

CÁC HÀNH VI BỊ NGHIÊM CẤM THEO ĐIỂM Đ KHOẢN 2 ĐIỀU 7 LUẬT AN NINH MẠNG 2025: THỰC TIỄN VÀ NHỮNG VẤN ĐỀ PHÁP LÝ ĐẶT RA

LÊ THỊ LINH
Trưởng Đại học Điện lực

Nhận bài ngày 10/7/2026. Sửa chữa xong 15/8/2026. Duyệt đăng 20/8/2026.

Abstract

This article provides an overview of the principal provisions of the 2025 Law on Cybersecurity, with particular emphasis on the prohibited acts specified in Point (đ), Clause 2, Article 7. By clarifying the content and significance of this provision, the article examines the occurrence of these prohibited acts in cyberspace and identifies the associated risks and legal issues arising in practice. On this basis, it proposes preventive measures and recommendations to enhance the effectiveness of law enforcement, thereby contributing to ensuring security and safety in cyberspace.

Keywords: 2025 Law on Cybersecurity, cybersecurity, data security, prohibited acts.

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số diễn ra sâu rộng cùng với sự gia tăng về quy mô, tính chất và mức độ tinh vi của các hành vi vi phạm pháp luật trên không gian mạng (KGM), yêu cầu hoàn thiện cơ chế pháp lý về an ninh mạng ngày càng trở nên cấp thiết. Luật An ninh mạng 2025 của Việt Nam được ban hành nhằm tiếp tục hoàn thiện hành lang pháp lý về an ninh mạng (ANM), tăng cường hiệu lực, hiệu quả quản lý nhà nước, chủ động phòng ngừa, phát hiện và xử lý các nguy cơ, hành vi xâm phạm an ninh, an toàn trên KGM; đồng thời bảo vệ quyền và lợi ích hợp pháp của cá nhân, tổ chức, doanh nghiệp, trong đó có các nhóm chủ thể dễ bị tổn thương trong môi trường số. Trên cơ sở khái quát những nội dung cơ bản của Luật An ninh mạng 2025 (Báo Điện tử Chính phủ, 2026), bài viết tập trung nghiên cứu các hành vi bị nghiêm cấm về an ninh, an toàn thông tin mạng được quy định tại điểm đ khoản 2 Điều 7, bao gồm: "Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên KGM". Qua đó, bài viết phân tích nội hàm pháp lý của các hành vi nêu trên, đối chiếu với diễn biến thực tiễn và nhận diện những vấn đề đặt ra trong công tác phòng ngừa, đấu tranh, xử lý vi phạm, góp phần làm rõ giá trị và ý nghĩa thực tiễn của quy định pháp luật trong bảo đảm an ninh, an toàn trên KGM.

2. Nội dung nghiên cứu

2.1. Bối cảnh ban hành và khái quát những nội dung cơ bản của Luật An ninh mạng năm 2025

Sự phát triển nhanh chóng của khoa học, công nghệ, Internet và quá trình chuyển đổi số đang làm thay đổi sâu sắc phương thức vận hành của Nhà nước, hoạt động sản xuất, kinh doanh và đời sống xã hội. KGM ngày càng trở thành một bộ phận thiết yếu của đời sống kinh tế - xã hội, đồng thời là môi trường quan trọng để thực hiện các hoạt động quản lý nhà nước, cung cấp dịch vụ công, giao dịch thương mại, thanh toán điện tử, trao đổi thông tin và kết nối xã hội. Tuy nhiên, cùng với những cơ hội mà chuyển đổi số mang lại, KGM cũng phát sinh ngày càng nhiều nguy cơ và thách thức đối với an ninh quốc gia, trật tự, an toàn xã hội và quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Thực tiễn cho

