháp luật với ý nghĩa là nhân tố quan trọng nhất trong điều chỉnh quan hệ xã hội của nhà nước, nhằm tạo ra một xã hội ổn định, trật tự và phát triển, pháp luật luôn tác động và ảnh hưởng mạnh mẽ tới các quan hệ xã hội nói chung, cũng như tới tất cả các yếu tố của thượng tầng chính trị - pháp lý nói riêng. Quá trình tác động và ảnh hưởng của pháp luật thể hiện ở nhiều mức độ khác nhau tuỳ thuộc vào loại đối tượng và loại quan hệ cụ thể cần có sự điều chỉnh của pháp luật. Biểu hiện cụ thể của sự tác động đó bao giờ cũng phản ánh trong khuôn mẫu của các hành vi xử sự được xác định mà các chủ thể pháp luật phải tuân thủ, chấp hành hoặc lấy đó làm cơ sở để sử dụng hoặc áp dụng chúng cho phù hợp với những điều kiện tương ứng trên thực tế.

Dưới góc độ pháp luật thực định, quy định của pháp luật về ANM được hình thành trong quá trình thể chế hóa quan điểm, chủ trương của Đảng về xây dựng Nhà nước pháp quyền XHCN Việt Nam; hiện thực hóa và nâng cao hơn nữa hiệu lực, hiệu quả việc tổ chức, thực hiện pháp luật trong quản lý nhà nước đối với xã hội nói chung, quản lý nhà nước trên KGM nói riêng.

[23] Nguyễn Minh Đoan, *Giáo trình Lý luận về nhà nước và pháp luật*, Nxb, Chính trị Quốc gia sự thật, Hà Nội, 2017, tr. 77

Tất cả những hành vi xâm phạm bất hợp pháp an toàn, an ninh thông tin đều được các quốc gia trên thế giới quy định trong luật hình sự với các tiếp cận khác nhau như tội phạm xâm phạm an ninh không gian mạng (cybercrime), tội phạm máy tính (computer crime), tội phạm công nghệ cao (hightech crime). Về cơ bản, các khái niệm này có nội hàm thống nhất trong Công ước Budapest về tội phạm mạng năm 2001. Theo đó, các hành vi sau được coi là tội phạm mạng như: "truy cập bất hợp pháp; cản trở bất hợp pháp việc truyền tải dữ liệu máy tính; can thiệp trái phép vào dữ liệu; can thiệp trái phép vào hệ thống; sử dụng trái phép thiết bị; giả mạo liên quan đến máy tính; gian lận liên quan đến máy tính; vi phạm liên quan đến hình ảnh trẻ em khiêu dâm; vi phạm quyền tác giả và quyền liên quan qua hệ thống máy tính"[24].

Tội phạm mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ Luật hình sự. Đó là những tội phạm xâm phạm ANM được xác định có mục đích phá hoại chính trị hay trục lợi về kinh tế bằng việc sử dụng các thủ đoạn tấn công, xâm nhập, lấy cắp, phá hủy dữ liệu, truyền đưa thông tin nhạy cảm trái phép lên mạng, tấn công từ chối dịch vụ, lừa đảo, xâm phạm bí mật cá nhân, bí mật đời tư, bí mật kinh doanh...

Trong khoa học pháp lý hiện nay, chưa có khái niệm thống nhất về sự điều chỉnh của pháp luật đối với lĩnh vực ANM. Tuy nhiên, từ những khái niệm chung về pháp luật và sự phân tích mối liên hệ giữa pháp luật với những vấn đề về ANM, có thể đưa ra khái niệm pháp luật về ANM ở Việt Nam như sau: *Pháp luật về an ninh mạng là tổng thể các quy phạm pháp luật do Nhà nước ban hành và bảo đảm thực hiện nhằm điều chỉnh các quan hệ xã hội phát sinh trong hoạt động bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.*

Pháp luật về ANM ở Việt Nam hiện hành được quy định trong nhiều văn bản quy phạm pháp luật khác nhau, bao gồm Luật An ninh quốc gia năm 2004, Luật Giao dịch điện tử năm 2005, Luật Công nghệ thông tin năm 2006, Luật Công nghệ cao năm 2008, Luật Viễn thông năm 2009, Luật Tần số vô tuyến điện năm 2009, Luật Cơ yếu năm 2011, Luật Xử lý vi phạm hành chính năm 2012, Luật

[24] Liên minh Châu Âu (2001), *Công ước Budapest về tội phạm mạng*, được Hội đồng liên minh Châu âu thông qua ngày 23/11/2001, tại Budapest, Hungary.

Giáo dục quốc phòng và an ninh năm 2013, Luật An toàn thông tin mạng năm 2015, Bộ Luật hình sự năm 2015, Luật Bảo vệ bí mật nhà nước năm 2018, Luật Công an nhân dân năm 2018, Luật Quốc phòng năm 2018, Luật An ninh mạng năm 2018, Nghị định 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng, Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm hệ thống thông tin theo cấp độ, Nghị định 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin mạng, Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử, Nghị định 91/2020/NĐ-CP ngày 14/8/2020 của Chính phủ về chống tin nhắn rác, thư điện tử rác, cuộc gọi rác; Nghị định 53/NĐ-CP, ngày 15/08/2022, quy định chi tiết một số điều của Luật An ninh mạng 2018...

Nghiên cứu hệ thống các văn bản quy phạm pháp luật của Việt Nam về ANM cho thấy, nội dung điều chỉnh của pháp luật đối với các hành vi của các chủ thể pháp luật liên quan tới ANM bao gồm nhiều nhóm quy phạm pháp luật, tồn tại dưới những phương thức biểu hiện khác nhau, với nhiều tên gọi khác nhau cùng có thể tác động đến một hoặc nhiều nhóm quan hệ xã hội khác nhau nhưng cơ bản có cùng tính chất.

Trong phạm vi tiếp cận của cuốn sách này, chúng tôi chỉ tập trung nghiên cứu, làm rõ phạm vi điều chỉnh pháp luật về an ninh mạng (phạm vi tác động) thông qua 04 nhóm quy phạm chủ yếu như sau:

Thứ nhất, các quy định pháp luật về bảo vệ an ninh quốc gia trên không gian mạng

Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng đến an ninh quốc gia. Bảo vệ an ninh quốc gia trên KGM là bảo đảm hoạt động hệ thống thông tin quan trọng về an ninh quốc gia. Trên cơ sở tiêu chí của hệ thống thông tin quan trọng về an ninh quốc gia để áp dụng các biện pháp bảo vệ tương xứng, phù hợp với mức độ quan trọng của hệ thống thông tin này.

Các hoạt động bảo vệ an ninh quốc gia trên không gian mạng bao gồm:

- Thẩm định ANM là hoạt động xem xét, đánh giá những nội dung về ANM để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin.

- Đánh giá điều kiện ANM là xem xét sự đáp ứng về ANM của hệ thống thông tin trước khi đưa vào vận hành, sử dụng.

- Kiểm tra ANM là hoạt động xác định thực trạng ANM của hệ thống thông tin, kết cấu hạ tầng hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa ANM và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin.

- Giám sát ANM là thu thập, phân tích tình hình nhằm xác định nguy cơ đe dọa ANM, sự cố ANM, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để cảnh báo, khắc phục, xử lý.

- Ứng phó, khắc phục sự cố ANM đối với hệ thống thông tin là hoạt động phát hiện, xác định sự cố ANM; bảo vệ hiện trường, thu thập chứng cứ; phong tỏa, giới hạn phạm vi xảy ra sự cố ANM, hạn chế thiệt hại do sự cố ANM gây ra; xác định mục tiêu, đối tượng, phạm vi cần ứng cứu; xác minh, phân tích, đánh giá, phân loại sự cố ANM; triển khai phương án ứng phó, khắc phục sự cố ANM; xác minh nguyên nhân và truy tìm nguồn gốc; điều tra, xử lý theo quy định của pháp luật.

- Đấu tranh bảo vệ ANM là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ ANM thực hiện trên KGM nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

- Sử dụng mật mã để bảo vệ thông tin mạng là các biện pháp mã hóa bằng mật mã để bảo vệ thông tin mạng khi truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên KGM.

- Ngoài ra, để bảo vệ an ninh quốc gia trên KGM, pháp luật về ANM còn nghiêm cấm đối với các hành vi xâm phạm ANM, bao gồm:

Một là, không được đăng tải, phát tán, lan truyền,… các thông tin trên KGM có nội dung tuyên truyền chống Nhà nước CHXHCN Việt Nam: biểu hiện ở việc tuyên truyền xuyên tạc, phỉ báng, chống chính quyền nhân dân; chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân,

lãnh tụ, danh nhân, anh hùng dân tộc; tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa XHCN Việt Nam; xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc.

Hai là, không được tấn công mạng, khủng bố mạng, gián điệp mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia, vô hiệu hóa các biện pháp bảo vệ ANM, thể hiện ở:

+ Không được phát tán thư rác, phần mềm độc hại trên KGM; gây ảnh hưởng, cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính; sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật; hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

+ Không được hoạt động gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác bị nghiêm cấm trên KGM gồm: chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác gây ảnh hưởng đến quyền và lợi ích hợp pháp của cơ quan, tổ chức; cố ý xóa, sao chép, thất lạc, thay đổi và làm sai lệch thông tin thuộc bí mật nhà nước, bí mật công tác được truyền đưa, lưu trữ trên KGM; cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác; đưa lên KGM những thông tin thuộc bí mật nhà nước, bí mật công tác trái quy định của pháp luật; cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin khách hàng sử dụng mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã không rõ xuất xứ, nguồn gốc; hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác.

Thứ hai, các quy định pháp luật an ninh mạng về bảo đảm trật tự an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng

Hoạt động bảo đảm trật tự an toàn xã hội trên KGM được tổ chức, triển khai một cách đồng bộ, thống nhất trong hệ thống cơ quan nhà nước từ Trung ương tới địa phương. Các cơ quan, tổ chức, cá nhân có thẩm quyền triển khai hoạt động kiểm tra ANM đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia; triển khai bảo vệ ANM đối với cơ sở hạ tầng KGM quốc gia, cổng kết nối mạng quốc tế; bảo đảm an ninh thông tin trên KGM. Đồng thời triển khai các hoạt động nghiên cứu, phát triển ANM nhằm nâng cao năng lực tự chủ về ANM.

Để bảo đảm trật tự an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên KGM, pháp luật về ANM nghiêm cấm các hoạt động xâm phạm TTATXH trên KGM, như:

- Không được kích động, gây rối trật tự công cộng gồm: kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất TTATXH.

- Không được làm nhục, vu khống như xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác; thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

- Không được xâm phạm trật tự quản lý kinh tế bao gồm: thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

- Không được bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà

nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

- Không được xâm phạm bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư bị nghiêm cấm trên KGM gồm: chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cố ý xóa, sao chép, thất lạc, thay đổi và làm sai lệch thông tin thuộc bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên KGM; cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; đưa lên KGM những thông tin thuộc bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật; cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại cá nhân; hành vi khác cố ý xâm phạm bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.

Thứ ba, các quy định pháp luật về trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan

Các cơ quan, tổ chức, cá nhân tham gia hoạt động trên KGM cần có trách nhiệm: tuân thủ quy định của pháp luật về ANM; kịp thời cung cấp thông tin liên quan đến bảo vệ ANM, nguy cơ đe dọa ANM, hành vi xâm phạm ANM cho cơ quan có thẩm quyền, lực lượng bảo vệ ANM; thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ ANM; phối hợp, giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ ANM. Chính phủ thống nhất quản lý nhà nước về ANM. Chính phủ giao Bộ Công an thực hiện quản lý nhà nước về ANM và chịu trách nhiệm trước Chính phủ.

Bộ Công an có trách nhiệm ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về ANM; xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ ANM; phòng ngừa, đấu tranh với hoạt động sử dụng KGM xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm mạng; bảo đảm an ninh thông tin trên KGM; xây dựng cơ chế xác thực thông tin đăng ký tài khoản số; cảnh báo, chia sẻ thông tin ANM, nguy cơ đe dọa ANM; tham mưu, đề xuất Chính phủ, Thủ tướng Chính phủ xem xét, quyết định việc phân

công, phối hợp thực hiện các biện pháp bảo vệ ANM, phòng ngừa, xử lý hành vi xâm phạm ANM trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều Bộ, ngành; tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố ANM đối với hệ thống thông tin quan trọng về an ninh quốc gia; kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về ANM.

Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về ANM trong phạm vi chức năng, quyền hạn theo quy định của pháp luật.

Theo quy định của Luật An ninh mạng 2018, Bộ Thông tin và Truyền thông có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong bảo vệ ANM; phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước Cộng hòa XHCN Việt Nam; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên KGM, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung vi phạm pháp luật về ANM trên dịch vụ, hệ thống thông tin do doanh nghiệp, cơ quan, tổ chức trực tiếp quản lý.

Ban Cơ yếu Chính phủ: tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, chương trình, kế hoạch về mật mã để bảo vệ ANM thuộc phạm vi Ban Cơ yếu Chính phủ quản lý; bảo vệ ANM đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp theo quy định; thống nhất quản lý nghiên cứu khoa học, công nghệ mật mã; sản xuất, sử dụng, cung cấp sản phẩm mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên KGM.

Các Bộ, ngành, Ủy ban nhân dân (UBND) cấp tỉnh phải thực hiện trách nhiệm bảo vệ an toàn, ANM đối với thông tin, hệ thống thông tin thuộc phạm vi quản lý; phối hợp với Bộ Công an thực hiện quản lý nhà nước về ANM của Bộ, ngành, địa phương.

Tổ chức, cá nhân là chủ quản hệ thống thông tin có trách nhiệm kiểm tra ANM nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa ANM; triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà

nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này; phối hợp, thực hiện yêu cầu của lực lượng chuyên trách ANM về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin.

Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước phải bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị khác hoặc trao đổi trên KGM theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Các doanh nghiệp cung cấp dịch vụ trên KGM tại Việt Nam có trách nhiệm cảnh báo khả năng mất ANM trong việc sử dụng dịch vụ trên KGM do mình cung cấp và hướng dẫn biện pháp phòng ngừa; xây dựng phương án, giải pháp phản ứng nhanh với sự cố ANM, phát hiện và xử lý kịp thời điểm yếu, lỗ hổng bảo mật, mã độc, tấn công mạng, xâm nhập mạng và rủi ro an ninh khác; khi xảy ra sự cố ANM, ngay lập tức triển khai phương án khẩn cấp, biện pháp ứng phó thích hợp, đồng thời báo cáo với lực lượng chuyên trách bảo vệ ANM theo quy định; áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp xảy ra hoặc có nguy cơ xảy ra sự cố lộ, lọt, tổn hại hoặc mất dữ liệu thông tin người sử dụng, cần lập tức đưa ra giải pháp ứng phó, đồng thời thông báo đến người sử dụng và phối hợp, tạo điều kiện cho lực lượng chuyên trách trong bảo vệ ANM.

Thứ tư, quy định pháp luật về chế tài xử lý những hành vi xâm phạm an ninh mạng

Để bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên KGM, pháp luật về ANM quy định các chế tài xử lý hành vi xâm phạm ANM. Với quy định chặt chẽ, sự tham gia đồng bộ của cơ quan nhà nước, doanh nghiệp và tổ chức, cá nhân, việc lạm dụng, lợi dụng thông tin để vu khống, làm nhục, xâm phạm danh dự, nhân phẩm, uy tín của người khác được xử lý nghiêm minh. Pháp luật về ANM quy định tương đối rõ về các hành vi bị nghiêm cấm và chế tài xử lý các hành vi vi phạm pháp luật trong lĩnh vực ANM. Các vi phạm pháp luật trong lĩnh vực ANM đều phải gánh chịu hậu quả theo quy định của pháp luật về ANM. Tổ chức, cá nhân nào

thực hiện các hành vi bị nghiêm cấm thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự.

Trường hợp gây thiệt hại thì phải bồi thường theo quy định của pháp luật, thông qua những chế tài được quy định trong pháp luật, cụ thể như sau:

- Chế tài hành chính: xử phạt hành chính (cảnh cáo, phạt tiền), các hình phạt bổ sung (tước quyền sử dụng giấy phép, tịch thu tang vật vi phạm), các biện pháp khác (vô hiệu hóa, buộc ngừng hoạt động, đình chỉ, tạm đình chỉ, buộc khôi phục tình trạng cũ, buộc cải chính, buộc xóa, gỡ, tiêu hủy thông tin, nội dung thông tin, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, internet, thiết bị phát, thu phát sóng vô tuyến; yêu cầu gỡ, xóa thông tin trái pháp luật hoặc thông tin sai sự thật; phong tỏa, hạn chế hoạt động, đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động hệ thống thông tin; thu hồi tên miền).

- Chế tài dân sự: pháp luật ANM quy định tổ chức, cá nhân cung cấp dịch vụ trên KGM không đảm bảo chất lượng thì phải bồi thường. Bộ Luật Dân sự năm 2015 quy định các biện pháp bảo vệ quyền lợi của khách hàng trong trường hợp giữa doanh nghiệp cung cấp dịch vụ và khách hàng có quan hệ hợp đồng sử dụng dịch vụ như bên cung ứng phải có trách nhiệm với dịch vụ cung ứng và có nghĩa vụ bảo hành với dịch vụ trong thời hạn quy định. Tổ chức, cá nhân kinh doanh hàng hóa, dịch vụ trên KGM không đảm bảo chất lượng, số lượng, chủng loại, mẫu mã,... gây thiệt hại cho khách hàng, mà chưa đến mức truy cứu trách nhiệm hình sự thì phải bồi thường theo quy định của pháp luật dân sự.

- Chế tài hình sự: các cá nhân, tổ chức vi phạm pháp luật hình sự về ANM, thỏa mãn cấu thành được quy định trong BLHS sẽ phải bị điều tra, truy tố theo quy định của Bộ luật Tố tụng hình sự. Các hình thức xử phạt chính là phạt cảnh cáo, phạt cải tạo không giam giữ, phạt tù, phạt tiền; các hình thức phạt bổ sung là phạt tiền, thu hồi một phần hoặc toàn bộ tài sản, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc liên quan đến bảo đảm an ninh KGM trong thời gian nhất định.

3. Nhận xét, đánh giá

a. Những ưu điểm của pháp luật về an ninh mạng ở Việt Nam

Sự hình thành pháp luật về ANM đánh dấu sự phát triển tương đối toàn diện, đồng bộ của hệ thống pháp luật Việt Nam. Do đó, vị thế của Việt Nam trong

lĩnh vực này đã có những cải thiện đáng kể so với các nước trong khu vực và trên thế giới. Pháp luật về ANM của Việt Nam đã thể hiện rõ tinh thần bảo vệ an ninh Tổ quốc, trật tự an toàn xã hội trên KGM, đáp ứng yêu cầu hội nhập quốc tế trong bối cảnh mới. Pháp luật về ANM hiện hành điều chỉnh tương đối bao quát các quan hệ xã hội chủ yếu phát sinh trên KGM. Cụ thể như sau:

- Việc ban hành pháp luật về an ninh mạng đánh dấu một cột mốc quan trọng trong tiến trình hoàn thiện hệ thống pháp lý của Việt Nam, góp phần nâng cao vị thế quốc gia trong lĩnh vực an ninh mạng, cả trong khu vực và trên trường quốc tế. Pháp luật về an ninh mạng không chỉ thể hiện quyết tâm bảo vệ an ninh quốc gia, trật tự và an toàn xã hội trong không gian mạng mà còn là một sự đáp ứng linh hoạt, kịp thời với yêu cầu hội nhập quốc tế trong bối cảnh toàn cầu hóa và cuộc cách mạng công nghiệp 4.0. Các quy định pháp lý hiện hành đã bao quát và điều chỉnh hầu hết các quan hệ xã hội phát sinh từ môi trường mạng, bảo vệ quyền lợi hợp pháp của tổ chức và cá nhân tham gia vào các hoạt động trên không gian mạng.

- Các nguyên tắc bảo vệ an ninh mạng đã được ghi nhận rõ ràng trong hệ thống pháp luật, tạo nền tảng vững chắc cho các cơ quan, tổ chức thực thi pháp luật về an ninh mạng. Điều này tạo điều kiện thuận lợi để hình thành và củng cố các lực lượng chuyên trách như Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an), Bộ Tư lệnh 86 (Bộ Quốc phòng) và Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT - Bộ Thông tin và Truyền thông). Nhờ đó, các cơ quan này đã đạt được những kết quả tích cực trong công tác bảo vệ không gian mạng và đối phó hiệu quả với các mối đe dọa tiềm ẩn từ môi trường mạng.

- Pháp luật về an ninh mạng được xây dựng với cấu trúc chặt chẽ và khoa học, bao gồm các quy định rõ ràng về hành vi bị cấm, các biện pháp phòng ngừa, phát hiện, ngăn chặn và xử lý vi phạm. Luật An ninh mạng năm 2018 đã thiết lập một chương riêng biệt nhằm phòng ngừa và xử lý các hành vi xâm phạm an ninh mạng, hình thành một hệ thống pháp lý hợp lý và dễ dàng tiếp cận cho các bên liên quan. Điều 6 của Luật An ninh mạng quy định rằng Nhà nước sẽ triển khai các biện pháp bảo vệ không gian mạng quốc gia, đồng thời phòng ngừa và xử lý quyết liệt các hành vi xâm phạm an ninh quốc gia và trật tự xã hội trên không gian

mạng, đồng thời nghiêm cấm mọi hành vi xâm phạm an ninh quốc gia trong môi trường này.

- Việt Nam đã xây dựng một khung pháp lý cơ bản và chặt chẽ về an ninh mạng, bao gồm các quy định về bảo vệ và xử lý vi phạm với các chế tài rõ ràng, từ xử lý vi phạm hành chính, xử lý hình sự cho đến các biện pháp khắc phục hậu quả. Khung pháp lý này mặc dù còn mới mẻ, nhưng đã đáp ứng kịp thời và hiệu quả những yêu cầu trong công tác bảo vệ an ninh mạng quốc gia, đồng thời khẳng định sự sẵn sàng ứng phó với các mối đe dọa từ không gian mạng.

- Pháp luật về an ninh mạng cũng đặc biệt chú trọng đến việc bảo vệ trẻ em trên không gian mạng, thể hiện tính nhân văn sâu sắc và sự nhạy bén trong việc giải quyết các vấn đề phát sinh. Trẻ em, đối tượng dễ bị tổn thương và chưa hoàn toàn nhận thức được các rủi ro trong môi trường mạng, cần được bảo vệ đặc biệt. Mặc dù tỷ lệ trẻ em sử dụng không gian mạng ngày càng gia tăng, nhưng không phải tất cả đều hiểu rõ các nguy cơ tiềm ẩn. Việt Nam đã cam kết bảo vệ trẻ em khỏi mọi hình thức bóc lột và lạm dụng trực tuyến trong khuôn khổ Hiệp hội các quốc gia Đông Nam Á (ASEAN) vào năm 2019, khẳng định sự quan tâm sâu sắc đến thế hệ tương lai của đất nước.

- Pháp luật về an ninh mạng được quy định trong nhiều văn bản quy phạm pháp luật có giá trị pháp lý cao, đồng thời chỉ rõ các hành vi bị cấm và xây dựng các quy định mang tính dự báo, phù hợp với sự phát triển nhanh chóng của công nghệ thông tin và sự gia tăng các mối nguy cơ về an ninh mạng, như các cuộc tấn công mạng, chiến tranh mạng và những hành vi mới (theo khoản 6 Điều 8 Luật An ninh mạng năm 2018).

Qua nghiên cứu, có thể nhận thấy rằng mặc dù pháp luật về an ninh mạng còn non trẻ, nhưng đã phát triển ổn định và liên tục, đặc biệt trong 5 năm qua. Thành quả đáng ghi nhận là việc xây dựng một khung pháp lý cơ bản và hợp lý, góp phần quan trọng bảo vệ an ninh quốc gia trên không gian mạng, bảo đảm môi trường mạng lành mạnh và bảo vệ quyền lợi hợp pháp của các tổ chức, cá nhân tham gia vào các hoạt động trong không gian mạng.

Thêm vào đó, những kết quả này đã được củng cố và phát triển thông qua việc triển khai thực tiễn, tạo nền tảng vững chắc cho công tác kiểm soát an ninh mạng và quản lý thông tin của các chủ thể có trách nhiệm. Điều này đã góp phần

đáng kể vào việc cải thiện hành vi, cách xử sự đúng đắn, hợp pháp và hiệu quả hơn của các chủ thể trên KGM.

b. Một số hạn chế của pháp luật về an ninh mạng ở Việt Nam

Bên cạnh những kết quả bước đầu rất đáng khích lệ, pháp luật về ANM đã và đang bộc lộ một số hạn chế nhất định, cụ thể như:

- Về tính thống nhất, đồng bộ: nhiều quy định pháp luật còn có hiện tượng chồng chéo, chưa phát huy hiệu quả điều chỉnh quan hệ xã hội trong lĩnh vực ANM, nhất là các quy định pháp luật về thực hiện chức năng, nhiệm vụ bảo vệ ANM giữa các bộ, ngành chức năng. Còn tình trạng nhận thức chưa thống nhất, còn nhầm lẫn về hai văn bản Luật An ninh mạng và Luật An toàn thông tin mạng. Thực tế cho thấy, một số nhà nghiên cứu còn coi ATTT mạng và ANM chỉ là hai cách nói khác nhau về cùng một vấn đề. Cần thống nhất nhận thức rằng, ANM bao gồm hoạt động bảo vệ an ninh quốc gia, trật tự, an toàn xã hội theo chức năng, nhiệm vụ của Bộ Công an; hoạt động tác chiến trên KGM bảo vệ chủ quyền quốc gia theo chức năng, nhiệm vụ của Bộ Quốc phòng và bảo đảm ATTT mạng theo chức năng, nhiệm vụ của Bộ Thông tin và Truyền thông. An toàn thông tin mạng là điều kiện bảo đảm cho ANM được thực thi có hiệu quả, bền vững. Sự trùng lặp ở Điểm d Khoản 1 Điều 8 và Khoản 5 Điều 16 của Luật An ninh mạng năm 2018 cùng điều chỉnh nội dung sử dụng KGM để thực hiện hành vi thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội....

- Về tính toàn diện: Nhà nước đã ban hành nhiều văn bản quy phạm pháp luật liên quan đến lĩnh vực ANM, nhưng hệ thống văn bản quy phạm pháp luật quy định cụ thể về ANM chưa cập nhật kịp với sự phát triển của xã hội, của khoa học công nghệ cũng như phương thức, thủ đoạn của tội phạm, nhất là chưa bao quát hết các dạng thức xâm phạm ANM trong thực tiễn. Các chủ thể áp dụng pháp luật về ANM còn thiếu căn cứ pháp lý để triển khai các biện pháp phòng ngừa, phát hiện, xử lý, đấu tranh với các nguy cơ đe dọa ANM, hành vi vi phạm pháp luật trên KGM. Còn thiếu quy định giảm nhẹ cho những người vô tình tham gia hoặc dừng ngay các hành vi vi phạm ANM khi cơ quan nhà nước can thiệp cũng như chưa có tình tiết tăng nặng cho những đối tượng đóng vai trò khởi xướng, tổ chức trong một vụ xâm phạm ANM. Hiện tượng đánh bạc trên mạng dưới nhiều hình thức như cá độ bóng đá, đá gà…; các chơi trò chơi trực tuyến, có thưởng; các hành vi lừa đảo qua mạng hay như hiện tượng vi phạm quyền sở hữu trí tuệ,

đặc biệt là xâm phạm quyền riêng tư là những khoảng trống mà pháp luật chưa điều chỉnh hiệu quả. Cách tiếp cận của pháp luật hiện hành về ANM còn nghiêng về mục tiêu đảm bảo hoạt động quản lý nhà nước trên KGM, thiếu các quy định mang tính ràng buộc cơ quan quản lý nhà nước trong việc đảm bảo các quyền con người tương ứng. Các quy định về xử lý vi phạm pháp luật về ANM mới chỉ dừng ở việc xử lý các hành vi vi phạm với các đối tượng thuộc phạm vi quản lý như các tổ chức, doanh nghiệp, cá nhân mà chưa quy định về xử lý vi phạm chủ thể có thẩm quyền trong trường hợp thực hiện không đúng hoặc không hiệu quả thẩm quyền quản lý.

- Về tính phù hợp, cụ thể: các quy định pháp luật hiện nay về ANM chưa đủ sức răn đe, ngăn chặn các hành vi xâm phạm KGM; chưa đáp ứng được yêu cầu thực tiễn của THPL về ANM đặt ra trong tình hình mới. Vấn đề bảo mật thông tin cá nhân luôn được các cơ quan nhà nước quan tâm, được quy định trong nhiều văn bản quy phạm pháp luật, song những quy định về vấn đề này mang tính nguyên tắc, mới chỉ xác định được một số hành vi cơ bản cần điều chỉnh và một số đối tượng chính. Trên thực tế, vấn đề này ngày càng diễn biến phức tạp ở Việt Nam, liên quan trực tiếp đến quyền con người, quyền công dân, vì thế cần có những quy định thắt chặt hơn nữa để bảo vệ thông tin cá nhân, đặc biệt là cần cụ thể hóa và thống nhất trong quá trình thực hiện. Trong khi Luật An ninh mạng năm 2018, văn bản quy phạm pháp luật chính thức, trực tiếp điều chỉnh lĩnh vực ANM, vẫn là luật khung và đến nay cơ quan có trách nhiệm vẫn chưa ban hành đầy đủ các văn bản hướng dẫn tổ chức thực hiện. Thực trạng này đã gây khó khăn, vướng mắc trong tổ chức, triển khai các phương án bảo đảm an ninh thông tin, ANM cũng như trong công tác phòng ngừa, đấu tranh ngăn chặn các hoạt động sử dụng mạng internet để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

- Về trình độ, kỹ thuật xây dựng pháp luật: nội dung một số điều, khoản trong Luật An ninh mạng năm 2018 chưa thực sự logic và còn bị trùng lặp. Luật dành toàn bộ chương IV quy định hoạt động bảo vệ ANM, tuy nhiên quy định tại Điều 6 chương I lại có nội dung về bảo vệ KGM và Điều 22 chương III quy định về đấu tranh bảo vệ ANM. Điều 23 quy định việc triển khai hoạt động bảo vệ ANM trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương. Hệ thống chính trị là tổ hợp có tính chỉnh thể các thể chế chính trị (cơ quan nhà nước, đảng chính trị, phong trào xã hội, tổ chức chính trị-xã hội, v.v.) được xây dựng

theo một kết cấu chức năng nhất định, vận hành theo những nguyên tắc, cơ chế và quan hệ cụ thể, nhằm thực thi quyền lực chính trị. Hệ thống chính trị ở Việt Nam bao gồm Đảng Cộng sản Việt Nam, Nhà nước Cộng hòa XHCN Việt Nam, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội,... Như vậy, cơ quan nhà nước đã thuộc hệ thống chính trị và là tổ chức chính trị. Quy định như Điều 23 vừa thừa lại vừa thiếu. Cụm từ cơ quan nhà nước, tổ chức chính trị còn lặp lại ở một số điều luật khác như Điều 35.

- Về chủ thể: lực lượng chuyên trách bảo vệ ANM được bố trí tại Bộ Công an, Bộ Quốc phòng; lực lượng bảo vệ ANM được bố trí tại Bộ, ngành, UBND cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia; chức năng, nhiệm vụ của lực lượng chuyên trách bảo vệ ANM rải rác ở nhiều điều luật, chưa được quy định thành chế định riêng, trong khi chức năng, nhiệm vụ của lực lượng bảo vệ ANM lại tương đối mờ nhạt. Điều này dẫn đến cách hiểu chưa thực sự thống nhất và chưa chính xác về lực lượng chuyên trách bảo vệ ANM, chuyên trách ADPL về ANM. Bên cạnh đó, pháp luật hiện hành về ANM quy định theo kiểu liệt kê các loại hành vi nghiêm cấm đã thu hẹp phạm vi điều chỉnh của pháp luật. Trong bối cảnh công nghệ thông tin phát triển như vũ bão, nguy cơ mất ATTT mạng, ảnh hưởng đến ANQG, nguy cơ chiến tranh mạng ngày một hiện hữu với nhiều hành vi, thủ đoạn mới, các cơ quan có thẩm quyền cần nghiên cứu để quy định chặt chẽ và thể hiện tính dự báo nhiều hơn.

Qua nghiên cứu có thể thấy một cách khái quát rằng, pháp luật về an ninh mạng tuy mới hình thành, nhưng có sự phát triển tương đối đều và liên tục, nhất là trong 05 năm trở lại đây. Kết quả bước đầu là tạo dựng được khung pháp lý cơ bản, quan trọng góp phần bảo vệ an ninh quốc gia trên KGM, đảm bảo môi trường mạng lành mạnh, quyền và lợi ích hợp pháp của các chủ thể hoạt động trên KGM bước đầu được quan tâm bảo vệ. Tuy nhiên, những bất cập như sự chồng chéo, chưa cụ thể, những hạn chế về tính chưa toàn diện, chưa đồng bộ của pháp luật về ANM đã tác động trực tiếp đến thực trạng thi hành và nhất là hiệu quả ADPL về ANM ở Việt Nam hiện nay.

II. KHÁI NIỆM, CÁC GIAI ĐOẠN, VAI TRÒ VÀ BIỆN PHÁP BẢO ĐẢM ÁP DỤNG PHÁP LUẬT VỀ AN NINH MẠNG

1. Khái niệm, đặc điểm, các giai đoạn và vai trò của áp dụng pháp luật về an ninh mạng

a. Khái niệm, đặc điểm, các giai đoạn áp dụng pháp luật về an ninh mạng

Về phương diện lý luận, áp dụng pháp luật (ADPL) là một hình thức thực hiện pháp luật (THPL), trong đó nhà nước thông qua các cơ quan có thẩm quyền hoặc nhà chức trách tổ chức cho các chủ thể pháp luật thực hiện những quy định của pháp luật, hoặc tự mình căn cứ vào các quy định của pháp luật để tạo ra các quyết định làm phát sinh, thay đổi, đình chỉ hoặc chấm dứt những quan hệ pháp luật cụ thể. Trong các hình thức THPL, nếu như tuân thủ pháp luật, thi hành pháp luật và sử dụng pháp luật là những hình thức mà mọi chủ thể pháp luật đều có thể thực hiện thì ADPL là hình thức luôn luôn có sự tham gia của nhà nước thông qua các cơ quan hoặc nhà chức trách có thẩm quyền[25]. ADPL là hình thức THPL luôn gắn với công quyền. Đó là toàn bộ những việc làm, những hoạt động, những phương thức nhằm thực hiện những yêu cầu đặt ra trong pháp luật, trong việc điều chỉnh các quan hệ xã hội nhằm cụ thể hóa (cá biệt hóa) quyền, nghĩa vụ của chủ thể trong quan hệ pháp luật.

ADPL là một hình thức rất quan trọng của THPL bởi lẽ pháp luật tác động vào các quan hệ xã hội, vào cuộc sống đạt hiệu quả cao nhất chỉ khi tất cả những quy định của nó đều được thực hiện chính xác, triệt để. Nhưng nếu chỉ thông qua các hình thức tuân theo pháp luật, thi hành pháp luật và sử dụng pháp luật thì sẽ có rất nhiều quy phạm pháp luật không được thực hiện. Lý do có thể là các chủ thể không muốn thực hiện hoặc không đủ khả năng tự thực hiện nếu thiếu sự tác động của cơ quan nhà nước có thẩm quyền. Do đó hoạt động ADPL chỉ được tiến hành trong một số trường hợp khá hạn chế, đó là: i) Khi cần áp dụng các biện pháp cưỡng chế nhà nước, hoặc áp dụng các chế tài pháp luật đối với những chủ thể có hành vi vi phạm pháp luật; ii) Khi những quyền và nghĩa vụ pháp lý của chủ thể không phát sinh nếu thiếu sự can thiệp của Nhà nước; iii) Khi xảy ra tranh chấp về quyền chủ thể và nghĩa vụ pháp lý giữa các bên tham gia quan hệ pháp luật mà các bên đó không tự giải quyết được; iiii) Trong một số các quan hệ pháp

[25] Xem, Trường Đại học CSND (2022), *Giáo trình Lý luận Nhà nước và pháp luật, Luật nhà nước*, TP Hồ CHí Minh.

luật mà nhà nước thấy cần thiết phải tham gia để kiểm tra, giám sát hoạt động của các bên trong quan hệ pháp luật đó hoặc cần phải xác nhận sự tồn tại hay không tồn tại ít nhất là từ góc độ pháp lý của một số sự việc, sự kiện thực tế.

