XU HƯỚNG PHÁT TRIỂN CỦA PHÁP LUẬT VỀ TỘI PHẠM MẠNG TRONG GIAI ĐOẠN PHÁT TRIỂN MỚI CỦA ĐẤT NƯỚC

TRẦN HỮU TRÁNG*

Tóm tắt: Bài viết phân tích các xu hướng phát triển của pháp luật hình sự quốc tế về các tội phạm mạng trên cơ sở so sánh giữa Công ước Budapest về tội phạm mạng năm 2001 với Công ước của Liên hợp quốc về chống tội phạm mạng năm 2024; phân tích các xu hướng phát triển của pháp luật hình sự Việt Nam về các tội phạm mạng. Từ đó, kiến nghị hướng hoàn thiện các quy định về tội phạm mạng trong pháp luật hình sự Việt Nam bảo đảm tương thích với pháp luật quốc tế cũng như đáp ứng yêu cầu phòng, chống tội phạm trong giai đoạn phát triển mới của đất nước.

Từ khóa: Pháp luật hình sự; tội phạm mạng; Công ước Budapest; Công ước của Liên hợp quốc về chống tội phạm mạng năm 2024

Ngày nhận bài: 10/7/2025; Biên tập xong: 03/8/2025; Duyệt đăng: 22/8/2025

DEVELOPMENT TRENDS OF LAW ON CYBERCRIMES IN VIETNAM'S NEW DEVELOPMENT STAGE

Abstract: The article analyzes the development trends of international criminal law on cybercrimes based on a comparison between the 2001 Budapest Convention on Cybercrime and the 2024 United Nations Convention against Cybercrime; analyzes the development trends of Vietnamese criminal law on cybercrimes. From there, it recommends directions for perfecting the provisions on cybercrimes in Vietnamese criminal law to ensure compatibility with international law as well as meet the requirements of crime prevention and control in the new development stage of the country.

Keywords: Criminal law; cybercrime; the Budapest Convention; the 2024 United Nations Convention against Cybercrime

Received: Jul 10, 2025; Editing completed: Aug 03, 2025; Accepted for publication: Aug 22, 2025

Đặt vấn đề

Xu hướng phát triển của pháp luật *"là những định hướng phát triển của pháp luật đang được định hình hoặc đã được định hình, chứng minh về sự tiến triển của vật chất pháp luật nói chung (ở mức độ toàn cầu hoặc ở mức độ khác) hoặc của các bộ phận cấu thành cụ thể của vật chất pháp luật (các ngành luật, các chế định pháp luật…)"*[1]. Như vậy, xu hướng phát triển của pháp luật hình sự về các tội phạm mạng trong kỷ nguyên mới được hiểu là những định hướng phát triển của pháp luật hình sự đang định hình hoặc đã định hình về tiến triển của pháp luật hình sự quốc tế cũng như ở các quốc gia về tội phạm mạng. Phân tích xu hướng phát triển của tội phạm mạng trên thế giới trong sự so sánh với xu hướng phát triển của tội phạm mạng trong pháp luật hình sự Việt Nam không chỉ cho thấy sự tương đồng mà còn là cơ sở để kiến nghị hướng hoàn thiện pháp luật hình sự Việt Nam về tội phạm mạng trong bối cảnh cách mạng 4.0, kinh tế số, xã hội số và trí tuệ nhân tạo (Artificial intelligence - AI), Internet vạn vật (Internet of Things - IoT), dữ liệu lớn, điện toán đám mây đang dần trở thành những công cụ sản xuất quan trọng trong nhiều ngành, nhiều lĩnh vực của nền kinh tế.

1. Khái niệm về tội phạm mạng

Hiện nay, trên thế giới cũng như ở Việt Nam vẫn chưa có sự thống nhất về nội hàm của khái niệm "Tội phạm mạng". Các tác giả Ammar Yassir và Smitha Nayak cho rằng: *"Tội phạm mạng được hiểu khái quát nhất*

[1] Võ Khánh Vinh, "Toàn cầu hóa và các xu hướng phát triển của pháp luật", *Tạp chí Nhà nước và Pháp luật*, số 7/2017, tr. 25-36 (30).

** Email: Huutrangstran@gmail.com*

Phó Giáo sư, Tiến sĩ, Phó Trưởng khoa phụ trách, Khoa Pháp luật hình sự và Kiểm sát hình sự, Trường Đại học Kiểm sát

là hành vi phạm tội thông qua việc sử dụng máy tính hoặc Internet"[2]. Osman Goni cho rằng, *"Tội phạm mạng là bất kỳ hành vi phạm tội nào diễn ra trên hoặc thông qua phương tiện máy tính hoặc Internet hoặc công nghệ khác được quy định trong Đạo luật Công nghệ Thông tin… Theo cách hiểu rộng hơn, tội phạm mạng bao gồm bất kỳ hành vi phạm tội nào mà máy tính hoặc Internet là công cụ hoặc mục tiêu của hành vi phạm tội hoặc cả hai"*[3]. Định nghĩa này đã nêu cụ thể hai nhóm tội phạm mạng là: 1) Nhóm hành vi phạm tội mà trong đó máy tính hoặc mạng máy tính là mục tiêu hoặc nơi diễn ra hành vi phạm tội, từ bẻ khóa điện tử đến các cuộc tấn công từ chối dịch vụ… 2) Nhóm các tội phạm sử dụng máy tính, Internet như là công cụ để thực hiện hành vi phạm tội, như hành vi sử dụng máy tính, Internet để lừa đảo trực tuyến nhằm chiếm đoạt tài sản. Cơ quan Cảnh sát Quốc gia Hà Lan định nghĩa tội phạm mạng là bất kỳ hành vi phạm tội nào mà việc sử dụng các thiết bị hoặc hệ thống máy tính để xử lý và truyền dữ liệu là một yếu tố quan trọng trong hành vi phạm tội, bao gồm cả các hành vi phạm tội "truyền thống" được thực hiện với sự trợ giúp của máy tính và Internet, như gian lận trực tuyến, lừa đảo qua cửa hàng trực tuyến và rửa tiền điện tử[4]... Như vậy, có thể thấy, kể cả các nhà khoa học cũng như người làm công tác thực tiễn đều định nghĩa tội phạm mạng là các hành vi phạm tội mà trong đó, máy tính hoặc mạng máy tính là mục tiêu hoặc nơi diễn ra hành vi phạm tội và các hành vi phạm tội sử dụng máy tính, Internet như là công cụ để thực hiện hành vi phạm tội.