Email: linhlet@epu.edu.vn

thấy, các phương thức, thủ đoạn sử dụng KGM để thực hiện hành vi vi phạm pháp luật ngày càng đa dạng và có tính chất phức tạp. Bên cạnh các hành vi tấn công, phá hoại hệ thống thông tin, xâm nhập trái phép, đánh cắp hoặc làm lộ dữ liệu, môi trường số còn bị lợi dụng để thực hiện lừa đảo chiếm đoạt tài sản, tổ chức đánh bạc, xâm phạm quyền sở hữu trí tuệ, mua bán hàng hóa, dịch vụ thuộc danh mục cấm và nhiều hành vi vi phạm pháp luật khác. Đặc biệt, sự phát triển của trí tuệ nhân tạo, công nghệ giả mạo hình ảnh, âm thanh, video và các công nghệ số mới đang tạo ra những phương thức vi phạm ngày càng khó nhận diện, qua đó đặt ra yêu cầu phải tiếp tục hoàn thiện pháp luật để thích ứng với sự biến đổi nhanh chóng của môi trường công nghệ.

Trong bối cảnh đó, yêu cầu hoàn thiện khuôn khổ pháp lý về ANM không chỉ xuất phát từ nhu cầu phòng ngừa, phát hiện và xử lý các hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên KGM mà còn nhằm bảo đảm sự thống nhất trong quản lý nhà nước, bảo vệ quyền và lợi ích hợp pháp của các chủ thể tham gia môi trường số. Trước khi Luật An ninh mạng năm 2025 được ban hành, hệ thống pháp luật về lĩnh vực này chủ yếu được điều chỉnh bởi Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015. Hai đạo luật có phạm vi điều chỉnh và cách tiếp cận khác nhau, dẫn tới yêu cầu phải tiếp tục rà soát, hoàn thiện và bảo đảm tính thống nhất, đồng bộ của hệ thống pháp luật trong điều kiện chức năng quản lý nhà nước về an ninh mạng và an toàn thông tin có sự thay đổi. Vì vậy, việc xây dựng một đạo luật mới trên cơ sở kế thừa và hợp nhất những quy định còn phù hợp của hai đạo luật nói trên được xác định là một yêu cầu có tính cấp thiết.

Ngày 10/12/2025, tại Kỳ họp thứ 10, Quốc hội khóa XV đã thông qua Luật An ninh mạng số 116/2025/QH15 với 434/443 đại biểu Quốc hội có mặt tán thành, đạt tỷ lệ 91,75%. Luật có hiệu lực thi hành từ ngày 01/7/2026. Đây là bước phát triển quan trọng trong quá trình hoàn thiện pháp luật về bảo vệ ANM ở Việt Nam, đồng thời thể hiện yêu cầu thể chế hóa chủ trương, chính sách của Đảng và Nhà nước về bảo vệ an ninh quốc gia, chủ quyền quốc gia trên KGM, gắn bảo đảm an ninh mạng với phát triển kinh tế - xã hội, khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia (Chính phủ, 2026a).

Về cấu trúc, Luật An ninh mạng năm 2025 gồm 08 chương, 45 điều, quy định tương đối toàn diện về ANM, bảo vệ ANM; quyền, nghĩa vụ và trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan (Quốc hội, 2025). Theo Điều 1, Luật điều chỉnh các vấn đề về ANM, bảo vệ ANM và trách nhiệm của các chủ thể có liên quan trong hoạt động bảo vệ ANM. Việc thiết kế phạm vi điều chỉnh theo hướng bao quát cả phương diện bảo vệ an ninh quốc gia, trật tự, an toàn xã hội và bảo vệ quyền, lợi ích hợp pháp của các chủ thể trên KGM cho thấy cách tiếp cận tương đối toàn diện của pháp luật Việt Nam đối với các vấn đề an ninh phát sinh trong môi trường số.

Một trong những điểm đáng chú ý của Luật là việc hợp nhất và hệ thống hóa các quy định về ANM và an toàn thông tin mạng. Theo đó, Luật kế thừa những quy định còn phù hợp của Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015, đồng thời bổ sung, hoàn thiện một số quy định nhằm đáp ứng yêu cầu mới của thực tiễn. Cách tiếp cận này nhằm khắc phục tình trạng phân tán, chồng chéo về quy định pháp luật, tạo cơ sở pháp lý thống nhất cho hoạt động quản lý, bảo vệ KGM và nâng cao hiệu quả tổ chức thực thi pháp luật. Đồng thời, Luật được xây dựng trong mối liên hệ với yêu cầu phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia, qua đó hướng tới sự cân bằng giữa yêu cầu bảo đảm ANM và yêu cầu phát triển kinh tế - xã hội trong môi trường số (Chính phủ, 2026b).