Nghiên cứu từ phương diện lý luận chung về nhà nước và pháp luật, áp dụng pháp luật có một số đặc điểm sau đây:

Thứ nhất, áp dụng pháp luật là hoạt động mang tính tổ chức, thể hiện quyền lực nhà nước, cụ thể là:

- Hoạt động áp dụng pháp luật chỉ do những cơ quan nhà nước hay nhà chức trách có thẩm quyền tiến hành. Mỗi cơ quan nhà nước hay nhà chức trách trong phạm vi thẩm quyền được giao thực hiện một số những hoạt động áp dụng pháp luật nhất định. Trong quá trình áp dụng pháp luật mọi khía cạnh, mọi tình tiết đều phải được xem xét cẩn trọng và dựa trên cơ sở các quy định, yêu cầu của quy phạm pháp luật đã được xác định để ra quyết định cụ thể. Như vậy pháp luật là cơ sở xuất phát điểm để các cơ quan nhà nước có quyền áp dụng pháp luật thực hiện chức năng của mình. Có một số trường hợp cá biệt, khi được Nhà nước trao quyền một số tổ chức xã hội cũng có thể tiến hành áp dụng pháp luật.

- Việc áp dụng pháp luật được xem là sự tiếp tục thể hiện ý chí của nhà nước. Do vậy, việc áp dụng pháp luật phải phù hợp với pháp luật, với chủ trương chính sách của nhà nước trong mỗi giai đoạn nhất định.

- Hoạt động áp dụng pháp luật được tiến hành chủ yếu theo ý chí đơn phương của các cơ quan nhà nước có thẩm quyền, không phụ thuộc vào ý chí của chủ thể bị áp dụng pháp luật.

- Áp dụng pháp luật có tính chất bắt buộc đối với chủ thể bị áp dụng và các chủ thể có liên quan.

- Văn bản áp dụng pháp luật chỉ do các cơ quan hay nhà chức trách có thẩm quyền áp dụng pháp luật ban hành. Văn bản áp dụng pháp luật mang tính bắt buộc phải thực hiện đối với những tổ chức và cá nhân có liên quan. Trong những trường hợp cần thiết, quyết định áp dụng pháp luật được bảo đảm thực hiện bằng sự cưỡng chế nhà nước.

Thứ hai, áp dụng pháp luật là hoạt động có hình thức thủ tục chặt chẽ do pháp luật quy định. Do tính chất quan trọng và phức tạp của hoạt động áp dụng pháp luật, chủ thể bị áp dụng pháp luật có thể được hưởng những lợi ích rất lớn nhưng cũng có thể phải chịu những hậu quả rất nghiêm trọng nên pháp luật xác

định rõ ràng cơ sở, điều kiện, trình tự, thủ tục quyền và nghĩa vụ của các bên trong quá trình áp dụng pháp luật.

Thứ ba, áp dụng pháp luật là hoạt động điều chỉnh cá biệt, cụ thể đối với các quan hệ xã hội xác định. Đối tượng của hoạt động áp dụng pháp luật là những quan hệ xã hội cần đến sự điều chỉnh cá biệt, bổ sung trên cơ sở những mệnh lệnh chung trong quy phạm pháp luật. Bằng hoạt động áp dụng pháp luật những quy phạm pháp luật nhất định được cá biệt hóa một cách cụ thể và chính xác.

Thứ tư, áp dụng pháp luật là hoạt động đòi hỏi tính sáng tạo. Khi áp dụng pháp luật, các cơ quan nhà nước có thẩm quyền phải nghiên cứu kỹ lưỡng vụ việc, làm sáng tỏ cấu thành pháp lý của nó để tù đó lựa chọn quy phạm, ra văn bản áp dụng pháp luật và tổ chức thi hành. Trong trường hợp pháp luật chưa quy định hoặc quy định chưa rõ thì phải vận dụng một cách sáng tạo bằng cách áp dụng pháp luật tương tự. Để đạt tới điều đó, đòi hỏi các nhà chức trách phải có ý thức pháp luật cao, có tri thức tổng hợp, có kinh nghiệm phong phú, có đạo đức cách mạng và có tay nghề cao.

Tóm lại, áp dụng pháp luật là hoạt động mang tính tổ chức, thể hiện quyền lực nhà nước, được thực hiện thông qua những cơ quan nhà nước có thẩm quyền, nhà chức trách hoặc các tổ chức xã hội khi được Nhà nước trao quyền, nhằm cá biệt hóa những quy phạm pháp luật vào các trường hợp cụ thể đối với các cá nhân, tổ chức cụ thể.

Khái niệm ADPL về ANM được xây dựng dựa trên cơ sở lý luận về THPL và ADPL nói chung, đồng thời, căn cứ vào những vấn đề mang tính chất lý luận và thực tiễn liên quan tới ANM để hình thành nên khái niệm ADPL về ANM.
Từ góc độ tiếp cận này, có thể đưa ra khái niệm ADPL về ANM như sau: *Áp dụng pháp luật về an ninh mạng ở Việt Nam là tổng thể các hoạt động mang tính tổ chức, thể hiện quyền lực nhà nước, được thực hiện thông qua những cơ quan nhà nước có thẩm quyền, nhà chức trách hoặc các tổ chức, cá nhân khi được Nhà nước trao quyền, nhằm cá biệt hóa những quy phạm pháp luật an ninh mạng vào các trường hợp cụ thể đối với cá nhân, tổ chức cụ thể nhằm bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.*

Áp dụng pháp luật về an ninh mạng là hình thức THPL đặc biệt mà ở đó, cơ quan có thẩm quyền tổ chức cho các chủ thể pháp luật thực hiện các quy định

của pháp luật về ANM hoặc tự mình căn cứ vào các quy định của pháp luật để ban hành các quyết định làm phát sinh, thay đổi, đình chỉ hoặc chấm dứt những quan hệ pháp luật cụ thể trong lĩnh vực ANM theo những thủ tục, trình tự luật định. Các cơ quan có thẩm quyền ở đây được xác định gồm: Bộ Công an, Bộ Quốc phòng, Bộ Khoa học – Công nghệ (trước đây là Bộ Thông tin & Truyền thông), Ban Cơ yếu chính phủ, UBND cấp tỉnh, cá nhân có thẩm quyền… theo quy định của pháp luật ANM, phù hợp với chức năng, nhiệm vụ được giao thực hiện các hoạt động quản lý nhà nước về ANM như: thanh, kiểm tra, giám sát, kiềm chế, phòng ngừa, xử lý đối với những hành vi vi phạm pháp luật về ANM.

ADPL về ANM là hoạt động mang tính tổ chức, thể hiện quyền lực nhà nước khi cần áp dụng các biện pháp cưỡng chế nhà nước, chế tài pháp luật đối với các chủ thể pháp luật có hành vi vi phạm pháp luật về ANM, được thực hiện thông qua các cơ quan nhà nước có thẩm quyền, lực lượng chuyên trách bảo vệ ANM được Nhà nước trao quyền nhằm cá biệt hóa các quy phạm pháp luật ANM vào các trường hợp cụ thể đối với cá nhân, tổ chức tham gia quan hệ pháp luật do pháp luật ANM điều chỉnh.

Hình thức ADPL về ANM được thể hiện thông qua những quyết định ADPL (quyết định pháp lý mang tính cá biệt, cụ thể) nhằm xử lý hành vi vi phạm pháp luật về ANM. Cụ thể, Bộ Công an có thẩm quyền ra quyết định ADPL về ANM nhằm ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật; yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên KGM 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; thu thập dữ liệu điện tử liên quan đến hoạt động 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 trên KGM; phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật; khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự; biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

Trên cơ sở nghiên cứu lý thuyết về THPL và ADPL nói chung, từ thực tiễn hoạt động ADPL về ANM, có thể đưa ra một số điểm đặc trưng của hoạt động ADPL về ANM như sau:

Thứ nhất, áp dụng pháp luật về an ninh mạng thể hiện ý chí của Nhà nước về bảo vệ chủ quyền quốc gia, bảo đảm trật tự an toàn xã hội trên không gian mạng, đồng thời yêu cầu ý thức chấp hành pháp luật triệt để của các chủ thể

Cũng như chủ quyền lãnh thổ đối với các bộ phận cấu thành lãnh thổ quốc gia, chủ quyền quốc gia trên KGM là quyền tối cao, tuyệt đối, đầy đủ đối với phạm vi KGM thuộc quyền kiểm soát của quốc gia. Bảo vệ vững chắc chủ quyền quốc gia trên KGM là một trong những mục tiêu quan trọng của ADPL về ANM. Đó là quyền quản lý, kiểm soát đối với cơ sở hạ tầng KGM và hệ thống thông tin quan trọng về an ninh quốc gia được tạo ra, lưu trữ, xử lý và truyền đưa trên KGM, được thực hiện thông qua xác lập chủ quyền, quyền tài phán theo luật pháp quốc tế đối với cơ sở hạ tầng mạng thuộc sở hữu cả ở trong và ngoài lãnh thổ quốc gia; đồng thời mã hóa thông tin số truyền đưa trên KGM toàn cầu. Cuộc chiến trên KGM là cuộc chiến có tính chất không biên giới. ADPL tốt về chủ quyền quốc gia trên KGM không chỉ là bảo đảm an toàn vận mệnh đất nước, bản chất và sự tồn tại của chế độ chính trị, mà còn là biện pháp phòng ngừa chủ động có ý nghĩa quyết định để xây dựng và phát triển đất nước. Trong ADPL về ANM, các cơ quan có thẩm quyền đại diện ý chí của Nhà nước vừa chủ động tự ADPL vừa tổ chức cho các chủ thể khác thực hiện và ADPL.

Pháp luật về ANM là công cụ quan trọng để Nhà nước bảo vệ chủ quyền quốc gia, đảm bảo TTATXH trên KGM. Chủ thể là các cơ quan nhà nước có thẩm quyền sử dụng pháp luật là công cụ cơ bản, sử dụng biện pháp hành chính, tố tụng có đặc trưng mệnh lệnh, mang tính bắt buộc và được bảo đảm thực hiện bằng sự cưỡng chế. Cơ quan nhà nước có thẩm quyền, theo quy định là Bộ Công an có thể quyết định điều tra tiền tố tụng mà không cần phải có đơn tố giác hay đơn kiện đối với trường hợp mà Bộ Công an nhận thấy có dấu hiệu xâm phạm ANM quốc gia hoặc có dấu hiệu vi phạm pháp luật về ANM. Khi điều tra, xét xử, các chủ thể khác phải chấp hành các yêu cầu, quyết định của cơ quan nhà nước có thẩm quyền. Các quyết định này có giá trị bắt buộc thi hành và được đảm bảo bằng sự cưỡng chế của Nhà nước.

Bên cạnh đó, trong hoạt động ADPL về ANM của các cơ quan chức năng, phụ thuộc nhiều vào ý thức pháp luật, sự triệt để tuân thủ, chấp hành pháp luật và THPL về ANM của các chủ thể khác. Đặc biệt là sự thượng tôn pháp luật của các cơ quan có thẩm quyền ADPL và nhất là cá nhân, các doanh nghiệp cung ứng dịch vụ trên KGM, người dùng mạng. Các cá nhân, các doanh nghiệp tự giác tuân thủ pháp luật, có ý thức chấp hành pháp luật sẽ có ý thức tự phòng vệ trước những cám dỗ lợi ích khi tham gia hoạt động trên KGM. Một trong những ngành nghề kinh doanh đem lại lợi nhuận cao và có xu hướng ngày càng phát triển cả trên thế giới và tại Việt Nam là dịch vụ trò chơi trực tuyến. Tuy nhiên, nếu không tỉnh táo, tự giác, người dùng dễ sa vào nhiều trò chơi trực tuyến mô phỏng cờ bạc hoặc có nội dung nhạy cảm về chính trị, chứa đựng yếu tố khiêu dâm, bạo lực; nhiều trò chơi trực tuyến bị đính kèm mã độc có chức năng nghe lén điện thoại, thu thập thông tin người dùng đang gia tăng trên KGM. Khi tham gia hoạt động kinh doanh, cung cấp dịch vụ trên KGM, doanh nghiệp cần ý thức cao độ trong việc cung cấp tài liệu, chứng cứ và chủ động hợp tác với cơ quan điều tra, tạo điều kiện điều tra, xử lý hiệu quả cho cơ quan điều tra thì có thể được xem xét miễn trừ hay giảm nhẹ chế tài.

Thứ hai, áp dụng pháp luật về an ninh mạng yêu cầu sự phối hợp chặt chẽ giữa các chủ thể có thẩm quyền và sự hợp tác giữa các nhà nước.

An ninh mạng là vấn đề an ninh phi truyền thống, không chỉ là vấn đề riêng của từng quốc gia mà với phạm vi tác động không biên giới, làm biên giới địa lý giữa các quốc gia trở nên "mềm hóa", thậm chí làm “biến mất” biên giới quốc gia. Các mối đe dọa ANM có thể bắt nguồn từ một cá nhân, ở một quốc gia nhất định do tính ẩn danh mà liên quan đến nhiều lĩnh vực, nhiều quốc gia, trở thành vấn đề toàn cầu, tác động trực tiếp và cả gián tiếp đến an ninh quốc gia.

Để ứng phó, xử lý các hành vi xâm phạm ANM không chỉ cần nhiều sự nỗ lực của các cơ quan nhà nước có thẩm quyền trong thực tiễn ADPL về ANM ở từng quốc gia, mà rất cần sự nỗ lực hợp tác chung của nhiều quốc gia, thậm chí của cả cộng đồng quốc tế. Thực tiễn cho thấy, nhiều vụ xâm phạm ANM không chỉ diễn ra trong phạm vi một quốc gia, mà tội phạm ở nước này lại tấn công vào mục tiêu KGM của nước khác. Do đó, quá trình điều tra, xử lý vi phạm, áp dụng chế tài của pháp luật về ANM ngoài sự phối hợp của các cơ quan, tổ chức trong nước với nhau, đối với các vụ xâm phạm ANM có tính quốc tế, các cơ quan quản

lý nhà nước về ANM phải hợp tác với cơ quan ANM của các quốc gia có liên quan trong việc cung cấp thông tin, điều tra và xử lý vi phạm. Qua đó, năng lực pháp lý trong việc kiểm soát ANM được củng cố và tăng cường.

Thứ ba, áp dụng pháp luật về an ninh mạng đòi hỏi các chủ thể có thẩm quyền phải có năng lực, trình độ chuyên môn cao về pháp luật, về công nghệ thông tin, công nghệ số và có phẩm chất đạo đức tốt

Áp dụng pháp luật về ANM (chủ yếu theo chức năng của các cơ quan bảo vệ pháp luật) yêu cầu các cơ quan có thẩm quyền phải có được trang thiết bị, cơ sở vật chất hiện đại, đồng bộ như máy tính, các thiết bị phần cứng công nghệ thông tin có kết nối, hệ thống ứng dụng công nghệ thông tin, phần mềm ứng dụng và cơ sở dữ liệu... Tuy nhiên, có cơ sở vật chất hiện đại, nhưng các chủ thể thiếu trình độ, hiểu biết về công nghệ thông tin sẽ là trở lực không nhỏ đối với ADPL về ANM. Thực tiễn cho thấy, sự phát triển vượt bậc của công nghệ thông tin, công nghệ số đã và sẽ tác động đáng kể đến hiệu quả thực tiễn ADPL về ANM. Do đó, đòi hỏi các chủ thể có thẩm quyền ADPL về ANM phải có trình độ, kỹ năng và hiểu biết chuyên sâu về lĩnh vực công nghệ thông tin, công nghệ số.

Khoa học công nghệ mạng, công nghệ thông tin, công nghệ số, làm cho thế giới ngày càng phẳng hơn với khả năng ứng dụng vượt trội. Những đột phá, tiện ích to lớn về công nghệ blockchain (chuỗi khối), công nghệ vạn vật kết nối IoT, công nghệ điện toán đám mây, công nghệ trí tuệ nhân tạo,… tiềm ẩn nhiều thách thức đối với các chủ thể thực hiện pháp luật về ANM. Lượng thông tin khổng lồ trên mạng cùng với những đột phá công nghệ đã trở thành tài sản của cá nhân, tổ chức và cả quốc gia. Nó có thể biến nhiều chủ thể trở nên giàu có khi tận dụng lợi thế các công nghệ này. Ngược lại, một số chủ thể có thẩm quyền, có chức năng quản lý nhà nước, có trình độ chuyên môn về CNTT, một số được giao nắm giữ một số vị trí quan trọng, nhưng lại thiếu đạo đức đã lợi dụng công cụ này để tìm cách chống phá Nhà nước, đi ngược lợi ích quốc gia, xâm hại ANQG, làm mất TTATXH, vi phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân bằng nhiều thủ đoạn như phát tán, lan truyền tin giả, tổ chức các đường dây cờ bạc, lừa đảo qua mạng, gây ra các vụ tấn công mạng... Với đặc tính lan truyền nhanh chóng, cộng với thói quen lướt tin không kiểm chứng của người dùng mạng sẽ tạo cơ hội cho một vài chủ thể thiếu ý thức đạo đức thực hiện chỉ bằng một hành vi không tuân thủ pháp luật về ANM sẽ để lại tổn thất nặng nề. Phẩm chất đạo đức

tốt là đòi hỏi quan trọng của các chủ thể ADPL về ANM để phòng ngừa hành vi nhỏ, hậu quả lớn.

Mục tiêu chuyển đổi số quốc gia, xây dựng chính phủ điện tử chỉ có thể thành công khi các hoạt động như cải cách thủ tục hành chính, thương mại điện tử, ngân hàng điện tử, cơ sở dữ liệu số... được đảm bảo diễn ra bình thường và an toàn trên KGM. Kiến thức của các chủ thể có thẩm quyền trong ADPL về ANM đã dần được cải thiện, nhưng cơ bản vẫn chưa đáp ứng đúng nhu cầu thực tiễn. Để ứng phó với các cuộc tấn công mạng do khai thác những công nghệ thông tin, công nghệ số ngày càng tinh vi, khó lường là những đòi hỏi cấp bách phải nâng cao trình độ chuyên sâu về khoa học công nghệ thông tin, công nghệ số, thường xuyên rèn luyện kỷ luật, trau dồi bản lĩnh, đạo đức cách mạng của những cá nhân có thẩm quyền, trách nhiệm ADPL về ANM. Đây cũng là cơ sở để các chủ thể có thẩm quyền tăng cường thực hiện có hiệu quả việc ADPL về ANM.

Thứ tư, áp dụng pháp luật an ninh mạng chính là hoạt động cá biệt hóa quy phạm pháp luật an ninh mạng đối với từng hành vi vi phạm pháp luật an ninh mạng theo hướng linh động, sáng tạo.

Đối tượng của hoạt động ADPL về ANM là những quan hệ xã hội cần đến sự điều chỉnh cá biệt, bổ sung trên cơ sở những mệnh lệnh chung trong quy phạm pháp luật ANM. Do vậy, kết quả của hoạt động ADPL về ANM có ảnh hưởng rất lớn đến hiệu quả, hiệu lực quản lý nhà nước về ANTT nói chung, quản lý nhà nước về ANM cũng như ảnh hưởng lớn đến quyền lợi ích của các chủ thể bị áp dụng chế tài pháp luật về ANM và kể cả những người có liên quan. ADPL về ANM – về nguyên tắc - chỉ do các chủ thể có thẩm quyền tiến hành, đó chỉ có thể là các cơ quan nhà nước có thẩm quyền, hoặc là các tổ chức, cá nhân được nhà nước trao quyền ADPL về ANM. Vì thế, hoạt động ADPL về ANM phải triệt để tuân thủ những quy định về trình tự, thủ tục, thẩm quyền, thời hiệu… Điều này đặt ra yêu cầu về tính chính xác, tính hiệu quả của hoạt động áp dụng pháp luật ANM phụ thuộc rất nhiều yếu tố, nhưng chủ yếu nhất vẫn là từ chính các chủ thể có thẩm quyền ADPL về ANM. Hơn nữa, ADPL về ANM được tiến hành chủ yếu thông qua việc áp dụng quy định của pháp luật về hành chính, hình sự, TTHS vì vậy, những vụ việc thực tế xảy ra trên KGM theo những diễn biến khác nhau và có liên quan đến nhiều đối tượng khác nhau đòi hỏi chủ thể ADPL về ANM

phải xác định rất rõ hình thức, nội dung, bản chất của từng vụ việc cũng như xác định tổng thể quy trình, giai đoạn ADPL về ANM.

Thực tế cho thấy, hoạt động ADPL về ANM của các cơ quan có thẩm quyền có những trường hợp khá đơn giản, diễn ra trong khoảng thời gian rất ngắn, tuy nhiên cũng có những trường hợp ADPL về ANM rất phức tạp, diễn ra trong thời gian khá dài, bao gồm rất nhiều vấn đề phải giải quyết, liên quan đến nhiều chủ thể khác nhau. Tựu trung lại, có thể chia toàn bộ quy trình ADPL về ANM thành bốn giai đoạn (bốn bước – phù hợp với lý luận về áp dụng pháp luật) như sau:

Một là, phân tích, đánh giá đúng, chính xác các tình tiết của sự việc thực tế đã xảy ra: Đây là giai đoạn rất quan trọng, là cơ sở cho các hoạt động tiếp theo bởi đặc thù về môi trường nơi xảy ra những vụ việc thực tế là không gian mạng.

Để có thể áp dụng pháp luật nói chung, ADPL về ANM một cách đúng đắn, đòi hỏi chủ thể có thẩm quyền ADPL về ANM phải gần như ngay lập tức, nhanh chóng thu thập thông tin đầy đủ, chính xác, kịp thời về vụ việc thực tế đã xảy ra, đánh giá khách quan, toàn diện và đầy đủ các tình tiết của vụ việc, xác định đúng bản chất, đặc trưng pháp lí của vụ việc. Trong những trường hợp cần thiết, cơ quan nhà nước có thẩm quyền có thể phải sử dụng các biện pháp chuyên môn đặc biệt, với sự trợ giúp của các phương tiện khoa học kỹ thuật hiện đại nhằm làm rõ sự thật khách quan của sự việc đã diễn ra trong thực tế trên môi trường KGM.

Hai là, lựa chọn quy phạm pháp luật để áp dụng: Sau khi đánh giá đúng bản chất của vụ việc, chủ thể có thẩm quyền ADPL phải lựa chọn quy phạm pháp luật và giải thích nội dung, ý nghĩa của chúng.

Khi lựa chọn quy phạm pháp luật để áp dụng cần lưu ý, quy phạm pháp luật về ANM được lựa chọn phải đang có hiệu lực ở thời điểm xảy ra vụ việc (trừ trường hợp pháp luật có quy định khác), nếu có những quy định chồng chéo, trùng lặp thì phải dựa vào giá trị pháp lí hay hiệu lực theo thời gian của văn bản để lựa chọn cho chính xác. Tiếp đó, chủ thể có thẩm quyền ADPL về ANM phải làm sáng tỏ nội dung, ý nghĩa của quy phạm được lựa chọn; đối chiếu, lí giải sự phù hợp giữa quy phạm pháp luật tìm được với sự việc cần áp dụng pháp luật, thấy được mối quan hệ mật thiết giữa chúng từ đó quyết định áp dụng quy phạm pháp luật trong lĩnh vực ANM để giải quyết vụ việc đã xảy ra.

Ba là, ra quyết định áp dụng pháp luật: Sau khi lựa chọn được quy phạm pháp luật phù hợp, chủ thể áp dụng pháp luật phải ra quyết định áp dụng pháp

luật. Quyết định ADPL phải xác định rõ quyền, nghĩa vụ hay trách nhiệm pháp lí của chủ thể được (bị) áp dụng pháp luật. Nội dung của quyết định áp dụng pháp luật ảnh hưởng trực tiếp đến lợi ích của chủ thể bị áp dụng pháp luật. Ra quyết định áp dụng là hoạt động thể hiện rất rõ năng lực, trình độ, bản lĩnh và sự sáng tạo của chủ thể có thẩm quyền áp dụng pháp luật. Quyết định ADPL về ANM phải đáp ứng yêu cầu cơ bản: Phải được ban hành hợp pháp (đúng thẩm quyền, có cơ sở pháp luật); phải có tính khả thi (phù hợp với điều kiện thực tế) và quyết định áp dụng pháp luật về ANM phải được thể hiện dưới hình thức văn bản được gọi là văn bản áp dụng pháp luật.

Bốn là, tổ chức thực hiện quyết định áp dụng pháp luật. Quyết định ADPL về ANM thực chất là những quyết định pháp lý mang tính cá biệt, cụ thể, trực tiếp xác định quyền, lợi ích hoặc nghĩa vụ pháp lý của chủ thể tham gia quan hệ pháp luật trên KGM. Tùy thuộc vào từng trường hợp, để thực hiện quyết định ADPL về ANM có hiệu quả cần có sự chuẩn bị về thời gian, điều kiện vật chất, kĩ thuật, nhân lực... Trong quá trình thực hiện quyết định ADPL về ANM cần phải có sự kiểm tra, giám sát… đảm bảo quyết định ADPL được thực hiện một cách nghiêm chỉnh, chính xác.

b. Vai trò của áp dụng pháp luật về an ninh mạng

Thứ nhất, áp dụng pháp luật về an ninh mạng là phương thức cơ bản, quan trọng góp phần hiện thực hóa và bảo vệ quan điểm, đường lối của Đảng về an ninh mạng

Đảng Cộng sản Việt Nam là lực lượng lãnh đạo Nhà nước và xã hội ở Việt Nam. Sự lãnh đạo đó được thể hiện thông qua những phương thức khác nhau nhưng trước tiên đó là việc đề ra quan điểm, chủ trương, đường lối, những nguyên tắc chung. Nhà nước thể chế hóa các chủ trương, đường lối lãnh đạo về các lĩnh vực xã hội của Đảng thành pháp luật và hiện thực hóa trong việc tổ chức thực hiện và ADPL. Nội dung của pháp luật về ANM là sự cụ thể hóa quan điểm, đường lối của Đảng bằng những quy phạm pháp luật về ANM. Vì vậy, ADPL về ANM là cách thức cơ bản, hiệu quả để quan điểm, đường lối của Đảng đi vào cuộc sống, phát huy hiệu lực, hiệu quả trong việc điều chỉnh các quan hệ xã hội, giúp các chủ thể nhận thức và thực hiện ngày càng tốt hơn quan điểm, đường lối của Đảng, pháp luật về ANM của nhà nước. Qua đó, tính đúng đắn, kịp thời trong quan điểm, đường lối của Đảng, tính hiệu quả, hiệu lực của quản lý nhà nước được kiểm

nghiệm trên thực tế, đồng thời có những điều chỉnh, bổ sung kịp thời trong tổ chức thực hiện để bảo đảm việc ADPL về ANM ngày càng hiệu quả hơn.

Thứ hai, áp dụng pháp luật về an ninh mạng góp phần củng cố, hình thành nhận thức và hành động chung của các chủ thể trong việc xây dựng không gian mạng an toàn

Trong suốt chiều dài phát triển của lịch sử nhân loại, chưa bao giờ con người đạt được những thành công vượt bậc, song cũng chưa bao giờ con người phải đối mặt với những nguy cơ khốc liệt đe dọa đến sự tồn vong của mình như hiện tại. Bên cạnh sự cạn kiệt tài nguyên, biến đổi khí hậu, ô nhiễm môi trường, thiên tai, dịch bệnh, tội phạm xuyên quốc gia… tình trạng xuất hiện ngày càng nhiều loại "rác" trên môi trường KGM khiến cuộc sống của con người trở nên ngột ngạt hơn. Mức độ nguy hiểm của loại rác (tội phạm mạng, gián điệp mạng, khủng bố mạng, chiến tranh mạng...), không khác gì mấy so với rác thải hạt nhân. Điều này làm cho hiệu quả, hiệu lực của việc ADPL về ANM không được đảm bảo một cách tối ưu. Do đó, mỗi chủ thể cần nhận thức đúng đắn và nghiêm túc về xây dựng một KGM an toàn.

Áp dụng pháp luật về ANM *(một hình thức đặc thù của thực hiện pháp luật ANM)* giúp các chủ thể nhận thức được giới hạn hành vi bị nghiêm cấm, không được phép hoặc bắt buộc phải thực hiện trên một "miền lãnh thổ" mới mẻ là KGM. Hơn nữa, ADPL về ANM còn giúp chủ thể có thẩm quyền phòng ngừa, ngăn chặn những hành vi vi phạm pháp luật và hành vi phạm tội trên KGM. Từ việc nhận thức đúng đắn đó, mỗi chủ thể có thẩm quyền ADPL về ANM sẽ chủ động thực thi quyền năng, trách nhiệm của mình để góp phần loại trừ nguyên nhân, điều kiện của các hành vi xâm hại ANM, hành vi xâm hại quyền, lợi ích hợp pháp của Nhà nước và các chủ thể khác trên KGM. Khi phát hiện chủ thể thực hiện hành vi vi phạm pháp luật xâm hại ANM, Cơ quan có thẩm quyền sẽ tiến hành các biện pháp yêu cầu chủ thể vi phạm chấm dứt hành vi vi phạm, khắc phục hậu quả hoặc áp dụng các biện pháp xử lý (chế tài) phù hợp với tính chất, mức độ vi phạm.

Thứ ba, áp dụng pháp luật về an ninh mạng góp phần bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, quyền và lợi ích hợp pháp của các chủ thể

Đối với cá nhân người dùng mạng, cần phải được bảo vệ quyền và lợi ích hợp pháp, nhất là các quyền con người, quyền tự do công dân, được tiếp cận với tài nguyên thông tin an toàn trên KGM. Quyền con người, quyền tự do công dân

và pháp luật là hai yếu tố có mối quan hệ chặt chẽ với nhau. Quyền con người, quyền tự do công dân chỉ có thể được thực hiện trên thực tiễn cuộc sống khi được quy định trong pháp luật. Pháp luật xác nhận, củng cố và hoàn thiện quyền con người, quyền công dân. Quyền con người, quyền công dân được pháp luật ghi nhận và bảo vệ. Để bảo đảm quyền con người, quyền công dân trong lĩnh vực ANM, pháp luật về ANM quy định những hành vi bị cấm và hành vi buộc phải làm; quyền của người sử dụng trên KGM.

Thực hiện các quy định pháp luật về an ninh mạng nói chung, ADPL về ANM nói riêng, góp phần bảo đảm, bảo vệ, thực hiện quyền con người, quyền công dân trên thực tiễn. Bởi lẽ các quyền con người, quyền công dân như quyền được an toàn; quyền tiếp cận thông tin; quyền được bảo vệ bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên KGM là các biểu hiện cụ thể của quyền con người, quyền công dân trên các lĩnh vực chính trị, kinh tế, xã hội. Một quốc gia không thể được đánh giá là đảm bảo ANQG, TTATXH, đảm bảo các quyền con người, quyền công dân khi các thông tin thuộc bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư bị chiếm đoạt, mua bán, trao đổi tràn lan trên KGM, làm ảnh hưởng, gây thiệt hại đến danh dự, uy tín, nhân phẩm và quyền và lợi ích hợp pháp của cá nhân. Với một hệ thống pháp luật về ANM được xây dựng theo hướng bảo đảm tính đồng bộ, thống nhất, toàn diện, kịp thời điều chỉnh các quan hệ xã hội phát sinh, tương thích với pháp luật quốc tế, đáp ứng xu thế hội nhập, nhất là khi KGM đã và đang trở thành phần không gian tất yếu trong đời sống hàng ngày, Việt Nam đang nỗ lực trong quá trình tổ chức thực hiện và ADPL về ANM để góp phần đạt được mục tiêu bảo vệ ANQG, bảo đảm TTATXH, bảo đảm quyền và lợi ích hợp pháp của con người, công dân.

Thứ tư, áp dụng pháp luật về an ninh mạng góp phần bảo đảm và tăng cường pháp chế xã hội chủ nghĩa

Tăng cường pháp chế XHCN có ý nghĩa lớn trong việc thúc đẩy phòng ngừa các hành vi vi phạm pháp luật về ANM. Pháp chế XHCN là một nguyên tắc cơ bản trong thực hiện và áp dụng pháp luật nói chung, ADPLvề ANM nói riêng. Pháp chế XHCN đòi hỏi tất cả các cơ quan, tổ chức, cá nhân phải triệt để tuân thủ pháp luật về ANM một cách nghiêm chỉnh. Thực tiễn cho thấy, pháp chế XHCN

trong thực hiện pháp luật nói chung và ADPL về ANM nói riêng là những nội dung quan trọng cần tăng cường ở Việt Nam.

Việc phòng ngừa, ngăn chặn và xử lý các hành vi xâm phạm KGM quốc gia, ít nhất là trong lĩnh vực ANM là một trong những yêu cầu tất yếu khách quan trong tăng cường pháp chế XHCN, xây dựng nhà nước pháp quyền XHCN ở Việt Nam. Thực hiện Nghị quyết 48-NQ/TW ngày 24/5/2005 của Bộ Chính trị về Chiến lược xây dựng và hoàn thiện pháp luật đến năm 2010, định hướng đến năm 2020, Nhà nước đã ban hành nhiều văn bản pháp luật để điều chỉnh các lĩnh vực của đời sống xã hội. Đối với lĩnh vực ANM, tháng 6/2018, Quốc hội nước Cộng hòa XHCN Việt Nam đã ban hành Luật An ninh mạng năm 2018 để điều chỉnh các quan hệ pháp luật ANM. Điều đó cho thấy, việc đưa pháp luật về ANM vào cuộc sống là đòi hỏi tất yếu, góp phần tăng cường pháp chế XHCN. Quy định pháp luật ANM phải được thực hiện, phải được coi là nguyên tắc trong hành động của các cơ quan, tổ chức, cá nhân. An toàn, trật tự trên KGM được đảm bảo sẽ góp phần tăng cường pháp chế XHCN.

Áp dụng pháp luật về ANM, phòng ngừa, ngăn chặn và xử lý các hành vi xâm phạm ANM ở Việt Nam hiện nay là cơ sở của pháp chế XHCN. ADPL về ANM không chỉ góp phần tạo dựng KGM an toàn mà còn thể hiện ý thức tự giác và trách nhiệm của các chủ thể trong xã hội, đặc biệt là thể hiện ý thức trách nhiệm của cơ quan, tổ chức, cá nhân có thẩm quyền, trách nhiệm; góp phần thượng tôn pháp luật, bảo đảm sự nghiêm minh của pháp luật, hiệu quả quản lý nhà nước về TTATXH trong điều kiện xây dựng, hoàn thiện Nhà nước pháp quyền XHCN của Nhân dân, do Nhân dân, vì Nhân dân ở Việt Nam hiện nay.

2. Bảo đảm áp dụng pháp luật về an ninh mạng

a. Bảo đảm về chính trị

Bảo đảm về chính trị chính là sự bảo đảm và phát huy tốt nhất sự lãnh đạo của Đảng Cộng sản Việt Nam đối với quá trình tổ chức thực hiện, áp dụng pháp luật, trong đó có ADPL về ANM. Sự lãnh đạo về chính trị của Đảng đối với ADPL về ANM thể hiện ở mức độ quan tâm và nhận thức của các cấp ủy Đảng đối với công tác ADPL về ANM. Các quan điểm của Đảng về ANM và ADPL về ANM phải được thể hiện nhất quán trong các văn kiện, nghị quyết của Đảng; phải thể chế hóa thành quy định của pháp luật ANM.

Hiến pháp năm 2013 tiếp tục khẳng định vai trò lãnh đạo trực tiếp, toàn diện về mọi mặt của Đảng trên tất các mặt, lĩnh vực của đời sống xã hội. Sự lãnh đạo của Đảng là tất yếu khách quan, quyết định mọi thắng lợi của cách mạng Việt Nam. Thực tiễn quá trình lãnh đạo của Đảng từ khi ra đời đến nay đã đúc rút được nhiều kinh nghiệm quý báu, một trong số đó là xác định nội dung, phương thức lãnh đạo của Đảng đối với Nhà nước, trong đó phân định rõ sự lãnh đạo của Đảng với chức năng quản lý của Nhà nước. Đảng không bao biện, làm thay công việc của Nhà nước, nhưng cũng không buông lỏng, khoán trắng cho Nhà nước. Trong điều kiện xây dựng nhà nước pháp quyền, sự phân định này càng phải mang tính pháp quyền. Cần phải thượng tôn Hiến pháp và triệt để tuân thủ pháp luật, nhất là trong việc lãnh đạo, chỉ đạo các cơ quan nhà nước ADPL, trong đó có ADPL về ANM.

