

Một số nội dung cần chú trọng trong truyền thông, phổ biến pháp luật về an ninh mạng hiện nay

Key issues in communicating and disseminating cyber security law today

ThS. NGUYỄN THANH HẢI

Trường Đại học Vinh; Email: hainguyenntv@gmail.com

Ngày nhận bài: 23/5/2026

Ngày phản biện: 02/6/2026

Ngày duyệt đăng: 25/6/2026

Chủ đề của bài viết thuộc lĩnh vực: Báo chí truyền thông

Tóm tắt: Bài viết nhấn mạnh vai trò của tuyên truyền, phổ biến pháp luật về an ninh mạng ở Việt Nam trong bối cảnh chuyển đổi số. Trên cơ sở Luật An ninh mạng năm 2025, bài viết làm rõ khái niệm, một số nội dung cần chú trọng trong truyền thông, phổ biến pháp luật về an ninh mạng hiện nay. Qua đó khẳng định việc nâng cao nhận thức pháp luật là giải pháp quan trọng nhằm bảo vệ chủ quyền quốc gia và bảo đảm môi trường mạng an toàn, lành mạnh.

Từ khóa: an ninh mạng; không gian mạng; Luật An ninh mạng 2025; truyền thông, phổ biến, pháp luật; chuyển đổi số.

Abstract: This article emphasizes the role of communication and legal dissemination regarding cyber security in Vietnam in the context of digital transformation. Based on the 2025 Law on Cyber Security, the article clarifies the concept of cyber security and identifies several key issues that should be emphasized in current communication and legal dissemination activities. It argues that improving public legal awareness is a crucial solution for safeguarding national sovereignty and ensuring a safe and healthy cyberspace.

Keywords: cyber security; cyberspace; 2025 Law on Cyber Security; communication and legal dissemination; digital transformation.

1. Đặt vấn đề

Sự phát triển mạnh mẽ của công nghệ số, Internet, trí tuệ nhân tạo và các nền tảng trực tuyến đang làm thay đổi sâu sắc mọi mặt của đời sống xã hội. Không gian mạng trở thành môi trường quan trọng phục vụ hoạt động quản lý nhà nước, phát triển kinh tế, giáo dục, văn hóa, giao tiếp xã hội và hội nhập quốc tế. Bên cạnh những lợi ích to lớn, không gian mạng cũng đặt ra nhiều thách thức đối với an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức và cá nhân. Trong những năm gần đây, tình trạng tấn công mạng, lừa đảo trực tuyến, đánh cắp dữ liệu cá nhân, phát tán thông tin giả, thông tin sai sự thật, xâm hại trẻ em trên không gian mạng và các hành vi vi phạm pháp luật khác có chiều hướng gia tăng, gây ảnh hưởng tiêu cực đến sự phát triển bền vững của đất

nước. Điều đó đòi hỏi phải tiếp tục hoàn thiện hệ thống pháp luật và nâng cao hiệu quả tổ chức thực hiện các biện pháp bảo vệ an ninh mạng. Ngày 10/12/2025, Quốc hội khóa XV đã thông qua Luật An ninh mạng năm 2025 (Luật số 116/2025/QH15), có hiệu lực thi hành từ ngày 01/7/2026 và thay thế Luật An ninh mạng năm 2018. Luật đã được bổ sung những điểm mới, tạo lập khuôn khổ pháp lý toàn diện hơn về bảo vệ an ninh mạng, bảo vệ dữ liệu, bảo vệ trẻ em trên không gian mạng và xác định rõ trách nhiệm của các cơ quan, tổ chức, doanh nghiệp và cá nhân trong bảo đảm an ninh mạng quốc gia.

Trong bối cảnh đó, công tác truyền thông, phổ biến pháp luật về an ninh mạng có ý nghĩa đặc biệt quan trọng nhằm nâng cao nhận thức pháp luật, xây dựng văn hóa ứng xử trên môi trường số, phát huy vai trò

của toàn xã hội trong phòng ngừa, phát hiện và đấu tranh với các hành vi vi phạm pháp luật trên không gian mạng. Trên cơ sở nghiên cứu các quy định của Luật An ninh mạng năm 2025, bài viết tập trung làm rõ một số nội dung cần chú trọng trong hoạt động truyền thông, phổ biến pháp luật về an ninh mạng hiện nay.

