ĐỊNH TỘI DANH ĐỐI VỚI CÁC TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN, MẠNG VIỄN THÔNG

NGUYỄN VĂN KHOÁT*

Tóm tắt: Bài viết giải quyết các vấn đề lý luận về định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, đồng thời tập trung phân tích việc định tội danh đối với một số tội cụ thể trong lĩnh vực này được quy định tại Mục 2 Chương XXI Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017 (sau đây gọi tắt là BLHS năm 2015).

Từ khóa: Bộ luật Hình sự; tội phạm; công nghệ thông tin, mạng viễn thông; định tội danh

Ngày nhận bài: 26/8/2024; Biên tập xong: 06/9/2024; Duyệt đăng: 20/9/2024

THE CRIMINALIZATION FOR CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS NETWORKS

Abstract: The article addresses theoretical issues on criminalization for crimes in the field of information technology and telecommunications networks, and focuses on analyzing the criminalization for some specific crimes in this field as prescribed in Section 2, Chapter XXI of the 2015 Penal Code, amended and supplemented in 2017.

Keywords: The Penal Code; crimes; information technology, telecommunications networks; criminalization

Received: Aug 26th, 2024; Editing completed: Sep 06th, 2024; Accepted for publication: Sep 20th, 2024

1. Một số vấn đề chung về định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Định tội danh là một hoạt động có tính tất yếu trong suốt quá trình tố tụng hình sự, từ khởi tố, điều tra cho tới truy tố, xét xử bởi đây là cơ sở cần thiết đầu tiên cho việc truy cứu trách nhiệm hình sự (TNHS). Về mặt thực tiễn, định tội danh là một hoạt động áp dụng pháp luật có vai trò, ý nghĩa hết sức quan trọng. Định tội danh đúng là cơ sở cho việc áp dụng chính xác, phù hợp các quy định của pháp luật hình sự và tố tụng hình sự vào giải quyết từng vụ án hình sự cụ thể, bảo đảm xử lý đúng người, đúng tội, đúng pháp luật.

Từ tính chất quan trọng của việc định tội danh mà nghiên cứu về vấn đề định tội danh luôn được nhiều nhà lý luận và cán bộ thực tiễn quan tâm. Hiện nay không có khái niệm lập pháp về định tội danh. Vì thế, quan niệm về định tội danh được các nhà nghiên cứu trình bày từ góc độ tiếp cận của khoa học pháp lý. Theo đó, đã có nhiều quan điểm đưa ra khái niệm về định tội danh[1]. Tiếp cận các quan niệm nêu trên về định tội danh, tác giả thấy rằng, dù về mặt diễn đạt có khác nhau, nhưng về mặt bản chất thì các nhà nghiên cứu đều xác định các vấn đề cốt lõi sau đây:

Một là, xét đến cùng thì định tội danh là hoạt động nhận thức của con người về việc có hay không sự phù hợp giữa các dấu hiệu của hành vi gây nguy hiểm cho xã hội xảy ra trong thực tiễn khách quan với quy định của pháp luật hình sự về một tội phạm cụ thể.

Hai là, định tội danh là hoạt động thực tiễn áp dụng pháp luật khi hoạt động đó do cơ quan, người có thẩm quyền theo quy định của pháp luật tiến hành. Bản chất của định tội danh là hoạt động áp dụng pháp luật hình sự, tuy vậy quá trình định tội danh các chủ thể còn áp dụng các quy định của pháp luật tố tụng hình sự để tiến hành.

Ba là, định tội danh là cơ sở quan trọng nhất cho việc quyết định hình phạt và giải quyết các vấn đề khác có liên quan đến TNHS của người phạm tội.

Từ những phân tích trên có thể hiểu: *Định tội danh là hoạt động thực tiễn áp dụng pháp luật hình sự và tố tụng hình sự của cơ quan và người có thẩm quyền để xác định, so sánh và ghi nhận về mặt pháp lý, sự phù hợp giữa các dấu hiệu của hành vi nguy hiểm cho xã hội xảy ra trong thực tiễn khách quan với quy định của pháp luật hình sự về một tội*

Email: Khoatnv@tks.edu.vn
Tiến sĩ, Hiệu trưởng Trường Đại học Kiểm sát Hà Nội

[1] Lê Cảm, "Một số vấn đề chung về định tội danh", *Giáo trình luật hình sự Việt Nam,* Trường Đại học Luật Hà Nội, Nxb. Công an nhân dân, Hà Nội, 2002, tr.171; Dương Tuyết Liên, *Định tội danh và quyết định hình phạt,* Nxb. Lao động - Xã hội, Hà Nội, 2005, tr.34; Võ Khánh Vinh, *Định tội danh và quyết định hình phạt trong luật hình sự Việt Nam,* Nxb. Công an nhân dân, Hà Nội, 2013, tr.9-10.

phạm cụ thể, qua đó làm tiền đề cho việc quyết định hình phạt và giải quyết các vấn đề khác có liên quan đến TNHS của người phạm tội.

