

BỘ GIÁO DỤC VÀ ĐÀO TẠO

BỘ TƯ PHÁP

TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

NGUYỄN QUÝ KHUYẾN

**TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN,
MẠNG VIỄN THÔNG THEO LUẬT HÌNH SỰ VIỆT NAM**

TÓM TẮT LUẬN ÁN TIẾN SĨ LUẬT HỌC

Hà Nội - 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO

BỘ TƯ PHÁP

TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

NGUYỄN QUÝ KHUYẾN

**TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN,
MẠNG VIỄN THÔNG THEO LUẬT HÌNH SỰ VIỆT NAM**

TÓM TẮT LUẬN ÁN TIẾN SĨ LUẬT HỌC

Chuyên ngành: Luật hình sự và tố tụng hình sự

Mã số: 9380104

Người hướng dẫn khoa học: **1. PGS.TS. Cao Thị Oanh**

2. TS. Lê Đăng Doanh

Hà Nội - 2021

DANH MỤC TỪ VIẾT TẮT

BLHS	Bộ luật hình sự
CNTT	Công nghệ thông tin
Công ước Budapest 2001	Công ước của Hội đồng Châu Âu về tội phạm mạng (2001)
CQĐT	Cơ quan điều tra
LHS	Luật hình sự
Luật mẫu 2002	Luật mẫu về tội phạm máy tính và liên quan đến máy tính của Khối thịnh vượng chung (Anh, Autrialia, Newzland v.v) 2002
MVT	Mạng viễn thông
NXB	Nhà xuất bản
TAND	Toà án nhân dân
TNHS	Trách nhiệm hình sự
VKS	Viện kiểm sát

PHẦN MỞ ĐẦU

Hiện nay, CNTT, MVT đã được ứng dụng phổ biến trong các lĩnh vực của đời sống xã hội. Song hành với sự phát triển và phổ biến của CNTT, MVT là sự xuất hiện của tội phạm trong lĩnh vực CNTT, MVT. Công tác đấu tranh với tội phạm này tuy đã đạt được những kết quả nhất định nhưng còn hạn chế. Tội phạm này đã được quy định trong BLHS năm 1999, được sửa đổi, bổ sung năm 2009 và BLHS năm 2015. Các quy định này ngày càng được bổ sung, hoàn thiện nhưng vẫn còn những tồn tại, hạn chế nhất định. Thực tiễn áp dụng các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT trong những năm qua (2009 -2020) cũng gặp phải một số khó khăn, vướng mắc. Trong khi đó, việc nghiên cứu về tội phạm này trong những năm qua chưa nhiều. Điều đó, đặt ra yêu cầu hiện nay là cần tiếp tục nghiên cứu về tội phạm này. Đó cũng là lý do tác giả lựa chọn đề tài nghiên cứu *“Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo Luật hình sự Việt Nam”* làm luận án tiến sỹ của mình.

Mục đích nghiên cứu của Luận án là xây dựng các giải pháp nâng cao hiệu quả áp dụng quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT trong thời gian tới. Nhiệm vụ nghiên cứu của Luận án bao gồm: (1) nghiên cứu những vấn đề lý luận về tội phạm trong lĩnh vực CNTT, MVT; (2) nghiên cứu quy định của pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT; (3) nghiên cứu các quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT; (4) nghiên cứu thực tiễn áp dụng các quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT trong những năm qua.

Đối tượng nghiên cứu của Luận án là các quan điểm khoa học trong và ngoài nước về tội phạm trong lĩnh vực CNTT, MVT; quy

định và thực tiễn áp dụng các quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT; quy định của văn bản pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT.

Phạm vi nghiên cứu của luận án dưới góc độ Luật hình sự thuộc chuyên ngành Luật hình sự và Tổ tụng hình sự. Thực tiễn áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT là thực tiễn áp dụng của ngành Tòa án trên toàn quốc trong giai đoạn từ năm 2009 đến năm 2020.

Những kết quả nghiên cứu của Luận án sẽ đóng góp những nội dung mới về lý luận và thực tiễn như sau:

Thứ nhất, xây dựng và hoàn thiện hệ thống lý luận như khái niệm, đặc điểm, phân loại tội phạm trong lĩnh vực CNTT, MVT.

Thứ hai, phân tích các dấu hiệu pháp lý và hình phạt của tội phạm trong lĩnh vực CNTT, MVT theo quy định của BLHS năm 2015.

Thứ ba, tổng kết, đánh giá thực tiễn áp dụng LHS về tội phạm trong lĩnh vực CNTT, MVT trong giai đoạn 2009 - 2020.

Thứ tư, đề xuất một số giải pháp nhằm nâng cao hiệu quả áp dụng quy định của BLHS năm 2015 về tội phạm này trong thời gian tới.

Về kết cấu, ngoài phần mở đầu, phần tổng quan về vấn đề nghiên cứu, phần kết luận, danh mục tài liệu tham khảo và phụ lục, nội dung của Luận án được kết cấu thành 3 chương như sau:

Chương 1. Những vấn đề chung về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

Chương 2. Quy định của luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

Chương 3. Thực tiễn áp dụng và giải pháp nâng cao hiệu quả áp dụng quy định của luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

CHƯƠNG 1.

NHỮNG VẤN ĐỀ CHUNG VỀ TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN, MẠNG VIỄN THÔNG

1.1. Những vấn đề lý luận về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

1.1.1. Khái niệm tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Môi trường không gian mạng là môi trường nhân tạo, được tạo ra từ sự kết nối của hạ tầng công nghệ thông tin, trong đó thông tin dữ liệu được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi; là nơi con người thông qua các công cụ, kỹ thuật giao tiếp, tương tác với nhau không bị giới hạn bởi không gian và thời gian.