Chú trọng tăng cường và kết hợp chặt chẽ giữa công tác kiểm tra Đảng với hoạt động giám sát, kiểm tra việc thực hiện pháp luật của các cơ quan, nhất là vai trò giám sát công tác tổ chức thực hiện và áp dụng pháp luật nói chung và đặc biệt là ADPL về ANM nói riêng. Đảm bảo về chính trị đóng vai trò rất quan trọng đối với việc thực hiện hiệu quả pháp luật ANM dưới sự lãnh đạo toàn diện của Đảng. Định hướng chính trị của Đảng luôn nhất quán, tuy nhiên, hiệu lực, kết quả ADPL còn phụ thuộc nhiều vào tư duy, nhận thức và hành động của các cấp ủy Đảng trong hệ thống các cơ quan nhà nước có thẩm quyền về xây dựng, ban hành pháp luật về ANM, nhất là trong việc tổ chức thực hiện và ADPL về ANM.

b. Bảo đảm về pháp lý

Một trong ba đột phá chiến lược mà Đại hội XIII của Đảng đã xác định đó là đột phá về thể chế (chính sách và pháp luật). Do đó, Nhà nước phải không ngừng hoàn thiện thể chế về an ninh mạng. Đảm bảo mối quan hệ giữa công tác xây dựng văn bản quy phạm pháp luật về ANM với hoạt động thực hiện và ADPL về ANM. Nghĩa là không chỉ chú trọng vào thực thi pháp luật mà buông lỏng việc ban hành văn bản quy phạm pháp luật về ANM. Từ rất lâu rồi, Mongtexkiơ khẳng định: "Có hai hiện tượng hư hỏng, một là nhân dân hoàn toàn không chấp hành pháp luật, hai là bản thân pháp luật làm hư hỏng nhân dân, tệ xấu nói sau không có cách gì chữa được, vì nó nằm ngay trong thuốc"[26]. Còn Lênin chỉ rõ: "Khi ban hành những đạo luật đáp ứng lòng mong đợi và hy vọng của quảng đại quần chúng

[26] C.L.Montesquieu (bản dịch tiếng Việt 1996), *Tinh thần pháp luật*, Nxb Giáo dục, Hà Nội.

nhân dân thì chính quyền mới cắm được những cái mốc trên con đường phát triển của những hình thức sinh hoạt mới"[27]. Sinh thời, Chủ tịch Hồ Chí Minh nhấn mạnh "vũ lực của cuộc cách mạng này là sự tiến bộ về chính trị, kinh tế, văn hóa, pháp luật"[28]. Trên cơ sở kế thừa tư tưởng của V.I. Lênin và Chủ tịch Hồ Chí Minh, trong công cuộc đổi mới, Đảng ta khẳng định: "Quản lý bằng pháp luật đòi hỏi phải quan tâm xây dựng pháp luật. Từng bước bổ sung và hoàn chỉnh hệ thống pháp luật"[29]. Điều kiện bảo đảm về mặt pháp lý thể hiện yêu cầu về một hệ thống pháp luật hoàn thiện, thể hiện ở sự đồng bộ, toàn diện, khả thi, phù hợp và kỹ thuật lập pháp cao.

Việc ứng dụng khoa học công nghệ qua KGM để kết nối, chia sẻ, trao đổi thông tin, qua đó biến thông tin thành nguồn lực, thành sức mạnh để tác động tích cực trở lại với mục đích phát triển xã hội hiện nay đã là một phần không thể thiếu trong cuộc sống hiện đại. Với Việt Nam, công nghệ thông tin, khoa học công nghệ còn là động lực quan trọng để phát triển, nhất là trong quá trình xây dựng quốc gia số. Hoàn thiện pháp luật về ANM là ưu tiên hàng đầu, trở thành một trong những công cụ sắc bén nhất của Nhà nước để tháo gỡ, loại bỏ các mối đe dọa từ việc sử dụng công nghệ cao xâm phạm KGM. Đây cũng là hành lang, là cơ sở pháp lý tạo nên môi trường mạng ổn định, bền vững để phát triển đất nước.

c. Bảo đảm về kinh tế, văn hóa - xã hội, giáo dục

Cùng với điều kiện bảo đảm về chính trị, pháp lý, đây là những điều kiện bảo đảm cần được chú ý trong thực hiện pháp luật và nhất là trong ADPL về ANM. Theo đó, bảo đảm về kinh tế được xác định là các điều kiện cần thiết về cơ sở vật chất, trang thiết bị công nghệ số, kinh phí và hạ tầng kỹ thuật cho các hoạt động tổ chức thực hiện và ADPL về ANM trong thực tiễn.

Pháp luật về ANM là một nội dung (tiểu hệ thống) pháp luật mới trong hệ thống pháp luật ở Việt Nam. Vì vậy việc ADPL về ANM chịu tác động rất lớn của nhiều yếu tố, trong đó có những tác động không nhỏ từ truyền thống, văn hóa - xã hội. Bên cạnh đó, trình độ nhận thức của các chủ thể thực hiện pháp luật và nhất là năng lực, trình độ ADPL về ANM cũng như tập quán, quan niệm xã hội… đều có tác động không nhỏ đến hiệu quả hoạt động ADPL về ANM.

---

[27] V.I. Lênin (1970), *Bàn về pháp chế xã hội chủ nghĩa*, Nxb Sự thật, Hà Nội.
[28] Hồ Chí Minh (1985), *Nhà nước và pháp luật*, Nxb Pháp lý, Hà Nội
[29] Đảng Cộng sản Việt Nam (1986), *Văn kiện Đại hội đại biểu toàn quốc lần thứ VI*, Nxb Chính trị quốc gia, Hà Nội.

Từ sau công cuộc đổi mới đất nước, cùng với phát triển nền kinh tế thị trường (KTTT) định hướng xã hội chủ nghĩa (XHCN), những chuẩn mực văn hóa pháp lý mới, tốt đẹp và thích ứng, hiện đại hơn đã có tác động tích cực trong ADPL về ANM. Song cũng phải nhìn nhận một cách khách quan rằng, vẫn còn cá biệt có hiện tượng tồn tại ở một bộ phận nhỏ cơ quan có thẩm quyền bảo vệ ANM, bảo vệ KGM quốc gia với những con người có năng lực, trình độ công nghệ, được trang bị những thiết bị hiện đại nhưng đánh mất bản lĩnh chính trị, suy thoái, bất chấp kỷ cương, vẫn vi phạm pháp luật về ANM.

Vì vậy, bên cạnh các bảo đảm về kinh tế, văn hoá - xã hội, việc đẩy mạnh công tác phổ biến, tuyên truyền, giáo dục pháp luật là điều kiện cần thiết để các chủ thể ADPL về ANM có quan niệm, nhận thức và hành động đúng, hạn chế và tiến đến loại bỏ các hành vi không tuân thủ pháp luật về ANM, bảo đảm ADPL về ANM hiệu quả.

d. Bảo đảm về tổ chức, bộ máy

Quá trình tổ chức, thực hiện pháp luật về ANM nói chung và nhất là hoạt động ADPL về an ninh mạng ngoài việc tuân thủ quy trình, thủ tục chặt chẽ, cần thiết phải có một hệ thống tổ chức chặt chẽ, đồng bộ và hoạt động hiệu quả.

Trong hoạt động quản lý nhà nước, pháp luật về ANM đã xác định tương đối bao quát các yêu cầu về tổ chức bảo vệ KGM quốc gia. Theo đó, Chính phủ thống nhất quản lý nhà nước về ANM. Chính phủ có trách nhiệm ban hành theo thẩm quyền và tổ chức thực hiện chính sách, pháp luật, bảo đảm cơ chế và biện pháp phối hợp giữa các bộ, ngành trong việc thực hiện pháp luật về ANM cũng như hoạt động chuyên biệt là ADPL về ANM. Nghiên cứu điều chỉnh pháp luật về ANM hiện nay cho thấy, ADPL về ANM do nhiều chủ thể có địa vị pháp lý khác nhau thực hiện, nhưng Cơ quan chủ công, đầu mối chủ trì, chịu trách nhiệm chính trước Chính phủ về bảo vệ ANQG, bảo đảm TTATXH trên lĩnh vực ANM là Bộ Công an. Đây là cơ quan được Chính phủ giao thống nhất quản lý nhà nước về ANM trên phạm vi toàn quốc. Ngoài ra, các cơ quan khác theo chức năng, nhiệm vụ của mình có trách nhiệm tham gia tổ chức việc thực hiện và ADPL về ANM như VKSND, TAND, Bộ Quốc phòng, Ban Cơ yếu Chính phủ, Bộ Thông tin và Truyền thông... Tuy vậy, cũng cần lưu ý rằng không phải tất cả các thiết chế thuộc các Cơ quan nêu trên đều có thẩm quyền ADPL về ANM mà đối với hoạt động

ADPL về ANM thì chỉ có các cơ quan, thiết chế cụ thể, theo luật định mới có thẩm quyền tổ chức, thực hiện pháp luật và ADPL về ANM.

Luật An ninh mạng 2018 quy định lực lượng chuyên trách bảo vệ ANM được bố trí ở Bộ Công an và Bộ Quốc phòng. Ngoài ra, còn có lực lượng bảo vệ ANM ở các bộ, ngành, UBND cấp tỉnh trong phạm vi của mình, thực hiện và ADPL về ANM đối với lĩnh vực trực tiếp quản lý. Việc tổ chức xây dựng lực lượng bảo vệ ANM có ý nghĩa đặc biệt quan trọng trong bảo đảm ADPL về ANM. Do vậy, việc tiếp tục kiện toàn tổ chức và nguồn nhân lực ADPL về ANM cần được quan tâm đầu tư nhiều hơn trong giai đoạn hiện nay.

CHƯƠNG 2
THỰC TIỄN ÁP DỤNG PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM VÀ PHƯƠNG HƯỚNG NÂNG CAO HIỆU QUẢ

I. THỰC TRẠNG ÁP DỤNG PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM

1. Tình hình vi phạm pháp luật trong lĩnh vực an ninh mạng

a. Hoạt động chống phá của các thế lực thù địch

Việt Nam hiện là một trong 20 quốc gia có số lượng người sử dụng Internet cao nhất thế giới. Mặc dù mạng xã hội và KGM mang lại nhiều lợi ích lớn lao, nhưng chúng cũng đồng thời tạo ra những mối đe dọa nghiêm trọng đối với ANQG, an ninh con người, và TTATXH.

Môi trường mạng đang trở thành nơi thuận lợi để các thế lực thù địch lợi dụng, thực hiện các hoạt động chống phá. Những thế lực này, bao gồm các tổ chức phản động và các phần tử cơ hội, thường xuyên xuyên tạc, chống lại Đảng và Nhà nước ta nhằm xóa bỏ nền tảng tư tưởng của Đảng Cộng sản Việt Nam và phá hoại vai trò lãnh đạo của Đảng. Đây là mặt trận quan trọng mà chúng ta không thể lơ là, cần có sự nhận thức đầy đủ về những thuận lợi và thách thức để đối phó hiệu quả. Công tác đấu tranh tư tưởng trên không gian mạng hiện nay là nhiệm vụ cấp thiết, đòi hỏi sự quyết tâm cao độ của mỗi cá nhân và lực lượng thực hiện.

Các thế lực thù địch thường xuyên khai thác không gian mạng để thu thập thông tin về đường lối, chính sách của Đảng, Nhà nước, cũng như các bí mật quốc gia và quân sự, nhằm tìm kiếm lợi thế trong quan hệ quốc tế. Đồng thời, họ sử dụng mạng để phát tán thông tin sai lệch, xuyên tạc, và thực hiện các chiến lược "diễn biến hòa bình" với mục đích làm bất ổn tình hình chính trị và xã hội, đe dọa an ninh quốc gia và phá hoại nền tảng tư tưởng của Đảng. Những hành động này làm suy giảm niềm tin của nhân dân vào Đảng, Nhà nước, và con đường tiến lên chủ nghĩa xã hội. Khi xảy ra mâu thuẫn hoặc tranh chấp, các thế lực thù địch lợi dụng không gian mạng để tấn công vào các hệ thống thông tin quan trọng của quốc gia, gây hỗn loạn trong công tác lãnh đạo và chỉ đạo của Đảng, Nhà nước và Quân đội. Họ cũng kích động biểu tình, bạo loạn, tạo cớ để can thiệp quân sự.

Các thế lực thù địch cũng lợi dụng tình hình công tác nhân sự, việc xử lý kỷ luật cán bộ lãnh đạo, xử lý sai phạm của các cán bộ cấp cao, hoặc những vấn đề nhạy

cảm khác để xuyên tạc sự thật trên Internet và mạng xã hội. Họ sử dụng các bài viết, hình ảnh, video nhằm hạ thấp uy tín của Đảng, Nhà nước và các lãnh đạo, làm giảm niềm tin của nhân dân vào hệ thống chính trị. Ngoài ra, những thế lực này còn thường xuyên phát tán thông tin xuyên tạc, bịa đặt, vu khống, nhằm chống phá Đảng và Nhà nước qua hàng trăm trang web, blog, tài khoản mạng xã hội. Các hành vi này không chỉ gây hoang mang trong dư luận mà còn làm giảm hiệu quả lãnh đạo của Đảng, Nhà nước, tạo cơ hội cho các tổ chức phản động mở rộng ảnh hưởng.

Chỉ riêng trong năm 2020, các cơ quan chức năng đã phát hiện gần 250 trang web, blog, và hàng trăm tài khoản Facebook, YouTube đăng tải thông tin sai sự thật. Trong 10 tháng đầu năm 2022, Bộ Công an đã điều tra và khởi tố 572 vụ án phạm tội trên không gian mạng, tăng 144% so với cùng kỳ năm trước. Chỉ trong hai tuần cuối tháng 1/2024, Bộ Công an đã phát hiện 40.965 bài đăng trên các trang thông tin điện tử, blog, 88.108 tin, bài đăng trên facebook thu hút hơn 500 nghìn lượt bình luận, 4,5 triệu lượt chia sẻ và 207 video, clip trên youtube có nội dung sai sự thật. Hàng chục vụ lợi dụng danh nghĩa bảo vệ môi trường, khiếu kiện đất đai, kêu gọi qua mạng để tụ tập đông người, biểu tình tại một số địa phương như Hà Nội, Thành phố Hồ Chí Minh, Nghệ An, Bình Định, Hà Tĩnh, Tiền Giang…

Bên cạnh đó, các đối tượng thù địch còn kêu gọi biểu tình, kích động hành động trái pháp luật, nhằm phá hoại an ninh trật tự. Trung bình mỗi tháng, chúng phát tán hơn 130.000 bài viết, video xuyên tạc trên các nền tảng mạng xã hội, với hơn 80.000 bài viết trên Facebook và 40.000 bài viết trên YouTube. Các tổ chức phản động xây dựng các kênh truyền thông trên mạng xã hội để phát tán thông tin xấu độc, làm hoang mang dư luận, và kêu gọi sự tham gia vào các hành vi bất hợp pháp. Nội dung xuyên tạc của các thế lực thù địch rất đa dạng, bao gồm các vấn đề tư tưởng, chính trị, văn hóa, xã hội và xây dựng Đảng, tập trung chủ yếu vào việc tấn công vào hệ tư tưởng và đường lối của Đảng Cộng sản Việt Nam. Những thông tin sai lệch này không chỉ gây ảnh hưởng tiêu cực đến niềm tin của nhân dân mà còn tạo ra những xáo trộn trong xã hội, đe dọa sự ổn định và phát triển của đất nước.

b. Hoạt động tấn công mạng

Tấn công mạng là hành vi sử dụng không gian mạng để tiến hành các hoạt động tấn công, xâm nhập vào hệ thống mạng máy tính, cơ sở dữ liệu, hạ tầng mạng, thông tin dữ liệu, thiết bị của cá nhân hoặc tổ chức, với mục đích có thể tốt hoặc xấu. Tình trạng tấn công mạng hiện nay đã trở thành một mối lo ngại nghiêm trọng trên toàn cầu, trong đó có Việt Nam. Các cuộc tấn công mạng đang đặt ra thách thức lớn đối với các doanh nghiệp hoạt động trong môi trường trực tuyến. Với sự phát triển không ngừng của công nghệ, các hình thức tấn công mạng qua Internet ngày càng trở nên đa dạng và tinh vi hơn.

Trong những năm gần đây, mặc dù số vụ tấn công trực tuyến tại Việt Nam có xu hướng giảm, nhưng theo những nghiên cứu năm 2022, Việt Nam vẫn đứng thứ 49 trên toàn cầu về số lượng các cuộc tấn công mạng. Trong 2 năm gần nhất, số vụ được phát hiện và ngăn chặn trong năm 2023 là 63.482.728 vụ, và năm 2024 là 41.989.163 vụ (giảm 33,8%).

Theo số liệu từ Công ty Công nghệ An ninh mạng Quốc gia Việt Nam NCS, trong 6 tháng đầu năm 2023, số vụ tấn công an ninh mạng vào các hệ thống của Việt Nam đã giảm khoảng 12% so với năm 2022, với 5.100 vụ. Tuy nhiên, các vụ tấn công có chủ đích (APT) vào các cơ sở trọng yếu lại tăng khoảng 9%, do các cơ sở này chứa nhiều dữ liệu quan trọng, là mục tiêu hấp dẫn của tin tặc. Các chiến dịch tấn công APT trong nửa đầu năm 2023 tập trung vào ba phương thức chính: tấn công qua e-mail giả mạo, tấn công qua lỗ hổng phần mềm trên máy chủ và tấn công qua lỗ hổng website. Các cuộc tấn công bằng e-mail lừa đảo rất tinh vi, đặc biệt khi tin tặc có thể chiếm quyền kiểm soát e-mail của các lãnh đạo cấp cao, khiến công tác phòng ngừa trở nên khó khăn. Ngoài ra, trong nửa đầu năm 2023, đã ghi nhận việc hacker tấn công vào các website của các cơ quan nhà nước với tên miền gov.vn và một số tổ chức giáo dục với tên miền edu.vn, chèn mã quảng cáo cờ bạc và cá độ vào gần 400 website. Các hacker có thể đánh cắp cơ sở dữ liệu, bao gồm thông tin cá nhân của người dùng, và có thể phát tán các nội dung độc hại hoặc mã độc[30]. Chẳng hạn như: đầu năm 2018, máy chủ thư điện tử của Tập đoàn Dầu khí quốc gia Việt Nam tồn tại lỗ hổng bảo mật nghiêm trọng, bị cài cắm loại mã độc tin tặc nước ngoài thường hay sử dụng để duy trì kiểm

[30] Xem: Nguyễn Thị Trường Giang, *An ninh mạng ở Việt Nam hiện nay, những vấn đề lý luận và thực tiễn",* Nxb Đại học Quốc gia Hà Nội

soát, điều khiển máy chủ từ xa, chiếm đoạt thông tin, tài liệu. Ngày 22/01/2018, hệ thống giao dịch tại Sở Giao dịch chứng khoán Thành phố Hồ Chí Minh gặp sự cố không thể thực hiện khớp lệnh trong đợt giao dịch định kỳ xác định giá đóng cửa. Ngày 28/01/2018, hệ thống check-in của Hãng hàng không Vietjet Air bị tấn công khiến nhiều chuyến bay phải tạm hoãn.

Gần đây, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) cho biết tính từ đầu năm 2023 đến nay, đã có hơn 13.750 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam gây ra sự cố nghiêm trọng. Riêng trong quý I-2024, các cơ quan chức năng đã phát hiện 32.265 nguy cơ tấn công mạng nhằm vào các mạng công nghệ thông tin trọng yếu của các cơ quan Đảng, Chính phủ và các doanh nghiệp nhà nước, tăng 18,7% so với cùng kỳ năm 2023. Trong quý I/2025, đã ghi nhận và xử lý hơn 3.400 cuộc tấn công mạng, giảm 6,3% so với cùng kỳ năm trước; riêng trong tháng 3, số vụ tấn công giảm mạnh, xuống còn 525 vụ, giảm 68,9% so với tháng 2 và 49,3% so với tháng 3/2024.

Tấn công mạng không chỉ đe dọa an ninh thông tin mà còn tiềm ẩn nguy cơ lớn đối với các hệ thống quan trọng quốc gia. Các thế lực thù địch và phản động cũng gia tăng các hoạt động tình báo, gián điệp và khủng bố nhằm phá hoại hệ thống thông tin, phát tán thông tin sai lệch, độc hại để tác động đến chính trị nội bộ và can thiệp vào các chính sách, pháp luật của Việt Nam. Trong suốt giai đoạn từ 2015 đến 2023, đã có hơn 63.000 lượt cổng thông tin điện tử có tên miền ".vn" bị tấn công, trong đó có hơn 2.300 lượt tấn công vào các trang web của các cơ quan Đảng, Nhà nước, gây ra hậu quả nghiêm trọng. Các mối đe dọa an ninh phi truyền thống trên môi trường mạng đang ngày càng gia tăng, khi tin tặc có thể truy cập vào mọi cơ sở dữ liệu, đánh cắp thông tin quan trọng, cài phần mềm độc hại hoặc xóa thông tin cần thiết.

Mặc dù số lượng các cuộc tấn công mạng đã giảm nhờ các chiến dịch ngăn chặn mã độc và việc cung cấp thông tin cảnh báo kịp thời, nhưng nguy cơ về đánh cắp dữ liệu và tấn công nhằm vào cơ sở dữ liệu để thực hiện các hành vi lừa đảo hoặc đòi tiền chuộc vẫn là những mối nguy lớn. Do đó, các cơ quan và tổ chức cần rà soát và kiểm tra hệ thống website, cổng thông tin của mình, thu thập đầy đủ nhật ký hoạt động, và đầu tư vào lực lượng chuyên trách hoặc dịch vụ bảo mật mạng để đảm bảo ATTT.

c. Hoạt động gián điệp mạng

Theo các báo cáo thống kê, Việt Nam hiện vẫn là một trong những quốc gia chịu tác động mạnh mẽ từ mã độc. Việt Nam dẫn đầu thế giới về tỷ lệ lây nhiễm mã độc qua thiết bị lưu trữ ngoài như USB, thẻ nhớ, ổ cứng di động, với tỷ lệ lên tới 70,83% các máy tính bị lây nhiễm. Đồng thời, hơn 39,95% người dùng đối mặt với mã độc từ không gian mạng. Tình hình gián điệp mạng và các vụ rò rỉ bí mật nhà nước trên không gian mạng đang ngày càng phức tạp. Năm 2019, hàng trăm trang web với tên miền quốc gia đã bị tấn công, trong đó có 127 trang web và 349 cổng thông tin điện tử của nhiều cơ quan, đơn vị có lỗ hổng bảo mật nghiêm trọng. Đặc biệt, đã có 40 vụ lộ bí mật nhà nước qua Internet, với 241 tài liệu quan trọng bị rò rỉ[31]. Một điểm đáng chú ý là tin tặc đã gia tăng các cuộc tấn công vào các cơ sở trọng yếu và các tập đoàn kinh tế lớn nhằm thu thập và chiếm đoạt thông tin mật. Các đối tượng này không ngừng duy trì các chiến dịch tấn công, áp dụng các kỹ thuật mới và liên tục nâng cấp mã độc để đối phó với các biện pháp phòng ngừa, đồng thời bám sát tình hình chính trị, xã hội trong nước để thay đổi thủ đoạn phát tán mã độc, với mục tiêu xâm nhập thành công. Đặc biệt, trong giai đoạn dịch bệnh COVID-19, tin tặc đã lợi dụng tình hình để phát tán mã độc qua các thư điện tử giả mạo Chỉ thị của Thủ tướng Chính phủ về phòng chống dịch bệnh, dụ dỗ người dùng nhấn vào các tệp đính kèm, qua đó xâm nhập vào hệ thống máy tính và đánh cắp dữ liệu, đặc biệt là các thông tin liên quan đến Chính phủ và các bộ, ngành.

Từ góc độ ANQG, KGM đã làm thay đổi hoàn toàn phương thức hoạt động của tình báo và gián điệp quốc tế. Gián điệp mạng đang nổi lên như một mối đe dọa mới, khi các cơ quan tình báo nước ngoài có thể tuyển mộ đối tượng qua không gian mạng, bao gồm cả một số thành viên trong lực lượng vũ trang Việt Nam. Cụ thể, gần đây, đã xuất hiện các hoạt động móc nối và chỉ đạo qua mạng để thực hiện các nhiệm vụ phá hoại, như vụ việc tổ chức Pháp Luân Công có ý đồ phá hoại tượng đài Lênin tại Hà Nội, hay đối tượng Đinh Nguyên Kha nhận chỉ đạo từ tổ chức phản động "Việt Nam Quốc Dân Đảng" để thực hiện hành động khủng bố tại tượng đài Chủ tịch Hồ Chí Minh.

[31] Xem: Nguyễn Thị Trường Giang, *An ninh mạng ở Việt Nam hiện nay, những vấn đề lý luận và thực tiễn",* Nxb Đại học Quốc gia Hà Nội 2022

Một thực tế đáng lo ngại là Việt Nam hiện đang phụ thuộc nhiều vào hạ tầng và dịch vụ mạng do các quốc gia khác cung cấp, điều này tiềm ẩn nguy cơ bị giám sát và kiểm soát từ bên ngoài. Phần lớn hạ tầng công nghệ, từ các thiết bị cá nhân đến các hạ tầng lõi của mạng viễn thông, đều nhập khẩu từ nước ngoài, chủ yếu là từ Trung Quốc và Mỹ. Các hệ thống viễn thông và thiết bị mạng của các nhà cung cấp dịch vụ trong nước cũng phần lớn được sản xuất bởi các hãng của Trung Quốc. Đặc biệt, các hệ thống điều khiển tự động trong các ngành như năng lượng, luyện kim và hóa chất cũng có xuất xứ từ Trung Quốc, thông qua các hợp đồng tổng thầu EPC. Những thiết bị này tiềm ẩn nguy cơ bị lén cài sẵn chương trình kiểm soát, tạo ra các lỗ hổng bảo mật và phát tán mã độc, ảnh hưởng nghiêm trọng đến ANQG.

d. Hoạt động khủng bố mạng

Hiện nay, với sự phát triển mạnh mẽ của khoa học - công nghệ và những tiến bộ của Cách mạng Công nghiệp 4.0, các tổ chức khủng bố đã và đang tận dụng triệt để các tiện ích của Internet và mạng xã hội để tuyên truyền, kích động, hướng dẫn và kêu gọi các cuộc tấn công khủng bố dưới nhiều hình thức khác nhau. Tội phạm khủng bố qua mạng thường sử dụng Internet như một công cụ để khởi động các cuộc tấn công, xâm nhập vào hệ thống an ninh hoặc phát tán mã độc. Internet trở thành một phương tiện mạnh mẽ cho những kẻ khủng bố khi chúng có thể kết nối, chia sẻ thông tin, phối hợp tấn công, tuyên truyền, gây quỹ và tuyển dụng qua các nền tảng trực tuyến.

Khủng bố mạng là một trong những mối đe dọa của an ninh phi truyền thống, thuộc những vấn đề phức tạp mang tính toàn cầu mà không một quốc gia nào có thể giải quyết đơn độc. Vì vậy, việc đối phó đòi hỏi sự hợp tác chặt chẽ và trách nhiệm từ các quốc gia trên toàn thế giới. Hơn nữa, an ninh phi truyền thống có tính chất "động", có thể tiếp tục phát triển với nhiều đặc trưng mới. Công nghệ kỹ thuật số đang làm gia tăng những căng thẳng về pháp lý, nhân đạo và chuẩn mực đạo đức, đồng thời làm giảm bớt các rào cản đối với quyền truy cập, mở ra những tiềm năng mới cho các xung đột và tấn công cả trong và ngoài khu vực nhà nước. Khủng bố mạng đang trở thành một thách thức toàn cầu khi không gian mạng trở thành môi trường lý tưởng cho các tổ chức khủng bố quốc tế tuyên truyền, tuyển dụng, huấn luyện và chỉ đạo các hoạt động khủng bố.

Trong thời gian qua, một số tổ chức phản động, cực đoan và tội phạm có tổ chức đã lợi dụng thành tựu khoa học - công nghệ để tấn công cá nhân, quốc gia trên "vùng lãnh thổ mới" này. Chúng đã lợi dụng không gian mạng để chuyển hóa chế độ chính trị, kích động biểu tình, phá hoại an ninh, thực hiện cách mạng màu, cách mạng đường phố, bạo loạn và lật đổ chính quyền.

Việt Nam đã và đang phải đối mặt với hàng loạt âm mưu, hoạt động khủng bố từ các tổ chức người Việt, như "Việt Tân", "Chính phủ quốc gia Việt Nam lâm thời", "Triều đại Việt"… Những tổ chức này đã lợi dụng các khu vực ở nước ngoài như Philippines, Thái Lan, Malaysia để xâm nhập và thực hiện các hoạt động tại Việt Nam. Chúng sử dụng Internet, mạng xã hội và các blog cá nhân để tuyên truyền, xúi giục và hướng dẫn các phần tử xấu trong nước chế tạo bom và tiến hành các cuộc tấn công khủng bố. Trong thời gian gần đây, nhiều trang web của các bộ, ngành đã bị tấn công, tình hình an ninh mạng đang trở nên phức tạp hơn. Số lượng các vụ tấn công mạng và xâm nhập vào các hệ thống công nghệ thông tin nhằm mục đích do thám, trục lợi, phá hoại dữ liệu, ăn cắp tài sản, cạnh tranh không lành mạnh và các vụ mất an toàn thông tin khác đang gia tăng đáng kể, ngày càng tinh vi và phức tạp. Các loại virus, mã độc và vũ khí mạng xuất hiện nhiều hơn, một số loại được thiết kế chuyên biệt và vô cùng nguy hiểm. Trong khi đó, hệ thống mạng thông tin quốc gia vẫn còn nhiều lỗ hổng bảo mật nghiêm trọng, chưa được kiểm tra và đánh giá thường xuyên.

Các tổ chức khủng bố đã lợi dụng mạng xã hội và Internet để tuyên truyền tư tưởng cực đoan, phát hành tạp chí khủng bố trực tuyến nhằm thu hút các phần tử mới tham gia; tổ chức các khóa huấn luyện từ xa, dạy cách thực hiện tấn công hoặc lựa chọn các mục tiêu qua mạng. Mạng Internet, với tính chất dễ khai thác, chi phí thấp và khả năng lan tỏa rộng, trở thành công cụ lý tưởng cho việc phát tán khủng bố trên toàn cầu. Điển hình như năm 2022, tổ chức phản động Ủy ban cứu người vượt biển (BPSOS) đã tổ chức Diễn đàn trực tuyến với chủ đề "Hội luận về Thiên Chúa giáo ở vùng Tây Nguyên-thách đố và triển vọng" nhằm xuyên tạc tình hình tự do tôn giáo ở Việt Nam, kích động hận thù, vận động người dân trong nước tham gia diễn đàn, kêu gọi quốc tế gây sức ép yêu cầu Nhà nước Việt Nam "cải thiện tự do tôn giáo, tín ngưỡng".

Việc kiểm soát không gian mạng để chống khủng bố trở nên phức tạp bởi những kẻ khủng bố có thể truyền tải tư tưởng cực đoan từ xa mà không cần trung

tâm chỉ huy, xúi giục những cá nhân mới tiến hành khủng bố mà không cần xuất hiện trực tiếp. Đây là một hình thức tổ chức khủng bố phi truyền thống. Các hoạt động khủng bố như vậy dẫn đến sự xuất hiện của những "con sói đơn độc", gây ra những thách thức rất lớn đối với các cơ quan tình báo. Các tổ chức khủng bố tiếp tục lợi dụng Internet, mạng xã hội và blog cá nhân để tuyên truyền, xúi giục và hướng dẫn các phần tử xấu chế tạo bom. Tuy nhiên, cho đến nay, Việt Nam vẫn chưa ghi nhận vụ tấn công khủng bố nào do cá nhân hay tổ chức khủng bố nước ngoài thực hiện. Mặc dù vậy, các nguy cơ khủng bố từ bên ngoài đối với an ninh quốc gia Việt Nam vẫn hiện hữu và tiềm ẩn, cụ thể: (1) Việt Nam có những mục tiêu khủng bố có thể bị nhắm đến, như các trụ sở ngoại giao nước ngoài; (2) Nguy cơ từ dòng phiến quân IS chuyển hướng về Đông Nam Á từ Trung Đông; (3) Việt Nam là quốc gia có lượng người dùng Internet lớn, vì vậy khả năng bị ảnh hưởng là cao; (4) Các tổ chức phản động lưu vong và các phần tử cực đoan lợi dụng các vấn đề dân tộc, tôn giáo để thực hiện các hành động khủng bố.

đ. Tội phạm xâm phạm an ninh mạng

Việt Nam đang chứng kiến sự gia tăng mạnh mẽ của người dùng Internet và các mạng xã hội phổ biến như Facebook, YouTube, TikTok, Zalo, Instagram, Mocha, Lotus… Việt Nam hiện là một trong số ít những quốc gia trên thế giới có tốc độ phát triển và sử dụng các ứng dụng mạng internet rất cao. Số liệu thống kê cho thấy, tại Diễn đàn Internet Việt Nam 2017, Việt Nam đã đạt con số khoảng 50 triệu người sử dụng internet chỉ trong 20 năm phát triển, đứng thứ 20 trên thế giới về các quốc gia có số người sử dụng internet nhiều nhất. Năm 2019, số lượng người sử dụng internet của Việt Nam đã đạt hơn 64 triệu người, chiếm hơn 2/3 dân số (66%), tăng hơn 19% so với năm 2018, xếp thứ 13 trên thế giới về số người dùng, trong đó có 58 triệu tài khoản Facebook, 62 triệu tài khoản Google. Điều này cũng đồng nghĩa với việc nguy cơ đối mặt với các mối đe dọa an ninh quốc gia và trật tự an toàn xã hội trên không gian mạng ngày càng trở nên phức tạp. Các cuộc tấn công mạng lớn vào hạ tầng công nghệ thông tin trọng yếu, tấn công khủng bố mạng, kêu gọi tài trợ khủng bố, gián điệp mạng, tội phạm mạng và phát tán tin giả đang gây ra những hậu quả nghiêm trọng và khó lường.

Theo thống kê của Bộ Công an, trong 5 năm kể từ khi Luật An ninh mạng có hiệu lực, đã phát hiện, đấu tranh và xử lý hơn 2.300 chuyên án, khởi tố hơn 1.100 vụ, với hơn 1.000 đối tượng bị bắt giữ và 51 vụ bị xử phạt hành chính liên

quan đến tội phạm lừa đảo chiếm đoạt tài sản qua không gian mạng. Theo thông tin trên cổng Cảnh báo an toàn thông tin Việt Nam (NCSC) thuộc Bộ Thông tin và Truyền thông đã thống kê năm 2023 ghi nhận khoảng 16.000 phản ánh lừa đảo trực tuyến hướng đến người dùng Internet Việt Nam, gây thiệt hại hơn 390.000 tỷ đồng, tương đương 3,6% GDP; tăng 64,78% so với năm 2022. Bộ Công an đã khởi tố nhiều vụ án vì tội lừa đảo trên không gian mạng và xác định tổng số tiền người dân bị chiếm đoạt khoảng 8.000 – 10.000 tỷ đồng. Năm 2024, Cục An ninh mạng và phòng, chống tội phạm mạng sử dụng công nghệ cao (A05) đã phát hiện, tiếp nhận hơn 3.500 vụ việc, tổng số tiền thiệt hại từ 3.500 vụ việc là khoảng hơn 2.487 tỷ đồng.

Kết quả từ chương trình đánh giá an ninh mạng dành cho người sử dụng cá nhân do Tập đoàn công nghệ Bkav công bố ngày 18/1/2025 cho thấy, thiệt hại do tội phạm mạng, sử dụng các virus máy tính gây ra đối với người dùng Việt Nam ở mức 17.300 tỷ đồng, tiếp tục giảm so với các năm trước. Năm 2024, hệ thống giám sát và cảnh báo virus của Bkav ghi nhận có tới 745.000 máy tính bị nhiễm virus đánh cắp tài khoản (Facebook, ngân hàng), tăng 40% so với năm 2023.

Theo Bộ Thông tin truyền thông, trong 4 tháng đầu năm 2020, tổng cộng có 1.056 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam, bao gồm 553 cuộc tấn công Phishing, 280 cuộc Deface và 223 cuộc Malware, giảm khoảng 51,4% so với cùng kỳ năm 2019. Tuy nhiên, tình hình bảo mật của các thiết bị IoT (Internet of Things) còn nhiều lỗ hổng. Hơn 73.000 camera IP trên toàn cầu, trong đó có gần 1.000 camera tại Việt Nam, đã bị tấn công. Điều này phần lớn là do người dùng chưa có thói quen bảo mật các thiết bị này và không thay đổi mật khẩu mặc định trước khi kết nối Internet. Năm 2021, các hệ thống thông tin tại Việt Nam tiếp tục phải đối mặt với hơn 11.100 sự cố tấn công mạng. Riêng trong năm tháng đầu năm 2022, Bộ Thông tin và Truyền thông đã ghi nhận 5.463 vụ tấn công mạng gây sự cố. Cũng trong năm này, Cục An toàn thông tin đã cảnh báo và hướng dẫn xử lý 11.213 cuộc tấn công mạng, trong đó có 3.930 cuộc tấn công Phishing, 1.524 cuộc Deface và 5.759 cuộc Malware.