2. Xu hướng phát triển của pháp luật hình sự quốc tế về các tội phạm mạng

Công ước Budapest về tội phạm mạng (gọi tắt là Công ước Budapest năm 2001) đã đưa ra đánh giá về xu hướng của tội phạm mạng: *"Nhận thức được những thay đổi sâu sắc trong tiến trình số hóa, hội nhập và toàn cầu hóa của mạng máy tính; Quan ngại về nguy cơ các mạng máy tính và thông tin điện tử có thể được sử dụng để thực hiện các hành vi phạm tội và chứng cứ liên quan đến các hành vi phạm tội đó có thể được lưu trữ và chuyển giao qua các mạng máy tính và thông tin điện tử này"*[5]. Từ đó, Công ước đưa ra 04 nhóm tội danh được coi là tội phạm mạng, gồm: Nhóm 1 là các tội xâm phạm tính bảo mật, toàn vẹn và tính khả dụng của hệ thống dữ liệu máy tính, gồm truy cập bất hợp pháp (Illegal access); chặn dữ liệu bất hợp pháp (Illegal interception); can thiệp dữ liệu (Data interference); can thiệp hệ thống (System interference) và sử dụng sai mục đích các thiết bị (Misuse of devices); Nhóm 2 là các tội phạm liên quan đến máy tính, gồm tội làm giả dữ liệu liên quan đến máy tính (Computer-related forgery) và tội gian lận liên quan đến máy tính (Computer-related fraud); Nhóm 3 là các tội phạm liên quan đến nội dung - khiêu dâm trẻ em (Content-related offences - Offencesrelated to child pornography); và Nhóm 4 là các tội xâm phạm bản quyền và quyền liên quan thông qua hệ thống máy tính (Offences related to infringements of copyright and related rights)[6].

Công ước của Liên hợp quốc về chống tội phạm mạng (gọi tắt là Công ước LHQ năm 2024) được thông qua ngày 24/12/2024, tại phần mở đầu đã đưa ra khuyến cáo *"Lưu ý rằng công nghệ thông tin và truyền thông, một mặt có tiềm năng to lớn thúc đẩy sự phát triển của xã hội, mặt khác cũng tạo ra những cơ hội mới cho người phạm tội, có thể góp phần làm gia tăng tỷ lệ và tính đa dạng của các hành vi phạm tội…"*. Khuyến cáo này cho thấy, việc lợi dụng công nghệ thông tin, mạng máy tính, mạng viễn thông phạm tội không chỉ làm gia tăng tính đa dạng, phức tạp của hành

[2] Ammar Yassir, Smitha Nayak, "Cybercrime: A threat to Network Security", *International Journal of Computer Science and Network Security*, No. 2(12)/2012, p. 84-88.

[3] Osman Goni, "Introduction to Cyber Crime", *International Journal of Engineering and Artificial Intelligence*, No. 1(3)/2022, p. 9-23 (9).

[4] Geralda Odinot, Maite Verhoeven, Ronald Pool, Christianne De Poot (2017), "Organised Cybercrime in the Netherlands", *Empirical findings and implications for law enforcement*, tr. 22, https://www.researchgate.net/publication/313706519.

[5] Lời nói đầu của Công ước Budapest năm 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[6] Mục 1, Chương II của Công ước Budapest năm 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

vi phạm tội, mở rộng phạm vi thực hiện tội phạm ra nhiều lĩnh vực mới, mà còn gây ra các hậu quả ngày càng nguy hiểm cho xã hội.

Chương 2 của Công ước xác định các dạng hành vi được coi là tội phạm mạng, từ Điều 7 đến Điều 17, gồm: Truy cập bất hợp pháp; Chặn dữ liệu bất hợp pháp; Can thiệp vào dữ liệu điện tử; Can thiệp vào hệ thống công nghệ thông tin và truyền thông; Tội phạm liên quan đến thiết bị, mật khẩu, thông tin xác thực truy cập, chữ ký điện tử hoặc dữ liệu tương tự (sản xuất, mua, bán, trao đổi…); Làm giả dữ liệu liên quan đến hệ thống công nghệ thông tin và truyền thông; Trộm cắp hoặc làm giả dữ liệu liên quan đến hệ thống công nghệ thông tin và truyền thông nhằm chiếm đoạt tài sản; Tội phạm lạm dụng tình dục trẻ em hoặc bóc lột tình dục trẻ em trực tuyến; Dụ dỗ hoặc lôi kéo người khác thực hiện hành vi xâm phạm tình dục trẻ em; Phát tán trái phép hình ảnh cá nhân; Rửa tiền do phạm tội mà có…

So sánh Công ước LHQ năm 2024 với Công ước Budapest năm 2001 cho thấy, các xu hướng phát triển trong quy định về tội phạm mạng như sau:

- Xu hướng thể hiện đầy đủ, cụ thể, chi tiết, rõ ràng hơn các hành vi phạm tội

Về tổng quan, so với Công ước Budapest năm 2001, Công ước LHQ năm 2024 đã bổ sung thêm hai tội phạm là tội dụ dỗ hoặc lôi kéo người khác phạm tội xâm phạm tình dục đối với trẻ em và tội rửa tiền có được từ hành vi phạm tội[7]. Mặt khác, nhiều tội danh khuyến nghị trong Công ước LHQ năm 2024 đã bổ sung thêm các tình tiết hoặc các dạng hành vi phạm tội để thể hiện cụ thể, chi tiết, rõ ràng hơn so với Công ước Budapest năm 2001. Ví dụ, Điều 8 Công ước Budapest năm 2001 khuyến nghị tội lừa đảo liên quan đến máy tính với hai dạng hành vi là "*hành vi nhập, thay đổi, xóa hoặc loại bỏ dữ liệu máy tính*", "*hành vi can thiệp trái phép vào chức năng của hệ thống máy tính, với mục đích lừa đảo nhằm thu lợi ích kinh tế…*"[8]. Điều 13 Công ước LHQ năm 2024 quy định về tội trộm cắp hoặc lừa đảo liên quan đến hệ thống công nghệ thông tin và truyền thông với 03 dạng hành vi là "*hành vi nhập dữ liệu, thay đổi, xóa hoặc loại bỏ dữ liệu điện tử*"; "*hành vi can thiệp vào chức năng của hệ thống công nghệ thông tin và truyền thông*"; "*hành vi lừa dối về các tình huống thực tế được thực hiện thông qua hệ thống công nghệ thông tin và truyền thông…, với mục đích lừa đảo nhằm thu lợi trái phép*"[9]. Các quy định này cho thấy, tên của tội danh tại Điều 13 Công ước LHQ năm 2024 bao trùm hơn tên tội danh tại Điều 8 Công ước Budapest năm 2001. Nội dung của Điều 13 Công ước LHQ năm 2024 không chỉ mở rộng phạm vi đối tượng tác động từ hệ thống máy tính sang "hệ thống công nghệ thông tin và truyền thông" mà còn bổ sung thêm dạng hành vi "lừa dối về các tình huống thực tế được thực hiện…". Đây là dạng hành vi khá phổ biến, trở thành một thủ đoạn thường xuyên của những người thực hiện hành vi phạm tội trong thời gian gần đây. Tương tự, nhiều quy định khác trong Công ước LHQ năm 2024 cũng đưa ra các khuyến nghị về tội phạm cụ thể, chi tiết, rõ ràng hơn so với Công ước Budapest năm 2001[10].

- Xu hướng cập nhật những tiến bộ của cách mạng 4.0 và những thành tựu ứng dụng trí tuệ nhân tạo trong phòng, chống tội phạm công nghệ cao

Công ước Budapest năm 2001 mới chỉ đề cập đến bối cảnh "*những thay đổi sâu sắc trong tiến trình số hóa, hội nhập và toàn cầu hóa của mạng máy tính*"[11], từ đó khuyến nghị: "*Quan ngại về nguy cơ các mạng máy tính và thông tin điện tử có thể được sử dụng để thực hiện các hành vi phạm tội…*". Công ước LHQ năm 2024 đã thể hiện đầy đủ, rõ ràng hơn tác động của sự phát triển của cách mạng 4.0 trong việc "*tạo ra những cơ hội mới cho người phạm tội, có thể góp phần làm gia tăng tỷ lệ và tính đa dạng của các hành vi phạm tội và có*

[7] Điều 15 và Điều 17 của Công ước LHQ năm 2024, https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf.

[8] Điều 8 của Công ước Budapest về Tội phạm mạng – Hiệp ước 185, Tlđd.

[9] Điều 13 của Công ước chống tội phạm mạng của Liên hợp quốc, Tlđd.

[10] Điều 9 của Công ước Budapest về tội phạm mạng – Hiệp ước 185, Tlđd và Điều 14 của Công ước chống tội phạm mạng của Liên hợp quốc, Tlđd.

[11] Lời nói đầu của Đại hội đồng, Công ước chống tội phạm mạng của Liên hợp quốc, Tlđd.

thể có tác động tiêu cực đến các quốc gia, doanh nghiệp và phúc lợi của cá nhân là toàn xã hội"[12]. Những tiến bộ vượt bậc mang tính đột phá trong cuộc cách mạng 4.0, nhất là những tiến bộ trong ứng dụng trí tuệ nhân tạo tạo sinh (Generative AI) khi đã bị người phạm tội sử dụng để thực hiện tội phạm thì sẽ không chỉ làm gia tăng về mức độ của tính nguy hiểm cho xã hội của hành vi phạm tội mà còn "*có tác động đáng kể đến quy mô, tốc độ và phạm vi của các tội phạm*" và "*số lượng nạn nhân của tội phạm mạng ngày càng tăng*"[13]. Đây là xu hướng dễ nhận thấy khi số lượng tội phạm mạng đang có sự gia tăng nhanh chóng trên toàn cầu. Ví dụ, tại Hoa Kỳ, Trung tâm tiếp nhận tin báo về tội phạm Internet năm 2023 đã nhận được số lượng tin báo kỷ lục là 880.418 vụ, với thiệt hại vượt quá 12,5 tỷ đô la, tăng gần 10% về số vụ và tăng 22% mức thiệt hại so với năm 2022. Tuy vậy, theo FBI, số lượng tin báo này chỉ chiếm khoảng 20% số liệu thực tế[14]. Báo cáo về tội phạm mạng của Cybersecurity Ventures tính toán chi phí tội phạm mạng hàng năm trên toàn cầu sẽ tăng từ 400 tỷ đô la vào đầu năm 2015 lên 6 nghìn tỷ đô la vào năm 2021[15]. Từ năm 2012 đến tháng 7/2017, Bang Maharashtra của Ấn Độ có tỷ lệ tội phạm mạng được báo cáo là 10.419 vụ, tuy nhiên chỉ có 34 vụ bị kết án (chiếm tỷ lệ 0,3%). Lý do chính của tỷ lệ kết án thấp là thiếu luật hình sự về tội phạm mạng và thiếu các quy định về thủ tục để thu giữ và phân tích bằng chứng kỹ thuật số. Ấn Độ cũng chưa cập nhật các luật về tội phạm mạng để xử lý các trường hợp tội phạm mạng vượt ra ngoài ranh giới của quốc gia và nạn nhân ở nhiều khu vực pháp lý[16].

