ĐẤU TRANH PHÒNG NGỪA TỘI PHẠM CÔNG NGHỆ CAO Ở VIỆT NAM HIỆN NAY

HÀ THỊ TRÂM
Học viện Cảnh sát nhân dân

Nhận bài ngày 07/10/2025. Sửa chữa xong 27/11/2025. Duyệt đăng 27/12/2025.

Abstract

In the context of rapid digital transformation and deep international integration, high-tech crime in Vietnam has been increasing significantly in both scale and sophistication, causing serious consequences for national security, social order and safety, and citizens' rights. This article analyzes the current situation of high-tech crime in Vietnam, identifies key difficulties and challenges in combating and preventing these crimes, and proposes several solutions to enhance the effectiveness of prevention and law enforcement efforts in the coming period.

Keywords: *Cybersecurity, digital transformation, high-tech crime, crime prevention, solutions, Vietnam.*

1. Đặt vấn đề

Cuộc Cách mạng công nghiệp lần thứ tư với nền tảng là công nghệ số, trí tuệ nhân tạo, dữ liệu lớn và Internet vạn vật đã và đang làm thay đổi sâu sắc mọi lĩnh vực của đời sống kinh tế - xã hội. Tại Việt Nam, quá trình chuyển đổi số quốc gia diễn ra mạnh mẽ, gắn liền với sự phát triển của chính phủ điện tử, kinh tế số và xã hội số. Bên cạnh những lợi ích to lớn mang lại, sự phát triển nhanh chóng của công nghệ thông tin và mạng Internet cũng đặt ra nhiều thách thức mới đối với công tác bảo đảm an ninh, trật tự, đặc biệt là sự gia tăng của tội phạm công nghệ cao. Tội phạm công nghệ cao xuất hiện và phát triển song hành với tiến bộ khoa học, công nghệ, lợi dụng không gian mạng, tính ẩn danh và khả năng xuyên biên giới của Internet để thực hiện hành vi phạm tội. Các hành vi như lừa đảo chiếm đoạt tài sản qua mạng, xâm nhập trái phép vào hệ thống thông tin, đánh cắp dữ liệu cá nhân, tấn công mạng, sử dụng trí tuệ nhân tạo để giả mạo thông tin, hình ảnh và giọng nói ngày càng phổ biến, gây thiệt hại nghiêm trọng về kinh tế, xâm phạm quyền con người, quyền công dân và làm suy giảm niềm tin xã hội vào môi trường số. Ở Việt Nam, tình hình tội phạm công nghệ cao trong những năm gần đây diễn biến ngày càng phức tạp, với phương thức, thủ đoạn liên tục thay đổi và ngày càng tinh vi. Không chỉ gia tăng về số lượng, loại tội phạm này còn có xu hướng tổ chức chặt chẽ, hoạt động theo đường dây, ổ nhóm, nhiều vụ việc có yếu tố xuyên quốc gia, gây khó khăn lớn cho công tác phát hiện, điều tra và xử lý.

2. Nội dung nghiên cứu

2.1. Tội phạm công nghệ cao - một số vấn đề lý luận

Trong bối cảnh phát triển mạnh mẽ của khoa học, công nghệ và quá trình số hóa toàn diện các hoạt động kinh tế - xã hội, tội phạm công nghệ cao đã trở thành một hiện tượng xã hội pháp lý mang tính toàn cầu. Không giống với các loại tội phạm truyền thống, tội phạm công nghệ cao gắn chặt với sự phát triển của công nghệ thông tin, mạng Internet và các hệ thống thông tin số. Đây là loại tội phạm sử dụng công nghệ cao như máy tính, mạng viễn thông, Internet, phần mềm, trí tuệ nhân tạo và các phương tiện điện tử hiện đại làm công cụ, phương tiện hoặc môi trường để thực hiện hành vi phạm tội.