2. Phương pháp nghiên cứu

Trên cơ sở kế thừa các nghiên cứu trước, tác giả sử dụng phương pháp nghiên cứu tài liệu, trong đó các văn bản của Nhà nước về vai trò của tuyên truyền, phổ biến pháp luật về an ninh mạng ở Việt Nam trong bối cảnh chuyển đổi số. Phương pháp thu thập số liệu thông qua các số liệu thứ cấp được đăng tải trên web của các tổ chức trong và ngoài nước.

3. Kết quả nghiên cứu và thảo luận

Thứ nhất, làm rõ các hệ thống khái niệm làm nền tảng cho quản lý và bảo vệ an ninh mạng

Trước hết, cần làm rõ và thống nhất nhận thức về một số khái niệm liên quan đến an ninh mạng, từ đó tổ chức tuyên truyền, phổ biến sâu rộng trong quần chúng nhân dân. Trên thế giới hiện nay vẫn tồn tại nhiều cách tiếp cận khác nhau về khái niệm không gian mạng. Thực tiễn cho thấy, trên phạm vi quốc tế hiện nay vẫn chưa tồn tại một khái niệm thống nhất về không gian mạng. Cụ thể, Cộng hòa Liên bang Đức tiếp cận không gian mạng như một không gian ảo bao trùm toàn bộ các hệ thống công nghệ thông tin được kết nối trên phạm vi toàn cầu. New Zealand xác định không gian mạng là hệ thống toàn cầu bao gồm hạ tầng mạng công nghệ thông tin, mạng viễn thông và các hệ thống máy tính, nơi diễn ra các hoạt động giao tiếp của con người. Trong khi đó, Vương quốc Anh cho rằng không gian mạng là một trường tương tác gồm các hệ thống mạng kỹ thuật số có chức năng lưu trữ, xử lý và truyền tải thông tin. Liên minh Viễn thông quốc tế (ITU) thuộc Liên hợp quốc quan niệm không gian mạng là môi trường bao gồm người sử dụng, Internet, các thiết bị tính toán cùng các ứng dụng, dịch vụ kết nối trực tiếp hoặc gián tiếp với Internet và các mạng thế hệ mới. Theo các Chỉ thị số 54 về An ninh quốc gia và Chỉ thị số 23 năm 2008 về An ninh nội địa của Tổng thống Hoa Kỳ, không gian mạng được xác định là mạng lưới kết nối các cơ sở hạ tầng quan trọng, bao gồm Internet, mạng viễn thông, hệ thống

máy tính và các hệ thống xử lý, điều khiển trong các ngành công nghiệp trọng yếu; đồng thời là môi trường ảo nơi diễn ra sự trao đổi thông tin và tương tác giữa con người không bị giới hạn bởi không gian và thời gian.

Ở Việt Nam, Luật An ninh mạng được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam thông qua ngày 10/12/2025 đã có sự điều chỉnh quan trọng về kỹ thuật lập pháp khi tiến hành chuẩn hóa và thống nhất hệ thống các khái niệm cơ bản liên quan đến an ninh mạng. Đây được xem là bước tiến có ý nghĩa nền tảng trong hoạt động xây dựng pháp luật, góp phần khắc phục tình trạng thiếu đồng bộ, phân tán giữa các khái niệm “an toàn thông tin mạng” và “an ninh mạng” trong giai đoạn trước. Trên cơ sở đó, Luật tạo lập khuôn khổ pháp lý rõ ràng, thống nhất, phục vụ hiệu quả cho việc tổ chức thi hành trong thực tiễn. Cụ thể, trước hết Luật đã thống nhất cách tiếp cận và phạm vi của khái niệm “an ninh mạng”. Theo khoản 1 Điều 2, an ninh mạng được hiểu là trạng thái ổn định, an toàn của không gian mạng; trong đó các hệ thống thông tin, dữ liệu và hoạt động trên môi trường mạng được bảo đảm không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, cũng như quyền và lợi ích hợp pháp của cơ quan, tổ chức và cá nhân. Việc quy định theo hướng này giúp mở rộng phạm vi điều chỉnh, đồng thời tạo sự thống nhất trong nhận thức và áp dụng pháp luật.