Về nội dung, Luật An ninh mạng năm 2025 tập trung vào một số nhóm vấn đề cơ bản như: xác định những nguyên tắc, chính sách và trách nhiệm trong bảo vệ ANM; quy định các hành vi bị nghiêm cấm trên KGM; phòng ngừa, phát hiện và xử lý hành vi xâm phạm ANM; 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; bảo vệ hệ thống thông tin; bảo vệ trẻ em và các nhóm đối tượng có nguy cơ bị xâm hại trên KGM; trách nhiệm của cơ quan, tổ chức, doanh nghiệp và cá nhân; kinh doanh sản phẩm, dịch vụ ANM cũng như hợp tác quốc tế về ANM. Việc mở rộng và cụ thể hóa các nhóm nội dung này cho thấy pháp luật về ANM không chỉ hướng tới xử lý hậu quả của các cuộc tấn công hoặc hành vi vi phạm mà còn chú trọng xây dựng

cơ chế phòng ngừa, quản trị rủi ro và bảo vệ các quyền, lợi ích hợp pháp trong môi trường số. Đặc biệt, Điều 7 Luật An ninh mạng năm 2025 quy định các hành vi bị nghiêm cấm về ANM, trong đó khoản 2 liệt kê các hành vi thực hiện trên KGM bị pháp luật nghiêm cấm. Đáng chú ý, điểm đ khoản 2 Điều 7 quy định: “Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên KGM” (Quốc hội, 2025). Quy định này có ý nghĩa đặc biệt trong bối cảnh các hoạt động kinh tế, giao dịch tài chính, thương mại điện tử và sáng tạo nội dung ngày càng dịch chuyển lên môi trường số. Việc ghi nhận cụ thể các nhóm hành vi nêu trên trong điều khoản về các hành vi bị nghiêm cấm có tác dụng xác lập ranh giới pháp lý giữa hoạt động sử dụng KGM hợp pháp với việc lợi dụng công nghệ, phương tiện điện tử để xâm phạm quyền và lợi ích hợp pháp của chủ thể khác. Đồng thời, quy định cũng cho thấy sự chuyển dịch trong phương thức tiếp cận của pháp luật: không chỉ coi ANM là vấn đề bảo vệ hệ thống kỹ thuật và thông tin mà còn đặt trọng tâm vào việc kiểm soát những hành vi có khả năng trực tiếp gây thiệt hại về tài sản, quyền sở hữu trí tuệ, trật tự xã hội và lợi ích hợp pháp của cá nhân, tổ chức.

Đối với hành vi lừa đảo chiếm đoạt tài sản, quy định tại điểm đ khoản 2 Điều 7 có ý nghĩa đáng chú ý bởi KGM đã trở thành môi trường để các đối tượng thực hiện nhiều phương thức lừa đảo mới, từ giả mạo tài khoản, website, ứng dụng, tổ chức, cá nhân đến sử dụng công nghệ trí tuệ nhân tạo (AI) để tạo lập hình ảnh, âm thanh, video giả nhằm tạo lòng tin và chiếm đoạt tài sản. Luật An ninh mạng năm 2025 đồng thời bổ sung quy định liên quan đến việc sử dụng AI hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật, cho thấy pháp luật đã bước đầu tính đến những phương thức xâm phạm mới phát sinh cùng với sự phát triển của công nghệ. Bên cạnh đó, việc đặt tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm; vi phạm bản quyền và sở hữu trí tuệ trong cùng nhóm hành vi bị nghiêm cấm phản ánh tính đa dạng của các nguy cơ đối với trật tự, an toàn xã hội trên KGM. Đây không chỉ là những hành vi xâm phạm lợi ích của từng cá nhân, tổ chức cụ thể mà trong một số trường hợp còn có khả năng tạo ra tác động tiêu cực trên phạm vi rộng, làm phát sinh thiệt hại về kinh tế, ảnh hưởng đến môi trường kinh doanh số và làm suy giảm tính an toàn, lành mạnh của KGM.

