LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu khoa học độc lập của riêng tôi.

Các kết quả nghiên cứu trong Luận án này chưa được công bố trong bất kỳ công trình nào khác. Các số liệu được sử dụng trong Luận án là trung thực, có nguồn gốc rõ ràng, được trích dẫn đúng theo quy định.

Tôi xin chịu trách nhiệm về tính chính xác và trung thực của Luận án này.

Tác giả luận án

Nguyễn Quý Khuyến

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

DANH MỤC CÁC BẢNG, BIỂU

MỤC LỤC

PHẦN MỞ ĐẦU

1. Lý do lựa chọn đề tài

Hiện nay, cuộc cách mạng khoa học - công nghệ đang phát triển nhanh chóng trên phạm vi toàn cầu, trong đó có lĩnh vực công nghệ thông tin, mạng viễn thông. Có thể nói, công nghệ thông tin, mạng viễn thông đã được ứng dụng phổ biến trong các lĩnh vực của đời sống xã hội. Sự phát triển vượt bậc của công nghệ số đã và đang là nền tảng cho sự phát triển các lĩnh vực kinh tế, xã hội, từ các ngành sản xuất, công nghiệp, dịch vụ thông tin đến văn hóa, giải trí, giao thông, y tế. Trong tương lai, công nghệ thông tin, mạng viễn thông ngày càng có vai trò quan trọng hơn. Ở Việt Nam trong những năm gần đây, công nghệ thông tin, mạng viễn thông đã phát triển mạnh mẽ. Theo Bảng xếp hạng chỉ số tích hợp phát triển bưu chính do Liên minh Bưu chính thế giới công bố, năm 2018 Việt Nam xếp hạng 45/172 quốc gia trên thế giới. Trong lĩnh vực an toàn thông tin mạng, theo Báo cáo chỉ số an toàn thông tin toàn cầu năm 2018 của Liên minh viễn thông quốc tế, Việt Nam xếp thứ 50/194 quốc gia trên thế giới, đứng thứ 5 trong các nước ASEAN[1].

Song hành với sự phát triển và phổ biến của công nghệ thông tin, mạng viễn thông là sự xuất hiện ngày càng phức tạp của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Hiện nay ở Việt Nam, tội phạm này đã gây ra những tác hại không nhỏ đến trật tự, an toàn xã hội. Nhiều lĩnh vực của đời sống xã hội đang ứng dụng công nghệ thông tin, mạng viễn thông đã bị gây thiệt hại. Trong lĩnh vực tư tưởng, văn hóa, người phạm tội thường tập trung lợi dụng kênh truyền thông qua mạng internet để xuyên tạc, vu khống cơ quan, tổ chức, xâm phạm thông tin cá nhân, tuyên truyền những tư tưởng

[1] Nguồn: Bộ Thông tin và Truyền thông (2020), *Sách trắng công nghệ thông tin và truyền thông Việt Nam năm 2019,* NXB. Thông tin và Truyền thông.

kích động bạo lực, trái với thuần phong mỹ tục của Việt Nam. Trong lĩnh vực trật tự, an toàn xã hội, Việt Nam tiếp tục bị coi là địa chỉ vi phạm thường xuyên của những kẻ tấn công với nhiều vụ tấn công, phá hoại, lây nhiễm vi rút, phầm mềm gián điệp, mã tin học độc hại... nhằm vào hệ thống mạng của cơ quan, doanh nghiệp với mức độ, tính chất ngày càng nghiêm trọng, làm rối loạn hoạt động của hệ thống và lộ lọt thông tin. Tình trạng sử dụng các phương tiện điện tử đánh cắp thông tin, làm giả thẻ tín dụng để mua vé máy bay, hàng hóa ở nước ngoài chuyển về Việt Nam tiêu thụ tiếp tục gia tăng, gây thiệt hại lớn cho nạn nhân và xã hội nói chung. Các tổ chức tội phạm tại Việt Nam liên kết chặt chẽ với các tổ chức tội phạm ở nước ngoài tạo thành những đường dây tội phạm hoạt động tinh vi, kín đáo thông qua công cụ là công nghệ thông tin, mạng viễn thông. Tình trạng lừa đảo trong lĩnh vực thương mại điện tử và thanh toán điện tử gia tăng, dẫn đến hậu quả nhiều nước trên thế giới không chấp nhận giao dịch qua mạng internet có địa chỉ IP xuất phát từ Việt Nam, làm ảnh hưởng nghiêm trọng đến uy tín và hình ảnh của Việt Nam trong lĩnh vực thương mại điện tử nói riêng và lĩnh vực kinh tế quốc tế nói chung. Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông có đặc điểm là việc thực hiện tội phạm không bị giới hạn bởi biên giới quốc gia. Do đó, việc xử lý người phạm tội thực hiện tội phạm ở ngoài biên giới quốc gia nhưng lại gây thiệt hại cho nạn nhân ở Việt Nam trong những năm gần đây gặp nhiều khó khăn.

Bộ luật hình sự được coi là công cụ sắc bén để đấu tranh với tội phạm nói chung và với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông nói riêng. Dù chưa được quy định thành tên riêng như hiện nay nhưng Bộ luật hình sự năm 1999 đã có quy định về tội phạm này tại 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). Do mặt trái của sự phát triển trong lĩnh vực công nghệ thông tin, mạng viễn thông, các hành vi phạm tội mới dần xuất hiện. Điều đó dẫn đến nhu cầu sửa đổi, bổ sung Bộ luật hình sự năm 1999 vào năm 2009. Trong lần sửa đổi, bổ sung này, các quy định của Bộ luật hình sự năm 1999 về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông cũng được sửa đổi, bổ sung nhiều quy định mới. Theo đó, các quy định tại Điều 224, Điều 225 và Điều 226 đã được sửa đổi, bổ sung đáng kể; đồng thời đã bổ sung thêm hai 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). Đến Bộ luật hình sự năm 2015, các quy định về tội phạm trong lĩnh vực công nghệ thong tin lại tiếp tục được sửa đổi, bổ sung với nhiều nội dung quan trọng như quy định tên riêng cho nhóm tội này; sửa đổi, bổ sung các tội hiện có, đồng thời bổ sung thêm bốn tội danh mới bao gồm: 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); Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291); 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); Tội cố ý gây nhiễu có hại (Điều 294). Có thể thấy, quy định của Bộ luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông ngày càng được bổ sung, hoàn thiện. Tuy nhiên, các quy định này vẫn còn những điểm hạn chế nhất định, chưa đạt yêu cầu đấu tranh phòng chống tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông hiện nay, cũng như trong thời gian tới. Bên cạnh đó, thực tiễn áp dụng quy định của Bộ luật hình sự để xét xử tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn

thông trong những năm qua (2009 - 2020) đã đạt được những kết quả nhất định. Tòa án đã xét xử được 445 vụ án với 933 bị cáo phạm tội trong lĩnh vực công nghệ thông tin, mạng viễn thông [2]. Tuy nhiên, trong thực tiễn vẫn còn xuất hiện những khó khăn, vướng mắc cần kịp thời tháo gỡ, giải quyết để hoạt động này đạt hiệu quả cao hơn. Về lý luận, tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là tội phạm mới, liên quan đến lĩnh vực kỹ thuật cao, phức tạp nên số lượng công trình nghiên cứu về tội phạm này không nhiều, nhất là từ khi Bộ luật hình sự năm 2015 được bạn hành.

Với những lý do trên, tác giả mạnh dạn lựa chọn đề tài "*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.

2. Mục đích và nhiệm vụ nghiên cứu

Mục đích nghiên cứu của Luận án là xây dựng các 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 trong thời gian tới.

Để đạt được mục đích đề ra, Luận án có nhiệm vụ nghiên cứu những nội dung sau đây:

Thứ nhất, nghiên cứu những vấn đề lý luận về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông như khái niệm, đặc điểm và phân loại tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông; cơ sở của việc quy định về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong Bộ luật hình sự. Qua đó, xây dựng và hoàn thiện hệ thống lý luận về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

Thứ hai, nghiên cứu quy định của pháp luật quốc tế về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Hiểu rõ các quy định của pháp luật quốc tế về tội phạm này là cơ sở để chứng minh cho những vấn đề

[2] Số liệu thống kê của Tòa án nhân dân tối cao năm 2009 - 2020.

lý luận, đồng thời là căn cứ để so sánh, đánh giá với các quy định của Luật hình sự Việt Nam.

Thứ ba, nghiên cứu các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Nội dung nghiên cứu làm rõ thực trạng quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông; so sánh, đánh giá các quy định với các quy định của pháp luật quốc tế và xu thế chung trong Luật hình sự của các nước trên thế giới. Qua đó tìm ra những kết quả đạt được, cũng như những tồn tại, hạn chế trong quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Từ đó, xác định được những vấn đề cần phải tiếp tục nghiên cứu sửa đổi, bổ sung quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

Thứ tư, nghiên cứu thực tiễn áp dụng các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong những năm qua. Qua đó, xác định rõ những kết quả đạt được cũng như những những khó khăn, tồn tại, vướng mắc trong thực tiễn áp dụng; tìm ra nguyên nhân của những khó khăn, tồn tại, vướng mắc đó. Đây cũng là một trong những cơ sở quan trọng để đề xuất các giải pháp nâng cao hiệu quả áp dụng các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong thời gian tới.

3. Đối tượng và phạm vi nghiên cứu

3.1. Đối tượng nghiên cứu

Đối tượng nghiên cứu của Luận án là các quan điểm khoa học ở trong và ngoài nước về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông; quy định và thực tiễn áp dụng các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông; quy định

của văn bản pháp luật quốc tế về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

3.2. Phạm vi nghiên cứu

Nội dung của Luận án nghiên cứu về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông dưới góc độ Luật hình sự thuộc chuyên ngành Luật hình sự và Tố tụng hình sự.

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 được nghiên cứu trong Luận án là thực tiễn áp dụng của ngành Tòa án trên toàn quốc trong giai đoạn từ năm 2009 đến năm 2020.

4. Cơ sở lý thuyết, câu hỏi nghiên cứu và giả thuyết nghiên cứu

4.1. Cơ sở lý thuyết của luận án

Luận án nghiên cứu về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trên cơ sở hệ thống lý luận duy vật biện chứng của chủ nghĩa Mác - Lê nin và lý luận về tội phạm và hình phạt của Luật hình sự Việt Nam. Các giải pháp đề xuất nhằm 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 dựa trên chính sách hình sự của Đảng và Nhà nước về tội phạm nói chung và tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông nói riêng.

4.2. Câu hỏi nghiên cứu của luận án

Câu hỏi nghiên cứu chung của Luận án là trong giai đoạn hiện nay, các quy định của Luật hình sự Việt Nam đã đáp ứng yêu cầu đấu tranh chống và phòng ngừa hiệu quả đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông hay chưa? Để giải quyết câu hỏi nghiên cứu này, Luận án cần giải quyết những vấn đề cụ thể như sau:

Thứ nhất, hệ thống lý luận về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông đã đầy đủ, hoàn thiện và thống nhất hay chưa?

Thứ hai, các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông có phù hợp, phục vụ có hiệu quả công tác đấu tranh chống và phòng ngừa hiệu quả đối với tội phạm này hay không?

Thứ ba, thực tiễn áp dụng các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong những năm qua như thế nào? Cơ quan có thẩm quyền đã đạt được những kết qủa, cũng như gặp phải khó khăn, vướng mắc gì? Nguyên nhân của những khó khăn, vướng mắc đó là gì?

Thứ tư, trong thời gian tới, cần phải có giải pháp gì để nâng cao hiệu quả áp dụng các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông?

4.3. Giả thuyết nghiên cứu của luận án

Trên cơ sở câu hỏi nghiên cứu trên, Luận án xây dựng giả thuyết nghiên cứu sau đây:

Về tổng thể Luận án giả thiết rằng, Luật hình sự Việt Nam hiện nay cơ bản đã đáp ứng yêu cầu của công tác đấu tranh đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Tuy nhiên, vẫn còn có những tồn tại, hạn chế, vướng mắc nhất định, cần phải tiếp tục hoàn thiện và đề ra giải pháp thực hiện có hiệu quả hơn trong thời gian tới. Cụ thể:

Thứ nhất, hệ thống lý luận về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông đã được xác định rõ nhưng vẫn còn có nội dung chưa thống nhất, chưa hoàn thiện. Do đó, cần xây dựng và hoàn thiện hệ thống lý luận về tội phạm này.

Thứ hai, các quy định của Luật hình sự Việt Nam cơ bản đã đáp ứng được yêu cầu đấu tranh chống và phòng ngừa tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, nhưng vẫn còn một số tồn tại, hạn chế, làm

ảnh hưởng đến hiệu quả đấu tranh chống và phòng ngừa tội phạm này. Trong thời gian tới, các quy định này cần được tiếp tục nghiên cứu sửa đổi, hoàn thiện.

Thứ ba, việc áp dụng quy định của Luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong những năm qua (2009 - 2020) đã đạt được những kết quả nhất định, nhưng vẫn còn những tồn tại, hạn chế, vướng mắc. Những tồn tại, hạn chế, vướng mắc này do những nguyên nhân chủ quan và khách quan khác nhau. Cần phải tìm ra những giải pháp để hạn chế, giải quyết những nguyên nhân này trong thời gian tới.

5. Phương pháp nghiên cứu

Trên cơ sở phương pháp luận duy vật biện chứng và phương pháp duy vật lịch sử, Luận án chủ yếu sử dụng phương pháp phân tích, phương pháp tổng hợp và phương pháp so sánh luật.

Phương pháp phân tích được sử dụng trong tất cả các chương của Luận án. Trên cơ sở phân tích các công trình nghiên cứu của các tác giả trong và ngoài nước về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, Luận án tổng hợp, phân loại các nghiên cứu đó theo từng trường phái và từng vấn đề nghiên cứu. Từ đó có cái nhìn tổng thể về tình hình nghiên cứu đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông ở trong và ngoài nước.

Phương pháp phân tích và phương pháp tổng hợp được sử dụng để phân tích những vấn đề lý luận, các quan điểm khoa học, từ đó tổng hợp, khái quát thành hệ thống những vấn đề lý luận về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

Phương pháp phân tích, phương pháp tổng hợp thường xuyên sử dụng để phân tích làm rõ các quy định của Luật hình sự Việt Nam về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông và thực tiễn áp dụng các

quy định này trong những năm qua ở Việt Nam. Bên cạnh đó, phương pháp so sánh luật cũng được sử dụng để phân tích, so sánh giải thích sự tương đồng và khác biệt giữa quy định của Luật hình sự Việt Nam với pháp luật quốc tế và xu hướng chung của các nước trên thế giới về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

6. Ý nghĩa khoa học và thực tiễn

Đây là công trình khoa học cấp độ luận án tiến sỹ chuyên ngành Luật hình sự và Tố tụng hình sự đầu tiên về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông ở Việt Nam. Những đóng góp về khoa học và thực tiễn của Luận án được thể hiện thông qua những điểm mới sau đây:

Thứ nhất, xây dựng và hoàn thiện hệ thống lý luận như khái niệm, đặc điểm của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Đây là những vấn đề phức tạp, hiện nay còn có quan điểm khác nhau. Với hệ thống lý luận về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thong được xây dựng và hoàn thiện trong Luận án sẽ góp phần làm rõ vấn đề lý luận, làm giầu thêm tri thức về tội phạm này.

Thứ hai, phân tích các dấu hiệu pháp lý và hình phạt của tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo quy định của Bộ luật hình sự năm 2015. Bình luận, so sánh, đánh giá các quy định này với những chuẩn mực và xu hướng của pháp luật quốc tế về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông để tìm ra điểm tương thích và chưa tương thích của Luật hình sự Việt Nam. Trong bối cảnh Bộ luật hình sự năm 2015 vừa được ban hành và có hiệu lực chưa lâu, những phân tích, đánh giá trong Luận án giúp hiểu rõ bản chất các quy định của Bộ luật hình sự năm 2015 về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Đó là cơ sở cần thiết trong việc áp dụng đúng các quy định này trong thực tiễn.

Thứ ba, tổng kết, đánh giá thực tiễn 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. Trên cơ sở đó, đề xuất một số giải pháp nhằm nâng cao hiệu quả áp dụng quy định của Bộ luật hình sự năm 2015 về tội phạm này trong thời gian tới. Đây là những kiến nghị mang tính thực tiễn có giá trị tham khảo đối với các cơ quan có thẩm quyền trong việc ban hành pháp luật và trong công tác đấu tranh phòng chống tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông hiện nay.

7. Kết cấu của Luận án

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.

PHẦN TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU

1. Tình hình nghiên cứu về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

1.1. Tình hình nghiên cứu ở Việt Nam

Ở Việt Nam, lĩnh vực CNTT, MVT mới chỉ được ứng dụng phổ biến vào đầu những năm 90 của thế kỷ XX. Do đó, việc nghiên cứu về tội phạm trong lĩnh vực CNTT, MVT cũng chỉ được quan tâm nghiên cứu sau đó, nhưng không nhiều. Đến khi BLHS năm 1999 quy định về tội phạm trong lĩnh vực CNTT, MVT tại Điều 224, Điều 225 và Điều 226, số lượng nghiên cứu về tội phạm này mới tăng lên đáng kể. Cho đến nay, các nghiên cứu này tập trung ở một số chủ đề như: (1) nghiên cứu những vấn đề lý luận về tội phạm trong lĩnh vực CNTT, MVT; (2) phân tích, bình luận các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT; (3) phân tích những bất cập trong thực tiễn áp dụng quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT và đề xuất, kiến nghị phương án khắc phục; (4) nghiên cứu về các văn bản quốc tế, cũng như kinh nghiệm của các nước về tội phạm trong lĩnh vực CNTT, MVT.

Khái niệm tội phạm trong lĩnh vực CNTT, MVT là chủ đề nghiên cứu được quan tâm nhất từ trước đến nay. Bởi vì tội phạm trong lĩnh vực CNTT, MVT là tội phạm mới nên khái niệm của nó cần phải được nghiên cứu rõ trước tiên. Nội dung các nghiên cứu về khái niệm tội phạm trong lĩnh vực CNTT, MVT ở Việt Nam được chia làm 2 giai đoạn:

Giai đoạn đầu khi mới xuất hiện, tội phạm trong lĩnh vực CNTT, MVT được hiểu là hành vi sử dụng CNTT, MVT để tấn công môi trường không gian mạng. Trong đó, CNTT, MVT chính là mục tiêu tấn công của tội phạm. Lúc này tội phạm trong lĩnh vực CNTT, MVT có thể được gọi bằng các thuật

ngữ khác nhau như tội phạm máy tính, tội phạm vi tính, tội phạm mạng…Tuy nhiên, chúng đều có đặc điểm chung là coi CNTT, MVT là mục tiêu tấn công. Quan niệm về tội phạm trong lĩnh vực CNTT, MVT như vậy thường được gọi là tội phạm trong lĩnh vực CNTT, MVT theo nghĩa hẹp. Quan niệm này được thể hiện trong các bài viết của các tác giả Trần Cảnh Hưng, Dương Tuyết Miên và Nguyễn Ngọc Khanh. Theo tác giả Trần Cảnh Hưng, tội phạm máy tính được hiểu là *"các hành vi tác động trực tiếp hoặc gián tiếp vào sự hoạt động của máy tính, mạng máy tính, các thiết bị ngoại vi, cơ sở dữ liệu, các quá trình điều khiển dựa trên sự hoạt động của các thiết bị tin học nhằm mục đích phá hoại, lừa đảo, che dấu, đánh cắp thông tin"*[3]. Theo định nghĩa này, tội phạm máy tính có hai đặc trưng cơ bản: (1) người phạm tội sử dụng máy tính, mạng máy tính, các thiết bị ngoại vi, thiết bị tin học để thực hiện tội phạm; (2) mục đích phạm tội là để "phá hoại, lừa đảo, che dấu, đánh cắp thông tin". Cũng theo xu hướng này, tác giả Dương Tuyết Miên và Nguyễn Ngọc Khanh khi bàn về khái niệm "tội phạm máy tính" cho rằng, khái niệm này thường được nghiên cứu dưới hai góc độ, theo nghĩa rộng và theo nghĩa hẹp. Tội phạm vi tính theo nghĩa rộng bao gồm tất cả các tội phạm liên quan đến máy tính; còn theo nghĩa hẹp bao gồm các hành vi sao chép, lấy cắp, phá hủy, làm hư hỏng, thay đổi dữ liệu, cản trở, khai thác trái phép dịch vụ vi tính... Đồng thời các tác giả cũng nhận định "đa số các chuyên gia khi bàn về tội phạm vi tính thì chỉ đề cập tới tội phạm vi tính theo nghĩa hẹp"[4]. Có thể thấy, khái niệm tội phạm máy tính mà các tác giả trên đưa ra chính là một trong những dạng đặc trưng nhất của tội phạm trong lĩnh vực CNTT, MVT.

---

[3] Xem: Trần Cảnh Hưng (2003), "Một số vấn đề lý luận và thực tiễn về tội phạm máy tính", *Tạp chí kiểm sát*, số 1/2003, tr. 26.

[4] Xem: Dương Tuyết Miên, Nguyễn Ngọc Khanh (2000), "Tội phạm vi tính", *Tạp chí Tòa án nhân dân*, số 5/2000, tr.18.

Khái niệm tội phạm trong lĩnh vực CNTT, MVT theo nghĩa hẹp là đúng nhưng chưa đủ. Bởi vì khi CNTT, MVT được ứng dụng rộng rãi trong đời sống xã hội sẽ xuất hiện xu hướng phạm tội mới. Trong đó người phạm tội sẽ dùng CNTT, MVT làm công cụ, phương tiện để thực hiện các tội phạm khác. Do vậy, cần phải mở rộng khái niệm tội phạm trong lĩnh vực CNTT, MVT theo nghĩa hẹp đã đề cập ở trên.

Giai đoạn thứ hai, khái niệm tội phạm trong lĩnh vực CNTT, MVT được mở rộng phạm vi. Theo đó, tội phạm trong lĩnh vực CNTT, MVT là tội phạm có liên quan đến CNTT, MVT với vai trò là mục đích phạm tội và công cụ, phương tiện phạm tội. Hầu hết các nghiên cứu sau này về khái niệm tội phạm trọng lĩnh vực CNTT, MVT, ở mức độ khác nhau đều theo xu hướng này. Chúng ta có thể kể đến một số nghiên cứu sau:

Về sách chuyên khảo có cuốn "*Tội phạm trong lĩnh vực công nghệ thông tin*" của TS. Phạm Văn Lợi chủ biên (NXB. Tư pháp, 2007) và cuốn "*Tội phạm trong lĩnh vực bưu chính - viễn thông và giải pháp phòng ngừa, đấu tranh"* của Viện chiến lược và Khoa học công an (NXB. Công an nhân dân, 2007).

Luận văn thạc sỹ có các luận văn *"Các tội phạm trong lĩnh vực tin học theo Luật hình sự Việt Nam"* của ThS. Trần Thị Hồng Lê (Luận văn thạc sỹ luật học, khoa Luật, ĐHQG Hà Nội, năm 2009) và *"Tội phạm công nghệ thông tin trong Bộ luật hình sự Việt Nam"* của ThS.Trần Thanh Thảo (Luận văn thạc sỹ luật học, Trường đại học luật thành phố Hồ Chí Minh, năm 2013).

Bài nghiên cứu đăng trên tạp chí chuyên ngành có: "*Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học*," của tác giả Nguyễn Mạnh Toàn đăng trên Tạp chí Nhà nước và Pháp luật, số 3/2002; bài viết "*Khái niệm và đặc điểm của tội phạm công nghệ thông tin- Sự khác nhau giữa tội phạm công nghệ thông tin và tội phạm thông thường"* của tác giả Đặng Trung Hà đăng

trên Tạp chí Dân chủ và Pháp luật, số 3/2009; bài viết "Tội phạm máy tính - Khái niệm, đặc trưng và một số giải pháp phòng, chống", của tác giả Nguyễn Hòa Bình đăng trên *Tạp chí Công an nhân dân*, tháng 8/2003.

Theo các nghiên cứu trên, tội phạm trong lĩnh vực CNTT, MVT là tội phạm có liên quan đến CNTT, MVT với những vai trò khác nhau. Trong đó, CNTT, MVT thường liên quan đến tội phạm với 4 vai trò: (1) CNTT, MVT là mục đích của tội phạm; (2) CNTT, MVT là công cụ, phương tiện phạm tội; (3) CNTT, MVT là chủ thể của tội phạm; (4) CNTT, MVT là vật trung gian, cất giấu, lưu trữ dấu vết tội phạm[5]. Các tác giả như Nguyễn Mạnh Toàn, Đặng Trung Hà tiếp cận khái niệm "tội phạm tin học" hoặc "tội phạm công nghệ thông tin" cũng cho rằng tội phạm máy tính là tội phạm có liên quan đến máy tính với vai trò mục đích của tội phạm, công cụ phạm tội và vật trung gian để cất giấu, lưu giữ những thứ đã chiếm đoạt được[6].

Theo cách tiếp cận này, khái niệm tội phạm trong lĩnh vực CNTT, MVT có phạm vi rất rộng, tuỳ theo mục đích và góc độ nghiên cứu. Chính vì vậy dẫn đến việc các tác giả xác định phạm vi khái niệm tội phạm trong lĩnh vực CNTT, MVT không thống nhất. Có trường hợp xác định phạm vi tội phạm này quá rộng như trong cuốn sách chuyên khảo "*Tội phạm trong lĩnh vực bưu chính - viễn thông và giải pháp phòng ngừa, đấu tranh"* của Viện chiến lược và Khoa học công an. Các tác giả cuốn sách này cho rằng, từ trước đến nay chưa có khái niệm chính thức về loại tội phạm này, mà chỉ liệt kê một số hành vi vi phạm phải bị xử lý bằng pháp luật trong các văn bản pháp luật

[5] Xem: Phạm Văn Lợi (2007), *Tội phạm trong lĩnh vực công nghệ thông tin*, NXB. Tư pháp, tr.28.

[6] Xem: Nguyễn Mạnh Toàn, "Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học", *Tạp chí Nhà nước và Pháp luật*, số 3/2002, tr.30.

khác nhau[7]. Thông qua việc xác định những hành vi bị pháp luật xử lý trong lĩnh vực này trong các văn bản pháp luật từ năm 1945 đến khi có BLHS năm 1999, tác giả khẳng định: "*các hành vi vi phạm các điều cấm trong công tác quản lý và sử dụng các dịch vụ bưu chính - viễn thông do Nhà nước và các cơ quan có thẩm quyền đặt ra là các hành vi của tội phạm trong lĩnh vực bưu chính- viễn thông*"[8]. Do đó, tội phạm trong lĩnh vực bưu chính - viễn thông được quy định trong BLHS năm 1999 bao gồm: tội phản bội Tổ quốc (Điều 78), tội gián điệp (Điều 80), Tội xâm phạm bí mật an toàn thư tín của người khác (Điều 125), Tội sử dụng trái phép thông tin trên mạng và trong máy tính (Điều 226), Tội trộm cắp cước viễn thông (Điều 138), Tội phá hủy công trình, phương tiện quan trọng về an ninh quốc gia (Điều 231), Tội vô ý làm lộ tài liệu bí mật trong công tác (Điều 287), Tội lợi dụng chức vụ và quyền hạn trong khi thi hành công vụ (Điều 281), Tội tham ô (Điều 278), Tội tàng trữ, vận chuyển, mua bán trái phép chất ma túy (Điều 195)[9]. Có thể thấy, các tác giả này đã xác định đã xác định tội phạm trong lĩnh vực viễn thông quá rộng. Như một số tác giả đã nhận xét, cứ theo cách xác định này thì bất kể tội nào cũng có thể được coi là tội phạm trong lĩnh vực viễn thông.

Có thể thấy việc mở rộng khái niệm tội phạm trong lĩnh vực CNTT, MVT là cần thiết, phù hợp với thực tiễn phát triển của tội phạm này. Các nghiên cứu đã chỉ ra đặc trưng quan trọng của tội phạm này là sự liên quan đến CNTT, MVT ở các vai trò khác nhau. Đây là điểm thống nhất quan trọng để xác định khái niệm tội phạm này. Tuy nhiên, tội phạm liên quan đến CNTT, MVT ở mức độ nào thì được coi là tội phạm trong lĩnh vực CNTT, MVT vẫn chưa có sự thống nhất.

---

[7] Xem: Viện chiến lược và khoa học công an (2007), *Tội phạm trong lĩnh vực bưu chính - viễn thông và giải pháp phòng ngừa, đấu tranh,* NXB. Công an nhân dân, tr. 30.

[8] Xem: Viện chiến lược và khoa học công an (2007), Tlđd, tr. 43.

[9] Xem: Viện chiến lược và khoa học công an (2007), Tlđd, tr. 43 - 45.

Vấn đề đặc điểm của tội phạm trong lĩnh vực CNTT, MVT cũng được một số tác giả nghiên cứu. Theo tác giả Phạm Văn Lợi, tội phạm trong lĩnh vực CNTT cũng có các đặc điểm của tội phạm nói chung. Ngoài ra, tội phạm trong lĩnh vực CNTT còn có một số điểm đặc trưng khác với những tội phạm khác như: (1) có vai trò của máy tính, mạng máy tính và các thiết bị công nghệ thông tin có liên quan; (2) chủ thể phạm tội là người thông minh, có kiến thức và am hiểu về công nghệ mới; (3) hậu quả của tội phạm thường nghiêm trọng; (4) hành vi phạm tội thường có tính chất tinh vi, phức tạp[10]. Điều này cũng được trình bày trong bài nghiên cứu "*Khái niệm và đặc điểm của tội phạm công nghệ thông tin - Sự khác nhau giữa tội phạm công nghệ thông tin và tội phạm thông thường"* của tác giả Đặng Trung Hà đăng trên Tạp chí Dân chủ và Pháp luật, số 3/2009. Bài viết đã phân tích rõ sự khác nhau giữa tội phạm trong lĩnh vực CNTT, MVT với các tội phạm khác là cơ sở để BLHS có quy định riêng về tội phạm này. Đặc điểm các yếu tố của tội phạm trong lĩnh vực CNTT cũng được nghiên cứu. Theo đó, các yếu tố của tội phạm trong lĩnh lực CNTT như khách thể của tội phạm, mặt khách quan của tội phạm, mặt chủ quan của tội phạm và chủ thể của tội phạm[11]. Thông qua việc nghiên cứu đặc điểm cấu trúc của tội phạm trong lĩnh vực CNTT, MVT giúp chúng ta có cơ sở để lựa chọn dấu hiệu nào sẽ được BLHS quy định trong cấu thành tội phạm.

Phân loại tội phạm trong lĩnh vực CNTT, MVT là nội dung có ý nghĩa quan trọng về cả lý luận và thực tiễn. Tuy nhiên, nội dung này ít được nghiên cứu ở Việt Nam. Có tác giả nghiên cứu đến nhưng còn sơ sài. Chẳng hạn, theo tác giả Đặng Trung Hà, tội phạm trong lĩnh vực CNTT, MVT được chia thành 2 nhóm: (1) tội phạm CNTT xâm phạm, làm ảnh hưởng đến hoạt động

[10] Xem: Phạm Văn Lợi (2007), Tlđd, tr. 41 - 46.

[11] Xem: Phạm Văn Lợi (2007), Tlđd, tr. 33 - 41.

bình thường của hệ thống máy tính, mạng máy tính và thiết bị điện tử; (2) tội phạm CNTT sử dụng máy tính và mạng máy tính làm công cụ để xâm phạm đến lợi ích chính đáng của cá nhân, pháp nhân, tổ chức, ảnh hưởng đến trật tự công cộng[12]. Cách phân loại này đúng nhưng còn quá khái quát, không có nhiều ý nghĩa; chưa xác định được tiêu chí phân loại cụ thể làm căn cứ phân loại.

Từ khi tội phạm trong lĩnh vực CNTT, MVT được quy định trong BLHS năm 1999, một số tác giả nghiên cứu về các quy định này. Tuy nhiên, các nghiên cứu chủ yếu nhằm mục đích giải thích, bình luận nội dung các điều luật trong BLHS. Cụ thể: *"Giáo trình Luật hình sự Việt Nam"* (Tập II) của Trường Đại học luật Hà Nội (NXB. Công an nhân dân, 2015); *"Bình luận khoa học Bộ luật hình sự 1999"* (Phần các tội phạm) do TS. Nguyễn Đức Mai chủ biên (NXB. Chính trị quốc gia, 2013). Khi BLHS năm 2015 được ban hành với nhiều quy định được sửa đổi, bổ sung về tội phạm trong lĩnh vực CNTT, MVT nhiều công trình nghiên cứu đã làm rõ các dấu hiệu pháp lý và hình phạt của tội này như: *"Giáo trình Luật hình sự Việt Nam" (Phần các tội phạm) Tập 2* của Trường Đại học kiểm sát Hà Nội (NXB. Đại học quốc gia Hà Nội, năm 2016; *"Bình luận khoa học BLHS năm 2015, sửa đổi, bổ sung năm 2017"* do TS. Lê Đăng Doanh và PGS.TS. Cao Thị Oanh chủ biên (NXB. Hồng Đức, 2018); "Bình luận khoa học Bộ luật hình sự năm 2015, được sửa đổi, bổ sung năm 2017 (Phần các tội phạm), quyển 2 do GS.TS. Nguyễn Ngọc Hòa chủ biên (NXB. Tư pháp, 2018); "Bình luận khoa học Bộ luật hình sự năm 2015 (sửa đổi, bổ sung năm 2017) phần các tội phạm của các tác giả PGS.TS. Trần Văn Luyện, PGS.TS. Phùng Thế Vắc, TS. Lê Văn Thư,

[12] Xem: Đặng Trung Hà (2009), "Khái niệm và các đặc điểm của tội phạm công nghệ thông tin - Sự khác biệt giữa tội phạm công nghệ thông tin và tội phạm thông thường", *Tạp chí Nhà nước và Pháp luật*, số 3/2009.