Tiếp theo, Luật đã phân định rõ khái niệm “an ninh thông tin mạng” như một cấu phần mang tính kỹ thuật trong tổng thể an ninh mạng. Theo khoản 2 Điều 2, an ninh thông tin mạng tập trung vào việc bảo đảm các thuộc tính cơ bản của thông tin như tính toàn vẹn, tính bảo mật và tính sẵn sàng, đồng thời ngăn ngừa các hành vi truy cập, sử dụng, tiết lộ, thay đổi hoặc phá hoại trái phép thông tin trên không gian mạng. Quy định này góp phần tách bạch giữa yếu tố kỹ thuật - công nghệ và yêu cầu quản lý an ninh mạng mang tính tổng hợp về chính trị, pháp lý và xã hội, qua đó tạo điều kiện thuận lợi cho việc xây dựng các giải pháp bảo vệ hạ tầng thông tin.

Một điểm mới quan trọng khác là việc bổ sung và ghi nhận khái niệm “an ninh dữ liệu” như một nội dung pháp lý độc lập. Theo khoản 3 Điều 2, an ninh dữ liệu được hiểu là sự bảo đảm về chất lượng dữ liệu

và quá trình thu thập, xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội và chuyển đổi số quốc gia, đồng thời phòng ngừa các hành vi truy cập, khai thác, tiết lộ, chỉnh sửa hoặc phá hoại dữ liệu trái phép. Quy định này phản ánh sự thay đổi trong tư duy quản lý, trong đó dữ liệu được xác định là nguồn lực quan trọng cần được bảo vệ như một tài sản chiến lược trong kỷ nguyên số.

Bên cạnh đó, Luật cũng xác lập khái niệm “không gian mạng quốc gia” tại khoản 6 Điều 2, theo đó đây là phần không gian mạng thuộc chủ quyền, quyền tài phán và quyền kiểm soát của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam. Quy định này có ý nghĩa đặc biệt quan trọng khi khẳng định cơ sở pháp lý cho việc thực thi chủ quyền số, đồng thời bảo đảm quyền quản lý của Nhà nước đối với các hoạt động diễn ra trong phạm vi không gian mạng thuộc lãnh thổ quốc gia trong bối cảnh hội nhập và kết nối toàn cầu ngày càng sâu rộng. Tổng thể, việc chuẩn hóa và thống nhất hệ thống khái niệm trong Luật An ninh mạng năm 2025 đã góp phần xác định rõ ràng phạm vi điều chỉnh và đối tượng áp dụng của Luật. Đồng thời, điều này giúp hạn chế tình trạng chồng chéo, thiếu thống nhất trong quản lý nhà nước, tạo nền tảng pháp lý vững chắc cho việc triển khai đồng bộ và hiệu quả các quy định pháp luật về an ninh mạng trong giai đoạn mới.

Thông qua việc hướng dẫn, làm rõ các khái niệm cơ bản của Luật An ninh mạng năm 2025, quần chúng nhân dân, đặc biệt là thế hệ trẻ, sẽ có nhận thức tổng quát và đầy đủ hơn về an ninh mạng cũng như yêu cầu phòng, chống các hành vi vi phạm pháp luật trên không gian mạng. Việc phổ biến khái niệm này giúp người dân hiểu rằng không gian mạng không chỉ giới hạn ở Internet mà bao gồm nhiều hệ thống thông tin quan trọng liên quan trực tiếp đến an ninh quốc gia.