Trong môi trường không gian mạng, bằng công cụ kỹ thuật, con người có thể tương tác với nhau và thực hiện các hoạt động theo mục đích của mình nên con người cũng có thể thực hiện tội phạm trong môi trường đó. Tội phạm được thực hiện trong môi trường không gian mạng, sử dụng CNTT, MVT để phạm tội hoặc tấn công trực tiếp vào môi trường không gian mạng, được gọi là tội phạm liên quan đến CNTT, MVT. Tuy nhiên, hiện nay còn nhiều quan điểm khác nhau về nội hàm khái niệm, cũng như tên gọi của tội phạm này. Có thể hiểu, tội phạm liên quan đến CNTT, MVT là hành vi nguy hiểm cho xã hội được quy định trong BLHS, do người có năng lực TNHS sử dụng CNTT, MVT thực hiện với lỗi cố ý, xâm phạm đến các quan hệ xã hội được LHS bảo vệ. Tội phạm liên quan đến CNTT, MVT có những đặc điểm sau: (1) đó là tội phạm mới so với tội phạm

truyền thông; (2) CNTT, MVT có liên quan đến tội phạm ở một trong các vai trò là mục tiêu tấn công của tội phạm hoặc là công cụ để thực hiện tội phạm khác; (3) phạm vi của tội phạm liên quan đến CNTT, MVT rất rộng.

Tội phạm trong lĩnh vực CNTT, MVT là một trong số những tội phạm liên quan đến CNTT, MVT. Tội phạm trong lĩnh vực CNTT, MVT có phạm vi hẹp hơn tội phạm liên quan đến CNTT, MVT. Theo đó, tội phạm trong lĩnh vực CNTT, MVT chỉ bao gồm những hành vi phạm tội xâm hại đến quan hệ xã hội đảm bảo an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. Còn những tội phạm mà người phạm tội sử dụng CNTT, MVT để thực hiện tội phạm nhưng xâm phạm đến những nhóm quan hệ xã hội khác sẽ không phải là tội phạm trong lĩnh vực CNTT, MVT. Do đó, có thể rút ra khái niệm tội phạm trong lĩnh vực CNTT, MVT như sau:

Tội phạm trong lĩnh vực CNTT, MVT là hành vi nguy hiểm cho xã hội được quy định trong BLHS, do người có năng lực TNHS sử dụng CNTT, MVT thực hiện với lỗi cố ý, xâm phạm an toàn mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử.

1.1.2. Đặc điểm của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Tội phạm trong lĩnh vực CNTT, MVT có những đặc điểm sau:

Thứ nhất, người phạm tội sử dụng CNTT, MVT làm công cụ, phương tiện để thực hiện tội phạm trong lĩnh vực CNTT, MVT:

Thứ hai, hành vi khách quan của tội phạm trong lĩnh vực CNTT, MVT rất đa dạng, phức tạp với những thủ đoạn tinh vi,

thường xuyên thay đổi theo sự phát triển và ứng dụng của CNTT, MVT trong đời sống

Thứ ba, hậu quả của tội phạm thường rất nghiêm trọng nhưng lại dễ che giấu, khó phát hiện ra.

Thứ tư, tội phạm trong lĩnh vực CNTT, MVT được thực hiện mà không bị giới hạn về không gian và thời gian.

Thứ năm, chủ thể thực hiện tội phạm thường là người có kiến thức về CNTT, MVT và liên quan đến nước ngoài.

Thứ sáu, tội phạm được thực hiện với lỗi cố ý.

Thứ bảy, khách thể của tội phạm là quan hệ xã hội đảm bảo an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử bị tội phạm này xâm phạm.

1.1.3. Phân loại tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Có nhiều cách khác nhau phân loại tội phạm trong lĩnh vực CNTT, MVT. Tùy theo mục đích khác nhau sẽ có các tiêu chí phân loại khác nhau. Cụ thể:

(1) Căn cứ theo tính chất và mức độ nguy hiểm cho xã hội của hành vi phạm tội được quy định trong BLHS, tội phạm trong lĩnh vực CNTT, MVT được chia thành 04 loại: tội phạm ít nghiêm trọng, tội phạm nghiêm trọng, tội phạm rất nghiêm trọng và tội phạm đặc biệt nghiêm trọng.

(2) Căn cứ theo vai trò của CNTT, MVT đối với tội phạm trong lĩnh vực CNTT, MVT, tội phạm này có thể được chia làm hai loại: *Thứ nhất*, tội phạm trong lĩnh vực CNTT, MVT, trong đó mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử là

mục tiêu tấn công của tội phạm. *Thứ hai*, tội phạm trong lĩnh vực CNTT, MVT, trong đó người phạm tội sử dụng CNTT, MVT để thực hiện các hành vi phạm tội, xâm phạm các lợi ích của cơ quan, tổ chức, quyền và lợi ích hợp pháp của cá nhân trong môi trường không gian mạng.

(3) Căn cứ vào vai trò của CNTT, MVT và mục đích phạm tội, tội phạm trong lĩnh vực CNTT, MVT được chia thành 4 nhóm: *Thứ nhất*, tội phạm trong lĩnh vực CNTT, MVT có mục đích xâm phạm tính toàn vẹn, tính bí mật hoặc tính khả dụng của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. *Thứ hai*, tội phạm trong lĩnh vực CNTT, MVT trong đó người phạm tội có mục đích chiếm đoạt tài sản. *Thứ ba*, tội phạm trong lĩnh vực CNTT, MVT, trong đó người phạm tội sử dụng CNTT, MVT để xâm phạm quyền, lợi ích của cơ quan, tổ chức, cá nhân. *Thứ tư*, tội phạm trong lĩnh vực CNTT, MVT, trong đó người phạm tội sử dụng CNTT, MVT để xâm phạm an toàn, trật tự trong lĩnh vực tần số vô tuyến điện.

1.1.4. Cơ sở và ý nghĩa của việc quy định tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong Bộ luật hình sự

Cơ sở lý luận và thực tiễn của việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS là chúng ta có đủ điều kiện để mô tả hành vi phạm tội này; hành vi phạm tội nguy hiểm đáng kể cho xã hội; hành vi phạm tội diễn ra phổ biến trong xã hội.

Việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS đã đáp ứng nhu cầu công tác đấu tranh chống và phòng ngừa tội phạm; bảo vệ trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân; giải quyết những vướng mắc, tồn tại hiện nay;

phù hợp với xu thế của các nước trên thế giới và các quy định của pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT.