Ở nước ta, tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông được quy định tại Mục 2 Chương XXI BLHS năm 2015, từ Điều 285 đến Điều 294. Đây là loại tội phạm do người có năng lực TNHS thực hiện bằng việc cố ý trực tiếp sử dụng tri thức, kỹ năng, công cụ, phương tiện công nghệ ở trình độ cao tác động trái pháp luật đến thông tin, dữ liệu được lưu trữ, xử lý, truyền tải trong hệ thống mạng máy tính, mạng viễn thông, thiết bị số, xâm hại đến trật tự an toàn thông tin, gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân. Từ nhận thức về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông và định tội danh, có thể đưa ra khái niệm định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông như sau: *Định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là hoạt động thực tiễn áp dụng pháp luật hình sự và tố tụng hình sự của cơ quan có thẩm quyền và người có thẩm quyền tố tụng để xác định, so sánh và ghi nhận về mặt pháp lý sự phù hợp chính xác giữa các dấu hiệu của hành vi cố ý trực tiếp sử dụng tri thức, kỹ năng, công cụ, phương tiện công nghệ ở trình độ cao tác động trái pháp luật đến thông tin, dữ liệu được lưu trữ, xử lý, truyền tải trong hệ thống mạng máy tính, mạng viễn thông, thiết bị số, xâm hại đến trật tự an toàn thông tin, gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân đã xảy ra trong thực tế với các dấu hiệu cấu thành của các tội trong lĩnh vực công nghệ thông tin, mạng viễn thông, làm tiền đề cho việc quyết định hình phạt và giải quyết các vấn đề khác có liên quan đến TNHS của người phạm tội.*

2. Định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo các yếu tố cấu thành tội phạm

Định tội danh về mặt bản chất là quá trình đối chiếu những tình tiết thực tế của hành vi nguy hiểm đã xảy ra với các dấu hiệu của cấu thành một loại tội phạm nhất định. Tội phạm là một thể thống nhất gồm bốn yếu tố: Khách thể, mặt khách quan, chủ thể, mặt chủ quan. Do đó, định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo bốn yếu tố cấu thành tội phạm là xác định các vấn đề sau đây:

Thứ nhất, xác định khách thể trong việc định tội danh đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Khách thể của loại tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là trật tự an toàn thông tin (trong đó, trật tự an toàn thông tin được hiểu là những quy tắc xử sự pháp lý, đạo đức hoặc quy tắc chuyên môn...) được Nhà nước và xã hội xác lập nhằm đảm bảo an toàn thông tin được lưu trữ, xử lý trong các hệ thống máy tính, quyền và lợi ích hợp pháp của các cá nhân, tổ chức trong việc khai thác, sử dụng các thông tin đó. Mặt khác, an toàn thông tin bao gồm ba thuộc tính là: Tính bảo mật, tính toàn vẹn và tính khả dụng. Như vậy, khi nói đến trật tự an toàn thông tin còn bao gồm các quy tắc đảm bảo an toàn thông tin và những quy tắc liên quan đến trật tự pháp luật trong khai thác sử dụng thông tin. Mỗi tội phạm cụ thể trong lĩnh vực công nghệ thông tin, mạng viễn thông có thể tác động đến một hoặc một số khía cạnh của trật tự an toàn thông tin.

Thứ hai, xác định mặt khách quan trong việc định tội danh đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Trong những yếu tố thuộc mặt khách quan, hành vi khách quan của tội phạm và công cụ, phương tiện thực hiện tội phạm là những dấu hiệu pháp lý bắt buộc trong tất cả các cấu thành tội phạm của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Các yếu tố còn lại của mặt khách quan không phải là dấu hiệu bắt buộc trong mọi cấu thành tội phạm của loại tội này. Mặt khách quan để xác định thuộc một tội danh nào cụ thể được xác định như sau:

Một là, Tội sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (Điều 285)

Hành vi khách quan của tội phạm thể hiện ở việc: Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, viễn thông, phương tiện điện tử như: Các phần mềm vi rút, phần mềm có khả năng gây rối loạn hoạt động của máy tính, mạng máy tính, mạng viễn thông, thiết bị viễn thông, thiết bị điện tử; có thể phong tỏa, sao chép, làm biến dạng, huỷ hoại các dữ liệu; có thể làm sai lệch thiết bị điện tử đo, đếm; có thể ngăn chặn việc truyền tải dữ liệu, chiếm quyền điều khiển, quản lý, vận hành, khai thác mạng máy tính, mạng viễn thông...) để sử dụng vào mục đích trái pháp luật như: Để truy cập bất hợp pháp vào mạng nội bộ của cơ quan, tổ chức nhằm làm ngưng trệ, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, thiết bị điện tử; để lấy cắp thông tin riêng hợp pháp của cơ quan, cá nhân, tổ chức; để hủy hoại dữ liệu; để được sử dụng trái phép các dịch vụ; hoặc để thiết lập, cung cấp trái phép dịch vụ viễn thông,

Internet nhằm chiếm đoạt tài sản... Tội phạm có cấu thành hình thức, không yêu cầu có hậu quả thiệt hại. Khi chủ thể thực hiện một trong bốn loại hành vi gồm sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử để sử dụng vào mục đích trái pháp luật thì tội phạm hoàn thành.