Thứ hai, truyền thông phổ biến sâu rộng một số điểm mới các quy định của Luật An ninh mạng năm 2025

Một là, cần đẩy mạnh truyền thông về nhóm quy định liên quan đến hành vi bị nghiêm cấm trong không gian mạng. Đây là nội dung có ý nghĩa đặc biệt quan trọng nhằm định hướng hành vi xã hội trong môi trường số. Theo đó, người dân cần được phổ biến rõ các hành vi như: sử dụng không gian mạng để chống phá Nhà nước, tuyên truyền thông tin sai sự thật,

xuân tạc, kích động gây rối, xúc phạm danh dự, nhân phẩm, hoặc thực hiện các hành vi vi phạm đạo đức xã hội, thuần phong mỹ tục. Đồng thời, cần nhấn mạnh các hành vi liên quan đến tấn công mạng, xâm nhập trái phép hệ thống thông tin, phát tán mã độc, đánh cắp dữ liệu hoặc lợi dụng không gian mạng để thực hiện hành vi phạm tội.

Đối với luật an ninh mạng 2025 đã bổ sung, cụ thể hóa các hành vi bị nghiêm cấm gắn với sự phát triển của khoa học, công nghệ và các phương thức hoạt động mới trên không gian mạng. Luật An ninh mạng 2025 đã kịp thời cập nhật và luật hóa nhiều hành vi vi phạm mới phát sinh trong quá trình ứng dụng công nghệ cao, khắc phục khoảng trống pháp lý của các quy định trước đây, tạo cơ sở pháp lý đầy đủ cho công tác phòng ngừa, đấu tranh và xử lý vi phạm trên không gian mạng.

- Kiểm soát chặt chẽ việc lạm dụng trí tuệ nhân tạo và công nghệ mới (Deepfake, AI): Trước thực trạng tội phạm sử dụng công nghệ trí tuệ nhân tạo để giả mạo hình ảnh, giọng nói, video nhằm lừa đảo, chiếm đoạt tài sản hoặc xâm phạm danh dự, nhân phẩm của người khác, Luật đã bổ sung quy định nghiêm cấm hành vi sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái pháp luật tại điểm g khoản 2 Điều 7. Quy định này tạo cơ sở pháp lý trực tiếp để xử lý các hành vi lừa đảo qua cuộc gọi video giả mạo, cũng như các hành vi bôi nhọ, vu khống bằng công nghệ ghép hình, ghép video.

- Nhận diện và phòng, chống các phương thức xâm phạm an ninh kinh tế trên không gian mạng: Luật đã cụ thể hóa các hành vi bị nghiêm cấm liên quan đến lĩnh vực tài chính, tiền tệ và thị trường số. Theo điểm d khoản 1 Điều 7, hành vi đưa thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, kinh doanh đa cấp, chứng khoán, trái phiếu... gây hoang mang dư luận và thiệt hại cho nền kinh tế bị nghiêm cấm. Đồng thời, tại điểm e khoản 4 Điều 13, Luật xác định hành vi thiết lập, cung cấp dịch vụ trái phép cho các sàn giao dịch tài sản số, tiền ảo hoặc tổ chức hoạt động kinh doanh đa cấp trái phép trên không gian mạng là hành vi xâm phạm an ninh quốc gia.

- Tăng cường bảo vệ danh tính số và dữ liệu cá nhân: Đáp ứng yêu cầu cấp thiết trong bối cảnh dữ liệu

cá nhân bị khai thác, mua bán trái phép tràn lan, Luật nghiêm cấm tuyệt đối hành vi thu thập, sử dụng, phát tán, trao đổi, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân theo quy định tại điểm h khoản 2 Điều 7. Bên cạnh đó, các hành vi sử dụng danh tính giả, giấy tờ giả để đăng ký tài khoản ngân hàng, tài khoản số hoặc tạo lập “tài khoản rác” phục vụ hoạt động phạm tội cũng được xác định là hành vi xâm phạm trật tự, an toàn xã hội tại điểm g khoản 4 Điều 13, qua đó góp phần ngăn chặn các hành vi lừa đảo, rửa tiền trên không gian mạng. Những quy định nêu trên đã mở rộng đáng kể phạm vi điều chỉnh của Luật An ninh mạng 2025, tạo cơ sở pháp lý vững chắc để các lực lượng chức năng chủ động phòng ngừa, phát hiện và xử lý kịp thời các nguy cơ an ninh mạng mới phát sinh, đáp ứng yêu cầu bảo vệ an ninh quốc gia, trật tự, an toàn xã hội trong bối cảnh chuyển đổi số toàn diện.