1.2. Pháp luật quốc tế về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

1.2.1. Công ước của Hội đồng Châu Âu về tội phạm mạng (2001)

Theo Công ước Budapest 2001, tội phạm mạng được chia thành thành 4 nhóm sau đây:

- Nhóm các tội xâm phạm tính bí mật, toàn vẹn và khả dụng của dữ liệu máy tính và hệ thống máy tính gồm: tội truy cập bất hợp pháp; tội ngăn chặn bất hợp pháp; tội gây rối dữ liệu máy tính; tội gây rối hệ thống; tội lạm dụng các thiết bị;

- Nhóm các tội liên quan đến máy tính gồm: tội giả mạo liên quan đến máy tính; tội lừa đảo liên quan đến máy tính;

- Nhóm các tội liên quan đến nội dung gồm: các tội phạm liên quan đến tài liệu khiêu dâm trẻ em; các tội phân biệt chủng tộc hoặc bài ngoại thông qua hệ thống máy tính;

- Nhóm các tội xâm phạm quyền tác giả và quyền liên quan.

1.2.2. Luật mẫu về tội phạm máy tính và liên quan đến máy tính của Khối thịnh vượng chung (2002)

Luật mẫu 2002 không có quy định về khái niệm tội phạm máy tính và liên quan đến máy tính, mà chỉ quy định cụ thể về những tội sau: tội truy cập bất hợp pháp; tội gây rối dữ liệu; tội gây rối hệ thống máy tính; tội ngăn chặn bất hợp pháp dữ liệu; tội lạm dụng các công cụ, thiết bị liên quan đến máy tính; tội phạm liên quan đến tài liệu khiêu dâm trẻ em;

1.2.3. Công ước của các nước Châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân (2014)

Theo đó, tội phạm mạng bao gồm các tội sau:

- *Các tội phạm tấn công hệ thống máy tính bao gồm:* Truy cập hoặc cố ý truy cập bất hợp pháp vào một phần hoặc toàn bộ hệ thống máy tính hoặc vượt quá thẩm quyền truy cập; Truy cập hoặc cố ý truy cập bất hợp pháp vào một phần hoặc toàn bộ hệ thống máy tính hoặc vượt quá thẩm quyền truy cập với ý định phạm một tội khác hoặc chuẩn bị phạm tội khác; Gian dối để duy trì hoặc cố ý duy trì quyền truy cập vào một phần hoặc toàn bộ hệ thống máy tính; Che giấu, làm sai lệch hoặc cố ý giấu, làm sai lệch chức năng của hệ thống máy tính; Nhập hoặc cố ý nhập dữ liệu giả vào hệ thống máy tính; Hủy hoại hoặc cố ý hủy hoại; xóa hoặc cố ý xóa; làm hư hỏng hoặc cố ý làm hư hỏng; thay thế hoặc cố ý thay thế; thay đổi hoặc cố ý thay đổi dữ liệu máy tính một cách gian dối;

- *Các tội phạm xâm hại dữ liệu máy tính, bao gồm các tội phạm sau:* Chặn hoặc cố ý chặn dữ liệu máy tính trái phép bằng các biện pháp kỹ thuật trong quá trình truyền tải dữ liệu (không công khai) tới hệ thống máy tính, từ hệ thống máy tính hoặc bằng hệ thống máy tính; Cố ý đưa vào, thay thế, xóa hoặc ngăn chặn dữ liệu máy tính để tạo ra các dữ liệu giả, sau đó cố ý sử dụng dữ liệu giả này như một dữ liệu thật; Sử dụng dữ liệu mà biết rõ dữ liệu đó được thu thập một cách gian dối từ một hệ thống máy tính; Mua bán gian dối cho mình hoặc cho người khác bất kỳ một lợi ích nào bằng việc thêm vào, thay thế, xóa hoặc ngăn chặn dữ liệu máy tính hoặc bất kỳ hành vi can thiệp nào tới chức năng của một hệ thống máy tính; Cố ý hoặc vô

ý không tuân thủ đúng quy trình trong việc xử lý dữ liệu cá nhân; Gia nhập hoặc thành lập tổ chức tội phạm để chuẩn bị hoặc để phạm một hoặc một số tội phạm được quy định trong Công ước này.

- *Các tội phạm về nội dung có liên quan đến CNTT, MVT:* Sản xuất, đăng ký, đề nghị, cung cấp, phân phối và truyền tải hình ảnh hoặc cuộc biểu diễn khiêu dâm trẻ em thông qua hệ thống máy tính; Mua bán cho mình hoặc cho người khác, nhập khẩu hoặc đã nhập khẩu; xuất khẩu hoặc đã xuất khẩu hình ảnh hoặc cuộc biểu diễn khiêu dâm trẻ em thông qua hệ thống máy tính; Sở hữu một hình ảnh hoặc cuộc biểu diễn khiêu dâm trẻ em trong hệ thống máy tính hoặc phương tiện lưu giữ dữ liệu máy tính; Tạo điều kiện hoặc cung cấp quyền truy cập vào dữ liệu có hình ảnh, tài liệu, âm thanh hoặc cuộc biểu diễn về khiêu dâm trẻ em; Tạo ra, tải xuống, phân phối hoặc cung cấp bất kể tài liệu viết, tin nhắn, hình ảnh, hình vẽ hoặc các hình thức thể hiện khác về tư tưởng hoặc học thuyết phân biệt chủng tộc, sắc tộc thông qua hệ thống máy tính; Thông qua hệ thống máy tính, đe dọa sẽ phạm tội chống lại người khác vì lý do chủng tộc, màu da, nguồn gốc, quốc tịch hoặc tôn giáo, tín ngưỡng; Thông qua hệ thống máy tính, xúc phạm người khác vì lý do chủng tộc, màu da, nguồn gốc, quốc tịch hoặc tôn giáo, tín ngưỡng; Thông qua mạng máy tính, chấp nhận, khuyến khích hoặc biện minh cho các hành vi phạm tội diệt chủng hoặc tội phạm chống loài người

- *Tội phạm về tài sản liên quan đến CNTT, MVT (khoản 1 Điều 30):* đó là các tội sử dụng CNTT, MVT để thực hiện trộm cắp tài sản, lừa đảo, tiêu thụ tài sản trộm cắp, lạm dụng tín nhiệm, tổng tiền, khủng bố và rửa tiền.