Từ cấu thành cơ bản của tội phạm quy định tại Điều 285 BLHS năm 2015 cho thấy, người phạm tội chưa có hành vi tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử. Do đó, cần lưu ý:

+ Nếu chủ thể có hành vi sử dụng công cụ, thiết bị, phần mềm thực hiện hành vi làm tổn hại hoặc thay đổi phần mềm, dữ liệu điện tử hoặc ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc có hành vi khác cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử nhằm thu lợi bất chính thì xem xét xác định hành vi theo Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287 BLHS năm 2015).

+ Trường hợp người phạm tội sử dụng công cụ, thiết bị, phần mềm thực hiện việc phát tán chương trình tin học gây hại cho mạng máy tính, mạng viễn thông, phương tiện điện tử thu lợi bất chính thì xem xét xác định hành vi theo 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 năm 2015).

+ Trường hợp người phạm tội sử dụng công cụ, thiết bị, phần mềm thực hiện hành vi cố ý vượt qua cảnh báo, mã truy cập, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác, chiếm quyền điều khiển; can thiệp vào chức năng hoạt động của phương tiện điện tử; lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép các dịch vụ thì xem xét xác định hành vi theo Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289 BLHS năm 2015).

Hai là, 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)

Hành vi khách quan của tội phạm là hành vi phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. Đó là hành vi cố ý lan truyền chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử nhằm gây rối loạn hoạt động, phong tỏa, sao chép, làm biến dạng, huỷ hoại các dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử[2]. Người phạm tội cố ý lan truyền chương trình tin học gây hại đến nhiều mạng máy tính, mạng viễn thông, phương tiện điện tử. Nạn nhân sẽ là bất kỳ người dùng nào vô tình bị lây nhiễm chương trình tin học gây hại đó.

Đối tượng của hành vi phát tán là chương trình tin học có tính năng gây hại. Đó là chương trình tự động hóa xử lý thông tin, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số[3]. Chương trình tin học có tính năng gây hại được chia làm 02 loại bao gồm: (1) Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin như sâu máy tính (worm), horse trojan, phần mềm gián điệp (spyware), phần mềm quảng cáo (adware), botnet, phishing, phần mềm tống tiền (ransomware); (2) Vi-rút máy tính là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

Ba là, Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287)

Hành vi khách quan của tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử bao gồm 03 nhóm sau:

+ Nhóm các hành vi tự ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu điện tử. Đó là các hành vi cố ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu điện tử mà không được sự đồng ý của chủ thể quản lý phần mềm, dữ liệu điện tử đó[4]. Trong đó: (1) Xoá phần mềm, dữ liệu điện tử là hành vi làm cho phần mềm, dữ liệu điện tử không còn tồn tại ở mạng máy tính, mạng viễn thông, phương tiện điện tử; (2) Làm tổn hại phần mềm, dữ liệu máy tính là các

[2] Khoản 1 Điều 6 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012 về Hướng dẫn áp dụng quy định của BLHS về một số tội phạm trong lĩnh vực công nghệ thông tin và viễn thông.

[3] Khoản 1 Điều 2 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC.

[4] Khoản 1 Điều 7 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC.

hành vi làm cho phần mềm, dữ liệu không còn sử dụng được; (3) Thay đổi phần mềm, dữ liệu điện tử là những hành vi thay thế, lược bỏ, nén lại, đưa thêm thông tin vào phần mềm, dữ liệu điện tử.

+ Nhóm các hành vi ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử. Đó là các hành vi bất hợp pháp, cố ý làm cho việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử bị gián đoạn, không thực hiện được hoặc không sử dụng được[5]. Phương thức thực hiện tội phạm thường là tấn công từ chối dịch vụ (DDos-Botnet); tấn công vào cơ sở dữ liệu, can thiệp vào phần mềm hệ thống, phá hoại dữ liệu, từ đó làm tê liệt hoạt động bình thường của hệ thống máy tính, mạng viễn thông, phương tiện điện tử; sử dụng các thủ đoạn, công nghệ để lấy cắp, chiếm đoạt tên miền (domain), làm gián đoạn truy cập của người dùng vào trang web bị tấn công, đồng thời hướng việc truy cập của người dùng vào trang web của người lấy trộm (để lấy thông tin).