Sáu tháng đầu năm 2024, Công ty Công nghệ An ninh Mạng Quốc gia Việt Nam ghi nhận 5.100 vụ tấn công mạng vào các hệ thống thông tin tại Việt Nam, giảm 12% so với năm 2023. Tuy nhiên, các cuộc tấn công có chủ đích (APT) vào các cơ sở trọng yếu lại tăng 9% so với cùng kỳ năm trước. Dự báo trong những

năm tới, các cuộc tấn công APT sẽ tiếp tục gia tăng, đặc biệt là các cuộc tấn công đánh cắp dữ liệu từ các kho dữ liệu hình thành trong quá trình chuyển đổi số. Những cuộc tấn công này chủ yếu xảy ra qua ba hình thức: (1) Tấn công người dùng qua e-mail giả mạo, (2) Tấn công phần mềm trên máy chủ, đặc biệt là các hệ thống Microsoft như Exchange, SharePoint, và (3) Tấn công lỗ hổng website, đặc biệt là SQL Injection và dò mật khẩu quản trị website.

Năm 2024 - 2025 chứng kiến sự bùng phát của các vụ lừa đảo trực tuyến. Mặc dù nhiều cảnh báo đã được đưa ra, nhưng số nạn nhân của các vụ lừa đảo vẫn không ngừng tăng, với thiệt hại lên đến hàng chục tỷ đồng trong một số trường hợp. Các hình thức lừa đảo ngày càng tinh vi và khó lường hơn. Chỉ trong hơn 3 tháng đầu năm 2025, số vụ lừa đảo đã tăng 64,78% so với cùng kỳ năm 2024 và 37,82% so với nửa cuối năm 2024. Đáng chú ý, các nhóm đối tượng bị lừa đảo có sự chuyển dịch mạnh mẽ sang những người cao tuổi, trẻ em, sinh viên và những người có thu nhập thấp. Nguyên nhân chính của sự gia tăng này là do các lỗ hổng bảo mật ngày càng tăng theo từng năm, tạo cơ hội cho tội phạm mạng lợi dụng.
Riêng đối với tội phạm công nghệ cao, thống kê của các cơ quan chức năng cho thấy, tội phạm công nghệ cao hiện nay đứng thứ hai trong danh sách các loại tội phạm nguy hiểm nhất, chỉ sau tội phạm khủng bố[32]. Việt Nam đang nằm trong top 7 quốc gia bị đe dọa bởi các cuộc tấn công mạng. Các vụ án liên quan đến tội phạm sử dụng công nghệ cao ngày càng gia tăng, với các phương thức tấn công tinh vi và có sự phối hợp giữa các tội phạm trong và ngoài nước. Các kỹ thuật tấn công như Phishing (lừa đảo), Deface (xâm nhập), Malware (phần mềm độc hại) được sử dụng để tấn công vào hệ thống của người sử dụng. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao cho biết, trong 6 tháng đầu năm 2024, Bộ Công an đã phát hiện và xử lý 840 chuyên án, vụ việc liên quan đến lừa đảo, chiếm đoạt tài sản qua mạng, tăng 42% so với cùng kỳ năm 2023. Các nhóm hacker sử dụng nhiều công cụ đặc thù để phát tán tin nhắn giả, lừa đảo người dùng, cũng như tấn công vào các hệ thống hạ tầng số trong các lĩnh vực như ngân hàng, tài chính, giáo dục và giao thông vận tải.

Thống kê của Bộ Lao động, Thương binh và Xã hội trong 06 tháng đầu năm 2024, phát hiện 682 vụ xâm hại 735 em, trong đó xâm hại tình dục 572 vụ với 562

[32] Xem: Nguyễn Thị Trường Giang, *An ninh mạng ở Việt Nam hiện nay, những vấn đề lý luận và thực tiễn",* Nxb Đại học Quốc gia Hà Nội

em bị xâm hại. Tội phạm xâm hại tình dục trẻ em qua mạng internet có chiều hướng gia tăng với diễn biến phức tạp, khó lường. Theo công bố Kết quả khảo sát ý kiến của tổ chức UNICEF ngày 6/9/2019, kết quả 21% thanh thiếu niên Việt Nam tham gia khảo sát cho biết các em là nạn nhân của bắt nạt trên mạng và hầu hết (75%) không biết về đường dây nóng hoặc các dịch vụ có thể giúp các em nếu bị bắt nạt hoặc bị bạo lực trên mạng[33].

Tội phạm công nghệ cao không chỉ xảy ra ở các thành phố lớn mà còn lan rộng đến các khu vực nông thôn, với các hình thức và thủ đoạn ngày càng tinh vi hơn, gây ra hậu quả nghiêm trọng đối với tài sản của các tổ chức và cá nhân. Đặc biệt, nhiều đối tượng phạm tội còn trẻ và có đam mê về công nghệ thông tin, chúng tổ chức các nhóm tội phạm qua mạng để chia sẻ công cụ và cách thức, thủ đoạn thực hiện hành vi phạm tội, chia sẻ cách qua mặt cơ quan chức năng.

Các hình thức lừa đảo trên KGM sử dụng công nghệ cao ngày càng trở nên tinh vi, như giả mạo các cơ quan điều tra (công an, viện kiểm sát, tòa án) thông báo các vụ án, yêu cầu nạn nhân chuyển tiền hoặc cung cấp thông tin ngân hàng. Các đối tượng cũng có thể giả danh cán bộ ngân hàng, cơ quan nhà nước để chiếm đoạt tài khoản ngân hàng hoặc thông qua các sàn giao dịch điện tử giả mạo để lừa đảo người tham gia đầu tư.

Các phương thức lừa đảo phổ biến gồm việc kết bạn qua mạng xã hội như Zalo, Facebook, Telegram, Tinder... dụ dỗ nạn nhân đầu tư vào các sàn giao dịch điện tử có vẻ hợp pháp nhưng thực chất là lừa đảo. Sau một thời gian, sàn giao dịch sẽ thông báo dừng hoạt động hoặc lỗi hệ thống khiến người chơi không thể rút tiền hoặc bị mất hết tiền trong tài khoản. Các đối tượng còn lợi dụng công nghệ để giả mạo số điện thoại hoặc sử dụng các phần mềm giả mạo đầu số để tạo ra các cuộc gọi, đe dọa nạn nhân liên quan đến các vụ án hoặc yêu cầu cung cấp thông tin cá nhân. Một phương thức khác là chiếm quyền điều khiển tài khoản mạng xã hội của nạn nhân để mượn tiền từ bạn bè hoặc người thân. Ngoài ra, một số đối tượng còn lợi dụng hệ quả kéo dài của dịch bệnh COVID-19 và sự dịch chuyển nhiều hoạt động lên KGM lừa đảo bằng hình thức tuyển dụng nhân viên làm việc online, yêu cầu chuyển tiền trước và lừa đảo qua các tài khoản ngân hàng. Các đối tượng này lợi dụng sự thiếu cảnh giác của nạn nhân và tạo ra lòng tin để thực

[33] Dorothea Czarnecki (2016), *Báo cáo đánh giá năng lực bảo vệ trẻ em trên môi trường mạng tại Việt Nam*, Bộ Lao động, Thương binh và Xã hội, UNICEF, Hà Nội.

hiện hành vi phạm tội. Theo thống kê, trên cổng cảnh báo an toàn thông tin của Bộ Thông tin truyền thông ghi nhận, gần 16.000 phản ánh lừa đảo trực tuyến, gây thiệt hại hơn 390 nghìn tỷ đồng, tương đương 3,6% GDP; trong đó 91% liên quan lĩnh vực tài chính, tăng 64,78% so với năm 2022, tỷ lệ người dùng nhận tin nhắn, cuộc gọi lừa đảo trực tuyến là 73%[34].

Điểm chung của các vụ lừa đảo trên KGM này là tội phạm sử dụng công nghệ cao thu thập và kiểm soát thông tin cá nhân của nạn nhân, từ đó thực hiện các hành vi lừa đảo, đe dọa qua mạng xã hội. Việc điều tra và xử lý các vụ án lừa đảo qua mạng gặp nhiều khó khăn vì các đối tượng sử dụng các phương thức rất tinh vi và có thể giả mạo nhiều vỏ bọc khác nhau để lừa đảo nạn nhân. Ngoài ra, hoạt động lừa đảo chiếm đoạt tài sản trên KGM xảy ra ở nhiều lĩnh vực, số lượng nạn nhân lớn, không tập trung, hầu hết rất khó thu thập chứng cứ…

2. Thực trạng áp dụng pháp luật về an ninh mạng ở Việt Nam

a. Thực trạng áp dụng pháp luật hành chính

Nghiên cứu thực tiễn việc tổ chức thực hiện và áp dụng pháp luật ANM của các cơ quan có thẩm quyền thời gian quan cho thấy, các chủ thể có thẩm quyền như: Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và truyền thông (Bộ TTTT) hay UBND cấp tỉnh… đã rất chủ động trong các hoạt động như: thẩm định ANM; đánh giá điều kiện ANM; kiểm tra ANM; giám sát ANM; ứng phó, khắc phục sự cố ANM; bảo vệ ATTT mạng; phòng, chống vi phạm pháp luật về ANM. Để bảo vệ thông tin mạng, các cơ quan, tổ chức, cá nhân tăng cường sử dụng các biện pháp kỹ thuật theo dõi, giám sát ANM như sử dụng hệ thống tường lửa, kiểm soát truy nhập, kiểm soát lưu lượng mạng. Trong quá trình thực thi trách nhiệm, các chủ thể này đã xác định các mối đe dọa gây sự cố ảnh hưởng đến ANM để ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật; yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên KGM xâm phạm ANQG, TTATXH, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Bộ Công an đã chủ động phối hợp với Bộ Quốc phòng, Bộ Thông tin và Truyền thông trong phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại hoạt

[34] Xem: Hiệp hội An ninh mạng quốc gia, *Tài liệu Hội thảo chủ đề: "Phòng, chống lừa đảo trên không gian mạng"*, ngày 13/5/2024, Hà Nội.

động sử dụng KGM tuyên truyền phá hoại tư tưởng, kích động biểu tình, âm mưu lật đổ chính quyền nhân dân của các thế lực thù địch, phản động, chống đối. Bộ Tư lệnh tác chiến KGM trực thuộc Bộ Quốc phòng (Bộ Tư lệnh 86) đã phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông triển khai thực hiện nhiều biện pháp quản lý nhà nước bảo vệ an toàn, an ninh các hệ thống thông tin quan trọng quốc gia; phối hợp với các đơn vị chức năng thuộc Bộ Quốc phòng, Bộ Công an trong đấu tranh phòng chống tội phạm mạng; nghiên cứu hoàn thiện Công ước Liên Hợp Quốc về đấu tranh với tội phạm mạng.

Để đảm bảo ATTT cho KGM Việt Nam, Bộ Thông tin và Truyền thông chủ động thực hiện những hoạt động tích cực mà pháp luật về ANM quy định như phối hợp với Bộ Công an, Bộ Quốc phòng, các bộ và cơ quan ngang bộ trong điều phối ứng cứu các sự cố mạng, tấn công mạng; chủ động rà quét KGM, giám sát, phát hiện, cảnh báo về sự cố, lỗ hổng, mã độc, botnet, APT và các tấn công mạng khác; kiểm tra, rà quét lỗ hổng, mã độc và đánh giá mức độ ATTT cho các hệ thống thông tin; phân tích, điều tra mã độc và hướng dẫn phòng chống, xử lý; tổ chức đào tạo, huấn luyện, diễn tập về ATTT mạng. Ngoài ra, Bộ còn tư vấn tổ chức hoạt động các đội ứng cứu sự cố mạng, tư vấn về giải pháp, chiến lược, kế hoạch, dự án bảo đảm ATTT mạng; hỗ trợ ngăn chặn, hạn chế thư rác, tin nhắn rác; cung cấp các dịch vụ về ATTT mạng.

Bộ Thông tin và Truyền thông đẩy mạnh công tác đánh giá, thống kê đồng thời đẩy mạnh tuyên truyền, cảnh báo để người dùng nhận biết, phòng tránh khi tham gia hoạt động trên KGM bằng việc phát hành cuốn "Cẩm nang bảo đảm an toàn thông tin trong đại dịch Covid-19" hướng dẫn người dùng mạng các kỹ năng an toàn về làm việc từ xa, học trực tuyến, giải trí khi kết nối trực tuyến và Bộ Quy tắc ứng xử trên mạng xã hội năm 2021 áp dụng cho cơ quan nhà nước, cán bộ, viên chức, người lao động trong các cơ quan nhà nước sử dụng mạng xã hội; tổ chức, cá nhân khác sử dụng mạng xã hội; nhà cung cấp dịch vụ mạng xã hội tại Việt Nam. Xây dựng được mạng lưới giám sát ATTT mạng. Trong đó, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) triển khai khoảng 30 điểm giám sát tập trung để giám sát các hệ thống, dịch vụ công nghệ thông tin như cổng thông tin điện tử, hệ thống thư điện tử, hệ thống mạng người dùng,... hỗ trợ đảm bảo ATTT cho Văn phòng Chính phủ, Báo điện tử Đảng Cộng sản, Trung tâm dữ liệu của Hà Nội, Vĩnh Phúc,... VNCERT hiện là mắt xích quan trọng trong mạng lưới

ứng cứu sự cố toàn cầu, có kết nối với tất cả các tổ chức an toàn mạng khu vực, hỗ trợ nhiều nước như Hoa Kỳ, Nhật Bản,... ngăn chặn các cuộc tấn công mạng có nguồn gốc xuất phát từ Việt Nam.

Các chủ thể là các cơ quan có thẩm quyền tổ chức thi hành pháp luật, ADPL về ANM đã ban hành nhiều văn bản hướng dẫn thi hành pháp luật về ANM như: Năm 2016, Chính phủ đã ban hành Nghị định 108/2016/NĐ-CP quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng. Năm 2020, Chính phủ ban hành Nghị định 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử. Năm 2022, Chính phủ ban hành Nghị định 52/2022/NĐCP, ngày 15/8/2022, quy định chi tiết một số điều của Luật An ninh mạng.

Trên cơ sở xác định thi hành Luật An ninh mạng năm 2018 là một trong những nhiệm vụ tiên quyết, ngày 01/02/2019, Thủ tướng Chính phủ đã ban hành Quyết định số 12/QĐ-TTg ban hành Kế hoạch triển khai thi hành Luật An ninh mạng, tổ chức các Hội nghị quán triệt, phổ biến tới các bộ, ngành chức năng, UBND tỉnh, thành phố trực thuộc Trung ương, các đối tượng tác động của Luật An ninh mạng để người dân nhận thức và thực hiện nghiêm túc.

Bộ Thông tin và Truyền thông đã ban hành Thông tư 03/2017/TT-BTTTT quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Thông tư 12/2019/TT-BTTTT sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước. Bộ Công an ban hành Thông tư 38/2020/TT-BCA ngày 17/4/2020 quy định về công tác bảo vệ bí mật nhà nước, trong đó quy định máy tính dùng để đăng ký tài liệu, vật chứa bí mật nhà nước không được nối mạng internet. Bộ Công an đã và đang chủ trì nghiên cứu, dự thảo một số văn bản hướng dẫn thi hành văn bản quy phạm pháp luật về ANM như Nghị định quy định xử phạt vi phạm hành chính trong lĩnh vực ANM...

Bộ Công an cũng đã phối hợp với Bộ Thông tin và Truyền thông cùng các cơ quan chức năng khác để tham mưu cho Quốc hội xây dựng và hoàn thiện các văn bản pháp lý nhằm tăng cường công tác quản lý và phòng chống vi phạm hành

chính trong lĩnh vực an ninh mạng. Bộ Công an đề nghị Chính phủ rà soát, sửa đổi các quy định không còn phù hợp với thực tiễn và bổ sung các quy định mới để khắc phục sơ hở, đáp ứng yêu cầu bảo đảm an ninh trật tự trên không gian mạng. Đồng thời, Bộ cũng yêu cầu tăng cường công tác kiểm tra, giám sát và phát hiện vi phạm, cải thiện việc tổ chức triển khai thực hiện Luật An ninh mạng 2018, nhằm nâng cao hiệu quả công tác bảo vệ an ninh mạng trong tương lai.

Trong lĩnh vực an ninh mạng, bất kỳ một sự cố nào không được xử lý ngay đều có thể trở thành một vấn đề lớn và có thể dẫn tới sự phá hủy dữ liệu hoặc làm sụp đổ hệ thống. VNCERT được thành lập từ năm 2005 và đến năm 2019, được tổ chức lại thành Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC). Trung tâm đã chủ động phối hợp với nhiều cơ quan chức năng triển khai các biện pháp theo dõi, phát hiện, phòng chống các cuộc tấn công vào hệ thống mạng, bóc gỡ mạng lưới máy tính ma ở Việt Nam. Năm 2013, cuộc tấn công từ chối dịch vụ vào một số báo điện tử cho thấy, do chưa nhận thức đầy đủ tầm quan trọng của VNCERT và không triển khai các biện pháp bảo vệ, một số tờ báo điện tử bị tấn công dai dẳng và gánh chịu thiệt hại nặng nề. Theo Bộ Thông tin và Truyền thông, năm 2023, Việt Nam thuộc nhóm các quốc gia được phát hiện là có nhiều tội phạm mạng nhất, chiếm tỷ lệ 5,16%, tăng 3,89% so với năm 2020. Lực lượng An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao trên toàn quốc đã phát hiện, tiếp nhận hơn 3.500 vụ việc, tổng số tiền thiệt hại hơn 2.487 tỷ đồng.

Chỉ trong 06 tháng đầu năm 2024, phát hiện 3.787 website của Việt Nam (.vn), trong đó có 112 website của các cơ quan giáo dục (.edu.vn), 26 website của cơ quan chính phủ (.gov.vn)… bị tin tặc tấn công, thay đổi giao diện, chỉnh sửa nội dung. Trong khi đó, 06 tháng cùng kỳ năm 2013, chỉ phát hiện 2.147 trang, cổng thông tin điện tử trong nước (có tên miền.vn), nhưng trong số đó có đến 80 trang thuộc quản lý của các cơ quan nhà nước bị tấn công, chiếm quyền điều khiển, thay đổi giao diện. Khủng bố mạng nổi lên như một thách thức đe dọa nghiêm trọng tới an ninh quốc gia. Đến nay, nhờ nỗ lực hợp tác của VNCERT/CC, các cuộc tấn công mạng theo ba loại hình này đã cơ bản được cảnh báo, ngăn chặn và xử lý. Thống kê của Trung tâm Xử lý tin giả Việt Nam (VAFC) thuộc Bộ Thông tin và Truyền thông, trong 6 tháng đầu năm 2024, Trung tâm nhận được

hơn 2,1 nghìn lượt báo cáo tin giả. Sau quá trình xác minh, Trung tâm đã công bố dán nhãn 384 tin giả, tin sai sự thật.

Đối với hoạt động xử lý vi phạm pháp luật trên KGM bằng các biện pháp chế tài hành chính, nghiên cứu Báo cáo công tác năm của các cơ quan có thẩm quyền xử lý (gồm cả xử phạt) vi phạm hành chính trong lĩnh vực KGM cho thấy: tình hình vi phạm an ninh mạng tại Việt Nam có sự gia tăng đáng kể cả về số lượng vụ việc lẫn số tiền phạt. Cụ thể, số trường hợp vi phạm tăng từ 905 vụ vào năm 2021 lên 2.318 vụ vào năm 2024, phản ánh sự gia tăng nhanh chóng trong các hành vi vi phạm an ninh mạng. Số tiền phạt cũng tăng theo, từ 153,37 tỷ đồng vào năm 2021 lên 322,82 tỷ đồng vào năm 2024, cho thấy mức độ xử lý nghiêm khắc hơn đối với các hành vi này. Tổng cộng trong giai đoạn này, đã có 6.157 vụ vi phạm và số tiền phạt lên tới 884,18 tỷ đồng. Những con số này không chỉ minh chứng cho sự gia tăng của các hành vi vi phạm mà còn phản ánh nỗ lực mạnh mẽ của các cơ quan chức năng trong việc xử lý và đảm bảo an ninh mạng[35].

Nhìn chung, hoạt động áp dụng pháp luật hành chính, nhất là công tác xử lý vi phạm hành chính trong lĩnh vực an toàn, ANM đã được triển khai đúng thẩm quyền, thủ tục pháp lý, đạt hiệu quả cao và công bằng, giúp ngăn chặn và xử lý kịp thời các hành vi vi phạm, đồng thời nâng cao ý thức chấp hành pháp luật của tổ chức và cá nhân. Tính đến nay, chưa có vụ kiện hành chính nào liên quan đến xử phạt trong lĩnh vực này.

b. Thực trạng áp dụng pháp luật hình sự

Là đơn vị chủ công trong phòng, chống tội phạm và vi phạm pháp luật trên KGM, Bộ Công an phối hợp với các bộ, ngành liên quan nhanh chóng xây dựng kế hoạch, biện pháp để triển khai thi hành pháp luật về ANM, nhiều dịch vụ trực tuyến như hải quan, thuế, đăng ký doanh nghiệp... có chuyển biến tích cực, hạn chế được trục trặc, cải thiện sự tương tác và ANM được bảo đảm. Đến quý I/2014, đã hình thành một hệ thống quản lý văn bản điện tử thống nhất, thông suốt từ trung ương đến địa phương, cho phép tự động nhận biết được trạng thái xử lý văn bản giữa các cơ quan. Với tư cách là đầu mối quản lý nhà nước về ANM, Bộ Công an đã chỉ đạo triển khai thực hiện nhiều biện pháp nhằm phát hiện, điều tra, đấu tranh, xử lý tội phạm mạng. Trên tinh thần kiên quyết giảm thiểu những nguy cơ,

[35] Xem: Báo cáo công tác năm (từ 2021 – 2024) của Cục An ninh mạng và phòng chống tội phạm công nghệ cao, Bộ Cộng an (A05).

thách thức, vi phạm pháp luật về ANM, bảo đảm hoạt động trên KGM không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân, trong những năm gần đây, Bộ Công an đã tăng cường các biện pháp đấu tranh làm rõ phương thức, thủ đoạn mới của tội phạm sử dụng công nghệ cao trong hoạt động thanh toán thẻ, thanh toán điện tử; triệt phá nhiều đường dây tội phạm cờ bạc, cá độ bóng đá qua mạng internet[36].

Trong khuôn khổ trách nhiệm bảo vệ an ninh mạng, Bộ Công an phối hợp chặt chẽ với các cơ quan chức năng khác, thực hiện giám sát, kiểm tra và xử lý vi phạm pháp luật về an ninh mạng, qua đó góp phần đảm bảo không gian mạng an toàn và lành mạnh. Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao (A05) đã tham mưu cho lãnh đạo Bộ Công an triển khai nhiều nhiệm vụ công tác nhằm huy động sức mạnh, hình thành thế trận toàn dân phòng chống tội phạm lừa đảo trên không gian mạng. Đáng chú ý, phối hợp với các doanh nghiệp viễn thông, internet trong nước, ngân hàng thương mại và các đơn vị cung cấp dịch vụ xuyên biên giới Google, Facebook... tiến hành rà soát, ngăn chặn hàng chục nghìn trang mạng, tài khoản mạng xã hội, tài khoản ngân hàng. Các biện pháp này được triển khai mạnh mẽ và có hiệu quả, thể hiện sự quyết tâm của Bộ trong việc ngăn chặn và xử lý các hành vi vi phạm trong lĩnh vực này.

Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao cũng đã phối hợp chặt chẽ với các đơn vị chức năng như Bộ Thông tin và Truyền thông, Ngân hàng Nhà nước Việt Nam… tham mưu triển khai các biện pháp rà soát, định danh xác thực thuê bao di động, tài khoản ngân hàng với cơ sở dữ liệu quốc gia về dân cư, nhằm hạn chế tình trạng sim rác, tài khoản ngân hàng rác, áp dụng phương thức xác thực sinh trắc học đối với những giao dịch, chuyển tiền ngân hàng… nhằm ngăn chặn, hạn chế giao dịch chuyển dòng tiền vi phạm pháp luật.

[36] Năm 2018, điều tra và đưa ra xét xử vụ đại án Nguyễn Thanh Hóa, nguyên Cục trưởng Cục Cảnh sát phòng chống tội phạm công nghệ cao, phạm tội Lợi dụng chức vụ, quyền hạn trong khi thi hành công vụ, tiếp tay cho hành vi tổ chức đánh bạc trực tuyến qua mạng internet, rửa tiền, chiếm đoạt tài sản do Phan Sào Nam cầm đầu với giá trị hàng nghìn tỷ đồng; Năm 2019, Cơ quan CSĐT BCA đã bắt giữ 10 đối tượng trong đường dây đánh bạc, tổ chức đánh bạc qua mạng internet với số tiền khoảng 500 tỷ đồng tại Hà Nội; vụ bắt 29 đối tượng đánh bạc qua internet với số tiền trên 1.000 tỷ đồng tại Hưng Yên; vụ bắt giữ 13 đối tượng đánh bạc qua internet với số tiền 12 tỷ đồng, xác định có khoảng 100 tài khoản ở 33 tỉnh, thành trong cả nước tham gia đánh bạc tại Nghệ An, tội phạm là người nước ngoài sử dụng công nghệ cao tại Việt Nam. Điều tra, bắt giữ nhiều đối tượng lập nhiều trang web, facebook, zalo ảo, lừa đảo hàng tỷ đồng. Phát hiện 352 vụ, 503 đối tượng phạm tội, vi phạm pháp luật trong lĩnh vực viễn thông, tin học (tăng17,73% số vụ so với cùng kỳ 2018). Đã khởi tố 164 vụ, 304 bị can (tăng 17,99% số vụ và tăng 6,29% bị can so với cùng kỳ năm 2018); . Tháng 02/2020, công an tỉnh Quảng Nam triệt phá thành công đường dây đánh bạc qua mạng internet với hình thức cá độ bóng đá và lô đề với số tiền hơn 40 tỷ đồng.

Theo thống kê của Bộ Công an, trong giai đoạn từ năm 2021 đến 2024, số vụ vi phạm trong lĩnh vực tội phạm công nghệ cao tại Việt Nam đã tăng mạnh. Cụ thể, năm 2021, lực lượng chức năng phát hiện 1.257 vụ vi phạm, với 1.405 đối tượng tham gia, trong đó 262 vụ được khởi tố và 392 bị can bị truy tố. Sang năm 2022, số vụ vi phạm tiếp tục gia tăng lên 1.327 vụ với 1.575 đối tượng, trong đó có 382 vụ được khởi tố và 429 bị can bị truy tố. Đặc biệt, năm 2023, các đơn vị đã đấu tranh, khởi tố hơn 1.500 vụ án, với hơn 500 bị can, góp phần bảo đảm trật tự, an toàn xã hội, răn đe, trấn áp các loại tội phạm lừa đảo trên không gian mạng. Bộ Công an đã và đang triển khai hiệu quả các biện pháp quyết liệt để đấu tranh với tội phạm sử dụng công nghệ cao trong các hoạt động thanh toán điện tử, đồng thời triệt phá nhiều đường dây tội phạm cờ bạc qua mạng. Một số vụ đáng chú ý bao gồm vụ triệt phá đường dây đánh bạc tại Thừa Thiên Huế, Phú Yên, với số tiền giao dịch lên đến hàng trăm tỷ đồng, vụ triệt phá đường dây cá độ bóng đá qua mạng với số tiền lên tới 800 tỷ đồng tại Hà Nội. Ngoài ra, năm 2024, lực lượng Công an còn phát hiện 3.264 vụ vi phạm pháp luật liên quan đến viễn thông, tin học, tăng 22,4% so với cùng kỳ năm 2023. Số vụ khởi tố đạt 615 vụ, với 822 bị can bị truy tố, tăng 20,11% về số vụ và 33,44% về số bị can so với năm 2023. Nghiên cứu dữ liệu cho thấy, tội phạm trên không gian mạng, nhất là tội phạm lừa đảo, tội phạm sử dụng công nghệ cao, tội phạm ma túy, buôn bán người… diễn biến phức tạp, không theo quy luật với nhiều phương thức, thủ đoạn mới, tinh vi hơn[37]. Năm 2023, lực lượng Công an phát hiện, xử lý hơn 7.100 vụ lừa đảo chiếm đoạt tài sản (hơn 3.200 vụ lừa đảo trên không gian mạng). Từ đầu năm 2024 đến nay, phát hiện, xử lý hơn 3.900 vụ lừa đảo chiếm đoạt tài sản (hơn 2.500 vụ lừa đảo trên không gian mạng)[38]. Những con số nói trên không chỉ phản ánh sự gia tăng mạnh mẽ về số vụ vi phạm và số đối tượng liên quan đến tội phạm trên KGM mà còn cho thấy sự quyết liệt trong công tác ADPL của lực lượng CAND, nhất là trong việc điều tra và xử lý của các cơ quan có thẩm quyền.

Tại Hội nghị tổng kết 05 năm thực hiện chương trình Hành động phòng, chống tệ nạn xã hội, phòng, chống mại dâm giai đoạn 2020-2025, báo cáo của Bộ Công an cho thấy hàng loạt đường dây đánh bạc trực tuyến, hoạt động mại dâm

[37] Tổng cộng, từ năm 2021 đến 2024, lực lượng chức năng đã phát hiện 8.515 vụ vi phạm pháp luật hình sự về an ninh mạng, với 8.914 đối tượng tham gia thực hiện hành vi phạm tội. Số vụ khởi tố trong giai đoạn này là 1.771 vụ, với 2.259 bị can bị truy tố.

[38] Cục An ninh mạng và phòng, chống tội phạm công nghệ cao, Bộ Công an, *Báo cáo tổng kết các mặt công tác Công an năm 2024,* Hà Nội.

qua mạng xã hội đã bị triệt phá. Tuy nhiên, tình trạng mại dâm qua mạng internet, mạng xã hội, tình hình tội phạm đánh bạc trên KGM vẫn diễn biến phức tạp do chưa có nhiều biện pháp ngăn chặn triệt để và đạt hiệu quả cao nhất. Nhiều mạng xã hội, trang web có máy chủ đặt ở nước ngoài và chưa có cơ chế hoặc cơ chế phối hợp xử lý giữa các lực lượng chức năng của Việt Nam với các quốc gia khác chưa đạt hiệu quả cao. Báo cáo cho thấy, hơn 3 năm qua, lực lượng chức năng đã phát hiện, điều tra và xử lý gần 200 vụ xâm hại trẻ em trên KGM. Trên thực tế, con số chưa được phát hiện và xử lý còn lớn hơn nhiều. Quá trình thu thập, điều tra chứng cứ điện tử trong các vụ xâm hại trẻ em trên KGM còn lúng túng và hiện chưa có chế độ thông tin, báo cáo, thống kê chính thức về tội phạm xâm hại trẻ em trên KGM.

Về hoạt động xét xử của Tòa án Nhân dân[39]: Trong hệ thống các cơ quan nhà nước có thẩm quyền áp dụng pháp luật đối với an ninh mạng, Tòa án đóng vai trò quan trọng trong việc xét xử các vụ án hình sự trong lĩnh vực này. Chức năng, nhiệm vụ, quyền hạn của Tòa án không chỉ ảnh hưởng sâu rộng đến an ninh quốc gia, TTATXH mà còn tác động mạnh mẽ đến an toàn, ANM thậm chí có sự tác động rất lớn đến sự ổn định của xã hội. Hoạt động xét xử của Tòa án góp phần tạo dựng niềm tin vào hệ thống pháp luật. Trước khi thụ lý hồ sơ, Tòa án có quyền áp dụng các biện pháp khẩn cấp tạm thời để bảo vệ quyền và lợi ích hợp pháp của Nhà nước, xã hội và cá nhân. Trong quá trình xét xử, Tòa án luôn tuân thủ nghiêm ngặt các quy định về trình tự, thủ tục theo Bộ luật Tố tụng hình sự, bảo đảm tính khách quan và công minh. Đồng thời, các chế tài được áp dụng không chỉ mang tính răn đe, phòng ngừa mà còn có giá trị giáo dục, thuyết phục góp phần nâng cao nhận thức pháp lý trong cộng đồng mạng.

Thực tiễn xét xử trong ngành Tòa án những năm qua cho thấy số vụ án hình sự liên quan đến an ninh mạng đang có xu hướng gia tăng mạnh mẽ. Dữ liệu thống kê từ Tòa án nhân dân tối cao chỉ ra rằng tội phạm trong lĩnh vực công nghệ thông tin và mạng viễn thông ngày càng gia tăng, với số lượng vụ án ngày càng nhiều, đặc biệt là các hành vi sử dụng mạng viễn thông và internet để thực hiện các hoạt động lừa đảo, đánh bạc, tổ chức đánh bạc quy mô lớn, gây hậu quả nghiêm trọng cho xã hội. Các hành vi này không chỉ diễn ra ở nhiều địa phương mà còn liên quan đến các giao dịch tài chính lớn, cho thấy một khoảng trống trong công tác

[39] Xem thêm: Cục Thống kê, Tòa án nhân dân Tối cao, *Báo cáo công tác ngành Tòa án* (các năm 2021 – 2024)

phòng ngừa, điều tra và xử lý tội phạm mạng. Hầu hết các vụ án liên quan đến đảm bảo an toàn KGM hoặc ANM tập trung vào các tội danh như "đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông", "xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác", "sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để chiếm đoạt tài sản" và "thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng", theo các Điều 288, 289, 290 và 291 của Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung 2017).

Dữ liệu thống kê từ năm 2021 đến 2024 chỉ ra sự gia tăng đáng kể cả về số lượng vụ án và số bị cáo trong các vụ án liên quan đến tội phạm mạng. Cụ thể, số vụ án đã tăng mạnh từ 141 vụ vào năm 2021 lên 281 vụ vào năm 2024, tương ứng với mức tăng gần 100%. Tương tự, số bị cáo cũng tăng từ 50 lên 159 người trong cùng giai đoạn, với tỷ lệ tăng trưởng đạt gần 218%. Điều này không chỉ phản ánh sự gia tăng về số lượng vụ án mà còn cho thấy xu hướng gia tăng sự phức tạp trong mỗi vụ án, khi một vụ có thể liên quan đến nhiều bị cáo.

Khoảng thời gian từ 2021 đến 2024 chứng kiến sự thay đổi rõ rệt trong số lượng vụ án và bị cáo bị xét xử sơ thẩm liên quan đến tội phạm công nghệ thông tin (CNTT) và mạng viễn thông (MTV). Nghiên cứu báo cáo của ngành Tòa án trong những năm gần đây cho thấy:

- Đối với các hành vi phạm tội liên quan tới Điều 285 Tội sản xuất, mua bán, trao đổi công cụ và phần mềm trái phép, cũng như Điều 286 Tội phát tán chương trình gây hại, không có vụ án nào được ghi nhận trong giai đoạn này. Ngược lại, Điều 287 về hành vi cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông và phương tiện điện tử ghi nhận sự gia tăng nhẹ, với một vụ án và một bị cáo được xét xử mỗi năm từ 2022 đến 2024. Đặc biệt, Điều 288 về tội sử dụng trái phép thông tin mạng thể hiện sự gia tăng rõ rệt, từ không có vụ án nào vào năm 2020 đến 16 vụ án và 28 bị cáo vào năm 2024.

- Các tội phạm liên quan đến Điều 290 và Điều 291 đã có sự gia tăng mạnh mẽ, phản ánh sự phát triển nhanh chóng của tội phạm mạng trong bối cảnh công nghệ số ngày càng thịnh hành. Cụ thể, tội phạm theo Điều 290 đã tăng từ 37 vụ án và 45 bị cáo vào năm 2021 lên 82 vụ án và 90 bị cáo vào năm 2024. Điều này cho thấy các hành vi chiếm đoạt tài sản qua mạng, như lừa đảo qua email, website giả mạo, hoặc tấn công vào hệ thống thanh toán trực tuyến, đã trở thành mối đe

dọa nghiêm trọng, gây thiệt hại tài chính lớn và làm suy giảm niềm tin của người dân vào hệ thống bảo mật trực tuyến.

- Tội phạm theo Điều 291 liên quan đến thông tin tài khoản ngân hàng cũng ghi nhận sự gia tăng mạnh mẽ từ 3 vụ án và 4 bị cáo vào năm 2021 lên 32 vụ án và 45 bị cáo vào năm 2024. Các hành vi xâm nhập trái phép vào tài khoản ngân hàng để chiếm đoạt tiền hoặc thông tin tài chính nhạy cảm ngày càng phổ biến thông qua các phương thức như phishing, tấn công phần mềm độc hại, hoặc khai thác lỗ hổng bảo mật trong các dịch vụ tài chính trực tuyến. Sự gia tăng này không chỉ gây thiệt hại tài sản cá nhân mà còn tạo ra những thách thức lớn trong công tác bảo vệ an ninh tài chính và bảo mật thông tin trong môi trường số hiện nay.