Việc tuyên truyền rõ các chế tài này sẽ góp phần răn đe, phòng ngừa vi phạm, đồng thời nâng cao ý thức tuân thủ pháp luật trong cộng đồng. Luật An ninh mạng được thông qua là cơ sở pháp lý quan trọng để bảo vệ an ninh quốc gia; xử lý đối với các hành vi vi phạm pháp luật. Cá nhân và tổ chức phải chịu trách nhiệm về các hành vi và ứng xử trên mạng xã hội, đồng thời phối hợp với các cơ quan chức năng để xử lý các hành vi, nội dung thông tin vi phạm pháp luật.

Hai là, công tác truyền thông cần tập trung phổ biến các quy định về bảo vệ dữ liệu cá nhân và an ninh thông tin trong Luật An ninh mạng năm 2025. Luật an ninh mạng 2025 khẳng định bảo đảm an ninh dữ liệu là bộ phận quan trọng của bảo vệ an ninh mạng. Điều này thể hiện sự thay đổi căn bản trong tư duy quản lý nhà nước về an ninh mạng, từ cách tiếp cận chủ yếu tập trung bảo vệ hạ tầng kỹ thuật sang bảo vệ dữ liệu - tài nguyên số có giá trị cốt lõi của nền kinh tế số và xã hội số. Lần đầu tiên, khái niệm “an ninh dữ liệu” được luật hóa một cách đầy đủ, xác lập vị trí độc lập trong hệ thống pháp luật, với các nội dung trọng tâm sau đây:

- Xác lập an ninh dữ liệu như một khái niệm pháp lý độc lập và toàn diện. Khác với các quy định trước đây chỉ đề cập rải rác đến bảo vệ dữ liệu dưới góc độ an toàn thông tin, Luật An ninh mạng 2025 đã đưa ra định nghĩa riêng về “an ninh dữ liệu” tại khoản 3 Điều 2. Theo đó, an ninh dữ liệu không chỉ dừng lại ở việc

phòng, chống truy cập trái phép, phá hoại hoặc đánh cắp dữ liệu, mà còn bao gồm yêu cầu bảo đảm tính toàn vẹn, độ chính xác, tính sẵn sàng và khả năng khai thác hiệu quả của dữ liệu nhằm phục vụ phát triển kinh tế - xã hội và chuyển đổi số quốc gia. Quy định này đặt nền tảng pháp lý cho việc bảo vệ chất lượng và giá trị sử dụng của dữ liệu, coi dữ liệu là nguồn lực chiến lược của quốc gia.

- Thiết lập hành lang pháp lý toàn diện để bảo đảm an ninh dữ liệu. Tại Điều 26, Luật quy định cụ thể các biện pháp bảo đảm an ninh dữ liệu, bao gồm việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật; sử dụng mật mã bảo vệ dữ liệu; kiểm soát nhân sự tham gia xử lý dữ liệu; và thực hiện đánh giá rủi ro an ninh dữ liệu một cách định kỳ. Đáng chú ý, Luật lần đầu tiên đặt ra yêu cầu kiểm tra, đánh giá việc chuyển dữ liệu xuyên biên giới, qua đó tăng cường năng lực quản lý nhà nước đối với dòng chảy dữ liệu, nhất là dữ liệu quan trọng, dữ liệu cốt lõi, nhằm ngăn ngừa nguy cơ thất thoát hoặc bị lợi dụng gây phương hại đến lợi ích quốc gia.

- Tăng cường chế tài xử lý vi phạm dữ liệu tại Việt Nam. Nhằm xử lý triệt để tình trạng thu thập, mua bán, trao đổi dữ liệu trái phép, Luật quy định rõ tại điểm h khoản 2 Điều 7 hành vi thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân là hành vi bị nghiêm cấm. Đây là cơ sở pháp lý quan trọng để tăng cường khả năng kiểm soát, thanh tra, xử lý vi phạm và bảo vệ quyền, lợi ích hợp pháp của người dùng Việt Nam.