3. Xu hướng phát triển của pháp luật hình sự Việt Nam về các tội phạm mạng

Tại Việt Nam, Bộ luật Hình sự (BLHS) không có quy định về tội phạm mạng mà chỉ có quy định về các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông (CNTT, MVT). Tội phạm trong lĩnh vực CNTT, MVT lần đầu tiên quy định trong BLHS năm 1999, sửa đổi, bổ sung năm 2009, sau đó tiếp tục được hoàn thiện thành một mục riêng trong Chương XXI của BLHS năm 2015, sửa đổi, bổ sung năm 2017. Luật sửa đổi, bổ sung một số điều của BLHS số 86/2025/QH15 không sửa đổi quy định về các tội phạm trong lĩnh vực CNTT, MVT. Nghiên cứu các tội phạm trong lĩnh vực CNTT, MVT trong lịch sử lập pháp hình sự Việt Nam cho thấy các xu hướng sau:

- Xu hướng tội phạm hóa ngày càng đầy đủ, cụ thể, chi tiết, rõ ràng hơn các hành vi phạm tội trong lĩnh vực công nghệ thông tin, mạng viễn thông

Trong BLHS năm 1999, tại chương XIX: Các tội xâm phạm an toàn công cộng, trật tự công cộng chỉ có 03 điều luật quy định các tội phạm trong lĩnh vực CNTT, MVT là: Tội tạo ra và lan truyền, phát tán các chương trình vi rút tin học (Điều 224); Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử (Điều 225) và Tội sử dụng trái phép thông tin trên mạng và trong máy tính (Điều 226). Luật số 37/2009/QH12 sửa đổi, bổ sung một số điều của BLHS đã sửa đổi, bổ sung cả 03 điều luật trên thành: Tội phát tán vi rút, chương trình tin học có tính năng gây hại cho hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số (Điều 224), tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số (Điều 225) và tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, mạng Internet (Điều 226). Ngoài ra, Luật này cũng bổ sung 02 điều luật với các tội danh là: Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác (Điều 226a) và Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản (Điều 226b). BLHS năm 2015, sửa đổi, bổ sung năm 2017 đã tách nhóm tội phạm

[12] Lời nói đầu của Đại hội đồng, Công ước chống tội phạm mạng của Liên hợp quốc, Tlđd.

[13] Lời nói đầu của Đại hội đồng, Công ước chống tội phạm mạng của Liên hợp quốc, Tlđd.

[14] Federal Bureau of Investigation, *Internet Crime Report 2023*, tr. 3, 8.

[15] Steve Morgan, *Hackerpocalypse Cybercrime Report, Cybersecurity Ventures*, 2016.

[16] Juneed Iqbal, Bilal Maqbool Beigh, "Cybercrime in India: Trends and Challenges", *International Journal of Innovations & Advancement in Computer Science*, Vol. 6, Issue 12/2017, p. 187-196 (193).

trong lĩnh vực CNTT và MVT thành một nhóm tội quy định tại Mục 2 Chương XXI của BLHS với 09 điều luật, tăng 4 điều luật so với BLHS năm 1999, sửa đổi, bổ sung năm 2009. Như vậy, các tội phạm trong lĩnh vực CNTT và MVT từ 03 điều luật quy định trong BLHS năm 1999 đã tăng lên 05 điều luật trong BLHS năm 1999, sửa đổi, bổ sung năm 2009 và tăng lên 09 điều luật trong BLHS năm 2015, sửa đổi, bổ sung năm 2017[17].

Không chỉ bổ sung (tội phạm hóa) các hành vi phạm tội trong lĩnh vực CNTT và MVT mà các quy định về các dạng hành vi phạm tội của từng tội phạm trong nhóm tội phạm trong lĩnh vực CNTT và MVT cũng ngày càng hoàn thiện theo hướng quy định cụ thể, chi tiết, rõ ràng, đầy đủ, chính xác hơn các dạng hành vi phạm tội. Ví dụ, "*Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử*" tại Điều 225 trong BLHS năm 1999 được sửa tên thành "*Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số*" và đến BLHS hiện hành được sửa thành "*Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử*". Việc sửa tên tội danh vừa bảo đảm phù hợp với các dạng hành vi trong cấu thành tội phạm, vừa bao quát đầy đủ, chính xác hơn các đối tượng thuộc khách thể bảo vệ của pháp luật hình sự.

