THỰC TRẠNG VÀ GIẢI PHÁP ĐỐI VỚI TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO Ở VIỆT NAM HIỆN NAY

Nguyễn Ngọc Mai*
Trần Tuấn Minh**

Tóm tắt: *Bài viết phân tích về thực trạng tội phạm sử dụng công nghệ cao ở nước ta trong những năm gần đây, nhằm đưa ra bức tranh toàn cảnh về thực trạng cũng như những hạn chế, khó khăn còn tồn tại trong thực tiễn phòng ngừa và đấu tranh chống loại tội phạm này. Trên cơ sở đó, bài viết đề xuất các kiến nghị hoàn thiện pháp luật hình sự nhằm ứng phó hiệu quả với nhóm tội phạm sử dụng công nghệ cao trong kỷ nguyên số.*

Từ khóa: *Tội phạm, công nghệ cao, kỷ nguyên số.*

Abstract: *The article analyzes the current situation of high-tech crime in Vietnam in recent years, aiming to provide an overall picture of the reality as well as the limitations and difficulties that still exist in the practice of preventing and combating this type of crime. On that basis, the article proposes recommendations for improving criminal law to effectively respond to high-tech crime in the digital era.*

Keywords: *Crime, high technology, digital era.*

Đặt vấn đề

Sự phát triển nhanh chóng của công nghệ số và mạng Internet trong những thập niên gần đây đã mang lại nhiều lợi ích to lớn cho đời sống kinh tế-xã hội. Trong kỷ nguyên của cuộc Cách mạng công nghiệp lần thứ tư, Việt Nam đang chứng kiến sự chuyển mình mạnh mẽ với công cuộc chuyển đổi số quốc gia sâu rộng. Sự phát triển vượt bậc của công nghệ thông tin và viễn thông đã đóng vai trò là nền tảng, hạ tầng thúc đẩy các ngành kinh tế khác phát triển nhanh và bền vững. Tính đến đầu năm 2025, Việt Nam đã ghi nhận con số ấn tượng với gần 80 triệu người sử dụng Internet, chiếm gần 79% dân số[1], cùng với đó là sự phủ sóng rộng khắp của các thiết bị thông minh và hạ tầng mạng 4G, 5G. Tuy nhiên, thực tiễn này đồng thời cũng tạo ra những thách thức nghiêm trọng về mặt an ninh, trong đó nổi bật là sự gia tăng của các loại tội phạm sử dụng công nghệ cao. Số liệu thống kê cũng như tài liệu nghiên cứu và thực tiễn phòng chống về tội phạm sử dụng công nghệ cao trên thế giới đã cho thấy nhóm tội phạm này hiện đang là vấn đề toàn cầu, đòi hỏi các nước cần có phản ứng

* ThS., Viện Nhà nước và Pháp luật, Viện Hàn lâm Khoa học xã hội Việt Nam.
** NCS., Viện Nhà nước và Pháp luật, Viện Hàn lâm Khoa học xã hội Việt Nam.
Bài viết thuộc khuôn khổ đề tài cấp cơ sở: "*Chính sách pháp luật hình sự đối với nhóm tội phạm sử dụng công nghệ cao*" của Viện Nhà nước và Pháp luật do ThS. Nguyễn Ngọc Mai làm chủ nhiệm.

[1] Simon Kemp, *Digital 2025: Vietnam*, 3/3/2025, https://datareportal.com/reports/digital-2025-vietnam, truy cập ngày 25/7/2025.

chính sách phù hợp[2]. Với đặc điểm không giới hạn không gian, tính ẩn danh, quy mô xuyên quốc gia và thủ đoạn ngày càng tinh vi, nhóm tội phạm này đã và đang đặt ra yêu cầu cấp thiết đối với hệ thống pháp luật hình sự ở mỗi quốc gia, trong đó có Việt Nam.

Trong bối cảnh chuyển đổi số và hội nhập quốc tế ngày càng sâu rộng, việc nhận diện rõ đặc trưng nhóm tội phạm sử dụng công nghệ cao và hoàn thiện pháp luật hình sự đối với nhóm tội phạm này trở thành yêu cầu cấp thiết. Bài viết này tập trung làm rõ khái niệm, đặc điểm của tội phạm sử dụng công nghệ cao; từ đó phân tích thực trạng và đề xuất kiến nghị hoàn thiện pháp luật hình sự nhằm nâng cao hiệu lực, hiệu quả phòng ngừa và đấu tranh chống nhóm tội phạm sử dụng công nghệ cao ở Việt Nam hiện nay.

1. Khái niệm, đặc điểm về tội phạm sử dụng công nghệ cao

Tội phạm sử dụng công nghệ cao, còn gọi là tội phạm ảo hay tội phạm không gian mạng, được hiểu là mọi hành vi vi phạm pháp luật có liên quan đến máy tính hoặc hệ thống mạng. Máy tính có thể đóng vai trò là công cụ để tiến hành các hoạt động phạm pháp, hoặc chính nó trở thành mục tiêu bị tấn công trong hành vi phạm tội.

Hiện nay vẫn còn tồn tại nhiều thuật ngữ khác nhau về tội phạm sử dụng công nghệ cao như: Tội phạm công nghệ cao (high-tech crime); tội phạm máy tính (computer crime): Tội phạm liên quan đến máy tính (computer-related crime); tội phạm mạng (cybercrime)... Điều này dẫn tới những cách hiểu, quan điểm khác nhau về tội phạm sử dụng công nghệ cao.

Ví dụ, trong Từ điển luật học Black's Law sử dụng thuật ngữ tội phạm máy tính và đưa ra định nghĩa là: "Một hành vi phạm tội có liên quan đến việc sử dụng máy tính, chẳng hạn như phá hoại hoặc đánh cắp dữ liệu được lưu trữ dưới dạng điện tử"[3]. Trong bảng thuật ngữ của mình, Tổ chức Tiêu chuẩn hóa quốc tế (ISO) định nghĩa tội phạm mạng là "việc thực hiện các hành vi phạm pháp trong không gian mạng"[4]. Hoặc, một nghiên cứu định nghĩa tội phạm sử dụng công nghệ cao là: "Hành vi phạm pháp có chủ đích đối với một cá nhân, một nhóm người hay một tổ chức nào đó, gây ảnh hưởng xấu đến danh tiếng của nạn nhân hoặc gây hại về mặt vật chất hoặc tinh thần cho nạn nhân một cách trực tiếp hoặc gián tiếp bằng những công nghệ hiện đại liên quan đến mạng viễn thông như Internet và điện thoại"[5].

Trong pháp luật các quốc gia, khái niệm về tội phạm sử dụng công nghệ cao cũng được ghi nhận rất đa dạng. Tại Mỹ, khái niệm tội phạm sử dụng công nghệ cao – tội phạm mạng được định nghĩa là bất kỳ hành vi vi phạm pháp luật nào được thực hiện thông qua máy tính hoặc mạng Internet[6]. Hoặc, Luật Hình sự năm 1995 của

[2] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P., *Conceptualizing cybercrime: Definitions, typologies and taxonomies*, Forensic sciences, 2(2), 2022, 379-398.

[3] Yemisi Dina, *Cyber Laws and Cybercafes: Analysis of Operational Legislation in some Commonwealth Jurisdictions and the United States*, Security and Software for Cybercafes, 1/2008, p. 222.

[4] Colin Murphy, Understanding Cybercrime, 3/2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf, truy cập ngày 25/7/2025.

[5] Halder, D., & Jaishankar, K., *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global, 2011, pp. 14-16.

[6] US Immigration and Customs Enforcement, What is cybercrime?, https://www.ice.gov/about-ice/his/investigate/cybercrime, truy cập ngày 25/7/2025.