Về mặt khái niệm, tội phạm công nghệ cao (hay còn gọi là tội phạm mạng), với sự phát triển nhanh chóng của công nghệ thông tin và Internet đã mang lại nhiều lợi ích to lớn cho đời sống kinh tế - xã hội nhưng đồng thời cũng tạo ra những phương thức, thủ đoạn phạm tội mới. Trong bối cảnh đó, tội

Email: hatram885@gmail.com

phạm công nghệ cao nổi lên như một dạng tội phạm đặc thù, gây ra nhiều hậu quả nghiêm trọng về kinh tế - xã hội và an ninh quốc gia [1, tr. 32]. Trên bình diện khoa học pháp lý, tội phạm công nghệ cao thường được hiểu là hành vi nguy hiểm cho xã hội, do cá nhân hoặc tổ chức thực hiện thông qua việc sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông và các thiết bị số nhằm xâm hại lợi ích hợp pháp của Nhà nước, tổ chức, cá nhân hoặc gây rối loạn trật tự, an toàn xã hội.

Ở bình diện quốc tế, khái niệm "cybercrime" đã được tiếp cận theo nhiều hướng khác nhau: Liên Hợp Quốc coi đây là những hành vi phạm tội được thực hiện bằng phương tiện điện tử hoặc nhằm vào hệ thống thông tin; Liên minh châu Âu mở rộng phạm vi đến cả các hành vi gian lận, rửa tiền và khủng bố mạng.

Tại Việt Nam, mặc dù Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017) chưa đưa ra định nghĩa chính thức, song qua các quy định tại các điều 285 - 289 có thể xác định phạm vi các hành vi như truy cập trái phép hệ thống thông tin, phát tán mã độc, tổ chức đánh bạc trực tuyến, lừa đảo chiếm đoạt tài sản qua mạng… đều được coi là tội phạm công nghệ cao.

Xét về bản chất xã hội, tội phạm công nghệ cao phản ánh mặt trái của sự phát triển công nghệ trong điều kiện kinh tế thị trường và hội nhập quốc tế. Công nghệ vốn là công cụ trung tính nhưng khi bị con người lợi dụng với mục đích phạm tội, nó trở thành phương tiện gây nguy hại lớn cho xã hội. Trong môi trường số, ranh giới không gian và thời gian bị xóa nhòa, tạo điều kiện cho tội phạm có thể thực hiện hành vi từ xa, ẩn danh và tác động đến nhiều đối tượng trong thời gian rất ngắn. Điều này làm gia tăng đáng kể mức độ nguy hiểm của tội phạm công nghệ cao so với nhiều loại tội phạm truyền thống.

Xét về đặc điểm, tội phạm công nghệ cao là tính ẩn danh và khó xác định chủ thể phạm tội. Đối tượng phạm tội thường sử dụng các công cụ che giấu danh tính như mạng riêng ảo (VPN), máy chủ trung gian, tài khoản ảo, danh tính giả hoặc công nghệ mã hóa dữ liệu. Việc che giấu này khiến cơ quan chức năng gặp nhiều khó khăn trong việc xác định nguồn gốc hành vi phạm tội, thu thập chứng cứ và truy vết đối tượng. Trong nhiều trường hợp, hành vi phạm tội diễn ra hoàn toàn trong không gian mạng, không để lại dấu vết vật chất rõ ràng như các loại tội phạm truyền thống [2, tr. 31].

Tội phạm công nghệ cao thường mang tính xuyên biên giới rõ nét. Không gian mạng không bị giới hạn bởi biên giới quốc gia, cho phép đối tượng phạm tội dễ dàng thực hiện hành vi từ quốc gia này nhưng gây hậu quả ở quốc gia khác. Điều này đặt ra thách thức lớn cho hoạt động điều tra, truy tố và xét xử, bởi sự khác biệt về hệ thống pháp luật, thẩm quyền tài phán và cơ chế hợp tác quốc tế giữa các quốc gia. Trong nhiều vụ việc, việc xử lý tội phạm không chỉ phụ thuộc vào pháp luật trong nước mà còn cần đến sự phối hợp chặt chẽ giữa các cơ quan thực thi pháp luật quốc tế.