1.2.4. Công ước các nước Á - rập về chống tội phạm công nghệ thông tin

Các hành vi phạm tội được Công ước quy định từ Điều 6 đến Điều 18, bao gồm: tội truy cập bất hợp pháp (Điều 6); tội can thiệp bất hợp pháp (Điều 7); tội xâm phạm tính toàn vẹn của dữ liệu (Điều 8); tội lạm dụng công cụ, phần mềm dùng để phạm tội (Điều 9); tội giả mạo (Điều 10); tội phạm lừa đảo (Điều 11); tội phạm về tài liệu khiêu dâm trẻ em (Điều 12); tội phạm về đánh bạc và khai thác tình dục thông qua việc sử dụng CNTT, MVT (Điều 13); tội phạm xâm phạm quyền riêng tư (Điều 14); tội phạm khủng bố thông qua CNTT, MVT (Điều 15); tội phạm liên quan như: rửa tiền, buôn ma túy, buôn người, tổ chức buôn người, buôn vũ khí (Điều 16); tội phạm về quyền tác giả và các quyền liên quan (Điều 17); tội sử dụng bất hợp pháp các công cụ thanh toán điện tử (Điều 18).

CHƯƠNG 2.

QUY ĐỊNH CỦA LUẬT HÌNH SỰ VIỆT NAM VỀ TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN, MẠNG VIỄN THÔNG

2.1. Khái quát lịch sử lập pháp về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

2.1.1. Giai đoạn từ năm 2010 trở về trước

BLHS năm 1985 không có quy định nào về tội phạm trong lĩnh vực CNTT, MVT. Tội phạm trong lĩnh vực CNTT, MVT lần đầu tiên được quy định trong BLHS năm 1999 gồm 3 điều luật gồm: Điều 224 (Tội tạo ra và lan truyền, phát tán các chương trình vi - rút tin học), Điều 225 (Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử) và Điều 226 (Tội sử dụng trái phép thông tin trên mạng và trong máy tính).

2.1.2. Giai đoạn từ năm 2010 đến năm 2017

Sau 10 năm thực hiện, quy định về tội phạm trong lĩnh vực CNTT, MVT trong BLHS năm 1999 được sửa đổi, bổ sung khá nhiều. Cụ thể:

- Bổ sung thêm 2 điều luật mới là Điều 226a (Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác) và Điều 226b (Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản).

- Sửa đổi Điều 224, Điều 225 và Điều 226 theo hướng thiết kế điều luật cụ thể hơn, rõ ràng hơn, đưa thêm vào cấu thành tăng nặng một số tình tiết định khung

Mặc dù tội phạm trong lĩnh vực CNTT, MVT đã được quy

định trong BLHS năm 1999 và được sửa đổi, bổ sung vào năm 2009, nhưng các quy định này vẫn còn những hạn chế nhất định. Đặc biệt là những thủ đoạn phạm tội mới xuất hiện (hậu quả tiêu cực của sự phát triển trong lĩnh vực CNTT, MVT) đặt ra vấn đề cần tiếp tục sửa đổi, bổ sung hoàn thiện quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT. Đó chính là lý do BLHS năm 2015 đã có những sửa đổi, bổ sung đáng kể các quy định về tội phạm trong lĩnh vực CNTT, MVT so với BLHS năm 1999

2.2. Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo quy định của Bộ luật hình sự năm 2015

2.2.1. Dấu hiệu pháp lý của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

2.2.1.1. Mặt khách quan của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

** Nhóm 1: Mặt khách quan của các tội xâm phạm tính nguyên vẹn, tính bí mật hoặc tính khả dụng của dữ liệu điện tử, mạng máy tính, mạng viễn thông, phương tiện điện tử*

(1) 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 là các hành vi 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. Đối tượng tác động của tội phạm là công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, mạng viễn thông hoặc phương tiện điện tử.

(2) 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. Đối tượng của hành vi phát tán là chương trình tin học có tính năng gây hại. Hành vi phát tán chương trình tin học có tính năng gây hại cho hoạt động của mạng máy tính, mạng viễn thông, thiết bị điện tử bị coi là tội phạm trong các trường hợp: (1) thu lợi bất chính từ 50 triệu đồng trở lên; (2) gây thiệt hại từ 50 triệu đồng trở lên; (3) làm lây nhiễm cho từ 50 phương tiện điện tử trở lên hoặc lây nhiễm cho 01 hệ thống thông tin mà có từ 50 người sử dụng trở lên; (4) đã bị xử phạt hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích lại có hành vi phát tán chương trình tin học có tính năng gây hại.

(3) 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 gồm 3 nhóm sau: hành vi tự ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu điện tử; hành vi ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử; hành vi khác gây rối loạn hoạt động của mạng máy tính, mạng 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: (1) Phần mềm, dữ liệu điện tử; (2) Mạng máy tính, mạng viễn thông, phương tiện điện tử.

Hành vi trên 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 thông, phương tiện điện tử dưới 30 phút và dưới 3 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.

(4) 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 thủ đoạn 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 phạm vi 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 sau: (1) chiếm quyền điều khiển mạng máy tính, mạng viễn thông, 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.

** Nhóm 2: Mặt khách quan của tội phạm trong lĩnh vực CNTT, MVT xâm phạm quyền sở hữu của người khác:*

Nhóm này chỉ có Tội sử dụng trái phép 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 phạm là hành vi sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để chiếm đoạt tài sản của người khác thuộc một trong các trường hợp sau:

Thứ nhất, 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.

Thứ hai, làm, tàng trữ, mua bán, sử dụng, lưu hành thẻ ngân hàng giả nhằm chiếm đoạt tài sản của chủ tài khoản, chủ thẻ hoặc thanh toán hàng hóa, dịch vụ.

Thứ ba, truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản.

Thứ tư, 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.

Thứ năm, thiết lập, cung cấp trái phép dịch vụ viễn thông, internet nhằm chiếm đoạt tài sản.