Australia, tội phạm máy tính được định nghĩa "là sự xâm nhập máy tính một cách trái phép; sự sửa đổi trái phép đối với dữ liệu được lưu trữ trong máy tính; bất kỳ hành vi làm cản trở trái phép việc trao đổi thông tin điện tử đến hoặc từ một máy tính"[7]. Ngoài ra, theo Công ước của Hội đồng châu Âu về Tội phạm mạng (Công ước Budapest) năm 2001: Tội phạm mạng còn được hiểu là những hành vi truy cập, cản trở bất hợp pháp việc truyền tải dữ liệu máy tính, can thiệp trái phép dữ liệu, sử dụng trái phép thiết bị, giả mạo, lừa đảo liên quan đến máy tính, vi phạm liên quan đến hình ảnh, khiêu dâm trẻ em, vi phạm quyền tác giả và quyền liên quan qua hệ thống máy tính[8]…

Hiện nay, tại Việt Nam, theo khoản 1 Điều 3 Nghị định số 25/2014/NĐ-CP của Chính phủ ngày 7/4/2014 về Phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao quy định: "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". Đây là một khái niệm còn chung chung, chưa chỉ ra được những đặc trưng cơ bản của loại tội phạm này. Luật An ninh mạng năm 2018 cũng đưa ra khái niệm về 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"[9]. Trong hệ thống các văn bản pháp quy hiện hành của Việt Nam cũng chưa đưa ra một khái niệm hoàn chỉnh về tội phạm sử dụng công nghệ cao, mà chỉ có quy định một số tội cụ thể với những hành vi tương ứng được quy định tại Mục 2, Chương XXI về các hành vi phạm tội có sử dụng công nghệ cao, gồm 9 điều luật từ Điều 285 đến Điều 294 trong Bộ luật Hình sự năm 2015.

Như vậy, về bản chất, có thể hiểu tội phạm sử dụng công nghệ cao là hành vi sử dụng công nghệ thông tin để thực hiện hoặc hỗ trợ một hành vi phạm tội. Theo cách hiểu thông thường hơn, tội phạm sử dụng công nghệ cao được xem là việc sử dụng hoặc khai thác công nghệ thông tin và truyền thông và/hoặc Internet để phạm tội. Có thể lập luận rằng, tội phạm công nghệ cao không phải là một loại tội phạm hoàn toàn mới; nó chỉ đơn giản là một cách thức mới để thực hiện các hành vi phạm tội nói chung.

Từ đó, có thể định nghĩa tội phạm sử dụng công nghệ cao là: "Các hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự, do người có năng lực trách nhiệm hình sự thực hiện với lỗi cố ý, thông qua việc sử dụng, khai thác tri thức chuyên môn, kỹ năng, công cụ, phương tiện công nghệ thông tin, điện tử, viễn thông, mạng Internet và các thiết bị số để xâm phạm đến tính nguyên vẹn, an toàn, bảo mật và khả dụng của hệ thống thông tin, dữ liệu số; hoặc sử dụng các công nghệ này như phương thức, thủ đoạn chủ yếu để xâm phạm quyền sở hữu, trật tự quản lý kinh tế, an ninh quốc gia và các trật tự xã hội khác được pháp luật hình sự bảo vệ, gây ra những

[7] Australian Government, Criminal Code Act 1995, https://www.ato.gov.au/law/view/print?DocID=PAC%2F19950012%2FSch-477.1&PiT=99991231235958, truy cập ngày 25/7/2025.

[8] Nguyễn Đức Hạnh, *Tội phạm mạng, tội phạm sử dụng công nghệ cao, chứng cứ điện tử và những vấn đề đặt ra đối với hoạt động đào tạo ngành luật ngành luật trong các trường đại học ở Việt Nam hiện nay*, Tạp chí Khoa học Đại học Thủ Dầu Một, số 6 (73) 2024, tr.41.

[9] Khoản 7 Điều 2 Luật An ninh mạng năm 2018.

hậu quả nhất định, làm ảnh hưởng đến an ninh quốc gia và trật tự an toàn xã hội".

Từ định nghĩa này, chúng ta có thể dễ dàng nhận thấy các đặc điểm chính của tội phạm sử dụng công nghệ cao thông qua các yếu tố cấu thành tội phạm:

- Về chủ thể: Ngoài yêu cầu chung của chủ thể do luật Hình sự quy định, điều đặc trưng ở đây là chủ thể của loại tội phạm này luôn có trình độ nhất định về công nghệ cao và sử dụng nó như một điều kiện cần để thực hiện hành vi phạm tội. Chủ thể cũng có thể là bất kỳ tổ chức nào có khả năng thực hiện hành vi phạm tội bằng cách sử dụng công nghệ thông tin và mạng Internet.

- Về khách thể: Khách thể bị xâm hại là quyền và lợi ích hợp pháp của các cá nhân, tổ chức, sự ổn định của xã hội, được quy định trong Bộ luật Hình sự, làm ảnh hưởng đến an ninh quốc gia và trật tự an toàn xã hội. Các khách thể này có thể bao gồm an ninh mạng, quyền bảo mật thông tin và dữ liệu, quyền lợi của người tiêu dùng…

- Về mặt chủ quan: Hành vi được thực hiện dưới hình thức là lỗi cố ý hoặc vô ý. Mục đích phạm tội thường là để chiếm đoạt tài sản, thông tin cá nhân, lợi ích tài chính hoặc phá hoại các hệ thống, tổ chức.

- Về mặt khách quan: Đó là các hành vi thông qua việc khai thác, sử dụng công cụ, phương tiện công nghệ thông tin, điện tử, viễn thông, mạng Internet và các thiết bị số để:

+ Xâm nhập hệ thống máy tính (hacking): Lợi dụng các lỗ hổng bảo mật để truy cập trái phép vào hệ thống máy tính, mạng máy tính hoặc dữ liệu.

+ Phát tán phần mềm độc hại (malware, virus, trojan): Cài đặt phần mềm độc hại vào hệ thống của người khác để chiếm đoạt thông tin, gây thiệt hại hoặc phá hoại hệ thống.

+ Lừa đảo qua mạng: Sử dụng các hình thức lừa đảo trực tuyến như giả mạo website, gửi email giả mạo để chiếm đoạt tài sản hoặc thông tin của người khác.

+ Đánh cắp dữ liệu: Chiếm đoạt, làm lộ hoặc sử dụng trái phép thông tin cá nhân của người khác.

+ Tấn công DDoS (Distributed Denial of Service): Sử dụng nhiều máy tính để tấn công và làm nghẽn các hệ thống mạng hoặc website, khiến hệ thống không thể hoạt động bình thường.

2. Thực trạng tội phạm sử dụng công nghệ cao ở Việt Nam hiện nay

2.1. Một số kết quả đạt được trong công tác phòng ngừa và đấu tranh chống tội phạm sử dụng công nghệ cao ở Việt Nam

Trong những năm gần đây, các cơ quan thực thi pháp luật Việt Nam đã chủ động phối hợp phát hiện, điều tra và xử lý nhiều vụ án liên quan đến tội phạm công nghệ cao. Lực lượng chuyên trách về an ninh mạng và phòng ngừa và đấu tranh chống tội phạm sử dụng công nghệ cao, với nòng cốt là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) - Bộ Công an, đã được hình thành và ngày càng khẳng định vai trò xung kích, chủ lực. Mô hình này được tổ chức thống nhất từ Trung ương xuống Công an các tỉnh, thành phố, cho phép tập trung nguồn lực, nghiệp vụ và công nghệ để đối phó hiệu quả với loại tội phạm này. Trong những năm qua, lực lượng này đã phối hợp với công an các địa phương đấu tranh, triệt phá thành công hàng trăm chuyên án, đường dây tội phạm sử dụng công nghệ cao có quy mô lớn, hoạt động có tổ chức và mang tính xuyên quốc gia. Nhiều vụ án điển hình đã gây tiếng vang lớn, thể hiện sự quyết tâm và năng lực của các cơ quan chức năng.