+ Nhóm các hành vi khác gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. Đó là hành vi cố ý của người không có quyền quản lý, vận hành, khai thác mạng máy tính, mạng viễn thông, phương tiện điện tử làm ảnh hưởng đến hoạt động bình thường của mạng máy tính, mạng viễn thông, phương tiện điện tử bằng cách làm hư hỏng, xóa, làm suy giảm, thay thế hoặc nén dữ liệu máy tính, thiết bị viễn thông, phương tiện điện tử. Đối tượng tác động của Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử bao gồm 02 đối tượng sau: (1) Phần mềm, dữ liệu điện tử: Khi bị xóa, làm tổn hại hoặc thay đổi, phần mềm, dữ liệu điện tử sẽ mất tính toàn vẹn và tính khả dụng. Khi phần mềm, dữ liệu điện tử bị xâm hại có thể làm ảnh hưởng đến hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. Tuy nhiên, cũng có trường hợp dữ liệu điện tử bị xâm hại không ảnh hưởng gì đến hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. Do đó, dữ liệu điện tử cũng được coi là đối tượng tác động độc lập. (2) Mạng máy tính, mạng viễn thông, phương tiện điện tử: Theo khoản 3 Điều 2 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012 về Hướng dẫn áp dụng quy định của BLHS về một số tội phạm trong lĩnh vực công nghệ thông tin và viễn thông (gọi tắt là Thông tư liên tịch số 10/2012) quy định: *"Mạng máy tính là tập hợp nhiều máy tính kết nối với nhau, có thể chia sẻ dữ liệu cho nhau"*. Còn theo khoản 14 Điều 3 Luật Viễn thông năm 2023: *"Mạng viễn thông là tập hợp thiết bị viễn thông được liên kết với nhau bằng đường truyền dẫn để cung cấp dịch vụ viễn thông, dịch vụ ứng dụng viễn thông"*. Trong đó, theo khoản 15, 16 Điều 3 Luật Viễn thông năm 2023, mạng viễn thông được chia làm 2 loại: (1) Mạng viễn thông công cộng là mạng viễn thông do doanh nghiệp viễn thông thiết lập để cung cấp dịch vụ viễn thông, dịch vụ ứng dụng viễn thông cho công chúng nhằm mục đích sinh lợi; (2) Mạng viễn thông dùng riêng là mạng viễn thông do tổ chức hoạt động tại Việt Nam thiết lập để cung cấp dịch vụ viễn thông, dịch vụ ứng dụng viễn thông cho các thành viên của mạng không nhằm mục đích sinh lợi trực tiếp từ hoạt động của mạng. Trong khi đó, hiện nay đa số các văn bản pháp luật quốc tế quy định tách tội này thành hai tội độc lập là tội cản trở trái phép dữ liệu máy tính và tội cản trở trái phép mạng máy tính[6].

Theo khoản 1, 2, 3 Điều 7 Thông tư liên tịch số 10/2012 thì thủ đoạn thực hiện tội phạm này là các biện pháp mang tính công nghệ, kỹ thuật. Người phạm tội sử dụng công nghệ thông tin, mạng viễn thông để thực hiện tội phạm. Việc sử dụng các phương thức vật lý như đốt, phá huỷ thiết bị để phạm tội sẽ không bị xử theo tội này, mà bị xử lý theo các tội khác như tội huỷ hoại tài sản hoặc tội phá huỷ công trình quan trọng về an ninh quốc gia (nếu đủ điều kiện).

Cũng cần lưu ý, theo Điều 287 BLHS năm 2015, các hành vi trên chỉ bị coi là Tội cản trở hoặc gây rối hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử nếu "không thuộc trường hợp quy định tại Điều 286 và Điều 289" của BLHS năm 2015. Hành vi cản trở hoặc gây rối hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử bị coi là tội phạm nếu thuộc một trong các trường hợp sau đây: (1) Thu lợi bất chính từ 50.000.000 đồng trở lên; (2) Gây thiệt hại từ 100.000.000 đồng trở lên; (3) Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 30 phút trở lên hoặc từ 03 lần trở lên trong thời gian 24 giờ (trường hợp có thể làm ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử mỗi lần dưới 30 phút nhưng làm nhiều lần, từ 3 - 10 lần trong 01 ngày); (4) Làm đình trệ hoạt động của cơ quan, tổ chức từ 24 giờ trở lên (có thể là trường hợp làm ngưng trệ hoạt động của mạng máy tính, mạng viễn

[5] Khoản 2 Điều 7 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC.

[6] Điều 4, Điều 5 Công ước Budapest năm 2001 và Điều 6 và Điều 7 Luật mẫu năm 2002.

thông, phương tiện điện tử dưới 30 phút và dưới 03 lần trong 24 giờ, nhưng để khắc phục sự cố cơ quan, tổ chức phải đình trệ hoạt động từ 24 giờ trở lên); (5) Đã bị xử phạt vi phạm hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm.

Bốn là, Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288)

Theo cấu thành tội phạm quy định tại Điều 288 BLHS năm 2015 cho thấy có 03 nhóm hành vi khách quan gồm:

+ Hành vi đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật. Thông tin trái với quy định pháp luật được hiểu là thông tin có nội dung xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của cá nhân; kích động tội ác, tệ nạn xã hội, thuần phong mỹ tục… Cần lưu ý rằng, hành vi đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật trong phạm vi Điều 288 này không bao gồm các hành vi như: Hành vi phát tán, tuyên truyền thông tin, tài liệu, vật phẩm nhằm chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam như xuyên tạc, phỉ báng chính quyền nhân dân, thông tin có nội dung bịa đặt, gây hoang mang trong nhân dân, gây chiến tranh tâm lý… (quy định tại Điều 117 BLHS năm 2015); hoặc hành vi làm nhục người khác bằng cách đưa thông tin xúc phạm nghiêm trọng nhân phẩm, danh dự của người khác (quy định tại Điều 155 BLHS năm 2015); hoặc hành vi vu khống người khác bằng cách bịa đặt thông tin nhằm xúc phạm nghiêm trọng danh dự, nhân phẩm người khác hoặc tố cáo người khác phạm tội với cơ quan nhà nước (quy định tại Điều 156 BLHS năm 2015); hoặc hành vi truyền bá văn hóa phẩm đồi trụy (quy định tại Điều 326 BLHS năm 2015).