TS. Mai Văn Bộ, LS.ThS. Phạm Thanh Bình, TS. Nguyễn Ngọc Hà, LS.Phạm Thị Thu (NXB. Công an nhân dân, 2018).

Vấn đề kỹ thuật lập pháp của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT được nghiên cứu trong đề tài khoa học cấp Bộ *"Nghiên cứu tính thống nhất giữa Bộ luật hình sự trong việc quy định các tội phạm với các luật khác trong hệ thống pháp luật Việt Nam"* (2016) do GS.TS Nguyễn Ngọc Hòa làm chủ nhiệm, trong đó có chuyên đề *"Đánh giá tính thống nhất giữa Bộ luật hình sự 2015 với luật công nghệ thông tin"* của TS. Nguyễn Văn Hương. Thông qua việc nghiên cứu, so sánh giữa các tội thuộc lĩnh vực CNTT được quy định trong BLHS 2015 với các quy định về hành vi bị cấm trong Luật công nghệ thông tin, tác giả đưa ra nhận xét đánh giá *"hầu hết các hành vi bị nghiêm cấm trong Luật công nghệ thông tin (có tính nguy hiểm đáng kể cho xã hội) đều được quy định trong BLHS 2015. So với BLHS 1999, các tội thuộc lĩnh vực công nghệ thông tin trong BLHS 2015 được bổ sung thêm ba tội danh mới. Tuy nhiên, các quy định trong BLHS 2015 vẫn còn có những hạn chế nhất định và điều đó đòi hỏi cần được tiếp tục hoàn thiện"*[13]. Để hoàn thiện quy định của BLHS năm 2015, tác giả đưa ra một số đề xuất như: (1) quy định trách nhiệm hình sự của pháp nhân đối với Điều 285 và Điều 292; (2) chuyển Điều 290 về chương các tội xâm phạm sở hữu; (3) thu hẹp phạm vi điều chỉnh của Điều 292; (4) bổ sung dấu hiệu làm rõ ranh giới của hành vi bị coi là tội phạm với hành vi vi phạm (bị xử phạt hành chính) quy định tại Điều 290.

Hướng nghiên cứu về thực tiễn áp dụng quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT và đề xuất, kiến nghị các giải pháp nâng

[13] Xem: Ban chủ nhiệm đề tài khoa học cấp Bộ của Bộ Tư pháp (2016), *Tài liệu hội thảo cấp Bộ "Tính thống nhất giữa Bộ luật hình sự với các luật khác trong hệ thống pháp luật Việt Nam"*, Hà Nội, tr. 83.

cao hiệu quả áp dụng các quy định này được rất nhiều tác giả quan tâm. Các tác phẩm nghiên cứu này khá phong phú bao gồm sách chuyên khảo, luận án, luận văn và các bài nghiên cứu công bố trên các tạp chí chuyên ngành. Trong tác phẩm "*Tội phạm trong lĩnh vực công nghệ thông tin*", thông qua việc nghiên cứu tình hình tội phạm và các quy định pháp luật về phòng, chống tội phạm trong lĩnh vực công nghệ thông tin ở nước ta cho đến trước năm 2007, các tác giả nêu ra một số khó khăn, vướng mắc trong quá trình điều tra, truy tố, xét xử loại tội phạm này[14]. Để giải quyết những khó khăn, vướng mắc trên các tác giả đưa ra một số giải pháp đấu tranh phòng, chống tội phạm trong lĩnh vực công nghệ thông tin như (1) các giải pháp về thiết chế; (2) các giải pháp về thể chế, trong đó có việc nghiên cứu pháp luật quốc tế như Công ước Budapest 2001 để bổ sung vào BLHS năm 1999 một loạt các hành vi tội phạm trong lĩnh vực CNTT mới phát sinh[15]; bổ sung một số điều luật liên quan đến chứng cứ điện tử trong BLTTHS năm 2003 về chứng cứ điện tử; (3) Các giải pháp về các điều kiện đảm bảo; (4) các giải pháp khác như nâng cao năng lực đội ngũ cán bộ trong cơ quan bảo vệ pháp luật; nâng cao hiệu quả các biện pháp xử lý vi phạm pháp luật trong lĩnh vực CNTT; tăng cường công tác tuyên truyền, giáo dục ý thức pháp luật; tăng cường sự phối hợp giữa cơ quan chuyên ngành với cơ quan thực thi pháp luật và hợp tác quốc tế trong phòng, chống tội phạm trong lĩnh vực CNTT. Các giải pháp mà các tác giả nêu ra có những ý nghĩa tham khảo nhất định nhất là những giải pháp bổ sung, hoàn thiện pháp luật hình sự và áp dụng pháp luật hình sự trong lĩnh vực này. Trong tác phẩm *"Tội phạm trong lĩnh vực bưu chính - viễn thông và giải pháp phòng ngừa, đấu tranh"* của Viện chiến lược và khoa học công an (NXB. Công an nhân dân, 2007), các tác giả đã nêu ra một số khó khăn của

[14] Xem: Phạm Văn Lợi (2007), Tlđd, tr. 90 - 104.

[15] Xem: Phạm Văn Lợi (2007), Tlđd, tr. 128 - 130.

ngành công an khi áp dụng các quy định của BLHS năm 1999 để đấu tranh với các tội phạm trong lĩnh vực bưu chính - viễn thông như (1) thiếu các quy định về lĩnh vực viễn thông quốc tế và tần số vô tuyến điện dẫn đến phải vận dụng các điều luật tương tự để xử lý do đó hiệu quả răn đe giáo dục còn hạn chế; (2) trình độ của cán bộ chiến sỹ an ninh trong việc phòng ngừa và trực tiếp đấu tranh với loại tội phạm này còn nhiều hạn chế; (3) công tác kiểm tra nghiệp vụ trước khi đưa vào sử dụng thiết bị công nghệ mới ít được hỗ trợ về kinh phí để thử nghiệm[16]. Trên cơ sở xác định những khó khăn, hạn chế trên, tác giả đưa ra một số giải pháp, gồm: (1) hoàn thiện pháp luật hình sự như bổ sung quy định tội danh thiết lập hệ thống viễn thông quốc tế trái phép; tội phạm hóa một số hành vi trong lĩnh vực máy tính, internet; tội phạm hóa một số hành vi trong lĩnh vực tần số vô tuyến điện; (2) hoàn thiện hệ thống pháp luật chuyên ngành có liên quan; (3) các giải pháp về mặt tổ chức; tăng cường đầu tư và phát triển khoa học công nghệ cho lực lượng an ninh[17].

Những khó khăn, vướng mắc trong việc áp dụng các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT để xử lý tội phạm này cũng được nhiều tác giả nghiên cứu. Vấn đề này có thể kể đến các bài viết như bài viết "*Viện kiểm sát nhân dân trước những khó khăn, thách thức của các tội phạm về công nghệ thông tin"* của tác giả Nguyễn Minh Đức đăng trên Tạp chí Kiểm sát số 19/2008; bài viết*"Về việc xác định tội danh đối với một số hành vi vi phạm trong lĩnh vực viễn thông"* của tác giả Mai Thế Bảy đăng trên Tạp chí Nhà nước và Pháp luật số 3/2002; bài viết *"Xác định tội trộm cắp tài sản đối với người lắp đặt thiết bị thu phát viễn thông để thu lợi bất chính là có căn cứ"* của tác giả Đỗ Văn Chỉnh đăng trên Tạp chí Tòa án nhân dân số 19/2004; bài viết *"Về định tội danh đối với hành vi làm, sử dụng thẻ tín dụng*

[16] Xem: Viện chiến lược và khoa học công an (2007), Tlđd, tr. 136 - 138.

[17] Xem: Viện chiến lược và khoa học công an (2007), Tlđd, tr. 184 - 193.

giả hay các loại thẻ khác để mua hàng hóa hoặc rút tiền tại các máy trả tiền tự động của các ngân hàng" của tác giả Lê Đăng Doanh đăng trên Tạp chí Tòa án nhân dân số 17/2006. Trong các bài viết này, các tác giả đã chỉ ra những khó khăn trong việc áp dụng quy định của BLHS để xét xử những hành vi phạm tội mới xuất hiện; khó khăn trong việc định tội đối với một số tội gây nhầm lẫn. Đồng thời, các tác giả cũng đề xuất nhưng phương án để giải quyết những khó khăn, vướng mắc trên.

Nguyên nhân của những khó khăn, vướng mắc trong thực tiễn áp dụng quy định của BLHS đã được nhiều tác giả nghiên cứu và chỉ ra. Trong đó có nguyên nhân từ quy định của pháp luật như BLHS chưa có quy định hoặc chưa có văn bản hướng dẫn của cơ quan có thẩm quyền. Một số bài viết về chủ đề này như bài viết "*Cần sớm có văn bản hướng dẫn thực hiện Luật sửa đổi, bổ sung một số điều của Bộ luật hình sự về các tội phạm trong lĩnh vực công nghệ thông tin"* của tác giả Nguyễn Văn Hoàn đăng trên Tạp chí kiểm sát, số 4/2010; bài viết "*Quy định của Bộ luật hình sự và các văn bản hướng dẫn thi hành Luật sửa đổi, bổ sung Luật hình sự 2009 về tội phạm trong lĩnh vực CNTT, MVT ở Việt Nam*" của tác giả Phạm Minh Tuyên đăng trên Tạp chí Kiểm sát, số 23/2013; bài viết *"Về tội sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị phần mềm có khả năng tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử theo BLHS năm 2015"* của tác giả Nguyễn Quý Khuyến đăng trên Tạp chí Toà án nhân dân, số 1/2018; bài viết "*Cần sớm có văn bản hướng dẫn thực hiện Luật sửa đổi, bổ sung một số điều của Bộ luật hình sự về các tội phạm trong lĩnh vực công nghệ thông tin"* của tác giả Nguyễn Văn Hoàn đăng trên Tạp chí kiểm sát, số 4/2010; bài viết*"Chưa có căn cứ để truy cứu trách nhiệm hình sự đối với hành vi lắp đặt, sử dụng thiết bị viễn thông trái phép"* của tác giả Lê Đăng Doanh đăng trên Tạp chí Tòa án nhân dân số 17/2004; bài viết*"Lắp đặt sử dụng thiết bị viễn thông để*

thu lợi cước phí điện thoại trái phép - có thể truy tố tội kinh doanh trái phép" của tác giả Trần Vũ Hải đăng trên Tạp chí Tòa án nhân dân số 22/2004; bài viết*"Về hành vi lắp đặt, sử dụng thiết bị viễn thông trái phép thu cước điện thoại - phạm tội gì?"* của tác giả Dương Tuyết Miên đăng trên Tạp chí Tòa án nhân dân số 17/2004; bài viết "*Cần tội phạm hoá các hành vi nguy hiểm liên quan đến máy tính"* của tác giả Bùi Văn Nhơn và Phạm Quang Beo đăng trên Tạp chí Dân chủ và Pháp luật, số 3/2005.

Theo các tác giả trên, mặc dù BLHS năm 1999 đã có quy định liên quan đến tội phạm mạng nhưng còn nhiều bất cập như nội dung các điều luật chưa cụ thể, khó áp dụng; các điều luật chưa bao quát hết các hành vi của tội phạm mạng có thể diễn ra; hệ thống chế tài chưa tương xứng với tính nguy hiểm cho xã hội của hành vi phạm tội trên mạng… do đó cần phải tội phạm hóa và cụ thể hóa các hành vi nguy hiểm liên quan đến máy tính[18]. Việc không có quy định đầy đủ cũng gây khó khăn cho việc xử lý những hành vi nguy hiểm cho xã hội phát sinh như hành vi "*lắp đặt, sử dụng thiết bị viễn thông trái phép thu cước điện thoại"*. Khi BLHS năm 1999 được sửa đổi năm 2009, các quy định của BLHS liên quan đến tội phạm này đã được sửa đổi, bổ sung để phù hợp hơn. Tuy nhiên, quy định mới ra đời nhưng đã có bất cập, khó áp dụng như các dấu hiệu định khung chưa rõ, một số khái niệm chưa được giải thích cần thiết phải có văn bản hướng dẫn thực hiện của cơ quan có thẩm quyền[19]. Tuy nhiên, có thể thấy những bài viết về tội phạm trong lĩnh vực CNTT, MVT theo quy định của BLHS năm 2015 còn ít, chưa phong phú, cần được tiếp tục nghiên cứu.

---

[18] Xem: Bùi Quang Nhơn & Phạm Quang Beo (2005), "Cần tội phạm hóa và cụ thể hóa các hành vi nguy hiểm liên quan đến máy tính", *Tạp chí Dân chủ & Pháp luật*, số 3/2005.

[19] Xem: Nguyễn Văn Hoàn (2010), "Cần sớm có văn bản hướng dẫn thực hiện luật sửa đổi, bổ sung một số điều của Bộ luật hình sự về các tội phạm trong lĩnh vực công nghệ thông tin", *Tạp chí Kiểm sát*, số 4 (tháng 2/2010), tr. 24.

1.2. Tình hình nghiên cứu ở nước ngoài

Theo tác giả Debra Littejohn Shinder, lịch sử của tội phạm mạng gắn liền với lịch sử ra đời của máy vi tính. Vào những năm 60 của thế kỷ XX, khi máy vi tính mới ra đời có kích thước và giá trị rất lớn, không ai có thể mua để sở hữu cá nhân. Do vậy, mọi người phải sử dụng máy vi tính chung. Điều đó làm cho dữ liệu và chương trình của máy tính dễ bị gây hại. Đối với kẻ phạm tội, đây là cơ hội để thực hiện hành vi phạm tội[20].

Kể từ khi tội phạm trong lĩnh vực CNTT, MVT mới xuất hiện, trong nghiên cứu đã có cuộc tranh luận gay gắt về chủ đề có nên coi tội phạm này là tội phạm mới hay không? Có cần quy định riêng trong LHS về tội phạm này hay không? Hai câu hỏi này có quan hệ chặt chẽ với nhau. Nếu cho rằng tội phạm trong lĩnh vực CNTT, MVT là tội phạm mới thì cần có quy định riêng trong LHS về tội phạm này. Ngược lại, nếu cho rằng tội phạm này không phải là tội phạm mới thì không cần có quy định riêng trong LHS. Trong các nghiên cứu về vấn đề này có thể xếp thành hai xu hướng sau:

Một là, đa số các tác giả từ trước đến nay đều cho rằng, tội phạm trong lĩnh vực CNTT, MVT là tội phạm mới. Do đó, các nghiên cứu thường xây dựng khái niệm cho tội phạm này[21]. Lý do tội phạm này được coi là tội phạm mới vì việc thực hiện loại tội phạm này luôn gắn với các thiết bị công nghệ cao, đòi hỏi người thực hiện phải có kiến thức về máy tính; việc điều tra, truy tố, xét xử cũng phải do người có kiến thức về máy tính thực hiện; người phạm tội thường không có mặt khi xảy ra thiệt hại; không có mối liên hệ trước giữa

---

[20] Xem: Debra Littejohn Shinder (2002), *Scene of the Cybercrime,* Syngress Publishing, Inc, tr. 51 - 89.

[21] Dẫn theo Chawki, M (2005), "*A Critical Look at the Regulation of Cybercrime"* The ICFAI Journal of Cyberlaw : <http://www.findarticles.com/p/articles/mi_m2194/is_8_70/ai_78413303>

người phạm tội và nạn nhân[22]. Do đây là tội phạm mới, có đặc điểm khác với những tội phạm truyền thống khác, nên LHS cần có quy định riêng về tội phạm này.

Hai là, ngược lại một số tác giả cho rằng tội phạm trong lĩnh vực CNTT, MVT không phải là tội phạm mới, nó vẫn là các tội phạm như đã có từ trước, chỉ khác nhau là cách thức, công cụ thực hiện mới (bằng CNTT, MVT) mà thôi. Do đó, tội phạm trong lĩnh vực CNTT, MVT chỉ là hình thức thể hiện mới của tội phạm đã có từ trước (tội phạm truyền thống). Ví dụ: hành vi sử dụng trái phép thông tin tài khoản ngân hàng của người khác để chiếm đoạt tài sản cũng là hành vi trong tội trộm cắp tài sản hoặc lừa đảo chiếm đoạt tài sản. Do vậy, không phải vì các tội này liên quan đến CNTT, MVT mà coi nó là tội phạm mới; hơn nữa trong các tội phạm truyền thống, công cụ phạm tội (như sử dụng công nghệ thông tin, mạng viễn thông) không phải là yếu tố bắt buộc trong cấu thành tội phạm. Tác phẩm thể hiện xu hướng này có thể kể đến là tác phẩm*"Cybercrime: An Introduction"* (Giới thiệu về tội phạm mạng) của tác giả Li, Xingan (Joensuu, Finland: LEX, 2005)[23].

Vấn đề khái niệm tội phạm trong lĩnh vực CNTT, MVT đã được nhiều tác giả quan tâm nghiên cứu. Theo tác giả Debra Littejohn Shinder, tội phạm mạng được rất nhiều người quan tâm, nhưng chưa có khái niệm chính thức về tội phạm này. Các quan điểm về tội này cũng không có sự thống nhất. Dưới góc độ nhận thức chung, có thể hiểu tội phạm mạng là tội phạm có liên quan đến máy tính và mạng máy tính ở những vai trò như công cụ phạm tội, mục tiêu tấn công của tội phạm hoặc phục vụ cho mục đích có liên quan đến tội phạm như lưu giữ thông tin mua bán ma túy trái phép[24]. Các tác giả Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus,

[22] Dẫn theo: Phạm Văn Lợi (2007), Tlđd, tr. 22.

[23] Xem: Phạm Văn Lợi (2007), Tlđd, tr. 21.

[24] Xem: Debra Littejohn Shinder (2002), Tlđd, tr.5 - 6.

Eva Ignatuschtschenko cũng cho rằng, trên phạm vi toàn cầu, chưa có sự thống nhất về khái niệm tội phạm mạng. Tội phạm này thường được gọi là "tội phạm mạng", "tội phạm máy tính", "tội phạm công nghệ cao", … Do đó, các tác giả không có ý định đưa ra một khái niệm chung về tội phạm mạng, mà sử dụng phương pháp liệt kê những hành vi phạm tội nào được coi là tội phạm mạng[25]. Theo đó, nhiều hành vi phạm tội khác nhau được coi là tội phạm mạng như: tội truy cập bất hợp pháp; tội truy cập trái phép, ngăn chặn, chặn bắt bất hợp pháp dữ liệu máy tính; tội gây rối dữ liệu; tội gây rối hệ thống; tội lạm dụng các thiết bị; tội xâm phạm bí mật đời tư; tội giả mạo liên quan đến máy tính; tội lừa đảo liên quan đến máy tính[26].

Ngoài ra, khái niệm tội phạm trong lĩnh vực CNTT, MVT còn được trình bày trong một số tác phẩm khác như: tác phẩm *"Understanding cybercrime: phenomena, challenges and legal response"* (Luận giải về tình hình, thách thức và biện pháp pháp lý đối với tội phạm mạng) của tác giả Marco Gercke (Tổ chức viễn thông quốc tế Liên hợp quốc (ITU) phát hành năm 2012); tác phẩm *"Handbook of Internet Crime"* (Sổ tay tội phạm mạng) của tác giả Yvonne Jewkes và Majid Yar (Nxb. Routledge, New York, 2011); tác phẩm*"Policing Cyber Crime"* (Chính sách về tội phạm mạng) của tác giả Petter Gottschalk; "*Handbook on Identity- Related Crime"* (Sổ tay về tội phạm liên quan đến thông tin danh tính cá nhân) {United National (UNODC) phát hành năm 2011}; bài viết "*A Critical Look at the Regulation of Cybercrime"* (Bình luận các quy định về tội phạm mạng) của tác giả Chawki,

[25] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko, (2013), *Comprehensive Study On Cybercrime*, United Nations (UNODC), tr. 11 - 12: https://www.unodc.org/...**crime**/...**2013**/**CYBERCRIME_STUDY** 210213.pdf

[26] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), Tlđd, tr. 77 - 81.

M, đăng trên tạp chí The ICFAI Journal of Cyberlaw (2005); bài viết *"An introduction to Cybercrime"* (Giới thiệu về tội phạm mạng) của tác giả Marco Gercke (Giáo sư Trường Đại học Cologne, Đức); bài viết *"Cybercrime theory and discerning if there is a crime: the case of digital piracy"* (Lý thuyết và nhận thức rõ về tội phạm mạng: trường hợp xâm phạm bản quyền kỹ thuật số) của tác giả Frances P Bernat và David Makin, đăng trên Tạp chí International Review of modern sociology, Volume 40, số 2/2014.

Có thể thấy rằng, mặc dù có sự thống nhất về nhận thức chung, nhưng khi xác định cụ thể phạm vi của tội phạm trong lĩnh vực CNTT, MVT lại chưa thống nhất. Có những quan điểm xác định phạm vi tội phạm này quá rộng. Ví dụ, Bộ tư pháp Hoa Kỳ cho rằng, tội phạm máy tính bao gồm *"mọi hành vi phạm tội có sử dụng kiến thức kỹ thuật máy tính để phạm tội, điều tra hoặc xét xử"*[27]. Với quan điểm như vậy, phạm vi tội phạm máy tính sẽ rất rộng.

Trước thực trạng chưa có sự thống nhất về phạm vi khái niệm tội phạm trong lĩnh vực CNTT, MVT nên các nghiên cứu thường chú trọng tới việc phân loại tội phạm này. Việc phân loại vừa có ý nghĩa lý luận để xác định phạm vi của tội phạm này; vừa có ý nghĩa thực tiễn khi đấu tranh, phòng chống tội phạm này. Tất nhiên, mỗi tác giả sẽ có cách phân loại khác nhau, dựa trên các tiêu chí phân loại khác nhau. Theo tác giả Debra Littejohn Shinder, dựa vào tính chất của hành vi có tính bạo lực đối với con người hay không, tội phạm mạng được chia làm 3 loại chính: (1) Các tội phạm xâm phạm hoặc đe dọa xâm phạm đến con người - con người vật lý (khủng bố qua mạng, tấn công đe dọa nạn nhân, theo dõi nạn nhân, khiêu dâm trẻ em); (2) Các tội phạm không bạo lực, xâm phạm thế giới ảo (xâm phạm mạng, lừa đảo qua mạng, trộm cắp qua mạng; phá hoại mạng máy tính, mạng viễn thông; các tội phạm khác); (3) Các tội phạm không bạo lực khác (quảng cáo trái phép

[27] Xem: Chawki, M (2005), Tlđd, tr. 9.

trên mạng, cờ bạc quan mạng, mua bán trái phép ma túy qua mạng, rửa tiền qua mạng, chuyển giao bất hợp pháp qua mạng)[28]. Còn theo tác giả Chawki, M. căn cứ hành vi và mục đích phạm tội, tội phạm trong lĩnh vực CNTT, MVT được chia thành 6 nhóm sau[29]: (1) Các tội phạm truy cập bất hợp pháp (hacking) vào máy tính, mạng máy tính để thu thập thông tin hoặc các mục đích khác; (2) Các tội phạm liên quan đến virus và mã độc như tội sản xuất, phân phối, tàng trữ, sở hữu trái phép virus; tội phát tán virus; hoặc sử dụng virus để thực hiện các tội khác như truy cập trái phép hoặc cản trở, phá hủy mạng máy tính, phương tiện điện tử…(3) Các tội phạm lừa đảo qua máy tính, mạng máy tính, mạng viễn thông: trong quá trình hoạt động của máy tính, tất cả các giai đoạn (nhập thông tin đầu vào, xử lý thông tin, xuất thông tin đầu ra hoặc trao đổi thông tin) đều có thể trở thành hoạt động phạm tội hoặc là mục đích của tội phạm của tội phạm trong lĩnh vực CNTT, MVT; (4) Các tội phạm có hành vi theo dõi, đe dọa, nói xấu cá nhân, tổ chức qua mạng; (5) Tội phạm khủng bố qua mạng; (6) Các tội phạm trộm cắp qua mạng.

Một trong những đặc trưng của tội phạm trong lĩnh vực CNTT, MVT là tính quốc tế và không bị giới hạn bởi không gian lãnh thổ. Việc thực hiện tội phạm thông qua mạng internet có thể gây thiệt hại cho nạn nhân ở quốc gia khác mà không cần trực tiếp có mặt ở đó. Người phạm tội có thể ẩn danh để che giấu tội phạm dễ dàng. Do đó, để đấu tranh hiệu quả với loại tội phạm này, đã có nhiều văn bản pháp luật quốc tế quy định ra đời quy định về tội phạm trong lĩnh vực CNTT, MVT[30]. Nội dung các văn bản này rất phong phú, đa dạng, nhưng chủ yếu tập trung vào 4 vấn đề chính là: (1) hình sự hóa các

[28] Xem: Debra Littejohn Shinder (2002), Tlđd, tr.19 - 33.

[29] Xem: Chawki, M (2005), Tlđd, tr. 18 - 28.

[30] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), Tlđd, tr. 268.

hành vi phạm tội trong lĩnh vực CNTT, MVT; (2) hợp tác quốc tế trong đấu tranh phòng chống tội phạm trong lĩnh vực CNTT, MVT; (3) xác định thẩm quyền xử lý tội phạm trong lĩnh vực CNTT, MVT; (4) thủ tục tố tụng trong xử lý tội phạm trong lĩnh vực CNTT, MVT như vấn đề chứng cứ điện tử. Để hiểu rõ những văn bản này, nhiều tác giả đã nghiên cứu làm rõ nội dung của các văn bản, đánh giá sự tương thích của các văn bản này với pháp luật hình sự của một số quốc gia. Trong số các công trình nghiên cứu đó, có một tác phẩm tiêu biểu là tác phẩm "*Comprehensive Study On Cybercrime"* (Nghiên cứu tổng quan về tội phạm mạng) của các tác giả Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko do United Nations (UNODC) dự thảo năm 2013. Tác phẩm này đã nghiên cứu một cách tổng thể, khái quát rất nhiều văn bản quốc tế về tội phạm trong lĩnh vực CNTT, MVT từ trước đến nay, đặc biệt tại chương 2 và chương 3 của cuốn sách. Trong chương 2 về tình hình tội phạm mạng toàn cầu, các tác giả không chỉ nêu lên tình hình tội phạm mà còn mô tả bức tranh về người phạm tội này. Trong chương 3, các tác giả làm rõ vai trò của pháp luật, trong đó có pháp luật quốc tế trong đấu tranh phòng chống tội phạm này. Nội dung quy định về hình sự hoá các hành vi phạm tội trong lĩnh vực CNTT, MVT đã được phân tích chi tiết cụ thể. Ngoài ra, tác phẩm còn có sự so sánh, đánh giá quy định của các văn bản quốc tế với nhau và so sánh đánh giá với kết quả khảo cứu về quy định luật hình sự của gần hơn 80 quốc gia trên thế giới.

Ngoài ra còn có một số tác phẩm khác cũng nghiên cứu về văn bản pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT như tác phẩm "*Understanding cybercrime: phenomena, challenges and legal response"* (Luận giải về tình hình, thách thức và biện pháp pháp lý đối với tội phạm mạng) của tác giả Marco Gercke (Tổ chức viễn thông quốc tế Liên hợp quốc (ITU), phát hành năm 2012); tác phẩm "*The History of Global Harmonization*

on Cybercrime Legislation - The Road to Geneva"(Lịch sử của hài hòa quốc tế trong lĩnh vực lập pháp đối với tội phạm mạng - Đường tới Geneva) của tác giả Stein Schjolberg (2008); tác phẩm *"Global Cybercrime: The Interplay of Politics and Law"* (Tội phạm mạng toàn cầu: Sự tương tác của chính sách và pháp luật) của tác giả Aaron Shul (2014); Tác phẩm*"The Emerging Consensus on Criminal Conduct in Cybercrime"* (Sự thống nhất nổi bật về hành vi phạm tội đối với loại tội phạm mạng) của các tác giả Marc D. Goodman và Susan W. Brenner; "*The Council of Erope Convention on Cybercrime"* (Công ước về tội phạm mạng của Hội đồng Châu Âu) của tác giả Mike Keyser, CNS Đại học luật Seattle, Mỹ…

2. Đánh giá tình hình nghiên cứu về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Thông qua việc nghiên cứu với số lượng đáng kể các công trình nghiên cứu trong và ngoài nước, tác giả luận án cho rằng có đủ căn cứ để đánh giá tình hình nghiên cứu về tội phạm trong lĩnh vực CNTT, MVT qua một số vấn đề sau:

Thứ nhất, nhận thức và lý luận về tội phạm trong lĩnh vực CNTT, MVT:

Các nghiên cứu từ trước đến nay ở cả trong nước và ngoài nước đều nghiên cứu về tội phạm trong lĩnh vực CNTT, MVT dưới góc độ là tội phạm mới, xuất hiện cùng với sự ra đời và phát triển của CNTT, MVT. Về nhận thức chung các nghiên cứu đều thống nhất rằng, tội phạm trong lĩnh vực CNTT, MVT là tội phạm có sự liên quan đến CNTT, MVT ở những vai trò là mục tiêu tấn công của tội phạm và công cụ để thực hiện tội phạm. Dưới góc độ nghiên cứu như vậy nên tội phạm trong lĩnh vực CNTT, MVT có phạm vi rộng và ngày càng mở rộng thêm. Với tốc độ phát triển và khả năng ứng dụng ngày càng rộng của CNTT, MVT trong đời sống như hiện nay, người phạm tội càng ngày càng có cơ hội sử dụng CNTT, MVT để thực hiện nhiều tội

phạm khác nhau. Tuy nhiên, phạm vi khái niệm tội phạm trong lĩnh vực CNTT, MVT còn nhiều quan điểm khác nhau. Điều đó cho thấy nhận thức cụ thể về tội phạm này chưa rõ ràng và thống nhất.

Bên cạnh đó, đặc điểm của tội phạm trong lĩnh vực CNTT, MVT cũng được các tác giả quan tâm nghiên cứu. Các tác giả đã chỉ ra một số đặc điểm khác biệt giữa tội phạm trong lĩnh vực CNTT, MVT với các tội phạm khác làm cơ sở cho việc khẳng định đây là tội phạm mới và LHS cần có quy định riêng về tội phạm này.

Do chưa thống nhất trong việc xác định phạm vi khái niệm tội phạm trong lĩnh vực CNTT, MVT nên việc phân loại, sắp xếp các hành vi phạm tội có đặc điểm giống nhau thành nhóm để dễ nhận biết và giải quyết được nhiều người quan tâm nghiên cứu. Tuy nhiên, tiêu chí để phân loại tội phạm này không có sự thống nhất, do đó có nhiều cách phân loại khác nhau.

Thứ hai, nghiên cứu quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT:

Từ khi BLHS năm 1999 quy định về tội phạm trong lĩnh vực CNTT, MVT, đã có một số nghiên cứu về nội dung này. Các nghiên cứu này đa số là các giáo trình, sách bình luận khoa học, các bài viết trên các tạp chí chuyên ngành. Nội dung của các nghiên cứu chủ yếu làm rõ nội dung, dấu hiệu pháp lý và hình phạt của từng điều luật. Có rất ít các nghiên cứu tổng thể, chuyên sâu về các quy định này. Hơn nữa, các nghiên cứu cho đến nay, đa số về các định của BLHS năm 1999, nghiên cứu các quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT còn ít, chưa phong phú.

Thứ ba, nghiên cứu pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT:

Xu hướng hợp tác quốc tế trong đấu tranh phòng chống tội phạm trong lĩnh vực CNTT, MVT đang rất được quan tâm, thể hiện ở chỗ có rất nhiều văn bản pháp luật quốc tế về vấn đề này. Việc nghiên cứu các văn bản pháp

luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT chưa được quan tâm nghiên cứu ở Việt Nam, nhưng ở nước ngoài có rất nhiều tác giả nghiên cứu. Các nghiên cứu đó đã làm rõ các nội dung các quy định của văn bản pháp luật quốc tế, nhất là nội dung về hình sự hoá các hành vi phạm tội trong lĩnh vực CNTT, MVT. Những nội dung trên sẽ được tiếp thu trong luận án để làm cơ sở cho việc nghiên cứu, so sánh, đánh giá với quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT.