** Nhóm 3: Mặt khách quan của các tội xâm phạm quyền, lợi ích của tổ chức, cá nhân trong lĩnh vực CNTT, MVT:*

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

Tội phạm được thực hiện thông qua một trong các hành vi khách quan sau:

Thứ nhất, đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật, trừ các trường hợp quy định tại Điều 117, Điều 155, Điều 156 và Điều 326 BLHS năm 2015. Đối tượng tác động của tội phạm là những thông tin trái với quy định của pháp luật.

Thứ hai, 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. Đối tượng tác động của tội phạm là “thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân”.

Thứ ba, hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông.

Các hành vi trên bị coi là tội phạm nếu thuộc các trường hợp như thu lợi bất chính từ 50 triệu đồng trở lên hoặc gây thiệt hại từ 100 triệu đồng trở lên hoặc gây dư luận xấu làm giảm uy tín của cơ quan, tổ chức, cá nhân.

(2) 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 của tội phạm là một trong các hành vi thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin tài khoản ngân hàng của người khác. Đối tượng tác động của tội phạm là “thông tin tài khoản ngân hàng”.

Hành vi trên bị coi là tội phạm nếu thuộc một trong hai trường hợp: (1) thu thập, tàng trữ, trao đổi, mua bán, công khai hoá trái phép từ 20 tài khoản trở lên; (2) thu thập, tàng trữ, trao đổi, mua bán, công khai hoá trái phép dưới 20 tài khoản nhưng người phạm tội đã thu lợi bất chính từ 20 triệu đồng trở lên.

** Nhóm 4: Mặt khách quan của các tội xâm phạm an toàn, trật tự trong lĩnh vực tần số vô tuyến điện:*

(1) 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 là 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 vào mục đích khác. Đối tượng tác động của tội phạm là 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 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 bị coi là tội phạm khi gây thiệt hại từ 200 triệu đồng trở lên hoặc đã bị xử lý hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm.

(2) Tội cố ý gây nhiễu có hại (Điều 294):

Hành vi khách quan của tội phạm là hành vi gây nhiễu có hại.

Hành vi gây nhiễu có hại bị coi là tội phạm nếu gây thiệt hại từ 200 triệu 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.

2.2.1.2. Chủ thể của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Theo quy định tại Điều 12 BLHS năm 2015, người từ đủ 16 tuổi trở lên, không bị mất khả năng nhận thức hoặc khả năng điều khiển hành vi phải chịu TNHS về mọi tội phạm. Do đó, những người này có thể là chủ thể của tất cả các tội phạm trong lĩnh vực CNTT, MVT. Đối với người từ đủ 14 tuổi đến dưới 16 tuổi phải chịu TNHS đối với tội phạm trong lĩnh vực CNTT, MVT, quy định tại khoản 3 Điều 286, khoản 3 Điều 287, khoản 3 Điều 289 và khoản 3, 4 Điều 290 BLHS năm 2015.

2.2.1.3. Mặt chủ quan của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Lỗi của tội phạm trong lĩnh vực CNTT, MVT đều là lỗi cố ý, không có hình thức lỗi vô ý. Tội phạm có thể được thực hiện với lỗi cố ý trực tiếp hoặc cố ý gián tiếp.

Mục đích phạm tội là dấu hiệu bắt buộc đối với một số tội phạm trong lĩnh vực CNTT, MVT.

2.2.2. Hình phạt đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo quy định của Bộ luật hình sự năm 2015

2.2.2.1. Loại và mức hình phạt đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

- Hình phạt chính được áp dụng đối với tội phạm trong lĩnh vực CNTT, MVT bao gồm: hình phạt tiền, hình phạt cải tạo không giam giữ, hình phạt tù có thời hạn.

- Hình phạt bổ sung có thể được áp dụng đối với tội phạm trong lĩnh vực CNTT, MVT bao gồm: Hình phạt cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định; hình phạt tịch thu một phần hoặc toàn bộ tài sản

2.2.2.2. Các dấu hiệu định khung của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Các dấu hiệu định khung tăng nặng của tội phạm trong lĩnh vực CNTT, MVT theo quy định của BLHS năm 2015 gồm nhiều dấu hiệu khác nhau nhưng có thể chia thành 4 nhóm sau đây:

Thứ nhất, các dấu hiệu định khung liên quan đến hành vi phạm tội, bao gồm các dấu hiệu làm gia tăng tính nguy hiểm cho xã hội của tội phạm như: (1) phạm tội có tổ chức, (2) phạm tội từ 2 lần trở lên, (3) phạm tội có tính chất chuyên nghiệp.

Thứ hai, các dấu hiệu định khung liên quan đến hậu quả của tội phạm gồm: (1) Các dấu hiệu tăng nặng phản ánh hậu quả là sự biến đổi hoạt động bình thường của cơ quan, tổ chức, xử sự bình thường của cá nhân; (2) các dấu hiệu định khung tăng nặng phản ánh hậu quả là thiệt hại về an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử; (3) Các dấu hiệu định khung tăng nặng phản ánh số lượng người dùng, số lượng phương tiện điện tử bị ảnh hưởng tính theo số lượng người dùng hoặc tính theo số người dùng phương tiện đó; (4) Các dấu hiệu định khung tăng nặng phản ánh thiệt hại là lợi ích vật chất bị hủy hoại, hư hỏng, mất mát do hành vi phạm tội trong lĩnh vực CNTT, MVT gây ra và được quy thành một số tiền nhất định; (5) Các dấu hiệu định khung tăng nặng phản ánh thiệt hại là doanh thu, lợi ích bất chính hoặc số tiền người phạm tội chiếm đoạt được.

Thứ ba, các dấu hiệu định khung liên quan đến nhân thân của người phạm tội bao gồm: (1) tái phạm nguy hiểm; (2) lợi dụng quyền quản trị mạng máy tính, mạng viễn thông; (3) lợi dụng chức vụ, quyền hạn.