+ Hành vi mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu hoặc người quản lý thông tin đó. Thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân là những thông tin thuộc sở hữu của cơ quan, tổ chức, cá nhân được pháp luật bảo vệ, được hiểu là những thông tin như tên, ngày tháng năm sinh, số chứng minh nhân dân, số điện thoại, địa chỉ, bí mật đời tư của cá nhân; thông tin, bí mật của tổ chức; các thông tin khác được quy định trong Hiến pháp, Bộ luật Dân sự… (quy định tại Điều 2 Thông tư liên tịch số 10/2012) và khoản 15 Điều 3 Luật An toàn thông tin năm 2015).

+ Các hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông. Hiện nay chưa có văn bản pháp luật nào quy định cụ thể hành vi nào thuộc nhóm các hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông. Tuy nhiên, thực tiễn cho thấy, một số hành vi thuộc nhóm này như là hành vi theo dõi, thu thập thông tin bất hợp pháp về cá nhân, tổ chức khác; không được phép sử dụng thông tin nhưng vẫn sử dụng; không đăng ký, chưa được cấp phép nhưng vẫn sử dụng thông tin… Hoặc khi chủ thể thực hiện một trong ba nhóm hành vi nêu trên và thu lợi bất chính từ 50.000.000 đồng trở lên; hoặc gây thiệt hại từ 100.000.000 đồng trở lên; hoặc gây dư luận xấu làm giảm uy tín của cơ quan, tổ chức, cá nhân; hoặc dẫn đến người bị xâm phạm tự sát, dẫn đến biểu tình hoặc gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội, quan hệ đối ngoại của Việt Nam.

Năm là, Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289)

Hành vi khách quan của tội phạm là hành vi truy cập vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử mà không được sự đồng ý của người chủ sở hữu hoặc người quản lý điều hành mạng máy tính, mạng viễn thông hoặc phương tiện điện tử đó. Hành vi này được thực hiện thông qua các phương thức như: (1) Vượt qua cảnh báo là vượt qua thông báo không cho phép người không có thẩm quyền truy cập vào cơ sở dữ liệu; (2) Vượt qua mã truy cập là vượt qua những điều kiện bắt buộc đáp ứng một tiêu chí chuẩn nhất định trước khi sử dụng, truy cập tới thiết bị, nội dung dữ liệu được bảo vệ; (3) Vượt qua tường lửa để xâm nhập trái phép, trong đó, tường lửa là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm hoặc phần cứng được đặt giữa hai hay nhiều mạng nhằm kiểm soát tất cả những kết nối từ bên trong ra bên ngoài và ngược lại, đồng thời ngăn chặn việc xâm nhập, kết nối trái phép; (4) Sử dụng quyền quản trị của người khác là sử dụng quyền quản lý, vận hành, khai thác và duy trì hoạt động ổn định hệ thống mạng máy tính, mạng viễn thông của cá nhân, tổ chức; (5) Các phương thức xâm nhập trái phép khác như bẻ khóa, trộm mật khẩu, mật mã của người khác để xâm nhập trái phép hoặc xâm nhập vật lý như mở khóa cửa vào phòng, khu vực không thuộc phận sự để truy cập vào mạng máy tính, mạng viễn thông, phương tiện điện tử…

Sau khi xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện

điện tử của người khác, người phạm tội thực hiện một trong những hoạt động: (1) Chiếm quyền điều khiển mạng máy tính, mạng viễn thông hoặc phương tiện điện tử; (2) Can thiệp vào chức năng hoạt động của phương tiện điện tử; (3) Lấy cắp dữ liệu điện tử; (4) Thay đổi, huỷ hoại dữ liệu điện tử; (5) Làm giả dữ liệu điện tử; (6) Sử dụng trái phép các dịch vụ.

Sáu là, Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290)

Hành vi khách quan của tội này thể hiện ở một trong những dạng hành vi sau nhằm chiếm đoạt tài sản của cơ quan, tổ chức, cá nhân:

+ Sử dụng thông tin về tài khoản, thẻ ngân hàng của cơ quan, tổ chức, cá nhân để chiếm đoạt tài sản của chủ thẻ, chủ tài khoản hoặc thanh toán dịch vụ, mua hàng hóa (tài khoản ở đây được hiểu là tài khoản ngân hàng và tài khoản các ví điện tử). Hành vi được thực hiện thông qua các thủ đoạn như trộm cắp, lừa đảo để có được thông tin về tài khoản, thẻ ngân hàng của người khác, sau đó dùng thông tin đó để chiếm đoạt tài sản của chủ tài khoản.