Một đặc điểm quan trọng khác của tội phạm công nghệ cao là khả năng gây thiệt hại trên diện rộng trong thời gian ngắn. Chỉ với một đoạn mã độc hoặc một chiến dịch lừa đảo được thiết kế tinh vi, đối tượng phạm tội có thể tấn công hàng nghìn, thậm chí hàng triệu người dùng cùng lúc. Hậu quả không chỉ dừng lại ở thiệt hại tài sản mà còn làm rò rỉ dữ liệu cá nhân, ảnh hưởng đến uy tín của tổ chức, doanh nghiệp và gây bất ổn xã hội. Trong bối cảnh kinh tế số, những thiệt hại này có thể lan truyền nhanh chóng và khó khắc phục triệt để.

Xét về chủ thể phạm tội, tội phạm công nghệ cao thường do những người có trình độ nhất định về công nghệ thông tin thực hiện. Đối tượng phạm tội có thể là cá nhân đơn lẻ nhưng ngày càng phổ biến là các nhóm tội phạm có tổ chức, phân công vai trò rõ ràng như người lập trình, người quản lý hệ thống, người thực hiện giao dịch tài chính và người che giấu dòng tiền. Đặc điểm này cho thấy tội phạm công nghệ cao không chỉ mang tính tự phát mà ngày càng có xu hướng chuyên nghiệp hóa, hoạt động như một "ngành công nghiệp ngầm" trong không gian mạng [3, tr. 14].

Về hành vi phạm tội, tội phạm công nghệ cao có phạm vi rất rộng, bao gồm nhiều nhóm hành vi khác nhau. Có thể kể đến các hành vi xâm nhập trái phép vào hệ thống thông tin, phá hoại hoặc làm tê liệt hệ thống mạng; đánh cắp, mua bán dữ liệu cá nhân và bí mật kinh doanh; lừa đảo chiếm đoạt tài sản thông qua các hình thức như giả mạo website, email, tin nhắn, mạng xã hội; tổ chức đánh bạc, rửa tiền và huy động vốn trái phép trên không gian mạng. Những hành vi này không chỉ gây thiệt hại về kinh tế mà còn ảnh hưởng nghiêm trọng đến an ninh thông tin và trật tự quản lý xã hội. Ngoài ra, tội phạm công nghệ

cao còn có tính biến đổi nhanh chóng về phương thức và thủ đoạn. Khi các biện pháp phòng ngừa và công nghệ bảo mật được nâng cao, đối tượng phạm tội cũng nhanh chóng thay đổi cách thức tấn công, lợi dụng các công nghệ mới như trí tuệ nhân tạo, học máy, công nghệ giả mạo hình ảnh và giọng nói để đánh lừa nạn nhân. Sự biến đổi liên tục này khiến công tác phòng ngừa và đấu tranh với tội phạm công nghệ cao luôn trong trạng thái "chạy đua" với sự phát triển của công nghệ [4, tr. 10].

Từ góc độ pháp lý, tội phạm công nghệ cao đặt ra yêu cầu phải không ngừng hoàn thiện hệ thống pháp luật hình sự và pháp luật liên quan. Nhiều hành vi phạm tội mới xuất hiện nhanh hơn tốc độ điều chỉnh của pháp luật, tạo ra những khoảng trống pháp lý mà tội phạm có thể lợi dụng. Do đó, việc nhận diện đầy đủ bản chất, đặc điểm và xu hướng phát triển của tội phạm công nghệ cao có ý nghĩa đặc biệt quan trọng, không chỉ phục vụ cho công tác lập pháp mà còn là cơ sở cho việc xây dựng các chiến lược phòng ngừa và đấu tranh hiệu quả.