Cùng với đó, các dạng hành vi trong cấu thành tội phạm cũng được sửa đổi, hoàn thiện. Hành vi mô tả trong Điều 225 BLHS năm 1999 là hành vi của người "*được sử dụng mạng máy tính mà vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính gây rối loạn hoạt động, phong toả hoặc làm biến dạng, làm huỷ hoại các dữ liệu của máy tính hoặc đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm*". Hành vi mô tả trong Điều 225 Luật số 37/2009/QH12 được sửa thành "*Tự ý xoá, làm tổn hại hoặc thay đổi phần mềm, dữ liệu thiết bị số; Ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số; Hành vi khác cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số*". Từ quy định này cho thấy, các dạng hành vi mô tả trong Điều 225 Luật số 37/2009/QH12 cụ thể, chính xác hơn so với hành vi mô tả trong Điều 225 BLHS năm 1999. Trong Điều 225 BLHS năm 1999, việc "*gây rối loạn hoạt động của máy tính*", "*phong toả hoặc làm biến dạng các dữ liệu của máy tính*", "*làm huỷ hoại các dữ liệu của máy tính*" được diễn đạt như là hậu quả của hành vi của người "*được sử dụng mạng máy tính mà vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính*". Diễn đạt này là chưa chính xác, vì "*gây rối loạn hoạt động*", "*phong toả hoặc làm biến dạng*", "*làm huỷ hoại các dữ liệu*" là các dạng hành vi chứ không phải hậu quả. Hơn nữa, đối tượng hướng đến để xâm hại của các dạng hành vi này là khác nhau chứ không phải đều tác động đến máy tính.

Để khắc phục các hạn chế này, Điều 225 Luật số 37/2009/QH12 đã sửa thành 03 dạng hành vi cụ thể với các đối tượng tác động cụ thể của từng dạng hành vi này như đã trích dẫn ở trên. BLHS năm 2015, sửa đổi, bổ sung năm 2017 tiếp tục sửa tên tội danh này là "*Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử*". Việc thay cụm từ "*phương tiện điện tử*" cho cụm từ "*thiết bị số*" sẽ vừa bao quát, chính xác, đầy đủ hơn, vừa phù hợp với quy định của Luật Giao dịch điện tử. Nội dung của điều luật cũng được diễn đạt lại để vừa bảo đảm tính chính xác, xác định rõ mức hậu quả của hành vi phạm tội, tránh quy định mang tính định tính "*gây hậu quả nghiêm trọng*" dẫn đến khó khăn, vướng mắc

[17] BLHS số 100/2015/QH13 có 10 điều quy định về các tội phạm trong lĩnh vực CNTT, MVT, từ Điều 285 đến Điều 295. Tuy nhiên, Luật số 12/2017/QH14 ngày 20/6/2017 của Quốc hội sửa đổi, bổ sung một số điều của BLHS số 100/2015/QH13 đã bỏ Điều 292 với lý do: Nội dung quy định về cấu thành tội phạm này không phản ánh rõ mối nguy hại cho an toàn công cộng, trật tự công cộng mà thực chất đây là cấu thành tội "kinh doanh trái phép" trên môi trường mạng"… (Chính phủ, *Tờ trình về dự án Luật sửa đổi, bổ sung một số điều của BLHS số 100/2015/QH13, điểm 2đ, phần IV,* tr. 8).

trong thực tiễn áp dụng. Quy định về các tội phạm trong lĩnh vực CNTT và MVT trong BLHS năm 2015, sửa đổi, bổ sung năm 2017 cũng bảo đảm phân biệt rõ ranh giới giữa tội phạm và không phải là tội phạm khi quy định rõ khoản lợi bất chính thu được từ hành vi phạm tội hoặc mức thiệt hại do hành vi phạm tội gây ra hoặc dấu hiệu nhân thân người phạm tội.

Như vậy, từ khi bắt đầu tội phạm hóa các hành vi xâm phạm lĩnh vực CNTT, MVT trong BLHS năm 1999 cho đến BLHS năm 2015, sửa đổi, bổ sung năm 2017 và năm 2025 thì các tội phạm trong lĩnh vực CNTT, MVT đã qua 03 lần sửa đổi vào năm 2009, 2015 và 2017 (Luật số 86/2025/QH15 không sửa đổi nhóm tội này). Từ đó, các quy định về các tội phạm trong lĩnh vực CNTT, MVT đã dần hoàn thiện về tên điều luật, nội dung các dấu hiệu pháp lý và các chế tài xử lý.

- Xu hướng hoàn thiện các quy định về tội phạm mạng bảo đảm tương thích với pháp luật quốc tế

Đây là xu hướng phổ biến và tất yếu của các quốc gia trên thế giới nhằm phòng, chống hiệu quả đối với loại tội phạm rất đặc thù này. Tội phạm mạng là tội phạm mang tính toàn cầu, không chỉ ở quy mô hoạt động và hậu quả thiệt hại mà còn ở chỗ nó được thực hiện xuyên biên giới, không có bất kỳ giới hạn địa lý nào. Quyền tài phán là rào cản lớn nhất trong quá trình truy tố tội phạm mạng vì chứng cứ có thể nằm ở một số quốc gia có luật riêng. Vì vậy, cần có luật với các quy định đặc biệt để có thể giải quyết 03 rào cản đang đặt ra là: Thiếu khung pháp lý hữu hiệu, thiếu thẩm quyền tố tụng và thiếu các điều khoản tương trợ tư pháp có thể thực thi với nước ngoài 18.

Tại Indonesia, Luật Thông tin và Giao dịch điện tử là cơ sở pháp lý quan trọng trong phòng, chống tội phạm mạng. Tuy nhiên, các luật này cũng chưa quy định đầy đủ các hình thức đe dọa tấn công mạng mới xuất hiện, như các cuộc tấn công đe dọa dai dẳng tinh vi hoặc các cuộc tấn công dựa trên trí tuệ nhân tạo… Điều này dẫn đến các quy định của Luật bị tụt hậu, không theo kịp sự phát triển của công nghệ cũng như phương thức, thủ đoạn mới, tinh vi của tội phạm mạng..., đặt ra yêu cầu cấp thiết cần hoàn thiện quy định của pháp luật[19]. Pháp luật Ấn Độ cũng chưa cập nhật các luật về tội phạm mạng để xử lý các trường hợp tội phạm mạng vượt ra ngoài ranh giới của quốc gia và nạn nhân ở nhiều khu vực pháp lý. Vì vậy, việc thu thập chứng cứ thường không khả thi, dẫn đến chưa đủ cơ sở pháp lý đầy đủ để truy cứu trách nhiệm hình sự trong các trường hợp này[20].