Thông qua các quy định nêu trên, Luật An ninh mạng 2025 đã hình thành khung pháp lý tương đối đầy đủ về an ninh dữ liệu, tạo nền tảng cho việc phòng ngừa, phát hiện và xử lý các hành vi xâm phạm dữ liệu, qua đó góp phần bảo vệ an ninh quốc gia, trật tự, an toàn xã hội và củng cố niềm tin của người dân, doanh nghiệp trong môi trường số.

Đây là một trong những nội dung mới, có tính thời sự cao trong bối cảnh dữ liệu trở thành nguồn tài nguyên quan trọng của nền kinh tế số. Việc thu thập, xử lý, lưu trữ và chia sẻ dữ liệu phải tuân thủ chặt chẽ quy định pháp luật, bảo đảm quyền của chủ thể dữ liệu và an toàn thông tin trong toàn bộ quá trình xử lý. Qua đó, nâng cao nhận thức của người dân và doanh nghiệp về trách nhiệm bảo vệ dữ liệu, đồng thời phòng ngừa nguy cơ rò rỉ, mua bán và khai thác

dữ liệu trái phép.

Ba là, cần tăng cường phổ biến, truyền thông các quy định về trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng. Luật An ninh mạng năm 2025 đã thể hiện bước chuyển quan trọng trong tư duy quản lý nhà nước đối với các doanh nghiệp cung cấp dịch vụ trên không gian mạng, từ cơ chế phối hợp mang tính khuyến khích, tự nguyện trước đây sang cơ chế xác lập nghĩa vụ pháp lý bắt buộc, có tính ràng buộc cao. Quy định này được áp dụng thống nhất đối với cả doanh nghiệp trong nước và doanh nghiệp nước ngoài hoạt động tại Việt Nam, qua đó bảo đảm sự bình đẳng về nghĩa vụ pháp lý và tăng cường hiệu lực quản lý nhà nước trong lĩnh vực an ninh mạng. Trên cơ sở đó, Luật đã cụ thể hóa nhiều nhóm trách nhiệm của doanh nghiệp nhằm nâng cao tính chủ động, kịp thời và hiệu quả trong công tác phòng ngừa, phát hiện và xử lý thông tin vi phạm pháp luật trên không gian mạng. Trước hết, Luật quy định rõ về thời hạn bắt buộc trong việc xử lý thông tin vi phạm, qua đó khắc phục tình trạng chậm trễ trong việc ngăn chặn, gỡ bỏ các nội dung xấu, độc trên môi trường mạng. Theo quy định tại điểm b khoản 2 Điều 25, doanh nghiệp có trách nhiệm thực hiện việc ngăn chặn chia sẻ, xóa bỏ thông tin hoặc gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm trong thời hạn chậm nhất là 24 giờ kể từ khi nhận được yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an. Đối với các trường hợp khẩn cấp, có nguy cơ gây ảnh hưởng nghiêm trọng đến an ninh quốc gia hoặc trật tự, an toàn xã hội, thời gian xử lý được rút ngắn xuống không quá 06 giờ, nhằm bảo đảm khả năng phản ứng nhanh và hạn chế tối đa tác động tiêu cực phát sinh. Tiếp theo, Luật đặt ra yêu cầu doanh nghiệp phải chủ động thực hiện các biện pháp kỹ thuật và quản trị nhằm phòng ngừa rủi ro ngay từ giai đoạn đầu. Theo khoản 1 Điều 14, các chủ quản hệ thống thông tin và doanh nghiệp cung cấp dịch vụ trên không gian mạng có trách nhiệm triển khai đồng bộ các giải pháp kỹ thuật, công nghệ và quản lý để phát hiện sớm, ngăn chặn và loại bỏ kịp thời các thông tin vi phạm pháp luật. Các hành vi này bao gồm, nhưng không giới hạn ở việc tuyên truyền chống phá Nhà nước, kích động gây rối, phá hoại an ninh, trật tự công cộng hoặc xâm phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân. Quy định này thể

hiện rõ xu hướng chuyển từ “xử lý bị động” sang “quản lý chủ động” trong bảo đảm an ninh mạng.