2.2. Thực trạng đấu tranh phòng ngừa tội phạm công nghệ cao ở Việt Nam hiện nay

Trong bối cảnh chuyển đổi số mạnh mẽ và sự gia tăng nhanh chóng của các dịch vụ số, hoạt động tội phạm công nghệ cao ở Việt Nam đang diễn biến hết sức phức tạp và có xu hướng gia tăng cả về số lượng lẫn mức độ tinh vi. Theo thống kê của Cơ quan chức năng, chỉ trong 8 tháng đầu năm 2025, lực lượng chức năng tại Việt Nam đã ghi nhận hơn 1.500 vụ lừa đảo trực tuyến, với thiệt hại ước tính lên tới khoảng 1,66 nghìn tỷ đồng (tương đương hơn 60 triệu USD), tăng 65% so với cùng kỳ năm trước, phản ánh xu hướng phạm tội ngày càng gia tăng và tính chất ngày càng tinh vi của các hình thức lừa đảo, chiếm đoạt tài sản trên không gian mạng.

Ngoài lừa đảo trực tuyến, kích thước và phạm vi các hành vi tội phạm công nghệ cao khác cũng rất đáng lo ngại. Một báo cáo cho thấy trong năm 2024, tổng số vụ tội phạm mạng tại Việt Nam đạt hơn 100.000 vụ, trong đó có 29.000 vụ tấn công bằng ransomware, gây thiệt hại ước tính khoảng 12 nghìn tỷ đồng (hơn 456 triệu USD), cho thấy sự xâm lấn sâu rộng của phần mềm mã độc vào hệ thống dữ liệu và hạ tầng số của các tổ chức, doanh nghiệp và cá nhân.

Mức độ thiệt hại do tội phạm công nghệ cao gây ra không chỉ thể hiện ở số lượng vụ việc mà còn hiện lên qua các khảo sát rộng hơn về tác động kinh tế - xã hội. Theo một báo cáo khảo sát an ninh mạng năm 2024 tại Việt Nam, thiệt hại do tội phạm mạng và lừa đảo trực tuyến gây ra được ước tính lên tới khoảng 18,9 nghìn tỷ đồng (khoảng 743 triệu USD), tương đương với tỷ lệ 1/220 người dùng smartphone là nạn nhân của lừa đảo mạng, phản ánh rằng cả người dân và doanh nghiệp đều là mục tiêu thường xuyên của tin tặc và tội phạm mạng. Trong khi đó, đối tượng và thủ đoạn phạm tội cũng ngày càng biến hóa, có cả yếu tố xuyên biên giới và chuyên nghiệp hóa. Một số báo cáo chỉ ra rằng nhiều tội phạm tổ chức hoạt động từ ngoài lãnh thổ Việt Nam, lợi dụng sự khác biệt trong hệ thống pháp luật và hạn chế về năng lực điều tra quốc tế để né tránh sự truy cứu trách nhiệm. Các thủ đoạn lừa đảo qua mạng thường bao gồm giả danh các cơ quan cấp phép, ngân hàng, tòa án, thậm chí mời chào đầu tư tiền ảo hay các chiêu trò "trò chơi tài chính hấp dẫn", khiến người dân dễ bị mắc bẫy. Trước bối cảnh trên, công tác phòng ngừa tội phạm công nghệ cao đã được triển khai theo nhiều hướng khác nhau. Về pháp lý, Việt Nam đã có nhiều khung pháp luật liên quan bao gồm Bộ luật Hình sự, Luật An ninh mạng, Luật Giao dịch điện tử và các nghị định hướng dẫn thực hiện, tạo hành lang pháp lý cho việc xử lý các hành vi vi phạm trong không gian mạng. Các văn bản này đã bổ sung tội danh, tăng mức xử phạt đối với nhiều hành vi sử dụng công nghệ cao để lừa đảo và chiếm đoạt tài sản, góp phần tăng cường tính răn đe. Tuy nhiên, do tốc độ phát triển công nghệ quá nhanh, vẫn xuất hiện những "khoảng trống" pháp lý đối với các hành vi mới như sử dụng trí tuệ nhân tạo để giả mạo nội dung (deepfake), đánh lừa nhận diện sinh trắc học hoặc lừa đảo tài chính bằng các tiền điện tử. Đây là thách thức lớn đối với hệ thống pháp luật hiện hành trong việc theo kịp và điều chỉnh phù hợp các hành vi phạm tội mới phát sinh.