So sánh các quy định của BLHS Việt Nam với Công ước LHQ năm 2024 cho thấy, về cơ bản, BLHS hiện hành đã tội phạm hóa nhiều hành vi tương thích với các hành vi được khuyến nghị trong Công ước LHQ năm 2024, như nghe lén trái phép (Điều 8), can thiệp vào dữ liệu điện tử (Điều 9), lạm dụng thiết bị (Điều 11), trộm cắp hoặc gian lận liên quan đến hệ thống CNTT và MVT (Điều 13). Có thể thấy, mặc dù các tội phạm trong lĩnh vực CNTT, MVT mới chỉ được quy định trong BLHS năm 1999 cho đến nay, nhưng nhiều hành vi phạm tội đã được quy định trong BLHS, bước đầu thể hiện sự tương thích với pháp luật quốc tế và pháp luật của một số quốc gia trên thế giới.

4. Kiến nghị hướng hoàn thiện các quy định về tội phạm mạng bảo đảm tương thích với pháp luật quốc tế và đáp ứng yêu cầu của đất nước trong giai đoạn mới

Mặc dù BLHS Việt Nam đã có nhiều hành vi quy định tương thích với Công ước LHQ năm 2024 nhưng vẫn còn một số hành vi chưa được tội phạm hóa gồm: Hành vi truy cập bất hợp pháp (Điều 7), hành vi làm giả dữ liệu liên quan đến hệ thống CNTT và MVT (Điều 12), hành vi liên quan đến các tài liệu lạm dụng tình dục trẻ em hoặc bóc lột tình dục trẻ em trực tuyến (Điều 14), hành

[18] Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technol. Law Journa*l, No. 1 (18)/2003, p. 425-446.

[19] Muhammad Ahfadh Fazlurrohman, Surya Nita, Muhammad Erza Aminanto, "Comparative studies on trends and strategies for combating cybercrime between Indonesia and developed countries", *Policy, Law, Notary and Regulatory Issues*, No. 4 (3)/2024, tr. 498-515.

[20] Juneed Iqbal, Bilal Maqbool Beigh, Tlđd, p. 187-196 (193).

vi dụ dỗ, lôi kéo người khác phạm tội xâm phạm tình dục trẻ em trực tuyến (Điều 15), hành vi phát tán hình ảnh riêng tư thông qua hệ thống CNTT và MVT (Điều 16) và hành vi rửa tiền (Điều 17). Chính vì vậy, BLHS hiện hành cần tiếp tục hoàn thiện các quy định về các tội phạm trong lĩnh vực CNTT và MVT để bảo đảm ngày càng tương thích với pháp luật quốc tế.

Mặt khác, trên thực tiễn áp dụng các quy định của BLHS về các tội phạm trong lĩnh vực CNTT và MVT, một số quy định chưa phát huy hiệu quả điều chỉnh. Số liệu thống kê tổng hợp của Viện kiểm sát nhân dân tối cao giai đoạn 2018-2024 cho thấy: Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290 BLHS) là tội có số lượng lớn nhất với 511 vụ và 898 người phạm tội (chiếm 70,6% số vụ và 60,7% số bị cáo). Số lượng cao thứ hai là tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291 BLHS) với 113 vụ và 318 người phạm tội. Tiếp theo là tội xâm nhập trái phép vào mạng máy tính, mạng trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289 BLHS) với 50 vụ và 126 người phạm tội. Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288 BLHS) có 40 vụ và 117 người phạm tội. Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287 BLHS); hành vi sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (Điều 285 BLHS) chỉ có 05 vụ với 09 người phạm tội; tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 286 BLHS) có 02 vụ và 02 người phạm tội; tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh (Điều 293 BLHS) và tội cố ý gây nhiễu có hại (Điều 294) không có người phạm tội[21].

Một trong 07 định hướng chiến lược đưa đất nước vào kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc là "*chuyển đổi số*". Đây là "*quá trình xác lập một phương thức sản xuất mới tiên tiến, hiện đại – "phương thức sản xuất số", "Mục tiêu đến năm 2030, Việt Nam sẽ đứng trong nhóm 50 quốc gia hàng đầu thế giới và xếp thứ 3 trong ASEAN về chính phủ điện tử, kinh tế số*"[22]. Theo đó, một trong những đặc trưng của kỷ nguyên mới là kinh tế số, xã hội số. Chiến lược quốc gia phát triển kinh tế số và xã hội số đến năm 2025, định hướng đến năm 2030 đã xác định: "*Phát triển kết cấu hạ tầng đồng bộ, gồm hạ tầng số và hạ tầng thiết yếu phục vụ kinh tế số và xã hội số. Điểm đột phá là nhanh chóng phổ cập điện thoại thông minh tới mỗi người dân, phổ cập Internet cáp quang băng rộng tốc độ cao tới mỗi hộ gia đình, phổ cập dịch vụ điện toán đám mây tới mỗi doanh nghiệp*"[23]. Thực hiện Chiến lược này sẽ tạo ra những động lực quan trọng thúc đẩy sự phát triển bứt phá mạnh mẽ nền kinh tế - xã hội, tăng năng suất lao động, tạo ra nguồn lực to lớn để nâng cao chất lượng đời sống của mọi tầng lớp người dân trong xã hội. Tuy nhiên, cùng với những tiến bộ vượt bậc về khoa học, công nghệ, trí tuệ nhân tạo; sự phát triển mạnh mẽ của hạ tầng số, dịch vụ số cũng như sự phổ cập người dùng Internet thì tội phạm mạng cũng lợi dụng triệt để nhằm vận dụng trong thực hiện các hành vi phạm tội với phương thức, thủ đoạn ngày càng tinh vi, xảo quyệt, liên tục thay đổi, mang tính xuyên quốc gia, xuyên châu lục, phi địa giới; quy mô, phạm vi, tính chất, mức độ nguy hiểm và hậu quả ngày càng gia tăng nhanh chóng.