Giai đoạn 2010–2014, lực lượng Cảnh sát phòng chống tội phạm sử dụng công nghệ cao đã tiếp nhận và xử lý gần 100 thông tin, hỗ trợ điều tra nhiều vụ án xuyên quốc gia. Trong một vụ việc, theo yêu cầu của Cảnh sát Liên bang Úc, Việt Nam đã điều tra đường dây nhập lậu thiết bị điện tử trị giá khoảng 2 triệu đô la Úc, có liên quan đến các nhân viên hàng không và hải quan. Hàng hóa chủ yếu là máy tính xách tay bị trộm tại Úc, vận chuyển trái phép về Việt Nam[10].

Cũng trong giai đoạn từ năm 2010 đến 2017, lực lượng Công an Việt Nam đã điều tra gần 200 vụ án lừa đảo qua mạng, chủ yếu do người Trung Quốc thực hiện tại Việt Nam. Trong đó, có vụ điển hình là tháng 5/2019, Bộ Công an phát hiện gần 400 đối tượng Trung Quốc tổ chức đánh bạc trực tuyến tại khu đô thị Our City (Hải Phòng), giao dịch hơn 12.000 tỷ đồng[11]. Sau điều tra, toàn bộ đối tượng và tang vật được bàn giao cho phía Trung Quốc xử lý theo hiệp định hợp tác song phương. Một vụ án lớn khác là đường dây do Vương Huy Long (Tp.Hồ Chí Minh) cầm đầu, chuyên đánh cắp thông tin thẻ tín dụng của công dân Hoa Kỳ và các nước phát triển để mua hàng, sau đó vận chuyển về Việt Nam thông qua hệ thống "Dropper" tại Hoa Kỳ. Vụ án được Bộ Công an Việt Nam phối hợp với Bộ An ninh nội địa Hoa Kỳ triệt phá năm 2013, thu giữ hơn 29.000 thông tin thẻ tín dụng, xác định thiệt hại hơn 15 tỷ đồng và hàng trăm triệu USD. Chuyên án được quốc tế đánh giá cao, nâng uy tín của lực lượng cảnh sát Việt Nam trong hợp tác phòng chống tội phạm mạng[12].

Giai đoạn 2022-2023, Bộ Công an đã chỉ đạo đồng loạt triệt phá hàng trăm ứng dụng (app) cho vay nặng lãi, khủng bố đòi nợ. Điển hình là chuyên án triệt phá 3 nhóm tín dụng đen qua app với lãi suất 900%/ năm (năm 2023)[13]. Điều này đã làm giảm đáng kể tình trạng tín dụng đen trực tuyến vốn gây bức xúc dư luận.

Trong năm 2024-2025, Công an tỉnh Nghệ An phối hợp với Bộ Công an triệt phá đường dây lừa đảo chiếm đoạt hơn 2.000 tỷ đồng do các đối tượng người nước ngoài cầm đầu, hoạt động từ Myanmar và Philippines[14]. Công an tỉnh Hà Tĩnh cũng phối hợp với Công an Lào triệt phá tổ chức tội phạm mua bán người, lừa đảo qua mạng tại đặc khu kinh tế Bò Kẹo (Lào), bắt giữ 155 đối tượng người Việt Nam[15]. Gần đây, Cục Cảnh sát hình sự đã triệt phá đường dây

[10] Trần Văn Doanh, *Hợp tác quốc tế trong phòng, chống tội phạm sử dụng công nghệ cao và vấn đề đặt ra trong công tác đào tạo, bồi dưỡng cán bộ*, Kỷ yếu hội thảo khoa học Phòng, chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo, Học viện Cảnh sát nhân dân tháng 11/2014.

[11] Thế Dũng, *Vụ 395 người Trung Quốc đánh bạc ở Hải Phòng: Việt Nam không thiệt hại gì*!, 04/9/2019, https://nld.com.vn/chinh-tri/vu-395-nguoi-trung-quoc-danh-bac-o-hai-phong-viet-nam-khong-thiet-hai-gi-20190904103959592.htm, truy cập ngày 25/7/2025.

[12] Đỗ Quý Hoàng (2021), tlđd, tr.149.

[13] Phú Lữ, *Triệt phá 3 nhóm đối tượng hoạt động "tín dụng đen" với lãi suất 900%/năm*, 15/12/2023, https://cand.com.vn/tai-chinh-40/triet-pha-3-nhom-doi-tuong-hoat-dong-tin-dung-den-voi-lai-suat-900-nam-i717080, truy cập ngày 25/7/2025.

[14] Trần Trung Hiếu, *Công an Nghệ An triệt xóa băng nhóm lừa đảo công nghệ cao, bắt giữ gần 100 đối tượng*, 25/6/2025, https://nhandan.vn/cong-an-nghe-an-triet-xoa-bang-nhom-lua-dao-cong-nghe-cao-bat-giu-gan-100-doi-tuong-post889352.html, truy cập ngày 25/7/2025.

[15] Thái Huyền, Đức Quang, *Công an Hà Tĩnh triệt phá tổ chức tội phạm lừa đảo quốc tế, bắt giữ 155 đối tượng tại tỉnh Bò Kẹo*, 8/8/2024, https://congan.hatinh.gov.vn/tin-tuc-su-kien/an-ninh-trat-tu/cong-an-ha-tinh-triet-pha-to-chuc-duong-day-lua-dao-chiem-doat-tai-san-tri-gia-tram-ty-tai-dac-khu-kinh-te-tam-giac-vang_1723027183.caht, truy cập ngày 25/7/2025.

lừa đảo quy mô cực lớn do Trần Quang Đạo cầm đầu, chuyên nhắm vào người già trên 50 tuổi, chiếm đoạt hàng trăm tỷ đồng của hàng trăm nghìn nạn nhân[16]. Các vụ án khác như triệt phá đường dây lừa đảo chiếm đoạt tài sản trên không gian mạng của nhóm đối tượng người Trung Quốc lừa đảo trực tuyến tại Tp. Hồ Chí Minh cũng cho thấy sự chủ động và hiệu quả trong công tác trấn áp[17].

Những kết quả trên cho thấy việc triển khai chính sách hình sự và hợp tác quốc tế trong đấu tranh chống tội phạm công nghệ cao tại Việt Nam đã đạt được một số kết quả tích cực, đáng ghi nhận. Nhìn chung, tình hình phòng ngừa, đấu tranh chống tội phạm sử dụng công nghệ cao ở Việt Nam trong thời gian qua đã thể hiện được tư tưởng, quan điểm và sự quyết tâm của Đảng, Nhà nước ta. Cùng với đó, chúng ta đã đạt được nhiều thành tựu, qua đó từng bước hiện đại hóa để phù hợp với điều kiện phát triển công nghệ.

Về hợp tác quốc tế, Việt Nam vẫn luôn hướng tới sự chủ động, tích cực hội nhập trong lĩnh vực tư pháp hình sự và đấu tranh chống tội phạm sử dụng công nghệ cao. Tính đến tháng 9/2017, Việt Nam là thành viên của 22 điều ước quốc tế đa phương về tương trợ tư pháp hình sự, dẫn độ và chuyển giao người bị kết án, cùng với 27 hiệp định song phương về tương trợ tư pháp hình sự và dân sự. Trong số này, nhiều điều ước có nội dung điều chỉnh hành vi tội phạm công nghệ cao hoặc tội phạm xuyên quốc gia có yếu tố sử dụng công nghệ. Tuy nhiên, Việt Nam không coi 10/22 điều ước là cơ sở pháp lý trực tiếp để dẫn độ, ví dụ như Công ước chống tham nhũng 2003, Công ước chống tra tấn… Ngoài ra, Việt Nam đã ký 12 hiệp định dẫn độ song phương với các nước như Hàn Quốc, Pháp, Trung Quốc, Tây Ban Nha, Indonesia…

Gần đây, vào năm 2019, Đại hội đồng Liên hợp quốc đã thông qua Nghị quyết 74/247 thành lập Ủy ban chuyên trách liên chính phủ nghiên cứu khả năng xây dựng một công ước quốc tế toàn diện về chống sử dụng công nghệ thông tin và truyền thông cho mục đích tội phạm. Và, sau 5 năm, đến 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 này sẽ góp phần tạo khuôn khổ pháp lý bao trùm, đáp ứng nhu cầu cấp bách về hợp tác quốc tế nhằm thúc đẩy pháp quyền trong không gian mạng[18]. Lần đầu tiên một địa điểm của Việt Nam được ghi danh và gắn với một điều ước đa phương toàn cầu liên quan đến một lĩnh vực quan trọng và được cộng đồng quốc tế hết sức quan tâm. Việc đăng cai Lễ mở ký "Công ước Hà Nội" cũng là cơ hội để Việt Nam tiếp tục phát huy vai trò một thành viên có trách nhiệm,

[16] Hà Lâm Quang, *Triệt phá đường dây lừa đảo công nghệ cao quy mô "khủng" chuyên nhắm vào người già*, 20/6/2025, https://vtv.vn/phap-luat/triet-pha-duong-day-lua-dao-cong-nghe-cao-quy-mo-khung-chuyen-nham-vao-nguoi-gia-20250620194953301.htm, truy cập ngày 25/7/2025.