Bên cạnh đó, Luật còn thiết lập cơ chế xử lý nghiêm đối với các trường hợp vi phạm nghiêm trọng thông qua việc quy định trách nhiệm ngừng hoặc không cung cấp dịch vụ cho các đối tượng có hành vi vi phạm. Theo điểm c khoản 2 Điều 25, khi có yêu cầu từ lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, doanh nghiệp có nghĩa vụ thực hiện biện pháp tạm dừng hoặc chấm dứt cung cấp dịch vụ đối với tổ chức, cá nhân đăng tải, phát tán thông tin có nội dung vi phạm nghiêm trọng. Quy định này có ý nghĩa quan trọng trong việc cắt đứt nguồn phát tán thông tin vi phạm, đồng thời tăng cường tính răn đe và hiệu quả phòng ngừa trong thực tiễn. Tổng thể, các quy định nêu trên đã góp phần nâng cao vai trò, trách nhiệm xã hội và pháp lý của doanh nghiệp trong môi trường số.

Bốn là, cần chú trọng tăng cường phổ biến, truyền thông các quy định về nội dung bảo vệ trẻ em trên không gian mạng, đồng thời mở rộng yêu cầu bảo vệ đối với người cao tuổi và người có khó khăn trong nhận thức, làm chủ hành vi. Đây là nhóm đối tượng dễ bị tổn thương và chịu nhiều rủi ro trong môi trường số. Luật An ninh mạng 2025 tiếp tục khẳng định quan điểm nhất quán của Nhà nước trong việc bảo vệ con người làm trung tâm của quá trình chuyển đổi số, đặc biệt là trẻ em và các nhóm đối tượng dễ bị tổn thương trên không gian mạng. Luật không chỉ tăng cường các biện pháp bảo vệ trẻ em, mà còn mở rộng yêu cầu bảo vệ đối với người cao tuổi và người có khó khăn trong nhận thức, làm chủ hành vi. Các quy định này được thiết kế theo hướng xác định rõ trách nhiệm của các chủ thể liên quan, bảo đảm sự phối hợp đồng bộ giữa gia đình, nhà trường và doanh nghiệp cung cấp dịch vụ trên không gian mạng.

- Luật hóa trách nhiệm của gia đình trong việc quản lý, giám sát hoạt động của trẻ em trên không gian mạng. Nhằm khắc phục tình trạng trẻ em tự ý đăng ký, sử dụng các dịch vụ mạng xã hội, trò chơi trực tuyến và các dịch vụ giá trị gia tăng khác mà không có sự kiểm soát, khoản 2 Điều 16 quy định rõ cha, mẹ hoặc người giám hộ có trách nhiệm quản lý, giám sát việc trẻ em truy cập, sử dụng thông tin và dịch vụ trên không gian mạng. Trường hợp trẻ em sử dụng các dịch

vụ yêu cầu đăng ký tài khoản, cha, mẹ hoặc người giám hộ phải đứng tên đăng ký và chịu trách nhiệm đối với việc sử dụng tài khoản đó. Quy định này nhằm gắn trách nhiệm pháp lý cụ thể của gia đình với hành vi của trẻ em, qua đó tăng cường hiệu quả phòng ngừa từ sớm.

- Xác lập nghĩa vụ chủ động của doanh nghiệp trong việc phòng ngừa và xử lý nội dung xâm hại trẻ em. Luật chuyển cách tiếp cận từ yêu cầu xử lý bị động sang yêu cầu doanh nghiệp phải chủ động bảo vệ người sử dụng, nhất là trẻ em. Theo quy định tại khoản 3 Điều 16 và khoản 2 Điều 25, doanh nghiệp cung cấp dịch vụ trên không gian mạng có trách nhiệm triển khai các biện pháp kỹ thuật và biện pháp quản lý cần thiết để phát hiện, ngăn chặn, gỡ bỏ kịp thời các thông tin có nội dung xâm hại trẻ em, kích động bạo lực, khiêu dâm, đồi trụy hoặc lôi kéo trẻ em tham gia các hành vi vi phạm pháp luật. Đồng thời, doanh nghiệp phải thiết lập cơ chế, công cụ thuận tiện để người sử dụng phản ánh, tố giác nhanh chóng các nội dung xấu, độc liên quan đến trẻ em.