Hình phạt đối với các bị cáo trong các vụ án liên quan đến tội phạm công nghệ thông tin và mạng viễn thông cho thấy một số xu hướng đáng chú ý. Phần lớn bị cáo (49,9%) nhận hình phạt chính là tù từ 3 năm trở xuống, cho thấy đa phần các tội phạm này không gây ra hậu quả đặc biệt nghiêm trọng. Tuy nhiên, một tỷ lệ đáng kể (25,2%) bị cáo bị kết án từ 3 đến 7 năm tù, phản ánh sự nghiêm trọng hơn trong một số vụ án. Một bộ phận nhỏ bị cáo (17,4%) nhận hình phạt tù từ 7 đến 15 năm, đặc biệt đối với các tội phạm liên quan đến xâm phạm thông tin cá nhân và tài sản qua mạng. Tỷ lệ áp dụng hình phạt bổ sung (như phạt tiền) chỉ chiếm 4,6%, cho thấy mức phạt tài chính không phải là phương án chủ yếu trong việc xử lý các tội phạm sử dụng công nghệ cao trên KGM.

Một điểm đáng chú ý trong giai đoạn này là sự tham gia của người nước ngoài trong các vụ án tội phạm công nghệ thông tin và mạng viễn thông. Tỷ lệ bị cáo là người nước ngoài có sự biến động qua các năm. Năm 2021, tỷ lệ này chiếm 2,78% trong tổng số bị cáo, nhưng đến năm 2023, đã tăng lên 13,57%. Tuy nhiên, đến năm 2024, tỷ lệ này giảm xuống còn 5,03%. Mặc dù có sự gia tăng trong một số năm, tỷ lệ người nước ngoài bị xét xử trong các vụ án hình sự liên quan đến tội phạm mạng vẫn ở mức thấp và có sự biến động khó dự báo qua từng năm.

Tình hình xét xử các vụ án liên quan đến an ninh mạng từ 2021 đến 2024 cho thấy sự gia tăng về số lượng và tính chất phức tạp của các tội phạm công nghệ thông tin và mạng viễn thông. Điều này phản ánh sự phát triển nhanh chóng của tội phạm công nghệ cao trong bối cảnh xã hội chuyển hướng mạnh mẽ sang nền kinh tế số. Việc áp dụng hình phạt nghiêm khắc, linh hoạt và phù hợp với từng vụ án sẽ góp phần nâng cao hiệu quả công tác đấu tranh với tội phạm trên KGM.

3. Nhận xét, đánh giá

a. Những ưu điểm, kết quả đạt được

Trên cơ sở pháp lý là hệ thống pháp luật về ANM, thời gian qua, hoạt động ADPL về ANM đã ghi nhận những kết quả quan trọng, cụ thể như:

Một là, hoạt động ADPL về ANM, đặc biệt là công tác xử lý vi phạm pháp luật hành chính và xử lý các loại tội phạm trên KGM đã được thực hiện một cách chính xác, nhanh chóng và kịp thời. Việc phát hiện và xử lý các hành vi vi phạm ngày càng trở nên nhanh chóng và hiệu quả hơn, góp phần đảm bảo pháp chế trong việc thực thi pháp luật về an ninh mạng. Đặc biệt, nhiều hoạt động đã nhận được sự tài trợ từ các tổ chức trong nước và quốc tế, phản ánh sự tích cực và chủ động trong công tác phối hợp của các cơ quan quản lý nhà nước về lĩnh vực an ninh mạng.

Nỗ lực của các cơ quan quản lý nhà nước trong việc thi hành chức năng, nhiệm vụ của mình đã nhận được phản hồi tích cực từ xã hội. Hoạt động thực thi pháp luật về an ninh mạng ngày càng được tăng cường và phát huy hiệu quả, góp phần đưa Việt Nam trở thành một trong những quốc gia hàng đầu về an ninh mạng trong khu vực và trên thế giới. Điều này có ý nghĩa quan trọng trong việc ngăn chặn và phòng ngừa các hành vi xâm phạm an ninh quốc gia, trật tự và an toàn xã hội trên không gian mạng.

Hơn nữa, việc xử lý vi phạm pháp luậttrong lĩnh vực an ninh mạng không chỉ đảm bảo an toàn cho không gian mạng mà còn bảo vệ quyền và lợi ích hợp pháp của tổ chức và cá nhân. Kết quả của công tác xử phạt cũng đã đóng góp một nguồn thu đáng kể vào ngân sách nhà nước.

Hai là, công tác phối hợp trong việc phát hiện, ban hành và tổ chức thực hiện các văn bản pháp luật liên quan đến an ninh mạng giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ủy ban nhân dân các cấp, cùng các cơ quan, đơn vị có liên quan trong ngành thông tin và truyền thông đã được triển khai một cách thống nhất, đồng bộ và hiệu quả. Thực tế cho thấy các cơ quan, cá nhân có thẩm quyền đã nghiêm túc thực thi pháp luật trong việc xử lý các vi phạm trong lĩnh vực an ninh mạng. Nhiều tổ chức, cá nhân vi phạm đã chấp hành các hình thức xử phạt kịp thời và đúng quy định. Lực lượng chuyên trách bảo vệ an ninh mạng gồm: Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao

thuộc Bộ Công an; Cục Bảo vệ an ninh Quân đội, Tổng cục Chính trị và Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng.

Lực lượng Công an đã phối hợp chặt chẽ với lực lượng Quân đội, các bộ, ban, ngành, địa phương chủ động phát hiện, đấu tranh vô hiệu hóa nhiều âm mưu, hoạt động chống phá của các thế lực thù địch, phản động và các loại tội phạm trên không gian mạng, đóng góp quan trọng vào những thành tựu chung của đất nước. Phối hợp với lực lượng chức năng, các doanh nghiệp hoạt động trong lĩnh vực an ninh mạng hoạt động rất tích cực, hiệu quả.

Các cơ quan chuyên trách bảo vệ an ninh mạng đã phối hợp chặt chẽ với các cơ quan truyền thông ngoài lực lượng đẩy mạnh tuyên truyền về truyền thống vẻ vang, lan tỏa những chiến công, thành tích, gương điển hình tiên tiến, gương người tốt việc tốt của Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao,... Tại các địa phương, lực lượng chuyên trách đã phối hợp rất tốt với các cơ sở đào tạo, đặc biệt là các trường phổ thông để tổ chức tuyên truyền về Luật An ninh mạng, kỹ năng nhận diện hành vi xâm phạm an ninh mạng và các kiến thức có liên quan khác.

Hầu hết các tổ chức, cá nhân bị thanh tra, kiểm tra và xử lý vi phạm đã có sự kiềm chế và không tiếp tục thực hiện những hành động trái pháp luật trong lĩnh vực an ninh mạng. Nhìn chung, các hành vi cản trở quá trình xử lý vi phạm của cơ quan có thẩm quyền đã giảm đáng kể.

Ba là, năng lực áp dụng pháp luật về an ninh mạng của các cá nhân và tổ chức có thẩm quyền đã được nâng cao, chất lượng xử lý các vụ việc xâm phạm an ninh mạng bước đầu được đảm bảo, đồng thời giảm thiểu sai sót trong quá trình tố tụng. Những người có thẩm quyền xử lý vi phạm trong lĩnh vực an ninh mạng được đào tạo bài bản, trang bị đầy đủ kiến thức và nắm vững quy trình xử lý. Nhờ đó, việc phát hiện và xử lý vi phạm pháp luật trong lĩnh vực an ninh mạng diễn ra chính xác, nhanh chóng và thuận lợi.

Các cơ quan chức năng đã thực hiện xử lý vi phạm pháp luật trong lĩnh vực an ninh mạng theo đúng trình tự, thủ tục pháp lý quy định, đảm bảo xử lý đúng người, đúng hành vi. Đồng thời, các cơ quan này cũng linh hoạt vận dụng các quy định và quy trình xử lý để đáp ứng yêu cầu về chính trị, pháp luật và nghiệp vụ, phục vụ hiệu quả công tác quản lý nhà nước trong không gian mạng.

Bốn là, xây dựng được lực lượng bảo vệ an ninh mạng.

Bên cạnh lực lượng chuyên trách bảo vệ an ninh mạng, Việt Nam đã từng bước xây dựng và hoàn thiện lực lượng bảo vệ an ninh mạng.

Ngày 16/03/2017, Thủ tướng Chính phủ ban hành Quyết định số 05/2017/QĐ-TTg Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia. Theo đó, Cục An toàn thông tin, mạng lưới ứng cứu sự cố an toàn thông tin mạng Việt Nam được thành lập. Đến nay, mạng lưới đã có hơn 220 thành viên bao gồm các đơn vị chuyên trách về ứng cứu sự cố và các cơ quan, tổ chức, doanh nghiệp liên quan trên toàn quốc.

Bộ Thông tin và Truyền thông đã khai trương Hệ thống Chia sẻ và Giám sát thông tin phục vụ Chính phủ điện tử vào ngày 29/11/2019. Hệ thống được Trung tâm Giám sát không gian mạng quốc gia NCSC (thuộc Cục An toàn thông tin) phối hợp cùng các thành viên trong Liên minh xử lý mã độc và phòng chống tấn công mạng gồm Viettel, VNPT, CMC, FPT, BKAV xây dựng; giúp giám sát, phân tích thông tin từ đó chia sẻ và đưa ra cảnh báo sớm cho các bộ, ngành, địa phương nhằm bảo đảm an toàn, an ninh mạng cho Chính phủ điện tử.

Bộ Thông tin và Truyền thông cũng tập trung thúc đẩy phát triển doanh nghiệp và hệ sinh thái sản phẩm an toàn thông tin mạng Việt Nam. Các giải pháp, dịch vụ của doanh nghiệp sẽ được kết nối và chia sẻ với "Hệ thống Chia sẻ và Giám sát an toàn thông tin phục vụ Chính phủ điện tử" tại Trung tâm Giám sát an toàn không gian mạng quốc gia (SoC quốc gia) thuộc Cục An toàn thông tin. Đây sẽ là nền tảng phục vụ Chính phủ điện tử, đô thị thông minh và hệ thống thông tin quan trọng quốc gia.

Việt Nam cũng đã thiết lập được Trung tâm An ninh mạng quốc gia, có công suất xử lý 300.000.000 nội dung/ngày, áp dụng công nghệ phân tích các bài đăng trên mạng xã hội. Bên cạnh đó, đã xây dựng Trung tâm Phòng chống tin giả và hoạt động rất hiệu quả. Xây dựng quy trình khẩn cấp để xử lý tin sai sự thật, yêu cầu các nền tảng xuyên biên giới loại bỏ thông tin sai lệch, vi phạm pháp luật.

Nhìn chung, hoạt động xử lý vi phạm pháp luật trong lĩnh vực an ninh mạng được tiến hành đúng trình tự, thủ tục và nội dung mà pháp luật đã quy định, bảo đảm tính hợp lý và chính xác của việc xử lý vi phạm hành chính trong lĩnh vực an ninh mạng. Việc áp dụng nghiêm minh các quy định pháp luật về phòng ngừa và xử lý hành vi xâm phạm an ninh mạng đã tạo ra hiệu ứng phòng ngừa và răn đe tích cực trong không gian mạng. Quá trình áp dụng pháp luật cũng đảm bảo tính

chính xác, khách quan và công bằng, thể hiện sự vào cuộc quyết liệt của các chủ thể có trách nhiệm.

Những thành tựu, kết quả khả quan đã đạt được trong hoạt động tổ chức thực hiện, ADPL về ANM đến từ những nguyên nhân:

- Thực hiện, ADPL về ANM xuất phát từ chủ trương nhất quán của Đảng về bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên KGM. Quá trình ADPL về ANM nhận được sự lãnh đạo, chỉ đạo sát sao của các cấp ủy Đảng, sự phối hợp của các cấp chính quyền, các bộ ban ngành có chức năng quản lý nhà nước về ANM, được xã hội ủng hộ. Chủ trương này là động lực quan trọng để các chủ thể thực hiện tốt pháp luật về ANM.

- Các cơ quan nhà nước có thẩm quyền đã tổ chức thực hiện và ADPL về ANM đã quán triệt nghiêm túc, hiện thực hóa kịp thời chủ trương đúng đắn này. ADPL về ANM chính là để phòng ngừa, điều tra, xử lý hành vi xâm phạm ANM, đó là yêu cầu cấp bách để góp phần bảo vệ, xây dựng KGM an toàn, bảo đảm chủ quyền KGM quốc gia, góp phần phát triển kinh tế - xã hội đất nước một cách bền vững trong quá trình hội nhập quốc tế.

- Quá trình triển khai, ADPL về ANM nhận được sự điều hành quyết liệt của Chính phủ, cộng với nỗ lực thực thi trách nhiệm của các cơ quan chủ quản, nhất là Bộ Công an. Bộ Công an đã khẩn trương và quyết liệt thực hiện việc bổ sung nhân lực, hoàn thiện bộ máy, tạo điều kiện để lực lượng chuyên trách bảo vệ ANM nhanh chóng đi vào hoạt động. Bộ chủ quản cũng nỗ lực tìm kiếm các biện pháp phối hợp tổ chức thực hiện và ADPL về ANM hiệu quả với Bộ Quốc phòng, Bộ Thông tin và Truyền thông,... chú trọng hiệu quả công tác ADPL về ANM đối với từng hệ lực lượng trong CAND, từng bước bảo đảm ATTT ạng cho người dân, nâng cao hơn nữa nhận thức cho toàn xã hội. Điều này có được là nhờ sự kịp thời tuyên truyền phổ biến, hướng dẫn pháp luật từ các cơ quan quản lý nhà nước khi các tổ chức, doanh nghiệp nảy sinh thắc mắc. Từ đó, pháp luật về ANM thẩm thấu sâu dần vào thực tiễn cuộc sống.

- Quá trình tổ chức thực hiện và ADPL về ANM nhận được sự đồng thuận nhiều quốc gia hữu quan, của các tổ chức trong nước và các tổ chức quốc tế. Quá trình này, Việt Nam đã nhận được sự hỗ trợ thiết thực từ một số quốc gia trên thế giới như Liên bang Nga, Hoa Kỳ, Xingapo,... cùng với sự đồng thuận từ các doanh

nghiệp cung cấp dịch vụ kinh doanh trên KGM và cá nhân người dùng mạng. Mặt khác, cư dân mạng đã ngày càng nhận thức đầy đủ hơn về ATTT mạng và cùng với cơ quan quản lý nhà nước về ANM, thực hiện nghiêm chỉnh quy định của pháp luật ANM, qua đó góp phần xây dựng văn hóa mạng ngày càng lành mạnh.

b. Một số hạn chế và nguyên nhân

Bên cạnh những ưu điểm đạt được, hoạt động ADPL về ANM ở Việt Nam còn tồn tại không ít hạn chế. Những hạn chế xuất phát từ nhiều nguyên nhân, đòi hỏi Nhà nước cần tiến hành đồng bộ, kịp thời các giải pháp để tăng cường bảo vệ an ninh mạng trong thời gian tới.

Một là, cơ sở hạ tầng viễn thông và công nghệ thông tin của Việt Nam chưa đáp ứng yêu cầu bảo mật thiết yếu; hệ thống mạng thông tin còn nhiều lỗ hổng bảo mật, bị các thế lực thù địch, phản động và tội phạm sử dụng công nghệ cao lợi dụng tấn công xâm nhập, phá hoại, gây thiệt hại lớn cho các cơ quan Nhà nước, tổ chức và nhân dân. Hạ tầng viễn thông, công nghệ thông tin còn chậm về tốc độ, chưa đáp ứng được các yêu cầu phát triển Internet vạn vật, thành phố thông minh, phương tiện tự động, sản xuất thông minh,...; việc tiếp cận dịch vụ băng rộng ở khu vực nông thôn, miền núi còn hạn chế; hạ tầng vật lý chưa đáp ứng được yêu cầu ứng dụng các phương thức quản lý thông minh; hệ thống hạ tầng cơ sở dữ liệu dùng chung quốc gia còn chậm được triển khai; cơ sở dữ liệu quy mô quốc gia tạo nền tảng cho kinh tế số còn phân tán, thiếu, chưa được chuẩn hóa và đồng bộ; hạ tầng thanh toán số chưa đồng bộ, chưa tận dụng được các hạ tầng chung, độ phủ chưa lớn; hạ tầng điện phục vụ cho hạ tầng viễn thông còn có những điểm chưa đáp ứng được yêu cầu. Việc quy hoạch và triển khai hạ tầng viễn thông còn thiếu đồng bộ, đặc biệt giữa hạ tầng viễn thông và các hạ tầng kỹ thuật khác (giao thông, cấp thoát nước, chiếu sáng, điện lực...); việc chia sẻ, sử dụng chung cơ sở hạ tầng viễn thông giữa các doanh nghiệp còn hạn chế; đối với lĩnh vực di động, việc đầu tư triển khai các công nghệ mới có xu hướng chậm, chưa tạo được sự bứt phá về phát triển hạ tầng so với khu vực. Quá trình chuyển đổi, xử lý các công nghệ mạng thế hệ cũ còn chậm.

Hai là, một số cấp ủy, chính quyền, cán bộ, đảng viên và nhân dân chưa nhận thức đúng và đầy đủ về an ninh, an toàn thông tin; công tác quản lý nhà nước về an ninh, an toàn thông tin của các cơ quan chức năng có lúc, có nơi còn bị động, lúng túng....

Nhận thức của các cơ quan, doanh nghiệp và cá nhân về bảo vệ bí mật nhà nước trên không gian mạng còn hạn chế, ý thức trách nhiệm của nhiều cán bộ, nhân viên trong bảo mật thông tin trên không gian mạng còn chưa cao, chế tài xử phạt chưa đủ răn đe. Không gian mạng đang ứng dụng sâu rộng vào mọi lĩnh vực của đời sống xã hội, tuy nhiên sự phụ thuộc vào thiết bị công nghệ thông tin có nguồn gốc từ nước ngoài là mối đe dọa tiềm tàng đối với an ninh mạng nếu xảy ra xung đột. Thêm vào đó, các máy chủ dịch vụ OTT (over-the-top cung cấp nội dung thông qua các ứng dụng mạng) xuyên biên giới vào Việt Nam đều được đặt ở nước ngoài, nằm ngoài phạm vi kiểm soát của các cơ quan quản lý nhà nước; cơ sở hạ tầng số còn chậm phát triển hơn nhiều quốc gia trên thế giới, nguồn lực tài chính phát triển còn hạn chế; chất lượng nguồn nhân lực đáp ứng yêu cầu trong kỷ nguyên số còn thấp.

Ba là hệ thống pháp luật liên quan tới việc tổ chức thực hiện và ADPL về ANM, nhất là những quy định của pháp luật hành chính và pháp luật hình sự còn bộc lộ một số hạn chế, bất cập. Cụ thể:

- *Pháp luật xử lý vi phạm hành chính*

+ Thực tế cho thấy, trong ADPL về ANM không dễ để tìm kiếm quy định về xử lý vi phạm hành chính đối với hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng. Cụ thể quy định về hành vi trên nằm trong Nghị định số 144/2021/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng và chữa cháy; phòng, chống bạo lực gia đình, cụ thể tại điểm c khoản 1 Điều 15. Quy định như vậy sẽ dẫn tới khó khăn trong việc tra cứu quy định pháp luật về các hành vi bị xử lý vi phạm hành chính, đặc biệt là đối với những người không được đào tạo về luật.

+ Việc xử lý vi phạm hành chính đối với hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng trên thực tiễn chưa đảm bảo được tính răn đe. Bởi lẽ, khi hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng bị xử lý vi phạm hành chính với trị giá tiền chiếm đoạt dưới 2.000.000 đồng nhưng mức xử phạt cho hành vi trên chỉ từ 2.000.000 đồng đến 3.000.000 đồng là chưa tương xứng, chưa đủ tính răn đe. Trong trường hợp đối tượng chiếm đoạt thành công mà bị phát hiện thì cũng chỉ bị xử phạt tối đa 3.000.000 đồng, đây không phải là mức xử phạt đủ mạnh khiến các đối tượng cảm thấy lo sợ, cân nhắc trước khi thực hiện hành vi của mình.

+ Điểm c, khoản 1 Điều 15 Nghị định số 144/2021/NĐ-CP quy định như sau: *"Dùng thủ đoạn gian dối hoặc bỏ trốn để chiếm đoạt tài sản hoặc đến thời điểm trả lại tài sản do vay, mượn, thuê tài sản của người khác hoặc nhận được tài sản của người khác bằng hình thức hợp đồng, mặc dù có điều kiện, khả năng nhưng cố tình không trả"*. Có thể hiểu quy định trên theo hai cách sau:

1) Điểm này quy định ba dạng hành vi độc lập, gồm: 1) Dùng thủ đoạn gian dối để chiếm đoạt tài sản; 2) Bỏ trốn để chiếm đoạt tài sản; 3) Đến thời điểm trả lại tài sản do vay, mượn, thuê tài sản của người khác hoặc nhận được tài sản của người khác bằng hình thức hợp đồng, mặc dù có điều kiện, khả năng nhưng cố tình không trả.

2) Điểm này quy định ba dạng hành vi, gồm: 1) Dùng thủ đoạn gian đối để chiếm đoạt tài sản do vay, mượn, thuê tài sản của người khác hoặc nhận được tài sản của người khác bằng hình thức hợp đồng; 2) Bỏ trốn để chiếm đoạt tài sản do vay, mượn, thuê tài sản của người khác hoặc nhận được tài sản của người khác bằng hình thức hợp đồng; 3) Đến thời điểm trả lại tài sản do vay, mượn, thuê tài sản của người khác hoặc nhận được tài sản của người khác bằng hình thức hợp đồng, mặc dù có điều kiện, khả năng nhưng cố tình không trả. Có thể hiểu theo cách này, bởi nó tương thích với quy định của BLHS năm 2015 về hành vi lạm dụng tín nhiệm chiếm đoạt tài sản tại điểm b khoản 1 Điều 175 BLHS năm 2015: *"Vay, mượn, thuê tài sản của người khác hoặc nhận được tài sản của người khác bằng hình thức hợp đồng rồi dùng thủ đoạn gian dối hoặc bỏ trốn để chiếm đoạt tài sản đó hoặc đến thời hạn trả lại tài sản mặc dù có điều kiện, khả năng nhưng cố tình không trả"*.

Từ hai cách hiểu khác nhau trên đã khiến nhiều cơ quan có thẩm quyền ra quyết định xử phạt vi phạm hành chính khác nhau đối với hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng. Điều này đặt ra yêu cầu hoàn thiện pháp luật xử lý vi phạm hành chính sao cho rõ ràng, cụ thể hơn.

- Pháp luật hình sự

Trong hệ thống pháp luật hình sự Việt Nam, quy định về "Tội lừa đảo chiếm đoạt tài sản" tại Điều 174 BLHS năm 2015 gần như là hoàn hảo, có giá trị lý luận cũng như thực tiễn cao. Tuy nhiên, đối với "Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản" tại Điều 290 BLHS năm 2015 lại có nhiều bất cập trong quy định, gây ra những khó khăn nhất

định trong thực tiễn áp dụng pháp luật. Có thể điểm qua một số bất cập trong quy định tại Điều 290 BLHS năm 2015, cụ thể như:

Thứ nhất, với kĩ thuật liệt kê, nhà làm luật đã liệt kê các hành vi phạm tội của tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản giúp người áp dụng pháp luật có thể dễ dàng, nhanh chóng xác định hành vi phạm tội trên thực tế. Tuy nhiên, với tốc độ phát triển khoa học công nghệ nhanh chóng như hiện tại, các hình thức phạm tội ngày càng phát triển tinh vi, xảo quyệt và khó lường. Mặt khác, để ban hành một văn bản pháp luật mới, mất rất nhiều thời gian để thực hiện theo quy trình nhất định và luật cũng không thể nào thay đổi quá nhiều trong một khoảng thời gian nhất định. Sự thay đổi của pháp luật cần phải có đủ thời gian để người dân nắm bắt luật, hiểu luật và tuân theo pháp luật. Như vậy, pháp luật mới thực hiện được sứ mệnh vốn có của mình. Do đó, việc xây dựng quy định pháp luật theo kĩ thuật liệt kê như vậy không thể theo kịp được thời đại, không liệt kê được toàn bộ hành vi phạm tội; từ đó có thể dẫn đến bỏ lọt tội phạm, định tội danh sai, không đúng với ý chí của nhà làm luật.

Thứ hai, chưa thực sự có sự tách bạch rõ ràng giữa quy định về tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290 BLHS năm 2015) và tội lừa đảo chiếm đoạt tài sản (Điều 174 BLHS năm 2015). Điều 290 BLHS năm 2015 chỉ quy định những hành vi nếu không thuộc Điều 173 và 174 BLHS năm 2015 thì phạm tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản. Về bản chất, đây cũng là hành vi lừa đảo chiếm đoạt tài sản mà đã được quy định tại Điều 174 BLHS năm 2015, chỉ là hành vi này diễn ra theo cách thức và núp dưới hình thức đặc biệt. Như vậy, trong nhiều trường hợp, khi hành vi của người phạm tội thỏa mãn cấu thành tội phạm của cả hai tội, người áp dụng pháp luật khó có thể xác định được chính xác tội danh.

Thứ ba, chưa có sự tương thích giữa quy định BLHS năm 2015 với Luật ANM năm 2018. Theo đó:

i) Luật ANM năm 2018, người phạm tội sử dụng các phương tiện, thiết bị điện tử, không gian mạng làm công cụ để thực hiện tất cả tội phạm quy định tại BLHS năm 2015 thì bị coi là tội phạm mạng. Tuy nhiên, Điều 290 BLHS năm 2015 đã quy định *"Người nào sử dụng mạng máy tính, mạng viễn thông hoặc*

phương tiện điện tử", quy định này vô hình trung làm hẹp đi khái niệm "Tội phạm mạng" được quy định trong Luật ANM năm 2018.

Hai khái niệm *"mạng máy tính"* và *"mạng viễn thông"* không thể bao trùm được hết không gian mạng được. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu. Nếu sử dụng quy định hiện nay tại Điều 290 năm 2015 thì việc sử dụng mạng Internet thực hiện hành vi chiếm đoạt tài sản sẽ được quy vào tội nào? Hơn nữa, công nghệ thông tin là tập hợp các phương pháp khoa học, công nghệ và công cụ kỹ thuật hiện đại để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số. Khái niệm trên rõ ràng không nhắm tới KGM, mà là tiền đề của KGM bao gồm phương pháp khoa học, công nghệ và công cụ kỹ thuật hiện đại. Điều 290 BLHS năm 2015 đã không thể bao trùm được những vấn đề rộng lớn như vậy. Điều đó khiến cho khi có hành vi phạm tội mới xuất hiện trên các môi trường này thì người có thẩm quyền sẽ không biết để định tội danh như thế nào.
ii) Điểm d, khoản 1 Điều 290 BLHS năm 2015 quy định việc lừa đảo chiếm đoạt tài sản chỉ bị xử lý về tội này khi xảy ra trong trong thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp hoặc giao dịch chứng khoán qua mạng. Quy định này vô hình chung đã bó hẹp lại phạm vi xử lý hành vi lừa đảo chiếm đoạt tài sản trên không gian mạng bị truy cứu trách nhiệm hình sự.

Bốn là, sự phối hợp giữa các bộ, ban, ngành, giữa trung ương và địa phương trong công tác bảo vệ an ninh mạng còn thiếu chặt chẽ. Do chưa xác định nội hàm sự cố an ninh mạng nên khi xảy ra các sự cố nguy hại, ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội, việc triển khai hoạt động ứng phó, xử lý, khắc phục hậu quả của cơ quan chức năng có liên quan rất lúng túng, chưa có quy trình thống nhất, cơ quan có trách nhiệm bảo vệ an ninh mạng chưa thể chủ động triển khai các biện pháp, phương án phù hợp.

Năm là, sự thiếu hụt nhân lực chất lượng cao về bảo vệ an ninh mạng. Hiện nay, ở Việt Nam, lĩnh vực an ninh mạng đang thiếu trầm trọng các chuyên gia có kinh nghiệm và thực lực. Những tác động bất lợi của tình trạng thiếu nhân lực chất lượng cao về bảo vệ an ninh mạng ngày càng trở nên rõ ràng khi các cuộc tấn công mạng đang ngày càng xuất hiện nhiều về số lượng và biến đổi nhanh

chóng về thủ đoạn, các công nghệ hiện đại như điện toán đám mây, tự động hóa, trí tuệ nhân tạo, blockchain,... được sử dụng triệt để trong việc gây ra các cuộc tấn công mạng, khủng bố mạng, gián điệp mạng... "Tại Việt Nam, đến hết năm 2020, lực lượng dân sự về an toàn, an ninh mạng của Việt Nam là khoảng 50.000 người, trong khi ước tính đến hết năm 2021 sẽ cần khoảng 700.000 nhân lực. Vì vậy, Việt Nam cũng đang thiếu hụt nhân lực về an toàn, an ninh mạng." Cục An toàn thông tin Bộ Thông tin và Truyền thông cho biết, nguồn nhân lực trong lĩnh vực này chưa đáp ứng được nhu cầu cả về số lượng và chất lượng, nhất là ở cấp độ địa phương. Thực tế cho thấy rất hiếm đơn vị, tổ chức nào, nhất là các đơn vị hành chính sự nghiệp có đủ nhân lực phục vụ cho công tác đảm bảo an toàn thông tin mạng. Nhiều tổ chức, doanh nghiệp cũng thiếu nhân lực an toàn thông tin, dẫn đến khó triển khai các giải pháp an toàn thông tin mới. Rủi ro về an ninh mạng ngày càng leo thang do tình trạng thiếu hụt nhân sự. Số lượng tổ chức, doanh nghiệp phải đối mặt với 5 vụ vi phạm an ninh trong 1 năm đã tăng tới 53%.
Những tồn tại và hạn chế vừa nêu được gây ra bởi các nguyên nhân sau:

Thứ nhất, hệ thống pháp luật về xử lý vi phạm trong lĩnh vực an ninh mạng hiện nay còn thiếu sót và chưa đáp ứng đầy đủ yêu cầu bảo vệ an ninh mạng trong bối cảnh phát triển nhanh chóng của công nghệ số. Các văn bản pháp lý hiện tại chủ yếu mang tính chỉ đạo và không có hiệu lực pháp lý cao, thiếu các quy định cụ thể và chi tiết về công tác quản lý an ninh, trật tự trên không gian mạng cũng như xử lý vi phạm pháp luật trong lĩnh vực này. Các quy định trong các văn bản pháp lý hiện hành chưa đủ mạnh để phòng ngừa và xử lý các hành vi vi phạm, chủ yếu chỉ tập trung vào xử lý những vấn đề đã phát sinh.

Mặc dù Việt Nam đã ban hành nhiều văn bản quy phạm pháp luật liên quan đến chính phủ điện tử, thương mại điện tử, giao dịch điện tử, và các hoạt động kinh tế chia sẻ, tạo cơ sở pháp lý cho nền kinh tế số và chính phủ số, nhưng vẫn chưa có một văn bản riêng biệt quy định rõ ràng về xử lý vi phạm trong lĩnh vực an toàn, an ninh mạng. Các quy định về xử lý vi phạm an ninh mạng hiện nay bị phân tán trong nhiều văn bản khác nhau, thiếu sự chi tiết và tính khả thi trong thực tế. Điều này dẫn đến tình trạng các quy định mơ hồ, dễ hiểu và áp dụng không thống nhất, gây khó khăn trong công tác thực thi pháp luật.

Một ví dụ điển hình là các quy định về chứng cứ điện tử và xử lý vi phạm trong các văn bản pháp lý hiện tại, như Bộ luật Tố tụng hình sự năm 2015, chỉ bổ

sung quy định về dữ liệu điện tử mà chưa quy định rõ ràng về chứng cứ điện tử, gây khó khăn trong việc thu thập, bảo quản và xử lý chứng cứ. Bên cạnh đó, thiếu trang thiết bị và quy trình nghiêm ngặt trong xử lý chứng cứ điện tử cũng là yếu tố cản trở công tác thực thi pháp luật. Trình tự xử lý vi phạm trong các văn bản chỉ đạo, hướng dẫn còn thiếu sự rõ ràng, dễ gây hiểu lầm và thực hiện không thống nhất giữa các cơ quan có thẩm quyền.

Do đó, cơ sở pháp lý cho công tác xử lý vi phạm trong lĩnh vực an ninh mạng hiện vẫn chưa hoàn thiện, kéo dài thời gian và làm giảm hiệu quả của công tác xử lý các hành vi vi phạm pháp luật trong lĩnh vực này. Các quy định đã cũ và chưa được sửa đổi, bổ sung kịp thời càng làm cho công tác thực thi pháp luật trở nên khó khăn hơn.

Thứ hai, công tác quản lý nhà nước về an ninh mạng gặp nhiều khó khăn do đội ngũ cán bộ làm công tác thanh tra, kiểm tra, giám sát và xử lý vi phạm chưa đáp ứng đầy đủ yêu cầu. Trình độ chuyên môn của cán bộ không đồng đều, đặc biệt là thiếu sự kết hợp giữa chuyên môn công nghệ thông tin và nghiệp vụ pháp lý. Những cán bộ giỏi công nghệ thông tin (thường tuyển ngoài ngành) lại thiếu kiến thức pháp lý và nghiệp vụ, trong khi những người có kiến thức pháp lý tốt lại yếu về công nghệ thông tin. Điều này làm giảm hiệu quả công tác xử lý vi phạm.

Thực tế cho thấy, công tác xử lý vi phạm hành chính chủ yếu do các cơ quan thuộc Bộ Thông tin và Truyền thông, và các đơn vị nghiệp vụ ngành Công an thực hiện. Tuy nhiên, việc phát hiện và xử lý vi phạm còn chậm, nhiều khi chỉ nhờ vào thông tin từ báo chí, truyền thông mới có thể xác minh và xử lý. Cán bộ làm công tác quản lý nhà nước về an ninh mạng còn thiếu kỹ năng trong việc thu thập, thu giữ và xử lý chứng cứ điện tử, đặc biệt là việc thu thập và xác minh dữ liệu điện tử trong các vụ vi phạm. Việc thu thập chứng cứ điện tử cũng gặp khó khăn, bởi quy trình và phương thức thu thập chưa được hướng dẫn rõ ràng, đặc biệt là trong các vụ vi phạm liên quan đến mạng xã hội hoặc các máy chủ ở nước ngoài.

Mặc dù Bộ Công an là cơ quan chủ trì về quản lý ANM, nhưng hiện nay chưa có trung tâm đào tạo chuyên sâu về nghiệp vụ an ninh mạng trong bộ này. Công tác đào tạo, bồi dưỡng nghiệp vụ cho cán bộ làm công tác quản lý nhà nước về an ninh mạng, dù đã tổ chức hàng năm, nhưng vẫn chưa hiệu quả và chưa đáp

ứng được nhu cầu ngày càng cao. Điều này làm ảnh hưởng đến năng lực chuyên môn của đội ngũ cán bộ trong việc xử lý các hành vi vi phạm, cũng như sự phối hợp giữa các cơ quan trong Bộ Công an, Bộ Thông tin và Truyền thông và Bộ Quốc phòng, khi các nhiệm vụ và trách nhiệm chưa được phân định rõ ràng, thiếu sự phối hợp nhịp nhàng, từ đó ảnh hưởng đến hiệu quả công tác quản lý nhà nước về an ninh mạng.

Thứ ba, ý thức chấp hành pháp luật của một bộ phận công dân và tổ chức trong lĩnh vực an ninh mạng còn hạn chế. Một nguyên nhân chính là hiểu biết pháp luật về an ninh mạng còn yếu, dẫn đến việc vi phạm pháp luật hoặc cố ý lợi dụng kẽ hở của pháp luật để thực hiện hành vi vi phạm. Bên cạnh đó, công tác tuyên truyền, phổ biến và giáo dục pháp luật về xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng vẫn còn hạn chế, mang tính hình thức và chưa đi vào chiều sâu. Đặc biệt, chưa có kế hoạch triển khai cụ thể đối với các đơn vị có nhiệm vụ thực hiện công tác này.

Ngoài ra, nhận thức về tầm quan trọng của công tác quản lý nhà nước về an ninh mạng của nhiều cán bộ, chiến sĩ còn hạn chế, nhất là về yêu cầu, nhiệm vụ cũng như các nguyên tắc trong quản lý an ninh, trật tự trên không gian mạng để bảo đảm an ninh quốc gia. Điều này dẫn đến việc thực hiện nhiệm vụ của một số cán bộ, chiến sĩ còn chủ quan, thiếu cảnh giác và thiếu ý thức nghiệp vụ, tạo ra sơ hở trong công tác. Việc thiếu hiểu biết pháp luật về an ninh mạng cũng là một yếu tố góp phần làm cho việc tuân thủ các quy định về xử lý vi phạm chưa được thực hiện đúng đắn, gây khó khăn trong việc áp dụng các biện pháp cưỡng chế thi hành quyết định xử phạt.