Thứ tư, các dấu hiệu định khung liên quan đến đối tượng tác động của tội phạm: (1) hệ thống dữ liệu thuộc bí mật nhà nước; (2) hệ thống thông tin phục vụ quốc phòng, an ninh; (3) cơ sở hạ tầng thông tin quốc gia; (4) hệ thống thông tin điều hành lưới điện quốc gia; (5) hệ thống thông tin tài chính, ngân hàng; (6) hệ thống thông tin điều khiển giao thông; (7) trạm trung chuyển internet quốc gia, hệ thống cơ sở dữ liệu tên miền và hệ thống máy chủ tên miền quốc gia.

CHƯƠNG 3.

THỰC TIỄN ÁP DỤNG VÀ GIẢI PHÁP NÂNG CAO HIỆU QUẢ ÁP DỤNG QUY ĐỊNH CỦA LUẬT HÌNH SỰ VIỆT NAM VỀ TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN, MẠNG VIỄN THÔNG

3.1. Thực tiễn áp dụng quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

3.1.1. Kết quả đạt được trong việc áp dụng quy định của Luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Trong giai đoạn 2009 - 2020 Tòa án trong cả nước đã xét xử sơ thẩm được 445 vụ án với 933 bị cáo về tội phạm trong lĩnh vực CNTT, MVT

Trong quá trình áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT Tòa án đã có nhiều cố gắng nâng cao hiệu quả giải quyết các vụ án. Tuy còn nhiều khó khăn, nhưng tỷ lệ giải quyết vụ các vụ án đạt trung bình 82,4% trong giai đoạn 2009 - 2020.

Trong quá trình Tòa án xét xử, có một số điều luật thường xuyên được áp dụng. Ngược lại, một số quy định chưa được áp dụng hoặc ít khi được áp dụng.

Việc quyết định hình phạt đối với tội phạm trong lĩnh vực CNTT, MVT: đa số bị cáo bị áp dụng hình phạt tù. Mức hình phạt tù phổ biến là từ 3 năm tù trở xuống. Trong đó, Tòa án đã cho hưởng án treo với tỷ lệ rất cao, chiếm 21,6% trên tổng số bị cáo. Hình phạt bổ sung ít được áp dụng.

Người nước ngoài phạm tội trong lĩnh vực CNTT, MVT tại Việt Nam chiếm tỷ lệ cao.

3.1.2. Hạn chế, khó khăn, vướng mắc trong thực tiễn áp dụng quy định của Luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Trong quá trình thực hiện từ năm 2009 đến năm 2020, đã xuất hiện một số hạn chế, khó khăn, vướng mắc sau:

Thứ nhất, mặc dù đã có quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT và thực tế loại tội phạm này cũng xuất hiện khá phổ biến nhưng các cơ quan có thẩm quyền lại không thể xử lý hoặc xử lý được một số lượng hạn chế.

Thứ hai, trong nhiều trường hợp các cơ quan tiến hành tố tụng áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT chưa thống nhất.

Thứ ba, các cơ quan có thẩm quyền gặp khó khăn khi xử lý những hành vi, thủ đoạn phạm tội mới xuất hiện trong lĩnh vực CNTT, MVT.

Thứ tư, các cơ quan tiến hành tố tụng còn nhầm lẫn khi định tội danh đối với tội phạm trong lĩnh vực CNTT, MVT.

Thứ năm, việc quyết định hình phạt đối với tội phạm trong lĩnh vực CNTT, MVT còn chưa chính xác và thống nhất.

Thứ sáu, khó khăn của các cơ quan tiến hành tố tụng khi phải giải quyết vụ án liên quan đến người nước ngoài.

3.1.3. Nguyên nhân của hạn chế, khó khăn, vướng mắc trong thực tiễn áp dụng quy định của Luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

3.1.3.1. Nguyên nhân từ những tồn tại, bất cập trong các quy định của Bộ luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Thứ nhất, BLHS còn thiếu các quy định cụ thể để xử lý những

thủ đoạn phạm tội mới phát sinh, trong khi đó việc sửa đổi, bổ sung quy định của BLHS chưa kịp thời;

Thứ hai, quy định của BLHS còn mang tính khái quát, chưa cụ thể gây khó hiểu trong quá trình áp dụng;

Thứ ba, còn nhiều tội quy định hậu quả của tội phạm là dấu hiệu bắt buộc trong cấu thành tội phạm cơ bản, trong khi hậu quả của tội phạm này rất khó xác định, dẫn đến một số điều luật ít được áp dụng hoặc không được áp dụng để xử lý đối với các tội phạm đã xảy ra trong thực tế;

Thứ tư, một số quy định cụ thể của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT còn bất cập, hạn chế nên đã hoặc sẽ gây ra những khó khăn trong quá trình áp dụng;

Thứ năm, kỹ thuật lập pháp của LHS chưa hợp lý gây ra khó hiểu, hiểu lầm khi áp dụng một số điều luật.

3.1.3.2. Nguyên nhân từ sự chậm trễ, thiếu giải thích, hướng dẫn của cơ quan có thẩm quyền để áp dụng quy định của Bộ luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Tội phạm trong lĩnh vực CNTT, MVT là loại tội phạm mới, liên quan đến lĩnh vực kỹ thuật chuyên ngành nên rất khó hiểu đối với đa số người áp dụng pháp luật. Hơn nữa, thực tế quy định của BLHS còn khái quát, nhiều nội dung chưa cụ thể. Do đó, công tác giải thích, hướng dẫn áp dụng BLHS có vai trò rất quan trọng. Tuy nhiên, trong những năm qua công tác này còn chậm trễ gây ra những khó khăn cho cơ quan tiến hành tố tụng.

3.1.3.3 Nguyên nhân từ những hạn chế trong công tác tổ chức thực hiện quy định của Luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Thứ nhất, nhân lực thực hiện công tác đấu tranh chống và

phòng ngừa tội phạm trong lĩnh vực CNTT, MVT còn hạn chế.

Thứ hai, đầu tư về trang thiết bị, cơ sở vật chất để đấu tranh đối với tội phạm trong lĩnh vực CNTT, MVT chưa đáp ứng được yêu cầu.

Thứ ba, hoạt động hợp tác quốc tế trong đấu tranh chống và phòng ngừa tội phạm trong lĩnh vực CNTT, MVT chưa được quan tâm đúng mức.