Thứ tư, nghiên cứu về thực tiễn áp dụng và các giải pháp nâng cao hiệu quả áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT:

Thực tiễn áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT ở Việt Nam đã trải qua hơn 20 năm. Cho đến nay, có nhiều vấn đề đã được đặt ra để nghiên cứu giải quyết. Các nghiên cứu này đa số là các bài viết trên các tạp chí chuyên ngành. Các bài viết đã chỉ ra những khó khăn, vướng mắc trong thực tiễn áp dụng các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT; đồng thời đề xuất nhiều giải pháp để khắc phục những khó khăn, vướng mắc này. Tuy nhiên, các bài viết này chủ yếu viết về thực tiễn áp dụng quy định của BLHS năm 1999, nhiều nội dung đã cũ. Bởi vì BLHS năm 2015 đã được thi hành được 3 năm nên nghiên cứu về thực tiễn thi hành BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT còn ít. Do đó, cần nghiên cứu, tổng kết thực tiễn áp dụng quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT để có giải pháp nâng cao hơn nữa hiệu quả áp dụng các quy định này.

3. Những vấn đề Luận án tiếp tục nghiên cứu

Trên cơ sở tình hình nghiên cứu về tội phạm trong lĩnh vực CNTT, MVT và mục đích nghiên cứu của luận án, những vấn đề luận án tiếp tục nghiên cứu được thể hiện qua những nội dung sau:

Về tổng thể, Luận án sẽ nghiên cứu về lý luận và thực tiễn áp dụng các quy

định của LHS về tội phạm trong lĩnh vực CNTT, MVT, qua đó đề ra các giải pháp nâng cao hiệu quả áp dụng các quy định này trong thời gian tới. Cụ thể:

Thứ nhất, Luận án sẽ nghiên cứu để xây dựng và hoàn thiện về lý luận của tội phạm trong lĩnh vực CNTT, MVT. Hệ thống lý luận về tội phạm trong lĩnh vực CNTT, MVT được nghiên cứu trong Luận án này với tư cách là một nhóm tội cụ thể, được quy định trong BLHS xâm hại tới quan hệ xã hội đảm bảo an toàn thông tin dữ liệu, mạng máy tính, mạng viễn thông, phương tiện điện tử. Lý luận về tội phạm trong lĩnh vực CNTT, MVT trong Luận án có phạm vi hẹp hơn so với các nghiên cứu của các tác giả trước đây. Trong khi đó, phạm vi nghiên cứu về tội phạm trong lĩnh vực CNTT, MVT của các tác giả trước đây bao gồm tất cả những tội phạm có liên quan đến CNTT, MVT thuộc các lĩnh vực khác nhau như xâm phạm an ninh quốc gia, xâm phạm tính mạng, sức khoẻ, xâm phạm lĩnh vực kinh tế và các lĩnh vực khác.

Thứ hai, nghiên cứu các quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT từ trước đến nay một cách toàn diện, tổng thể, nhất là quy định của BLHS năm 2015; có đánh giá các quy định này với các quy định của pháp luật quốc tế và xu hướng chung của các nước thế giới hiện nay. Để đưa ra được giải pháp áp dụng hiệu quả quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT, cần có nghiên cứu xem các quy định này đã thực sự hợp lý, khoa học hay chưa. Các nghiên cứu hiện nay về vấn đề này đã có nhiều nhưng đa số đã cũ, các quy định của BLHS năm 2015 còn mới nên ít được nghiên cứu. Hơn nữa, ít có nghiên cứu so sánh, đánh giá quy định của BLHS Việt Nam với văn bản pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT.

Thứ ba, nghiên cứu thực tiễn áp dụng các quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT trên phạm vi cả nước trong những năm quan (2009 - 2020). Thông qua đó, đánh giá những kết quả đạt được, cũng như những khó khăn, vướng mắc trong thực tiễn áp dụng các quy định

này. Đồng thời nghiên cứu, xác định nguyên nhân của những khó khăn, vướng mắc đó.

Thứ tư, trên cơ sở kết quả nghiên cứu về lý luận, các quy định của LHS và thực tiễn áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong những năm qua, Luận án sẽ đề xuất một số giải pháp mang tính tổng thể, toàn diện để nâng cao hiệu quả áp dụng các quy định của LHS Việt Nam về tội phạm này trong thời gian tới.

Kết luận phần tổng quan về vấn đề nghiên cứu

Phần tổng quan về vấn đề nghiên cứu của Luận án đã phân tích, hệ thống hoá các công trình, bài viết được công bố từ trước đến nay ở trong nước và nước ngoài về tội phạm trong lĩnh vực CNTT, MVT. Các công trình, bài viết này có số lượng rất lớn và phong phú. Tội phạm trong lĩnh vực CNTT, MVT được nghiên cứu với nhiều nội dung khác nhau, bao gồm: các nghiên về lý luận của tội phạm trong lĩnh vực CNTT, MVT như khái niệm, đặc điểm, phân loại tội phạm; các nghiên cứu về quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT; các nghiên cứu về luật quốc tế quy định về tội phạm trong lĩnh vực CNTT, MVT; các nghiên cứu về thực tiễn áp dụng quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT trong những năm qua; cũng như những giải pháp nâng cao hiệu quả áp dụng các quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT.

Thông qua việc phân tích và hệ thống hoá các công trình nghiên cứu của các tác giả về tội phạm trong lĩnh vực CNTT, MVT từ trước đến nay, tác giả Luận án đã đưa ra những nhận xét, đánh giá về kết quả đạt được cũng như những tồn tại hạn chế cần tiếp tục nghiên cứu trong thời gian tới. Trên cơ sở đó, tác giả Luận án xác định những vấn đề cần nghiên cứu, giải quyết trong phần nội dung của Luận án. Theo đó, Luận án tiếp tục nghiên cứu giải quyết 4

vấn đề sau đây: (1) xây dựng và hoàn thiện hệ thống lý luận về tội phạm trong lĩnh vực CNTT, MVT; (2) phân tích, đánh giá và so sánh các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT; (3) nghiên cứu thực tiễn áp dụng các quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong những năm qua; (4) đề xuất những giải pháp để nâng cao hiệu quả áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong thời gian tới.

PHẦN KẾT QUẢ NGHIÊN CỨU

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

Để hiểu rõ khái niệm tội phạm trong lĩnh vực CNTT, MVT, trước tiên chúng ta cần làm rõ khái niệm môi trường không gian mạng. Theo tác giả Daniel T. Kuehl, trước đây con người chỉ có hai môi trường hoạt động với những đặc điểm vật lý khác nhau là đất liền và trên biển. Về sau, do sự phát triển của khoa học kỹ thuật, con người có thể hoạt động ở môi trường thứ ba là môi trường không gian quanh trái đất (aerospace). Khi con người bắt đầu chinh phục và tiến tới có thể hoạt động trong môi trường vũ trụ, con người có thêm môi trường thứ tư là môi trường không gian vũ trụ (outer space). Khi máy tính, mạng máy tính ra đời, chúng ta có thêm môi trường hoạt động thứ năm đó là môi trường không gian mạng (cyberspace)[31]. Khái niệm về môi trường không gian mạng hiện nay có nhiều quan điểm và tên gọi khác nhau. Có tác giả cho rằng, môi trường không gian ảo là "môi trường trong đó thông tin số hóa được truyền thông qua mạng máy tính"; có tác giả cho rằng không gian ảo là "môi trường có đặc trưng là việc sử dụng điện tử và phổ điện từ để lưu trữ, sửa đổi và trao đổi thông tin qua các hệ thống thông tin nối mạng và

[31] Xem: Daniel T. Kuehl (2009), *From Cyberspace to Cyberpower: Defining the Problem*, Washing, D.C. National Defense University Press, tr. 2.

cơ sở hạ tầng vật lý"; tác giả khác lại cho rằng đó là một mạng lưới phụ thuộc lẫn nhau của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng máy tính, mạng viễn thông, hệ thống máy tính và các bộ xử lý nhúng trong các ngành công nghiệp" hoặc đó là "môi trường giao tiếp điện tử"[32]. Các khái niệm trên đều định nghĩa về môi trường không gian mạng ở những lĩnh vực cụ thể khác nhau, chưa có tính khái quát. Ở Việt Nam, khái niệm môi trường không gian mạng được sử dụng bằng các thuật ngữ khác nhau như "môi trường mạng", "không gian mạng". Theo Luật công nghệ thông tin (2006), môi trường mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin. Trong đó, cơ sở hạ tầng thông tin là hệ thống trang thiết bị phục vụ cho việc sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số, bao gồm mạng viễn thông, mạng Internet, mạng máy tính và cơ sở dữ liệu[33]. Theo Luật an ninh mạng (2018), "không gian mạng" là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian[34].

Môi trường không gian mạng có những đặc điểm rất khác so với các môi trường vật lý còn lại. Chính những đặc điểm này quyết định đến đặc điểm của tội phạm trong lĩnh vực CNTT, MVT. Tác giả đồng ý với nhận xét của tác giả Whittle, B. David[35], theo đó môi trường không gian mạng có một số đặc điểm sau:

---

[32] Xem: Daniel T. Kuehl (2009), Tlđd, tr. 3.

[33] Xem: khoản 3,4 Điều 4 Luật công nghệ thông tin (2006).

[34] Xem: khoản 3 Điều 2 Luật an ninh mạng (2018).

[35] Xem: Whittle, B. David (1996), *Cyberspace: The Human Dimension*, W.H. Freeman Co., New York, tr. 7.

(1) Môi trường không gian mạng không phải là môi trường vật lý, nó giống như một trạng thái của ý nghĩ, một nơi nửa thực tế, nửa nhân tạo. Nó có thể được so sánh với trạng thái ảo tưởng khi con người ở trong đó và cảm nhận các giao tiếp bằng âm thanh hoặc hình ảnh như đọc, viết, quan sát, xem hình ảnh, nghe nhạc… Môi trường không gian mạng có được là do kết quả sáng tạo của con người, sự phát triển của lĩnh vực CNTT, MVT. Do đặc điểm này nên nhiều người còn gọi đây là môi trường ảo.

(2) Con người chỉ có thể thực hiện các hoạt động trong không gian mạng thông qua các công cụ, thiết bị truy cập vật lý với một quá trình xử lý nhân tạo (dữ liệu) của máy móc như máy điện toán số, phần mềm có khả năng kết hợp với các thiết bị khác bằng mạng kết nối vật lý. Nếu không có các thiết bị này con người không thể giao tiếp, tương tác với nhau trong môi trường không gian mạng được. Do đó, để hoạt động trong môi trường không gian mạng, con người cần phải sử dụng công cụ, phương tiện là CNTT, MVT.

(3) Môi trường không gian mạng có thể tương tác và kết nối giữa cá nhân, nhóm và sản phẩm sáng tạo của họ một cách rộng rãi, độc lập trong không gian và thời gian. Mặc dù là môi trường nhân tạo, có tính chất ảo nhưng những hoạt động của con người trong môi trường đó lại có tác động đến đời sống thực thông qua sự tương tác và kết nối giữa con người với nhau. Hơn nữa, sự tương tác của con người trong không gian mạng không bị giới hạn bởi khoảng cách không gian và thời gian như tương tác thông thường.

Từ những phân tích trên có thể rút ra khái niệm môi trường không gian mạng như sau:

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.

Như vậy, môi trường không gian mạng là môi trường được tạo ra trong lĩnh vực CNTT, MVT. Khái niệm CNTT được quy định trong Luật công nghệ thông tin (2006) là tập hợp các phương pháp khoa học, công nghệ và công cụ kỹ thuật hiện đại để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số; trong đó thông tin số là thông tin được tạo lập bằng phương pháp dùng tín hiệu số[36]. Trong Luật viễn thông (2009), khái niệm mạng viễn thông được hiểu 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"[37]. Trong đó, thiết bị viễn thông là thiết bị kỹ thuật, bao gồm phần cứng và phần mềm, được dùng để thực hiện viễn thông; đường truyền dẫn là tập hợp thiết bị viễn thông dùng để xác lập một phần hoặc toàn bộ đường truyền thông tin giữa hai điểm xác định; dịch vụ viễn thông là dịch vụ gửi, truyền, nhận và xử lý thông tin giữa hai hoặc một nhóm người sử dụng dịch vụ viễn thông, bao gồm dịch vụ cơ bản và dịch vụ giá trị gia tăng; dịch vụ ứng dụng viễn thông là dịch vụ sử dụng đường truyền dẫn viễn thông hoặc mạng viễn thông để cung cấp dịch vụ ứng dụng trong lĩnh vực công nghệ thông tin, phát thanh, truyền hình, thương mại, tài chính, ngân hàng, văn hóa, thông tin, y tế, giáo dục và lĩnh vực khác[38]. Lĩnh vực CNTT, MVT liên quan đến việc ứng dụng, phát triển CNTT, MVT. Việc ứng dụng và phát triển CNTT, MVT tạo ra môi trường không gian mạng. Cũng giống như các môi trường công cộng khác mà con người tham gia, môi trường không gian mạng cũng cần phải được đảm bảo an toàn và có trật tự.

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

[36] Xem: khoản 1, 2 Điều 4 Luật công nghệ thông tin (2006).

[37] Xem: khoản 10 Điều 3 Luật viễn thông (2009).

[38] Xem: khoản 2,7,8,9 Điều 3 Luật viễn thông (2009).

nên con người cũng có thể thực hiện hành vi phạm tội. Các hành vi phạm tội này 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 (thông qua các đối tượng cụ thể là mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử). Tội phạm này rất đa dạng nhưng đều có đặc điểm chung là có liên quan trực tiếp đến CNTT, MVT như được thực hiện trong môi trường không gian mạng, sử dụng CNTT, MVT để phạm tội, tấn công không gian mạng. Trong Luận án này, tội phạm trên được gọi là tội phạm liên quan đến CNTT, MVT. Trên thực tế hiện nay, tội phạm liên quan đến CNTT, MVT được các tác giả khác sử dụng bằng nhiều thuật ngữ khác nhau như tội phạm máy tính, tội phạm về vi tính, tội phạm mạng, tội phạm công nghệ thông tin, tội phạm công nghệ cao, tội phạm có sử dụng công nghệ cao.

Theo "Từ điển luật học" (2006) của Viện khoa học pháp lý, Bộ tư pháp, tội phạm vi tính là *"tội phạm xâm phạm trật tự an toàn xã hội được thực hiện trong lĩnh vực công nghệ thông tin, có hành vi khách quan liên quan đến sử dụng máy tính và các tính năng của nó gây rối loạn hoạt động, phong tỏa hoặc làm biến dạng, hủy hoại các dữ liệu hoặc đưa vào mạng những thông tin trái với quy định của pháp luật gây hậu quả nghiêm trọng"*[39]. Theo định nghĩa này, tội phạm vi tính có hai dấu hiệu: (1) máy tính và các tính năng của nó được sử dụng như là công cụ phạm tội; (2) tội phạm xâm phạm an toàn, trật tự trong không gian mạng bằng cách gây rối loạn hoạt động, phong tỏa hoặc làm biến dạng, hủy hoại các dữ liệu hoặc đưa vào mạng những thông tin trái với quy định của pháp luật. Tác giả M.E. Kabay cũng cho rằng, trong những năm đầu khi CNTT mới ra đời, tội phạm máy tính chủ yếu là các hành vi gây thiệt hại vật chất đối với hệ thống máy tính như sử dụng quyền truy cập

[39] Xem: Viện khoa học pháp lý (2006), *Từ điển luật học*, NXB. Từ điển bách khoa và NXB. Tư pháp, tr. 794 - 795.

để sửa đổi, hủy dữ liệu[40]. Theo tác giả Trần Cảnh Hưng, *"tội phạm máy tính là các hành vi tác động trực tiếp hoặc gián tiếp vào hoạt động của máy tính, mạng máy tính, các thiết bị ngoại vi, cơ sở dữ liệu, các quá trình điều khiển dựa trên sự hoạt động của các thiết bị tin học nhằm mục đích phá hoại, lừa đảo, che dấu, đánh cắp thông tin"*[41]. Tác giả Dương Tuyết Miên và Nguyễn Ngọc Khanh khi bàn về khái niệm "tội phạm máy tính" cho rằng, khái niệm này thường được nghiên cứu dưới hai góc độ, theo nghĩa rộng và theo nghĩa hẹp. Tội phạm vi tính theo nghĩa rộng bao gồm tất cả các tội phạm liên quan đến máy tính; còn theo nghĩa hẹp bao gồm các hành vi sao chép, lấy cắp, phá hủy, làm hư hỏng, thay đổi dữ liệu, cản trở, khai thác trái phép dịch vụ vi tính... Theo các tác giả, "*đa số các chuyên gia khi bàn về tội phạm vi tính thì chỉ đề cập tới tội phạm vi tính theo nghĩa hẹp*"[42]. Có thể thấy, khái niệm tội phạm máy tính trong quan điểm của các tác giả trên khá thống nhất và phổ biến trong bối cảnh CNTT, MVT mới ra đời và mới được ứng dụng trong đời sống xã hội. Tác giả Luận án cho rằng, những khái niệm trên đã phản ánh chính xác về bản chất của tội phạm này. Tuy nhiên về sau, trước sự phát triển không ngừng của lĩnh vực CNTT, MVT, người phạm tội không chỉ sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để gây thiệt hại cho môi trường không gian mạng, mà còn thực hiện nhiều loại tội phạm truyền thống khác. Do đó, phạm vi khái niệm tội phạm máy tính cần được mở rộng thêm.

---

[40] Xem: M.E.Kabay, "A Brief History of Computer Crime: An Introduction for Students", tr.4: http://www.mekabay.com/overviews/history.pdf (truy cập ngày 12/3/2018).

[41] Xem: Trần Cảnh Hưng (2003), "Một số vấn đề lý luận và thực tiễn về tội phạm máy tính", *Tạp chí Kiểm sát*, số 1/2003, tr.26.

[42] Xem: Dương Tuyết Miên, Nguyễn Ngọc Khanh (2000), "Tội phạm vi tính", *Tạp chí Tòa án nhân dân*, số 5/2000, tr.18.

Theo Từ điển "Black's Law Dictionary" (1996) của tác giả Bryan A. Garner chủ biên, tội phạm máy tính là "*tội phạm cần phải sử dụng kiến thức về kỹ thuật máy tính như phá hoại hoặc trộm cắp dữ liệu máy tính hoặc sử dụng máy tính để phạm các tội khác*"[43]. Còn tội trộm cắp qua mạng là "*hành vi sử dụng dịch vụ máy tính trực tuyến như mạng Internet để trộm cắp tài sản của người khác hoặc cản trở người khác sử dụng và hưởng lợi tài sản của mình*"[44]. Các định nghĩa này cho thấy quan niệm về "tội phạm máy tính" đã được mở rộng, không chỉ là những hành vi sử dụng "kiến thức về kỹ thuật máy tính" để tấn công không gian mạng như phá hoại, trộm cắp dữ liệu máy tính, mà còn sử dụng máy tính để thực hiện các tội phạm khác như trộm cắp tài sản qua mạng, cản trở người khác sử dụng tài sản của mình… Như vậy, khái niệm tội phạm máy tính là những tội phạm sử dụng máy tính và các tính năng của máy tính để gây thiệt hại cho môi trường không gian mạng hoặc để thực hiện những tội phạm khác trong môi trường không gian mạng.

Tác giả Debra Littejohn Shinder sử dụng khái niệm tội phạm mạng để chỉ những tội phạm liên quan đến CNTT, MVT. Theo tác giả, tội phạm mạng là tội phạm mà máy tính, mạng máy tính liên quan đến tội phạm ở 3 vai trò: (1) máy tính, mạng máy tính là mục tiêu tấn công của tội phạm khi tội phạm gây thiệt hại cho sự an toàn của máy tính, mạng máy tính (xâm hại tính bí mật, tính toàn vẹn và tính khả dụng); (2) máy tính, mạng máy tính là công cụ thực hiện các tội phạm "truyền thống" khác; (3) máy tính, mạng máy tính được dùng với mục đích phụ như lưu trữ số liệu về việc mua bán ma túy trái phép[45]. Trong khi đó, tác giả Chawki, M lại cho rằng tội phạm mạng là tội phạm có liên quan và có sự tham gia của máy tính với 4 vai trò: (1) máy tính

[43] Xem: Bryan A. Garner (1996), *Black's Law Dictionary*, West Publishing Co. tr.161-162.

[44] Xem: Bryan A. Garner (1996), Tlđd, tr.169.

[45] Xem: Debra Littejohn Shinder (2002), Tlđd, tr.5.

là mục tiêu của tội phạm khi tội phạm phá huỷ hoặc trộm cắp máy tính; (2) máy tính là chủ thể của tội phạm khi máy tính tạo ra môi trường để công nghệ kỹ thuật phạm tội; (3) máy tính là công cụ phạm tội; (4) máy tính là vật biểu tượng để dụ dỗ, lừa rối người khác[46]. Tuy sử dụng các thuật ngữ khác nhau như tội phạm CNTT, tội phạm tin học nhưng các tác giả khác như Phạm Văn Lợi, Nguyễn Mạnh Toàn, Đặng Trung Hà cũng thống nhất với quan điểm về khái niệm tội phạm mạng của tác giả Chawki, M [47]. Có thể thấy, dù phạm vi của khái niệm tội phạm mạng còn có sự khác nhau nhưng nội hàm khái niệm của tội phạm này khá thống nhất. Đó là tội phạm liên quan đến CNTT, MVT ở những vai trò khác nhau như: (1) CNTT, MVT được sử dụng như công cụ phạm tội; (2) CNTT, MVT (thông quan các đối tượng cụ thể là mạng máy tính, mạng viễn thông, phương tiện điện tử) là mục tiêu tấn công của tội phạm. Tác giả Luận án đồng ý với quan điểm cho rằng vai trò của CNTT, MVT là "vật biểu tượng để dụ dỗ, lừa rối người khác" thực chất cũng được sử dụng như công cụ để phạm tội[48]. Tác giả Luận án không đồng ý với quan điểm cho rằng, máy vi tính có thể được xem như chủ thể phạm tội. Quan điểm này không những được ít người ủng hộ mà còn trái với lý luận trong khoa học LHS Việt Nam. Theo đó chủ thể của tội phạm phải là con người hoặc pháp nhân. Luật an ninh mạng (2018) cũng sử dụng khái niệm tội phạm mạng. Theo đó, "*Tội phạm mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự*"[49]. Như vậy, khái niệm tội phạm mạng được sử dụng khá phổ

[46] Xem: Chawki, M (2005), Tlđd, tr. 8.

[47] Xem: Nguyễn Mạnh Toàn (2002), "Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học", *Tạp chí Nhà nước và Pháp luật*, số 3/2002, tr. 30

[48] Xem: Phạm Văn Lợi (2007), Tlđd, tr. 25.

[49] Xem: khoản 7 Điều 2 Luật an ninh mạng 2018

biến. Theo đó, tội phạm mạng là tội phạm có liên quan đến CNTT, MVT ở với vai trò là mục tiêu tấn công của tội phạm hoặc công cụ để thực hiện những tội phạm khác. Với quan điểm như vậy phạm vi của khái niệm tội phạm mạng sẽ rất rộng, bao gồm tội phạm ở nhiều lĩnh vực khác nhau.

Tác giả Trần Văn Hoà sử dụng khái niệm tội phạm có sử dụng công nghệ cao. Theo đó,*"tội phạm có sử dụng công nghệ cao là những hành vi vi phạm pháp luật hình sự, do người có năng lực trách nhiệm hình sự sử dụng thiết bị kỹ thuật số, mạng máy tính làm công cụ, tấn công trái pháp luật vào website, cơ sở dữ liệu, máy tính, mạng máy tính một cách cố ý hoặc vô ý, hoặc sử dụng thiết bị kỹ thuật số, mạng máy tính, để thực hiện các hành vi phạm tội khác, xâm phạm đến an ninh quốc gia, trật tự an toàn xã hội, gây nguy hiểm cho xã hội, quyền và lợi ích hợp pháp của tổ chức và của công dân"*[50]. Người phạm tội sử dụng CNTT, MVT như công cụ phạm tội để tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc để thực hiện các tội phạm khác. Khái niệm này dựa vào tiêu chí là công cụ mà người phạm tội sử dụng để thực hiện tội phạm là "công nghệ cao". Trong đó, sử dụng "công nghệ cao" được hiểu là sử dụng thiết bị kỹ thuật số, mạng máy tính. Như vậy, khái niệm tội phạm có sử dụng công nghệ cao cũng sẽ có phạm vi rất rộng giống như khái niệm tội phạm mạng. Hơn nữa, thuật ngữ "công nghệ cao" cũng là một thuật ngữ có phạm vi rộng, không chỉ trong lĩnh vực CNTT, MVT. Bởi vì theo Luật công nghệ cao (2008), *"Công nghệ cao là công nghệ có hàm lượng cao về nghiên cứu khoa học và phát triển công nghệ; được tích hợp từ thành tựu khoa học và công nghệ hiện đại; tạo ra sản phẩm có chất lượng, tính năng vượt trội, giá trị gia tăng cao, thân thiện với môi trường; có vai trò quan trọng đối với việc hình thành ngành sản xuất, dịch vụ mới hoặc*

[50] Xem: Trần Văn Hoà (2011), *An toàn thông tin và công tác phòng chống tội phạm sử dụng công nghệ cao*, NXB. Công an nhân dân, tr.20.

hiện đại hóa ngành sản xuất, dịch vụ hiện có"[51]. Như vậy, CNTT, MVT chỉ là một trong những lĩnh vực của công nghệ cao. Hiện nay, khái niệm tội phạm có sử dụng công nghệ cao được sử dụng khá phổ biến trong lực lượng công an và một số văn bản dưới luật. Theo Nghị định 25/2014/NĐ-CP ngày 07/4/2014 của Chính phủ quy định về phòng chống tội phạm và vi phạm khác có sử dụng công nghệ cao, *"Tội phạm có sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự có sử dụng công nghệ cao"*[52]. Tuy nhiên, tác giả Luận án thấy rằng, khái niệm "công nghệ cao" theo quy định của pháp luật hiện nay có phạm vi rộng hơn khái niệm "thiết bị kỹ thuật số, mạng máy tính" được sử dụng trong khái niệm trên. Do đó, việc sử dụng khái niệm tội phạm có sử dụng công nghệ cao để chỉ tội phạm liên quan đến CNTT, MVT là không phù hợp.

Trong khi khái niệm về tội phạm liên quan đến CNTT, MVT chưa có sự thống nhất thì pháp luật của các quốc gia trên thế giới và pháp luật quốc tế cũng ít có quy định về khái niệm này. Theo khảo sát của tác giả, hiện chỉ có một số ít văn bản pháp luật quốc tế quy định về khái niệm này như Thỏa thuận hợp tác xử lý tội phạm liên quan đến thông tin máy tính của Các nước độc lập trong Khối thịnh vượng (2001)[53] và Thỏa thuận hợp tác trong lĩnh vực an ninh thông tin quốc tế của Tổ chức hợp tác Thượng Hải (2010)[54]. Theo khoản a Điều 1 Thỏa thuận hợp tác xử lý tội phạm liên quan đến thông tin máy tính của Các nước độc lập trong Khối thịnh vượng (2001), "tội phạm liên

[51] Xem: khoản 1 Điều 3 Luật công nghệ cao 2008;

[52] Xem: khoản 1 Điều 3 Nghị định 25/2014/NĐ-CP ngày 07/4/2014 của Chính phủ quy định về phòng chống tội phạm và vi phạm khác có sử dụng công nghệ cao.

[53] Các nước tham gia gồm: Nga, Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyz, Moldova, Tajikistan, Turkmenistan, Uzbekistan, Ukraine.

[54] Các nước tham gia: Trung Quốc, Nga, Kazakhstan, Tajikistan, Uzbekistan và Kyrgyz.

quan đến thông tin máy tính" là hành vi phạm tội xâm hại đến thông tin máy tính. Trong đó, "thông tin máy tính" được hiểu là thông tin được lưu trữ trong bộ nhớ của máy tính, máy móc hoặc thiết bị lưu trữ khác được định dạng để máy tính có thể đọc được hoặc có thể truyền được qua các kênh viễn thông (khoản b Điều 1). Tại Phụ lục số 2 của Thỏa thuận giữa các quốc gia thành viên của Tổ chức hợp tác Thượng Hải trong lĩnh vực đảm bảo an ninh thông tin quốc tế (2010) có quy định về khái niệm "tội phạm thông tin" (Information crime)[55]. Theo đó, tội phạm thông tin là hành vi của cá nhân, tổ chức sử dụng bất hợp pháp nguồn thông tin hoặc can thiệp trái phép vào nguồn thông tin nhằm mục đích phạm tội. Đặc điểm của tội phạm thông tin là vi phạm hệ thống thông tin thông qua việc xâm hại tính nguyên vẹn, tính khả dụng và tính bảo mật của thông tin; cố ý sản xuất và phát tán vi - rút máy tính hoặc các chương trình mã độc khác; tấn công DoS (từ chối dịch vụ) và các ảnh hưởng tương tự; phá hủy nguồn thông tin; xâm phạm trái phép quyền và tự do của công dân trong lĩnh vực thông tin, bao gồm quyền sở hữu trí tuệ, thông tin cá nhân; sử dụng phương pháp và nguồn thông tin để phạm các tội phạm khác như lừa đảo, trộm cắp, tống tiền, buôn lậu, vận chuyển trái phép ma túy, phân phối tài liệu khiêu dâm trẻ em…

Tại cuộc họp lần thứ 10 của Đại hội đồng liên hợp quốc về ngăn chặn và xử lý tội phạm tổ chức tại thành phố Viên (Áo) từ ngày 10/10/2000 đến ngày 17/10/2000, các nước đã thảo luận và đi đến nhận thức chung về tội phạm này. Theo đó, tại điểm 9 mục III của văn bản hội nghị số A/CONF.187/10, đề cập đến khái niệm tội phạm mạng bao gồm tất cả những tội phạm: (1) được thực hiện bằng hệ thống máy tính hoặc hệ thống mạng; (2) được thực hiện trong môi trường mạng máy tính hoặc hệ thống mạng; (3) tấn

[55] Nguồn: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

công hệ thống máy tính hoặc hệ thống mạng[56]. Theo điểm 14 mục III của văn bản này, tội phạm mạng được chia làm 2 loại: *thứ nhất,* tội phạm mạng theo nghĩa hẹp (tội phạm máy tính) bao gồm tất cả những hành vi trực tiếp sử dụng phương tiện kỹ thuật điện tử để phạm tội nhằm xâm hại an ninh mạng máy tính và quá trình lưu giữ, xử lý dữ liệu máy tính; *thứ hai*, tội phạm mạng theo nghĩa rộng (tội phạm liên quan đến máy tính) là những hành vi bất hợp pháp được thực hiện bằng hệ thống máy tính, mạng máy tính hoặc có liên quan đến hệ thống máy tính, mạng máy tính, bao gồm cả những tội phạm như chiếm hữu, tặng cho hoặc phân phối bất hợp pháp thông tin bằng hệ thống máy tính, mạng máy tính.

Thông qua việc phân tích các khái niệm trên cho thấy, khái niệm tội phạm liên quan đến CNTT, MVT hiên nay chưa có sự thống nhất về phạm vi và thuật ngữ. Tuỳ theo góc độ và mục đích nghiên cứu của mình, mỗi tác giả lại đưa ra khái niệm và thuật ngữ khác nhau. Tuy nhiên, cho dù ở phạm vi rộng hay hẹp và sử dụng thuật ngữ nào, khái niệm về tội phạm liên quan đến CNTT, MVT mà các tác giả sử dụng đều có một số đặc điểm chung như sau:

Thứ nhất, đó là tội phạm mới so với tội phạm truyền thống, bởi vì nó được thực hiện trong môi trường không gian mạng và người phạm tội sử dụng CNTT, MVT để thực hiện tội phạm. Điều đó làm cho tội phạm liên quan đến CNTT, MVT khác cơ bản so với các tội phạm truyền thống.

Thứ hai, 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, phương tiện để thực hiện tội phạm khác.

---

[56] Xem: Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders:https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017 ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf (truy cập ngày 2/3/2020).

Thứ ba, tội phạm liên quan đến CNTT, MVT có phạm vi rộng. Người phạm tội có thể sử dụng CNTT, MVT để thực hiện nhiều tội phạm truyền thống khác như các tội xâm phạm an ninh quốc gia, các tội xâm phạm tính mạng, sức khoẻ, nhân phẩm danh dự con người, các tội xâm phạm sở hữu trí tuệ, các tội xâm phạm trật tự quản lý kinh tế, các tội xâm phạm an toàn công cộng, trật tự công cộng. Phạm vi này sẽ ngày càng mở rộng theo sự phát triển và ứng dụng rộng rãi của CNTT, MVT trong các lĩnh vực của đời sống xã hội. Do đó, tội phạm liên quan đến CNTT, MVT có thể được quy định ở nhiều chương khác nhau trong BLHS.

Từ những phân tích trên có thể rút ra khái niệm tội phạm liên quan đến CNTT, MVT như sau:

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.