Về tổ chức thực thi, lực lượng phòng, chống tội phạm công nghệ cao trong Công an nhân dân và các cơ quan chức năng đã được nâng cao cả về số lượng và trang thiết bị kỹ thuật. Các đơn vị này đã triển khai nhiều chiến dịch điều tra, truy quét các đường dây lừa đảo trực tuyến, thu giữ tang vật và

truy tố nhiều đối tượng. Bên cạnh đó, việc phối hợp với các doanh nghiệp công nghệ, ngân hàng và tổ chức dịch vụ số đã được đẩy mạnh để thiết lập các hệ thống cảnh báo sớm, chặn các tài khoản gian lận, phishing và các tên miền độc hại. Dù vậy, do nguồn lực kỹ thuật, nhân sự có trình độ chuyên sâu về an ninh mạng còn hạn chế so với quy mô và tính phức tạp của tội phạm công nghệ cao, việc phản ứng kịp thời và xử lý triệt để các vụ việc vẫn gặp nhiều khó khăn.

Trong lĩnh vực tuyên truyền và nâng cao nhận thức cộng đồng, các chiến dịch về an toàn thông tin, phòng tránh lừa đảo trực tuyến cũng được tiến hành rộng khắp, thông qua các phương tiện truyền thông đại chúng, mạng xã hội và các chương trình đào tạo kỹ năng số cho người dân. Những nỗ lực này giúp cho người dùng hiểu rõ hơn về các thủ đoạn tội phạm công nghệ cao, từ đó chủ động bảo vệ bản thân và giảm nguy cơ bị tấn công. Tuy nhiên, hiệu quả của các hoạt động này còn chưa đồng đều ở nhiều địa phương, đặc biệt là trong nhóm người cao tuổi, người ở vùng nông thôn và những người có ít kiến thức về công nghệ, khiến họ vẫn dễ trở thành mục tiêu bị lợi dụng.

Ngoài ra, hợp tác quốc tế trong đấu tranh phòng ngừa tội phạm công nghệ cao cũng ngày càng được chú trọng, với việc Việt Nam tham gia các diễn đàn, hiệp định và mạng lưới chia sẻ thông tin tình báo, giúp xử lý các vụ án có yếu tố xuyên biên giới. Song thực tế cho thấy, sự khác biệt về khung pháp lý giữa các quốc gia và phạm vi quyền hạn trong điều tra quốc tế làm cho việc thu thập chứng cứ, dẫn độ và truy tố đối tượng gặp nhiều rào cản, ảnh hưởng đến hiệu quả xử lý những vụ việc phức tạp.

Bên cạnh đó, việc điều tra và xử lý tội phạm công nghệ cao ở Việt Nam hiện nay đang gặp nhiều trở ngại, bắt nguồn từ đặc thù loại tội phạm này cũng như hạn chế trong cơ chế quản lý và năng lực thực thi như: 1) Tính ẩn danh trên không gian mạng khiến việc truy vết trở nên khó khăn. Các đối tượng sử dụng công nghệ mã hóa, mạng riêng ảo (VPN), tài khoản ảo, sim rác và đặc biệt là tiền điện tử để che giấu danh tính. Trong nhiều trường hợp, việc xác định được thủ phạm thật sự gần như bất khả thi nếu thiếu sự hợp tác quốc tế; 2) Dữ liệu phạm tội thường phân tán ngoài lãnh thổ. Phần lớn các máy chủ được đặt ở nước ngoài, khiến cơ quan chức năng khó tiếp cận dữ liệu chứng cứ. Điều này dẫn đến việc điều tra kéo dài, nhiều vụ án không thể hoàn tất do thiếu bằng chứng điện tử; 3) Cơ chế hợp tác quốc tế còn hạn chế. Mặc dù Việt Nam đã ký nhiều hiệp định tương trợ tư pháp hình sự nhưng cơ chế dẫn độ và chia sẻ dữ liệu điện tử còn chậm và phức tạp. Đây là rào cản lớn trong xử lý các vụ án xuyên quốc gia; 4) Năng lực và phương tiện kỹ thuật còn bất cập. Tội phạm công nghệ cao thường đi trước một bước về công nghệ, trong khi lực lượng chức năng chưa được trang bị đồng bộ về công cụ, thiết bị điều tra số. Nhiều vụ án vì thế bị đình trệ hoặc rơi vào bế tắc [5, tr. 11].