[17] ANTV, *Triệt phá đường dây lừa đảo trên mạng với thủ đoạn rất tinh vi*, 29/4/2025, https://antv.gov.vn/pha-an-184/triet-pha-duong-day-lua-dao-chiem-doat-tai-san-tren-khong-gian-mang-do-cac-doi-tuong-nguoi-trung-quoc-cam-dau--6DF22D08A.html, truy cập ngày 25/7/2025.

[18] Văn Lộc, *Công ước Hà Nội: Dấu mốc quan trọng trong đối ngoại đa phương*, 31/12/2024, https://qptd.vn/chong-dien-bien-hoa-binh/lam-that-bai-am-muu-dien-bien-hoa-binh/cong-uoc-ha-noi-dau-moc-quan-trong-trong-doi-ngoai-da-phuong.html, truy cập ngày 25/7/2025.

tin cậy của cộng đồng quốc tế, tích cực thúc đẩy chủ nghĩa đa phương, tham gia dẫn dắt quá trình xây dựng và định hình các khuôn khổ quản trị số toàn cầu, bảo đảm an ninh mạng và chủ quyền quốc gia trên không gian mạng, tạo tiền đề triển khai thành công chiến lược chuyển đổi số để đưa đất nước sẵn sàng bước vào kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc[19].

Sự kết hợp giữa định hướng chính trị rõ ràng của Đảng, hệ thống pháp luật trong nước ngày càng hoàn thiện và sự hội nhập quốc tế sâu rộng đã tạo nên một nền tảng vững chắc cho pháp luật hình sự Việt Nam trong hợp tác quốc tế về đấu tranh với tội phạm sử dụng công nghệ cao. Đây là điều kiện quan trọng để bảo vệ chủ quyền số, an ninh quốc gia và an toàn của người dân trong kỷ nguyên số hóa trên thực tế.

2.2. Những hạn chế, khó khăn còn tồn tại

Bên cạnh những kết quả đạt được, công tác đấu tranh phòng, chống tội phạm sử dụng công nghệ cao vẫn còn tồn tại nhiều khó khăn, hạn chế. Trong những năm gần đây, số người sở hữu các phương tiện điện tử, tài khoản ngân hàng, tham gia các dịch vụ trực tuyến trên mạng Internet tại Việt Nam đang tăng lên rất nhanh. Việc sử dụng Internet và dịch vụ số tại Việt Nam tăng mạnh, với khoảng 93,5 triệu thuê bao smartphone[20], 78,44 triệu người dùng Internet[21] và hạ tầng 4G phủ rộng, 5G đang thử nghiệm. Giao dịch tài chính, mua bán trực tuyến phát triển nhanh, đem lại nhiều tiện ích. Tuy nhiên, tội phạm sử dụng công nghệ cao, đặc biệt là lừa đảo chiếm đoạt tài sản qua mạng, cũng ngày càng phổ biến, tinh vi và phức tạp, gây thiệt hại lớn cho người dân, ảnh hưởng an ninh trật tự, sản xuất kinh doanh và đời sống xã hội. Xu hướng phạm tội này vẫn tiếp tục gia tăng.

Các số liệu thống kê từ các cơ quan chức năng và các tổ chức uy tín đã vẽ nên một bức tranh toàn cảnh về một vấn nạn đang ngày càng lan rộng, gây ra những thiệt hại khổng lồ cho nền kinh tế và sự bất an trong xã hội. Trong 10 năm (2013–2023), cả nước xét xử tổng cộng 592 vụ án tội phạm công nghệ cao, với 1.163 bị cáo. Trong đó, 361 vụ án là tội phạm sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để chiếm đoạt tài sản (theo Điều 290 Bộ luật Hình sự), chiếm 60,98% tổng số vụ tội phạm công nghệ cao. Tỷ lệ này tăng liên tục, đến năm 2022 chiếm 75,45% số vụ án tội phạm công nghệ cao. Về số bị cáo, nhóm tội danh theo Điều 290 có 642 bị cáo, chiếm 55,20% tổng số bị cáo tội phạm công nghệ cao. Riêng trong năm 2022, số bị cáo nhóm này chiếm tới 80,47%, phản ánh xu hướng gia tăng mạnh mẽ và chiếm tỷ lệ áp đảo trong cơ cấu tội phạm công nghệ cao hiện nay[22].

---

[19] TTXVN, *Đại hội đồng Liên hợp quốc thông qua "Công ước Hà Nội" về tội phạm mạng*, 25/12/2024, https://www.qdnd.vn/quoc-te/tin-tuc/dai-hoi-dong-lien-hop-quoc-thong-qua-cong-uoc-ha-noi-ve-toi-pham-mang-808651, truy cập ngày 25/7/2025.

[20] Duy Vũ, *Việt Nam hiện có 93,5 triệu thuê bao sử dụng smartphone*, 29/03/2022, https://vietnamnet.vn/viet-nam-hien-co-935-trieu-thue-bao-su-dung-smartphone-i407583.html, truy cập ngày 25/7/2025.

[21] TTTT, *Internet Việt Nam: Ba mươi năm phát triển thần tốc*, 27/12/2024, https://mst.gov.vn/internet-viet-nam-ba-muoi-nam-phat-trien-than-toc-197241227122858638.htm, truy cập ngày 25/7/2025.

[22] Cao Anh Đức (2023), *Phòng ngừa tình hình tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản tại Việt Nam*, Luận án tiến sĩ luật học, Học viện Khoa học xã hội, Hà Nội.

Theo báo cáo nghiên cứu, khảo sát an ninh mạng năm 2024 do Hiệp hội An ninh mạng quốc gia thực hiện, thiệt hại do lừa đảo trực tuyến tại Việt Nam trong năm 2024 ước tính lên đến 18.900 tỷ đồng (tương đương khoảng 740 triệu USD)[23]. Báo cáo này cũng chỉ ra một tỷ lệ đáng lo ngại: Cứ 220 người sử dụng điện thoại thông minh thì có 1 người trở thành nạn nhân của lừa đảo. Con số thiệt hại này, theo một số nguồn tin khác, có thể lên tới 390.000 tỷ đồng, tương đương 3,6% GDP, trong đó 91% liên quan đến lĩnh vực tài chính, tăng 64,78% so với năm 2022, tỷ lệ người dùng nhận tin nhắn, cuộc gọi lừa đảo là 73%[24]. Theo một thống kê năm 2024 của Bộ Công an, công tác phòng, chống tội phạm và vi phạm pháp luật năm 2024 (từ tháng 10/2023 đến hết tháng 9/2024) đã triệt phá 28 chuyên án tội phạm sử dụng công nghệ cao, khởi tố 22 vụ án, 72 bị can; làm rõ âm mưu, thủ đoạn mới của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng[25]. Theo Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) - Bộ Công an, chỉ tính riêng từ đầu năm 2025 đến nay, đã phát hiện hơn 1.500 kênh, hội nhóm quảng cáo, đánh bạc trực tuyến; hơn 1.500 kênh, hội nhóm hoạt động liên quan giao dịch tiền ảo, tiền mã hóa; gần 200 kênh, hội nhóm có nội dung quảng cáo, mua bán chất gây nghiện… Các hoạt động tấn công mạng cũng diễn ra ngày càng nguy hiểm hơn. Từ năm 2024 đến nay, phát hiện trên 42 triệu cảnh báo tấn công mạng, 420.000 cảnh báo phát hiện mã độc nhằm vào các hệ thống thông tin[26].