2.2. Nhận diện các hành vi bị nghiêm cấm theo điểm đ khoản 2 Điều 7 Luật An ninh mạng và thực tiễn áp dụng

Điểm đ khoản 2 Điều 7 Luật An ninh mạng năm 2025 quy định 5 nhóm hành vi bị nghiêm cấm trên KGM, gồm: lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm; vi phạm bản quyền, quyền sở hữu trí tuệ. Đây là những hành vi có tính chất phổ biến, phương thức thực hiện ngày càng tinh vi, thường gắn với việc lợi dụng công nghệ, dữ liệu cá nhân và các nền tảng số để che giấu chủ thể, mở rộng phạm vi tác động và gây khó khăn cho công tác phát hiện, xử lý.

2.2.1. Lừa đảo chiếm đoạt tài sản

Lừa đảo chiếm đoạt tài sản trên KGM ngày càng phổ biến với phương thức, thủ đoạn tinh vi, chủ yếu thông qua giả mạo cơ quan, tổ chức, cá nhân; website, ứng dụng, tài khoản mạng xã hội hoặc sử dụng trái phép thông tin cá nhân để tạo dựng kịch bản gian dối. Sự phát triển của ngân hàng số, thanh toán điện tử và công nghệ AI tạo điều kiện cho các hành vi này diễn biến phức tạp, đồng thời gây khó khăn cho việc xác định chủ thể, thu thập chứng cứ, truy vết dòng tiền và thu hồi tài sản.

Về pháp lý, điểm đ khoản 2 Điều 7 Luật An ninh mạng số 116/2025/QH15 nghiêm cấm hành vi “lừa đảo chiếm đoạt tài sản” trên KGM. Quy định này góp phần xác lập cơ sở pháp lý để phòng ngừa, phát hiện và xử lý các hành vi lợi dụng công nghệ, phương tiện điện tử nhằm xâm phạm tài sản của cá nhân, tổ chức. Tùy thuộc phương thức, thủ đoạn và dấu hiệu cấu thành cụ thể, hành vi có thể bị xử lý theo Điều 174 và Điều 290 Bộ luật Hình sự năm 2015, được sửa đổi, bổ sung năm 2017 (Quốc hội, 2017). Do đó, việc áp dụng pháp luật cần bảo đảm phân định rõ giữa hành vi lừa đảo nói chung và hành vi sử

dụng mạng máy tính, mạng viễn thông, phương tiện điện tử làm phương thức thực hiện hành vi chiếm đoạt tài sản. Trong thực tiễn, bên cạnh hoàn thiện quy định pháp luật cần tăng cường cơ chế xác thực danh tính, cảnh báo giao dịch bất thường, phối hợp giữa cơ quan chức năng với ngân hàng, doanh nghiệp viễn thông và nền tảng số nhằm kịp thời ngăn chặn, truy vết và thu hồi tài sản bị chiếm đoạt.

2.2.2. Tổ chức đánh bạc, đánh bạc qua Internet

Đánh bạc qua mạng Internet ngày càng diễn biến phức tạp với nhiều hình thức như cá cược thể thao, casino trực tuyến, lô đề và trò chơi có tính chất đối thưởng. Các đối tượng thường lợi dụng nền tảng số, tài khoản trung gian và phương thức thanh toán điện tử để tổ chức hoạt động, thậm chí thiết lập đường dây có yếu tố xuyên biên giới. Việc sử dụng công nghệ giúp mở rộng nhanh số lượng người tham gia, che giấu danh tính và phân tán dòng tiền, qua đó gây không ít khó khăn cho công tác phát hiện, thu thập chứng cứ và xử lý vi phạm.