Thứ tư, vi phạm pháp luật trong lĩnh vực an ninh mạng đang gia tăng nhanh chóng, với tính chất ngày càng phức tạp và đa dạng. Sự phát triển mạnh mẽ của công nghệ thông tin, viễn thông và Internet đã tạo ra cơ hội và động lực để phát triển kinh tế - xã hội, nhưng đồng thời cũng tạo ra những nguy cơ và lỗ hổng, tạo điều kiện cho các hành vi vi phạm an ninh mạng. Các đối tượng vi phạm, đặc biệt là tin tặc, lợi dụng các lỗ hổng này để thực hiện hành vi phạm pháp, đặc biệt là các hành vi xâm hại an ninh thông tin trên các nền tảng mạng công nghệ thông tin. Một trong những yếu tố đáng chú ý là sự phát triển mạnh mẽ của mạng xã hội, đã tạo môi trường thuận lợi cho các hành vi vi phạm pháp luật này. Các hành vi vi phạm trong lĩnh vực an ninh mạng rất đa dạng, với tỷ lệ gia tăng qua từng năm,

đồng thời phức tạp hơn về thành phần và phương thức thực hiện. Các đối tượng thù địch và tội phạm lợi dụng hệ thống mạng để xâm phạm an ninh, trật tự, thông qua các nền tảng xuyên biên giới hoặc các ứng dụng mạng xã hội, với các thủ đoạn tinh vi, khó phát hiện.

Do đó, công tác quản lý nhà nước về an ninh mạng cần phải thực hiện theo lộ trình có trọng tâm, trọng điểm. Lực lượng an ninh mạng, do Công an nhân dân làm nòng cốt, cần tập trung vào các nhiệm vụ bảo vệ an ninh quốc gia, trật tự và an toàn xã hội trên không gian mạng, đồng thời đáp ứng kịp thời với sự phát triển nhanh chóng của các mối đe dọa và vi phạm trong lĩnh vực này.

Thứ năm, mặc dù đã có sự quan tâm đầu tư vào cơ sở vật chất và phương tiện làm nhiệm vụ, công tác quản lý nhà nước trong lĩnh vực viễn thông, Internet, an toàn, an ninh mạng vẫn còn nhiều bất cập và chưa đáp ứng được yêu cầu. Hoạt động thương mại điện tử, thanh toán trực tuyến và các dịch vụ trực tuyến phát triển mạnh, nhưng công tác quản lý vẫn chưa theo kịp, tạo ra những sơ hở cho các hành vi lừa đảo, chiếm đoạt tài sản, và xâm hại nghiêm trọng đến chủ quyền không gian thanh toán và hệ sinh thái kỹ thuật số.

Cơ sở vật chất phục vụ công tác xử lý vi phạm pháp luật về an ninh mạng, mặc dù đã được quan tâm đầu tư, nhưng vẫn chưa đáp ứng được yêu cầu. Các phương tiện và công cụ hỗ trợ làm nhiệm vụ chưa đồng bộ và chưa đủ hiệu quả, gây khó khăn trong công tác thực thi pháp luật. Bên cạnh đó, các quy định về hình thức xử phạt đối với hành vi vi phạm còn chưa tương xứng và chưa đảm bảo tính răn đe. Một vấn đề nữa là dự án cơ sở dữ liệu quốc gia về xử lý vi phạm hành chính vẫn chưa hoàn thành và đi vào hoạt động, dẫn đến khó khăn trong việc cập nhật thông tin, báo cáo thống kê về tình hình vi phạm hành chính, áp dụng biện pháp xử lý hành chính, phân loại các lĩnh vực vi phạm, và xác định tái phạm để xử phạt hoặc xử lý hình sự.

II. MỘT SỐ YẾU TỐ TÁC ĐỘNG VÀ PHƯƠNG HƯỚNG NÂNG CAO HIỆU QUẢ ÁP DỤNG PHÁP LUẬT VỀ AN NINH MẠNG

1. Một số yếu tố tác động

Trong các nguy cơ từ an ninh phi truyền thống, an ninh mạng tiếp tục diễn biến phức tạp, khó kiểm soát. Các nước lớn xác định an ninh mạng là "vấn đề cốt lõi", đe dọa an ninh mạng là đe dọa an ninh quốc gia. Những năm gần đây, Việt Nam luôn là một trong những quốc gia có tỷ lệ nhiễm mã độc và hứng chịu các

cuộc tấn công mạng thuộc nhóm cao trên thế giới. Bên cạnh đó, mức độ sử dụng máy tính và các thiết bị thông minh tại Việt Nam tăng đột biến do ảnh hưởng của COVID-19 và đây cũng chính là môi trường lý tưởng để virus máy tính bùng phát, lây lan mạnh.

Hầu hết các cuộc tấn công xảy ra trong năm qua đều có quy mô lớn, nhằm vào các tổ chức, doanh nghiệp lớn trên toàn cầu. Chính vì những ảnh hưởng vô cùng lớn của hình thức tấn công này mà các nhóm hacker đang dần chuyển mục đích tấn công từ tài chính sang chính trị. Nguồn lợi tài chính không lớn, phạm vi ảnh hưởng sâu rộng... là những điều khiến tấn công chuỗi cung ứng sẽ vẫn là xu hướng tấn công phổ biến mà hacker hướng tới trong những năm tới. Ước tính đến năm 2025, sẽ có khoảng 75 tỷ thiết bị IoT trên toàn cầu. Càng ngày, mạng lưới kết nối giữa các thiết bị IoT càng trở nên rộng khắp với số lượng lớn người dùng khác nhau, khiến vấn đề an ninh trên các thiết bị này trở nên phức tạp.

Cùng với những bước tiến vượt bậc của công nghệ số, tội phạm mạng đã và đang trở thành một trong những vấn đề đáng lo ngại nhất đối với toàn cầu. Không chỉ làm tổn hại nền kinh tế thế giới với thiệt hại ước tính lên tới 8.000 tỷ USD trong năm 2023, con số này dự kiến còn tăng lên mức đáng báo động 10.500 tỷ USD vào năm 2025, lớn hơn GDP của hầu hết các nền kinh tế lớn nhất thế giới. Hơn cả những tổn thất về kinh tế, tội phạm mạng còn đặt ra mối đe dọa nghiêm trọng đối với an ninh quốc gia, sự ổn định chính trị và lòng tin của xã hội vào sự an toàn của các nền tảng công nghệ. Các cuộc tấn công mạng không chỉ gây gián đoạn hoạt động của các tổ chức và chính phủ mà còn làm gia tăng những rủi ro tiềm tàng đối với sự phát triển bền vững của các quốc gia trong tương lai.

Thời gian tới, Việt Nam hiện đang và sẽ phải đối mặt với không ít các nguy cơ, thách thức đe dọa đến ANQG và TTATXH từ môi trường không biên giới - không gian mạng. Đó là:

Những nguy cơ, thách thức từ bên ngoài

Nguy cơ rơi vào thế mắc kẹt giữa các cường quốc hiện nay, thách thức trong triển khai chính sách đối ngoại, đối với các mối đe dọa. Cục diện thế giới, khu vực biến đổi nhanh chóng, sự cạnh tranh, mặc cả chiến lược giữa các nước lớn; diễn biến khó lường, các điểm nóng khiến môi trường chính trị, an ninh khu vực ngày càng trở nên phức tạp, làm giảm lòng tin chiến lược giữa các quốc gia, kích

thích chạy đua vũ trang và tâm lý dân tộc cực đoan, làm gia tăng căng thẳng và phức tạp quá trình giải quyết tranh chấp có liên quan đến lợi ích an ninh quốc gia. Các cuộc tấn công có chủ đích (Advanced Persistent Threat - APT) với tính chất ngày càng tinh vi có xu hướng phát triển với tốc độ nhanh; hình thức tấn công này có mục tiêu cụ thể, tin tặc sử dụng công nghệ tiên tiến, kỹ thuật cao để đột nhập mạng mục tiêu và tập trung vào mục tiêu đó trong thời gian dài nhằm đánh cắp các tài sản trí tuệ, xâm nhập thông tin bí mật đời tư, phá hủy cơ sở hạ tầng của các cơ quan, tổ chức, thậm chí chiếm đoạt tên miền của tổ chức. Rất nguy hiểm khi sự tấn công có sự hậu thuẫn từ những thế lực thù địch hay được một số quốc gia cực đoan tài trợ, sử dụng các chiến thuật tinh vi nhằm vào các cơ quan nhà nước, vào Chính phủ với mục đích đơn giản là gây rối, đến mục tiêu phức tạp nhắm đến chính sách địa chính trị. Ngoài ra, căng thẳng địa chính trị góp phần cho sự xuất hiện và phát triển của chủ nghĩa tin tặc (hacktivism), không chỉ mang tính phá hoại mà còn nhằm mục đích truyền bá thông tin sai lệch, dẫn đến nhiều cuộc điều tra không cần thiết và kéo theo là sự cảnh báo liên tục của các nhà phân tích Trung tâm Điều hành An ninh mạng (SOC) và nhà nghiên cứu an ninh mạng.

Bên cạnh đó, chúng ta cũng đối mặt với nguy cơ gián điệp mạng. Các gián điệp mạng phần lớn là những hacker, làm việc cho các chính phủ hoặc tổ chức khủng bố hoặc có thể làm việc độc lập. Israel là một trong những quốc gia hiếm hoi công bố với thế giới về đội ngũ tình báo mạng của mình, gọi là Unit 8200. Trong Quân đội Trung Quốc, lực lượng đặc trách gián điệp - chiến tranh mạng thuộc biên chế của Lực lượng Chi viện Chiến lược. Cơ quan tình báo hiện nay đang nhắm vào KGM, một mặt trận mới để đối đầu với các tổ chức khủng bố hoặc phát hiện những mối đe dọa tiềm tàng. Thông qua hoạt động của gián điệp mạng, các cơ quan tình báo thu thập thông tin tình báo của các quốc gia khác, do đó nguy cơ về một cuộc chiến tranh mạng giữa các quốc gia là điều khó tránh khỏi.

Những thách thức, nguy cơ từ bên trong

Việc xây dựng đồng bộ hệ thống chiến lược thực hiện nhiệm vụ bảo vệ Tổ quốc còn chưa đồng bộ. Công tác tham mưu chiến lược chất lượng chưa cao, trên một số mặt chưa đáp ứng được đòi hỏi của tình hình, yêu cầu nhiệm vụ. Tình hình an ninh chính trị nội bộ xuất hiện một số biểu hiện tiêu cực. Các biểu hiện "tự diễn biến", "tự chuyển hóa" chưa được đẩy lùi, có mặt bộc lộ rõ nét, nghiêm trọng hơn. An ninh kinh tế tiềm ẩn những bất ổn; an ninh mạng tiếp tục diễn biến phức

tạp, khó kiểm soát; an ninh xã hội có nhiều yếu tố mất ổn định. Tình hình tội phạm diễn biến phức tạp.

Trước những nguy cơ, thách thức trên, bảo vệ an ninh mạng còn nhiều hạn chế cần khắc phục và đặt ra nhiều vấn đề phải lưu tâm, chẳng hạn như:

Thứ nhất, khung khổ pháp lý về bảo vệ an ninh mạng.

Xét về tổng thể, Việt Nam hiện nay đã có được hệ thống pháp luật về an ninh mạng tương đối toàn diện, đồng bộ. Pháp luật về an ninh mạng của Việt Nam đã thể hiện rõ tinh thần bảo vệ an ninh Tổ quốc, trật tự an toàn xã hội trên không gian mạng, đáp ứng yêu cầu hội nhập quốc tế trong bối cảnh mới. Pháp luật về an ninh mạng đã điều chỉnh được tương đối bao quát những quan hệ xã hội chủ yếu nảy sinh trên không gian mạng; ghi nhận các nguyên tắc bảo vệ an ninh mạng là cơ sở pháp lý trong xây dựng, tổ chức và hoạt động cho cơ quan có thẩm quyền trong hoạt động này; được thiết kế xây dựng theo cấu trúc quy định hành vi cấm/phòng ngừa, phát hiện, ngăn chặn/xử lý. Nghiêm cấm các hành vi xâm phạm an ninh quốc gia trên không gian mạng (dạng hành vi này chưa được điều chỉnh ở bất cứ văn bản quy phạm pháp luật nào). Điều này thể hiện một cấu trúc khá hợp lý, tạo điều kiện cho các chủ thể dễ dàng tiếp cận nội dung pháp luật. Đặc biệt, pháp luật về an ninh mạng đã có điều khoản quy định riêng về bảo vệ trẻ em trên không gian mạng.

Tuy nhiên, do diễn biến phức tạp của tình hình an ninh mạng hiện nay, vấn đề xây dựng và hoàn thiện pháp luật cần được tiến hành kịp thời, đồng bộ để đảm bảo khắc phục những mâu thuẫn trong hệ thống pháp luật.

Sự trùng lặp giữa Luật An ninh mạng và Luật An toàn thông tin mạng về các khái niệm cơ bản như khái niệm "hệ thống thông tin quan trọng quốc gia"; về tiêu chuẩn, thẩm quyền đánh giá về an toàn thông tin mạng, doanh nghiệp kinh doanh lĩnh vực an toàn thông tin.

Một số quy định chưa được hướng dẫn, giải thích cụ thể: Hành vi "phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe cộng đồng..."; "Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác." Một số nội dung trong Luật An ninh mạng có sự trùng lặp.

Hạn chế trong bảo mật thông tin cá nhân: Chưa có sự thống nhất giữa các văn bản về định nghĩa thông tin cá nhân; Quy định về các nội dung được coi là thông tin cá nhân chưa theo kịp thực tiễn sử dụng các dữ liệu này; Chưa có cơ chế bảo vệ thông tin cá nhân của người tiêu dùng khi tham gia các giao dịch thương mại điện tử xuyên quốc gia.

Thứ hai, vấn đề tư tưởng, lý luận.

Đảng ta lấy chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh làm nền tảng tư tưởng, kim chỉ nam cho hành động cách mạng. Các thế lực thù địch, phản động đang triệt để lợi dụng không gian mạng để tiến hành các hoạt động phá hoại nền tảng tư tưởng, nhằm thực hiện âm mưu chiến lược "diễn biến hòa bình", chống phá Việt Nam. Chúng chủ yếu sử dụng mạng xã hội, phổ biến là Facebook, Youtube để tuyên truyền, phá hoại nền tảng tư tưởng, thúc đẩy "tự diễn biến", "tự chuyển hóa" trong nội bộ, từng bước triển khai thực hiện mục tiêu thay đổi chế độ chính trị nước ta. Năm 2020, Bộ Công an đã phát hiện hơn 3.000 trang mạng có nội dung xấu, trong đó có 31 trang mạng, blog, 55 kênh Youtube, 49 trang fanpage, 765 tài khoản Facebook, 149 hội nhóm chống đối cực đoan, đăng tải hơn 800.000 bài viết, video, clip có nội dung xấu, độc hại. Trong các sự kiện chính trị quan trọng của đất nước, các thế lực thù địch không ngừng lợi dụng không gian mạng để tuyên truyền, phá hoại, phổ biến các quan điểm sai trái, thù địch nhằm chống phá Đảng, Nhà nước ta.

Vấn đề đặt ra là cần làm rõ thêm: những luận điệu, quan điểm, nguyên lý nào của chủ nghĩa Mác - Lênin có giá trị vĩnh viễn, trường tồn; những luận điểm, quan điểm, nguyên lý nào của chủ nghĩa Mác - Lênin đã bị thực tiễn lịch sử vượt qua; những luận điểm, quan điểm, nguyên lý nào cần bổ sung, phát triển. Trong tư tưởng Hồ Chí Minh thì tư tưởng nào là vận dụng, tư tưởng nào là bổ sung, phát triển chủ nghĩa Mác - Lênin để phù hợp thực tiễn cách mạng Việt Nam; nhằm hình thành cơ sở lý luận cho đường lối cách mạng của Đảng; phổ biến, truyền bá chủ trương, quan điểm, đường lối đổi mới của Đảng, làm cho cán bộ, đảng viên, nhân dân thấm nhuần, hiểu đúng, tin tưởng và có vũ, động viên các tầng lớp nhân dân biến thành hành động cách mạng cụ thể, thiết thực trong công cuộc xây dựng và bảo vệ Tổ quốc; ngăn chặn, đẩy lùi suy thoái về tư tưởng chính trị, đạo đức, lối sống, các biểu hiện "tự chuyển biến", "tự chuyển hóa" trong một bộ phận không nhỏ cán bộ, đảng viên; góp phần phòng, chống tham nhũng, lãng phí, tiêu cực;

góp phần bảo vệ vững chắc nền tảng tư tưởng của Đảng; đấu tranh, phê phán các quan điểm sai trái, luận điệu xuyên tạc, làm thất bại mọi âm mưu, thủ đoạn tinh vi chống phá cách mạng nước ta của chiến lược "diễn biến hòa bình" của các thế lực thù địch.

Trong sự nghiệp xây dựng chủ nghĩa xã hội và bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa, chúng ta phải vận dụng sáng tạo, bổ sung, phát triển không ngừng lý luận của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh.

Thứ ba, về nhận thức của cá nhân, tổ chức.

Do yêu cầu tất yếu của sự phát triển, các cơ quan, doanh nghiệp và người sử dụng ngày càng ứng dụng công nghệ thông tin và sử dụng các dịch vụ trên Internet nhiều hơn; vừa để phục vụ công việc, vừa để phục vụ các nhu cầu cá nhân. Để khai thác được hết lợi ích từ Internet thì người sử dụng phải trang bị kiến thức, kỹ năng cần thiết để bảo vệ mình trước sự tấn công cũng như tự mình tránh được lỗi do thiếu hiểu biết.

Rất nhiều người sử dụng mạng tự tin mình có kiến thức, kỹ năng. Tuy nhiên, đó chỉ là những thủ thuật cài đặt, hướng dẫn người dùng hay các thuật ngữ tương tác... trên nền tảng ứng dụng của mỗi loại hình; nhưng các kiến thức về các quy định, ràng buộc để người sử dụng Internet thể hiện trách nhiệm với luật pháp thì không có hoặc có rất mơ hồ. Họ có thể dễ dàng nhận ra nhà sáng lập Microsoft Bill Gates và hiểu rõ cách sử dụng "hashtags" trên trang mạng xã hội, song lại rất lúng túng khi được hỏi về các chính sách đảm bảo quyền riêng tư người sử dụng của các nhà cung cấp dịch vụ. Thậm chí còn nhầm lẫn Internet với www, trong khi www thực chất chỉ là một dịch vụ chạy trên Internet - mạng máy tính toàn cầu, kết nối các máy tính theo cùng một giao thức... Do đó, người sử dụng Internet chủ quan, chưa thực sự chú ý đến việc đảm bảo an toàn thông tin, phòng tránh lây nhiễm mã độc cho máy tính của mình. Người dùng vẫn còn có nhiều hành vi sử dụng Internet không an toàn như sử dụng các phần mềm lậu, truy cập các trang web không uy tín, hoặc không sử dụng các phần mềm bảo vệ máy tính của mình.

2. Phương hướng bảo đảm an ninh mạng và bảo đảm áp dụng pháp luật an ninh mạng ở Việt Nam

a. Phương hướng bảo đảm an ninh mạng ở Việt Nam thời gian tới

Văn kiện Đại hội XIII của Đảng khẳng định: "Kiên quyết, kiên trì bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc, lợi ích

quốc gia - dân tộc; bảo vệ Đảng, Nhà nước, nhân dân và chế độ xã hội chủ nghĩa; bảo đảm an ninh, trật tự, an toàn xã hội; giữ vững môi trường hòa bình, ổn định để phát triển đất nước". Trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư, các thế lực thù địch, phản động luôn lợi dụng thành tựu khoa học - kỹ thuật để chống phá Việt Nam, đặc biệt là gia tăng các hoạt động tuyên truyền phá hoại nền tảng tư tưởng của Đảng trên không gian mạng. Do đó, phương hướng để bảo vệ an ninh quốc gia trên không gian mạng theo tinh thần Đại hội XIII của Đảng, bảo vệ an ninh mạng tại Việt Nam trong thời gian tới được xác định:

Thứ nhất, bảo vệ an ninh quốc gia trên không gian mạng được xác định là trách nhiệm của toàn Đảng, toàn dân, toàn quân, các cấp, các ngành. Trong bối cảnh Cách mạng công nghiệp lần thứ tư, cần phải tăng cường hơn nữa bảo vệ an toàn, an ninh mạng các hệ thống thông tin quan trọng quốc gia; phòng ngừa, phát hiện và đấu tranh ngăn chặn các hoạt động xâm phạm an ninh quốc gia trên không gian mạng.

Thực tế cho thấy, không gian mạng quốc gia Việt Nam chứa đựng những yếu tố hết sức quan trọng, nếu bị xâm hại sẽ ảnh hưởng nghiêm trọng tới lợi ích, an ninh quốc gia. Hiện nay, các thế lực thù địch, phản động trong và ngoài nước vẫn không từ bỏ âm mưu, hoạt động chống phá Việt Nam. Chúng luôn lợi dụng thành tựu khoa học - kỹ thuật và không gian mạng vào các hoạt động chống phá với các thủ đoạn ngày càng tinh vi, nguy hiểm. Trong bối cảnh đó, yêu cầu bảo vệ an ninh quốc gia trên không gian mạng đặt ra trong tình hình hiện nay là hết sức cấp thiết. Chính vì vậy, Nghị quyết số 51-NQ/TW, ngày 5/9/2019, của Bộ Chính trị, về "Chiến lược bảo vệ an ninh quốc gia" xác định, cần phải tăng cường bảo vệ an toàn, an ninh mạng các hệ thống thông tin quan trọng quốc gia và các hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, phát hiện và đấu tranh ngăn chặn các hoạt động xâm phạm an ninh quốc gia trên không gian mạng; khắc phục điểm yếu, lỗ hổng bảo mật, nguy cơ mất an toàn, an ninh mạng, an ninh thông tin.

Bảo vệ an ninh quốc gia trên không gian mạng được xác định là trách nhiệm của toàn Đảng, toàn dân, toàn quân ta. Do đó, để triển khai công tác này, phải phát huy được sức mạnh dân tộc kết hợp với sức mạnh thời đại; đồng thời, xác định đây là cuộc đấu tranh của toàn dân, dưới sự lãnh đạo của Đảng, là nhiệm vụ trọng yếu của cuộc đấu tranh bảo vệ an ninh quốc gia, giữ gìn trật tự, an toàn xã hội, là

trách nhiệm của cả hệ thống chính trị, trong đó, lực lượng công an giữ vai trò nòng cốt, lực lượng an ninh mạng và cảnh sát phòng, chống tội phạm công nghệ cao có trách nhiệm trực tiếp thực hiện nhiệm vụ bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng. Đây là quan điểm, tư tưởng cơ bản, xuyên suốt của Đảng, quyết định thắng lợi cuộc đấu tranh bảo vệ an ninh, chủ quyền quốc gia trên không gian mạng. Các nguyên tắc cần quán triệt trong bảo vệ an ninh quốc gia trên không gian mạng bao gồm: Tuân thủ Hiến pháp, pháp luật, bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân; đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước, huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; lực lượng chuyên trách bảo vệ an ninh quốc gia trên không gian mạng làm nòng cốt. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh quốc gia với nhiệm vụ xây dựng, phát triển kinh tế, văn hóa, xã hội. Chủ động phòng ngừa, đấu tranh làm thất bại mọi âm mưu và hoạt động xâm phạm an ninh quốc gia trên không gian mạng.

Thứ hai, bảo vệ an ninh quốc gia trên không gian mạng là bảo vệ chế độ chính trị và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, bảo vệ độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ Việt Nam trên không gian mạng; bảo vệ an ninh về tư tưởng và văn hóa, khối đại đoàn kết toàn dân tộc, quyền lợi và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân trên không gian mạng; bảo vệ an ninh trong các lĩnh vực kinh tế, quốc phòng, đối ngoại và các lợi ích khác của quốc gia trên không gian mạng; bảo vệ bí mật nhà nước và các mục tiêu quan trọng về an ninh quốc gia trên không gian mạng; phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại và loại trừ các hoạt động xâm phạm an ninh quốc gia, nguy cơ đe dọa an ninh quốc gia trên không gian mạng.

Thứ ba, phát huy sức mạnh tổng hợp trong bảo đảm an ninh mạng.

Bảo đảm an toàn, an ninh mạng được xác định là một trong những nhiệm vụ chính trị quan trọng trong điều kiện, bối cảnh hiện nay. Công tác này phải được thực hiện một cách thường xuyên, liên tục, với những cơ chế, chính sách phù hợp. Phải huy động sức mạnh tổng hợp của cả hệ thống chính trị, của người dân và doanh nghiệp, trong đó các lực lượng chức năng làm nòng cốt. Đồng thời, nêu cao ý chí tự chủ, tự lực, tự cường trong bảo vệ an toàn, an ninh, chủ quyền trên không gian mạng. Trong đó, yếu tố sức mạnh tổng hợp của các chủ thể giữ vai trò đặc biệt quan trọng. Đa số các sự cố an ninh mạng của các cơ quan, tổ chức, doanh

nghiệp đều do con người trực tiếp hoặc gián tiếp vi phạm, bỏ qua các chính sách bảo mật thông tin. Do đó, việc vượt qua thách thức bảo toàn an ninh thông tin đòi hỏi không chỉ các giải pháp kỹ thuật công nghệ mà còn cần quản trị yếu tố con người; yếu tố con người được xem là mắt xích yếu nhất trong việc tạo ra môi trường kỹ thuật số an toàn và bảo mật.

Tại Việt Nam, những năm qua, các cấp có thẩm quyền đã ban hành các chính sách về an toàn, an ninh mạng; các chiến lược, đề án về an ninh mạng đã được xây dựng. Công tác bảo đảm an toàn, an ninh mạng đạt được nhiều kết quả tích cực, nhất là đối với hệ thống mạng thông tin quốc gia, hệ thống thông tin trọng yếu quốc gia; đấu tranh có hiệu quả với các hành vi vi phạm pháp luật về an toàn, an ninh mạng. Bảo đảm an toàn, an ninh mạng đối với hệ thống mạng thông tin quốc gia; bảo vệ uy tín của lãnh đạo Đảng, Nhà nước trên không gian mạng. Tăng cường hiệu lực, hiệu quả công tác quản lý nhà nước về an ninh mạng.

Tuy nhiên, bên cạnh kết quả đạt được vẫn còn một số tồn tại, hạn chế, như nhận thức về vị trí, vai trò, tầm quan trọng, sự thống nhất trong lãnh đạo, chỉ đạo về an toàn, an ninh mạng còn chưa cao. Hành lang pháp lý và hệ thống pháp luật về an toàn, an ninh mạng chưa hoàn thiện. Công tác quản lý nhà nước về an toàn, an ninh mạng chưa đáp ứng yêu cầu đặt ra, đặc biệt đối với các doanh nghiệp cung cấp dịch vụ xuyên biên giới. Hoạt động tấn công mạng gia tăng; vẫn còn tình trạng lộ bí mật nhà nước của một số bộ, ngành, địa phương. Tình trạng thu thập trái phép, mua bán thông tin, dữ liệu cá nhân vẫn diễn biến phức tạp. Tội phạm sử dụng công nghệ cao tiếp tục có chiều hướng gia tăng. Trong khi đó, chỉ có 17% doanh nghiệp Việt Nam được xếp ở giai đoạn triển khai nâng cao và sẵn sàng giải quyết các rủi ro bảo mật; 23% doanh nghiệp chuẩn bị tốt về dữ liệu; 31% doanh nghiệp chuẩn bị tốt về thiết bị cho giải quyết các vấn đề bảo mật; 53% tổ chức, doanh nghiệp mới đang ở giai đoạn bắt đầu. Điều này cho thấy việc chuẩn bị và mức độ sẵn sàng cho giải quyết vấn đề an ninh mạng chưa cao. Đây là một trong các nguyên nhân dẫn tới những hạn chế trong bảo đảm an toàn, an ninh mạng thời gian qua.

Nếu người dùng nhận thức đầy đủ và có kỹ năng bảo vệ an toàn thông tin cơ bản thì có thể tự phòng tránh được tới hơn 80% nguy cơ mất an toàn thông tin khi tham gia không gian mạng. Nhưng trên thực tế, nhận thức của nhiều cơ quan, tổ chức, doanh nghiệp và người sử dụng trong cộng đồng hiện nay còn nhiều tồn

tại, hạn chế, chưa đủ để tự bảo vệ mình trước những mối đe dọa về an toàn thông tin. Nhiều người dùng chưa có các kỹ năng bảo vệ an toàn thông tin, phòng tránh lây nhiễm mã độc; sử dụng các phần mềm lậu, truy cập các trang web không uy tín, hoặc không sử dụng các phần mềm bảo vệ thiết bị.

Ngày 25 tháng 8 năm 2023, tại phiên họp thứ hai của Ban Chỉ đạo an toàn, an ninh mạng quốc gia, Thủ tướng Phạm Minh Chính nêu rõ, không gian mạng đã trở thành không gian chiến lược; phải chủ động ứng phó với các thách thức từ không gian mạng, không để bị động, bất ngờ. Đồng thời, phải có sự tham gia, vào cuộc của cả hệ thống chính trị, cộng đồng doanh nghiệp, người dân; trong đó Ban Chỉ đạo, Văn phòng Ban Chỉ đạo, các Tiểu ban An toàn, An ninh mạng, các lực lượng bảo đảm an toàn, an ninh mạng là nòng cốt, là trực tiếp.

Để phát huy sức mạnh tổng hợp trong bảo đảm an toàn, an ninh mạng, cần đẩy mạnh giáo dục nâng cao nhận thức về bảo đảm an toàn, an ninh mạng. Thực hiện có hiệu quả Quyết định 1907/QĐ-TTg ngày 23/11/2020, về Đề án Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021-2025. Tăng cường giáo dục các quy định của pháp luật về quản lý không gian mạng; cách thức nhận diện các âm mưu, thủ đoạn tấn công mạng và các hình thái tiêu cực phát sinh trên không gian mạng cho toàn thể cán bộ, đảng viên và nhân dân.

Chú trọng nâng cao hiệu quả điều hành, chỉ đạo của Ban Chỉ đạo an toàn, an ninh mạng quốc gia. Tiếp tục bám sát các nhiệm vụ trọng tâm (an ninh mạng; an toàn thông tin mạng; thực hiện nhiệm vụ quốc phòng trên không gian mạng; đấu tranh xử lý thông tin xấu, độc). Tập trung lãnh đạo, chỉ đạo triển khai quyết liệt các nhiệm vụ, để công tác bảo đảm an toàn, an ninh mạng chuyển biến mạnh mẽ hơn, thực chất hơn, hiệu quả hơn. Tham mưu cho cấp có thẩm quyền hoàn thiện các chính sách về an toàn, an ninh mạng, thực hiện các chiến lược, đề án về an ninh mạng.

Thường xuyên phát huy vai trò nòng cốt của các lực lượng chuyên trách và các lực lượng tham gia trong bảo đảm an toàn, an ninh mạng. Nắm chắc tình hình có liên quan đến hoạt động bảo vệ an toàn, an ninh mạng; phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng; ngăn chặn hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia, trật tự, an toàn xã hội; chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng

nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội. Đặc biệt, cần nâng cao trách nhiệm và các kỹ năng cần thiết về an toàn, an ninh mạng của các cơ quan, tổ chức, cá nhân sử dụng không gian mạng. Tuyệt đối tuân thủ quy định của pháp luật về bảo vệ an toàn, an ninh mạng.

Mọi người đều phải thực hiện nghiêm yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an toàn, an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an toàn, an ninh mạng. Đồng thời, chú trọng hơn nữa việc đào tạo nguồn nhân lực, thực hiện tốt Đề án "Đào tạo nguồn nhân lực an ninh mạng, giai đoạn 2022-2025, tầm nhìn đến năm 2030". Nghiên cứu, đề xuất thí điểm một số chế độ ưu đãi và chế độ đặc thù đối với lực lượng chuyên trách bảo vệ an ninh mạng, nhân sự làm về an toàn thông tin mạng.

Thứ tư, phải chủ động ứng phó với các thách thức từ không gian mạng, không để bị động, bất ngờ.

Không gian mạng đã trở thành không gian chiến lược, phải chủ động ứng phó với các thách thức từ không gian mạng, không để bị động, bất ngờ. Đồng thời, phải có sự tham gia, vào cuộc của cả hệ thống chính trị, cộng đồng doanh nghiệp, người dân; trong đó Ban Chỉ đạo, Văn phòng, các Tiểu ban An toàn, An ninh mạng, các lực lượng bảo đảm an toàn, an ninh mạng là nòng cốt, là trực tiếp.

Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ xác định tầm nhìn đến năm 2030 Việt Nam trở thành quốc gia tự chủ về an toàn, an ninh mạng để bảo vệ sự thịnh vượng của Việt Nam trên không gian mạng. Khẳng định quan điểm nhất quán phải chủ động ứng phó với các thách thức từ không gian mạng, không để bị động, bất ngờ.

Nắm bắt kịp thời, tận dụng hiệu quả các cơ hội do không gian mạng mang lại để phát triển kinh tế, xã hội, đồng thời chủ động phòng ngừa, sẵn sàng ứng phó để hạn chế các tác động tiêu cực, bảo đảm quốc phòng, chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội và tính bền vững của quá trình phát triển đất nước trong thời đại Cách mạng công nghiệp lần thứ tư.

Phát huy sức mạnh của cả hệ thống chính trị và toàn xã hội, chủ động ứng phó từ sớm, từ xa với các nguy cơ, thách thức, hoạt động gây tổn hại tới chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng và an toàn thông tin mạng

quốc gia, trong đó cơ quan quản lý nhà nước giữ vai trò điều phối, gắn kết, chia sẻ thông tin.

Chuyển đổi căn bản về nhận thức và cách làm để thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa an toàn, an ninh mạng (cyber resilience): Từ mô hình bảo vệ phân tán sang mô hình bảo vệ tập trung; từ bị động ứng cứu sự cố sang chủ động dự báo sớm, cảnh báo sớm, phòng ngừa và ứng phó hiệu quả; từ đơn độc bảo vệ, giấu kín thông tin bị tấn công mạng sang chủ động hợp tác, chia sẻ thông tin nhằm chủ động phòng ngừa và hỗ trợ xử lý sự cố, phục hồi hoạt động bình thường của hệ thống thông tin.

Thúc đẩy chuyên gia, nghiên cứu, phát triển tự chủ về công nghệ, sản phẩm, dịch vụ an toàn, an ninh mạng Việt Nam là giải pháp căn cơ bảo đảm an toàn, an ninh mạng quốc gia; phát triển thị trường, doanh nghiệp, năng lực cạnh tranh về an toàn, an ninh mạng, đưa Việt Nam trở thành quốc gia có năng lực cao về bảo đảm an toàn, an ninh mạng.

Chủ động hội nhập quốc tế trong lĩnh vực an toàn, an ninh mạng trên tinh thần làm bạn, đối tác tin cậy, có trách nhiệm trong cộng đồng quốc tế, tôn trọng chủ quyền quốc gia trên không gian mạng của các nước khác, tuân thủ luật pháp quốc tế và các hiệp ước đa phương, song phương mà Việt Nam tham gia. Tham khảo kinh nghiệm trong lãnh đạo, chỉ đạo và mô hình an toàn, an ninh mạng trên thế giới.

Thứ năm, xây dựng lực lượng bảo đảm an toàn, an ninh mạng hiện đại, chuyên nghiệp, có đủ nguồn nhân lực chất lượng cao đáp ứng yêu cầu thực tiễn. Phát triển nguồn nhân lực là chủ trương lớn của Đảng và Nhà nước, chủ trương đó đã được khẳng định trong nhiều văn kiện của các kỳ Đại hội Đảng. Xây dựng đội ngũ chuyên gia về an toàn, an ninh mạng chất lượng cao được xem là một trong những trụ cột vững chắc để bảo đảm nền tảng an toàn, an ninh mạng quốc gia cũng như đòn bẩy, thúc đẩy tiến tới Chính phủ điện tử, Chính phủ số, xã hội số.

Một thách thức từ lâu đối với ngành đảm bảo an toàn an ninh mạng của Việt Nam là sự thiếu hụt nguồn nhân lực. Đây là một ngành có tính đặc thù, tính chuyên gia rất cao, và hiện tại rất thiếu về chất và lượng, đồng thời Việt Nam còn có nguy cơ bị chảy máu chất xám ra các nước phát triển hơn. Theo các chuyên gia, sự thiếu hụt nguồn cung từ khâu đào tạo là vấn đề then chốt, nhận thức được

những thách thức này, trong rất nhiều các chiến lược để đảm bảo an toàn thông tin mạng, Chính phủ đã chú trọng tới công tác phát triển nguồn nhân lực về an toàn thông tin. Nhiều chính sách đào tạo, khuyến khích mở rộng, phát triển và thu hút nhân tài ngành an toàn thông tin đã được áp dụng, triển khai đồng bộ trong cả nước.