Khái niệm tội phạm trong lĩnh vực CNTT, MVT được sử dụng trong luận án này có phạm vi hẹp hơn khái niệm tội phạm liên quan đến CNTT, MVT. Theo đó, tội phạm trong lĩnh vực CNTT, MVT chỉ là một bộ phận của tội phạm liên quan đến CNTT, MVT. Với tư cách là một nhóm tội riêng được quy định trong BLHS, tội phạm trong lĩnh vực CNTT, MVT bao gồm những tội phạm có mối quan hệ gắn bó, chặt chẽ với nhau. Theo lý luận của khoa học LHS hiện nay, các tội phạm trong cùng một nhóm có quan hệ với nhau thông qua khách thể chung của nhóm tội đó. Các tội phạm này cùng xâm hại đến các quan hệ xã hội có cùng tính chất (cùng loại) được LHS bảo vệ. Tội phạm trong lĩnh vực CNTT, MVT bao gồm các tội phạm cùng xâm phạm tới một nhóm quan hệ xã hội cùng loại được LHS bảo vệ. Đó là nhóm quan hệ xã hội đảm bảo sự an toàn của không gian mạng. Cụ thể là quan hệ xã hội đảm bảo sự an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ

liệu điện tử. Tội phạm trong lĩnh vực CNTT, MVT là một nhóm nhỏ nằm trong tội phạm liên quan đến CNTT, MVT, bao gồm các tội phạm xâm hại đến sự an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. Với sự phát triển và ứng dụng của CNTT, MVT hiện nay trong xã hội, người phạm tội có thể sử dụng CNTT, MVT để thực hiện nhiều loại tội phạm khác nhau. Tuy nhiên, không phải tất cả những tội phạm đó đều là tội phạm trong lĩnh vực CNTT, MVT. Chỉ những tội phạm 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 mới là tội phạm trong lĩnh vực CNTT, MVT. 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. Ví dụ: hành vi sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để khủng bố hoặc khủng bố nhằm chống chính quyền nhân dân; hành vi sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để đánh bạc không phải là tội phạm trong lĩnh vực CNTT, MVT mà thuộc về các nhóm tội phạm tương ứng là tội xâm phạm an toàn công cộng, tội xâm phạm an ninh quốc gia hay tội xâm phạm trật tự công cộng khác. Như vậy một số tội phạm được quy định trong BLHS năm 2015 tuy có sử dụng CNTT, MVT để phạm tội nhưng không được coi là tội phạm trong lĩnh vực CNTT, MVT bao gồm các tội phạm quy định tại điểm d khoản 2 Điều 113 Tội khủng bố nhằm chống chính quyền nhân dân), điểm e khoản 2 Điều 155 (Tội làm nhục người khác), điểm e khoản 2 Điều 156 (Tội vu khống), điểm d khoản 2 Điều 299 (Tội khủng bố), điểm c khoản 2 Điều 321 (Tội đánh bạc), điểm g khoản 2 Điều 326 (Tội truyền bá văn hóa phẩm đồi trụy).

Trên cơ sở phân tích trên, 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

Trên cơ sở khái niệm tội phạm trong lĩnh vực CNTT, MVT, chúng ta có thể rút ra một số đặc điểm của tội phạm này như sau:

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

Tội phạm trong lĩnh vực CNTT, MVT được thực hiện trong môi trường không gian mạng. Trong môi trường đó, con người chỉ có thể thực hiện các hành vi của mình thông qua các công cụ, biện pháp kỹ thuật là mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. Do đó để thực hiện tội phạm này, người phạm tội buộc phải sử dụng CNTT, MVT làm công cụ, phương tiện phạm tội. Do đó, theo quy định của BLHS Việt nam dấu hiệu sử dụng CNTT, MVT làm công cụ, phương tiện thực hiện tội phạm là dấu hiệu bắt buộc của tội phạm trong lĩnh vực CNTT, MVT. Đây cũng là dấu hiệu để phân biệt giữa tội phạm trong lĩnh vực CNTT, MVT với các tội phạm truyền thống khác. Chẳng hạn, cùng là hành vi lén lút chiếm đoạt tài sản, nhưng nếu sử dụng mạng máy tính, mạng viễn thông hoặc phương tiện điện tử sẽ bị coi là tội phạm trong lĩnh vực CNTT, MVT (Điều 290 BLHS năm 2015 Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản). Ngược lại nếu lén lút chiếm đoạt tài sản có giá trị từ 2 triệu trở lên mà không sử dụng mạng máy tính, mạng viễn thông hoặc phương tiện điện tử thì bị coi là tội phạm trộm cắp tài sản (Điều 173 BLHS năm 2015).

Đặc điểm 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:

Tội phạm trong lĩnh vực CNTT, MVT được thực hiện trong môi trường không gian mạng nên bằng mắt thường không thể nhìn thấy. Phải thông qua các phương tiện, thiết bị kỹ thuật phù hợp chúng ta mới có thể phát hiện ra hành vi phạm tội này. Với sự phát triển không ngừng của lĩnh vực CNTT, MVT, người phạm tội ngày càng có nhiều cơ hội lợi dụng CNTT, MVT để thực hiện tội phạm. Hành vi phạm tội ngày càng trở nên tinh vi, phức tạp, khó phát hiện. Dựa trên lý luận và thực tiễn có thể thấy hành vi khách quan của tội phạm trong lĩnh vực CNTT, MVT thường là các hành vi sau đây:

(1) *Truy cập bất hợp pháp vào hệ thống máy vi tính hoặc cơ sở dữ liệu:*

Truy cập bất hợp pháp vào hệ thống máy vi tính hoặc cơ sở dữ liệu là hành vi cố ý truy cập trái phép vào một phần hoặc toàn bộ hệ thống máy vi tính hoặc cơ sở dữ liệu. Hành vi này xâm phạm đến tính toàn vẹn, tính bí mật của hệ thống máy vi tính hoặc cơ sở dữ liệu. Truy cập bất hợp pháp cũng là dấu hiệu của nhiều tội khác như xâm nhập bất hợp pháp để trộm cắp thông tin; xâm nhập bất hợp pháp để chiếm đoạt tài sản. Do đó, tuỳ theo mục đích truy cập khác nhau mà sẽ cấu thành các tội khác nhau. Trong trường hợp này, việc truy cập vào hệ thống máy tính hoặc cơ sở dữ liệu không nhằm mục đích chiếm đoạt tài sản.

Đối tượng của hành vi truy cập bất hợp pháp là hệ thống máy tính hoặc dữ liệu điện tử. Đa số các quốc gia quy định hành vi truy cập bất hợp pháp vào hệ thống máy vi tính nói chung, chưa cần phải vào được tệp dữ liệu[57]. Chỉ rất ít nước quy định phải truy cập trái phép vào tệp dữ liệu, có nước còn giới

[57] Xem: Điều 2 Công ước Budapest 2001 và Điều 5 Luật mẫu 2002.

hạn hẹp hơn đối với hành vi này khi quy định là tội phạm đối với những hành vi truy cập trái phép vào "những thông tin được pháp luật bảo vệ"[58].

Về các thủ đoạn truy cập trái phép, hiện có hai quan điểm khác nhau. Đa số quan điểm cho rằng chỉ cần có hành vi cố ý truy cập trái phép vào hệ thống máy vi tính sẽ bị coi là tội phạm. Quan điểm khác cho rằng cần có thêm điều kiện như vượt qua tường lửa hoặc các biện pháp an ninh bảo vệ hệ thống máy tính hoặc cơ sở dữ liệu hoặc các ý định không trung thực như phá hủy, khóa, thay đổi hoặc sao chép thông tin hoặc phá hủy chức năng của máy vi tính, hệ thống máy tính hoặc mạng[59]. Điều này nhằm mục đích hạn chế xử lý hình sự những vi phạm nhỏ nhặt không cần thiết[60]. Như vậy, tuỳ theo mục đích mở rộng hay thu hẹp phạm vi xử lý hành vi này mà các quốc gia có sự lựa chọn khác nhau về những phương án trên.

(2) Duy trì sử dụng trái phép hệ thống máy tính:

Duy trì sử dụng trái phép hệ thống máy tính là hành vi tiếp tục sử dụng trái phép hệ thống máy tính, sau khi đã hết quyền sử dụng hệ thống máy tính đó. Hành vi này là một dạng của hành vi truy cập trái phép hệ thống máy tính, nhưng cũng có thể tách ra độc lập so với hành vi truy cập trái phép hệ thống máy tính. Một số văn bản quốc tế quy định cho phép các quốc gia không xử lý hình sự đối với hành vi này hoặc chỉ xử lý hình sự khi có yếu tố gian dối[61].

---

[58] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), Tlđd, tr. 82 – 83.

[59] Xem: Điều 2 Công ước Budapest 2001

[60] Xem: EU Decision on Attacks against Information Systems, Art.2.

[61] Xem: ECOWASDraft Directive, Art.5: https://ccdcoe.org/sites/default/files/documents/ECOWAS-110819 FightingCybercrime.pdf; và ITU/CARICOM/CTU Model Legilative Texts, Art.5: https://www.itu.int/ITUD/ rojects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-BModel-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf (truy cập ngày 8/4/2018).

(3) Truy cập, chặn bắt hoặc thu thập bất hợp pháp dữ liệu điện tử:

Đây là hành vi trộm cắp dữ liệu điện tử bằng các thủ đoạn truy cập, chặn bắt (trong quá trình truyền tải dữ liệu) hoặc thu thập (ví dụ sao chép) bất hợp pháp dữ liệu điện tử. Hành vi phạm tội xâm phạm tính bí mật của dữ liệu điện tử. Để có được dữ liệu điện tử một cách bất hợp pháp, người phạm tội có thể thực hiện các thủ đoạn như: (1) truy cập bất hợp pháp vào hệ thống máy tính hoặc cơ sở dữ liệu, sau đó sao chép dữ liệu điện tử; (2) chặn bắt dữ liệu điện tử trên mạng khi dữ liệu này đang trong quá trình truyền tải, ví dụ nghe lén thông tin; (3) các thủ đoạn thu thập bất hợp pháp dữ liệu điện tử, ví dụ nhân viên làm việc trong công ty đã sao chép bất hợp pháp tệp dữ liệu của công ty làm của riêng.

Đối tượng của hành vi phạm tội là dữ liệu điện tử. Dữ liệu điện tử là dữ liệu máy tính hoặc thông tin điện tử nói chung bao gồm cả thông tin liên lạc viễn thông và các bức xạ điện từ (ví dụ sóng vô tuyến). Về tính chất của dữ liệu điện tử, có 2 quan điểm khác nhau. Có quan điểm cho rằng chỉ những dữ liệu điện tử áp dụng biện pháp bảo vệ nhất định mới là đối tượng bảo vệ của tội phạm này. Do đó, người phạm tội phải có thủ đoạn để vượt qua các biện pháp an ninh bảo vệ dữ liệu điện tử như vượt qua tường lửa, bẻ khóa, chiếm quyền điều khiển. Hiện nay quan điểm này được thừa nhận phổ biến[62]. Quan điểm khác lại cho rằng đối tượng xâm hại của hành vi phạm tội này là dữ liệu điện tử nói chung, bao gồm cả dữ liệu được bảo vệ bằng các biện pháp an ninh và dữ liệu điện tử ở các mạng công cộng[63].

Công cụ thực hiện tội phạm là CNTT, MVT. Người phạm tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện hành vi

---

[62] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), Tlđd, tr. 86.

[63] Xem: The League Arab States Model Law, Art 8: http://itlaw.wikia.com/wiki/ Arab Convention on_Combating_Information_Technology_Offences .

truy cập, chặn bắt hoặc thu thập bất hợp pháp dữ liệu điện tử. Dữ liệu điện tử được tạo ra, được truyền đi hoặc lưu giữ trong môi trường không gian mạng, nếu không có các công cụ mang tính kỹ thuật con người không thể can thiệp vào môi trường này được. Do đó, việc sử dụng CNTT, MVT làm công cụ phạm tội là dấu hiệu bắt buộc của tội phạm này.

(4) Can thiệp trái phép vào dữ liệu máy tính hoặc hệ thống máy tính:

Bao gồm các hành vi cản trở chức năng của hệ thống máy tính, cũng như các hành vi hủy hoại, xóa, làm hư hỏng, thay thế hoặc vô hiệu hóa dữ liệu máy tính một cách trái phép. Hành vi này xâm phạm tính toàn vẹn, tính khả dụng của dữ liệu máy tính và sự hoạt động bình thường của chương trình máy tính hay hệ thống máy tính. Ví dụ, hành vi tấn công từ chối dịch vụ làm sập trang web hoặc xóa bỏ một số chương trình máy tính cần thiết để kết nối internet làm cho máy tính không thể vào mạng được hoặc ghi những thay đổi bất hợp pháp vào cơ sở dữ liệu máy tính làm cơ sở dữ liệu đó không còn chính xác nữa.

Do đặc tính tự nhiên của dữ liệu máy tính là vô hình nên một số quan điểm cho rằng hành vi này phải thực hiện bằng các biện pháp kỹ thuật, công nghệ, còn việc phá hủy tài sản (phần cứng) để phá hủy dữ liệu máy tính không phải là hành vi phạm tội này. Ví dụ: đốt phá trạm máy chủ để hủy dữ liệu không phải là hành vi phạm tội này. Do vậy, chỉ coi là tội phạm này nếu tấn công vào cơ sở dữ liệu (phần mềm). Trong khi đó, quan điểm khác lại cho rằng hành vi này bao gồm cả hành vi phá hủy phần cứng dẫn đến phá hủy dữ liệu bên trong. Quan điểm này thể hiện trong Điều 7 Luật mẫu 2002. Tác giả Luận án cho rằng quan điểm thứ nhất hợp lý hơn. Bởi vì tội phạm trong lĩnh vực CNTT, MVT được thực hiện trong môi trường không gian mạng, nên phải sử dụng các công cụ, thiết bị kỹ thuật như mạng máy tính, mạng viễn thông, phương tiện điện tử mới có thể thực hiện được. Việc phá huỷ trực tiếp

các thiết bị phần cứng sẽ bị xử lý theo tội huỷ hoại tài sản thuộc nhóm tội xâm phạm sở hữu hoặc tội xâm phạm an toàn công cộng.

(5) Lạm dụng trong việc sản xuất, phân phối hoặc sở hữu các công cụ, phương tiện, phần mềm máy tính:

Nhóm này bao gồm các hành vi phát triển hoặc phân phối trái phép các giải pháp phần cứng hoặc phần mềm được sử dụng để thực hiện tội phạm máy tính hoặc tội phạm có liên quan đến mạng máy tính. Ví dụ: hành vi tạo ra vi - rút trái phép để tấn công mạng máy tính. Các công cụ phạm tội được sử dụng trong môi trường kỹ thuật số như các mã độc, mật khẩu của nạn nhân, mã truy cập… trở thành các món hàng trên thị trường kinh doanh trái phép. Từ đó, người phạm tội dễ dàng có được công cụ để phạm tội. Do đó, cần xử lý hình sự đối với hành vi phạm tội này.

Hành vi khách quan của tội phạm này bao gồm: sản xuất, bán, nhập khẩu, sở hữu, phân phối, phổ biến, đề nghị sử dụng, chuyển giao cho người khác, tạo mẫu trái phép các công cụ máy tính để sử dụng cho mục đích phạm tội hay các hành vi trái pháp luật khác. Ngoài ra, hành vi công khai trái phép mật khẩu hoặc mã truy cập cũng có thể được coi là hành vi phạm tội của tội này.

Đối tượng tác động của tội phạm này bao gồm: (1) các phần mềm và các thiết bị, dụng cụ (bao gồm cả phần cứng và phần mềm); (2) các mật khẩu hoặc mã truy cập vào hệ thống máy tính và dữ liệu điện tử. Ngoài ra, các bài viết hướng dẫn lừa đảo máy tính (articles) cũng có thể trở thành đối tượng tác động của tội phạm này[64]. Các đối tượng trên có thể được sản xuất hoặc cải tiến để có tính năng cơ bản là tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử.

[64] Xem: EU Framework Decision 2001/413/JAI of 28 May 2001 (EU Decision on Fraud and Counterfeiting), Art.4: https://publications.europa.eu/en/publication-detail//publication /ea12bd64-beba-43e0-8eaf-e070480dc5c7/language-en (truy cập ngày 08/4/2019).

Mục đích của các hành vi sản xuất, bán, nhập khẩu, phân phối các đối tượng trên là để thực hiện tội phạm liên quan đến CNTT, MVT. Trường hợp các sản phẩm trên được sử dụng với mục đích hợp pháp như để nghiên cứu, học tập hoặc đảm bảo an ninh không bị coi là tội phạm này. Hiện nay đa số các văn bản pháp luật quốc tế đều quy định mục đích của hành vi sản xuất, bán, nhập khẩu, phân phối các đối tượng trên là để thực hiện tội phạm liên quan đến CNTT, MVT, chứ không phải là mục đích trái pháp luật nói chung[65]. Theo tác giả Luận án, đây là quan điểm hợp lý, góp phần hạn chế việc xử lý hình sự quá rộng đối với những hành vi trên.

(6) Các hành vi lừa đảo hoặc giả mạo liên quan đến máy vi tính:

Nhóm này gồm 2 hành vi:

Thứ nhất, hành vi lừa đảo liên quan đến máy tính là hành vi can thiệp (đưa vào, thay đổi, xóa hoặc nén dữ liệu điện tử), truy cập trái phép vào hệ thống máy tính hoặc dữ liệu điện tử với ý định gian dối hoặc không trung thực nhằm thu lợi, quyền lợi kinh tế bất hợp pháp cho mình hoặc cho người khác. Ví dụ: hành vi thay đổi phần mềm mà ngân hàng sử dụng để chuyển tiền của ngân hàng sang tài khoản cá nhân của mình.

Thứ hai, hành vi giả mạo liên quan đến máy tính là hành vi tạo ra dữ liệu điện tử giả (đưa vào, thay đổi, xóa, nén dữ liệu điện tử làm cho dữ liệu đó không chính xác và dùng nó với ý thức như là dữ liệu thật) hoặc dùng công nghệ thông tin, mạng viễn thông tạo ra giấy tờ, tài liệu giả (làm giấy tờ giả) để sử dụng cho các mục đích bất hợp pháp. Ví dụ, hành vi thay đổi thư điện tử của ngân hàng (thành thư điện tử giả) nhằm mục đích lừa đảo khách hàng. Người phạm tội cũng có thể gửi nhiều tin nhắn tới khách hàng để thu thập thông tin cá nhân hoặc lừa đảo.

---

[65] Xem: Điều 6 Công ước Budapest 2001 và Điều 9 Luật mẫu 2002.

Đối với hành vi giả mạo liên quan đến máy tính, dữ liệu giả mạo phải là các dữ liệu có ý nghĩa ràng buộc trách nhiệm pháp lý của nạn nhân. Ví dụ, hóa đơn thanh toán hoặc hợp đồng giả. Tuy nhiên, cũng có quan điểm cho rằng chỉ cần người phạm tội sử dụng tài liệu giả mạo có ý thức tạo ra trách nhiệm pháp lý cho nạn nhân, không yêu cầu trên thực tế có thực sự ràng buộc trách nhiệm pháp lý hay không.

(7) Xâm phạm thông tin cá nhân hoặc dữ liệu điện tử được bảo vệ:

Đó là các hành vi sử dụng hệ thống máy tính để chiếm đoạt, phổ biến, thu thập hoặc truy cập vào dữ liệu thông tin cá nhân hoặc vi phạm quy định về bảo vệ dữ liệu một cách bất hợp pháp. Hành vi phạm tội xâm hại tính bí mật của thông tin cá nhân, dữ liệu điện tử được bảo vệ. Thông tin cá nhân có thể là các bí mật cá nhân, các thông tin về ngày tháng năm sinh, số chứng minh thư, số điện thoại cá nhân, địa chỉ nhà … Ví dụ: một người sử dụng máy tính truy cập vào cơ sở dữ liệu thương mại điện tử sau đó công khai thông tin cá nhân của khách hàng mà đáng lẽ ra anh ta phải dữ bí mật.

(8). Hành vi phạm tội liên quan đến danh tính của cá nhân:

Bao gồm các hành vi chuyển dịch, chiếm đoạt hoặc sử dụng trái phép các thông tin nhận dạng cá nhân của người khác lưu trữ trong dữ liệu máy tính, với mục đích giúp sức hoặc thực hiện bất cứ hành vi phạm tội nào. Ví dụ: người phạm tội đã thu thập bất hợp pháp thông tin về giấy phép lái xe của người khác từ một hệ thống máy tính, sau đó bán hoặc dùng thông tin đó để che dấu thông tin trên giấy phép lái xe thật sự của họ để phạm một tội khác. Hành vi này còn được gọi là hành vi trộm cắp thông tin nhận dạng và dữ liệu cá nhân thông qua hệ thống máy tính. Đa số quan điểm cho rằng mục đích sử dụng các thông tin trên là để phạm một tội khác. Tuy nhiên, cũng có quan điểm cho rằng mục đích sử dụng thông tin này là để thực hiện mọi hành vi trái

pháp luật nói chung, ví dụ bán trái phép các thông tin đó[66].

Đối tượng tác động của tội phạm là các thông tin nhận dạng cá nhân trên các công cụ nhận dạng hoặc dữ liệu cá nhân như giấy phép láy xe, giấy chứng minh thư, thẻ hội viên, thẻ rút tiền, số tài khoản ngân hàng, hộ chiếu… như tên thật, địa chỉ nhà riêng, số chứng minh thư nhân dân, ngày sinh, thông tin tài chính, địa chỉ thư điện tử, số điện thoại cá nhân, tài khoản dùng internet, mật khẩu hoặc địa chỉ IP… Để hạn chế phạm vi xử lý hình sự đối với hành vi này, một số quan điểm trong đó có cả quan điểm của tác giả Luận án cho rằng chỉ những thông tin cá nhân trên một số công cụ nhận dạng cá nhân nhất định mới là đối tượng tác động của tội này. Ví dụ: giấy phép lái xe, giấy chứng minh thư nhân dân…

Thủ đoạn thực hiện để thu thập bất hợp pháp thông tin của cá nhân có thể thông qua việc truy cập trái phép vào hệ thống máy tính như sử dụng mã độc hoặc qua việc gửi tín lừa đảo hoặc duy trì sử dụng bất hợp pháp dữ liệu máy tính.

Đặc điểm thứ ba, hậu quả của tội phạm trong lĩnh vực CNTT, MVT thường rất nghiêm trọng nhưng lại dễ che giấu, khó phát hiện ra:

Hậu quả của tội phạm trong lĩnh vực CNTT, MVT là thiệt hại gây ra cho quan hệ xã hội đảm bảo an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. Những hậu quả này thường không để lại dấu vết dưới dạng vật chất, mà tồn tại dưới dạng dấu vết điện tử. Ví dụ, người phạm tội truy cập vào mạng máy tính sao chép trộm tài liệu nhưng không xoá tài liệu đó. Nạn nhân mặc dù bị thiệt hại nhưng không biết nên không phát hiện ra được. Do đó, rất khó phát hiện hậu quả của tội phạm và cũng rất khó

[66] Xem: ITU/CARICOM/CTU Model Legilative Texts, Art.14: https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf (truy cập ngày 8/4/2018).

tìm chứng cứ chứng minh hậu quả của tội phạm trong lĩnh vực CNTT, MVT. Điều này dẫn đến việc đấu tranh đối với tội phạm này gặp rất nhiều khó khăn.

Thiệt hại do tội phạm trong lĩnh vực CNTT, MVT gây ra có thể tồn tại ở những dạng sau đây:

(1) *An toàn dữ liệu điện tử bị xâm hại:*

Khi bị tội phạm trong lĩnh vực CNTT, MVT bị tấn công dẫn đến thông tin dữ liệu sẽ bị mất an toàn. Tính an toàn của thông tin dữ liệu sẽ bị mất nếu một trong ba thuộc tính sau đây của nó bị mất:

+ *Tính nguyên vẹn*: thông tin dữ liệu phải có tính toàn vẹn, không bị thay đổi so với nguyên gốc khi nó được tạo ra trong quá trình lưu giữ, khai thác, sử dụng. Khi tính nguyên vẹn bị xâm phạm, thông tin dữ liệu bị hủy hoại, thay đổi, thêm bớt, giả mạo… sẽ mất đi giá trị của nó.

+ *Tính bí mật*: thông tin dữ liệu phải được bảo đảm tính bí mật trong quá trình lưu trữ, khai thác, sử dụng. Chỉ người có quyền hợp pháp mới được truy cập, khai thác, sử dụng, công bố… Khi bị mất tính bí mật, thông tin dữ liệu sẽ không còn giá trị, cho dù nó không bị hủy hoại hay thay đổi.

+ *Tính khả dụng*: thông tin dữ liệu luôn phải có khả năng sẵn sàng để khai thác, sử dụng theo mục đích của người quản lý, sử dụng thông tin đó. Khi bị tấn công, dữ liệu đó có thể không sử dụng được hoặc bị gián đoạn khi sử dụng.

(2) Mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử bị cản trở hoặc rối loạn hoạt động:

Môi trường không gian mạng là môi trường nhân tạo, được tạo ra bởi mạng máy tính, mạng viễn thông, phương tiện điện tử. Do đó, tấn công vào môi trường không gian mạng chính là tấn công vào các đối tượng này. Hậu quả là làm cho mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử bị cản trở hoặc bị rối loạn trong thời gian nhất định. Trong thời đại hiện nay, CNTT, MVT được ứng dụng phổ biến trong đời sống xã hội, việc

mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử bị cản trở hoặc bị rối loại sẽ dẫn đến những hậu quả khó lường như cơ quan, tổ chức phải ngừng hoạt động trong thời gian nhất định, gây thiệt hại về kinh tế, xã hội, an ninh, quốc phòng…

(3) Quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân bị xâm hại:

Các lợi ích này có thể là tài sản, danh dự, nhân phẩm, thông tin riêng của cá nhân, tổ chức bị xâm phạm do tội phạm trong lĩnh vực CNTT, MVT gây ra. Các hậu quả này thường là rất lớn. Bởi vì nhờ có mạng máy tính, mạng viện thông, phương tiện điện tử, người phạm tội có thể trộm cắp tài sản của mỗi một người có giá trị không lớn, nhưng nếu của hàng ngàn người thì giá trị lại rất lớn và nhiều khi nạn nhân không hề hay biết. Hoặc hành vi vu khống, chỉ cần nhấn phím, là hàng triệu người trong cả nước và thế giới có thể biết. Thiệt hại dưới dạng này đôi khi được thể hiện thông qua những giá trị, lợi ích mà người phạm tội thu được một cách bất chính.

Đặc điểm thứ tư, tội phạm trong lĩnh vực CNTT, MVT được thực hiện mà không bị giới hạn về không gian và thời gian:

Tội phạm trong lĩnh vực CNTT, MVT có thể được thực hiện bất cứ thời gian nào, không kể ngày hay đêm. Đặc biệt là việc thực hiện tội phạm không bị giới hạn bởi không gian, kể cả biên giới quốc gia. Hiên nay, môi trường không gian mạng được kết nối toàn cầu thông qua mạng internet, mạng viễn thông quốc tế. Do đó, người phạm tội có thể ở một chỗ nhưng lại thực hiện tội phạm ở những địa điểm khác nhau, có khi ở các nước khác nhau. Với tốc độ kết nối internet và viễn thông như hiện nay, trong một thời gian ngắn, người phạm tội có thể thực hiện tội phạm và gây ra thiệt hại cho nhiều nạn nhân khác nhau trong phạm vi toàn thế giới.

Chính điều này làm cho tội phạm trong lĩnh vực CNTT, MVT còn có đặc điểm nữa là tính quốc tế rất cao. Tội phạm này có thể thực hiện và gây

thiệt hại cho nhiều nước khác nhau. Do đó, việc đấu tranh phòng chống tội phạm này cần có sự hợp tác của nhiều quốc gia và các tổ chức quốc tế.

Đặc điểm thứ năm, chủ thể thực hiện tội phạm trong lĩnh vực CNTT, MVT thường là người có kiến thức về CNTT, MVT và liên quan đến nước ngoài:

Để thực hiện tội phạm này, người phạm tội phải sử dụng CNTT, MVT, do đó chủ thể của tội phạm này thường là người trẻ tuổi, có nhiều hiểu biết về lĩnh vực CNTT, MVT. Trong giai đoạn đầu khi tội phạm này mới xuất hiện, không cá nhân nào đủ điều kiện để sở hữu máy tính riêng nên những người có thể sử dụng máy tính đều là những người có chuyên môn cao, được đào tạo để sử dụng máy vi tính. Người phạm tội cũng chính là số ít những người có hiểu biết này. Đây là lý do lúc đầu có tác giả sử dụng thuật ngữ tội phạm "cổ cồn trắng" để chỉ tội phạm này. Đó là loại tội phạm chỉ do những người có kiến thức, chuyên môn cao thực hiện. Cho đến này, mặc dù CNTT, MVT được phổ cập và ngày càng dễ sử dụng nhưng để thực hiện và che giấu không bị phát hiện, người thực hiện tội phạm này phải là người có hiểu biết rất sâu về lĩnh vực CNTT, MVT.

Những người trẻ tuổi, có mối liên hệ nhất định với nước ngoài hoặc người nước ngoài thường là người có điều kiện tiếp thu kiến thức mới trong lĩnh vực CNTT, MVT. Do đó, người phạm tội trong lĩnh vực CNTT, MVT thường là người trẻ tuổi, có liên hệ với nước ngoài hoặc là người nước ngoài. So với các tội khác, tỷ lệ người phạm tội là người nước ngoài ở loại tội phạm này rất cao[67].

Đặc điểm thứ sáu, tội phạm trong lĩnh vực CNTT, MVT được thực hiện với lỗi cố ý:

[67] Theo thống kê của TAND tối cao trong giai đoạn 2009-2020 tỷ lệ trung bình số bị cáo là người nước ngoài trên số bị cáo bị xét xử sơ thẩm về tội phạm trong lĩnh vực CNTT, MVT là 9%; đặc biệt năm 2013 tỷ lệ này rất cao, lên tới 35,2%.

Lỗi của tội phạm trong lĩnh vực CNTT, MVT đều phải là lỗi cố ý. Khi thực tội phạm, người phạm tội nhận thức rõ việc sử dụng CNTT, MVT để phạm tội là nguy hiểm cho xã hội, thấy trước hậu quả của hành vi đó, đồng thời mong muốn hoặc có ý thức để mặc cho hậu quả đó xảy ra. Việc ứng dụng CNTT, MVT vào trong các lĩnh vực xã hội phục vụ đời sống con người là nhu cầu không thể thiếu. Cũng giống như các lĩnh vực khác, trong quá trình sử dụng CNTT, MVT có thể xảy ra sai sót, vi phạm cần khắc phục, xử lý nhưng vẫn cần khuyến khích ứng dụng CNTT, MVT để phục vụ đời sống con người ngày càng tốt hơn. Để đạt được mục tiêu kép là vừa khuyến khích việc sử dụng CNTT, MVT trong đời sống, vừa đấu tranh đối với tội phạm trong lĩnh vực CNTT, MVT chỉ nên xử lý hình sự đối với những vi phạm có lỗi cố ý. Đối với những vi phạm có lỗi vô ý không xử lý hình sự mà xử lý bằng các hình thức khác. Ví dụ, hành vi vô ý truy cập vào trang web bảo mật của cơ quan, tổ chức sẽ không bị coi là 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).

Trên thế giới, đa số các văn bản pháp luật quốc tế quy định lỗi của tội phạm trong lĩnh vực CNTT, MVT là lỗi cố ý. Tuy nhiên, cũng có trường hợp cá biệt quy định lỗi vô ý. Ví dụ: Điều 6 Luật mẫu 2002 (Tội cản trở dữ liệu máy tính) quy định cả lỗi cố ý và lỗi vô ý (recklessly)[68]:

"Điều 6: Tội cản trở, gây rối dữ liệu:

1. Người nào cố ý hoặc vô ý thực hiện trái phép các hành vi sau:

a. Phá hủy hoặc thay đổi dữ liệu

b. Làm cho dữ liệu sai lệch ý nghĩa, sử dụng kém hoặc không có hiệu quả

c. Cản trở, ngăn chặn hoặc gây rối người dùng hợp pháp dữ liệu, hoặc

d. Từ chối quyền truy cập dữ liệu hợp pháp của người khác."

[68] Xem: Commoonwealth Model Law, Art.6: http://thecommonwealth.org/sites/default/files/key_reform_pdfs/ P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf

Quan điểm này cho rằng, mặc dù đa số các tội phạm trong lĩnh vực CNTT, MVT có lỗi cố ý, nhưng vẫn có trường hợp phạm tội với lỗi vô ý. Bởi vì dữ liệu máy tính tồn tại ở dạng dữ liệu điện tử nên dễ bị xâm phạm bằng các hành vi phá huỷ, thay đổi, làm sai lệnh dù là với lỗi vô ý. Ví dụ, hành vi bất cẩn của người vận hành hệ thống dữ liệu có thể xóa mất dữ liệu trên máy chủ, gây thiệt hại cho khách hàng. Để nâng cao hơn mức độ bảo vệ dữ liệu điện tử cần phải nâng cao trách nhiệm của người sử dụng CNTT, MVT. Do đó, cần quy định xử lý hình sự đối với cả lỗi vô ý gây thiệt hại đối với dữ liệu điện tử. Tác giả luận án cho rằng, quan điểm này hiện nay chưa hợp lý, bởi vì nó cản trở việc phát triển và ứng dụng CNTT, MVT vào trong cuộc sống. Trong thực tiễn, cũng rất ít nước trên thế giới quy định như vậy. Theo kết quả khảo sát của một nghiên cứu của các tác giả ở nước ngoài, trong số 81 nước trên thế giới được khảo sát, chỉ có 06 nước ở Nam Mỹ, Tây Âu và Châu Phi xử lý hình sự đối với hành vi cản trở hoặc gây rối dữ liệu với lỗi vô ý; 02 nước xử lý hình sự đối với hành vi vô ý truy cập trái phép[69].