Về pháp lý, điểm đ khoản 2 Điều 7 Luật An ninh mạng số 116/2025/QH15 nghiêm cấm hành vi “tổ chức đánh bạc, đánh bạc qua mạng Internet”. Tùy thuộc tính chất, mức độ và vai trò của chủ thể, hành vi có thể bị xử lý hình sự về tội đánh bạc theo Điều 321 hoặc tội tổ chức đánh bạc hoặc gá bạc theo Điều 322 Bộ luật Hình sự năm 2015, được sửa đổi, bổ sung năm 2017. Quy định này góp phần tăng cường cơ sở pháp lý để ngăn chặn việc lợi dụng KGM tổ chức các hoạt động cờ bạc trái pháp luật, đồng thời đặt ra yêu cầu nâng cao hiệu quả phối hợp giữa cơ quan chức năng, doanh nghiệp cung cấp dịch vụ viễn thông, nền tảng số và các tổ chức cung ứng dịch vụ thanh toán trong phát hiện, ngăn chặn và xử lý hành vi vi phạm (Quốc hội, 2017).

2.2.3. Trộm cắp cước viễn thông quốc tế trên nền Internet

Trộm cắp cước viễn thông quốc tế trên nền Internet thường được thực hiện thông qua việc khai thác trái phép hệ thống viễn thông, sử dụng công nghệ VoIP, thiết bị chuyển tiếp hoặc các phương thức kỹ thuật khác nhằm né tránh nghĩa vụ thanh toán cước hoặc thu lợi bất chính. Sự phát triển của hạ tầng Internet và các công nghệ truyền dẫn số khiến phương thức thực hiện ngày càng tinh vi, khó phát hiện và truy vết, không chỉ gây thiệt hại về kinh tế cho doanh nghiệp viễn thông mà còn tiềm ẩn nguy cơ ảnh hưởng đến an toàn, an ninh của hệ thống thông tin.

Về pháp lý, điểm đ khoản 2 Điều 7 Luật An ninh mạng số 116/2025/QH15 nghiêm cấm hành vi “trộm cắp cước viễn thông quốc tế trên nền Internet”. Tùy thuộc phương thức, thủ đoạn và mức độ vi phạm, hành vi có thể bị xử lý theo các quy định của pháp luật hình sự, trong đó Điều 289 Bộ luật Hình sự năm 2015, được sửa đổi, bổ sung năm 2017 quy định về tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác. Việc xử lý cần căn cứ vào dấu hiệu cấu thành cụ thể, bảo đảm phân định rõ giữa hành vi vi phạm nghĩa vụ thanh toán cước với hành vi sử dụng thủ đoạn kỹ thuật để xâm nhập, khai thác trái phép hệ thống viễn thông.

2.2.4. Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm

Không gian mạng làm gia tăng đáng kể khả năng tiếp cận và phát tán thông tin liên quan đến hàng hóa, dịch vụ bị pháp luật cấm, đồng thời tạo điều kiện cho các hoạt động quảng cáo, môi giới, mua bán diễn ra nhanh chóng và khó kiểm soát. Việc lợi dụng tài khoản ẩn danh, nhóm kín, website hoặc nền tảng trung gian để che giấu giao dịch đặt ra thách thức đối với công tác phát hiện và xử lý vi phạm. Vì vậy, việc xác định trách nhiệm pháp lý cần dựa trên tính chất, đối tượng và phương thức thực hiện hành vi, bảo đảm áp dụng đúng quy định về xử phạt hành chính hoặc truy cứu trách nhiệm hình sự tương ứng.

2.2.5. Vi phạm bản quyền và quyền sở hữu trí tuệ trên không gian mạng

Vi phạm bản quyền và quyền sở hữu trí tuệ trên KGM chủ yếu biểu hiện qua việc sao chép, phát tán, cung cấp hoặc khai thác trái phép phim, âm nhạc, sách điện tử, phần mềm và các đối tượng quyền sở hữu trí tuệ khác. Với đặc tính sao chép nhanh, phạm vi lan truyền rộng và khả năng vượt qua biên giới quốc gia, các hành vi này không chỉ gây thiệt hại cho chủ thể quyền mà còn đặt ra khó khăn trong xác định chủ thể vi phạm, thu thập và bảo toàn chứng cứ. Tùy tính chất, mức độ và hậu quả, hành vi có thể làm phát sinh trách nhiệm dân sự, hành chính hoặc hình sự theo pháp luật về sở hữu trí tuệ và Bộ luật Hình sự.