Nghị quyết số 36-NQ/TW ngày 01/07/2014 của Bộ Chính trị Ban Chấp hành Trung ương Đảng Cộng sản Việt Nam về đẩy mạnh ứng dụng, phát triển công nghệ thông tin, công nghệ số đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế đã xác định việc ứng dụng và phát triển công nghệ thông tin, công nghệ số phải gắn với phát triển nguồn nhân lực chất lượng cao và đặt mục tiêu "Phát triển nguồn nhân lực công nghệ thông tin, công nghệ số đạt chuẩn quốc tế, đảm bảo đáp ứng nhu cầu trong nước về số lượng và chất lượng, có khả năng cung cấp nguồn nhân lực công nghệ thông tin, công nghệ số chất lượng cao cho khu vực và thế giới".

Để cụ thể hóa chủ trương này, ngày 15/4/2015, Chính phủ ban hành Nghị quyết số 26/NQ-CP về việc ban hành Chương trình hành động của Chính phủ thực hiện Nghị quyết số 36-NQ/TW ngày 01/07/2014 của Bộ Chính trị Ban Chấp hành Trung ương Đảng Cộng sản Việt Nam. Theo đó, Nghị quyết đã đặt ra nhiều nhiệm vụ, trong đó có nhiệm vụ: Phát triển nguồn nhân lực công nghệ thông tin, công nghệ số đạt chuẩn quốc tế, đẩy mạnh nghiên cứu, ứng dụng, tiếp thu, làm chủ và sáng tạo công nghệ mới và xây dựng chính sách thu hút và đãi ngộ, chế độ phụ cấp đặc thù đối với cán bộ, công chức, viên chức làm công nghệ thông tin trong cơ quan nhà nước. Nghị quyết nêu trên đã cho thấy tầm quan trọng của việc phát triển nguồn nhân lực công nghệ thông tin, công nghệ số là một trong những yêu cầu chủ chốt nếu Việt Nam muốn tiếp tục phát triển và tăng trưởng ngành công nghệ thông tin, công nghệ số cũng như muốn thúc đẩy đổi mới sáng tạo và khởi nghiệp. Lực lượng lao động công nghệ thông tin được đào tạo bài bản cũng sẽ giúp Việt Nam chuyển đổi sang nền kinh tế tiên tiến dựa trên tri thức.

Điểm c, Khoản 2, Mục III, Quyết định số 964/QĐ-TTg đã khẳng định: "Hình thành lực lượng bảo đảm an toàn, an ninh mạng tại các bộ, ngành, cơ quan nhà nước, các tổ chức chính trị - xã hội và các tập đoàn, tổng công ty nhà nước; đảm bảo mỗi cơ quan, tổ chức, doanh nghiệp nhà nước có một bộ phận được giao nhiệm vụ làm đầu mối, chịu trách nhiệm về công tác bảo đảm an toàn, an ninh

mạng. Khuyến khích các doanh nghiệp khác có một đơn vị bảo đảm an toàn, an ninh mạng".

b. Bảo đảm áp dụng pháp luật an ninh mạng ở Việt Nam thời gian tới

Một là, bảo đảm về chính sách, pháp luật an ninh mạng

Thực hiện "xây dựng, hoàn thiện hệ thống pháp luật, cơ chế, chính sách về an ninh mạng" được ghi nhận trong Nghị quyết về Chiến lược An ninh mạng quốc gia ngày 25/7/2018 của Bộ Chính trị, để bảo đảm tính thống nhất và hiệu lực thi hành, các cơ quan nhà nước cần nhanh chóng thể chế hóa các văn bản của Đảng thành các văn bản quy phạm pháp luật. Chủ động nghiên cứu, rà soát, sửa đổi, bổ sung, xây dựng và tạo hang lang pháp lý hoàn thiện về ANM.

Trước hết, bảo đảm tính thống nhất, đồng bộ của pháp luật về ANM

Tính thống nhất, đồng bộ của pháp luật về ANM thể hiện ở các bộ phận cấu thành hệ thống pháp luật về ANM không được chồng chéo, trùng lặp, có khả năng áp dụng đối với tất cả các chủ thể hoạt động trên môi trường mạng. Các bộ phận phải có mối quan hệ chặt chẽ tạo thành một thể thống nhất. Pháp luật về ANM được thực hiện thống nhất trên phạm vi lãnh thổ KGM quốc gia, không phân biệt vùng miền, có tính ổn định, không sửa đổi liên tục để tạo sự nhất quán cho việc điều chỉnh các quan hệ xã hội phát sinh trong hoạt động bảo vệ an ninh quốc gia, trật tự an toàn xã hội trên KGM.

Trong lĩnh vực pháp luật về ANM hiện có các văn bản pháp luật như Luật An ninh quốc gia năm 2004, Luật Giao dịch điện tử năm 2005, Luật Công nghệ thông tin năm 2006, Luật Viễn thông năm 2009, Luật Tần số vô tuyến điện năm 2009, Luật Cơ yếu năm 2011, Luật Xử lý vi phạm hành chính năm 2012, Luật Giáo dục quốc phòng và an ninh năm 2013, Luật An toàn thông tin mạng năm 2015, Bộ Luật hình sự năm 2015, Luật Bảo vệ bí mật nhà nước năm 2018, Luật Công an nhân dân năm 2018, Luật Quốc phòng năm 2018, Luật An ninh mạng năm 2018. Dưới các văn bản này có rất nhiều văn bản gồm các nghị định, thông tư hướng dẫn, tổ chức thực hiện. Sự phức tạp này thực sự đã tạo rào cản nhất định trong quá trình tiếp cận nghiên cứu, tìm hiểu, thực hiện các quy định của pháp luật về ANM của các chủ thể, kể cả đối với các chuyên gia pháp lý. Trên thế giới, đa số các nước chỉ ban hành luật an ninh mạng và các luật có liên quan tạo thành pháp luật về ANM. Việt Nam đang thực hiện song song Luật An toàn thông tin mạng và Luật An ninh mạng, về bản chất cùng điều chỉnh các quan hệ xã hội phát

sinh trên KGM. Để khắc phục tình trạng trên, cần nghiên cứu hợp nhất tối đa, sắp xếp, sửa đổi một số văn bản luật để đảm bảo tính thống nhất cao của hệ thống pháp luật về ANM hiện hành và đơn giản hóa các quy định pháp luật về ANM để dễ tiếp cận. Bên cạnh đó, cần nghiên cứu, sửa đổi Luật Giao dịch điện tử theo hướng mở rộng phạm vi điều chỉnh của luật, bảo đảm giá trị pháp lý của các thông điệp dữ liệu điện tử trước sự phát triển nhanh chóng của KGM khiến nhiều quy định trong Luật Giao dịch điện tử năm 2005 đã trở nên bất cập.

Tính đồng bộ được thể hiện ở việc ban hành đầy đủ các văn bản hướng dẫn thi hành, người dân được kịp thời phổ biến, tuyên truyền, tránh tình trạng văn bản quy phạm pháp luật có hiệu lực khi vẫn còn là luật khung, luật ống mà chưa có hướng dẫn cụ thể để người dân thực hiện. Sau khi Luật An ninh mạng được thông qua, Bộ Công An có trách nhiệm chủ trì, phối hợp với các bộ, ngành liên quan xây dựng trình Chính phủ, Thủ tướng Chính phủ các văn bản quy định chi tiết và hướng dẫn thi hành Luật An ninh mạng. Trước mắt, tập trung nghiên cứu, xây dựng 03 Nghị định và 02 Quyết định, tránh các quy định chung chung như Chính phủ quy định chi tiết..., Chính phủ quy định trình tự, thủ tục áp dụng... Đó là: Nghị định của Chính phủ hướng dẫn một số điều trong Luật An ninh mạng, Nghị định của Chính phủ quy định xử lý vi phạm hành chính về an ninh mạng, Nghị định của Chính phủ quy định chi tiết về trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, Quyết định của Thủ tướng Chính phủ về Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, Quyết định của Thủ tướng Chính phủ về việc lưu trữ dữ liệu và đặt văn phòng đại diện tại Việt Nam.

Hoạt động trên KGM rất đặc thù và khác biệt so với các hoạt động trong các không gian truyền thống. KGM có tính chất không biên giới. Việc xác lập phạm vi thực thi chủ quyền về mặt lãnh thổ đối với hoạt động trên KGM sẽ không dễ dàng. Do đó, cần quy định thống nhất và rõ ràng một số nội dung của các văn bản pháp luật về ANM. Trước hết, cần nghiên cứu xác định và ban hành các quy định hướng dẫn chi tiết và khả thi trong việc xác định phạm vi điều chỉnh về lãnh thổ KGM để pháp luật về ANM có thể được thực thi hiệu quả như quy định các hành vi xúc phạm nhân phẩm người khác, xúc phạm vĩ nhân, danh nhân, anh hùng dân tộc: cần quy định cụ thể, giải thích cụ thể như thế nào là xúc phạm. Bên cạnh đó, đấu tranh bảo vệ ANM là một trong những hoạt động bảo vệ ANM. Do đó cần quy định nội dung này trong Chương quy định về hoạt động bảo vệ ANM trong

Luật An ninh mạng năm 2018. Khắc phục sự trùng lặp về nội dung sử dụng KGM thực hiện hành vi thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội.... tại Điểm d Khoản 1 Điều 8 và Khoản 5 Điều 16 của Luật An ninh mạng năm 2018.

Khắc phục các quy định mâu thuẫn, chồng chéo, chưa thực sự tường minh, khó ADPL vào từng trường hợp cụ thể trong Nghị định 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng, Nghị định 27/2018/NĐ-CP sửa đổi, bổ sung một số điều của Nghị định 72/2013/NĐ-CP, Nghị định 144/NĐCP... Thực tiễn cho thấy cần phải sửa đổi, bổ sung các quy định về an toàn, an ninh mạng quy định từ Điều 38 đến Điều 44 của Nghị định 72/2013/NĐ-CP để đảm bảo phù hợp với Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018.

Thứ hai, bảo đảm tính toàn diện của pháp luật về an ninh mạng

Cần thúc đẩy việc xây dựng các văn bản quy định chi tiết và hướng dẫn thi hành Luật An ninh mạng, đảm bảo pháp luật về ANM có cấu trúc chặt chẽ, đủ chế định cần thiết, trong đó mỗi chế định đảm bảo đủ quy phạm pháp luật điều chỉnh các quan hệ xã hội phát sinh trong lĩnh vực ANM.

Sửa đổi, bổ sung các chế tài trong pháp luật về ANM theo hướng quy định phải đủ sức răn đe, giáo dục đối với tất cả các chủ thể kể cả chủ thể có trách nhiệm quản lý nhà nước về ANM nhằm phòng ngừa, ngăn chặn tội phạm mạng và các hành vi vi phạm hoạt động trên KGM, bảo đảm tất cả các hành vi vi phạm pháp luật về ANM phải được xử lý kịp thời, nghiêm minh. Cần phải kể đến việc Chính phủ đã kịp thời ban hành Nghị định số 15/2020/NĐ-CP ngày 03/02/2020, trong đó quy định tăng mức xử phạt và hình thức xử lý rất nghiêm khắc đối với hành vi vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử. Tuy nhiên, với đặc thù của ANM, ngoài áp dụng các hình phạt chính là cảnh cáo và phạt tiền, cần áp dụng thêm một số hình thức phạt bổ sung, biện pháp khắc phục hậu quả như tước quyền sử dụng giấy phép, giấy chứng nhận, chứng chỉ hành nghề có thời hạn hoặc đình chỉ hoạt động có thời hạn, áp dụng các biện pháp buộc đính chính, buộc xin lỗi, buộc khôi phục, buộc gỡ bỏ, buộc kiểm tra, đánh giá, chứng nhận lại, buộc cải chính kết quả kiểm tra, đánh giá, chứng nhận. Do đó, Chính phủ cần khẩn trương nghiên cứu và ban hành Nghị định quy định xử phạt vi phạm hành chính về an ninh mạng.

Bổ sung và quy định rõ tình tiết giảm nhẹ đối với những người do trình độ, hiểu biết hạn chế, vô tình tiếp tay cho hành vi vi phạm ANM được phát hiện kịp thời, chưa gây hậu quả nghiêm trọng. Quy định tình tiết tăng nặng đối với những kẻ có vai trò khởi xướng, tổ chức trong hành vi vi phạm, ví dụ như hành vi phát tán tin giả trong bối cảnh dịch bệnh diễn biến phức tạp, làm tình hình trầm trọng hơn sẽ bị xử lý hình sự.

Rà soát, sửa đổi, bổ sung Bộ luật Tố tụng hình sự 2015, tập trung vào những quy định về trình tự, thủ tục, thẩm quyền thu thập chứng cứ điện tử và các biện pháp điều tra tố tụng đặc biệt. Đồng thời, nghiên cứu xây dựng Luật về chứng cứ điện tử, chứng cứ số để làm cơ sở áp dụng thống nhất trên thực tế. Trong đó tập trung sửa đổi các quy định về tố tụng, đặc biệt là trình tự, thủ tục, quy trình tố tụng về thu thập chứng cứ là dữ liệu điện tử, quy trình điều tra cho phù hợp. Tập trung vào xây dựng tiêu chuẩn kỹ thuật cho hệ thống, phần mềm tìm kiếm, phát hiện, thu thập, phân tích, giám định, đánh giá và sử dụng chứng cứ điện tử. Tăng cường sử dụng các phương tiện, thiết bị điện tử để hỗ trợ công tác điều tra, truy tố, xét xử tội phạm mạng, tội phạm trong lĩnh vực công nghệ thông tin một cách kịp thời, hiệu quả.

Bên cạnh đó, chúng tôi cho rằng với thực tế số người sử dụng mạng internet ở Việt Nam ngày càng tăng, xây dựng Luật Chính phủ điện tử để hình thành cơ chế minh bạch, rõ ràng đối với người dân là rất cần thiết. Khẩn trương nghiên cứu sửa đổi, đưa những vấn đề liên quan đến bảo vệ ANM để bổ sung vào Luật An ninh quốc gia.

Thứ ba, bảo đảm tính phù hợp, cụ thể.

Trên cơ sở vấn đề bảo mật thông tin cá nhân mang tính nguyên tắc, cần ban hành khung pháp lý phù hợp để bảo vệ bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên KGM. Quy định cụ thể chế tài đối với từng hành vi cố ý như chia sẻ, thích, bình luận, sao chép, tán phát, .v.v.. trên KGM ảnh hưởng nghiêm trọng đến quyền con người, quyền công dân.

Khẩn trương tổng kết thực tiễn, sửa đổi, bổ sung các chế tài cụ thể để quản lý, xử lý kịp thời đối với hoạt động kinh doanh, mua bán các loại tiền ảo, tiền điện tử, tài sản ảo, các loại thẻ thanh toán dịch vụ viễn thông được giao dịch trên môi trường mạng, bảo đảm giá trị pháp lý của các giao dịch điện tử.

Xây dựng quy chế và hướng dẫn thực hiện quy chế về sự phối hợp cụ thể và chặt chẽ hơn nữa giữa các cơ quan quản lý nhà nước về ANM, giữa các cơ quan, tổ chức, doanh nghiệp, cá nhân hoạt động trong lĩnh vực ANM trong nước và nước ngoài, nhất là trong vấn đề lưu trữ dữ liệu và đặt máy chủ tại Việt Nam.

Thứ tư, cơ quan, tổ chức, cá nhân có thẩm quyền ban hành các văn bản pháp luật về ANM phải thực sự am hiểu về công nghệ thông tin, công nghệ số.

Bộ phận pháp chế ở các bộ, ngành cần coi trọng việc lấy ý kiến người dân trong quá trình xây dựng các văn bản hướng dẫn pháp luật về ANM. Người dân là chủ thể quan trọng trong THPL về ANM. THPL về ANM có hiệu quả nhờ phần lớn vào ý thức tuân thủ pháp luật về ANM của người dân. Chủ thể là các cơ quan, tổ chức chủ trì soạn thảo và cơ quan, tổ chức có liên quan có trách nhiệm hướng dẫn, tạo điều kiện để các cơ quan, tổ chức, cá nhân tham gia góp ý kiến về đề nghị xây dựng văn bản pháp luật, dự thảo văn bản quy phạm pháp luật; tổ chức lấy ý kiến của đối tượng chịu sự tác động trực tiếp của văn bản quy phạm pháp luật. Tăng cường các biện pháp, hình thức tuyên truyền để người dân nhận thức, hiểu đúng, từ đó mới có những tham góp giá trị để THPL về ANM ngày càng hiệu quả.

Thứ năm, nâng cao hơn nữa trình độ kỹ thuật xây dựng pháp luật an ninh mạng và đẩy mạnh hợp tác quốc tế trong lĩnh vực an ninh mạng.

Trước hết, phải bảo đảm tính phù hợp với trình độ lập pháp của khu vực và thế giới với ngôn ngữ pháp lý chính xác, thống nhất cách diễn đạt, không quy định lại nội dung đã quy định ở văn bản quy phạm pháp luật khác. Cần hoàn thiện các quy định pháp luật, sửa đổi những quy định thiếu khả thi, bổ sung để điều chỉnh các quy định hiện hành, bãi bỏ những quy định chưa phù hợp, đồng bộ, thậm chí bất cập, chồng chéo với tinh thần của pháp luật về ANM.

Ngoài ra, quán triệt tinh thần Nghị quyết Đại hội XIII của Đảng về tiếp tục khẳng định đường lối đối ngoại độc lập, tự chủ và tích cực, chủ động hội nhập quốc tế. Chủ động, tích cực hội nhập quốc tế hiện nay còn thể hiện ở việc tham gia xây dựng chuẩn mực, "luật chơi" trong quan hệ quốc tế. Mới đây, ngày 7-6-2019, Thủ tướng Chính phủ đã ban hành Chỉ thị số 14/CT-TTg về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam tại GCI, trong đó nhấn mạnh việc "tăng cường hợp tác, tham gia các tổ chức, thỏa thuận quốc tế song phương, đa phương trong lĩnh vực an toàn, an ninh mạng".

Triển khai Chỉ thị số 14-CT-TTg, Việt Nam cần tham gia quá trình thảo luận và xây dựng các quy định, tập quán cũng như luật pháp về không gian mạng với các nước, các tổ chức quốc tế. Điều này đặc biệt có ý nghĩa trong bối cảnh các quá trình này mới ở giai đoạn khởi đầu, giúp Việt Nam có điều kiện và cơ hội để: 1- Xây dựng các quan hệ đối tác và tham gia các thể chế đa phương nhằm tăng cường các hành động và hợp tác tập thể trong việc ngăn ngừa và chống lại những nguy cơ chung về an ninh mạng; 2- Thúc đẩy hợp tác, hành động và ứng phó tập thể đối với các sự cố mạng, góp phần giải quyết các sự cố và ngăn chặn những hoạt động gây hại trên không gian mạng một cách hiệu quả; 3- Thúc đẩy chia sẻ chính sách và xây dựng đồng thuận chung cho sự ổn định không gian mạng toàn cầu nhằm thiết lập các quy chuẩn, quy định quốc tế và biện pháp trừng phạt đối với các hành vi đe dọa trên không gian mạng[40].

Việt Nam cần tích cực, chủ động tham gia, ký kết các Điều ước quốc tế đa phương về ANM; thực hiện tốt các cam kết pháp lý, tăng cường tham gia các diễn đàn về bảo đảm an ninh song phương và đa phương trên KGM, tham gia các tổ chức phòng, chống tội phạm quốc tế nhằm tiếp cận việc chuyển giao công nghệ, kỹ năng phòng, chống tội phạm, nhất là từ FIRST hoặc CAMP. Ngoài ra, Việt Nam cần thúc đẩy thực hiện văn kiện pháp lý về phòng chống tội phạm được ký kết giữa các quốc gia thành viên ASEAN. Đây là cơ hội để Việt Nam tích lũy kinh nghiệm cho các hoạt động hợp tác quốc tế trong THPL về ANM thông qua ký kết các biên bản làm việc, biên bản hợp tác với các cơ quan ANM khu vực và quốc tế. Bên cạnh đó, các diễn đàn hợp tác, hội nghị của các nước ASEAN và khu vực còn là kênh hiệu quả để Việt Nam tranh thủ nắm bắt kiến thức khoa học công nghệ về sử dụng các phương tiện hiện đại, kinh nghiệm phòng ngừa, phát hiện, đấu tranh với tội phạm, đặc biệt là kinh nghiệm điều tra, xét xử vụ án về tội phạm mạng. Điển hình là Hội nghị Bộ trưởng ASEAN về An ninh mạng (AMCC) được tổ chức thường niên; và các cuộc diễn tập ANM do APCERT tổ chức.

Việc tiếp thu, vận dụng có chọn lọc kinh nghiệm của các nước, đặc biệt từ Hoa Kỳ, Liên bang Nga, Đức, Xingapo, Trung Quốc còn giúp Việt Nam từ chủ yếu là tiếp nhận và tìm kiếm sự hỗ trợ THPL về ANM từ các cơ quan an ninh nước ngoài đến việc chủ động tham gia, chia sẻ thông tin liên quan, chuẩn bị các điều kiện cần thiết về tổ chức, bộ máy, trang thiết bị để phối hợp tổ chức thực hiện

[40] Xem: Bùi Thị Long (2023), *Thực hiện pháp luật về an ninh mạng ở Việt Nam*, Nxb Tư pháp, Hà Nội.

và ADPL về ANM, nhất là hoạt động hợp tác với các cơ quan an ninh nước ngoài trong quá trình phát hiện, điều tra, xử lý các hành vi vi phạm pháp luật nhằm bảo đảm hiệu quả hoạt động tổ chức, THPL và ADPL về ANM.

Mặc dù khái niệm an ninh mạng ở mỗi quốc gia có phạm vi khác nhau, nhằm vào các đối tượng khác nhau nhưng nhìn chung, các chiến lược an ninh mạng trên thế giới có 4 điểm tương đồng. Thứ nhất, tăng cường sự phối hợp giữa các chính phủ ở cấp độ chính sách và hoạt động. Thứ hai, tăng cường hợp tác công - tư. Thứ ba, tăng cường hợp tác quốc tế. Thứ tư, những giá trị cơ bản của Internet, bao gồm cả tính riêng tư, tự do ngôn luận và tự do trao đổi thông tin được tôn trọng và nêu bật trong chiến lược an ninh mạng của các quốc gia trên cơ sở bảo đảm tuân thủ pháp luật. Nhà nước cần xây dựng chính sách ngoại giao ANM phù hợp. Chính sách ngoại giao ANM của Việt Nam cần đảm bảo các yếu tố về ANM, về bảo vệ chủ quyền quốc gia trên KGM, có sự kết nối với các tổ chức ANM trong khu vực và quốc tế để học hỏi cách làm hay, kinh nghiệm tốt, nhưng phải tỉnh táo để không bị cuốn vào các cuộc cạnh tranh giữa các nhóm cường quốc về ANM.

Hai là, bảo đảm về tổ chức, bộ máy

Ở Việt Nam, việc tổ chức thực hiện và ADPL về ANM do nhiều chủ thể tiến hành, trong đó việc ADPL về ANM theo chức năng của các cơ quan quản lý nhà nước có thẩm quyền đóng vai trò dẫn dắt, định hướng. Vì thế các cơ quan quản lý nhà nước có thẩm quyền ADPL về ANM phải là lực lượng tiên phong, đi đầu trong ADPL về ANM, cần đẩy mạnh nghiên cứu lý luận, tổng kết thực tiễn; thúc đẩy công tác truyền thông như tuyên truyền, phổ biến, giáo dục pháp luật nhằm thay đổi và nâng cao nhận thức của các tổ chức, doanh nghiệp, cá nhân về vị trí, vai trò của thực hiện và ADPL về ANM, nhấn mạnh, khen thưởng, biểu dương kịp thời các hành vi thực tế, hợp pháp trong thực hiện pháp luật (THPL) và ADPL về ANM.

Các thế lực thù địch lợi dụng KGM để tuyên truyền chống Đảng, Nhà nước, xuyên tạc về Luật An ninh mạng đã tác động tiêu cực tới tư tưởng, nhận thức, quan điểm của một bộ phận cán bộ, đảng viên và người dân, gây nên tâm lý hoang mang, hoài nghi và nguy hiểm nhất là làm suy giảm lòng tin của người dân đối với đường lối, chủ trương, của Đảng, chính sách, pháp luật của Nhà nước. Sau khi Luật An ninh mạng được ban hành, công tác phối hợp giữa Bộ Công an với các Bộ, ban ngành, địa phương, nhất là Bộ Quốc phòng, Bộ Khoa học & Công nghệ

(trước đây là Bộ Thông tin và Truyền thông) và Ban Tuyên giáo Trung ương về tuyên truyền nâng cao nhận thức của người dân, tăng cường xử lý vi phạm pháp luật trên KGM cần phải được tăng cường.

Điều 16 Luật An ninh mạng đã quy định cụ thể các biện pháp phòng ngừa, xử lý thông tin trên KGM có nội dung tuyên truyền chống Nhà nước Cộng hòa XHCN Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống. Điều 26 Luật An ninh mạng đã quy định đầy đủ các nội dung của công tác bảo đảm an ninh thông tin trên KGM. Như vậy, lực lượng chức năng của Bộ Công an, các Bộ, ngành liên quan cũng như UBND các tỉnh, thành phố trực thuộc Trung ương đã có cơ sở pháp lý đủ mạnh, vững chắc trong phòng ngừa, phát hiện, đấu tranh, xử lý thông tin và hành vi tuyên truyền chống Đảng, Nhà nước trên KGM.

Cần phải nâng cao nhận thức và trách nhiệm trong THPL về ANM của các cơ quan quản lý nhà nước thông qua các nội dung sau đây:

- Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, Bộ Thông tin và Truyền thông rà soát, bổ sung nội dung THPL về ANM vào hệ thống giáo trình, tài liệu giảng dạy, nghiên cứu của các Học viện, trường thuộc hệ thống giáo dục đào tạo trong Công an nhân dân và các cơ sở giáo dục quốc phòng, an ninh trên toàn quốc.

- Kịp thời thông tin chính thống đến cán bộ, đảng viên, nhất là vào cácthời điểm trước khi diễn ra các sự kiện quan trọng, sự kiện thu hút sự quan tâm của dư luận, không để các thế lực thù địch lợi dụng tình trạng thiếu thông tin để tuyên truyền xuyên tạc. Có biện pháp kịp thời chấn chỉnh hoạt động đưa tin lệch lạc của báo chí điện tử, các trang mạng trong và ngoài nước.

- Tăng cường công tác quản lý nhà nước đối với các dịch vụ viễn thông, internet, các doanh nghiệp cung cấp, quản lý dịch vụ internet và thông tin điện tử trên mạng, thuê bao di động trả trước, thuê bao 3G, 4G, dịch vụ OTT, thực thi hiệu quả Bộ Quy tắc ứng xử trên KGM, chú trọng bồi dưỡng đạo đức nghề nghiệp trên KGM, một đặc thù rất khó để luật pháp hóa.

- Đẩy mạnh hoạt động kiểm tra, giám sát, theo dõi của Bộ Công an, Bộ Quốc phòng, Bộ Khoa học & Công nghệ (trước đây là Bộ Thông tin và Truyền thông), Ban Cơ yếu trong việc THPL và xử lý nghiêm minh những vi phạm pháp luật về ANM của tổ chức, cá nhân. Chủ động phối hợp nhằm xử lý triệt để các trang web, blog có nội dung tuyên truyền chống Đảng, Nhà nước, tán phát thông

tin giả, vi phạm pháp luật,v.v.. đáp ứng yêu cầu công tác bảo đảm an ninh, trật tự đặt ra trong tình hình mới.

- Chú trọng công tác phối hợp giữa các chủ thể là các cơ quan, tổ chức, doanh nghiệp nhà nước trong triển khai, thực hiện có hiệu quả pháp luật về ANM, trọng tâm là công tác bảo đảm an ninh thông tin mạng một cách tổng thể nhằm khắc phục các tồn tại, hạn chế, góp phần cải thiện hơn nữa xếp hạng của Việt Nam trong Chỉ số năng lực cạnh tranh toàn cầu (GCI). Chỉ định, kiện toàn đầu mối đơn vị chuyên trách về ATTT mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, ANM. Phối hợp chặt chẽ với cơ quan chuyên trách về an toàn, ANM của Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng trong giám sát, chia sẻ thông tin, kiểm tra, đánh giá an toàn, ANM.

- Các cơ quan quản lý nhà nước cần thường xuyên hệ thống hóa, pháp điển hóa pháp luật về ANM để các doanh nghiệp dễ dàng tiếp cận với các quy định mang tính thể chế, thông tin về THPL về ANM, đảm bảo doanh nghiệp được tự do tham gia hoạt động trên KGM mà pháp luật không cấm. Qua đó, tạo điều kiện để doanh nghiệp hoạt động và phát triển bền vững trong KGM, có ý thức tự giác tuân thủ pháp luật, có trách nhiệm với cộng đồng.

- Thực hiện chủ trương Người Việt dùng hàng Việt, ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ của doanh nghiệp Việt Nam đáp ứng yêu cầu, tiêu chuẩn an toàn về ANM theo quy định của pháp luật đối với hệ thống thông tin cấp độ 3 trở lên, các hệ thống thông tin phục vụ Chính phủ điện tử.

- Tiếp tục hoàn thiện cơ chế chính sách, hành lang pháp lý về ATTT mạng, ANM, tội phạm mạng, bảo vệ trẻ em trên môi trường mạng; chiến lược, quy hoạch, kế hoạch phát triển ATTT mạng; phát triển nguồn nhân lực an toàn, ANM; tiêu chuẩn, quy chuẩn kỹ thuật về ATTT mạng. Kịp thời cung cấp thông tin, số liệu về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác trong lĩnh vực an toàn, ANM phục vụ việc đánh giá, xếp hạng chỉ số GCI của Liên minh viễn thông quốc tế (ITU).

- Các cơ quan nhà nước cần thực hiện tổng thể, đồng bộ các biện pháp, tổ chức thực hiện có hiệu quả các văn bản pháp luật về ANM; định kỳ sơ kết, tổng kết, đánh giá công tác thực hiện để có phương hướng, giải pháp trọng tâm trong bảo đảm ANM. Qua đó, góp phần bảo vệ chủ quyền, lợi ích, an ninh quốc gia Việt

Nam trên KGM, hạn chế các thông tin giả, bẩn, độc, các hành vi tiêu cực, ảnh hưởng tới thuần phong mỹ tục, chuẩn mực đạo đức, vi phạm pháp luật về ANM của Việt Nam.

Bên cạnh những bảo đảm nói trên, trong thời gian tới, chúng tôi cho rằng phải xây dựng và củng cố nguồn nhân lực thực hiện pháp luật về an ninh mạng đảm bảo chất lượng, đủ về số lượng, phù hợp về cơ cấu. Cụ thể:

- Bộ máy quản lý nhà nước về công nghệ thông tin truyền thông, viễn thông là yếu tố quan trọng để quản lý nguồn nhân lực và quản lý thông tin trên không gian mạng. Rõ ràng, nhân lực THPL về ANM có trình độ chuyên sâu về công nghệ thông tin, am hiểu về công nghệ số là yếu tố rất quan trọng để quản lý và kiểm soát tốt mạch máu thông tin trên KGM. Tuy nhiên, hiện nay ở Việt Nam, nguồn nhân lực này có xu hướng phát triển theo chiều rộng hơn so với chiều sâu, rõ nhất là trên lĩnh vực bảo mật mạng còn thiếu chuyên gia giỏi, thiếu hụt nhân lực chất lượng cao. Tiếp tục thực hiện hiệu quả chủ trương của Đảng về vai trò của công nghệ thông qua Nghị quyết 36-NQ/TW ngày 01/7/2014 của Bộ Chính trị về phát triển nguồn nhân lực công nghệ thông tin đạt chuẩn quốc tế, bảo đảm đáp ứng nhu cầu trong nước về số lượng và chất lượng, có khả năng cung cấp nguồn nhân lực công nghệ thông tin chất lượng cao cho khu vực và thế giới. Gần đây, Văn kiện Đại hội đại biểu lần thứ XIII của Đảng nhấn mạnh "chú trọng đội ngũ nhân lực kỹ thuật, nhân lực số, nhân lực quản trị công nghệ. Ưu tiên phát triển công nghệ thông tin và truyền thông, công nghiệp…"[41].

- Thực hiện đầy đủ các chính sách nâng cao năng lực công nghệ cho đội ngũ những người làm công tác THPL về ANM ở các bộ, ngành, UBND cấp tỉnh, cơ quan, tổ chức. Đây là hoạt động có ý nghĩa quan trọng trong việc bảo đảm hiệu quả THPL về ANM. Năng lực công nghệ chính là năng lực sáng tạo và phát triển ứng dụng công nghệ của một quốc gia dựa vào trình độ phát triển của công nghệ mạng, công nghệ phần mềm, công nghệ điện tử. Thúc đẩy năng lực tự chủ nghiên cứu, phát triển hệ thống phần cứng, phần mềm, mạng xã hội an toàn do Việt Nam thiết kế và sản xuất. Việc từng bước tự chủ các sản phẩm, phần mềm ứng dụng công nghệ thông tin, công nghệ số giúp Việt Nam khai thác một cách bền vững và tối đa tiện ích của công nghệ, gia tăng lợi ích THPL về ANM.

[41] Đảng Cộng sản Việt Nam (2021), *Nghị quyết Đại hội Đảng toàn quốc lần thứ XIII*, Hà Nội.

- Các cơ quan, tổ chức cần đầu tư phát triển năng lực công nghệ theo hướng tăng cường bảo mật đi đôi với coi trọng phát triển ứng dụng cho nhân lực THPL về ANM nói chung và lực lượng chuyên trách bảo vệ ANM nói riêng. Triển khai đồng bộ các biện pháp đảm bảo an toàn cơ sở dữ liệu và truyền tải trên mạng, các biện pháp giám sát và xử lý sự cố ANM, thiết lập mô hình phòng thủ mạng.

- Để bảo đảm chất lượng và số lượng của nguồn nhân lực THPL về ANM, cần phải thực hiện tốt các nội dung sau:

+ Tăng cường tổ chức các hội thảo, tọa đàm, các khóa tập huấn, bồi dưỡng ngắn hạn bằng nhiều hình thức đảm bảo phù hợp, tiết kiệm, hiệu quả, trong đó coi trọng hình thức trực tuyến qua KGM.

+ Tập trung đổi mới chương trình, đào tạo toàn diện để tạo nguồn nhân lực THPL về ANM, chú trọng cải thiện số lượng, chất lượng, kỹ năng và trình độ công nghệ thông tin, công nghệ số cho lực lượng chuyên trách bảo vệ ANM cũng như lực lượng trực tiếp ADPL về ANM. Thống kê cho thấy, một quốc gia phát triển như Hàn Quốc đến năm 2022 vẫn còn thiếu khoảng 3.290 chuyên gia hàng đầu về công nghệ thông minh[42].

+ Xây dựng chương trình tập huấn đối với đội ngũ cán bộ điều tra, kiểm sát viên, thẩm phán để có khả năng hoàn thành tốt nhiệm vụ khi thực hiện điều tra, tham gia tố tụng các vụ án về ANM.

+ Xây dựng và củng cố tổ chức lực lượng chuyên trách bảo vệ ANM theo hướng bảo đảm tính độc lập, đủ thẩm quyền theo luật định, hoạt động tuân thủ pháp luật. Lực lượng chuyên trách bảo vệ và ADPL về ANM phải là một lực lượng đặc biệt có chức năng, thẩm quyền thẩm định ANM đối với hệ thống thông tin quan trọng về an ninh quốc gia, đồng thời điều tra, xử lý các hành vi vi phạm pháp luật ANM. Chức năng, nhiệm vụ của lực lượng này cần được quy định tại một điều luật riêng biệt. Qua đó, làm tốt nhiệm vụ dự báo và đảm bảo KGM mở rộng đến đâu thì hiệu quả THPL về ANM song hành đến đấy.

+ Lực lượng chuyên trách bảo vệ ANM của Bộ Công an, Bộ Quốc phòng quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia, phải nắm vững pháp luật về ANM, là chủ thể nòng cốt trong các khóa tập huấn Luật An ninh mạng. Nguồn nhân lực chuyên trách bảo vệ ANM phải là nguồn nhân lực

[42] Phạm Long Phương (2018), *"Quản lý thông tin mạng internet ở một số khu vực trên thế giới và kinh nghiệm cho Việt Nam"*, Tạp chí Quản lý nhà nước, Số 8/2018, Hà Nội.

chất lượng cao về công nghệ thông tin, hoạt động chuyên nghiệp và nắm vững kỹ thuật nghiệp vụ chuyên ngành. Lực lượng chuyên trách bảo vệ ANM cần tổ chức và triển khai các biện pháp nghiệp vụ theo quy định của pháp luật để thu thập thông tin, tài liệu về tình hình tại các khu vực, địa điểm phụ trách để phòng ngừa, ngăn chặn tội phạm mạng. Muốn vậy, phải có chế độ đào tạo, bồi dưỡng chuyên sâu đối với đội ngũ chuyên trách bảo vệ ANM không những vững về chính trị, phẩm chất đạo đức tốt, giỏi về chuyên môn, kỹ năng, mà còn am hiểu công nghệ và biết vận dụng tiến bộ, khoa học kỹ thuật vào thực hiện nhiệm vụ giám sát, phòng ngừa, cảnh báo sớm các nguy cơ tấn công mạng.