[21] Tổng hợp dựa trên số liệu thống kê của Cục Thống kê tội phạm và công nghệ thông tin, Viện kiểm sát nhân dân tối cao.

[22] Tô Lâm (2024), *Một số nội dung cơ bản về kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc; những định hướng chiến lược đưa đất nước bước vào kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc*, nguồn truy cập https://www.tapchicongsan.org.vn/media-story/, truy cập ngày 10/7/2025.

[23] Quyết định số 411/QĐ-TTg ngày 31/3/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược quốc gia phát triển kinh tế số và xã hội số đến năm 2025, định hướng đến năm 2030.

Bối cảnh kỷ nguyên kinh tế số, xã hội số đặt ra yêu cầu "*Thường xuyên rà soát, sửa đổi kịp thời các quy định không còn phù hợp... bảo đảm khung pháp lý không trở thành rào cản của sự phát triển, đồng thời bảo đảm an ninh quốc gia, bảo vệ quyền và lợi ích hợp pháp của người dân, doanh nghiệp*"[24]. Bối cảnh này đòi hỏi pháp luật hình sự nói chung, các quy định về các tội phạm trong lĩnh vực CNTT và MVT nói riêng cũng cần phải tiếp tục sửa đổi và hoàn thiện, đáp ứng yêu cầu của kỷ nguyên mới. Thực tiễn tình hình tội phạm trong lĩnh vực CNTT và MVT giai đoạn 2018-2024 đặt ra vấn đề là có cần thiết phải tội phạm hóa các hành vi phạm tội: Hành vi cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287 BLHS); hành vi sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (Điều 285 BLHS); hành vi phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 286 BLHS); hành vi sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh; hành vi cố ý gây nhiễu có hại (Điều 294). Đây là các hành vi rất ít hoặc gần như không bị xử lý trên thực tế trong giai đoạn 2018-2024, đòi hỏi pháp luật hình sự nói chung, các quy định về các tội phạm trong lĩnh vực CNTT và MVT nói riêng cũng cần phải tiếp tục sửa đổi và hoàn thiện, đáp ứng yêu cầu của kỷ nguyên mới. Thực tiễn tình hình tội phạm trong lĩnh vực CNTT và MVT giai đoạn này đặt ra vấn đề là có cần thiết phải tội phạm hóa các hành vi phạm tội: Hành vi cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287 BLHS); hành vi sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (Điều 285 BLHS); hành vi phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 286 BLHS); hành vi sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh; hành vi cố ý gây nhiễu có hại (Điều 294). Đây là các hành vi rất ít hoặc gần như không bị xử lý trên thực tế trong giai đoạn 2018-2024.

Quá trình tội phạm hóa và phi tội phạm hóa là "*do nhu cầu phát triển về mọi mặt của xã hội quyết định, nó là sự phản ánh, là kết quả của quá trình đó*"[25]. Hiện thực xã hội luôn vận động và phát triển dựa trên nguyên lý về mối liên hệ phổ biến, trong đó các sự vật, hiện tượng, quá trình "*vừa tách biệt nhau, vừa có sự liên hệ qua lại, thâm nhập và chuyển hóa lẫn nhau*"[26]. Quá trình này luôn phát sinh những nguy cơ đe dọa sự phát triển lành mạnh của các quan hệ xã hội, đe dọa các giá trị và nhu cầu xã hội của con người thể hiện trong pháp luật tự nhiên. "*Pháp luật tự nhiên là tổng thể các giá trị và nhu cầu xã hội của sự tồn tại của con người (tự do, bình đẳng, công bằng…), cũng như tổng thể các quy phạm và các nguyên tắc tổng thể tạo nên nền tảng của tất cả các hệ thống pháp luật của nền văn minh nhân loại*"[27]. Vấn đề quan trọng là cần nhận thức đúng, đầy đủ, khách quan, toàn diện các tác động của các mối quan hệ xã hội trong xu thế phát triển để làm rõ các nguy cơ nói trên, từ đó làm cơ sở để thể hiện pháp luật tự nhiên trong pháp luật thực chứng. Đây chính là quá trình tội phạm hóa. Ngược lại, khi các nguy cơ đe dọa sự phát triển lành mạnh của các quan hệ xã hội, đe dọa các giá

[24] Tô Lâm (2024), *Chuyển đổi số - động lực quan trọng phát triển lực lượng sản xuất, hoàn thiện quan hệ sản xuất đưa đất nước bước vào kỷ nguyên mới*, https://www.tapchicongsan.org.vn/media-story/-/asset_publisher/V8hhp4dK31Gf/content/chuyen-doi-so-dong-luc-quan-trong-phat-trien-luc-luong-san-xuat-hoan-thien-quan-he-san-xuat-dua-dat-nuoc-buoc-vao-ky-nguyen-moi, truy cập ngày 03/8/2025.

[25] Viện Nghiên cứu Nhà nước và Pháp luật, *Những vấn đề lý luận của việc đổi mới pháp luật hình sự trong giai đoạn hiện nay*, Nxb. Công an nhân dân, 1994, tr. 48.

[26] Hội đồng Trung ương chỉ đạo biên soạn Giáo trình Quốc gia các bộ môn khoa học Mác – Lênin, Tư tưởng Hồ Chí Minh (2004), Giáo trình Triết học Mác – Lê nin, Nxb. Chính trị Quốc gia, tr. 217.