Thực trạng đấu tranh phòng ngừa tội phạm công nghệ cao ở Việt Nam hiện nay phản ánh cả những nỗ lực đáng ghi nhận và những thách thức lớn cần giải quyết. Các số liệu về số vụ lừa đảo, thiệt hại kinh tế và mức độ phổ biến của các hình thức tội phạm mạng cho thấy nhu cầu cấp thiết phải tiếp tục hoàn thiện pháp luật, tăng cường năng lực kỹ thuật và phối hợp đa bên nhằm nâng cao hiệu quả đấu tranh phòng ngừa trong bối cảnh công nghệ số ngày càng phát triển mạnh mẽ.

2.3. Giải pháp nâng cao hiệu quả đấu tranh phòng ngừa tội phạm công nghệ cao ở Việt Nam hiện nay

Trong bối cảnh tội phạm công nghệ cao ngày càng gia tăng và diễn biến phức tạp, việc nâng cao hiệu quả đấu tranh phòng ngừa loại tội phạm này đòi hỏi phải triển khai đồng bộ nhiều giải pháp trên các phương diện pháp lý, tổ chức, con người, khoa học, công nghệ, xã hội và hợp tác quốc tế. Các giải pháp này cần được thực hiện một cách toàn diện, có trọng tâm, trọng điểm, phù hợp với điều kiện thực tiễn của Việt Nam trong giai đoạn chuyển đổi số hiện nay.

2.3.1. Hoàn thiện hệ thống pháp luật là giải pháp có ý nghĩa nền tảng trong đấu tranh phòng ngừa tội phạm công nghệ cao. Pháp luật cần được rà soát, sửa đổi và bổ sung kịp thời nhằm theo kịp sự phát triển nhanh chóng của khoa học, công nghệ và các phương thức phạm tội mới. Việc cụ thể hóa các dấu hiệu pháp lý của hành vi phạm tội sử dụng công nghệ cao trong Bộ luật Hình sự và các luật chuyên ngành sẽ giúp nâng cao tính minh bạch, khả thi và hiệu quả áp dụng pháp luật. Đồng thời, cần tăng cường các quy định về trách nhiệm pháp lý của tổ chức, doanh nghiệp cung cấp dịch vụ số trong việc

bảo đảm an toàn thông tin, bảo vệ dữ liệu cá nhân và phối hợp với cơ quan chức năng khi phát hiện hành vi vi phạm [7, tr. 35].

2.3.2. Nâng cao năng lực tổ chức và chất lượng nguồn nhân lực của các cơ quan chuyên trách là giải pháp mang tính quyết định. Đấu tranh phòng ngừa tội phạm công nghệ cao đòi hỏi đội ngũ cán bộ không chỉ vững vàng về chính trị, pháp luật mà còn có trình độ chuyên môn sâu về công nghệ thông tin, an ninh mạng và điều tra số. Do đó, cần chú trọng công tác đào tạo, bồi dưỡng chuyên sâu, cập nhật kiến thức công nghệ mới cho lực lượng chức năng, đồng thời có cơ chế thu hút và giữ chân nhân lực chất lượng cao trong lĩnh vực này. Việc xây dựng đội ngũ chuyên gia đầu ngành sẽ góp phần nâng cao năng lực phát hiện sớm, điều tra và xử lý hiệu quả các vụ án phức tạp.

2.3.3. Ứng dụng mạnh mẽ khoa học, công nghệ trong công tác phòng ngừa và đấu tranh là giải pháp không thể thiếu. Các cơ quan chức năng cần đẩy mạnh đầu tư vào hạ tầng kỹ thuật, hệ thống phân tích dữ liệu lớn, trí tuệ nhân tạo và các công cụ giám sát không gian mạng nhằm phát hiện kịp thời các dấu hiệu bất thường và hành vi phạm tội. Việc ứng dụng công nghệ hiện đại không chỉ giúp nâng cao hiệu quả điều tra mà còn góp phần chuyển từ phương thức xử lý bị động sang phòng ngừa chủ động. Tuy nhiên, quá trình này cần đi kèm với việc bảo đảm quyền riêng tư và quyền con người, tránh lạm dụng công nghệ trong hoạt động quản lý và giám sát.