Đến nay, trong lĩnh vực ANM, mới có Quyết định 05/2015/QĐ-HH ngày 30/01/2015 của Hiệp hội an toàn thông tin Việt Nam về Bộ quy tắc đạo đức nghề nghiệp về an toàn thông tin. Các tổ chức, cá nhân hoạt động trong lĩnh vực cung cấp dịch vụ ATTT cần đảm bảo các quy định đạo đức nghề ATTT. Theo đó, với xã hội, cộng đồng: bảo vệ hệ thống công nghệ thông tin của cơ quan, tổ chức, cá nhân, không thực hiện hành vi xâm hại đến hệ thống; thái độ hành nghề: trung thực, khách quan trong mọi tình huống, đảm bảo tính bí mật, tính toàn vẹn của thông tin; với chất lượng dịch vụ: tận tâm cung ứng dịch vụ ATTT chuyên nghiệp, chính xác, ưu tiên lợi ích của tổ chức, cá nhân; với nghề ATTT: nâng cao trình độ, nỗ lực cung ứng dịch vụ chất lượng và mở rộng, phát triển nghề ATTT trong xã hội. Những nội dung quan trọng này có thể tham khảo để xây dựng bộ văn bản quy định đạo đức nghề nghiệp trong lĩnh vực ANM.

+ Song song với xây dựng nguồn nhân lực THPL về ANM đáp ứng sự phát triển của khoa học công nghệ thông tin, công nghệ số, cần phải hướng đến xây dựng thiết chế bảo vệ ANM gọn nhẹ, nhưng đủ mạnh, đủ năng lực tác chiến trong mọi tình huống. Xây dựng lực lượng chuyên trách bảo vệ ANM có năng lực, trình độ ADPL về ANM ngày càng bảo đảm về chất lượng, số lượng, đáp ứng hiệu quả thực hiện chức năng, nhiệm vụ, quyền hạn mà pháp luật quy định, đồng thời thể hiện sự chuyên biệt của lực lượng chuyên trách bảo vệ, ADPL về ANM so với các lực lượng bảo vệ KGM nói chung. Cần thống nhất Bộ Quốc phòng thành lập lực lượng chuyên trách bảo vệ chủ quyền KGM quốc gia, ở Bộ Công an và Bộ Thông tin truyền thông thành lập lực lượng chuyên trách ADPL về ANM, còn ở các cơ quan nhà nước khác chỉ thành lập bộ phận có trách nhiệm bảo đảm thi hành pháp luật ANM.

Ba là, những bảo đảm về kinh tế, hạ tầng, văn hóa, xã hội

Thứ nhất, đảm bảo cơ sở hạ tầng công nghệ, trang thiết bị, kinh phí cho thực hiện pháp luật về an ninh mạng

Do xuất phát điểm về vốn, hạ tầng khoa học và công nghệ của Việt Nam không cao, do đó trang thiết bị, công nghệ phần mềm, công nghệ mạng... còn chủ yếu phụ thuộc vào các nhà cung cấp nước ngoài do năng lực công nghệ chưa đáp ứng yêu cầu thực tiễn. Điều này tiềm ẩn nguy cơ mất ANM. Việc đầu tư vào cơ sở hạ tầng công nghệ đặc biệt là nền tảng công nghệ số, từng bước không lệ thuộc vào các sản phẩm công nghệ nhập khẩu, qua đó góp phần làm giảm những tác động xấu của những mối đe dọa ANM mang tính chất vật lý là thực hiện chủ trương của Đảng về "ứng dụng và phát triển công nghệ mới, ưu tiên công nghệ số, kết nối 5G và sau 5G, trí tuệ nhân tạo, chuỗi khối, in 3D, internet kết nối vạn vật, an ninh mạng,… để chuyển đổi, nâng cao năng suất, hiệu quả của nền kinh tế".

Trong hoạt động ADPL về ANM bên cạnh cơ chế, chính sách thì đòi hỏi có hạ tầng tiên tiến và nguồn nhân lực có trình độ công nghệ thông tin chuyên sâu. Do đó, giải pháp để bảo đảm thực hiện và ADPL về ANM một cách hiệu quả trước hết chú trọng bảo đảm hai cấu phần cơ bản, mang tính nền tảng trên KGM gồm: (i) không gian vật lý như cơ sở hạ tầng kỹ thuật, trang thiết bị, cơ sở dữ liệu; (ii) không gian xã hội như thể chế, thiết chế, năng lực công nghệ, nguồn nhân lực, ý thức của các chủ thể. Khi chúng ta làm tốt những nội dung này trong điều kiện, hoàn cảnh đất nước còn chưa thực sự tiến bộ về khoa học công nghệ là một nỗ lực rất lớn, cần được ghi nhận. Đây là cơ sở để tiếp tục nghiên cứu, tìm hiểu, thực hiện tự chủ về khoa học công nghệ thông tin, công nghệ số, thúc đẩy sáng tạo, phát triển.

Ưu tiên đầu tư cơ sở hạ tầng công nghệ, trang thiết bị hiện đại cho các cơ quan có lực lượng chuyên trách bảo vệ ANM. Tội phạm mạng hiện nay ngày càng khó lường, hoạt động không đơn lẻ, mà là những tổ chức, cá nhân có trình độ, hoạt động bài bản, có đầu tư. Chúng luôn có những chiêu trò tinh vi để kiếm lợi từ những tổn thất chúng gây ra, ví dụ như phát tán mã độc ransomware ra khắp thế giới. Đó là lý do tại sao hãng phần mềm Microsoft (Hoa Kỳ) đầu tư hơn một tỷ đô mỗi năm cho việc nâng cao năng lực nghiên cứu và phát triển công nghệ mới, một trong số đó là công nghệ phòng chống tội phạm mạng cho đám mây, nơi lưu giữ hàng triệu thông tin dữ liệu. Các loại công nghệ này không chỉ phòng

ngừa, ngăn chặn được các cuộc tấn công mạng, mà nó còn cảnh báo, dự liệu nguy cơ, rủi ro có thể xảy đến.

Với điều kiện là một nước đang phát triển, cơ sở hạ tầng công nghệ, trang thiết bị, kinh phí cũng như trình độ khoa học, kỹ thuật và công nghệ còn hạn chế, chưa có nhiều kinh nghiệm trong quản lý nhà nước về ANM, việc nghiên cứu, tiếp thu một cách có chọn lọc những kinh nghiệm của các quốc gia đi trước trong THPL về ANM như Hoa Kỳ, Nga, Trung Quốc là rất cần thiết. Do đó, thay vì nhập khẩu, gia công, lắp ráp các trang thiết bị, sản phẩm mạng, sử dụng các dịch vụ mạng nước ngoài, Việt Nam cần có chính sách kinh phí theo hướng ưu tiên, tập trung nguồn lực tài chính để nghiên cứu, xây dựng nền công nghiệp ANM có khả năng sản xuất, kiểm tra, đánh giá và thẩm định các sản phẩm và dịch vụ mạng nội sinh. Muốn có lời giải hiệu quả đối với THPL về ANM, những gì thuộc về Việt Nam, thuộc về người Việt Nam phải được đặt trên lãnh thổ Việt Nam và được sử dụng theo quy định của pháp luật Việt Nam về ANM. Chính phủ cần triển khai đồng bộ các biện pháp nhằm từng bước đảm bảo và nâng cao năng lực độc lập và tự chủ về ANM như đầu tư cho các cơ quan, doanh nghiệp để thúc đẩy phát triển doanh nghiệp khoa học, công nghệ, doanh nghiệp công nghệ cao, phát triển công nghệ thông tin, công nghệ số, làm chủ và phát triển các sản phẩm ứng dụng công nghệ tiên tiến trong lĩnh vực ANM dành cho người Việt. Phấn đấu đến năm 2030, tỷ lệ doanh nghiệp có hoạt động đổi mới sáng tạo đạt 40%[43].

Thứ hai, nâng cao nhận thức và trách nhiệm thực hiện pháp luật về an ninh mạng cho doanh nghiệp

Các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ internet, viễn thông, các doanh nghiệp hoạt động trong lĩnh vực tài chính, ngân hàng, thanh toán điện tử, thương mại điện tử là chủ thể quan trọng trong THPL về ANM. Thực tiễn cho thấy, hầu hết các doanh nghiệp trong nước kinh doanh trên môi trường mạng hiện nay chỉ quan tâm đến lợi nhuận mà chưa quan tâm đúng mức đến nâng cao năng lực bảo vệ ANM, nhất là công tác phòng ngừa sự cố ANM, khả năng bị tấn công, xâm nhập, chiếm quyền điều khiển, chiếm đoạt dữ liệu luôn ở mức cao. Nhiều trường hợp chỉ chú trọng công tác bảo vệ ANM khi đã xảy ra hậu quả, thiệt hại.

[43] 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.

Tình hình liên quan tới các cuộc tấn công mạng mang mục đích lừa đảo, mã độc tống tiền, sự cố hệ thống, thu thập dữ liệu, trộm cắp thông tin, lộ lọt thông tin của các doanh nghiệp diễn biến phức tạp cộng với các loại tội phạm trong lĩnh vực tài chính, ngân hàng, thương mại điện tử như lắp đặt thiết bị công nghệ cao Skimming tại các máy ATM nhằm trộm cắp thông tin, làm giả thẻ ngân hàng, chiếm đoạt tiền, hoạt động rút tiền mặt, đáo hạn ngân hàng bằng thẻ tín dụng, giả mạo website dịch vụ chuyển tiền quốc tế, các ngân hàng thương mại hoặc giả làm nhân viên ngân hàng, tòa án, công an,.v.v.. để lừa người dùng truy cập, yêu cầu cung cấp các thông tin bảo mật bao gồm số tài khoản, tài khoản đăng nhập, mật khẩu, mã OTP, lừa đảo chiếm đoạt tài sản trên KGM.

Điều này đặt ra vấn đề muốn nâng cao nhận thức và trách nhiệm THPL về ANM cho doanh nghiệp, trước hết cần phải tăng cường phổ biến, tuyên truyền pháp luật ANM với các hình thức phù hợp, hiệu quả để các doanh nghiệp quan tâm, đầu tư, tìm kiếm các giải pháp bảo mật thế hệ mới, nâng cao năng lực bảo vệ ANM đối với hoạt động kinh doanh, củng cố uy tín và niềm tin của khách hàng khi sử dụng dịch vụ. Lấy tần suất sử dụng dịch vụ của khách hang là một loại thước đo hiệu quả KGM an toàn và từ ý thức cảnh giác bảo mật thông tin, dữ liệu, các doanh nghiệp cần chủ động nghiên cứu, đầu tư cơ sở hạ tầng kỹ thuật và các giải pháp công nghệ phù hợp, bảo đảm an toàn, an ninh thông tin, củng cố khả năng phòng ngừa, chống lại các sự cố mạng.

Bên cạnh đó, hiện nay một số dịch vụ xuyên biên giới của các doanh nghiệp cung cấp các dịch vụ về mạng xuyên biên giới vào Việt Nam đã trở thành môi trường thực hiện các hành vi phạm tội nhưng chưa có biện pháp, chính sách ngăn chặn triệt để. Đây không chỉ là thách thức riêng đối với Việt Nam, mà là thách thức chung với tất cả các quốc gia trên thế giới. Do đó, cần huy động tổng thể các nguồn lực và lực lượng tham gia hoạt động trên KGM để giải quyết được bài toán phức tạp này. Cùng với sự quản lý của Nhà nước, với sự nỗ lực của các cơ quan có thẩm quyền ADPL về ANM, cần phải tăng cường tuyên truyền tới người dân, doanh nghiệp với các hình thức phù hợp để các doanh nghiệp cung cấp dịch vụ xuyên biên giới nhận thức đầy đủ về vai trò cũng như trách nhiệm quan trọng trong giám sát, hạn chế các hành vi vi phạm pháp luật về ANM.

Trên cơ sở nhận thức đúng đắn trách nhiệm đối với THPL về ANM, các doanh nghiệp sẽ có ý thức tuân thủ các quy định pháp luật về ANM như: không

sản xuất, lưu hành những dịch vụ, sản phẩm vi phạm pháp luật; không để dịch vụ của mình trở thành môi trường thực hiện hành vi phạm tội như tán phát thông tin vi phạm pháp luật, thực hiện hành vi vi phạm pháp luật; chủ động loại bỏ, xử lý các nguy cơ, hành vi vi phạm pháp luật trên dịch vụ, sản phẩm của mình; chú trọng bảo vệ ANM cho hệ thống dịch vụ của doanh nghiệp cung cấp cho khách hàng; bảo vệ dữ liệu cá nhân của khách hàng, không mua bán, giao dịch dữ liệu cá nhân của khách hàng với bên thứ ba mà không được sự đồng ý hoặc thực hiện các hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân; tăng cường phối hợp với cơ quan chức năng có thẩm quyền trong phòng ngừa, điều tra, xử lý các hành vi vi phạm pháp luật có liên quan tới dịch vụ, sản phẩm do doanh nghiệp cung cấp.

Để phòng ngừa, xử lý hành vi vi phạm pháp luật về ANM cần có sự phối hợp, tham gia chia sẻ của các doanh nghiệp cung cấp dịch vụ viễn thông, internet, ứng dụng công nghệ thông tin trong việc thu thập dấu vết, chứng cứ điện tử. Các doanh nghiệp hoạt động trong lĩnh vực công nghệ thông tin, viễn thông có trách nhiệm lưu trữ và cung cấp các dữ liệu điện tử. Điều này có vai trò rất quan trọng, nâng cao hiệu quả hoạt động điều tra, truy tố, xét xử các vụ án về tội phạm mạng, góp phần thực hiện tốt pháp luật về ANM. Nếu các doanh nghiệp hoạt động kinh doanh về cung cấp hạ tầng mạng và dịch vụ internet, viễn thông, các doanh nghiệp hoạt động trong lĩnh vực tài chính, ngân hàng… nhận thức tốt những yêu cầu nêu trên thì hoạt động ADPL về ANM của các cơ quan có thẩm quyền sẽ đạt hiệu quả cao hơn.

Thứ ba, nâng cao hơn nữa nhận thức của cá nhân trong thực hiện pháp luật an ninh mạng

Có thể khẳng định, tất cả thời gian, công sức và tiền của đầu tư vào hệ thống phòng ngừa, ngăn chặn các hành vi vi phạm ANM sẽ trở nên vô nghĩa nếu cá nhân người dùng mạng không ý thức rõ ràng và đầy đủ trách nhiệm trong việc bảo vệ ANM. Nhận thức, quan niệm, thái độ,... của người dân đối với pháp luật về ANM đều tác động trực tiếp đến thực hiện và ADPL về ANM, từ đó hình thành hành vi thực hiện đúng đắn hay vi phạm pháp luật. Ý thức trách nhiệm của cá nhân người dùng mạng phải được coi là một loại văcxin đặc hiệu, trở thành viên gạch lửa để tạo bức tường có sức đề kháng chắc chắn trước các thách thức đối với KGM. Ý thức pháp luật càng cao thì người dân càng nhận thức đúng về pháp luật, có niềm tin đối với pháp luật, tự giác THPL và ngược lại. Việc người dân có ý thức tôn

trọng chính sách, pháp luật, quy tắc kỹ thuật nghiệp vụ về ANM, thực hiện tốt Bộ quy tắc ứng xử trên mạng xã hội do Bộ Thông tin và Truyền thông ban hành năm 2021 góp phần quan trọng trong việc bảo vệ ANM. Mặt trái của công nghệ thông tin chính là sự thiếu ý thức của người dân khi tham gia hoạt động trên KGM. Không tuân thủ pháp luật về ANM là vấn đề nhức nhối và làm mất trật tự an toàn xã hội trên KGM. Việc người dùng mạng nhận thức đúng các quy định pháp luật về ANM cũng như thái độ tự giác tuân thủ, thi hành, sử dụng pháp luật của các doanh nghiệp cộng với thái độ nghiêm minh trong ADPL của các cơ quan quản lý nhà nước sẽ bảo đảm hiệu quả THPL về ANM.

Để nâng cao nhận thức của người dân về THPL về ANM, cần thực hiện các biện pháp sau:

Một là, Tăng cường tuyên truyền, phổ biến pháp luật từ phía các cơ quan quản lý nhà nước đối với người dân. Công tác này có vai trò đặc biệt cần thiết đối với lĩnh vực mới mẻ như THPL về ANM. Cần phải đổi mới theo hướng đa dạng hóa các hình thức tuyên truyền về THPL về ANM. Nhanh chóng thiết lập hệ thống phương tiện truyền thông khai thác từ hạ tầng mạng sẵn có để thông tin cho các cơ quan, tổ chức, cá nhân về pháp luật ANM. Kết hợp nội dung tuyên truyền, phổ biến pháp luật về ANM và các văn bản hướng dẫn thi hành với nhiều phương thức linh hoạt, đa dạng, dễ hiểu. Đặc biệt quan tâm đến đối tượng tuyên truyền là người dân vì đây là lĩnh vực pháp luật mới, có nhiều quy định liên quan đến khoa học công nghệ, công nghệ thông tin, công nghệ số có đặc điểm không thực sự dễ hiểu, dễ bị kẻ xấu lợi dụng xuyên tạc. Các cơ quan quản lý nhà nước cần tích cực, chủ động tận dụng lợi thế của KGM để đẩy mạnh tuyên truyền phổ biến rộng rãi pháp luật về ANM trên các phương tiện truyền thông bằng nhiều hình thức đa dạng, phong phú, dễ hiểu, dễ tiếp cận. Thực hiện cập nhật các phóng sự, phim tài liệu về các vấn đề THPL về ANM. Xây dựng các chuyên đề, chuyên trang, chuyên mục về ANM trên các phương tiện truyền thông từ trung ương đến địa phương, đặc biệt là các chương trình tin tức để truyền thông kịp thời những vấn đề về THPL về ANM.

Hai là, cần phải chú trọng hơn nữa biện pháp tăng cường tuyên truyền, nâng cao ý thức tuân thủ pháp luật về ANM cho mọi chủ thể trong xã hội. Tăng cường tuyên truyền để các chủ thể trong xã hội cảnh giác trước những luận điệu tuyên truyền phản động của các thế lực thù địch trên KGM. Tuyên truyền nội dung, kết

quả của công tác đấu tranh chống tham nhũng, làm trong sạch nội bộ. Đẩy mạnh công tác điều tra, nghiên cứu dư luận xã hội về ANM làm cơ sở cho Đảng, Nhà nước ban hành chủ trương, chính sách, pháp luật, tạo sự đồng thuận trong xã hội, từ đó hạn chế nảy sinh và loại bỏ tâm lý bức xúc, bất mãn, thể hiện thái độ tiêu cực của người dân trên KGM.

Pháp luật về an ninh mạng quy định rõ các hành vi bị nghiêm cấm, nếu thiếu hiểu biết, không nắm vững quy định thì ranh giới giữa người dùng mạng thông thái và "giặc mạng" (tin tặc, tội phạm mạng) rất mong manh. Hiện nay nhiều người lầm tưởng rằng khi tham gia KGM, họ thoải mái thể hiện ý kiến như chia sẻ, phát tán thông tin mà không bị bất cứ ai kiểm soát. Một cuộc khảo sát cho thấy chỉ có khoảng 50% người dùng mạng dành thời gian đọc toàn bộ tin nhắn trước khi có hành động tiếp theo. Điều đó cho thấy tầm quan trọng của công tác phổ biến, tuyên truyền để người dân hiểu, nắm vững và tuân thủ các quy định pháp luật về ANM. Nếu coi KGM là một quốc gia thì đây là quốc gia có số dân đông nhất thế giới. Vì lẽ đó, thiệt hại và hậu quả khi KGM bị xâm phạm có sức tàn phá nền kinh tế-xã hội còn ghê gớm hơn cả năng lượng hạt nhân.

Tổ chức nhiều Hội nghị, Hội thảo về áp dụng pháp luật an ninh mạng nhằm tuyên truyền, phổ biến nội dung Luật An ninh mạng, nâng cao nhận thức, hiểu biết để nhận diện các mối đe dọa đến từ KGM, đặc biệt ở các khu vực nguy cơ cao. Tổ chức các diễn đàn, các hội thảo chuyên sâu bàn các giải pháp nâng cao hiệu quả ADPL về ANM. Tổ chức các phong trào, cuộc thi tìm hiểu về ANM và thực hiện, ADPL về ANM. Cần có kiến thức nhất định để phân biệt nguy cơ gây mất ANM đến từ yếu tố chính sách, kỹ thuật hay con người. Nguy cơ bắt nguồn từ phần cứng thiết bị kết nối mạng, từ môi trường truyền dẫn có/không dây, từ nhóm quản trị hệ thống hay nhóm vận hành hệ thống, từ nhóm người dùng hay từ chính những bất cẩn của cá nhân người dùng...

Đối với người dùng mạng là trẻ em: triển khai, lồng ghép chương trình giáo dục về THPL về ANM vào các cấp học từ cấp tiểu học trở lên. Đặc biệt lưu ý các tầng lớp thanh niên, thiếu niên, sinh viên, học sinh nhằm trang bị kiến thức, kỹ năng nhận biết, phòng chống tội phạm xâm hại trẻ em qua KGM. Tăng cường bồi dưỡng, giáo dục để các em có kỹ năng sử dụng các thiết bị mạng an toàn, tự bảo vệ bản thân, có tinh thần cảnh giác cao độ trước các nguy cơ xâm hại. Các doanh

nghiệp cung ứng dịch vụ trên mạng cũng cần nghiên cứu và thiết lập bộ lọc kiểm soát người dùng về độ tuổi, giới tính... để có hình thức đáp ứng phù hợp.

Ba là đẩy mạnh tuyên truyền, phổ biến, nâng cao nhận thức của người dân về các dấu hiệu, thủ đoạn của hành vi vi phạm pháp luật về an ninh mạng và hình thành ý thức cảnh giác của người dân trong phòng ngừa tội phạm mạng nói riêng và vi phạm pháp luật về an ninh mạng nói chung.

Hoạt động đào tạo về an ninh mạng phải được tiến hành ở tất cả các bậc học, phù hợp với trình độ nhận thức của các đối tượng học sinh, sinh viên khác nhau. Đối với cấp học trung học cơ sở và trung học phổ thông, nội dung hướng dẫn giáo dục về an toàn thông tin, kỹ năng tương tác an toàn, lành mạnh trên không gian mạng và khả năng tự đọc tin, phân biệt được nội dung an toàn có thể tiếp cận và loại bỏ những nội dung, thông tin sai lệch, thông tin vi phạm pháp luật cần được lồng ghép linh hoạt vào các môn học như: Tin học, Giáo dục công dân hoặc các hoạt động ngoại khóa,... Đối với đối tượng sinh viên, những nội dung pháp luật về an ninh mạng, các nguy cơ và kỹ năng cần thiết để tương tác lành mạnh, an toàn trên không gian mạng phải được quy định là nội dung bắt buộc trong các học phần: Pháp luật đại cương, Tin học ứng dụng...

Trên thực tế, ở Việt Nam hiện nay, nhận thức của không ít cơ quan, tổ chức, doanh nghiệp và người dân còn nhiều hạn chế. Phần lớn các cá nhân, tổ chức chưa đủ kiến thức, kỹ năng để tự bảo vệ mình trước những mối đe dọa về an toàn thông tin nói riêng và an ninh mạng nói chung. Nhiều người sử dụng mạng chưa có các kỹ năng bảo vệ an toàn thông tin của bản thân, phòng tránh lây nhiễm mã độc; vẫn thường xuyên sử dụng các phần mềm không có bản quyền, truy cập website không uy tín, hoặc không sử dụng các phần mềm bảo vệ thiết bị và dữ liệu. Vì vậy, người sử dụng mạng cần được trang bị đầy đủ và cập nhật thường xuyên kiến thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng, phòng ngừa các hành vi xâm phạm an ninh mạng.

Các cơ quan quản lý nhà nước về an toàn, an ninh mạng có thể nghiên cứu, xuất bản, phát hành miễn phí "Cẩm nang phòng chống tội phạm mạng và tội phạm công nghệ cao"; "Cẩm nang an toàn trên không gian mạng";... để cung cấp các kiến thức, kỹ năng nhận biết, tự phòng ngừa, ứng phó với các nguy cơ khi các cơ quan, tổ chức, cá nhân tham gia vào không gian mạng. Một trong những phương thức hiệu quả có thể áp dụng trên diện rộng đó là việc Bộ Thông tin và Truyền

thông đã và đang triển khai các chiến dịch tuyên truyền về nhận diện và phòng chống lừa đảo trực tuyến với sự tham gia của tất cả các bộ, ngành, địa phương; xuất bản hơn 2.000 video, 1.550 bài viết tuyên truyền... đạt 2,1 tỷ lượt xem từ 20,85 triệu người dùng.

TÀI LIỆU THAM KHẢO

1. Bộ Chính trị (2018), *Nghị quyết số 29-NQ/TW ngày 25/7/2018 về Chiến lược bảo vệ Tổ quốc trên không gian mạng*, Hà Nội.
2. Bộ chính trị (2024), *Nghị quyết số 57-NQ/TW ngày 22/12/2024 về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia*, Hà Nội.
3. Bộ Công an (2018), *Báo cáo số 403/BC-A68-P1 ngày 13/3/2018 "Báo cáo sơ kết 04 năm thực hiện Chỉ thị số 28-CT/TW của Ban Bí thư về tăng cường công tác bảo đảm an ninh, an toàn thông tin mạng trong tình hình mới"*, Hà Nội.
4. Bộ Thông tin và Truyền thông (2018), *Quyết định số 1616/QĐ-BTTTT ngày 05 tháng 10 năm 2018 Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin*, Hà Nội.
5. Bộ Thông tin và Truyền thông (2021), *An ninh mạng trong cuộc cách mạng công nghiệp 4.0*, Nxb Thông tin và Truyền thông, Hà Nội.
6. Bộ Thông tin và Truyền thông (2021), *An toàn thông tin khi sử dụng mạng xã hội*, Nxb Thông tin và Truyền thông, Hà Nội.
7. Bộ Thông tin và Truyền thông (2021), *Sách trắng Công nghệ thông tin và Truyền thông Việt Nam*, Nxb Thông tin và Truyền thông, Hà Nội.
8. Bộ Thông tin và Truyền thông (2022), *Báo cáo tổng hợp quy hoạch phát triển mạng lưới cơ sở báo chí, phát thanh, truyền hình, thông tin điện tử, cơ sở xuất bản thời kỳ 2021 - 2030, tầm nhìn đến năm 2050*, Hà Nội.
9. Nguyễn Mai Bộ (2018), *"Về khái niệm, đối tượng bảo vệ an ninh mạng và giải thích từ ngữ tại Điều 3 Dự thảo Luật An ninh mạng"*, Tạp chí Nghiên cứu lập pháp, số 7/359, Hà Nội.
10. Ngọc Châm và Mạnh Sơn (2016), *"Các giải pháp đảm bảo an ninh truyền thông trên mạng Internet"*, Tạp chí Công nghệ và Thông tin, 31/08/2016.
11. Phan Công Chính, Lê Hoàng Việt Lâm (2022), *Nguy cơ đe dọa đến an ninh con người tại Việt Nam và những vấn đề đặt ra đối với công tác phòng ngừa, ngăn chặn*, Nxb Công an nhân dân, Hà Nội.

12. Chính phủ (1997), *Nghị định số 21-CP của Chính phủ ngày 05/3/1997 ban hành Quy chế tạm thời về quản lý, thiết lập, sử dụng mạng Internet*, Hà Nội.
13. Chính phủ (2001), *Nghị định số 55/NĐ-CP của Chính phủ ngày 23/8/2001 về quản lý, cung cấp và sử dụng dịch vụ Internet*, Hà Nội.
14. Chính phủ (2009), *Nghị định số 28/2009/NĐ-CP của Chính phủ ngày 20/03/2009 quy định về việc xử phạt hành chính trong việc quản lý và sử dụng dịch vụ Internet và thông tin điện tử trên Internet*, Hà Nội.
15. Chính phủ (2013), *Nghị định số 72/2013/NĐ-CP của Chính phủ ngày 15/7/2013 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng*, Hà Nội.
16. Chính phủ (2020), *Nghị định số 15/2020/NĐ-CP của Chính phủ ngày 03/02/2020 quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử*, Hà Nội.
17. Chính phủ (2022), *Nghị định số 14/2022/NĐ-CP ngày 27/01/2022 sửa đổi Nghị định 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử và Nghị định 119/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong hoạt động báo chí, hoạt động xuất bản*, Hà Nội.
18. Chính phủ (2022), *Nghị định số 53/2022/NĐ-CP của Chính phủ ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng*, Hà Nội.
19. Chính phủ (2023), *Nghị định số 13/2023/NĐ-CP của Chính phủ ngày 17/4/2023 về bảo vệ dữ liệu cá nhân*, Hà Nội.
20. Chính phủ (2024), *Nghị định số 147/2024/NĐ-CP của Chính phủ ngày 09/11/2024 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng*, Hà Nội.
21. Chính phủ (2024), *Nghị định số 147/2024/NĐ-CP của Chính phủ ngày 13/11/2023 quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện*, Hà Nội.
22. Chính phủ (2019), *Nghị quyết số 22/NQ-CP ngày 18 tháng 10 năm 2019 của Chính phủ ban hành Chương trình hành động thực hiện Nghị quyết số*

30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược an ninh mạng quốc gia, Hà Nội.

23. Cục An toàn thông tin – Bộ TTTT (2016), *Báo cáo về "Không gian mạng và các nguy cơ mất an toàn thông tin"*, Hà Nội.
24. Cục Thống kê, Tòa án nhân dân Tối cao, *Báo cáo công tác ngành Tòa án* (các năm 2021 – 2024)
25. Cao Anh Dũng (2022), *"Bảo vệ an ninh quốc gia trên không gian mạng trong bối cảnh Cuộc cách mạng công nghiệp lần thứ tư theo định hướng Đại hội XIII của Đảng"*, Tạp chí Tuyên giáo, https://tuyengiao.vn/bao-ve-nen-tang-tu-tuong-cua-dang/bao-ve-an-ninh-quoc-gia-tren-khong-gian-mang-trong-boi-canh-cuoc-cach-mang-cong-nghiep-lan-thu-tu-theo-dinh-huong-dai-137538
26. Đinh Thế Cường (2019), *"Bộ Tư lệnh 86 với việc đấu tranh chống các luận điệu sai trái, thù địch trên không gian mạng"*, http://tapchiqptd.vn/vi/75-nam-ngay-truyen-thong-tcct/bo-tu-lenh-86-voi-viec-dau-tranh-chong-cac-luan-dieu-sai-trai-thu-dich-tren-khong-gian-mang/14811.html, truy cập ngày 18-12-2022.
27. Đảng Cộng sản Việt Nam (2011), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XI*, Nxb Chính trị Quốc gia Sự thật, Hà Nội.
28. Đảng Cộng sản Việt Nam (2016), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XII*, Nxb Chính trị Quốc gia Sự thật, Hà Nội.
29. 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.
30. Dorothea Czarnecki (2016), *Báo cáo đánh giá năng lực bảo vệ trẻ em trên môi trường mạng tại Việt Nam*, Bộ Lao động, Thương binh và Xã hội, UNICEF, Hà Nội.
31. Hoàng Phương Đông (2021), *Xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng*, Luận văn Thạc sĩ luật học, Đại học Luật Hà Nội, Hà Nội.
32. Nguyễn Thị Trường Giang, Trần Thái Hà, Đỗ Thu Hiền, Đoàn Thị Quỳnh Nga (2024), *An ninh mạng ở Việt Nam hiện nay – Những vấn đề lý luận và thực tiễn*, Nxb. Đại học Quốc gia Hà Nội, Hà Nội.

33. Phạm Thị Việt Hà (2021*), Pháp luật về xử phạt hành chính trong lĩnh vực an toàn, an ninh mạng giai đoạn hiện nay*, Luận văn Thạc sĩ luật học, Đại học Luật Hà Nội, Hà Nội.
34. Trần Văn Hòa (2015), *Phòng chống tội phạm sử dụng công nghệ cao*, Nxb Công an nhân dân, Hà Nội.
35. Đỗ Quí Hoàng (2021), *Pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao - những vấn đề đặt ra đối với Việt Nam*, Luận án Tiến sĩ luật học, Đại học Luật Hà Nội, Hà Nội.
36. Học viện An ninh nhân dân (2015), *Giáo trình Những vấn đề cơ bản về phòng, chống tội phạm sử dụng công nghệ cao*, Nxb CAND, Hà Nội.
37. Trần Mạnh Hùng (2020), *Gián điệp mạng từ góc nhìn mối đe dọa an ninh toàn cầu,* Nxb Công an nhân dân, Hà Nội.
38. Tô Lâm (2017), *An ninh truyền thống trong thời kỳ hội nhập quốc tế*, Nxb Công an nhân dân, Hà Nội.
39. Tô Lâm (2021), *Chủ quyền không gian mạng: Yêu cầu thách thức và nghĩa vụ quốc gia*, Nxb Công an nhân dân, Hà Nội.
40. Nguyễn Việt Lâm (2019), *Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam*, Nxb Chính trị quốc gia, Hà Nội.
41. Liên minh Châu Âu (2001), *Công ước Budapest về tội phạm mạng*, được Hội đồng liên minh Châu âu thông qua ngày 23/11/2001, tại Budapest, Hungary.
42. Bùi Thị Long (2023), *Thực hiện pháp luật về an ninh mạng ở Việt Nam*, Nxb Tư pháp, Hà Nội.
43. Nguyễn Thành Lợi (2014), *Tác nghiệp báo chí trong môi trường truyền thông hiện đại*, Nxb Thông tin và Truyền thông, Hà Nội
44. Mark Rhodes-Ousley (2013), *Tham khảo toàn diện về bảo mật thông tin (The Complete Reference Information Security)*, Bản dịch xuất bản lần 2, Hà Nội.
45. C.L.Montesquieu (bản dịch tiếng Việt 1996), *Tinh thần pháp luật*, Nxb Giáo dục, Hà Nội.
46. Ngân hàng Nhà nước Việt Nam (2015), *Thông tư 31/2015/TT-NHNN ngày 28/12/2015 quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng*, Hà Nội.

47. Phạm Long Phương (2018), *"Quản lý thông tin mạng internet ở một số khu vực trên thế giới và kinh nghiệm cho Việt Nam"*, Tạp chí Quản lý nhà nước, Số 8/2018, Hà Nội.
48. Quốc hội (2004), *Luật An ninh quốc gia*, Nxb Chính trị quốc gia, Hà Nội
49. Quốc hội, *Luật Giao dịch điện tử năm 2005*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2006.
50. Quốc hội, *Luật Công nghệ thông tin năm 2006*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2007.
51. Quốc hội, *Luật Công nghệ cao năm 2008*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2009.
52. Quốc hội, *Luật Viễn thông năm 2009*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2010.
53. Quốc hội, *Luật An toàn thông tin mạng năm 2015*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2016.
54. Quốc hội (2018), *Luật An ninh mạng 2018*, Nxb Chính trị quốc gia Sự thật, Hà Nội.
55. Quốc hội (2018), *Luật Bảo vệ bí mật nhà nước*, Nxb Chính trị quốc gia Sự thật, Hà Nội.
56. Quốc hội (2018), *Luật Công an nhân dân năm 2018,* Nxb. Chính trị quốc gia Sự thật, Hà Nội.
57. Thủ tướng Chính phủ (2022), *Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 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*, Hà Nội.
58. Thủ tướng Chính phủ (2022), *Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam*, Hà Nội.
59. Nguyễn Anh Tuấn, Trần Thị Lâm Thi (Đồng chủ biên) (2020), *Một số vấn đề cơ bản của Luật An ninh mạng*, Nxb Công an nhân dân, Hà Nội.
60. Nguyễn Anh Tuấn (2023), *Bảo vệ an ninh, trật tự ở Việt Nam trong bối cảnh chuyển đổi số*, Nxb Công an nhân dân, Hà Nội.

61. Trung tâm từ điển học (2010), *Từ điển tiếng Việt 2010*, Nxb Đà Nẵng, Hà Nội.
62. Trường Đại học CSND (2022), *Giáo trình Lý luận Nhà nước và pháp luật, Luật nhà nước*, TP Hồ CHí Minh
63. Viện Khoa học pháp lý (2006), *Từ điển luật học*, Nxb Từ điển Bách khoa và Nxb Tư pháp, Hà Nội, tr.648.
64. Nguyễn Như Ý (1999), *Đại từ điển Tiếng Việt*, Nxb Văn hóa thông tin, Thành phố Hồ Chí Minh.