Nhìn tổng thể, các hành vi thuộc điểm đ khoản 2 Điều 7 Luật An ninh mạng năm 2025 đều có đặc điểm chung là lợi dụng tính mở, tốc độ lan truyền, khả năng ẩn danh và phạm vi xuyên biên giới của KGM để thực hiện hành vi vi phạm. Vì vậy, phòng ngừa và xử lý hiệu quả không chỉ phụ thuộc vào hoàn thiện pháp luật mà còn cần kết hợp các giải pháp công nghệ, nâng cao ý thức tuân thủ pháp luật và tăng cường phối hợp giữa cơ quan nhà nước, doanh nghiệp cung cấp dịch vụ số và các chủ thể có liên quan.

2.3. Biện pháp phòng ngừa các hành vi vi phạm pháp luật trên không gian mạng

2.3.1. Đối với người dân

Phòng ngừa từ phía người dân là một trong những yếu tố quan trọng nhằm hạn chế các hành vi vi phạm pháp luật trên KGM. Trước hết, mỗi cá nhân cần chủ động nâng cao nhận thức pháp luật và kỹ năng an toàn số, đặc biệt về an ninh mạng, bảo vệ dữ liệu cá nhân, giao dịch điện tử, phòng, chống tội phạm sử dụng công nghệ cao và sở hữu trí tuệ. Việc nhận diện được các phương thức, thủ đoạn phổ biến của lừa đảo trực tuyến, đánh bạc qua mạng, mua bán hàng hóa, dịch vụ bị cấm và xâm phạm bản quyền sẽ góp phần giảm thiểu nguy cơ trở thành nạn nhân hoặc vô tình tiếp tay cho hành vi vi phạm. Bên cạnh đó, người dân cần chủ động bảo vệ thông tin cá nhân và tài khoản số. Không cung cấp tùy tiện số căn cước, thông tin tài khoản ngân hàng, mật khẩu, mã OTP, mã xác thực hoặc dữ liệu đăng nhập; sử dụng mật khẩu có độ bảo mật cao, xác thực đa yếu tố và thường xuyên kiểm tra hoạt động bất thường trên các tài khoản quan trọng. Đối với các cuộc gọi, tin nhắn, thư điện tử hoặc tài khoản mạng xã hội yêu cầu chuyển tiền, cung cấp thông tin hoặc truy cập đường dẫn cần xác minh độc lập danh tính và mục đích trước khi thực hiện.

Đối với hoạt động đánh bạc và giao dịch hàng hóa, dịch vụ trên Internet, người dân cần tuyệt đối không tham gia, tổ chức, quảng bá, môi giới hoặc thực hiện trung gian thanh toán cho các hoạt động bị pháp luật cấm. Đồng thời, cần tôn trọng quyền tác giả và quyền sở hữu trí tuệ, không tự ý sao chép, phát tán hoặc khai thác thương mại các tác phẩm, phần mềm, phim, âm nhạc, sách điện tử và các sản phẩm trí tuệ khi chưa được phép của chủ thể quyền. Khi phát hiện dấu hiệu vi phạm, người dân cần chủ động lưu giữ và cung cấp chứng cứ điện tử như tin nhắn, hình ảnh, đường dẫn, số điện thoại, tài khoản mạng xã hội, thông tin giao dịch và chứng từ chuyển tiền cho cơ quan có thẩm quyền. Việc kịp thời báo cáo nội dung vi phạm cho nền tảng cung cấp dịch vụ và cơ quan chức năng có ý nghĩa quan trọng trong việc ngăn chặn hành vi tiếp diễn và hạn chế thiệt hại. Đặc biệt, cần chú trọng trang bị kỹ năng an toàn số cho trẻ em, người cao tuổi và những người hạn chế về khả năng tiếp cận công nghệ. Gia đình, nhà trường và cộng đồng cần phối hợp hướng dẫn các nhóm này nhận biết dấu hiệu lừa đảo, nội dung độc hại, trò chơi có yếu tố cờ bạc và các hình thức dụ dỗ, thao túng trên KGM. Như vậy, trách nhiệm của người dân không chỉ dừng ở việc tự bảo vệ mà còn thể hiện ở nguyên tắc không tham gia, không tiếp tay, không phát tán và chủ động tố giác hành vi vi phạm.