Qua xu hướng gia tăng đáng kể của nhóm tội phạm sử dụng công nghệ cao, có thể thấy rõ rằng hệ thống pháp luật hình sự hiện hành ở Việt Nam vẫn còn tồn tại nhiều hạn chế và bất cập, chưa theo kịp sự phát triển nhanh chóng, phức tạp của loại tội phạm này. Cụ thể:

Thứ nhất, hành lang pháp lý còn thiếu đồng bộ, chưa đầy đủ và chậm được hướng dẫn thi hành. Mặc dù Bộ luật Hình sự năm 2015 đã bổ sung các quy định xử lý tội phạm công nghệ cao, nhưng đến nay vẫn chưa có các văn bản hướng dẫn thi hành cụ thể. Điều này gây lúng túng trong quá trình áp dụng và giải thích pháp luật tại các cơ quan tố tụng. Đặc biệt, Tòa án nhân dân tối cao chưa ban hành hướng dẫn xét xử rõ ràng cho các tòa án cấp dưới, dẫn đến khả năng áp dụng không thống nhất, thậm chí bỏ lọt tội phạm. Ngoài ra, trách nhiệm hình sự của pháp nhân thương mại cũng đang bị bỏ sót khi trong 33 tội danh tại Điều 76 không hề có bất kỳ tội nào về tội phạm sử dụng công nghệ cao. Điều này tạo ra một vùng miễn trừ pháp lý cho các doanh nghiệp công nghệ, nhà cung cấp dịch vụ Internet, nền tảng mạng xã hội... dù họ có

[23] HM, *Thiệt hại do lừa đảo trực tuyến ước tính 18.900 tỷ đồng năm 2024*, 16/12/2024, https://baochinhphu.vn/thiet-hai-do-lua-dao-truc-tuyen-uoc-tinh-18900-ty-dong-nam-2024-102241216153209577.htm, truy cập ngày 25/7/2025.

[24] Việt Nga, *Lừa đảo trực tuyến gây thiệt hại 390.000 tỷ đồng, tương đương 3,6% GDP*, 13/5/2024, https://hanoimoi.vn/lua-dao-truc-tuyen-gay-thiet-hai-390-000-ty-dong-tuong-duong-3-6-gdp-666160.html, truy cập ngày 25/7/2025.

[25] Thu Hằng, *Bộ trưởng Công an: Triệt phá 28 chuyên án phạm tội sử dụng công nghệ cao*, 17/10/2024, https://vietnamnet.vn/bo-truong-cong-an-triet-pha-28-chuyen-an-pham-toi-su-dung-cong-nghe-cao-2332657.html, truy cập ngày 25/7/2025.

[26] Chí Hiếu, *Đầu năm 2025 đến nay phát hiện gần 1.500 vụ việc lừa đảo qua mạng*, 5/8/2025, https://tuoitre.vn/dau-nam-2025-den-nay-phat-hien-gan-1-500-vu-viec-lua-dao-qua-mang-20250805220548384.htm, truy cập ngày 10/8/2025.

thể vô tình hoặc cố ý tạo điều kiện cho tội phạm hoạt động.

Một vấn đề nữa liên quan đến hoạt động xử lý tội phạm sử dụng công nghệ cao đó là các quy định về chứng cứ điện tử. Đây được xem là vướng mắc lớn nhất và mang tính nền tảng trong thực tiễn tố tụng hình sự đối với tội phạm công nghệ cao. Mặc dù Bộ luật Tố tụng hình sự năm 2015 đã có một bước tiến khi lần đầu tiên chính thức ghi nhận dữ liệu điện tử là một nguồn chứng cứ (Điều 87, 99); nhưng luật lại thiếu vắng các văn bản dưới luật hướng dẫn chi tiết về quy trình thu thập, phục hồi, giám định và chuyển hóa dữ liệu điện tử thành chứng cứ có thể sử dụng tại tòa. Sự thiếu hụt này dẫn đến khó khăn trong việc đảm bảo 03 thuộc tính của chứng cứ là tính khách quan, tính hợp pháp và tính liên quan. Ngoài ra, các chứng cứ điện tử cũng rất dễ bị xóa, dễ thay đổi và ẩn danh. Việc thu thập chứng cứ điện tử trong nhiều vụ án hết sức khó khăn bởi tội phạm sử dụng công nghệ cao để che giấu thông tin khi có nguy cơ bị lộ thường đánh sập các trang web hoặc xoá bỏ các thông tin liên quan, tiêu hủy thiết bị điện tử, nên việc phục hồi dữ liệu mất nhiều thời gian và không phải trường hợp nào cũng thu thập và phục hồi được[27].

Thứ hai, pháp luật về tội phạm công nghệ cao của Việt Nam thiên về bảo vệ an ninh quốc gia, kiểm soát thông tin và yêu cầu lưu trữ dữ liệu trong nước, nhưng lại chưa đầy đủ về cơ chế bảo vệ người dùng, tổ chức tư nhân và chưa theo kịp sự phát triển nhanh chóng của các loại hình tội phạm mạng. Bộ luật Hình sự quy định một số hành vi như phát tán phần mềm độc hại (Điều 286), nhưng còn thiếu khung pháp lý để ứng phó đối với các hành vi mới. Cụ thể, hiện nay, tội phạm sử dụng công nghệ cao đang áp dụng rất nhiều thủ đoạn mới, tinh vi, phong phú. Trong đó, các thủ đoạn lừa đảo tinh vi sử dụng công nghệ mới như Deepfake, tấn công bằng AI, hay lừa đảo trên các nền tảng tài sản ảo (tiền mã hóa, NFT) hiện chưa được quy định cụ thể trong Bộ luật Hình sự. Hoặc, nhiều hành vi như sử dụng mạng để lừa đảo, xâm nhập hệ thống thông tin quốc phòng, phát tán virus gây gián đoạn vận hành cũng chưa được định danh riêng biệt. Để khởi tố, các cơ quan tố tụng thường phải áp dụng tương tự các tội danh truyền thống như Tội lừa đảo chiếm đoạt tài sản (Điều 174) hoặc Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính (Điều 288). Tuy nhiên, các tội danh này chưa thực sự bao quát được tính chất, mức độ của các thủ đoạn mới này của tội phạm sử dụng công nghệ cao và bị giới hạn trong khung của các tội đó, khiến việc xử lý thiếu linh hoạt và bỏ sót hành vi vi phạm.

Bên cạnh đó, mức phạt tiền trong Bộ luật Hình sự đang có biên độ dao động lớn, thiếu tính thống nhất và khó đảm bảo nguyên tắc phân hóa hình phạt. Một nghiên cứu đã đánh giá nếu so với pháp luật Nhật Bản khi chỉ quy định mức phạt tối đa và để mức tối thiểu tại phần chung, hoặc theo pháp luật Nga là dựa trên tỷ lệ thu nhập thì cách làm của Việt Nam chưa khoa học[28]. Hơn nữa, pháp luật Việt Nam cũng chưa

[27] Cao Anh Đức, Ngô Thị Bích Thu, Biện pháp thu thập, chuyển hóa, sử dụng chứng cứ điện tử trong vụ án sử dụng công nghệ cao, 30/12/2021, https://tapchitoaan.vn/bien-phap-thu-thap-chuyen-hoa-su-dung-chung-cu-dien-tu-trong-vu-an-su-dung-cong-nghe-cao5605.html, truy cập ngày 25/7/2025.