3.2. Giải pháp nâng cao hiệu quả áp dụng quy định của Luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

3.2.1. Giải pháp hoàn thiện quy định của Bộ luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Thứ nhất, quy định bổ sung các hành vi “chiếm hữu, sở hữu nhằm cho người khác sử dụng” và “đề nghị người khác sử dụng, nhập khẩu” công cụ, thiết bị, phần mềm để sử dụng vào mục đích phạm tội tại Điều 285 (Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật).

Thứ hai, sửa đổi, bổ sung quy định về cấu thành tội phạm cơ bản và cấu thành tăng nặng của một số tội cụ thể:

Một là, đối với Điều 286 (Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử), bổ sung dấu hiệu đối tượng tác động của tội phạm là “hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh” vào cấu thành cơ bản tại khoản 1 và cấu thành tăng nặng tại khoản 3.

Hai là, đối với Điều 287 (Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử), bổ sung các đối tượng sau vào cấu thành cơ bản tại khoản 1: (1) hệ

thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh; (2) cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông.

Ba là, đối với Điều 288 (Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông), bổ sung thêm đối tượng là “những thông tin có tác hại lớn cho xã hội” vào cấu thành cơ bản của tội phạm. Theo đó, hành vi phạm tội cho dù chưa gây ra thiệt hại, chưa gây dư luận xấu làm giảm uy tín của Cơ quan, tổ chức, cá nhân hoặc chưa thu được lợi bất chính, nhưng đối với “những thông tin có tác hại lớn cho xã hội” sẽ bị coi là tội phạm đã hoàn thành.

Thứ ba, sửa đổi những bất cập trong một số điều luật của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT:

(1) Đối với Tội 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):

Một là, thay cụm từ “mục đích trái pháp luật” tại tên điều luật và khoản 1 bằng cụm từ “mục đích phạm tội” để thu hẹp phạm vi xử lý của điều luật này.

Hai là, bỏ dấu hiệu định khung tăng nặng quy định tại điểm đ khoản 2 và điểm b khoản 3 Điều 285 BLHS năm 2015 (gây thiệt hại về tài sản từ 100 triệu đồng trở lên).

Ba là, bổ sung quy định truy cứu TNHS đối với pháp nhân thương mại.

(2) Đối với Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287) sửa đổi một số nội dung sau:

*Một là, sửa tội danh Điều 287 thành: “**Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc dữ liệu điện tử**”*

Hai là, sửa đổi điểm e khoản 2 Điều 287 và điểm d khoản 3 Điều 287. Cụ thể:

+ Đối với điểm e khoản 2 Điều 287 “*Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 24 giờ đến 168 giờ hoặc từ 10 lần đến 50 lần trong thời gian 24 giờ*”, sẽ được sửa đổi thành: “***Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 24 giờ đến 168 giờ hoặc từ 10 lần đến 50 lần trong thời gian từ 24 giờ đến 168 giờ***”.

+ Đối với điểm d khoản 3 Điều 287, “*Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 168 giờ trở lên hoặc từ 50 lần trở lên trong thời gian 24 giờ*”, tương tự như trên được sửa thành: “***Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 168 giờ trở lên hoặc từ 50 lần trở lên trong thời gian trên 168 giờ***”.

(3) Đối với Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288) sửa đổi nội dung sau:

Bổ sung dấu hiệu tăng nặng định khung “tái phạm nguy hiểm” vào điểm h khoản 2 Điều 288 BLHS.

(4) Đối với Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290) sửa đổi các nội dung sau:

Một là, sửa đổi khoản 1 Điều 290 theo hướng bỏ cụm từ “nếu không thuộc trường hợp quy định tại Điều 173 và Điều 174 của Bộ luật này”.

Hai là, sửa đổi tăng mức cao nhất của khung hình phạt lên tù chung thân đối với tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản.

3.2.2. Giải pháp về giải thích, hướng dẫn áp dụng quy định của Bộ luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

** Giải thích một số thuật ngữ trong BLHS năm 2015 như sau:*

Một là, “Công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử” tại khoản 1 Điều 285 được hiểu là các công cụ, thiết bị phần cứng hoặc các chương trình máy tính được thiết kế hoặc cải tiến để có chức năng cơ bản là xâm nhập, cản trở, gây rối hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc thu thập, làm giả thông tin, dữ liệu điện tử.

Hai là, “Thông tin riêng hợp pháp của cơ quan, tổ chức, các nhân” tại khoản 1 Điều 288 BLHS năm 2015 là thông tin dữ liệu điện tử, gắn liền với mỗi cơ quan, tổ chức, cá nhân đó nhưng không được công khai hoặc chỉ công khai cho một hoặc một nhóm đối tượng đã được xác định danh tính, địa chỉ cụ thể.

Ba là, “Gây dư luận xấu” tại khoản 1 Điều 288 là gây ra những ý kiến của số đông nhận xét tiêu cực, chê bai, bài xích đối với cơ quan, tổ chức, các nhân làm giảm uy tín của cơ quan, tổ chức, các nhân đó.

Bốn là, “Dẫn đến biểu tình” tại điểm g khoản 2 Điều 288 BLHS năm 2015 là dẫn đến tụ tập đông người để bày tỏ ý chí, nguyện vọng hoặc biểu dương lực lượng chung.

** Hướng dẫn phân biệt các trường hợp dễ gây nhầm lẫn về định tội danh:*

Một là, phân biệt các trường hợp quy định tại Điều 286, Điều 287 và Điều 289 BLHS năm 2015.

Hai là, phân biệt các trường hợp quy định tại Điều 290 với Điều 173 và Điều 174 BLHS năm 2015.

3.2.3. Giải pháp về hoàn thiện, đổi mới công tác tổ chức thực hiện quy định của Luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

** Các giải pháp nâng cao trình độ chuyên môn, năng lực của người tiến hành tố tụng:*

Một là, nâng cao nhận thức của cán bộ các cơ quan tiến hành tố tụng về LHS nói chung, nhất là về tội phạm trong lĩnh vực CNTT, MVT.

Hai là, tích cực đào tạo, bồi dưỡng kiến thức về CNTT, MVT pháp lý cho người tiến hành tố tụng.