+ Làm, tàng trữ, mua bán, sử dụng, lưu hành thẻ ngân hàng giả nhằm để chiếm đoạt tài sản của chủ tài khoản, chủ thẻ hoặc thanh toán hàng hóa, dịch vụ. Thẻ ngân hàng là công cụ thanh toán do ngân hàng phát hành thẻ cấp cho khách hàng sử dụng theo hợp đồng ký kết giữa ngân hàng phát hành thẻ và chủ thẻ. Thẻ ngân hàng giả là thẻ không do ngân hàng có thẩm quyền phát hành thẻ đó phát hành. Làm thẻ ngân hàng giả là việc cá nhân không có thẩm quyền sản xuất, phát hành thẻ ngân hàng nhưng sản xuất giống như thẻ ngân hàng (trong đó chứa đựng thông tin, dữ liệu như thẻ của ngân hàng phát hành). Thủ đoạn phạm tội thường là người phạm tội mua thẻ nhựa trắng, mua hoặc đánh cắp thông tin thẻ, mật mã giao dịch. Sau đó dùng máy ghi thẻ để sản xuất thẻ giả, mua bán, sử dụng, lưu hành thẻ giả để chiếm đoạt tài sản của người khác. Hoặc dùng thẻ ngân hàng của nước ngoài đã hết hạn sử dụng vào nước khác để rút tiền…

+ Truy cập bất hợp pháp vào tài khoản là hành vi cố ý vượt qua cảnh báo, mã truy cập, tường lửa hoặc sử dụng mã truy cập của người khác mà không được sự cho phép của người đó để truy cập vào tài khoản không phải của mình, sau đó chiếm đoạt tiền của chủ tài khoản (tài khoản ở đây là tài khoản ngân hàng hoặc tài khoản các ví điện tử).

+ Lừa đảo trong thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp hoặc giao dịch chứng khoán qua mạng nhằm chiếm đoạt tài sản. Kẻ phạm tội đưa ra các thông tin gian dối trong các lĩnh vực trên nhằm tạo niềm tin cho người chủ tài sản, người quản lý tài sản, làm họ tưởng thật và mua, bán, giao dịch hoặc đầu tư vào lĩnh vực đó thông qua mạng. Ví dụ: Đối tượng phạm tội tạo dựng một website để huy động vốn theo kiểu kinh doanh đa cấp (như www.e-invest.com đã bị sập), giả danh các tập đoàn tài chính toàn cầu, huy động vốn với lãi suất cao, sau đó chiếm đoạt tiền của người góp vốn hoặc bán hàng qua mạng nhưng không giao hàng hoặc giao hàng không đúng…

+ Thiết lập, cung cấp trái phép dịch vụ viễn thông, Internet nhằm chiếm đoạt tài sản. Đó là việc thiết lập, cung cấp dịch vụ viễn thông, Internet nhưng không được phép hoặc không đúng giấy phép do cơ quan nhà nước có thẩm quyền cấp nhằm chiếm đoạt tài sản.

Các hành vi trên chỉ cấu thành tội này khi không thuộc trường hợp quy định tại Điều 173 BLHS năm 2015 về Tội trộm cắp tài sản và Điều 174 BLHS năm 2015 về Tội lừa đảo chiếm đoạt tài sản.

Bảy là, Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291)

Hành vi khách quan quy định trong cấu thành tội phạm bao gồm: Hành vi thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng của người khác, khi chủ thể thực hiện 01 trong 05 loại hành vi gồm thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản với số lượng từ 20 tài khoản trở lên hoặc dưới 20 tài khoản nhưng thu lợi bất chính từ 20.000.000 đồng trở lên thì hành vi sẽ thỏa mãn cấu thành tội phạm.

+ Đối với hành vi thu thập thông tin về tài khoản ngân hàng của người khác trong thực tế có hai dạng: Thu thập hợp pháp và thu thập bất hợp pháp (trái phép).

Thu thập hợp pháp thể hiện thông qua hoạt động của người được giao nhiệm vụ liên quan đến thu thập, quản lý (lưu trữ) thông tin về tài khoản và thực hiện các dịch vụ về thanh toán tài chính của khách hàng hoặc các hoạt động về thu chi tài chính trong các cơ quan, doanh nghiệp, tổ chức khác. Hành vi thu thập, quản lý (lưu trữ) thông tin về tài khoản của các chủ thể như trên không vi phạm pháp luật, nhưng nếu các chủ thể lợi dụng nhiệm vụ được giao để thực hiện hành vi mua bán, trao

đổi thông tin về tài khoản của người khác mà họ đang quản lý nhằm thu lợi bất chính hoặc nhằm mục đích bất hợp pháp, hoặc công khai hóa trái phép thông tin về tài khoản ngân hàng của người khác, thì hành vi đó là hành vi khách quan được mô tả trong cấu thành tội phạm. Căn cứ vào hành vi thực tế mà người phạm tội thực hiện để xác định hành vi đó phạm vào tội trao đổi hay mua bán hay công khai hóa trái phép thông tin về tài khoản ngân hàng.