Đặc điểm thứ bảy, 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:

Đây là đặc điểm phân biệt giữa tội phạm trong lĩnh vực CNTT, MVT với tội phạm liên quan đến CNTT, MVT hay tội phạm máy tính, tội phạm CNTT, tội phạm mạng hay tội phạm sử dụng công nghệ cao. Tội phạm liên quan đến CNTT, MVT có phạm vi khách thể rất rộng, bởi vì người phạm tội có thể sử dụng CNTT, MVT để thực hiện nhiều loại tội khác nhau. Khách thể của tội phạm liên quan đến CNTT, MVT có thể bao gồm nhiều nhóm như

[69] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), Tlđd, tr. 84 - 91.

quyền bảo vệ thông tin của cá nhân; các quyền kinh tế của cá nhân, tổ chức; quyền bảo vệ sở hữu trí tuệ; quyền được bảo vệ của trẻ em. Theo tác giả Đặng Trung Hà, khách thể của tội phạm CNTT được chia làm 2 nhóm: *Thứ nhất*, tội phạm công nghệ thông tin xâm phạm, làm ảnh hưởng đến hoạt động bình thường của hệ thống máy tính, mạng máy tính và thiết bị điện tử. Tội phạm làm hỏng hóc, sai lệch hoặc chiếm đoạt máy tính, mạng máy tính, thiết bị liên quan, cũng như các thông tin trong hệ thống máy tính và mạng máy tính. *Thứ hai*, tội phạm công nghệ thông tin sử dụng máy tính và mạng máy tính làm công cụ để xâm phạm đến lợi ích chính đáng của cá nhân, pháp nhân, tổ chức, ảnh hưởng đến trật tự công cộng. Đây là nhóm khách thể rất rộng, liên quan đến các tội phạm truyền thống nhưng sử dụng các công nghệ thông tin để thực hiện tội phạm.

Trong khi đó, khách thể của tội phạm trong lĩnh vực CNTT, MVT có phạm vi hẹp hơn. Khách thể của tội phạm trong lĩnh vực CNTT, MVT chỉ là nhóm quan hệ xã hội đảm bảo an của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử bị tội phạm này xâm hại. Trường hợp người phạm tội sử dụng CNTT, MVT để thực hiện tội phạm xâm phạm an ninh quốc gia, danh dự, nhân phẩm của con người, trật tự quản lý kinh tế, trật tự công cộng (nói chung) sẽ không coi là tội phạm trong lĩnh vực CNTT, MVT, mà thuộc về những nhóm tội tương ứng. Ví dụ, tội khủng bố nhằm chống chính quyền nhân dân bằng cách tấn công, xâm hại, cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử của cơ quan, tổ chức, cá nhân (điểm d khoản 2 Điều 113) sẽ thuộc các tội xâm phạm an ninh quốc gia, chứ không phải là tội phạm trong lĩnh vực CNTT, MVT.

Trong thực tế sẽ có trường hợp tội phạm xảy ra sẽ vừa xâm hại đến quan hệ xã hội bảo đảm an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử vừa xâm hại đến các quan hệ xã hội khác như

danh dự, nhân phẩm của con người, quyền sở hữu, bảo đảm trật tự xã hội. Theo lý luận của LHS, một tội phạm xảy ra có thể cùng lúc xâm hại nhiều quan hệ xã hội khác nhau. Quan hệ xã hội được coi là khách thể trực tiếp của tội phạm là quan hệ xã hội mà sự xâm hại quan hệ xã hội đó, xét một cách tổng thể, thể hiện được đầy đủ tính chất nguy hiểm cho xã hội của hành vi phạm tội[70]. Ví dụ, hành vi khủng bố nhằm chống chính quyền nhân dân bằng cách tấn công, xâm hại, cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử của cơ quan, tổ chức, cá nhân được coi là tội xâm phạm an ninh quốc gia sẽ thể hiện đầy đủ tính chất nguy hiểm cho xã hội của hành vi này. Tương tự như vậy, hành vi sử dụng CNTT, MVT để thực hiện các tội khủng bố (Điều 299), tội đánh bạc (Điều 321), tội truyên truyền văn hoá phẩm đồi truỵ (Điều 326) không phải là tội phạm trong lĩnh vực CNTT, MVT.

Đối tượng tác động của tội phạm là một bộ phận khách thể mà thông qua việc tác động vào bộ phận đó, tội phạm xâm hại đến quan hệ xã hội được LHS bảo vệ. Đối tượng tác động của tội phạm trong lĩnh vực CNTT, MVT bao gồm các nhóm sau:

(1) Dữ liệu điện tử: là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử[71]. Tội phạm trong lĩnh vực CNTT, MVT tác động vào dữ liệu điện tử, gây mất an toà của dữ liệu điện tử bằng cách xâm hại tính nguyên vẹn, tính bí mật và tính sẵn sang của dữ liệu đó.

---

[70] Xem: Nguyễn Ngọc Hoà (Chủ biên) (2017), *Giáo trình Luật hình sự Việt Nam (Phần chung)*, NXB. Công an nhân dân, tr. 100.

[71] Xem: Khoản 12 Điều 4 Luật giao dịch điện tử (2005)

(2) Mạng máy tính: mạng máy tính là tập hợp nhiều máy tính kết nối với nhau, có thể chia sẻ dữ liệu cho nhau[72].

(3) Mạng viễn thông: 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[73].

(4) Phương tiện điện tử: Phương tiện điện tử là phương tiện hoạt động dựa trên công nghệ điện, điện tử, kỹ thuật số, từ tính, truyền dẫn không dây, quang học, điện từ hoặc công nghệ tương tự[74].

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

Hiện nay, việc phân loại đối với tội phạm này có nhiều ý nghĩa. Về nhận thức chung, thông qua việc phân loại tội phạm chúng ta xác định được phạm vi của tội phạm trong lĩnh vực CNTT, MVT bao gồm những tội nào. Về lập pháp, việc phân loại giúp các nhà làm luật quy định các điều luật về tội phạm trong lĩnh vực CNTT, MVT cho phù hợp. Ví dụ: BLHS năm 2015 quy định thành nhóm riêng tại Mục 2 Chương XXI. Về thực tiễn áp dụng pháp luật, việc phân loại tội phạm giúp các cơ quan có thẩm quyền phân công cho các đơn vị có khả năng điều tra những tội phạm trong lĩnh vực CNTT, MVT; nắm bắt từng loại tội phạm để có biện pháp đấu tranh chống và phòng ngừa phù hợp. Theo tác giả Debra Littlejohn Shinder, việc phân loại, sắp xếp các tội phạm này thành nhóm giúp chúng ta nhận ra các tội phạm cụ thể và mối quan hệ giữa các tội phạm đó với nhau trong nhóm. Từ đó, những người thực

---

[72] Xem: Khoản 3 Điều 2 Thông tư liên tịch số 10/2012/ TTLT-BCA-BQP-BTP-BTT&TT-VKSNDT -TANDTC ngày 10/9/2012 hướng dẫn áp dụng quy định của Bộ luật hình sự về một số tội phạm trong lĩnh vực công nghệ thông tin và viễn thông.

[73] Xem: Khoản 10 Điều 3 Luật viễn thông (2009)

[74] Xem: Khoản 10 Điều 4 Luật giao dịch điện tử (2005);

thi pháp luật sẽ nhận dạng được các hành vi phạm tội và giải quyết nó giống như các tội phạm khác cùng loại, giúp họ thành thục và chuyên nghiệp hơn[75].

Với lý do trên, trong phạm vi rộng việc phân loại tội phạm liên quan đến CNTT, MVT rất được quan tâm nghiên cứu và đưa ra nhiều cách phân loại khác nhau. Do xuất phát từ những tiêu chí khác nhau nên việc phân loại cũng rất khác nhau, không có sự thống nhất. Sau đây là một số cách phân loại tội phạm liên quan đến CNTT, MVT tiêu biểu:

Cách thứ nhất, theo tác giả Chawki, M. căn cứ hành vi và mục đích phạm tội, tội phạm mạng được chia thành 6 nhóm sau[76]:

(1) Các tội phạm truy cập bất hợp pháp (hacking) vào máy tính, mạng máy tính để thu thập thông tin hoặc các mục đích khác. Tội phạm được thực hiện bằng nhiều thủ đoạn, công nghệ khác nhau như dò tìm, bão tấn công, bẻ khóa mật khẩu, tràn vùng đệm… Nhóm này còn bao gồm cả các hành vi như nghe trộm điện thoại hoặc các cuộc đàm thoại trên MVT hoặc mạng internet.

(2) Các tội phạm liên quan đến vi - rút và mã độc như tội sản xuất, phân phối, tàng trữ, sở hữu trái phép vi - rút; tội phát tán vi - rút; hoặc sử dụng vi - rút để thực hiện các tội khác như truy cập trái phép hoặc cản trở, phá hủy mạng máy tính, phương tiện điện tử…

(3) Các tội phạm lừa đảo qua máy tính, mạng máy tính, mạng viễn thông: trong quá trình hoạt động của máy tính, tất cả các giai đoạn (nhập thông tin đầu vào, xử lý thông tin, xuất thông tin đầu ra hoặc trao đổi thông tin) đều có thể trở thành hoạt động phạm tội hoặc là mục đích của tội phạm của tội phạm mạng. Mục đích của các tội phạm dạng này là tạo ra thông tin giả, sai lệnh (nhưng lại được dùng như thông tin thật) để sử dụng vào các mục

[75] Xem: Debra Littlejohn Shinder (2002), Tlđd, tr.18.

[76] Xem: Chawki, M (2005), Tlđd, tr. 18 - 28.

đích bất hợp pháp khác nhau như chiếm đoạt tài sản hoặc những thứ có giá trị, làm giả tài liệu, giấy tờ… Một số tội phạm mạng trong nhóm này gồm:

- Các tội phạm lừa đảo bằng các thao tác máy tính: những tài sản vô hình được mô tả dưới dạng dữ liệu như tiền trong tài khoản ngân hàng, thời gian làm việc trong công ty trong dữ liệu máy tính là mục tiêu của tội phạm loại này. Ví dụ, người phạm tội truy cập vào cơ sở dữ liệu của công ty thay đổi tăng số giờ làm việc của mình trong một tháng để nhận được tiền lương cao hơn. Người phạm tội cũng có thể thu thập những thông tin về tài khoản ngân hàng của người khác, cũng như thông tin cá nhân, thông tin tài chính của người khác, sau đó bán những thông tin này cho những người làm thẻ ngân hàng giả để thu lợi nhuận.

- Các tội phạm về giả mạo hoặc làm giả tài liệu liên quan đến máy tính: khi thay đổi dữ liệu trong hệ thống máy tính (để sử dụng như thông tin thật) đó là hành vi giả mạo. Trong trường hợp này hệ thống máy tính là mục đích tấn công của hành vi phạm tội. Bên cạnh đó, máy tính cũng có thể là công cụ để thực hiện hành vi giả mạo hoặc làm tài liệu giả. Ví dụ, người phạm tội sử dụng máy in, sao mầu tạo ra tài liệu giả để sử dụng cho mục đích phạm tội.

- Các tội phạm về thay đổi cơ sở dữ liệu hoặc chương trình: tội phạm này bao gồm cả những hành vi trực tiếp hoặc lén lút truy cập bất hợp pháp vào hệ thống máy tính bằng phần mềm mã độc. Hành vi thay đổi bất hợp pháp dữ liệu máy tính hoặc chức năng của máy tính với ý định cản trở, gây trở ngại chức năng thông thường của hệ thống máy tính được coi là tội phạm. Loại tội phạm này được xếp vào nhóm phá hoại máy tính. Tuy nhiên, đây cũng có thể được coi là công cụ để thu những lợi ích kinh tế. Ví dụ, người phạm tội xâm nhập vào hệ thống máy tính, thay đổi dữ liệu hoặc chương trình máy tính làm cho hệ thống máy tính của nạn nhân không hoạt động được. Sau đó, tống tiền

nạn nhân, buộc nạn nhân phải nộp một khoản tiền chuộc nhất định thì mới khôi phục hệ thống máy tính trở lại bình thường.

- Các tội phạm về lừa đảo bán hàng trên mạng: người bán hàng có thể có những hành vi cố ý tạo ra nhầm lẫn, nhận đơn đặt hàng hoặc tiền của khách hàng nhưng lại không giao hàng hoặc cung cấp hàng không đúng yêu cầu. Một trong những hành vi nổi bật của loại tội phạm này là hành vi lừa đảo trong đầu tư.

- Tội phạm liên quan đến thư điện tử giả: đó là tội phạm liên quan đến hành vi sử dụng thư điện tử lừa bịp hoặc giả mạo cho mục đích bất hợp pháp. Người phạm tội có thể sử dụng thư điện tử giả để thu thập bất hợp pháp thông tin của cá nhân, tổ chức; cũng có thể sử dụng nhiều thư điện tử không có nội dung (thư rác) để tấn công cản trở hoạt động bình thường của hệ thống máy tính; cũng có thể thư điện tử giả chữ ký số để lừa đảo trực tiếp nạn nhân. Ví dụ, nhắn tin lừa trúng thưởng số tiền lớn tới nạn nhân, yêu cầu nạn nhân nộp một số tiền nhất định vào tài khoản (của người phạm tội) để lĩnh thưởng.

(4) Các tội phạm có hành vi theo dõi, đe dọa, nói xấu cá nhân, tổ chức qua mạng: đặc điểm chung của các tội phạm này là mặc dù được thực hiện trên môi trường không gian mạng, nhưng tội phạm lại có khả năng tác động trực tiếp đến con người trong môi trường thực tại, gây thiệt hại hoặc đe dọa gây thiệt hại cho con người ngoài môi trường thực tại.

(5) Tội phạm khủng bố qua mạng: đây cũng là một loại tội phạm có tính bạo lực đối với con người như tội phạm ở nhóm (4). Mặc dù hành vi khủng bố được thực hiện trong môi trường không gian mạng nhưng hậu quả của tội phạm thì xảy ra trong môi trường thực tại, gây thiệt hại hoặc đe dọa gây thiệt hại cho con người như làm chết người, gây thương tích cho người khác, gây nổ hoặc tai nạn máy bay…

(6) Các tội phạm trộm cắp qua mạng: các tội phạm sử dụng máy tính, mạng máy tính để tham ô, đầu độc bộ nhớ sẵn, chiếm đoạt bất hợp pháp tài sản, xâm phạm quyền tác giả, sao chụp bất hợp pháp, trộm thông tin cá nhân để chiếm đoạt tài sản ….

Có thể thấy cách phân loại tội phạm mạng của tác giả Chawki, M là dựa vào tính chất và mục đích của hành vi phạm tội. Cách phân loại này giúp chúng ta dễ dàng phân biệt giữa các hành vi phạm tội với nhau hơn. Ví dụ: đều là hành vi truy cập trái phép nhưng nếu thủ đoạn phạm tội là đưa ra thông tin giả sẽ thuộc nhóm lừa đảo máy tính (nhóm 2); nếu dùng thủ đoạn lén lút chiếm đoạt thì thuộc nhóm trộm cắp qua mạng (nhóm 6).

Cách thứ hai, theo tác giả Marco Gercke căn cứ theo vai trò của CNTT, MVT đối với tội phạm, tội phạm mạng được chia thành 5 nhóm[77]:

(1) Các tội phạm phạm xâm phạm tính bí mật, nguyên vẹn, sẵn sàng của dữ liệu điện tử, hệ thống máy tính, mạng viễn thông. Đặc điểm chung của các tội phạm này là CNTT, MVT trở thành mục tiêu tấn công của tội phạm. Tội phạm tấn công vào mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc dữ liệu điện tử để xâm phạm tính nguyên vẹn, tính bí mật hoặc tính sẵn sàng của những đối tượng này. Các tội phạm thuộc nhóm này bao gồm: tội xâm nhập bất hợp pháp mạng máy tính hoặc dữ liệu điện tử; tội thu, nhận dữ liệu bất hợp pháp; tội ngăn chặn dữ liệu bất hợp pháp; tội can thiệp bất hợp pháp vào dữ liệu, hệ thống.

(2) Các tội phạm mà người phạm tội sử dụng CNTT, MVT làm công cụ, phương tiện để thực hiện tội phạm "truyền thống" khác như: tội phổ biến tài liệu khiêu dâm, khiêu dâm trẻ em qua mạng; tội phổ biến thông tin phân

[77] Xem Marco Gercke (2012), *Understanding cybercrime: Phenomena, Challengens and Legall Response*, ITU, tr. 16 - 40: http://www.itu.int/ITU-D/cyb/cybersecurity docs/ Cybercrime%20legislation%20EV6.pdf (truy cập ngày 12/2/2018).

biệt chủng tộc, nói xấu, kích động bạo lực qua mạng; tội phạm liên quan đến tôn giáo qua mạng; cờ bạc qua mạng trái phép; tội vu khống, bôi nhọ người khác qua mạng; tội phát tán thư rác; các tội phạm sử dụng mạng internet hoặc mạng viễn thông làm môi trường giao tiếp với nhau để gạ gẫm, đề nghị hoặc xúi giục phạm tội, bán hàng trái phép, cung cấp thông tin hoặc chỉ dẫn thực hiện những hành vi vi phạm pháp luật (hướng dẫn chế tạo thuốc nổ, vũ khí…).

(3) Các tội phạm liên quan đến quyền tác giả và nhãn hiệu hàng hóa: đặc trưng của các tội phạm này là người phạm tội sử dụng CNTT, MVT để xâm phạm quyền tác giả hoặc nhãn hiệu hàng hóa hoặc xâm phạm quyền tác giả, nhãn hiệu hàng hóa được các cá nhân, tổ chức số hóa và đưa lên môi trường mạng internet hoặc mạng viễn thông.

(4) Các tội phạm liên quan đến máy tính: đây cũng là nhóm tội phạm mà người phạm tội đã sử dụng CNTT, MVT để thực hiện tội phạm, nhưng khác các tội phạm ở nhóm (2) ở chỗ tính rõ ràng của tội phạm không được quy định chặt chẽ trong các quy định của pháp luật. Các tội phạm trong lĩnh vực CNTT, MVT trong nhóm này bao gồm: tội lừa đảo liên quan đến máy tính; tội làm giả liên quan đến máy tính; tội trộm cắp thông tin cá nhân; tội lạm dụng công cụ, thiết bị, phần mềm tin học.

(5) Các tội phạm mang tính phối hợp: đặc điểm của nhóm tội phạm này là CNTT, MVT là môi trường hoặc công cụ để thực hiện những tội phạm có sự kết hợp nhiều hành vi phạm tội khác nhau. Các tội phạm trong nhóm này gồm: tội khủng bố qua mạng (tuyên truyền cho khủng bố, thu thập thông tin phục vụ cho khủng bố, chuẩn bị tấn công khủng bố trong thế giới thực tại, phát hành những tài liệu để đào tạo khủng bố, liên hệ, giao tiếp với nhau để khủng bố, lập ngân quỹ cho khủng bố, tấn công chống lại những tổ chức đối lập); chiến tranh mạng (chiến tranh điện tử, chiến tranh thông tin); tội rửa tiền qua

mạng; phishing - lừa đảo để lấy thông tin hoặc bí mật của cá nhân, tổ chức.

Cách phân loại tội phạm mạng của tác giả Marco Gercke cho thấy rõ phạm vi và đặc điểm chung của tội phạm này. Thông qua cách phần loại này giúp chúng ta phân biệt và hiểu rõ nội dung cụ thể của từng tội phạm.

Tác giả Debra Littlejohn Shinder thì lại có cách phân loại khác. Ông dựa vào việc tội phạm có tính bạo lực đối với con người hay không để chia tội phạm mạng chia làm 3 loại chính[78]: (1) Tội phạm dùng bạo lực hoặc đe dọa dùng bạo lực: đây là nhóm tội phạm mà người phạm tội sử dụng CNTT, MVT để gây nguy hiểm về thể chất đến con người; (2) Các tội phạm không có tính bạo lực đối với con người là các tội được thực hiện và xâm phạm thế giới ảo mà không có sự giao tiếp, tiếp xúc vật lý trong thế giới thực tại; (3) Các tội phạm khác không có tính bạo lực đối với con người.

Có thể thấy các cách phân loại tội phạm trên dựa trên khái niệm tội phạm liên quan đến CNTT, MVT có phạm vi rộng. Do đó, tội phạm liên quan đến CNTT, MVT được chia thành các nhóm bao gồm nhiều tội khác nhau. Trong Luận án này việc phân loại tội phạm trong lĩnh vực CNTT, MVT (có phạm vi hẹp hơn so với tội phạm liên quan đến CNTT, MVT) có ý nghĩa cả về lý luận và thực tiễn. Có nhiều cách phân loại tội phạm trong lĩnh vực CNTT, MVT khác nhau. Mỗi cách phân loại lại có ý nghĩa 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. Đây là cách phân loại có ý nghĩa thực tiễn, rất quan trọng đối với các cơ quan có thẩm quyền tiến hành tố tụng trong việc xử lý hình sự đối với tội phạm này. Căn cứ vào cách phân loại này cơ quan có thẩm quyền tiến hành tố tụng mới có xác định

[78] Xem: Debra Littlejohn Shinder (2002), Tlđd, tr.19 - 33.

được các vấn đề như thời hiệu truy cứu TNHS; thẩm quyền, thời hạn điều tra, truy tố xét xử; thời hạn tạm giam …

(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 sau:

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. Trong nhóm này, CNTT, MVT là đối tượng tấn công của tội phạm. Tội phạm xâm phạm tính nguyên vẹn, tính bí mật, tính khả dụng của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. Các tội trong nhóm này bao gồm: tội truy cập bất hợp pháp, ngăn chặn bất hợp pháp, gây rối dữ liệu, gây rối hệ thống, lạm dụng các thiết bị CNTT, MVT.

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. Các lợi ích bị xâm hại có thể là về tài sản, danh dự, nhân phẩm, quyền bí mật đời tư. Các tội trong nhóm này bao gồm: tội sử dụng mạng máy tính, mạng viễn thong, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản; tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng; tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông.

Cách phân loại này cho thấy phạm vi và đặc điểm của tội phạm trong lĩnh vực CNTT, MVT. Tội phạm có mục tiêu tấn công là mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử thường được gọi là tội phạm trong lĩnh vực CNTT, MVT theo nghĩa hẹp. Tội phạm do người phạm tội sử dụng CNTT, MVT để thực hiện thường được gọi là tội phạm trong lĩnh vực CNTT, MVT theo nghĩa rộng. Tội phạm này trong tương lai có thể ngày càng được mở rộng theo mức độ ứng dụng ngày càng phổ biến của CNTT, MVT.

(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 sau đây:

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. Mục đích phạm tội của người phạm tội trong nhóm này là xâm phạm tính bí mật, tính toàn vẹn, tính khả dụng của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử nói chung. Các tội thuộc nhóm này bao gồm: 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), 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), Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287), 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.

Thứ hai, tội phạm trong lĩnh vực CNTT, MVT trong đó người phạm tội có mục đích chiếm đoạt tài sản. Người phạm tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện hành vi chiếm đoạt tài sản. Mục đích chiếm đoạt tài sản là dấu hiệu bắt buộc của tội này. Đây cũng là dấu hiệu để phân biệt với những tội khác. Trong trường hợp này, người phạm tội cũng có thể phải truy cập bất hợp pháp vào tài khoản của người khác nhưng với mục đích là chiếm đoạt tài sản. Tội phạm thuộc nhóm này là 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.

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. Cụ thể, người phạm tội sử dụng CNTT, MVT để đưa hoặc sử dụng trái

phép thông tin mạng máy tính, mạng viễn thông; thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng, qua đó thiệt hại về uy tín, nhân phẩm, danh dự và các lợi ích khác của cơ quan, tổ chức, cá nhân khác. Các tội trong nhóm này bao gồm: Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288), Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291) BLHS năm 2015.

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. Nhóm tội phạm này bao gồm: 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) và Tội cố ý gây nhiễu có hại (Điều 294) BLHS năm 2015.

Cách phân loại này có ưu điểm là chi tiết, cụ thể, giúp chúng ta có căn cứ phân biệt được giữa các tội phạm trong lĩnh vực CNTT, MVT với nhau. Ví dụ: hành vi xâm nhập trái phép vào mạng máy tính của người khác có thể là hành vi khách quan của tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289), nhưng cũng có thể là hành vi khách quan của tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (điểm c khoản 1 Điều 290). Cần phải xác định được mục đích của hành vi xâm nhạp trái phép vào mạng máy tính mới có thể phân biệt được hai tội trên. Cụ thể, nếu hành vi xâm nhập trái phép vào mạng máy tính của người khác nhằm chiếm đoạt tài sản sẽ phạm vào tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (điểm c khoản 1 Điều 290); nếu không có mục đích chiếm đoạt tài sản sẽ phạm vào tội xâm nhập trái phép vào

mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289).

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

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

Tội phạm trong lĩnh vực CNTT, MVT từ khi mới ra đời đã có những quan điểm khác nhau về việc có cần quy định riêng về tội phạm này trong LHS hay không? Tuy nhiên đến nay, đa số các nước trên thế giới, trong đó có Việt Nam đã quy định riêng về tội phạm trong lĩnh vực CNTT, MVT trong BLHS. Việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS xuất phát từ những cơ sở lý luận và thực tiễn sau đây:

Thứ nhất, cơ sở lý luận của việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS là các điều kiện cho phép nhà làm luật quy định về tội phạm đó. Các điều kiện cơ bản này bao gồm: (1) tội phạm trong lĩnh vực CNTT, MVT là một loại tội phạm mới xảy ra trong môi trường không gian mạng. Tuy nhiên, tội phạm này lại gây nguy hiểm cho xã hội và có xu hướng xuất hiện ngày càng phổ biến. (2) Mặc dù tội phạm trong lĩnh vực CNTT, MVT được thực hiện trong môi trường không gian mạng nhưng bằng các công cụ kỹ thuật chúng ta vẫn có thể nhận thức, mô tả rõ ràng về hành vi phạm tội, các thiệt hại xảy ra, cũng như xác định rõ chủ thể đã thực hiện hành vi phạm tội (để truy cứu TNHS). Như vậy, dù là một tội phạm mới nhưng hoàn toàn có đủ điều kiện để nhà làm luật có thể quy định trong BLHS để xử lý hình sự.

Thứ hai, hành vi phạm tội trong lĩnh vực CNTT, MVT có tính nguy hiểm đáng kể cho xã hội. Tính nguy hiểm của hành vi phạm tội trong lĩnh vực CNTT, MVT trước tiên thể hiện ở những thiệt hại mà nó gây ra hoặc đe dọa gây ra cho xã hội rất lớn. Khi CNTT, MVT được ứng dụng trong hầu hết các

lĩnh vực của đời sống, kinh tế, xã hội, phạm vi gây ra thiệt hại hoặc đe dọa gây ra thiệt hại của loại tội phạm này cũng sẽ ảnh hưởng đến nhiều lĩnh vực khác nhau như kinh tế, đời sống sinh hoạt của cá nhân, hoạt động công cộng. Hành vi phạm tội được thực hiện trong môi trường không gian mạng, nên không bị giới hạn bởi thời gian và không gian. Do đó, tội phạm được thực hiện ở quốc gia này nhưng gây thiệt hại cho nhiều quốc gia khác, thậm trí là toàn cầu.

Do ảnh hưởng đến nhiều lĩnh vực của đời sống xã hội, đồng thời trên phạm vi toàn cầu nên hậu quả mà tội phạm trong lĩnh vực CNTT, MVT gây ra hoặc đe dọa gây ra cho xã hội là rất lớn; đôi khi không thể tính hết được vì không thể thống kê, hơn nữa nhiều khi chính bản thân nạn nhân cũng không biết mình bị thiệt hại. Tính nguy hiểm của tội phạm trong lĩnh vực CNTT, MVT còn được thể hiện thông qua tính chất tinh vi của hành vi phạm tội mà người phạm tội đã thực hiện. Hành vi phạm tội thường được thực hiện bằng các biện pháp công nghệ hiện đại và trong môi trường không gian ảo nên ít để lại dấu vết vật chất, dễ che giấu, xóa dấu viết. Điều này làm cho công tác đấu tranh chống và phòng ngừa loại tội phạm này gặp không ít khó khăn.

Thứ ba, hành vi phạm tội trong lĩnh vực CNTT, MVT diễn ra phổ biến trong xã hội. Như trên đã trình bày, sự ra đời, tồn tại và phát triển của tội phạm trong lĩnh vực CNTT, MVT gắn liền với sự ra đời và ứng dụng của CNTT, MVT. Đây là mặt trái của việc ứng dụng và phát triển CNTT, MVT trong đời sống xã hội con người. Có thể khẳng định, khi CNTT, MVT càng phát triển và ứng dụng rộng rãi trong đời sống thì tội phạm trong lĩnh vực CNTT, MVT sẽ vẫn tồn tại và diễn ra phổ biến. Hiện nay, CNTT, MVT đã được ứng dụng trong hầu hết các lĩnh vực của đời sống con người. Trong tương lai, xu hướng số hóa các công cụ, thiết bị sản xuất, sinh hoạt của con người ngày càng phổ biến. Điều đó sẽ tạo ra ngày càng nhiều môi trường cho

việc thực hiện tội phạm này; đồng thời cũng cung cấp cho người phạm tội thêm nhiều công cụ hiện đại để thực hiện tội phạm.

Thứ tư, về kỹ thuật lập pháp, hành vi phạm tội trong lĩnh vực CNTT, MVT có thể được nhận thức và mô tả trong cấu thành tội phạm được quy định trong BLHS. Tội phạm trong lĩnh vực CNTT, MVT cho dù đa số được thực hiện trong môi trường không gian mạng, việc phạm tội lại ít để lại dấu vết, tuy nhiên với sự hỗ trợ của khoa học kỹ thuật hiện đại và sự hiểu biết của con người về lĩnh vực này, chúng ta hoàn toàn có thể nhận thức được về hành vi, thủ đoạn, hậu quả… của tội phạm này. Trên cơ sở đó, chúng ta hoàn toàn có thể mô tả loại tội phạm này trong BLHS, làm cơ sở pháp lý cho việc truy cứu TNHS đối với người phạm tội.

1.1.4.2. Ý nghĩa của việc quy định tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong Bộ luật hình sự

Việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS có những ý nghĩa rất quan trọng sau đây:

Thứ nhất, việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS đáp ứng nhu cầu công tác đấu tranh chống và phòng ngừa tội phạm trong lĩnh vực CNTT, MVT. Cùng với quá trình ngày càng phát triển của lĩnh vực CNTT, MVT, các vi phạm pháp luật nói chung và tội phạm nói riêng trong lĩnh vực CNTT, MVT cũng ngày càng phổ biến và phức tạp. Tội phạm trong lĩnh vực CNTT, MVT đã gây ra những thiệt hại lớn cho xã hội, không chỉ về tài sản mà còn ảnh hưởng đến nhiều lĩnh vực khác như an ninh, trật tự, an toàn xã hội. Điều đó, đặt ra yêu cầu cần đấu tranh chống và phòng ngừa tội phạm trong lĩnh vực CNTT, MVT. Việc quy định tội phạm trong lĩnh vực CNTT, MVT trong LHS là công cụ sắc bén để đấu tranh chống và phòng ngừa hiệu quả đối với loại tội phạm này.

Thứ hai, việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS góp phần bảo vệ trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân. Khi CNTT, MVT được ứng dụng trong đời sống xã hội, người phạm tội có thể sử dụng không gian mạng để xâm phạm lợi ích của nhà nước, trật tự, an toàn xã hội hoặc lợi ích hợp pháp của cá nhân, tổ chức. Hơn nữa, nhiều tài sản vô hình như thông tin dữ liệu, tiền trong tài khoản của cá nhân, tổ chức… cũng cần có biện pháp bảo vệ phù hợp, hiệu quả. Nếu không có quy định riêng về tội phạm trong lĩnh vực CNTT, MVT trong BLHS, mà chỉ sử dụng quy định chung (giống như bảo vệ các tài sản hữu hình) thì không thể bảo vệ hiệu quả quyền tài sản hợp pháp của cá nhân, tổ chức.