[28] Hà Lệ Thủy, *Phòng chống tội phạm công nghệ cao đáp ứng nhu cầu cải cách tư pháp*, Kỷ yếu hội thảo quốc gia "cải cách tư pháp trong lĩnh vực tư pháp hình sự", Trường Đại học luật (Đại học Huế) - Tạp chí Kiểm sát (Viện Kiểm Sát Nhân Dân Tối Cao), Thừa Thiên Huế, 2021, tr.199.

bao quát đầy đủ các tội phạm truyền thống có sử dụng công nghệ cao như Trung Quốc đã làm trong Điều 285–287 Bộ luật Hình sự của họ.

Thứ ba, công tác hợp tác quốc tế còn nhiều vướng mắc. Quy trình điều tra tố tụng hiện nay còn nặng về hình thức, chưa phù hợp với tính chất đặc thù của tội phạm công nghệ cao. Nhiều vụ án có yếu tố nước ngoài, hàng trăm bị hại ở nhiều quốc gia khác nhau, nhưng cơ quan điều tra vẫn bị yêu cầu phải xác minh và lấy lời khai của tất cả người bị hại, khiến việc điều tra kéo dài và không khả thi trên thực tế[29]. Ngoài ra, mặc dù đã có các quy chế, nhưng sự phối hợp giữa các cơ quan trong nước đôi khi còn mang tính hình thức, thiếu đồng bộ và kịp thời. Đặc biệt, do tính chất xuyên quốc gia của tội phạm sử dụng công nghệ cao, việc yêu cầu tương trợ tư pháp hình sự để thu thập chứng cứ, xác minh và dẫn độ đối tượng gặp rất nhiều khó khăn do sự khác biệt về hệ thống pháp luật, thời gian kéo dài (có thể lên đến hàng năm), và không phải lúc nào cũng nhận được sự hợp tác đầy đủ từ phía nước ngoài[30]. Tội phạm có thể tẩu tán tài sản hoặc xóa dấu vết trước khi yêu cầu tương trợ được thực hiện. Hiện, Việt Nam mới chỉ ký kết Hiệp định tương trợ tư pháp với 21 quốc gia; nhiều quy định của pháp luật Việt Nam chưa tương thích với luật pháp các nước, nên gặp khó khăn trong thực hiện ủy thác tư pháp và hợp tác quốc tế xử lý tội phạm sử dụng công nghệ cao[31]. So với Luật Sử dụng máy tính 1993 (sửa đổi 2020) của Singapore hay CFAA và CISA của Hoa Kỳ[32], pháp luật Việt Nam thiếu tính phân loại tội phạm rõ ràng, chưa có cơ chế phối hợp điều tra, chia sẻ dữ liệu liên ngành và chưa tham gia các điều ước quốc tế như Công ước Budapest về tội phạm mạng, làm giảm hiệu lực đấu tranh với tội phạm công nghệ cao xuyên biên giới.

Thứ tư, năng lực cán bộ tiến hành tố tụng ở Việt Nam vẫn là điểm nghẽn lớn trong phòng, chống tội phạm công nghệ cao. Dù Bộ luật Tố tụng Hình sự năm 2015 đã bổ sung nguồn chứng cứ điện tử, song để thu thập, phân tích và sử dụng hiệu quả loại chứng cứ này đòi hỏi điều tra viên phải có kỹ năng, kiến thức chuyên sâu về công nghệ thông tin, mạng viễn thông, điều mà đội ngũ hiện nay còn rất thiếu[33]. Nhìn chung, lực lượng chuyên trách của chúng ta hiện tại còn mỏng, thiếu chuyên gia đầu ngành, và các trang thiết bị phục vụ công tác phục hồi dữ liệu từ các thiết bị di động, máy chủ bị mã hóa (đặc biệt là các thiết bị đời mới của Apple, Google) chưa đáp ứng kịp yêu cầu. Năng lực giám định tư pháp về kỹ thuật số và điện tử cũng còn non trẻ, chưa đáp ứng được yêu cầu của thực tiễn.

---

[29] Trần Đoàn Hạnh, *Những vướng mắc trong đấu tranh, xử lý vi phạm pháp luật về tội phạm công nghệ cao*, Tạp chí Nghiên cứu lập pháp, 01/01/2016, https://lapphap.vn/Pages/TinTuc/208376/Nhung-vuong-mac-trong-dau-tranh--xu-ly-vi-pham-phap-luat-ve-toi-pham-cong-nghe-cao.html, truy cập ngày 25/7/2025.

[30] Nguyễn Thanh Liêm, Một số vấn đề về tương trợ tư pháp hình sự của Việt Nam, https://vksquangngai.gov.vn/mot-so-van-de-ve-tuong-tro-tu-phap-hinh-su-cua-viet-nam-2161.html, truy cập ngày 25/7/2025.

[31] Cao Anh Đức, Ngô Thị Bích Thu, Biện pháp thu thập, chuyển hóa, sử dụng chứng cứ điện tử trong vụ án sử dụng công nghệ cao, https://tapchitoaan.vn/bien-phap-thu-thap-chuyen-hoa-su-dung-chung-cu-dien-tu-trong-vu-an-su-dung-cong-nghe-cao5605.html, truy cập ngày 25/7/2025.

[32] Nguyen Van Khoat, *Analysis and recommendations for the Vietnam's legal framework on cybercrime*, Indonesian Law Journal, 13(1) 2025, 73–94. https://doi.org/10.15408/jch.v13i1.44612.

[33] Hà Lệ Thủy, tlđd, tr.200.

Thứ năm, hạn chế về nhận thức và công tác phòng ngừa. Mặc dù đã tuyên truyền rất nhiều, nhưng thực tế cho thấy một bộ phận không nhỏ người dân vẫn thiếu cảnh giác. Các thủ đoạn lừa đảo "việc nhẹ lương cao", "đầu tư sinh lời khủng", "combo du lịch giá rẻ" hay giả danh cơ quan công quyền... vẫn liên tục tìm được nạn nhân mới. Điều này xuất phát từ tâm lý ham lợi nhuận nhanh, sự sợ hãi, hoặc thiếu kỹ năng số cơ bản. Bên cạnh đó, nhiều nạn nhân (đặc biệt là các vụ lừa đảo tình cảm, lộ clip nhạy cảm) thường không trình báo cơ quan công an vì xấu hổ, hoặc vì số tiền bị lừa không quá lớn. Điều này vô hình trung tạo điều kiện cho tội phạm tiếp tục hoạt động và khiến cơ quan chức năng không có bức tranh toàn cảnh về tình hình tội phạm.

3. Kiến nghị nâng cao hiệu quả phòng ngừa và đấu tranh chống tội phạm sự dụng công nghệ cao ở Việt Nam

Việt Nam được đánh giá là một trong những quốc gia có tốc độ phát triển công nghệ thông tin, viễn thông nhanh nhất trên thế giới[34]. Dự báo trong thời gian tới, tình hình tội phạm sử dụng công nghệ cao trong tương lai gần sẽ còn phức tạp hơn nữa, với sự xuất hiện của các công cụ và phương thức tấn công mới, tinh vi hơn, dựa trên nền tảng các công nghệ đột phá.

Để nâng cao hiệu quả phòng ngừa và đấu tranh chống nhóm tội phạm sử dụng công nghệ cao trong bối cảnh số hóa mạnh mẽ và tính chất xuyên biên giới ngày càng rõ rệt, Việt Nam cần tập trung hoàn thiện pháp luật hình sự theo một số hướng sau:

Thứ nhất, cần rà soát, xây dựng hệ thống văn bản hướng dẫn thi hành Bộ luật Hình sự và Bộ luật Tố tụng hình sự liên quan đến tội phạm sử dụng công nghệ cao. Đây là yêu cầu cấp thiết nhất để đối phó hiệu quả với tội phạm sử dụng công nghệ cao. Việc hoàn thiện pháp luật hình sự cần được triển khai một cách toàn diện, đồng bộ, bao gồm cả luật nội dung (quy định về tội phạm và hình phạt) và luật hình thức (quy định về trình tự, thủ tục tố tụng).