Thu thập bất hợp pháp (trái phép) là hành vi của những người không có thẩm quyền và trách nhiệm trong thu thập, quản lý thông tin về tài khoản ngân hàng của người khác, nhưng đã sử dụng các biện pháp bất hợp pháp như sử dụng thiết bị, công cụ, phần mềm để xâm nhập, sao chép hoặc đột nhập, trực tiếp sao chép trái phép thông tin về tài khoản người khác… với số lượng từ 20 tài khoản trở lên thì tội phạm hoàn thành, cho dù sau đó đối tượng còn thực hiện hành vi tiếp theo là tàng trữ, mua bán, trao đổi hay công khai hóa trái phép thì hành vi cũng chỉ phạm vào Tội thu thập trái phép thông tin về tài khoản ngân hàng quy định tại khoản 1 Điều 291 BLHS năm 2015. Trường hợp thu thập bất hợp pháp thông tin về tài khoản ngân hàng với số lượng dưới 20 tài khoản, sau đó đối tượng mang ra mua bán, trao đổi hoặc công khai hóa và thu lợi bất chính từ 20.000.000 đồng trở lên thì hành vi sẽ phạm vào tội mua bán, hoặc trao đổi hoặc công khai hóa trái phép thông tin về tài khoản ngân hàng.

+ Hành vi tàng trữ trái phép thông tin về tài khoản ngân hàng của người khác là trường hợp người phạm tội do mua, được chuyển giao hoặc từ nguyên nhân nào đó mà họ có được thông tin về tài khoản ngân hàng của người khác sau đó người phạm tội đã thực hiện việc tàng trữ trái pháp luật. Đối với trường hợp tàng trữ thông tin về tài khoản ngân hàng của người khác nhằm mua bán, trao đổi hoặc công khai hóa thì căn cứ vào mục đích của hành vi để xác định tội danh.

+ Đối với hành vi mua bán, trao đổi hoặc công khai trái phép thông tin về tài khoản ngân hàng của người khác là trường hợp người phạm tội có được thông tin về tài khoản từ việc được giao nhiệm vụ theo quy định của pháp luật hoặc do mua mà có, do được chuyển giao hoặc do thu thập bất hợp pháp (như đã phân tích ở đoạn trên)... thông tin về tài khoản sau đó tiến hành bán, trao đổi, công khai hóa thông tin về tài khoản mà mình có được vì động cơ vụ lợi hoặc động cơ cá nhân.

Tám là, 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).

Hành vi khách quan của tội phạm thể hiện ở việc người được giao quản lý, vận hành, điều khiển tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh đã sử dụng tần số vô tuyến điện nói trên vào mục đích khác và đã gây thiệt hại từ 200.000.000 đồng trở lên hoặc đã bị xử phạt vi phạm hành chính về hành vi hoặc đã bị kết án về tội phạm trên, chưa được xóa án tích mà tiếp tục có 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 thì phải chịu TNHS về tội này. Đối với hành vi cố ý gây nhiễu có hại, cản trở hoạt động bình thường của hệ thống thông tin vô tuyến điện nói chung hoặc tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh thì hành vi đó có dấu hiệu của Tội cố ý gây nhiễu có hại Điều 294 BLHS năm 2015.

Chín là, Tội cố ý gây nhiễu có hại (Điều 294).

Hành vi khách quan của tội phạm là hành vi gây nhiễu có hại. Mức độ nhiễu trong vô tuyến điện được chia làm 03 mức độ, gồm: Nhiễu cho phép, nhiễu chấp nhận được và nhiễu có hại. Trong đó, nhiễu cho phép là gây nhiễu thấy được hoặc dự tính được mà thỏa mãn nhiều định lượng và các điều kiện dùng chung trong khuyến nghị của Liên minh viễn thông quốc tế hoặc thỏa thuận đặc biệt; nhiễu chấp nhận được là mức độ nhiễu cao hơn nhiễu cho phép và được sự đồng ý của các cơ quan quản lý mà không ảnh hưởng đến cơ quan khác; nhiễu có hại là ảnh hưởng có hại của năng lượng điện từ do việc phát xạ bức xạ hoặc cảm ứng gây mất an toàn hoặc cản trở, làm gián đoạn hoạt động của thiết bị, hệ thống thiết bị vô tuyến điện đang khai thác hợp pháp[7]. Theo quy định tại Điều 294 BLHS năm 2015, chỉ hành vi gây nhiễu có hại là hành vi khách quan của tội này. Hành vi gây nhiễu có hại có thể được thực hiện bằng các phương thức sau: (1) Sử dụng thiết bị phát sóng vô tuyến điện cố ý gây can nhiễu có hại làm cản trở đến hoạt động thông tin của các mạng và hệ thống thông tin vô tuyến điện khác; (2) Sử dụng thiết bị phát sóng vô tuyến điện gây nhiễu có hại nhưng không thực hiện yêu cầu của cơ quan quản lý nhà nước có thẩm quyền về việc áp dụng các biện pháp kỹ thuật cần thiết để khắc phục nhiễu; (3) Sử dụng thiết bị gây nhiễu

[7] Khoản 13 Điều 3 Luật Tần số vô tuyến điện năm 2009.

có hại cho thông tin vô tuyến khi đã có yêu cầu ngừng sử dụng thiết bị của cơ quan nhà nước có thẩm quyền. Hành vi gây nhiễu có hại bị coi là tội phạm nếu gây thiệt hại từ 200.000.000 đồng trở lên hoặc đã bị xử phạt vi phạm hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm.