Thứ ba, việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS đã giải quyết những vướng mắc, tồn tại trong quá trình đấu tranh chống và phòng ngừa tội phạm. Những hành vi, thủ đoạn của tội phạm trong lĩnh vực CNTT, MVT có nhiều điểm mới, khác biệt so với tội phạm "truyền thống". Nếu chỉ dựa vào các quy định chung của BLHS để xử lý loại tội phạm này thì sẽ gặp khó khăn trong quá trình định tội, gây ra những tranh luận, quan điểm khác nhau khi xét xử.

Thực tiễn xét xử ở Việt Nam đã phải đối mặt với khó khăn này khi xử lý hành vi "trộm cắp cước viễn thông". Khi BLHS năm 1999 chưa có quy định cụ thể để xử lý hành vi này, nên nhiều quan điểm khác nhau khi định tội danh đối với nó. Có quan điểm xác định đây là hành vi trộm cắp tài sản, nhưng cũng có quan điểm cho rằng đó là hành vi kinh doanh trái phép. Xét về bản chất, hành vi này cho dù xác định theo tội danh nào (trong những tội danh hiện có trong BLHS năm 1999) đều không thỏa mãn hoàn toàn. Bởi vì đây là hành vi phạm tội mới có những đặc điểm riêng của tội phạm trong lĩnh vực CNTT, MVT, cần phải có quy định riêng để xử lý nó. Những khó khăn, vướng mắc này chỉ được giải quyết khi BLHS năm 1999 được sửa đổi, bổ

sung bằng việc quy định Điều 226b (Tội sử dụng mạng máy tính, mạng viễn thông, mạng internet hoặc thiết bị số nhằm chiếm đoạt tài sản). Hơn nữa, tội phạm trong lĩnh vực CNTT, MVT có đặc điểm là ít để lại các dấu vết vật chất, mà tồn tại ở dạng dấu viết điện tử. Do đó, để xử lý tội phạm cần có quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT và quy định về chứng cứ điện tử trong luật tố tụng hình sự.

Thứ tư, việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS phù hợp với các quy định của pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT. Hiện nay, đa số các quốc gia đã quy định về tội phạm trong lĩnh vực CNTT, MVT trong LHS của mình, mặc dù quan niệm, phạm vi và kỹ thuật lập pháp có thể khác nhau. Các nước trên thế giới đều xác định được ý nghĩa to lớn của việc quy định loại tội phạm này trong LHS. Không những thế, để hợp tác quốc tế trong đấu tranh chống và phòng ngừa loại tội phạm này, các quốc gia còn hợp tác với nhau ký kết nhiều văn bản pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT như Công ước Budapest 2001, Luật mẫu 2002… Có thể nói việc quy định tội phạm trong lĩnh vực CNTT, MVT trong LHS là xu hướng phổ biến của các quốc gia trên thế giới. Đây là căn cứ thực tiễn quan trọng, đa dạng, phong phú để các nước, trong đó có Việt Nam nghiên cứu, rút kinh nghiệm trong việc quy định tội phạm trong lĩnh vực CNTT, MVT trong BLHS.

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:*

Thứ nhất, tội truy cập bất hợp pháp: Theo Điều 2, truy cập bất hợp pháp là hành vi cố ý truy cập một phần hoặc toàn bộ hệ thống máy tính mà không có quyền truy cập. Trong đó, "hệ thống máy tính" được hiểu là bất kỳ thiết bị hoặc nhóm thiết bị có liên hệ với nhau, thực hiện quá trình xử lý dữ liệu một cách tự động theo một chương trình định sẵn[79].

Để hạn chế phạm vi của tội phạm này, Công ước cho phép các quốc gia thành viên chỉ coi là tội phạm nếu việc truy cập bất hợp pháp vượt qua các biện pháp an ninh của hệ thống máy tính và có mục đích chiếm đoạt dữ liệu máy tính hoặc các ý định không trung thực khác hoặc có liên hệ với một hệ thống máy tính được kết nối với hệ thống máy tính khác.

Thứ hai, tội ngăn chặn bất hợp pháp: Theo Điều 3, tội ngăn chặn bất hợp pháp là hành vi cố ý ngăn chặn bất hợp pháp bằng các biện pháp kỹ thuật, việc truyền tải dữ liệu máy tính không công khai trong hệ thống máy tính hoặc từ hệ thống máy tính này đến hệ thống máy tính khác.

"Dữ liệu máy tính" là bất cứ sự thể hiện tình tiết thực tế, thông tin hoặc khái niệm theo một hình thức tương thích với việc xử lý trong hệ thống máy tính, bao gồm chương trình phù hợp với việc làm cho hệ thống máy tính thực hiện một chức năng nhất định[80]. Điều luật này cũng áp dụng đối với việc truyền các dữ liệu điện tử khác như điện thoại, fax, chuyển các tệp thông tin điện tử… Mục đích của điều luật là bảo vệ quyền riêng tư của dữ liệu thông tin liên lạc. Quyền này được quy định trong Điều 8 Công ước về quyền con người của Châu Âu.

Công ước Budapest 2001 cũng cho phép các nước thành viên hạn chế phạm vi của tội này, chỉ coi là tội phạm nếu việc ngăn chặn bất hợp pháp có

[79] Xem: điểm a Điều 1 Công ước Budapest 2001.

[80] Xem: điểm b Điều 1 Công ước Budapest 2001.

mục đích không trung thực hoặc có liên quan đến một hệ thống máy tính được kết nối với hệ thống máy tính khác.

Thứ ba, tội gây rối dữ liệu máy tính: Theo Điều 4, tội gây rối dữ liệu là hành vi bất hợp pháp của người không có thẩm quyền, cố ý làm hư hại, xóa, làm hỏng hoặc nén dữ liệu máy tính. Chỉ cần có hành vi gây rối dữ liệu là tội phạm đã hoàn thành, không cần phải gây ra thiệt hại thực tế. Tuy nhiên, Công ước cũng cho phép các quốc gia thành viên có thể lựa chọn quy định chỉ coi là tội phạm nếu gây ra thiệt hại nghiêm trọng. Việc giải thích thế nào là "thiệt hại nghiêm trọng" sẽ do các nước thành viên quy định.

Thứ tư, tội gây rối hệ thống: Theo Điều 5, gây rối hệ thống là hành vi bất hợp pháp của người không có thẩm quyền, cố ý cản trở nghiêm trọng hoạt động của hệ thống máy tính bằng cách đưa vào, truyền tải, làm hư hỏng, xóa, làm suy giảm, thay thế hoặc nén dữ liệu máy tính. Thủ đoạn thực hiện tội phạm này cũng giống như tội gây rối dữ liệu, chỉ khác nhau ở đối tượng phạm tội là hệ thống máy tính, chứ không phải là dữ liệu máy tính.

Thứ năm, tội lạm dụng các thiết bị: Theo Điều 6, lạm dụng các thiết bị là hành vi của người không có thẩm quyền, cố ý thực hiện một trong các hành vi:

(a) sản xuất, bán, đề nghị sử dụng, nhập khẩu, phân phối hoặc bằng các cách thức khác cung cấp: (i) thiết bị bao gồm chương trình máy tính, được thiết kế hoặc điều chỉnh để thực hiện tội phạm từ Điều 2 đến Điều 5 của Công ước; (ii) Mã số truy cập của máy tính, mật mã truy cập hoặc dữ liệu tương tự để truy cập vào một phần hoặc toàn bộ hệ thống máy tính với ý định sẽ sử dụng để thực hiện các hành vi phạm tội từ Điều 2 đến Điều 5 của Công ước.

(b) Chiếm hữu các đối tượng trên với ý định cho người khác sử dụng để thực hiện các hành vi phạm tội từ Điều 2 đến Điều 5 của Công ước với bất kể số lượng nào. Tuy nhiên, các quốc gia thành viên có quyền quy định chiếm hữu một số lượng thiết bị nhất định mới bị coi là tội phạm.

Theo khoản 3 Điều 6 của Công ước, các quốc gia thành viên có thể bảo lưu không quy định là tội phạm đối với các hành vi quy định tại khoản 1 Điều 6 trên, nhưng việc bán, phân phối hoặc cung cấp mã số truy cập của máy tính, mật mã truy cập hoặc dữ liệu tương tự để truy cập vào một phần hoặc toàn bộ hệ thống máy tính với ý định sẽ sử dụng để thực hiện các hành vi phạm tội từ Điều 2 đến Điều 5 của Công ước, buộc phải coi là tội phạm.

** Nhóm các tội liên quan đến máy tính:*

Thứ nhất, tội giả mạo liên quan đến máy tính: Theo Điều 7, tội giả mạo liên quan đến máy tính là hành vi của người không được phép, cố ý đưa vào, thay đổi, xóa hoặc nén dữ liệu máy tính làm cho dữ liệu máy tính không chính xác, nhưng sử dụng các dữ liệu này cho các mục đích hợp pháp với ý thức như dữ liệu máy tính chính xác.

Công ước cũng cho phép các quốc gia thành viên chỉ coi là tội phạm nếu việc giả mạo được thực hiện với mục đích lừa đảo hoặc các ý định không trung thực khác.

Thứ hai, tội lừa đảo liên quan đến máy tính: Theo Điều 8, tội lừa đảo liên quan đến máy tính là hành vi của người không có thẩm quyền, cố ý, gây thiệt hại về tài sản cho người khác bằng cách đưa vào, thay đổi, xóa hoặc nén dữ liệu máy tính hoặc bất cứ hành vi gây rối nào đối với sự vận hành của hệ thống máy tính để lừa đảo hoặc không trung thực nhằm thu lợi hoặc có được quyền lợi kinh tế bất chính.

** Nhóm các tội liên quan đến nội dung:*

Thứ nhất, các tội phạm liên quan đến tài liệu khiêu dâm trẻ em: Theo Điều 9 Công ước, các tội phạm liên quan đến tài liệu khiêu dâm trẻ em là các hành vi của người không được phép, cố ý thực hiện một trong những hành vi sau: (a) sản xuất tài liệu khiêu dâm trẻ em để phát tán qua hệ thống máy tính; (b) đề nghị cung cấp hoặc cung cấp tài liệu khiêu dâm trẻ em qua hệ thống

máy tính; (c) phát tán hoặc truyền tải tài liệu khiêu dâm trẻ em qua hệ thống máy tính; (d) mua tài liệu khiêu dâm trẻ em cho mình hoặc cho người khác thông qua hệ thống máy tính; (e) sở hữu tài liệu khiêu dâm trẻ em trong hệ thống máy tính hoặc trong phương tiện lưu trữ dữ liệu máy tính. Theo đó, "tài liệu khiêu dâm trẻ em" bao gồm bất cứ tài liệu nào bằng hình ảnh mô tả người chưa thành niên thực hiện hành vi tình dục; người giống người chưa thành niên thực hiện hành vi tình dục; hình ảnh thực tế diễn tả người chưa thành niên thực hiện hành vi tình dục. Người chưa thành niên là người dưới 18 tuổi. Các quốc gia có thể quy định thấp hơn nhưng không dưới 16 tuổi. Để hạn chế phạm vi của các tội phạm này, Công ước cho phép các nước thành viên bảo lưu các điểm d, e khoản 1 và điểm b, c khoản 2 Điều 9 của Công ước. Theo đó, việc mua hoặc sở hữu tài liệu khiêu dâm trẻ em thông qua hệ thống máy tính không phải là tội phạm. Đồng thời, "tài liệu khiêu dâm trẻ em" không bao gồm hình ảnh về hành vi tình dục của người giống người chưa thành niên hoặc hình ảnh thực tế diễn tả hành vi tình dục của người chưa thành niên.

Thứ hai, các tội phân biệt chủng tộc hoặc bài ngoại thông qua hệ thống máy tính: Các tội phạm này được quy định trong Nghị định thư bổ sung Công ước Budapest năm 2003[81]. Theo Điều 3 của Nghị định thư, tội phân biệt chủng tộc hoặc bài ngoại thông qua hệ thống máy tính các hành vi của người không có thẩm quyền, cố ý phân phối hoặc phát tán các tài liệu phân biệt chủng tộc hoặc bài ngoại thông qua hệ thống máy tính. Trong đó, theo Điều 2 của Nghị định thư, "tài liệu phân biệt chủng tộc hoặc bài ngoại" là bất kỳ tài liệu viết, hình ảnh hoặc các hình thức thể hiện ý tưởng, học thuyết ủng hộ,

[81] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f (truy cập ngày 20/2/2020).

quảng bá, kích động thù hận, phân biệt, bạo lực chống lại cá nhân hoặc nhóm người dựa trên tiêu chí chủng tộc, mầu da, nguồn gốc, dân tộc, tôn giáo, các yếu tố khác.

** Nhóm các tội xâm phạm quyền tác giả và các quyền liên quan:*

Theo Điều 10 của Công ước, các tội xâm phạm quyền tác giả và các quyền liên quan là hành vi cố ý xâm phạm các quyền tác giả và các quyền liên quan theo quy định về quyền tác giả và quyền liên quan của quốc gia đó, phù hợp với công ước quốc tế về quyền tác giả và quyền liên quan, với quy mô lớn có ý nghĩa về thương mại thông qua hệ thống máy tính. Tuy nhiên, các quốc gia thành viên có thể bảo lưu quy định này nếu có các biện pháp hữu hiệu khác.

Ngoài bốn nhóm tội phạm trên, Công ước Budapest 2001 còn quy định là tội phạm các hành vi đồng phạm xúi giục hoặc giúp sức để thực hiện các tội phạm theo quy định từ Điều 2 đến Điều 10 của Công ước. Bên cạnh đó, Công ước cũng quy định các nước thành viên có thể quy định là tội phạm đối với hành vi phạm tội chưa đạt đối với các tội phạm theo quy định tại Điều 3 đến Điều 5, Điều 7, Điều 8 và Điều 9.1 a và c của Công ước.

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

Luật mẫu 2002 là văn bản quốc tế không có giá trị bắt buộc, nhưng các nước trong khối tham khảo để đưa vào luật của nước mình. 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 đây:

Thứ nhất, tội truy cập bất hợp pháp: Theo Điều 5, tội truy cập bất hợp pháp là hành vi của người không có thẩm quyền, cố ý truy cập vào một phần hoặc toàn bộ hệ thống máy tính. Theo đó, "hệ thống máy tính" là một thiết bị hoặc một nhóm các thiết bị có liên hệ với nhau, bao gồm Internet, thực hiện

quá trình xử lý dữ liệu một cách tự động hoặc thực hiện chức năng khác theo một chương trình. So với tội truy cập bất hợp pháp quy định trong Công ước Budapest 2001, tội truy cập bất hợp pháp trong Luật mẫu 2002 có sự tương đồng với nhau. Điểm khác của Công ước Budapest 2001 là cho phép các quốc gia thu hẹp phạm vi tội này bằng cách giải thích khái niệm "hệ thống máy tính" hẹp hơn (đã được phân tích ở trên).

Thứ hai, tội gây rối dữ liệu: Theo Điều 6, tội gây rối dữ liệu là hành vi của người không có thẩm quyền, cố ý thực hiện một trong các hành vi: (a) tiêu hủy hoặc thay đổi dữ liệu; (b) đưa ra các dữ liệu không có ý nghĩa, không có giá trị sử dụng hoặc không có hiệu lực; (c) cản trở, ngăn chặn hoặc gây rối người khác trong việc sử dụng hợp pháp dữ liệu; (d) từ chối tiếp cận dữ liệu đối với người có quyền tiếp cận dữ liệu. Nội hàm của tội gây rối dữ liệu theo Luật mẫu 2002 rộng hơn nội hàm của tội gây rối dữ liệu của Công ước Budapest 2001. Ngoài hành vi tiêu hủy hoặc thay đổi dữ liệu (giống như Công ước Budapest 2001), Luật mẫu 2002 còn quy định thêm các hành vi khác như: đưa ra các dữ liệu không có ý nghĩa, không có giá trị sử dụng hoặc không có hiệu lực; cản trở, ngăn chặn hoặc gây rối người khác trong việc sử dụng hợp pháp dữ liệu; từ chối tiếp cận dữ liệu đối với người có quyền tiếp cận dữ liệu.

Thứ ba, tội gây rối hệ thống máy tính: Theo Điều 7, tội gây rối hệ thống máy tính là hành vi của người không có thẩm quyền, cố ý thực hiện một trong các hành vi sau: (a) cản trở hoặc gây rối sự vận hành của một hệ thống máy tính; (b) cản trở hoặc gây rối người đang sử dụng hoặc vận hành hợp pháp một hệ thống máy tính. Trong đó, hành vi "cản trở" bao gồm nhiều loại hành vi khác nhau như: cắt nguồn cung cấp điện đối với hệ thống máy tính; tạo ra sự gây rối điện từ đối với hệ thống máy tính; làm hư hại hệ thống máy tính bằng bất cứ phương tiện nào; nạp, xóa hoặc thay đổi dữ liệu máy tính[82].

[82] Xem: khoản 2 Điều 7 Luật mẫu 2002.

Nội hàm của tội gây rối hệ thống máy tính theo quy định của Luật mẫu 2002 rộng hơn so với quy định của Công ước Budapest 2001 ở cả hai góc độ: (1) đối tượng của tội phạm gây rối hệ thống máy tính không chỉ là "hệ thống máy tính" mà còn có hành vi sử dụng bình thường của người sử dụng hoặc vận hành hệ thống máy tính; (2) thủ đoạn gây rối hệ thống máy tính hoặc hoạt động bình thường của người sử dụng hoặc vận hành hệ thống máy tính không chỉ bằng các biện pháp kỹ thuật máy tính như nạp, xóa hoặc thay đổi dữ liệu máy tính, mà còn bằng các biện pháp trực tiếp như: cắt nguồn cung cấp điện đối với hệ thống máy tính; tạo ra sự gây rối điện từ đối với hệ thống máy tính; làm hư hại hệ thống máy tính bằng bất cứ phương tiện nào.

Thứ tư, tội ngăn chặn bất hợp pháp dữ liệu: Theo Điều 8, tội ngăn chặn bất hợp pháp dữ liệu là hành vi của người không có thẩm quyền, cố ý ngăn chặn bằng các phương tiện kỹ thuật bất cứ sự truyền tải dữ liệu không công khai nào tới, từ hoặc trong một hệ thống máy tính; hoặc sự phát ra các tín hiệu điện từ mang dữ liệu từ hệ thống máy tính. Quy định này khá tương đồng với quy định của Công ước Budapest 2001, ngoại trừ việc Công ước Budapest 2001 cho phép các quốc gia thành viên có thể giới hạn phạm vi tội này chỉ đối với những hành vi ngăn chặn bất hợp pháp dữ liệu với ý định không trung thực hoặc có liên quan đến hệ thống máy tính được kết nối với hệ thống máy tính khác.

Thứ năm, tội lạm dụng các công cụ, thiết bị liên quan đến máy tính: Theo Điều 9, tội lạm dụng các công cụ, thiết bị liên quan đến máy tính là một trong các các hành vi: (1) cố ý hoặc vô ý, không có lý do hợp pháp mà sản xuất, bán, mời sử dụng, nhập khẩu, xuất khẩu, phân phối hoặc bằng các cách thức khác cung cấp: (i) thiết bị bao gồm chương trình máy tính được thiết kế hoặc được điều chỉnh để thực hiện hành vi phạm tội nêu tại Điều 5, 6, 7, 8 của Luật mẫu; (ii) mã số truy cập của máy tính, mật mã truy cập hoặc dữ liệu

tương tự mà nhờ mã số ấy toàn bộ hoặc một phần của hệ thống máy tính có thể được truy cập; (2) chiếm hữu các công cụ, thiết bị trên với ý định cho người khác sử dụng để thực hiện các hành vi phạm tội quy định tại Điều 5, 6, 7, 8 của Luật mẫu 2002. Được coi là chiếm hữu các công cụ, phương tiện với ý định cho người khác sử dụng để phạm tội khi chiếm hữu từ 2 đơn vị trở lên công cụ, phương tiện nêu tại mục (i) hoặc (ii). Có quan điểm cho rằng số lượng tối thiểu nêu trên nên quy định dưới dạng tùy nghi để các quốc gia cân nhắc quy định trong luật của nước mình[83].

Theo điểm a khoản 1 Điều 9 của Luật mẫu 2002, những hành vi lạm dụng công cụ, thiết bị liên quan đế máy tính, thực hiện với lỗi vô ý cũng bị coi là tội phạm. Đây là điểm khác so với Công ước Budapest 2001, cũng như đa số các văn bản pháp luật quốc tế khác. Bởi vì đa số các văn bản quốc tế quy định về tội phạm trong lĩnh vực CNTT, MVT đều có lỗi cố ý.

Thứ sáu, tội phạm liên quan đến tài liệu khiêu dâm trẻ em: Theo Điều 10, các tội liên quan đến tài liệu khiêu dâm trẻ em là hành vi cố ý phát hành bất hợp pháp tài liệu khiêu dâm trẻ em qua hệ thống máy tính hoặc sản xuất tài liệu khiêu dâm trẻ em để phát hành qua hệ thống máy tính hoặc sở hữu bất hợp pháp tài liệu khiêu dâm trẻ em trong hệ thống máy tính hoặc trong phương tiện lưu trữ dữ liệu máy tính. Trong đó, khái niệm "tài liệu khiêu dâm trẻ em" bao gồm bất cứ tài liệu nào bằng hình ảnh mô tả người chưa thành niên thực hiện hành vi tình dục, người giống người chưa thành niên thực hiện hành vi tình dục hoặc hình ảnh thực tế diễn tả người chưa thành niên thực hiện hành vi tình dục. Tuổi của người chưa thành niên do pháp luật quốc gia quy định. Hành vi "phát hành" tài liệu khiêu dâm trẻ em bao gồm các hành vi:

[83] Quan điểm này do Canada đề xuất thay thế cho khoản 3 Điều 9 Luật mẫu 2002.

(a) phân phối, truyền tải, phát tán, lưu hành, giao nhận, trưng bày, cho mượn, trao đổi, bán, chào bán, cho thuê, đề nghị cho thuê, đề nghị dưới hình thức khác, cung cấp dưới bất cứ cách thức nào, hoặc

(b) chiếm hữu, chiếm giữ hoặc kiểm soát để thực hiện hành vi nêu tại mục (a), hoặc in, chụp, nhân bản hoặc thực hiện bất kỳ hành vi nào khác với mục đích thực hiện hành vi tại mục (a).

Quy định này của Luật mẫu 2002 tương đồng với quy định của Công ước Budapest 2001. Có thể thấy Luật mẫu 2002 ra đời năm 2002, sau Công ước Budapest 2001 nên đã kế thừa và mở rộng nhiều phạm vi tội phạm trong lĩnh vực CNTT, MVT, bởi vì nhiều nước nằm trong Khối thịnh vương chung cũng tham gia Công ước Budapest năm 2001.

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

Nội dung Công ước không có quy định về khái niệm tội phạm mạng, mà chỉ quy định liệt kê những hành vi phạm tội trong lĩnh vực này tại Điều 29 và 30[84]. 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 (sau khi đã hết quyền truy cập vào hệ thống máy tính đó);

---

[84] Nguồn: https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (truy cập ngày 12/10/2019).

- Che giấu, làm sai lệch hoặc cố ý giấu, làm sai lệch chức năng của hệ thông 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;

Ngoài ra, Công ước khuyến khích các quốc gia thành viên thực hiện các quy định sau:

- Áp dụng các quy định cần thiết để các nhà cung cấp các sản phẩm thông tin truyền thông có chính sách đánh giá về các biện pháp an toàn và bảo mật đối với sản phẩm (bởi những chuyên gia độc lập và nhà nghiên cứu) và phát hiện ra các lỗ hổng bảo mật của sản phẩm, đưa ra các giải pháp để sửa chữa các lỗi đó cho khách hàng.

- Quy định là tội phạm đối với các hành vi sản xuất, bán, nhập khẩu, sở hữu, phổ biến, đề nghị, nhượng lại hoặc sửa chữa bất hợp pháp các thiết bị máy tính, chương trình hoặc bất kỳ công cụ hoặc dữ liệu được thiết kế hoặc sửa chữa lại để phạm tội hoặc vi phạm pháp luật hoặc sản xuất mật khẩu, mã truy cập hoặc các dữ liệu máy tính tương tự cho phép truy cập vào một phần hoặc toàn bộ hệ thống máy tính.

** Các tội phạm xâm hại dữ liệu máy tính, bao gồm:*

- 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. Trong trường hợp này, các quốc gia có thể chỉ coi là tội phạm với ý định gian dối hoặc không trung thực.

- 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, mầu 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, mầu 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, tống tiền, khủng bố và rửa tiền.

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

Các tội phạm công nghệ thông tin được Công ước quy định từ Điều 6 đến Điều 18, bao gồm:

Thứ nhất, tội truy cập bất hợp pháp (Điều 6): Truy cập bất hợp pháp là hành vi của người không có thẩm quyền đã truy cập hoặc kết nối với một phần hoặc toàn bộ thông tin dữ liệu hoặc thiết bị chứa thông tin dữ liệu. Hành vi bị coi là tội phạm nếu: (1) Truy cập bất hợp pháp dẫn đến xoá, thay đổi, làm sai lệch, thêm vào, di chuyển hoặc phá huỷ dữ liệu điện tử, thiết bị điện tử, hệ thống thiết bị điện tử, hệ thống mạng, gây thiệt hại cho người sử dụng hoặc người thụ hưởng; (2) Truy cập bất hợp pháp để thu thập thông tin bí mật của nhà nước.

Như vậy, đối với hành vi truy cập bất hợp pháp vào dữ liệu không phải là bí mất nhà nước chỉ bị coi là tội phạm khi có hậu quả thiệt hại xảy ra. Còn đối với truy cập bất hợp pháp để thu thập thông tin bí mật nhà nước thì chỉ cần có hành vi, không cần hậu quả xảy ra vẫn bị coi là tội phạm.

Thứ hai, tội can thiệp bất hợp pháp (Điều 7): Can thiệp bất hợp pháp là hành vi cố ý can thiệp bất hợp pháp sự di chuyển của thông tin dữ liệu bằng bất kỳ biện pháp kỹ thuật nào, làm gián đoạn sự truyền hoặc tiếp nhận thông tin dữ liệu. Theo quy định này, thủ đoạn người phạm tội sử dụng để can thiệp bất hợp pháp phải là biện pháp kỹ thuật, nghĩa là sử dụng CNTT, MVT để phạm tội. Trường hợp sử dụng các biện pháp phá huỷ trực tiếp như cắt đường truyền dữ liệu sẽ không bị coi là phạm tội này.

Thứ ba, tội xâm phạm tính toàn vẹn của dữ liệu (Điều 8): Xâm phạm tính toàn vẹn của dữ liệu điện tử là cố ý thực hiện bất hợp pháp hành vi phá huỷ, xoá, cản trở, thay đổi hoặc che giấu dữ liệu thông tin điện tử.

Theo quy định của điều luật này, hành vi xâm phạm tính toàn vẹn của dữ liệu thông tin điện tử bị coi là tội phạm khi có một trong các hành vi trên. Tuy nhiên, điều luật cũng cho phép các quốc gia thành viên quy định trong LHS của mình rằng, chỉ bị coi là tội phạm khi gây ra những hậu quả nhất định.

Thứ tư, tội lạm dụng công cụ, phần mềm dùng để phạm tội (Điều 9): Tội lạm dụng công cụ, phần mềm dùng để phạm tội là một trong các hành vi sau:

(1) Hành vi sản xuất, bán, mua, nhập khẩu, phân phối, cung cấp các đối tượng sau:

+ Tất cả các công cụ hoặc chương trình tin học được thiết kế hoặc được cải tiến nhằm mục đích làm công cụ để thực hiện các tội phạm quy định từ Điều 6 đến Điều 8 của Công ước này.

+ Thông tin mật khẩu của hệ thống, mật khẩu truy cập hoặc các thông tin tương tự cho phép truy cập vào hệ thống thông tin để thực hiện một trong số những tội phạm quy định từ Điều 6 đến Điều 8 của Công ước này.

(2) Có được công cụ hoặc chương trình tin học trên để sử dụng vào việc thực hiện một trong số những tội quy định tại Điều 6, 7, 8 của Công ước này.

Thứ năm, tội giả mạo (Điều 10): Tội giả mạo là hành vi sử dụng các biện pháp công nghệ thông tin để thay đổi dữ liệu thông tin điện tử thật thành thông tin dữ liệu giả, với ý thức sẽ sử dụng chúng như thật.

Thứ sáu, tội phạm lừa đảo (Điều 11): Tội phạm lừa đảo là hành vi cố ý và trái pháp luật gây thiệt hại cho người sử dụng hoặc người khác với mục đích lừa đảo để chiếm đoạt tài sản hoặc lợi ích vật chất cho mình hoặc người khác thông qua một trong các thủ đoạn sau: (1) Thêm vào, thay đổi, xoá hoặc che giấu thông tin và dữ liệu; (2) Can thiệp vào các chức năng hoạt động và

giao tiếp của hệ thống hoặc cố gắng phá huỷ hoặc thay đổi chúng; (3) Phá huỷ các phương tiện điện tử, chương trình tin học.

Thứ bảy, tội phạm về tài liệu khiêu dâm trẻ em (Điều 12): Tội phạm về tài liệu khiêu dâm trẻ em là các hành vi sử dụng công nghệ thông tin để sản xuất, trình diễn, phân phối, cung cấp, phát hành, mua, bán, nhập khẩu các tài liệu khiêu dâm trẻ em.

Thứ tám, tội phạm về đánh bạc và khai thác tình dục thông qua việc sử dụng CNTT, MVT (Điều 13).

Thứ chín, tội phạm xâm phạm quyền riêng tư (Điều 14): hành vi sử dụng CNTT, MVT để xâm phạm quyền riêng tư.

Thứ mười, tội phạm khủng bố thông qua CNTT, MVT (Điều 15): Tội khủng bố thông qua CNTT, MVT là việc sử dụng CNTT, MVT để thực hiện một trong các hành vi sau: (1) Phổ biến, truyên truyền các tư tưởng và quy tắc của các nhóm khủng bố; (2) Tài trợ và huấn luyện cho các hoạt động khủng bố, và tạo điều kiện liên lạc giữa các tổ chức khủng bố; (3) Phổ biến cách thức tạo ra chất nổ, đặc biệt là sử dụng thuốc nổ để thực hiện khủng bố; (4) Truyền bá chủ nghĩa cuồng tín tôn giáo và bất đồng chính kiến và tấn công các tôn giáo và tín ngưỡng.

Thứ mười một, tội phạm liên quan đến tổ chức phạm tội được thực hiện bằng công nghệ thông tin như: rửa tiền, buôn ma túy, buôn người, tổ chức buôn người, buôn vũ khí (Điều 16).

Thứ mười hai, tội phạm về quyền tác giả và các quyền liên quan thông qua công nghệ thông tin (Điều 17).

Thứ mười ba, tội sử dụng bất hợp pháp các công cụ thanh toán điện tử (Điều 18): Tội sử dụng bất hợp pháp các công cụ thanh toán điện tử bao gồm các hành vi sau: (1) Sử dụng, sản xuất hoặc giúp cho việc sử dụng bất hợp pháp các công cụ thanh toán điện tử; (2) Sở hữu và sử dụng bất hợp pháp

thông tin về công cụ thanh toán điện tử hoặc cung cấp cho người khác, giúp người khác sử dụng bất hợp pháp thông tin về công cụ thanh toán điện tử; (3) Sử dụng mạng máy tính hoặc công nghệ thông tin để truy cập bất hợp pháp vào tài khoản, dữ liệu của công cụ thanh toán điện tử; (4) Cố ý chấp nhận công cụ thanh toán điện tử giảo mạo.

Kết luận chương 1

Thông qua việc nghiên cứu những vấn đề chung về tội phạm trong lĩnh vực CNTT, MVT, có thể rút ra một số kết luận sau đây:

Thứ nhất, từ khi tội phạm liên quan đến CNTT, MVT ra đời cho đến nay, còn nhiều quan điểm khác nhau về khái niệm tội phạm này. Tuy nhiên, các quan điểm đều thống nhất rằng, CNTT, MVT có liên quan đến tội phạm này với vai trò là công cụ thực hiện tội phạm hoặc mục tiêu tấn công của tội phạm. Do đó, khái niệm tội phạm liên quan đến CNTT, MVT được định nghĩa như sau:

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 trong lĩnh vực CNTT, MVT có phạm vi hẹp hơn khái niệm tội phạm liên quan đến CNTT, MVT. Tội phạm trong lĩnh vực CNTT, MVT cũng sử dụng CNTT, MVT để thực hiện tội phạm hoặc tấn công không gian mạng. Tuy nhiên, tội phạm trong lĩnh vực CNTT, MVT chỉ xâm phạm sự an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. Trường hợp người phạm tội sử dụng CNTT, MVT để thực hiện tội phạm xâm phạm khách thể khác như an ninh quốc gia, xâm phạm an toàn công cộng, trật tự công cộng khác thì không được coi là tội phạm trong lĩnh vực CNTT, MVT. Trên cơ sở đó, Luận án rút ra kết luận 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.

Thứ hai, tội phạm trong lĩnh vực CNTT, MVT có những đặc điểm đặc trưng so với các nhóm tội phạm khác trong LHS. Những đặc điểm này bao gồm: (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.