2.3.4. Đẩy mạnh công tác phòng ngừa xã hội thông qua tuyên truyền, giáo dục và nâng cao nhận thức cộng đồng. Trong môi trường số, người dân vừa là đối tượng cần được bảo vệ, vừa là chủ thể tham gia trực tiếp vào quá trình phòng ngừa tội phạm. Do đó, cần triển khai thường xuyên các chương trình phổ biến kiến thức pháp luật, kỹ năng an toàn thông tin và nhận diện thủ đoạn của tội phạm công nghệ cao cho các nhóm đối tượng khác nhau trong xã hội. Việc nâng cao "miễn dịch số" cho cộng đồng sẽ góp phần làm giảm cơ hội phạm tội, qua đó nâng cao hiệu quả phòng ngừa một cách bền vững [6, tr. 41].

2.3.5. Tăng cường sự phối hợp liên ngành và trách nhiệm của doanh nghiệp trong phòng, chống tội phạm công nghệ cao là yêu cầu cấp thiết. Các cơ quan công an, tư pháp, thông tin, truyền thông, ngân hàng và doanh nghiệp công nghệ cần xây dựng cơ chế phối hợp chặt chẽ, chia sẻ thông tin kịp thời về các nguy cơ, phương thức phạm tội và đối tượng nghi vấn. Doanh nghiệp cung cấp dịch vụ số cần chủ động đầu tư vào các biện pháp bảo mật, nâng cao khả năng phát hiện và ngăn chặn hành vi gian lận, đồng thời hợp tác tích cực với cơ quan chức năng trong quá trình điều tra và xử lý vi phạm.

2.3.6. Mở rộng và nâng cao hiệu quả hợp tác quốc tế là giải pháp mang tính chiến lược lâu dài. Việt Nam cần tiếp tục tham gia tích cực vào các cơ chế hợp tác song phương và đa phương trong phòng, chống tội phạm mạng, tăng cường trao đổi thông tin, hỗ trợ kỹ thuật và đào tạo nguồn nhân lực. Đồng thời, cần từng bước hài hòa hóa pháp luật trong nước với các điều ước quốc tế, tạo điều kiện thuận lợi cho việc điều tra, truy tố và dẫn độ tội phạm công nghệ cao. Hợp tác quốc tế hiệu quả sẽ góp phần khắc phục những hạn chế về thẩm quyền và biên giới trong không gian mạng.

2.3.7. Đổi mới tư duy và phương thức đấu tranh phòng ngừa là giải pháp mang tính định hướng lâu dài. Công tác phòng, chống tội phạm công nghệ cao cần được đặt trong tổng thể chiến lược bảo đảm an ninh mạng quốc gia và phát triển bền vững kinh tế số. Việc chuyển trọng tâm từ xử lý hậu quả sang phòng ngừa chủ động, từ quản lý đơn lẻ sang quản trị tổng thể sẽ giúp nâng cao hiệu quả đấu tranh trong điều kiện công nghệ không ngừng phát triển. Điều này đòi hỏi sự vào cuộc đồng bộ của cả hệ thống chính trị, sự phối hợp chặt chẽ giữa Nhà nước, doanh nghiệp và xã hội.

Như vậy, các giải pháp đấu tranh phòng ngừa tội phạm công nghệ cao ở Việt Nam hiện nay cần được triển khai một cách toàn diện, đồng bộ và linh hoạt. Việc kết hợp chặt chẽ giữa hoàn thiện pháp luật, nâng cao năng lực con người, ứng dụng công nghệ hiện đại, phát huy vai trò của xã hội và tăng cường hợp tác quốc tế sẽ tạo nền tảng vững chắc để nâng cao hiệu quả phòng, chống tội phạm công nghệ cao, đáp ứng yêu cầu bảo đảm an ninh, trật tự trong bối cảnh chuyển đổi số.