Thứ ba, xác định chủ thể trong việc định tội danh đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Là bất kỳ người nào có đủ năng lực TNHS và đủ độ tuổi theo quy định của BLHS.

Thứ tư, xác định mặt chủ quan trong việc định tội danh đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Một là, lỗi của chủ thể là lỗi cố ý trực tiếp, người phạm tội nhận thức được việc thực hiện các hành vi như đề cập ở mặt khách quan là nguy hiểm cho xã hội, nhưng vẫn thực hiện và mong muốn xảy ra.

Hai là, mục đích phạm tội. Mục đích phạm tội được quy định là dấu hiệu định tội của một số tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Cụ thể:

+ Mục đích "sử dụng vào mục đích trái pháp luật" là dấu hiệu định tội bắt buộc của tội sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (Điều 285 BLHS năm 2015). Nếu sử dụng vào mục đích hợp pháp như nghiên cứu, học tập, thử nghiệm, áp dụng biện pháp điều tra tố tụng đặc biệt của cơ quan có thẩm quyền không bị coi là tội phạm.

+ Mục đích "chiếm đoạt tài sản" là một trong những dấu hiệu bắt buộc của tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290 BLHS năm 2015). Đây cũng là dấu hiệu quan trọng giúp phân biệt được tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản với các tội khác.

3. Kết luận

Định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là định tội danh đối với loại tội, các tội phạm cụ thể, mang đầy đủ các đặc điểm chung của định tội danh, như: (1) Là hoạt động áp dụng pháp luật, nếu chủ thể định tội danh là các cơ quan nhà nước có thẩm quyền và người có thẩm quyền; (2) Liên quan đến vấn đề chứng cứ đã được thu thập, kiểm tra, đánh giá. Bên cạnh đó, gắn với tính đặc thù của các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông mà định tội danh đối với nhóm tội danh này có một số điểm đặc trưng, đó là: (1) Hành vi khách quan của các tội trong lĩnh vực công nghệ thông tin, mạng viễn thông chỉ có thể được thực hiện thông qua phương tiện, thiết bị điện tử, các phần mềm, công cụ phần mềm; (2) Chứng cứ được sử dụng để định tội danh các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông chủ yếu được thu thập, khai thác từ nguồn chứng cứ là dữ liệu điện tử; (3) Để bảo đảm hiệu quả nhất của việc thu thập, khai thác chứng cứ cho việc định tội danh thì người tiến hành tố tụng thu thập, khai thác (Điều tra viên, Kiểm sát viên, Thẩm phán, Hội thẩm) cần phải có kiến thức chuyên môn, có hiểu biết về công nghệ thông tin, mạng máy tính, mạng viễn thông, mạng Internet và dữ liệu điện tử. Do đó, đòi hỏi trong quá trình khởi tố, điều tra, truy tố, xét xử đối với loại tội phạm này nói chung, định tội danh nói riêng, đội ngũ Điều tra viên, Kiểm sát viên, Thẩm phán, Hội thẩm phải có những hiểu biết nhất định về công nghệ thông tin (tin học, máy tính, phương tiện điện tử, mạng máy tính, mạng viễn thông...) và có kỹ năng thu thập, bảo quản, phân tích, đánh giá, sử dụng dữ liệu điện tử để phục vụ cho việc giải quyết vụ án./.

TÀI LIỆU THAM KHẢO

1. Nguyễn Hòa Bình (2009), *Tội phạm sử dụng công nghệ cao ở Việt Nam - Thực trạng và giải pháp phòng ngừa, điều tra của lực lượng Cảnh sát nhân dân*, Đề tài khoa học cấp Bộ, Bộ Công an;

2. Lê Cảm (2002), "Một số vấn đề chung về định tội danh", *Giáo trình luật hình sự Việt Nam*, Trường Đại học Luật Hà Nội, Nxb. Công an nhân dân, Hà Nội;

3. Lê Văn Công (2022), "Phát hiện, thu thập, bảo quản dấu vết điện tử trong khám nghiệm hiện trường và khám xét", *Tạp chí Kiểm sát*, số 23/2022;

4. Trần Đình Hòa, *An toàn thông tin và công tác phòng chống tội phạm sử dụng công nghệ cao*, (Sách chuyên khảo), Nxb. Công an nhân dân, Hà Nội, 2011;

5. Công ước của Hội đồng châu Âu về Tội phạm mạng (Công ước Budapest) năm 2001;

6. Phạm Văn Lợi, *Tội phạm trong lĩnh vực công nghệ thông tin* (Sách chuyên khảo), Nxb. Tư pháp, Hà Nội, 2007;

7. Nguyễn Xuân Thu (2015), *Phòng ngừa tội phạm sử dụng Internet, mạng viễn thông kỹ thuật số để chiếm đoạt tài sản*, Luận án tiến sĩ Luật, Học viện Cảnh sát nhân dân;

8. Trường Đại học kiểm sát Hà Nội, *Giáo trình luật hình sự Việt Nam*, Nxb. Công an nhân dân, Hà Nội, 2018;

9. Võ Khánh Vinh, *Lý luận chung về định tội danh*, Nxb. Khoa học xã hội, Hà Nội, 2013.