[27] Võ Khánh Vinh, "Về bản thể luận pháp luật", *Tạp chí Nhân lực Khoa học Xã hội*, số 1/2014, tr. 3-15 (9).

trị và nhu cầu xã hội của con người không còn hoặc không đáng kể hoặc tần suất xảy ra là rất ít thì cần phi tội phạm hóa các hành vi này để nâng cao hiệu quả điều chỉnh của pháp luật hình sự nói riêng, hệ thống pháp luật của quốc gia nói chung.

Từ quan điểm này, tác giả cho rằng, trong bối cảnh kỷ nguyên phát triển đột phá trong nền kinh tế số, xã hội số, xu hướng sắp tới của pháp luật hình sự đối với các tội phạm trong lĩnh vực CNTT và MVT là cần tiếp tục nghiên cứu để tội phạm hóa một số hành vi có mức độ nguy hiểm cho xã hội đáng kể, hành vi diễn ra tương đối phổ biến và việc xử lý hình sự các hành vi này là cần thiết nhằm bảo đảm, bảo vệ các giá trị, các quyền và lợi ích của cá nhân và xã hội, như các hành vi lạm dục, bóc lột tình dục trẻ em qua mạng hay các hành vi rửa tiền. Mặt khác, cũng cần nghiên cứu để quy định tình tiết "Sử dụng công nghệ thông tin và mạng viễn thông" hoặc tình tiết "Sử dụng công nghệ cao" là tình tiết tăng nặng định khung trong các cấu thành tội phạm tăng nặng và tình tiết tăng nặng trách nhiệm hình sự quy định tại Điều 52 BLHS. Ngược lại, cần nghiên cứu để phi tội phạm hóa một số hành vi phạm tội trong lĩnh vực CNTT và MVT mà mức độ nguy hiểm cho xã hội không đáng kể, tần suất xảy ra tương đối ít, thậm chí không xảy ra và việc phi tội phạm hóa không xâm hại các giá trị, các quyền và lợi ích của cá nhân và xã hội, bảo đảm nâng cao hiệu quả điều chỉnh của pháp luật hình sự./.

TÀI LIỆU THAM KHẢO

1. Quyết định số 411/QĐ-TTg ngày 31/3/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược quốc gia phát triển kinh tế số và xã hội số đến năm 2025, định hướng đến năm 2030;

2. Viện Nghiên cứu Nhà nước và Pháp luật, *Những vấn đề lý luận của việc đổi mới Pháp luật hình sự trong giai đoạn hiện nay*, Nxb. Công an nhân dân, 1994;

3. Hội đồng Trung ương chỉ đạo biên soạn Giáo trình Quốc gia các bộ môn khoa học Mác – Lê nin, Tư tưởng Hồ Chí Minh (2004), Giáo trình Triết học Mác – Lê nin, Nxb. Chính trị Quốc gia;

4. Võ Khánh Vinh, "Toàn cầu hóa và các xu hướng phát triển của pháp luật", *Tạp chí Nhà nước và Pháp luật*, số 7/2017;

5. Võ Khánh Vinh, "Về bản thể luận pháp luật", *Tạp chí Nhân lực Khoa học Xã hội*, số 1/2014;

6. Tô Lâm (2024), *Chuyển đổi số - động lực quan trọng phát triển lực lượng sản xuất, hoàn thiện quan hệ sản xuất đưa đất nước bước vào kỷ nguyên mới*, https://www.tapchicongsan.org.vn/media-story/-/asset_publisher/V8hhp4dK31Gf/content/chuyen-doi-so-dong-luc-quan-trong-phat-trien-luc-luong-san-xuat-hoan-thien-quan-he-san-xuat-dua-dat-nuoc-buoc-vao-ky-nguyen-moi;

7. Tô Lâm (2024), *Một số nội dung cơ bản về kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc; những định hướng chiến lược đưa đất nước bước vào kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc*, https://www.tapchicongsan.org.vn/media-story/;

8. Preamble of Budapest Convention on Cybercrime – Treaty 185 (Lời nói đầu của Công ước Budapest về Tội phạm mạng – Hiệp ước 185), https://www.coe.int/en/web/cybercrime/the-budapest-convention;

9. The General Assembly, Convention against Cybercrime of United Nations (Đại hội đồng, Công ước chống tội phạm mạng của Liên hợp quốc), https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf;

10. Federal Bureau of Inv;stigation, Internet Crime Report 2023;

11. Ammar Yassir, Smitha Nayak, "Cybercrime: A threat to Network Security", *International Journal of Computer Science and Network Security*, No. 2(12)/2012;

12. Osman Goni, "Introduction to Cyber Crime", *International Journal of Engineering and Artificial Intelligence*, No. 1(3)/2022;

13. Geralda Odinot, Maite Verhoeven, Ronald Pool, Christianne De Poot (2017), "Organised Cybercrime in the Netherlands", *Empirical findings and implications for law enforcement*, https://www.researchgate.net/publication/313706519;

14. Steve Morgan, *Hackerpocalypse Cybercrime Report, Cybersecurity Ventures*, 2016;

15. Juneed Iqbal, Bilal Maqbool Beigh, "Cybercrimein India: Trends and Challenges", *International Journal of Innovations & Advancement in Computer Science*, Vol. 6, Issue 12/2017;

16. Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technol. Law Journal*, No. 1 (18)/2003;

17. Muhammad Ahfadh Fazlurrohman, Surya Nita, Muhammad Erza Aminanto, "Comparative studies on trends and strategies for vcombating cybercrime between Indonesia and developed countries", No. 4 (3)/2024.