2.3.2. Đối với doanh nghiệp

Phòng ngừa các hành vi vi phạm pháp luật trên KGM cần được đặt trong tổng thể cơ chế quản trị rủi ro, bảo đảm an ninh hệ thống, bảo vệ dữ liệu và tuân thủ pháp luật. Doanh nghiệp trước hết phải xây dựng hệ thống quản lý an toàn thông tin phù hợp với quy mô, tính chất hoạt động và mức độ quan trọng của dữ liệu; thường xuyên cập nhật phần mềm, khắc phục lỗ hổng, kiểm soát quyền truy cập, mã hóa và sao lưu dữ liệu, đồng thời thiết lập cơ chế giám sát và cảnh báo sự cố.

Việc bảo vệ dữ liệu cá nhân của khách hàng và người lao động cần được thực hiện xuyên suốt quá trình thu thập, lưu trữ, xử lý và chia sẻ dữ liệu. Doanh nghiệp cần giới hạn quyền tiếp cận đối với dữ liệu nhạy cảm, kiểm soát lịch sử truy cập và kịp thời phát hiện hành vi sử dụng dữ liệu trái thẩm quyền. Đây không chỉ là yêu cầu về kỹ thuật mà còn là trách nhiệm pháp lý gắn với hoạt động của doanh nghiệp trong môi trường số (Trần Thị Thu Phương, 2021).

Đối với các doanh nghiệp vận hành nền tảng số, mạng xã hội, thương mại điện tử, viễn thông và thanh toán điện tử, cần tăng cường cơ chế xác thực người dùng, kiểm soát tài khoản, giám sát giao dịch và phát hiện hành vi bất thường. Các dấu hiệu liên quan đến lừa đảo, đánh bạc, quảng cáo hàng hóa, dịch vụ bị cấm hoặc xâm phạm quyền sở hữu trí tuệ cần được phát hiện, ngăn chặn và xử lý kịp thời. Đối với nội dung và hàng hóa được cung cấp trên nền tảng, cần xây dựng cơ chế thẩm định người bán,

sản phẩm và quảng cáo; đồng thời có quy trình tiếp nhận, xử lý khiếu nại và yêu cầu gỡ bỏ nội dung vi phạm. Doanh nghiệp cũng cần xây dựng cơ chế phòng, chống gian lận và ứng phó sự cố. Các ngân hàng, tổ chức trung gian thanh toán và doanh nghiệp thương mại điện tử cần có hệ thống cảnh báo giao dịch bất thường, hỗ trợ khóa hoặc hạn chế giao dịch có dấu hiệu rủi ro và phối hợp truy vết dòng tiền khi xảy ra lừa đảo. Đồng thời, xây dựng phương án xử lý khi hệ thống bị tấn công, dữ liệu bị xâm phạm hoặc phát hiện hoạt động phạm tội, trong đó xác định rõ trách nhiệm của từng bộ phận và cơ chế bảo toàn chứng cứ điện tử.

Một yếu tố không thể thiếu là đào tạo và nâng cao nhận thức của người lao động. Doanh nghiệp cần thường xuyên hướng dẫn nhân viên về bảo mật tài khoản, nhận diện thư điện tử giả mạo, lừa đảo trực tuyến, bảo vệ dữ liệu nội bộ và trách nhiệm pháp lý khi sử dụng hệ thống thông tin. Đồng thời, cần thiết lập cơ chế phối hợp với cơ quan chức năng để cung cấp thông tin, dữ liệu và chứng cứ khi phát hiện hành vi có dấu hiệu vi phạm.