3. Kết luận

Tội phạm công nghệ cao là hệ quả tất yếu của quá trình phát triển khoa học, công nghệ và chuyển

đổi số, đồng thời là một trong những thách thức an ninh phi truyền thống nghiêm trọng đối với mọi quốc gia, trong đó có Việt Nam. Thực tiễn cho thấy, loại tội phạm này không ngừng gia tăng về quy mô, tính chất và mức độ nguy hiểm, với phương thức, thủ đoạn ngày càng tinh vi, linh hoạt, thường xuyên biến đổi và mang tính xuyên quốc gia, gây thiệt hại lớn về kinh tế, xâm phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân, đồng thời tác động tiêu cực đến trật tự an toàn xã hội và niềm tin của người dân trong môi trường số. Trong bối cảnh chuyển đổi số quốc gia diễn ra mạnh mẽ, yêu cầu đặt ra đối với công tác đấu tranh phòng ngừa tội phạm công nghệ cao không chỉ dừng lại ở việc xử lý các vụ việc đã xảy ra mà cần chuyển mạnh sang phòng ngừa chủ động, lấy con người, công nghệ và pháp luật làm ba trụ cột cơ bản. Việc hoàn thiện hệ thống pháp luật theo hướng đồng bộ, linh hoạt, phù hợp với sự phát triển của công nghệ mới; nâng cao chất lượng nguồn nhân lực chuyên trách; tăng cường ứng dụng khoa học, công nghệ hiện đại trong phát hiện, điều tra và xử lý tội phạm; đồng thời đẩy mạnh tuyên truyền, nâng cao nhận thức, kỹ năng số cho người dân và doanh nghiệp là những giải pháp có ý nghĩa quyết định… giúp Việt Nam có thể nâng cao năng lực ứng phó với tội phạm công nghệ cao, góp phần bảo vệ vững chắc chủ quyền không gian mạng quốc gia. Đấu tranh phòng ngừa tội phạm công nghệ cao ở Việt Nam hiện nay là nhiệm vụ vừa cấp bách, vừa lâu dài, đòi hỏi sự vào cuộc đồng bộ của cả hệ thống chính trị, sự phối hợp chặt chẽ giữa các cơ quan nhà nước, doanh nghiệp và cộng đồng xã hội. Việc thực hiện hiệu quả các giải pháp đề xuất không chỉ góp phần bảo đảm an ninh, trật tự an toàn xã hội mà còn tạo nền tảng vững chắc cho sự phát triển bền vững của nền kinh tế số và xã hội số ở Việt Nam trong thời gian tới.

Tài liệu tham khảo

[1] Bộ Công an (2020). *Phòng, chống tội phạm sử dụng công nghệ cao ở Việt Nam - Thực trạng và giải pháp*. NXB Công an nhân dân, Hà Nội.

[2] Bộ Công an (2022). *Kỷ yếu Hội thảo khoa học về phòng, chống tội phạm công nghệ cao trong bối cảnh chuyển đổi số*. Hà Nội.

[3] Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2016). *Bộ luật Hình sự 2015, sửa đổi bổ sung năm 2017*. NXB Chính trị Quốc gia - Sự thật, Hà Nội.

[4] Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2018). *Luật An ninh mạng*. NXB Chính trị Quốc gia Sự thật, Hà Nội.

[5] Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023). *Luật Giao dịch điện tử*. NXB Chính trị Quốc gia Sự thật, Hà Nội.

[6] Trần Hữu Thắng (2022). *Nhận diện thủ đoạn của tội phạm công nghệ cao và yêu cầu đặt ra đối với công tác phòng ngừa.* Tạp chí Khoa học và Giáo dục an ninh, tháng 6.

[7] Võ Anh Phúc, Vũ Thị Thanh Huyền, Trương Anh Dủy, Đỗ Mạnh Hào (2025). *Tội phạm công nghệ cao ở Việt Nam - thực trạng và giải pháp*. Tạp chí Công thương, số 27.