Thứ ba, việc phân loại tội phạm trong lĩnh vực CNTT, MVT mang lại nhiều ý nghĩa. Có nhiều tiêu chí phân loại tội phạm trong lĩnh vực CNTT, MVT. Cụ thể: (1) Nếu dựa vào tính chất, mức độ nguy hiểm cho xã hội của hành vi phạm tội, tội phạm trong lĩnh vực CNTT, MVT được chia thành bốn loại, bao gồm: tội phạm ít nghiệm trọng, tội phạm nghiêm trọng, tội phạm rất nghiêm trọng và tội phạm đặc biệt nghiêm trọng. (2) Dựa vào vai trò của CNTT, MVT đối với tội phạm, tội phạm trong lĩnh vực CNTT, MVT được chia thành hai loại: tội phạm trong lĩnh vực CNTT, MVT trong đó mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử trở thành mục tiêu

tấn công của tội phạm; tội phạm trong lĩnh vực CNTT, MVT trong đó người phạm tội sử dụng CNTT, MVT thực hiện tội phạm trong môi trường không gian mạng. (3) Dựa vào vai trò của CNTT, MVT và mục đích phạm tội, tội phạm trong lĩnh vực CNTT, MVT được chia thành bốn loại, bao gồm: 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; tội phạm trong lĩnh vực CNTT, MVT trong đó người phạm tội có mục đích chiếm đoạt tài sản; 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; 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.

Thứ tư, trên cơ sở các kết luận trên có thể khẳng định tội phạm trong lĩnh vực CNTT, MVT là tội phạm mới. Chúng ta có đủ căn cứ lý luận và thực tiễn để quy định về tội phạm này trong BLHS.

Thứ năm, tội phạm trong lĩnh vực CNTT, MVT đã được nhiều văn bản quốc tế quy định như: Công ước Budapest 2001, Luật mẫu (2002, Công ước của các nước Châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân (2014), Công ước của các nước Ả - rập về chống tội phạm công nghệ thông tin. Mặc dù có nhiều điểm chung, nhưng phạm vi và nội dung của tội phạm trong lĩnh vực CNTT, MVT trong các văn bản này còn có nhiều điểm khác nhau.

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

Do bối cảnh kinh tế, xã hội ở Việt Nam những năm 80 của thế kỷ XX, CNTT, MVT chưa được ứng dụng phổ biến nên tội phạm trong lĩnh vực CNTT, MVT chưa xuất hiện. Do đó, BLHS năm 1985 không có quy định nào về tội phạm trong lĩnh vực CNTT, MVT. Khi soạn thảo, ban hành BLHS năm 1999, CNTT, MVT đã được sử dụng và áp dụng nhiều trong đời sống. Việc tiếp cận và sử dụng CNTT, MVT của cơ quan, tổ chức, cá nhân đã trở nên dễ dàng và phổ biến. Kéo theo đó, việc sử dụng CNTT, MVT để thực hiện tội phạm đã xuất hiện. Đó là những hành vi nguy hiểm, gây mất an toàn công cộng, xâm hại tài sản, quyền, lợi ích của cơ quan, tổ chức, quyền và lợi ích hợp pháp của cá nhân. Những hành vi này xuất hiện khá phổ biến và có xu hướng ngày càng tăng. Trong bối cảnh đó, BLHS năm 1999 đã quy định về tội phạm trong lĩnh vực CNTT, MVT tại Chương XIX (Các tội xâm phạm an toàn công cộng, trật tự công cộng), tại 3 điều luật là 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). Tuy nhiên theo quy định của BLHS năm 1999 những tội phạm này chưa được nhóm thành nhóm riêng, chưa được gọi là tội phạm trong lĩnh vực CNTT, MVT như hiện nay.

Theo quy định của BLHS năm 1999, khách thể loại của tội phạm trong

lĩnh vực CNTT, MVT là an toàn công cộng, trật tự công cộng. Bởi vì các điều 224, 225 và 226 đều thuộc Chương XIX (Các tội xâm phạm an toàn công cộng, trật tự công cộng) của BLHS năm 1999. Ngoài ra, ba điều luật này đều có khách thể trực tiếp là các quan hệ xã hội trong lĩnh vực CNTT, MVT, cho nên ba tội này có khách thể chung là an toàn công cộng, trật tự công cộng trong lĩnh vực CNTT, MVT. Như vậy, BLHS năm 1999 đã quy định phạm vi tội phạm trong lĩnh lực CNTT, MVT rất hẹp. Đây không chỉ là đặc điểm của tội phạm trong lĩnh vực CNTT, MVT khi mới ban hành BLHS năm 1999, mà các lần sửa đổi bổ sung sau và cả BLHS năm 2015 đều không thay đổi.

Theo quy định của BLHS năm 1999, tội phạm trong lĩnh vực CNTT, MVT bao gồm những tội sau đây:

Thứ nhất, tội tạo ra và lan truyền, phát tán các chương trình vi - rút tin học (Điều 224):

Tội tạo ra và lan truyền, phát tán các chương trình vi - rút được thực hiện bởi 2 hành vi, bao gồm hành vi tạo ra chương trình vi - rút và hành vi lan truyền hoặc phát tán chương trình vi - rút. Trong đó, chương trình vi - rút là một loại chương trình tin học có tính năng gây hại, có khả năng "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". Theo quy định, sau khi viết chương trình vi - rút, người phạm tội đã cố ý lan truyền hoặc phát tán chương trình vi - rút đó nhằm gây rối loạn hoạt động, phong tỏa, sao chép, làm biến dạng, huỷ hoại các dữ liệu của máy tính, thiết bị viễn thông, thiết bị số.

Việc quy định như vậy dẫn đến thu hẹp phạm vi xử lý hình sự đối với tội này, bởi vì người phạm tội phải trực tiếp tạo ra chương trình vi - rút, sau đó phát tán chương trình này mới bị coi là tội phạm. Nếu phát tán chương trình vi - rút không phải do mình tạo ra thì không bị coi là phạm tội này. Đây là điểm hạn chế của BLHS năm 1999. Sau 10 năm, hạn chế này được khắc

phục khi BLHS năm 2009 được sửa đổi, bổ sung vào năm 2009. Theo đó, tên tội danh được thay đổi 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). BLHS năm 1999 sửa đổi, bổ sung năm 2009 đã bỏ hành vi "tạo ra" chương trình vi - rút tin học, chỉ còn hành vi "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. Theo đó, chỉ cần có hành vi 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 gây thiệt hại về vật chất có giá trị từ 50 triệu đồng trở lên. Bên cạnh đó, BLHS năm 1999 sửa đổi, bổ sung năm 2009 cũng sửa đổi, bổ sung đối tượng phát tán là "chương trình vi - rút tin học" thành "Vi - rút, chương trình tin học có tính năng gây thiệt hại cho hoạt động của mạng máy tính, mạng viễn thông, thiết bị số". Bởi vì chương trình vi - rút tin học chỉ là một trong số nhiều chương trình tin học có tính năng gây thiệt hại khác. Ngoài ra, Điều 224 của BLHS năm 1999, sửa đổi bổ sung năm 2009 còn quy định cụ thể một số tình tiết tăng nặng như: phạm tội có tổ chức; gây thiệt hại về vật chất từ 200 triệu đồng đến dưới 500 triệu đồng; tái phạm nguy hiểm (khoản 2); phạm tội đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ an ninh, quốc phòng; đối với 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; gây thiệt hại vật chất từ 500 triệu đồng trở lên (khoản 3).

Thứ hai, tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử (Điều 225):

Hành vi khách quan của tội phạm là hành vi sử dụng mạng máy tính vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính gây rối

loạn hoạt động, phong tỏa hoặc làm biến dạng, làm hủy 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 "vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính" có phạm vi rất rộng bao gồm nhiều hành vi khác nhau dẫn đến hậu quả là "gây rối loạn hoạt động, phong tỏa hoặc làm biến dạng, làm hủy hoại các dữ liệu của máy tính" và cả những hành vi tuy không dẫn đến hậu quả này nhưng "đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm". Điều này dẫn đến có những hành vi không liên quan đến lĩnh vực CNTT, MVT cũng bị đưa vào hành vi khách quan của tội này. Đây cũng là một bất cập của BLHS năm 1999 đã được sửa đổi, bổ sung khắc phục vào năm 2009.

Theo BLHS năm 1999 sửa đổi, bổ sung năm 2009, Điều 225 đã được sửa đổi tên tội danh thành "tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số". Hành vi "vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử" được sửa thành hành vi "cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số". Sự thay đổi này không những thu hẹp phạm vi xử lý hình sự của Điều 225 mà còn phản ánh đúng bản chất của tội phạm này thông qua việc xác định chính xác hành vi khách quan của tội phạm. Theo đó, hành vi khách quan của tội phạm này gồm 3 hành vi sau: (1) tự ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu thiết bị số; (2) ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số; (3) hành vi khác cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số. Đó là hành vi cố ý của người không có quyền quản lý, vận hành, khai thác mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số làm ảnh hưởng đến hoạt động bình thường của mạng máy tính, mạng viễn thông, mạng Internet, thiết

bị số bằng việc đưa vào, truyền tải làm hư hỏng, xóa, làm suy giảm, thay thế hoặc nén dữ liệu máy tính, thiết bị viễn thông hoặc thiết bị số.

Thứ ba, tội sử dụng trái phép thông tin trên mạng và trong máy tính (Điều 226):

Hành vi khách quan của tội là hành vi sử dụng trái phép thông tin trên mạng và trong máy tính hoặc đưa vào mạng máy tính những thông tin trái với quy định của pháp luật gây hậu quả nghiêm trọng. Điều luật này được BLHS năm 1999, sửa đổi, bổ sung năm 2009 đổi tên tội danh thành "tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, mạng Internet". Theo đó, hành vi khách quan của tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, mạng Internet, bao gồm các hành vi sau: (1) đưa lên mạng máy tính, mạng viễn thông, mạng Internet những thông tin trái với quy định của pháp luật, nếu không thuộc trường hợp quy định tại Điều 88 và Điều 253 của BLHS năm 1999; (2) mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa những thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân khác trên mạng máy tính, mạng viễn thông, mạng Internet mà không được phép của chủ sở hữu thông tin đó; (3) hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, mạng Internet.

Lần đầu tiên tội phạm trong lĩnh vực CNTT, MVT được quy định trong BLHS năm 1999 còn khá đơn giản, còn nhiều điểm chưa hợp lý. Còn nhiều hành vi thuộc nhóm này chưa được quy định như: hành vi truy cập trái phép vào máy tính hoặc mạng máy tính, hành vi thay đổi cơ sở dữ liệu máy tính mà không được phép, hành vi cản trở trái phép hoạt động của máy tính, mạng máy tính, hành vi sử dụng, chiếm đoạt, mua bán hoặc công khai trái phép mã truy cập máy tính… Những thiếu sót, hạn chế này của BLHS năm 1999 sẽ phần nào được khắc phục, bổ sung trong các lần sửa đổi, bổ sung sau này.

2.1.2. Giai đoạn từ năm 2010 đến năm 2017

Sau 10 năm thực hiện, những biến đổi trong xã hội làm xuất hiện nhu cầu phải sửa đổi, bổ sung BLHS năm 1999. Theo Luật sửa đổi, bổ sung BLHS năm 1999 ngày 19/6/2009 có 44 điều luật được sửa đổi về nội dung hoặc sửa về kỹ thuật và bổ sung thêm 13 điều luật mới. Trong đó, quy định của BLHS năm 1999 về tội phạm trong lĩnh vực CNTT, MVT cũng được sửa đổi, bổ sung khá nhiều. Ngoài những sửa đổi, bổ sung trong các điều luật trên, BLHS năm 1999 còn được sửa đổi, bổ sung thêm các nội dung sau:

Thứ nhất, BLHS năm 1999, sửa đổi bổ sung năm 2009 đã quy định 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. Đây là quy định rất phù hợp với tình hình của Việt Nam lúc đó, cũng như phù hợp xu thế chung của thế giới. Mặc dù còn nhiều hành vi chưa được hình sự hóa, nhưng nói chung đến thời điểm này theo BLHS năm 1999, sửa đổi bổ sung năm 2009 đã khá đầy đủ.

Thứ hai, 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 như: "có tổ chức", "tái phạm nguy hiểm", "đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ an ninh, quốc phòng" (khoản 2 và 3 Điều 224); "Lợi dụng quyền quản trị mạng máy tính, mạng viễn thông, mạng Internet", "Đối với hệ thống dữ liệu thuộc bí mật nhà nước, hệ thống thông tin phục vụ an ninh quốc phòng", "Đối với 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" (khoản 2 và 3 Điều 225); "Lợi dụng quyền quản trị mạng máy tính, mạng viễn thông, mạng Internet", "Thu lợi bất chính từ một trăm triệu đồng

trở lên" (Điều 226). Cả ba điều luật này đều được sửa đổi theo hướng tăng nặng hình phạt tiền "từ năm triệu đồng đến một trăm triệu đồng" lên "từ hai mươi triệu đồng đến hai trăm triệu đồng" (khoản 1 Điều 224, và 225) và từ năm triệu đồng đến năm mươi triệu đồng lên "từ mười triệu đồng đến một trăm triệu đồng" (khoản 1 Điều 226). Hình phạt tiền là hình phạt bổ sung của Điều 224 và 225 không có sự sửa đổi so với luật cũ, nhưng hình phạt tiền là hình phạt bổ sung của Điều 226 đã nâng từ "3 triệu đồng đến 30 triệu đồng" lên "từ 20 triệu đồng đến 200 triệu đồng".

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. Cụ thể:

Thứ nhất, về cơ cấu, BLHS năm 2015 quy định riêng các tội trong lĩnh vực CNTT, MVT thành một mục riêng, bao gồm 9 điều luật trong Mục 2 (Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông) thuộc Chương XXI (Các tội xâm phạm an toàn công cộng, trật tự công cộng). Như vậy, lần đầu tiên BLHS năm 2015 đã quy định tên riêng cho nhóm tội này. Quy định này làm cho phạm vi các tội phạm trong lĩnh vực CNTT, MVT trong BLHS năm 2015 rõ ràng hơn.

Thứ hai, bổ sung thêm và cụ thể hóa 4 tội danh mới về tội phạm trong lĩnh vực CNTT, MVT xuất phát từ thực tiễn công tác đấu tranh, chống và phòng ngừa các tội phạm thời gian qua bao gồm: 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); Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291); 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); Tội cố ý gây nhiễu có hại (Điều 294). Những tội danh mới bổ sung này được quy định cụ thể về dấu hiệu hành vi, hậu quả thiệt hại tính toán được cũng như chế tài xử lý tương xứng với tính chất và hậu quả gây thiệt hại của người phạm tội.

Thứ ba, sửa đổi, bổ sung 5 tội danh về tội phạm trong lĩnh vực CNTT, MVT từ Điều 286 đến Điều 290 với việc bỏ dấu hiệu "gây hậu quả nghiêm trọng, rất nghiêm trọng, đặc biệt nghiêm trọng". Tuy nhiên, thực tế chưa xét xử được vụ nào, một phần là do bế tắc trong công tác giám định. Việc quy định cụ thể dấu hiệu hành vi và tính toán cụ thể hậu quả thiệt hại cụ thể (bằng số phút, số giờ; số tiền cụ thể…) giúp cho công tác phát hiện, điều tra, truy tố, xét xử được tiến hành nhanh chóng, kịp thời và chính xác hơn.

Thứ tư, tăng cường, mở rộng áp dụng chế tài phạt tiền là hình phạt chính áp dụng đối với nhóm tội phạm trong lĩnh vực CNTT, MVT thuộc trường hợp phạm tội ít nghiêm trọng (khung hình phạt đến 3 năm tù) hoặc nghiêm trọng (khung hình phạt từ trên 03 năm đến 07 năm tù) với mức phạt tiền thấp nhất là từ 20 triệu đồng đến mức cao nhất là 1,5 tỷ đồng. BLHS năm 2015 đã sửa đổi tăng mức phạt tiền là hình phạt bổ sung tại 8/9 tội danh; bổ sung thêm quy định "tịch thu một phần hoặc toàn bộ tài sản" do người phạm tội có được so với quy định trước đây.

Thứ năm, cụ thể hóa dấu hiệu hậu quả thiệt hại tại tất cả các tội danh qua các tình tiết tăng nặng TNHS như: Thu lợi bất chính, gây thiệt hại; Làm lây nhiễm phương tiện điện tử hoặc hệ thống thông tin; Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (theo số phút, giờ hoặc số lần truy cập trong thời gian 24 giờ; Làm đình trệ hoạt động của cơ quan, tổ chức (số giờ).

Thứ sáu, sửa đổi, bổ sung một số quy định mới về hậu quả thiệt hại tại khoản 2 liên quan đến "Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông" (Điều 288) xuất phát từ thực tiễn diễn biến phức tạp của loại tội phạm này thời gian qua cũng như hậu quả nguy hiểm do hành vi này mang lại như: Xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát; Gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội hoặc quan hệ đối ngoại của Việt Nam. Khoản 2 Điều 288 cũng bổ sung mức phạt tiền từ 200 triệu đồng đến 1 tỷ đồng đối với người phạm tội so với quy dịnh cũ nhằm tạo điều kiện cho người phạm tội khắc phục hậu quả thiệt hại do hành vi của mình gây ra.

Thứ bảy, sửa đổi, bổ sung một số quy định mới về "tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản" khi người phạm tội sử dụng mạng máy tính, mạng viễn thông hoặc phương tiện điện tử thực hiện những hành vi: Lừa đảo trong thanh toán điện tử, kinh doanh đa cấp hoặc thiết lập, cung cấp trái phép dịch vụ viễn thông, internet nhằm chiếm đoạt tài sản nhưng không thuộc trường hợp của tội trộm cắp tài sản và tội lừa đảo chiếm đoạt tài sản.

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

Theo lý luận khoa học LHS Việt Nam, mặt khách quan của tội phạm là mặt bên ngoài của tội phạm, bao gồm những biểu hiện của tội phạm diễn ra hoặc tồn tại bên ngoài thế giới khách quan như hành vi khách quan của tội phạm, hậu quả nguy hiểm cho xã hội, công cụ, phương tiện, phương pháp, thủ

đoạn, thời gian, địa điểm phạm tội[85]. 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 CNTT, MVT. Các yếu tố còn lại của mặt khách quan không phải là dấu hiệu bắt buộc trong mọi cấu thành tội phạm của tội này. Do tính chất phức tạp, đa dạng của tội phạm trong lĩnh vực CNTT, MVT, các dấu hiệu thuộc mặt khách quan của tội phạm sẽ được nghiên cứu theo 4 nhóm sau:

** 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. Hành vi khách quan của tội phạm có thể là từng hành vi riêng lẻ như sản xuất hoặc viết phần mềm hoặc mua bán hoặc trao đổi hoặc tặng cho, nhưng cũng có thể là một quá trình bao gồm nhiều hành vi như sản xuất, sau đó bán hoặc tặng cho người khác.

So với một số văn bản pháp luật quốc tế quy định về tội phạm này có thể thấy Điều 285 BLHS năm 2015 đã quy định khá đầy đủ các hành vi mang tính chất lạm dụng công cụ, thiết bị, phần mềm để sử dụng vào việc phạm tội. Tuy nhiên, còn một số hành vi khác chưa được quy định trong Điều 285 như hành vi chiếm hữu, sở hữu nhằm cho người khác sử dụng; đề nghị người khác

[85] Xem: Trường Đại học Luật Hà Nội (2015), *Giáo trình Luật hình sự Việt Nam*, NXB. Công an nhân dân, tr. 99.

sử dụng, nhập khẩu. Những hành vi nay đều đã được quy định trong các văn bản pháp luật quốc tế[86].

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. Các đối tượng này bao gồm cả phần cứng và phần mềm. Phần cứng như máy móc, các loại chíp điện tử để đọc dữ liệu thẻ, các thiết bị số dùng để thu, phát sóng, tín hiệu số hoặc phá sóng bất hợp pháp; các vi mạch, thiết bị ngoại vi, modul chương trình nhập số liệu bất hợp pháp; chương trình máy tính (vi - rút, phần mềm do thám), mã số truy cập của máy tính, mật mã truy cập hoặc dữ liệu tương tự để truy cập bất hợp pháp vào một phần hoặc toàn bộ hệ thống mạng máy tính, mạng viễn thông[87].

Đặc điểm chung của các đối tượng này là chúng đều có tính năng tấn công mạng máy tính, mạng viễn thông hoặc phương tiện điện tử. Các đối tượng trên có thể được sản xuất ra với mục đích để tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc được cải tiến để có được tính năng này.

(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. 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

---

[86] Ví dụ: Điều 6 Công ước Budapest 2001 và Điều 9 Luật mẫu 2002.

[87] Xem: Nguyễn Quý Khuyến (2017), "Tội sản xuất, mua bản, 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 theo BLHS năm 2015", *Tạp chí Toà án nhân dân*, số 1/2017.

mạng máy tính, mạng viễn thông, phương tiện điện tử[88]. 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.

Ví dụ: T là sinh viên một trường đại học tại Hà Nội, đã có hành vi phát tán vi - rút lây lan qua Yahoo, Messenger với tốc độ nhanh. Vi - rút này khi nhiễm vào một máy tính sẽ vừa gửi link nguy hại tới tất cả các nick YM trong list của người sử dụng, vừa đặt lại status (dòng trạng thái) của họ thành những câu bêu xấu lãnh đạo cơ quan, tổ chức khác và một số tin giật gân nhằm dễ dàng đánh lừa các nạn nhân như: "Thong Tin Ve Viec Dong Chi … Tham O Tien Bao Lut!! http://nh...vietnam.com"; "Su thuc ve moi lien quan giua Nam Cam va cac dong chi trong ... http://nh...vietnam.com"; "Doan DB Viet Nam sang My bi hanh hung boi Viet Kieu hai Ngoai... http://nh...vietnam.com".... Tiếp theo vi - rút sẽ thay đổi trang chủ của IE thành http://nh...vietnam.com và cấm không cho người sử dụng thay đổi lại trang chủ này.

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[89]. Chương trình tin học có tính năng gây hại được chia làm 2 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

---

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

[89] Xem: khoản 1 Điều 2 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012.

thông tin[90][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[91].

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 nếu thuộc một trong các trường hợp sau đây:

Thứ nhất, thu lợi bất chính từ 50 triệu đồng trở lên. Đó là trường hợp người phạm tội thu lợi ích bất hợp pháp từ việc phạm tội như phát tán chương trình tin học có tính năng gây hại, người phạm tội để có được thông tin có lợi (do sao chép, nghe lén), hoặc thông tin bị thay đổi có lợi cho người phạm tội hoặc mạng máy tính, mạng viễn thông, thiết bị điện tử của đối thủ cạnh tranh không hoạt động tạo ra lợi thế cho người phạm tội.

Thứ hai, gây thiệt hại từ 50 triệu đồng trở lên. Đó là trường hợp người phạm tội đã thực hiện hành vi phát tán chương trình tin học có tính năng gây hại, làm cho người sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử bị thiệt hại do phải khắc phục sự cố, ngừng hoạt động của cơ quan, tổ chức, mất dữ liệu. Tổng thiệt hại giá trị từ 50 triệu đồng trở lên.

Thứ ba, 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.

Thứ tư, 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. Trường hợp này, chỉ cần có hành vi, không cần gây ra hậu quả như trên vẫn bị coi là tội phạm.

---

[90] Xem: khoản 11 Điều 3 Luật an toàn thông tin mạng 2015.

[91] Xem: khoản 16 Điều 4 Luật công nghệ thông tin 2006.

(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 bao gồm 3 nhóm sau:

Thứ nhất, 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[92]. 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 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.

Các hành vi trên đều là hình thức tấn công chủ động đối với phần mềm, dữ liệu điện tử. Hình thức tấn công chủ động thường được thực hiện thông qua các hình thức như xóa, làm tổn hại phần mềm, dữ liệu điện tử; tấn công sửa đổi thông tin của dữ liệu điện tử (thông tin bị thay đổi, làm chậm trễ hoặc thay đổi trật tự để đạt được mục đích bất hợp pháp của kẻ tấn công); phá hủy thiết bị lưu trữ, phương tiện điện tử nếu đó phương tiện duy nhất lưu trữ dữ liệu điện tử. Sau khi dữ liệu, phần mềm bị xoá, bị làm tổn hại hoặc làm thay đổi mạng máy tính, mạng viễn thông, phương tiện điện tử sẽ ngừng, tạm ngừng hoạt động hoặc bị rối loạn.

Thứ hai, 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

[92] Xem: Khoản 1 Điều 7 Thông tư liên tịch 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012.

viễn thông, phương tiện điện tử bị gián đoạn, không thực hiện được hoặc không sử dụng được[93]. 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).

Thứ ba, 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 2 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 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC -TANDTC ngày 10/9/2012, "mạng máy tính là tập hợp nhiều

[93] Xem: khoản 2 Điều 7 Thông tư liên tịch 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012.

máy tính kết nối với nhau, có thể chia sẻ dữ liệu cho nhau." Còn theo khoản 10 Điều 3 Luật viễn thông, "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 11, 12 Điều 3 Luật viễn thông, MVT được chia làm 2 loại: (1) MVT công cộng là MVT 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) MVT 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 2 tội độc lập là tội cản trở trái phép dữ liệu máy tính và tội cản trở trái phép mạng máy tính[94]. Theo số liệu khảo sát quy định LHS của hơn 80 nước trên thế giới, có tới 70% số nước quy định tách riêng thành hai tội, chỉ có 22% số nước quy định chung trong một tội[95].

Theo khoản 1, 2, 3 Điều 7 Thông tư liên tịch số 10/2012/TTLT- BCA - BQP - BTP - BTT&TT - VKSNDTC - TANDTC ngày 10/9/2012, thủ đoạn thực hiện tội phạm này là các biện pháp mang tính công nghệ, kỹ thuật. Người phạm tội sử dụng CNTT, MVT 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). Trong khi đó, theo một kết quả nghiên cứu ở nước ngoài, có 50% số nước được khảo sát quy định việc thực hiện tội phạm này bằng các biện pháp mang tính

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

[95] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), Tlđd, tr. 88 - 89.

kỹ thuật, tức là sử dụng CNTT, MVT phạm tội[96] và 50% các nước quy định việc thực hiện tội phạm này bằng cả biện pháp kỹ thuật và biện pháp trực tiếp. Luật mẫu 2002 cũng quy định theo hướng bao gồm cả việc cản trở gây rối bằng biện pháp kỹ thuật và biện pháp phá huỷ ttrực tiếp[97]. Tuy nhiên, tác giả Luận án cho rằng, đặc điểm của tội phạm trong lĩnh vực CNTT, MVT là được thực hiện trong môi trường không gian mạng. Người phạm tội cần phải sử dụng các biện pháp mang tính kỹ thuật, CNTT, MVT mới có thể thực hiện trong môi trường này. Do đó, dấu hiệu bắt buộc của tội phạm này là người phạm tội phải sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để phạm tội. Nếu người phạm tội sử dụng các biện pháp đốt, phá trực tiếp sẽ xử lý về tội huỷ hoại tài sản hoặc tội phá huỷ công trình quan trọng về an ninh quốc gia tương ứng.

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

[96] Xem: Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), Tlđd, tr. 87 - 88.

[97] Xem: Điều 7 Luật mẫu 2002.

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 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 sau đây:

Thứ nhất, chiếm quyền điều khiển mạng máy tính, mạng viễn thông hoặc phương tiện điện tử. Sau khi xâm nhập vào mạng máy tính, mạng viễn thông, phương tiện điện tử, người phạm tội sẽ chiếm quyền điều khiển của mạng máy tính, mạng viễn thông hoặc phương tiện điện tử đó. Chiếm quyền sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử là việc người phạm tội vô hiệu hoá, khống chế quyền sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử của người có quyền, để sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử đó vào việc thực hiện những hành vi vi phạm pháp luật.

Ví dụ: tháng 7/2016, trang thông tin điện tử (website) của Hãng hàng không quốc gia Việt Nam bị tấn công chiếm quyền điều khiển. Người vi phạm đã xâm nhập trái phép chiếm quyền điều khiển. Màn hình điện tử tại sân bay Nội Bài đã bị cho hiển thị những nội dung thông tin xuyên tạc liên quan đến vấn đề biển Đông, xúc phạm Việt Nam, Philippines kèm theo những tiếng cười man dại[98].

Thứ hai, can thiệp vào chức năng hoạt động của phương tiện điện tử. Can thiệp vào chức năng hoạt động của phương tiện điện tử là những hành vi làm cho phương tiện điện tử không thể hoạt động bình thường. Để xử lý thông tin, các phương tiện điện tử thường có 4 chức năng hoạt động cơ bản[99]: (1)

---

[98] Xem: Thu Hà, "Hacker Trung Quốc gây sự cố tại sân bay Nội Bài, Tân Sơn Nhất": https://nld.com.vn/thoi-su-trong-nuoc/hacker-trung-quoc-gay-su-co-tai-san-bay-noi-bai-tan-son-nhat-20160729210104008.htm, (truy cập 14/2/2019)

[99] Xem: Đại học Nông lâm Huế (2017), *Giáo trình công nghệ thông tin cơ bản*, http://ciffl.huaf.edu.vn/uploads/page/giao_trinh_cntt.pdf (truy cập 02/2/2020)

Nhận thông tin (Receive input): thu nhận thông tin từ thế giới bên ngoài vào phương tiện điện tử. Đây là quá trình chuyển đổi các thông tin ở thế giới thực sang dạng biểu diễn thông tin trong phương tiện điện tử thông qua các thiết bị đầu vào. (2) *Xử lý thông tin (process information):* biến đổi, phân tích, tổng hợp, tra cứu... những thông tin ban đầu để có được những thông tin mong muốn. (3) *Xuất thông tin (produce output):* đưa các thông tin kết quả (đã qua xử lý) ra trở lại thế giới bên ngoài. Đây là quá trình ngược lại với quá trình ban đầu, phương tiện điện tử sẽ chuyển đổi các thông tin trong máy tính sang dạng thông tin ở thế giới thực thông qua các thiết bị đầu ra. (4) *Lưu trữ thông tin (store information):* ghi nhớ lại các thông tin đã được ghi nhận để có thể đem ra sử dụng trong những lần xử lý về sau. Người phạm tội có thể can thiệp vào bất cứ chức năng nào làm cho phương tiện điện tử đó hoạt động sai như can thiệp vào chức năng nhập thông tin bằng cách nhập vào thông tin sai lệnh để cho ra kết quả xử lý thông tin không đúng, như tăng thêm số ngày làm việc để được trả lương cao hơn; can thiệp để quá trình xử lý thông tin bị sai dẫn đến kết quả sai.

Ví dụ: Vụ Nguyễn Ngọc D, chuyên viên Phòng Đào tạo của một trường đại học đã truy cập vào cơ sở dữ liệu của trường để sửa điểm cho 42 sinh viên từ chưa đủ điều kiện tốt nghiệp thành tốt nghiệp, 14 sinh viên tốt nghiệp từ loại trung bình thành loại khá, 4 sinh viên tốt nghiệp sai điểm trung bình chung[100]. Như vậy, D đã có hành vi xâm nhập trái phép vào cơ sở dữ liệu của trường, sau đó can thiệp vào chức năng nhận thông tin (sửa điểm) của hệ thống quản lý điểm làm cho hệ thống xử lý thông tin sai.

Thứ ba, lấy cắp dữ liệu điện tử. Sau khi xâm nhập trái phép vào mạng

[100] Xem: Quốc Dũng, "Hack' hệ thống dữ liệu, nâng điểm cho 71 sinh viên": https://baotintuc.vn/phap-luat/hack-he-thong-du-lieu-nang-diem-cho-71-sinh-vien-20140825140005350.htm (truy cập ngày 20/2/2020).

máy tính, mạng viễn thông, phương tiện điện tử của nạn nhân, người phạm tội trộm cắp dữ liệu điện tử của mạng máy tính, mạng viễn thông, phương tiện điện tử đó. Trộm cắp dữ liệu được thực hiện bằng mọi thủ đoạn làm mất tính bí mật của dữ liệu điện tử như đọc trộm dữ liệu, nghe lén, sao chép trộm dữ liệu, … Ví dụ: Đối tượng T đã sử dụng phần mềm nghe lén theo dõi điện thoại di động để cài vào điện thoại cho khách hàng của mình. Sau khi khách hàng đưa điện thoại đó cho người sử dụng, tất cả những thông tin của người sử dụng như nội dung các cuộc gọi, danh bạ điện thoại, nội dung tin nhắn, định vị vị trí thiết bị, tự bật 3G, ra lệnh chụp hình từ xa… đều được ghi lại và gửi đến cho khách hàng mua phần mềm.