- Mở rộng phạm vi bảo vệ đối với người cao tuổi và người có khó khăn trong nhận thức, làm chủ hành vi. Xuất phát từ thực tiễn cho thấy người cao tuổi và người có hạn chế về nhận thức, khả năng làm chủ hành vi là nhóm đối tượng dễ trở thành nạn nhân của các hành vi lừa đảo, chiếm đoạt tài sản trên không gian mạng, khoản 5 Điều 16 đã bổ sung quy định yêu cầu cơ quan nhà nước có thẩm quyền và doanh nghiệp cung cấp dịch vụ trên không gian mạng phải có cơ chế hỗ trợ phù hợp, cảnh báo sớm các nguy cơ, đồng thời ưu tiên tiếp nhận, xử lý các phản ánh, khiếu nại, tố giác liên quan đến hành vi lừa đảo mạng đối với nhóm đối tượng này.

Các quy định trên đã thiết lập một hành lang pháp lý tương đối toàn diện, buộc các chủ thể liên quan cùng tham gia trách nhiệm bảo vệ trẻ em và các nhóm yếu thế trên không gian mạng. Trọng tâm của các quy định không chỉ là xử lý vi phạm, mà là phòng ngừa, ngăn chặn từ sớm, qua đó góp phần xây dựng môi trường số an toàn, lành mạnh và nhân văn. Do đó công tác truyền thông cần hướng tới việc nâng cao nhận thức của gia đình, nhà trường và xã hội về vai trò bảo vệ trẻ em; đồng thời trang bị cho trẻ em kỹ năng sử dụng Internet an toàn, nhận diện nguy cơ và biết cách

tự bảo vệ trong môi trường mạng.

4. Kết luận

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ và không gian mạng ngày càng trở thành một bộ phận thiết yếu của đời sống kinh tế - xã hội, công tác truyền thông, phổ biến pháp luật về an ninh mạng giữ vai trò đặc biệt quan trọng trong việc bảo đảm an ninh quốc gia, trật tự an toàn xã hội và bảo vệ quyền, lợi ích hợp pháp của tổ chức, cá nhân. Luật An ninh mạng năm 2025 đã bổ sung và hoàn thiện nhiều quy định mới về khái niệm, hành vi bị nghiêm cấm, bảo vệ dữ liệu, trách nhiệm của doanh nghiệp cũng như cơ chế bảo vệ các nhóm yếu thế trên không gian mạng. Đây là cơ sở pháp lý quan trọng để tăng cường hiệu lực quản lý nhà nước và nâng cao hiệu quả phòng ngừa, đấu tranh với các hành vi vi phạm trong môi trường số. Luật đã tạo lập hành lang pháp lý tương đối toàn diện, vừa kế thừa, vừa phát triển so với giai đoạn trước, đáp ứng yêu cầu quản lý nhà nước trong điều kiện khoa học – công nghệ phát triển nhanh chóng và phức tạp. Trong thời gian tới, cần tiếp tục đổi mới nội dung và phương thức truyền thông pháp luật theo hướng hiện đại, linh hoạt, phù hợp với từng nhóm đối tượng; đồng thời tăng cường sự phối hợp giữa các cơ quan nhà nước, doanh nghiệp và toàn xã hội. Chỉ khi công tác tuyên truyền được triển khai đồng bộ, thường xuyên và hiệu quả thì Luật An ninh mạng năm 2025 mới thực sự đi vào đời sống, góp phần xây dựng không gian mạng an toàn, lành mạnh, ổn định và phát triển bền vững./.

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.
2. Bộ Chính trị. (2018). Nghị quyết số 30-NQ/TW ngày 25/7/2018 về Chiến lược an ninh mạng quốc gia.
3. Đảng Cộng sản Việt Nam. (2021). Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII, Nxb Chính trị quốc gia Sự thật, Hà Nội.
4. Quốc hội. (2018). Luật An toàn thông tin mạng số 86/2015/QH13, Hà Nội.
5. Quốc hội. (2025). Luật An ninh mạng số 116/2025/QH15, Hà Nội.