Về luật nội dung, trong Bộ luật Hình sự, chúng ta cần chú ý đến việc đưa ra một định nghĩa cụ thể đối với nhóm tội phạm sử dụng công nghệ cao. Bởi lẽ, thông qua việc xác định chính xác đối tượng, chúng ta mới có thể có phương hướng cụ thể để phòng ngừa và đấu tranh chống loại tội phạm này. Cụ thể, nhóm tác giả đề xuất khái niệm về tội phạm sử dụng công nghệ cao là: "Các hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự, do người có năng lực trách nhiệm hình sự thực hiện với lỗi cố ý, thông qua việc sử dụng, khai thác tri thức chuyên môn, kỹ năng, công cụ, phương tiện công nghệ thông tin, điện tử, viễn thông, mạng Internet và các thiết bị số để xâm phạm đến tính nguyên vẹn, an toàn, bảo mật và khả dụng của hệ thống thông tin, dữ liệu số; hoặc sử dụng các công nghệ này như phương thức, thủ đoạn chủ yếu để xâm phạm quyền sở hữu, trật tự quản lý kinh tế, an ninh quốc gia và các trật tự xã hội khác được pháp luật hình sự bảo vệ, gây ra những hậu quả nhất định, làm ảnh hưởng đến an ninh quốc gia và trật tự an toàn xã hội".

Bên cạnh đó, Bộ luật Hình sự cũng cần hoàn thiện trách nhiệm hình sự của pháp

[34] Trần Bình, *Việt Nam là 1 trong 10 nước có tốc độ phát triển ICT nhanh nhất thế giới*, 29/3/2009, https://www.sggp.org.vn/viet-nam-la-1-trong-10-nuoc-co-toc-do-phat-trien-ict-nhanh-nhat-the-gioi-post359348.html, truy cập ngày 25/7/2025; Vân Anh, *Việt Nam đã vào tốp 10 quốc gia phát triển nhất thế giới về viễn thông*, 27/9/2018, https://vov.vn/cong-nghe/viet-nam-da-vao-top-10-quoc-gia-phat-trien-nhat-the-gioi-ve-vien-thong-819019.vov, truy cập ngày 25/7/2025.

nhân thương mại phạm tội đối với nhóm tội phạm sử dụng công nghệ cao. Bộ luật Hình sự hiện hành không quy định trách nhiệm hình sự của pháp nhân thương mại đối với bất kỳ tội danh nào trong lĩnh vực công nghệ thông tin, mạng viễn thông (Chương XXI). Đây là một khoảng trống pháp lý nghiêm trọng, không phù hợp với thực tiễn khi nhiều công ty công nghệ, nhà cung cấp dịch vụ có thể trực tiếp hoặc gián tiếp hưởng lợi từ các hoạt động tội phạm trên nền tảng của mình. Do đó, cần khẩn trương nghiên cứu, sửa đổi Điều 76 Bộ luật Hình sự theo hướng bổ sung các tội danh tại Mục 2, Chương XXI vào danh mục các tội mà pháp nhân thương mại phải chịu trách nhiệm hình sự. Bên cạnh đó, vẫn cần tiếp tục hoàn thiện hệ thống hình phạt theo hướng nghiêm khắc hơn đối với các đối tượng chủ mưu, cầm đầu, phạm tội có tổ chức, xuyên quốc gia. Đồng thời, tăng cường áp dụng các hình phạt bổ sung như cấm hành nghề, cấm đảm nhiệm chức vụ liên quan đến công nghệ thông tin, tịch thu tài sản để triệt tiêu nguồn lực kinh tế của tội phạm.

Về luật hình thức, trong Bộ luật Tố tụng hình sự, chúng ta cần chú trọng đánh giá những bất cập và hạn chế liên quan đến "dữ liệu điện tử" và "chứng cứ là dữ liệu điện tử". Tòa án nhân dân tối cao nên ban hành án lệ hoặc nghị quyết hướng dẫn cụ thể đối với quy trình thu thập, bảo quản chứng cứ điện tử, dữ liệu điện tử. Bởi lẽ, như đã phân tích ở trên, mặc dù Bộ luật Tố tụng hình sự năm 2015 đã công nhận dữ liệu điện tử là một nguồn chứng cứ, nhưng lại thiếu các văn bản hướng dẫn chi tiết về quy trình thu thập, phục hồi, giám định và sử dụng. Cần sớm ban hành một Thông tư liên tịch giữa Bộ Công an, Viện kiểm sát nhân dân tối cao, Tòa án nhân dân tối cao hoặc một Nghị quyết của Hội đồng Thẩm phán Tòa án nhân dân tối cao để hướng dẫn chi tiết về vấn đề này. Văn bản cần quy định rõ về quy trình thu thập, niêm phong, sao lưu để đảm bảo tính nguyên vẹn và chuỗi hành trình quản lý của chứng cứ; tiêu chuẩn kỹ thuật cho hoạt động giám định; và cách thức trình bày, đánh giá chứng cứ điện tử tại phiên tòa.

Thứ hai, cần hiện đại hóa quy trình điều tra, truy tố và xét xử tội phạm công nghệ cao. Điều này bao gồm việc tinh giản các yêu cầu hình thức không cần thiết (như yêu cầu lấy lời khai từng nạn nhân ở nhiều quốc gia), và tăng cường áp dụng các biện pháp điều tra đặc biệt như thu thập dữ liệu điện tử từ xa, giám định kỹ thuật số, truy vết IP, định danh số. Đồng thời, cần xây dựng cơ chế chia sẻ dữ liệu liên ngành giữa công an, kiểm sát, tòa án, và các doanh nghiệp cung cấp dịch vụ số. Chúng ta cũng cần nghiên cứu việc tội phạm hóa các hành vi mới một cách linh hoạt. Thay vì chờ đợi các vụ việc xảy ra rồi mới phản ứng, cần chủ động nghiên cứu để hình sự hóa các hành vi mới. Đồng thời, cần rà soát lại các tội danh trong Mục 2 Chương XXI Bộ luật Hình sự năm 2015 để khắc phục sự chồng chéo, thiếu tính khái quát. Nên sửa đổi các quy định theo hướng trung lập về công nghệ, tập trung vào bản chất của hành vi xâm phạm (ví dụ: truy cập trái phép, can thiệp trái phép vào dữ liệu...) thay vì mô tả các thủ đoạn công nghệ cụ thể, vốn rất dễ trở nên lạc hậu.

Ngoài ra, cần sửa đổi, bổ sung Bộ luật Hình sự theo hướng phân loại cụ thể các nhóm hành vi phạm tội công nghệ cao, tách biệt giữa các tội sử dụng công nghệ để chiếm đoạt tài sản, xâm phạm bí mật đời tư, xâm phạm an ninh mạng, tấn công hạ tầng số... Có thể tham khảo mô hình

của Singapore (Computer Misuse Act) hay Hoa Kỳ (CFAA, CISA), theo đó tội phạm mạng được phân nhóm chi tiết, phù hợp với đặc điểm kỹ thuật và mục tiêu tấn công. Đồng thời, cách quy định hình phạt cũng cần điều chỉnh để đảm bảo tính phân hóa – có thể áp dụng cách tính theo mức thu nhập như Bộ luật Hình sự của Nga, hoặc chỉ quy định mức tối đa như Bộ luật Hình sự Nhật Bản để tạo linh hoạt trong định lượng hình phạt[35].