2.3.3. Đối với cơ quan nhà nước

Phòng ngừa các hành vi vi phạm pháp luật trên KGM cần được triển khai đồng bộ trên các phương diện hoàn thiện pháp luật, quản lý nhà nước, năng lực thực thi, công nghệ và hợp tác quốc tế: Cần tiếp tục rà soát, hoàn thiện pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân, giao dịch điện tử và phòng, chống tội phạm sử dụng công nghệ cao nhằm bảo đảm tính thống nhất, rõ ràng và khả thi của hệ thống pháp luật. Cùng với đó, cần nghiên cứu hoàn thiện cơ chế xác định trách nhiệm của các nền tảng số, doanh nghiệp viễn thông, tổ chức tín dụng và trung gian thanh toán trong việc phát hiện, ngăn chặn và phối hợp xử lý hành vi vi phạm; Công tác quản lý, giám sát KGM cần chuyển mạnh từ phương thức xử lý sau vi phạm sang phòng ngừa chủ động và cảnh báo sớm. Các cơ quan chức năng cần tăng cường giám sát website, ứng dụng, tài khoản mạng xã hội, sàn thương mại điện tử và các phương thức thanh toán có dấu hiệu bất thường; kịp thời phát hiện, ngăn chặn website giả mạo, hoạt động lừa đảo, tổ chức đánh bạc, quảng bá hàng hóa bị cấm và các hành vi xâm phạm quyền sở hữu trí tuệ. Bên cạnh đó, cần nâng cao năng lực của lực lượng chuyên trách thông qua đầu tư cơ sở vật chất, công nghệ và nguồn nhân lực về điều tra số, giám định dữ liệu điện tử, phân tích dữ liệu và truy vết dòng tiền. Việc ứng dụng AI, dữ liệu lớn và các công cụ phân tích hiện đại cần được triển khai phù hợp nhằm nâng cao khả năng phát hiện sớm các mô hình, dấu hiệu và phương thức phạm tội mới. Do tính chất xuyên biên giới của nhiều hành vi phạm tội trên KGM, hợp tác quốc tế có ý nghĩa đặc biệt quan trọng. Các cơ quan chức năng cần tăng cường trao đổi thông tin, phối hợp điều tra, thu thập và chia sẻ chứng cứ điện tử, truy tìm dòng tiền, xử lý máy chủ và tài khoản liên quan đến hoạt động phạm tội ở nước ngoài. Cơ chế phối hợp quốc tế cần bảo đảm vừa hiệu quả trong đấu tranh phòng, chống tội phạm, vừa tôn trọng chủ quyền và pháp luật của các quốc gia liên quan; Nhà nước cần đẩy mạnh tuyên truyền, phổ biến pháp luật và nâng cao năng lực số cho cộng đồng. Nội dung tuyên truyền cần tập trung vào những thủ đoạn mới, có tính thực tiễn cao, hướng tới từng nhóm đối tượng, đặc biệt là trẻ em, người cao tuổi và người có hạn chế về kỹ năng số. Đồng thời, cần phát huy vai trò của gia đình, nhà trường, doanh nghiệp và các tổ chức xã hội trong xây dựng văn hóa sử dụng Internet an toàn, có trách nhiệm.

2.3.4. Nhận định chung

Có thể thấy, phòng ngừa các hành vi bị nghiêm cấm theo điểm đ khoản 2 Điều 7 Luật An ninh mạng không thể chỉ dựa vào biện pháp xử lý của cơ quan nhà nước mà cần hình thành cơ chế phòng ngừa đa chủ thể, trong đó Nhà nước giữ vai trò kiến tạo và điều phối, doanh nghiệp có trách nhiệm bảo đảm an toàn cho hệ thống và người sử dụng, còn cá nhân là chủ thể trực tiếp thực hiện và tuân thủ các chuẩn mực pháp luật trên KGM.

Sự kết hợp giữa hoàn thiện pháp luật, ứng dụng công nghệ, quản trị rủi ro, bảo vệ dữ liệu, nâng cao nhận thức và hợp tác quốc tế sẽ tạo cơ sở cho việc chuyển từ mô hình xử lý vi phạm mang tính bị động sang phòng ngừa chủ động. Đây là yêu cầu cần thiết nhằm bảo đảm an ninh, an toàn KGM, bảo vệ quyền và lợi ích hợp pháp của cá nhân, tổ chức và tạo môi trường số an toàn, lành mạnh, phục vụ quá trình chuyển đổi số tại Việt Nam.

Xem tiếp trang 405