Ba là, thường xuyên tập huấn, phổ biến kinh nghiệm đấu tranh đối với tội phạm trong lĩnh vực CNTT, MVT.

Bốn là, bố trí cán bộ Điều tra viên, Kiểm sát viên, Thẩm phán có trình độ, kinh nghiệm đấu tranh đối tội phạm trong lĩnh vực CNTT, MVT để giải quyết vụ án.

** Các giải pháp về tăng cường đầu tư cơ sở vật chất, trang thiết bị kỹ thuật phục vụ đấu tranh đối với tội phạm trong lĩnh vực CNTT, MVT:*

Đầu tư trang bị cho lực lượng chức năng những công cụ, phương tiện hiện đại nhất để phát hiện, đấu tranh đối với loại tội phạm này. Để có được trang thiết bị hiện đại nhất, các lực lượng chức năng không chỉ mua các phần mềm có sẵn trên thị trường, mà tùy

theo mục đích sử dụng có thể đặt hàng để các công ty công nghệ thiết kế, viết các phần mềm chuyên dụng cho mình.

** Các giải pháp về hợp tác quốc tế trong đấu tranh chống tội phạm trong lĩnh vực CNTT, MVT:*

Thứ nhất, ký kết và thực hiện các điều ước quốc tế để hoàn thiện hệ thống pháp luật về phòng chống tội phạm trong lĩnh vực CNTT, MVT.

Thứ hai, hợp tác với các nước để thực hiện tương trợ tư pháp khi điều tra, truy tố, xét xử các vụ án về tội phạm trong lĩnh vực CNTT, MVT.

Thứ ba, hợp tác với các quốc gia, tổ chức quốc tế trong việc thông tin, học hỏi kinh nghiệm đấu tranh phòng chống tội phạm trong lĩnh vực CNTT, MVT thông qua việc tổ chức các hội thảo, hội nghị quốc tế.

PHẦN KẾT LUẬN

Luận án đã giải quyết được những vấn đề sau đây:

Thứ nhất, Luận án đã khái quát những công trình nghiên cứu cả trong nước và quốc tế về tội phạm trong lĩnh vực CNTT, MVT.

Thứ hai, Luận án đã xây dựng và hoàn thiện hệ thống đề lý luận về tội phạm trong lĩnh vực CNTT, MVT. Trong đó:

Tội phạm trong lĩnh vực CNTT, MVT hành vi nguy hiểm cho xã hội được quy định trong BLHS, do người có năng lực TNHS sử dụng CNTT, MVT thực hiện với lỗi cố ý, xâm phạm an toàn mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử.

Tội phạm trong lĩnh vực CNTT, MVT có những đặc điểm cơ bản như: (1) Người phạm tội sử dụng CNTT, MVT làm công cụ, phương tiện để thực hiện tội phạm trong lĩnh vực CNTT, MVT; (2) Hành vi khách quan của tội phạm trong lĩnh vực CNTT, MVT rất đa dạng, phức tạp với những thủ đoạn tinh vi, thường xuyên thay đổi theo sự phát triển và ứng dụng của CNTT, MVT trong đời sống; (3) Hậu quả của tội phạm trong lĩnh vực CNTT, MVT thường rất nghiêm trọng nhưng lại dễ che giấu, khó phát hiện ra; (4) Tội phạm được thực hiện mà không bị giới hạn bởi không gian và thời gian; (5) Chủ thể của tội phạm thường là người có kiến thức về CNTT, MVT và liên quan đến nước ngoài; (6) Tội phạm được thực hiện với lỗi cố ý; (7) Khách thể của tội phạm trong lĩnh vực CNTT, MVT là quan hệ xã hội đảm bảo an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử bị tội phạm này xâm phạm.

Việc phân loại tội phạm trong lĩnh vực CNTT, MVT có thể dựa vào các tiêu chí khác nhau như: (1) dựa vào tính chất, mức độ nguy hiểm cho xã hội của hành vi phạm tội; (2) dựa vào vai trò của CNTT, MVT đối với tội phạm; (3) dựa vào vai trò của CNTT, MVT và mục đích phạm tội.

Thứ ba, Luận án đã nghiên cứu một cách khá đầy đủ các văn bản pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT như Công ước Budapest 2001, Luật mẫu (2002, ...

Thứ tư, Luận án đã phân tích, đánh giá quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT. Nội dung quy định của LHS đã từng bước được xây dựng và hoàn chỉnh phù hợp với các văn bản quốc tế. Tuy nhiên, vẫn còn có những nội dung cần được tiếp tục nghiên cứu hoàn thiện. Trong quá trình áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT còn xuất hiện những khó khăn, vướng mắc. Nguyên nhân của những khó khăn, vướng mắc là quy định của LHS còn nhiều bất cập; công tác giải thích, hướng dẫn áp dụng quy định của LHS còn thiếu và chậm trễ; công tác tổ chức và thực hiện quy định của LHS chưa thật hiệu quả.

Thứ năm, Luận án đã xây dựng được các nhóm giải pháp nâng cao hiệu quả áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong thời gian tới như nhóm giải pháp hoàn thiện quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT; nhóm giải pháp về giải thích, hướng dẫn áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT; nhóm giải pháp về đổi mới tổ chức, thực hiện quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT.

CÁC CÔNG TRÌNH KHOA HỌC CỦA TÁC GIẢ ĐÃ CÔNG BỐ CÓ LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN

1. Nguyễn Quý Khuyển, “Về tội 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) Bộ luật hình sự năm 2015”, *Tạp chí Tòa án nhân dân*, số 3/2017;

2. Nguyễn Quý Khuyển, “Dấu hiệu định lượng thiệt hại của các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo Bộ luật hình sự năm 2015”, *Tạp chí Kiểm sát*, số 18/2017;

3. *Bình luận khoa học Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017)*, TS. Lê Đăng Doanh và PGS.TS. Cao Thị Oanh (Chủ biên), Nhà xuất bản Hồng Đức, 2017, (*Nguyễn Quý Khuyển - Mục 2 Chương XXI: Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông*);

4. Nguyễn Quý Khuyển, “Về sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản”, *Tạp chí kiểm sát*, số 9/2020.