Thứ tư, Việt Nam cần tích cực, chủ động hơn trong việc đàm phán, ký kết các hiệp định tương trợ tư pháp hình sự song phương và đa phương, đặc biệt là tập trung vào các lĩnh vực như trao đổi thông tin, phối hợp phòng ngừa, ngăn chặn và đào tạo cán bộ. Đồng thời, cần khẩn trương nghiên cứu, xem xét việc gia nhập Công ước Budapest về Tội phạm mạng. Đây là bước đi chiến lược, giúp Việt Nam tiếp cận mạng lưới hợp tác quốc tế 24/7, rút ngắn đáng kể thời gian và nâng cao hiệu quả của hoạt động tương trợ tư pháp, vốn đang gặp nhiều khó khăn, chậm trễ.

Ngoài ra, hiện nay Việt Nam đang chuẩn bị tổ chức Lễ mở ký Công ước Liên hợp quốc về chống tội phạm mạng tại Hà Nội vào tháng 10 năm 2025. Đây không chỉ là một sự công nhận của cộng đồng quốc tế đối với vị thế của Việt Nam, mà còn là một thành tựu ngoại giao pháp lý thực chất. Bằng việc chủ động tham gia đàm phán, Việt Nam đã góp phần xây dựng nên một văn kiện pháp lý toàn cầu đầu tiên về lĩnh vực này, tạo ra cơ chế hợp tác chính thức (như Mạng lưới 24/7) để giải quyết điểm nghẽn lớn nhất mà chúng ta gặp phải đó là sự bất lực trong truy vết và thu thập chứng cứ khi tội phạm ẩn náu ở nước ngoài. Do đó, chúng ta cần khẩn trương phê chuẩn và nội luật hóa toàn diện các quy định của Công ước vào BLHS và Bộ luật tố tụng hình sự, đặc biệt là các quy định về chứng cứ điện tử và tội phạm hóa các hành vi mới. Bên cạnh đó, Việt Nam cần dùng Công ước để thúc đẩy các cơ chế hợp tác song phương linh hoạt hơn, như thành lập các Tổ công tác liên hợp với các nước láng giềng để chia sẻ thông tin tình báo và phối hợp, không cho tội phạm có thời gian trốn chạy hay xóa dấu vết. Cuối cùng, cần tăng cường hợp tác công - tư (PPP), xây dựng kênh liên lạc ưu tiên với các công ty công nghệ lớn như Google, Facebook để đẩy nhanh tốc độ xử lý các yêu cầu cung cấp dữ liệu phục vụ điều tra.

Thứ năm, tăng cường đầu tư cho đào tạo và phát triển năng lực cán bộ tư pháp trong lĩnh vực công nghệ thông tin. Đây là điều kiện tiên quyết để áp dụng pháp luật hiệu quả. Các cơ quan chức năng, đặc biệt là lực lượng Công an, cần thường xuyên tổng kết, rút kinh nghiệm từ các chuyên án đã đấu tranh thành công. Từ đó, xây dựng các tài liệu, cẩm nang nghiệp vụ để phổ biến, cảnh báo về các phương thức, thủ đoạn phạm tội mới cho các cơ quan tiến hành tố tụng trên cả nước, giúp nâng cao khả năng nhận diện và đấu tranh hiệu quả. Đồng thời, chúng ta cần xây dựng các chương trình đào tạo, bồi dưỡng chuyên sâu, cập nhật liên tục kiến thức về công nghệ và pháp luật cho đội ngũ Điều tra viên, Kiểm sát viên, Thẩm phán. Trên cơ sở những phản hồi thực tiễn trong quá trình công tác, các cơ sở đào tạo và bồi dưỡng sẽ điều chỉnh chương trình, mục tiêu, nội dung và phương pháp giảng dạy một cách phù hợp, nhằm đáp ứng yêu cầu thực tế của

[35] Hà Lệ Thủy, tlđd, tr.198-199.

công tác phòng ngừa và đấu tranh chống nhóm tội phạm sử dụng công nghệ cao.

Bên cạnh đó, đầu tư trang thiết bị, cơ sở vật chất là một nội dung không thể thiếu trong công tác phòng ngừa và đấu tranh chống nhóm tội phạm sử dụng công nghệ cao. Nhà nước cần ưu tiên đầu tư, hiện đại hóa trang thiết bị, phương tiện kỹ thuật cho các lực lượng chuyên trách, đặc biệt là các phòng thí nghiệm giám định kỹ thuật số, các phần mềm phân tích dữ liệu lớn và truy vết giao dịch tiền mã hóa. Việc ứng dụng các công nghệ hiện đại như camera giám sát, thiết bị bay không người lái, hệ thống định vị GPS cũng cần được tăng cường.

Thứ sáu, nâng cao nhận thức về tội phạm sử dụng công nghệ cao. Công tác phòng ngừa và đấu tranh chống nhóm tội phạm sử dụng công nghệ cao sẽ cần tới sự phối hợp giữa các cơ quan, tổ chức để đẩy mạnh việc tuyên truyền, nâng cao ý thức và trách nhiệm của người dân, hướng dẫn người dân, tổ chức tham gia phòng ngừa, đấu tranh với nhóm tội phạm này. Trong đó, các giải pháp nâng cao nhận thức cần phải phù hợp với từng nhóm đối tượng, qua đó mới có thể truyền tải được thông điệp tới người dân. Cụ thể:

- Đối với nhóm người cao tuổi: Cần phải tuyên truyền thông qua các tổ chức như tổ dân phố, hội người cao tuổi, hội cựu chiến binh… Trong đó, các nội dung sẽ tập trung vào kịch bản giả danh công an, viện kiểm sát, điện lực. Phải truyền thông điệp đơn giản: "Tất cả cơ quan công quyền không bao giờ làm việc qua điện thoại. Nếu yêu cầu chuyển tiền là lừa đảo 100%".

- Đối với nhóm học sinh, sinh viên: Đẩy mạnh tuyên truyền qua các kênh phương tiện, nền tảng xã hội trực tuyến như Facebook, Tiktok, Youtube… Nội dung và thông điệp cần chỉ ra các kịch bản như về lừa đảo tuyển cộng tác viên, đầu tư tài chính và lừa đảo tình cảm.

- Đối với nhóm văn phòng, người lao động: Cần đưa ra nội dung cảnh báo tội phạm công nghệ cao trong các buổi tập huấn, đào tạo nội bộ, qua các kênh nội bộ… Nội dung sẽ tập trung vào các hoạt động lừa đảo qua email, tín dụng đen, mã độc, xuất khẩu lao động,…

Kết luận

Trong bối cảnh cách mạng công nghiệp lần thứ tư và chuyển đổi số diễn ra mạnh mẽ, tội phạm sử dụng công nghệ cao không chỉ gây ra những hậu quả nghiêm trọng về kinh tế-xã hội, mà còn đặt ra thách thức lớn đối với hệ thống pháp luật hình sự hiện hành. Việt Nam đã có những nỗ lực đáng ghi nhận trong việc ban hành và hoàn thiện các quy định pháp luật nhằm phòng, chống loại tội phạm này, song thực tiễn vẫn cho thấy nhiều khoảng trống, bất cập cả về mặt pháp lý lẫn tổ chức thực thi. Hệ thống pháp luật hình sự hiện chưa theo kịp tốc độ phát triển của công nghệ và sự biến đổi nhanh chóng của phương thức phạm tội. Quy định pháp luật còn thiếu cụ thể, chưa được hướng dẫn đầy đủ, trong khi năng lực của đội ngũ cán bộ thực thi còn hạn chế, đặc biệt trong tiếp cận và xử lý chứng cứ điện tử, phối hợp quốc tế và điều tra xuyên biên giới. Do đó, việc tiếp tục hoàn thiện pháp luật hình sự theo hướng hiện đại, chuyên biệt hóa tội danh, nâng cao năng lực đội ngũ cán bộ tư pháp và mở rộng hợp tác quốc tế là yêu cầu cấp thiết. Những cải cách này không chỉ giúp nâng cao hiệu quả đấu tranh phòng, chống tội phạm công nghệ cao, mà còn góp phần bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân trong không gian mạng, đảm bảo an ninh quốc gia và trật tự an toàn xã hội trong kỷ nguyên số.