Thứ tư, thay đổi, huỷ hoại dữ liệu điện tử. Dữ liệu điện tử chỉ có giá trị khi có đầy đủ tính bí mật, tính toàn vẹn và tính sẵn sàng. Khi bị thay đổi hoặc huỷ hoại, dữ liệu điện tử sẽ mất đi tính toàn vẹn và không còn giá trị. Trường hợp này, sau khi xâm nhập trái phép mạng máy tính, mạng viễn thông, phương tiện điện tử, người phạm tội đã thay đổi, huỷ hoại làm mất đi tính toàn vẹn của dữ liệu điện tử của mạng máy tính, mạng viễn thông, phương tiện điện tử đó. Ví dụ: Vụ Tạ Thế L đã có hành vi "xâm nhập trái phép mạng máy tính, mạng viễn thông" như sau: trong thời gian khoảng tháng 1/2017, L sử dụng điện thoại cá nhân hiệu Oppo A3V xâm nhập trái phép vào mạng máy chủ của UBND huyện KB, tỉnh HN. Sau đó, L đã xóa một số lượng lớn văn bản, dữ liệu của các phòng ban thuộc UBND huyện này. Những văn bản, dữ liệu của chính quyền mà L xóa được xác định là rất khó, thậm chí là không thể khôi phục được[101].

Thứ năm, làm giả dữ liệu điện tử. Sau khi xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử, người phạm tội đã chèn vào

[101] Nguồn: https://vietnamnet.vn/vn/phap-luat/ho-so-vu-an/nam-thanh-nien-nghi-xam-nhap-xoa-sach-du-lieu-cua-ubnd-huyen-443941.html (truy cập ngày 22/2/2020).

đó các dữ liệu điện tử giả. Đây là hình thức tấn công nhằm vào tính xác thực của dữ liệu điện tử. Tính xác thực của thông tin, dữ liệu điện tử thể hiện ở chỗ thông tin, dữ liệu được gửi đi trong mạng máy tính hoặc mạng viễn thông phải do chính người gửi tạo ra. Nếu do người khác tạo ra và gửi đi trong mạng máy tính, mạng viễn thông sẽ tạo ra sự nhầm lẫn cho người nhận như nhận được cảnh báo sai lũ lụt, động đất, dịch bệnh, … dẫn đến hoảng loạn, sơ tán dân chúng.

Thứ sáu, sử dụng trái phép các dịch vụ. Người phạm tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử đang cung cấp các dịch vụ sử dụng có thu tiền để sử dụng trái phép các dịch vụ đó mà không phải trả tiền như: dịch vụ viễn thông, xem phim, nghe nhạc, mua vé, đặt hàng, …

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

Nhóm này chỉ có một tội là 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 (điểm a khoản 1 Điều 290 BLHS năm 2015). Tài khoản là bản ghi chép các giao dịch giữa các bên giao dịch[102]. Tài khoản ngân hàng là bản ghi chép các giao dịch giữa cá nhân, tổ chức với ngân hàng, được đăng ký tại ngân hàng, cho phép cá nhân, tổ chức gửi tiền vào để tiết kiệm hoặc thanh toán. Tài khoản ngân hàng thường được chia làm 2 loại là tài

[102] Xem: Nguyễn Văn Ngọc (2012), *Từ điển kinh tế học*, NXB. Đại học kinh tế quốc dân.

khoản tiền gửi không kỳ hạn (tài khoản vãng lai, tài khoản thanh toán) và tài khoản tiền gửi tiết kiệm có kỳ hạn. Thẻ ngân hàng là phương tiện thanh toán do tổ chức phát hành thẻ phát hành để thực hiện giao dịch thẻ theo các điều kiện và điều khoản được các bên thoả thuận. Thẻ ngân hàng bản chất là công cụ hỗ trợ khi cá nhân, tổ chức đăng ký mở tài khoản ngân hàng. Khi có thẻ ngân hàng, khách hàng có thể thực hiện các giao dịch chuyển tiền, rút tiền, thanh toán mà không cần phải đến quầy giao dịch của ngân hàng. Tuy nhiên, khi có tài khoản ngân hàng nếu không có thẻ ngân hàng khách hàng vẫn giao dịch được tại quầy giao dịch của ngân hàng.

Theo khoản 3,4 Điều 2 Nghị định 70/2000/NĐ-CP ngày 21/11/2000 của Chính phủ về việc giữ bí mật, lưu trữ và cung cấp các thông tin có liên quan đến tiền gửi và tài sản gửi của khách hàng, thông tin về tài khoản ngân hàng, thẻ ngân hàng gồm những thông tin liên quan đến tiền gửi của khách hàng (số hiệu tài khoản, mẫu chữ ký của chủ tài khoản hoặc người được chủ tài khoản uỷ quyền, các thông tin về doanh số hoạt động và số dư tài khoản); các thông tin liên quan đến giao dịch gửi, rút tiền, chuyển tiền và tài sản của khách hàng; nội dung các văn bản, giấy tờ, tài liệu; tên và mẫu chữ ký của người gửi tiền và tài sản; các thông tin khác như số thẻ, hiệu lực thẻ, mã số bảo vệ in trên mặt sau thẻ, mật khẩu giao dịch ngân hàng trực tuyến, mã PIN, mã số nhận thông tin và giao dịch về tiền gửi của khách hàng qua mạng máy tính[103].

Khi có thông tin tài khoản, thẻ ngân hàng của nạn nhân, người phạm tội sẽ sử dụng tài khoản, thẻ ngân hàng đó để chiếm đoạt tài sản của chủ tài khoản, chủ thẻ như rút tiền, chuyển tiền sang tài khoản khác hoặc thẻ ngân hàng khác hoặc thanh toán dịch vụ, mua hàng hóa mà người phạm tội sử dụng hoặc mua.

---

[103] Xem: Lê Đăng Doanh - Cao Thị Oanh (2017), *Bình luận khoa học BLHS năm 2015 (sửa đổi, bổ sung năm 2017)*, NXB. Hồng Đức, tr. 625.

Để có được thông tin tài khoản, thẻ ngân hàng của nạn nhân, người phạm tội có thể ngẫu nhiên biết được, trộm cắp thông tin, mua hoặc có được thông tin từ những người bán, cung cấp bất hợp pháp.

Ví dụ: H đã trộm cắp 01 thẻ ATM Shinhan Bank của chị O (cùng phòng trọ với nhau). Do biết được mật khẩu thẻ ATM của chị O, H đã dùng thẻ ATM trộm cắp được đến cây ATM để rút tiền. H đã rút được số tiền 2.250.000 đồng và chiếm đoạt số tiền này. Như vậy, H đã có hành vi sử dụng thẻ và mật khẩu thẻ ATM để chiếm đoạt số tiền trong tài khoản ngân hàng của nạn nhân. Hành vi của H bị Toà án kết án về tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản theo điểm a khoản 1 Điều 290 BLHS năm 2015[104].

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 (điểm b khoản 1 Điều 290 BLHS năm 2015). Thẻ ngân hàng là phương tiện thanh toán do tổ chức phát hành thẻ phát hành để thực hiện giao dịch thẻ theo các điều kiện và điều khoản được các bên thoả thuận. Thẻ ngân hàng bao gồm: thẻ ghi nợ, thẻ tín dụng, thẻ trả trước. Theo quy định của pháp luật, "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"[105]. Thẻ ngân hàng giả là thẻ không do tổ chức phát hành thẻ phát hành nhưng có chứa các thông tin của thẻ thật, chủ thẻ thật.

- Làm thẻ ngân hàng giả là hành vi cố ý của người không có thẩm quyền phát hành thẻ nhưng đã sản xuất, phát hành thẻ ngân hàng có chứa các thông tin của thẻ thật, chủ thẻ thật. Thủ đoạn sản xuất thẻ giả thường là người phạm tội mua hoặc đánh cắp thông tin về thẻ ngân hàng của người khác, sau

[104] Bản án số 59/2017/HSST ngày 28/9/2017 của TAND huyện Bình Xuyên, Vĩnh Phúc.

[105] Xem: điểm 6 Điều 2 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012.

đó dùng máy chuyên dụng để ghi thông tin thẻ ngân hàng vào dải băng từ của phôi thẻ ngân hàng trắng. Như vậy, người phạm tội đã làm ra được thẻ ngân hàng giả. Người phạm tội có thể thực hiện một hoặc tất cả các công đoạn của quá trình làm gia thẻ ngân hàng giả. Ví dụ: Năm 2011 Looi Hawshyan và A Phong người Malaysia đến Việt Nam. Sau khi đến Việt Nam, Looi HawShyan được A Phong hướng dẫn qua điện thoại cách sử dụng thiết bị làm thẻ ngân hàng giả. A Phong cho người có tên là Nun giao phôi thẻ đến Looi Hawshyan, sau 5 lần nhận tổng cộng khoảng từ 180-190 phôi thẻ do Nun giao. Sau khi nhận phôi thẻ, Looi HawShyan dùng thiết bị in dữ liệu vào thẻ (Dữ liệu do A Phong gửi vào email của Looi HawShyan). Kết quả Looi HawShyan đã làm được khoảng 175 thẻ ngân hàng giả, trong đó có 60 thẻ giả loại ATM, 115 thẻ giả loại Visa và Master. A Phong thỏa thuận chia cho Looi HawShyan hưởng 5% số tiền chiếm đoạt được và Looi HawShyan giao thẻ cho các đối tượng của A phong để thực hiện các giao dịch rút tiền và thanh toán hàng hóa, dịch vụ hàng trăm triệu đồng ở TP HCM.

- Tàng trữ, mua bán, sử dụng, lưu hành thẻ ngân hàng giả nhằm chiếm đoạt tài sản là hành vi của người biết rõ là thẻ ngân hàng giả nhưng vẫn cố ý tàng trữ, mua bán, sử dụng, lưu hành nhằm chiếm đoạt tài sản của người khác. Ví dụ: Hai đối tượng Tan Wei Hong và Choi quốc tịch Malaysia đã được một người quốc tịch Singgapore cung cấp cho 13 thẻ tín dụng giả để sử dụng. Theo thoả thuận nếu sử dụng thẻ ngân hàng giả, các đối tượng này sẽ được hưởng 30% giá trị tiền theo hoá đơn mua hàng. Hai đối tượng này đã sử dụng thẻ tín dụng giả trên để mua sắm hàng hoá, thanh toán vé máy bay, ăn, ở trong Khách sạn Metropol tại TP. Hồ Chí Minh trước khi bị bắt giữ. Hành vi của Tan Wei Hong và Choi là hành vi sử dụng thẻ ngân hàng giả.

Thứ ba, truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản (điểm c khoản 1 Điều 290 BLHS năm 2015):

Tài khoản của cơ quan, tổ chức, cá nhân bao gồm: tài khoản ngân hàng; tài khoản các mạng xã hội như Facebook, Zalo, email…

Hành vi truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản là hành vi vượt qua cảnh báo, mã truy cập, tường lửa, sử dụng quyền quản trị của người khác hoặc các phương thức khác truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản của người khác. Mục đích chiếm đoạt tài sản của người khác có thể là truy cập bất hợp pháp vào tài khoản ngân hàng của nạn nhân để rút tiền, chuyển tiền sang tài khoản khác; sử dụng tài khoản để lừa đảo chiếm đoạt tiền của người khác. Mục đích chiếm đoạt tài sản là điểm để phân biệt giữa hành vi truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản (Điều 290) với hành vi xâm nhập trái phép mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 289).

Ví dụ: H đã lừa chị L cung cấp tên đăng nhập và mật khẩu Facbook của mình cho H. Sau đó, H truy cập vào tài khoản Facebook của chị L, đổi mật khẩu để chiếm quyền sử dụng. H sử dụng tài khoản Facebooke của chị L gửi tin nhắn cho các tài khoản Facebook trong danh sách bạn bè của chị L với nội dung đang thiếu tiền, cần nhờ mua thẻ điện thoại để giải quyết công việc. Tưởng là tin nhắn của chị L, một số người bạn của chị đã mua các thẻ cào điện thoại di động của các nhà mạng, cào mã thẻ, chụp ảnh mã thẻ và số seri thẻ gửi qua facbook cho H. Sau khi nhận được mã thẻ cào điện thoại gửi đến, H đã chiếm đoạt và nạp vào tài khoản game của mình để chơi bài Rikvip. Tổng số tiền H chiếm đoạt của 3 nạn nhân là trên 3,5 triệu đồng. Như vậy, H đã có hành vi truy cập trái phép vào tài khoản facbook của chị L, sau đó sử dụng tài khoản này để chiếm đoạt tài sản của người khác. H đã bị Toà án kết án về tội sử dụng mạng internet chiếm đoạt tài sản của người khác[106].

[106] Bản án số 97/2017/HSST ngày 25/12/2017 của TAND huyện Đan Phương, TP. Hà Nội.

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 (điểm d khoản 1 Điều 290 BLHS năm 2015). Trong nhóm hành vi này, người phạm tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để lừa đảo nhằm chiếm đoạt tài sản của người khác thuộc một trong 5 lĩnh vực sau:

(1) Lừa đảo trong lĩnh vực thương mại điện tử:

Theo khoản 1 Điều 3 Nghị định 52/2013/NĐ-CP ngày 15/5/2013 về thương mại điện tử, hoạt động thương mại điện tử là việc tiến hành một phần hoặc toàn bộ quy trình của hoạt động thương mại bằng phương tiện điện tử có kết nối với mạng internet, mạng viễn thông di động hoặc các mạng mở khác. Lợi dụng đặc điểm của thương mại điện tử là người mua và người bán không trực tiếp gặp nhau và người mua phải trả tiền trước, người bán thường chào hàng không đúng với hàng được giao về số lượng, chất lượng, mẫu mã, chủng loại hoặc không giao hàng sau khi đã nhận tiền. Sau khi nhận được tiền, chúng nhanh chóng rút tiền và cắt đứt liên lạc trước khi bị phát hiện. Ví dụ: B đã có hành vi lừa đảo qua mạng internet bằng hình thức đăng quảng cáo trên mạng và giao bán đồ gia dụng như sau: khi có khách hàng mua, B yêu cầu đặt cọc nhưng sau đó không giao hàng, không trả lại tiền, cắt đứt liên lạc để chiếm đoạt tài sản của bị hại. Với thủ đoạn này, B đã lừa đảo 3 người, chiếm đoạt hơn 170 triệu đồng. Hành vi của B là hành vi sử dụng công nghệ thông tin lừa đảo trong thương mại điện tử. Với hành vi này, B đã bị Toà án kết án về tội sử dụng mạng internet chiếm đoạt tài sản của người khác[107].

(2) Lừa đảo trong thanh toán điện tử:

Theo cách hiểu chung, thanh toán điện tử là thanh toán tiền thông qua các thông điệp điện tử thay cho việc dùng tiền mặt hoặc séc trực tiếp hoặc qua

[107] Bản án số 701/2017/HS-PT ngày 22/9/2017 của TAND thành phố Hà Nội.

đường bưu điện khi mua hàng hóa hoặc sử dụng dịch vụ. Thủ đoạn phạm tội thường là đưa ra thông tin gian dối để nạn nhân tin là thật mà cung cấp thông tin về các công cụ thanh toán điện tử như: tên đăng nhập, mật khẩu truy cập, mật khẩu giao dịch (OTP). Sau đó người phạm tội sử dụng các thông tin trên truy cập vào tài khoản của các công cụ thanh toán để chiếm đoạt tài sản của nạn nhân bằng cách rút tiền, chuyển tiền sang tài khoản khác hoặc thanh toán các hàng hoá, dịch vụ mà người phạm tội đã mua, sử dụng. Hành vi lừa đảo trong thanh toán điện tử nhằm chiếm đoạt tài sản là những hành vi đưa ra thông tin gian dối làm cho người sử dụng các công cụ thanh toán điện tử nhầm lẫn mà cung cấp thông tin như thông tin đăng nhập, mật khẩu truy cập, mật khẩu giao dịch (OTP) của các công cụ thanh toán điện tử đó, nhằm chiếm đoạt tài sản.

Ví dụ: D truy cập vào web wix.com để mở tài khoản sử dụng có tên là transfermoney.wix.com trong đó có các mục như: tên ngân hàng, chủ thẻ, dãy số in trên thẻ, hiệu lực thẻ… Mục đích của D là khi bị hại vào trang web sẽ bị lừa để lại thông tin cá nhân của mình. D sẽ sử dụng những thông tin này để truy cập vào tài khoản của nạn nhân rút tiền qua dịch vụ internet banking. Sau đó, D chiếm đoạt quyền sử dụng của tài khoản Facebook của những người Việt Nam ở nước ngoài, mạo danh trò chuyện với người thân của họ đề nghị mượn số tài khoản ngân hàng để chuyển tiền từ nước ngoài về Việt Nam. D truy cập vào trang web http://www.vianett.com để đăng ký tin nhắn miễn phí có mã vùng nước ngoài rồi nhắn tin vào số điện thoại của người bị hại với nội dung “tài khoản của bạn đã nhận được tiền từ một tài khoản ở nước ngoài chuyển đến”; đồng thời cung cấp một đường link do D lập để người bị hại truy cập, điền các thông tin tài khoản ngân hàng để nhận tiền (những thông tin này thực chất sẽ được chuyển về cho D). D sử dụng các thông tin tài khoản ngân hàng của nạn nhân để truy cập vào tài khoản, chuyển tiền đến tài khoản ví điện tử của D. Sau đó, D tiếp tục trò chuyện với nạn nhân yêu cầu nhập mã

OTP gửi về điện thoại của chủ tài khoản (nạn nhân) để hoàn tất việc chuyển tiền. Sau khi có mã OTP của nạn nhân D nhập mã và hoàn tất chuyển tiền từ tài khoản của nạn nhân sang tài khoản của D. Với thủ đoạn này, D đã chiếm đoạt tài sản của 3 nạn nhân với tổng số tiền là 274 triệu đồng. Với các hành vi trên D bị Toà án kết án về tội sử dụng mạng internet thực hiện hành vi chiếm đoạt tài sản[108].

(3) Lừa đảo trong lĩnh vực kinh doanh tiền tệ, huy động vốn:

Thông qua mạng máy tính, mạng viễn thông, phương tiện điện tử, bằng thủ đoạn đưa ra thông tin gian dối trong kinh doanh tiền tệ, huy động vốn như hứa hẹn lãi suất cao, lợi nhuận lớn để khách hàng tin tưởng giao tài sản, nộp tiền cho mình, sau đó chiếm đoạt các tài sản đó. Ví dụ: T và V bàn bạc thống nhất với nhau thuê người lập website ảo, vận động nhiều người tham gia đầu tư tài chính có lãi suất cao để lừa đảo chiếm đoạt tiền. Hai đối tượng đã đưa ra thông tin website này có trụ sở hoạt động tại Campuchia, chuyên kinh doanh lĩnh vực sòng bài, vũ trường, du lịch…cần huy động vốn lớn, lợi nhuận cao. Nhiều người đã tin tưởng và gửi tiền góp vốn cho 2 đối tượng trên với số tiền là 7,1 tỷ đồng. Hai đối tượng trên đã chiếm đoạt số tiền trên của các nạn nhân. Như vậy, các đối tượng đã lập ra trang web giả để huy động vốn đầu tư, sau đó chiếm đoạt số vốn góp của các bị hại. Hai đối tượng đã bị Toà án kết án về tội sử dụng mạng máy tính thực hiện hành vi chiếm đoạt tài sản[109].

(4) Lừa đảo trong kinh doanh đa cấp:

Theo khoản 1 Điều 3 Nghị định 40/2018/NĐ-CP ngày 12/3/2018 của Chính phủ quy định về hoạt động kinh doanh đa cấp, kinh doanh theo phương thức đa cấp là hoạt động kinh doanh sử dụng mạng lưới người tham gia gồm nhiều cấp, nhiều nhánh, trong đó, người tham gia được hưởng hoa hồng, tiền thưởng và lợi ích kinh tế khác từ kết quả kinh doanh của mình và của những

[108] Bản án số 41/2017/HS-ST ngày 27/12/2017 của TAND tỉnh Quảng Trị

[109] Bản án số 169/2018/HS-PT ngày 17/4/2018 của TAND cấp cao tại TP. Hồ Chí Minh.

người khác trong mạng lưới. Người phạm tội sử dụng CNTT, MVT để thực hiện hành vi gian dối trong việc tuyển người vào hệ thống bán hàng đa cấp, bán hàng hoá theo mô hình đa cấp hoặc trả thưởng với lời hứa sẽ được hưởng hoa hồng, tiền thưởng hoặc lãi suất cao. Sau khi người tham gia mạng lưới bán hàng đa cấp nộp tiền, mua hàng để tham gia hệ thống, đối tượng sẽ chiếm đoạt tài sản đó. Ví dụ: H đã sử dụng thủ đoạn gian dối lập ra 3 website giao dịch thương mại điện tử gồm giaodichtructuyen.com.vn, nhadattay thanh. com.vn và vionline.com.vn để bán các gian hàng thương mại điện tử, kinh doanh bất động sản để hoạt động kinh doanh đa cấp không có giấy phép. Mặc dù không có gian hàng hoá để bán nhưng H đã đưa ra thông tin sai về hàng hoá và khả năng sinh lợi cao và các phần thưởng có giá trị để tạo niềm tin cho người bị hại đóng tiền tham gia. Với mô hình bán hàng đa cấp H đã bán cho khoảng 1800 người trên 20 tỉnh, thành phố trong cả nước, với số tiền trên 50 tỷ đồng. Qua đó chiếm đoạt của 245 bị hại số tiền hơn 5 tỷ đồng[110].

(5) Lừa đảo trong giao dịch chứng khoán:

Theo quy định của Luật chứng khoán (2006), "Chứng khoán là bằng chứng xác nhận quyền và lợi ích hợp pháp của người sở hữu đối với tài sản hoặc phần vốn của tổ chức phát hành. Chứng khoán được thể hiện dưới hình thức chứng chỉ, bút toán ghi sổ hoặc dữ liệu điện tử, bao gồm các loại sau đây: cổ phiếu, trái phiếu, chứng chỉ quỹ; quyền mua cổ phần, chứng quyền, quyền chọn mua, quyền chọn bán, hợp đồng tương lai, nhóm chứng khoán hoặc chỉ số chứng khoán"[111]. Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử lừa đảo trong giao dịch chứng khoán là hành vi sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện việc lừa đảo trong việc mua bán hoặc thanh toán các chứng khoán. Thủ đoạn phạm tội thường là sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử làm

[110] Bản án số 245/2018/HS-PT ngày 23/4/2018 của TAND cấp cao tại TP. Hồ Chí Minh.

[111] Xem: khoản 1 Điều 6 Luật chứng khoán 2006.

ra chứng khoán giả để bán hoặc hứa trả lợi nhuận cao để huy động vốn đầu tư chứng khoán sau đó chiếm đoạt vốn[112] hoặc dụ người mua cổ phiếu chuyển tiền đến tài khoản ngân hàng trung gian để chuyển cho Công ty chứng khoán nhưng thực chất là tài khoản của đối tượng lừa đảo và các đối tượng đã chiếm đoạt số tiền trên.

Thứ năm, thiết lập, cung cấp trái phép dịch vụ viễn thông, internet nhằm chiếm đoạt tài sản (điểm đ khoản 1 Điều 290 BLHS năm 2015). Thiết lập, cung cấp trái phép dịch vụ viễn thông, internet nhằm chiếm đoạt tài sản là hành vi 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. Thực tế đã xảy ra nhiều trường hợp này, nhưng BLHS năm 1999 chưa có quy định cụ thể, do đó còn nhiều quan điểm khác nhau. Các Toà án thường sử vào tội trộm cắp tài sản, nhưng có cho rằng nên xử về tội kinh doanh trái phép[113]. Việc quy định hành vi này trong Điều 290 BLHS năm 2015 đã giải quyết được những vướng mắc trong thực tiễn xử lý hình sự hành vi này. Hành vi phạm tội có thể được thực hiện bằng một trong hai thủ đoạn sau[114]:

Một là, người phạm tội sử dụng kỹ thuật VSAT (thiết bị đầu cuối khẩu độ nhỏ - very small aperture terminall) chiếm đoạt cước viễn thông. Người

---

[112] Xem: Nhật Minh, "Hai chiêu lừa phổ biến trên thị trường chứng khoán", https://vnexpress.net/kinh-doanh/2-chieu-lua-pho-bien-tren-thi-truong-chung-khoan-2715571.html (truy cập ngày 25/2/2019).

[113] Xem: Trần Vũ Hải (2004), "Lắp đặt, sử dụng thiết bị viễn thông để thu lợi cước điện thoại trái phép- Có thể bị truy tố về tội kinh doanh trái phép", *Tạp chí Tòa án nhân dân*, số 22 (tháng 11/2004).

[114] Xem: Nguyễn Quý Khuyến (2020), "Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản theo BLHS năm 2015", *Tạp chí Kiểm sát*, số 9/2020.

phạm tội sử dụng thiết bị thu phát tín hiệu qua vệ tinh để chuyển cuộc gọi ra nước ngoài bất hợp pháp. Với thiết bị là một ăng-ten parabol và một thiết bị xử lý tín hiệu chuyển đổi, các cuộc đàm thoại quốc tế sẽ giống như cuộc gọi trong nước. Do đó, người phạm tội chỉ phải thanh toán cước điện thoại trong nước thay vì phải thanh toán cước điện thoại quốc tế. Qua đó, chiếm đoạt được khoản tiền cước chênh lệch. Trước đây, người phạm tội hay sử dụng thủ đoạn này, nhưng do dễ bị phát hiện nên hiện nay ít sử dụng.

Ví du: tháng 12/1999, Chan Yiu Wah Bosco, quốc tịch Anh, ký hợp đồng với bà Mai Thị Khánh (Giám đốc kiêm Chủ tịch HĐQT Công ty cổ phần Hữu Nghị, trụ sở đặt tại 23 Quán Thánh, quận Ba Đình), thuê 8 phòng ngủ trên tầng 5. Bosco đã tổ chức lắp đặt trái phép hệ thống ăngten Parabol có đường kính 3,6 mét cùng nhiều phương tiện, máy móc thiết bị khác để thiết lập hoàn chỉnh trạm VSAT. Từ tháng 12/1999 đến tháng 5/2000, đối tượng đã chiếm đoạt được trên 15 tỷ đồng[115].

Hai là, sử dụng bất hợp pháp đường truyền internet để chiếm đoạt cước viễn thông. Thông thường, các cuộc gọi quốc tế được truyền qua mạng internet về Việt Nam sẽ được Công ty viễn thông quốc tế Việt Nam (VTI) dùng thiết bị ghép nối kênh PHS để kết nối với các máy điện thoại cố định hoặc thẻ SIM điện thoại di động trong nước và ngược lại. Người gọi phải trả cước viễn thông tính theo cuộc gọi, thời gian gọi, thường là mất nhiều tiền. Người sử dụng cũng có thể lập mạng viễn thông nội bộ bằng cách thuê kênh riêng của các nhà cung cấp hạ tầng mạng để lập ra mạng nội bộ để liên lạc với nhau trong phạm vi mạng nội bộ. Người sử dụng chỉ phải trả phí internet theo gói dữ liệu nên dẻ hơn nhiều so với cước viễn thông. Tuy nhiên, người sử dụng chỉ được phép liên lạc với nhau trong phạm vi mạng nội bộ, không được

[115] Nguồn: https://nld.com.vn/phap-luat/xet-xu-vu-trom-cap-cuoc-vien-thong-lon-nhat-tu-truoc-toi-nay-222158.htm (truy cập 10/2/2020).

kết nối với mạng điện thoại công cộng. Thủ đoạn người phạm tội sử dụng là thuê một kênh nội bộ, sau đó bí mật sử dụng bất hợp pháp thiết bị ghép nối kênh PHS để từ mạng nội bộ có thể liên lạc trực tiếp với mạng điện thoại công cộng bằng điện thoại cố định hoặc thẻ SIM điện thoại di động. Khi gọi điện thoại quốc tế, thay vì phải trả cước viễn thông quốc tế có chi phí cao, đối tượng chỉ phải trả tiền thuê kênh nội bộ có phí internet dẻ. Qua đó, người phạm tội chiếm đoạt được khoản tiền cước phí viễn thông quốc tế. Thủ đoạn này hiện nay đang được sử dụng phổ biến hơn kỹ thuật VSAT, vì khó phát hiện.

Ví dụ: Hai đối tượng Nong Wei Jie và Su Yong Rui đã lắp đặt hệ thống mạng viễn thông quốc tế tại khu đô thị Thanh Xuân, Hà Nội để chiếm đoạt cước viễn thông. Các đối tượng này đã thuê đường internet cáp quang có tốc độ đường truyền rất cao (FTTH, tốc độ 10 Gb/giây) của Công ty viễn thông FPT và Viễn thông Hà Nội. Sau đó sử dụng khoảng 6.700 SIM điện thoại di động của mạng Viettel dùng để kết nối vào mạng viễn thông của Việt Nam. Các đối tượng đã thực hiện các cuộc gọi quốc tế nhưng chỉ phải trả chi phí rất thấp (thuê đường internet), qua đó chiếm đoạt tiền cước viễn thông quốc tế[116].

Theo quy định tại khoản 1 Điều 290, các hành vi trên chỉ được xác định là Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản nếu "không thuộc trường hợp quy định tại Điều 173 và Điều 174" của BLHS năm 2015.

** 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):

---

[116] Trường Sơn, "Tội phạm Trung Quốc trộm cắp cước viễn thông ở Hà Nội": https://thanhnien.vn/thoi-su/phap-luat/toi-pham-trung-quoc-trom-cuoc-vien-thong-o-ha-noi-267710.html (truy cập ngày 20/3/2020).

Hành vi khách quan của tội phạm thuộc một trong các trường hợp sau:

Thứ nhất, hành vi 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. Thủ đoạn phạm tội thường là tạo ra một trang thông tin điện tử có chứa thông tin trái pháp luật, đưa trang thông tin điện tử đó lên internet; sử dụng các trang mạng xã hội như facebook, zalo… để đăng tải hoặc chia sẻ, bình luận về những thông tin trái quy định của pháp luật.

Đối tượng tác động của tội phạm là những thông tin trái với quy định của pháp luật. Đó là những thông tin mà theo quy định của pháp luật, không được đưa lên mạng máy tính, mạng viễn thông. Phạm vi những thông tin này rất rộng, được quy định ở trong nhiều quy định khác nhau. Theo Luật an ninh mạng, những thông tin này có thể là những thông tin nhằm xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; thông tin nhằm xúi giục, lôi kéo, kích động người khác phạm tội[117]; Trong đó, thông tin có nội dung xâm phạm trật tự quản lý kinh tế bao gồm: thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán[118].

[117] Xem: khoản 1 Điều 8 Luật an ninh mạng 2018.

[118] Xem: khoản 4 Điều 16 Luật an ninh mạng 2018.

Theo khoản 1 Điều 288 BLHS năm 2015, đối tượng tác động của tội phạm này không bao gồm các thông tin cấu thành các tội phạm tương ứng như: (1) thông tin, tài liệu 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 (Điều 117 BLHS năm 2015); (2) thông tin xúc phạm nghiêm trọng nhân phẩm, danh dự của người khác (Điều 155 BLHS năm 2015); (3) thông tin bịa đặt nhằm xúc phạm nghiêm trọng danh dự, nhân phẩm người khác hoặc tố cáo người khác phạm tội với cơ quan nhà nước (Điều 156 BLHS năm 2015); (4) thông tin liên quan đến văn hóa phẩm đồi trụy (Điều 326 BLHS năm 2015).

Thứ hai, 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. Đối tượng tác động của tội phạm là "thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân". Hiện nay chưa có khái niệm cụ thể về "thông tin riêng hợp pháp", chỉ có một số văn bản quy định về những nội dung có liên quan như: khoản 4 Điều 6 Luật viễn thông (2009); điểm a khoản 2 Điều 72 Luật công nghệ thông tin (2006); khoản 16 Điều 3 Nghị định 72/2013/NĐ-CP ngày 15/7/2013 quy định về quản lý, cung cấp và sử dụng dịch vụ internet và thông tin trên mạng; khoản 14, 15 Điều 3 Nghị định 72/2013/NĐ-CP ngày 15/7/2013 quy định về quản lý, cung cấp và sử dụng dịch vụ internet và thông tin trên mạng, thông tin công.

Thứ ba, hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông. Các hành vi này bao gồm nhiều loại khác nhau như 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; sử dụng thông tin giả. Đối tượng tác động của

tội phạm là thông tin điện tử trên mạng máy tính, mạng viễn thông về các lĩnh vực nói chung.

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. Đó là hành vi của người không có thẩm quyền nhưng đã cố ý thu thập, tàng trữ, trao đổi, mua bán, công khai hoá thông tin về tài khoản ngân hàng của người khác mà không được sự cho phép của chủ tài khoản ngân hàng đó.

Đối tượng tác động của tội phạm là "thông tin tài khoản ngân hàng". Đó là những thông tin liên quan đến tiền gửi của khách hàng (số hiệu tài khoản, mẫu chữ ký của chủ tài khoản hoặc người được chủ tài khoản uỷ quyền, các thông tin về doanh số hoạt động và số dư tài khoản) và các thông tin liên quan đến giao dịch gửi, rút tiền, chuyển tiền và tài sản của khách hàng; nội dung các văn bản, giấy tờ, tài liệu; tên và mẫu chữ ký của người gửi tiền và tài sản[119]; các thông tin khác như số thẻ, hiệu lực thẻ, mã số bảo vệ in trên mặt sau thẻ, mật khẩu giao dịch ngân hàng trực tuyến, mã PIN, mã số nhận thông tin và giao dịch về tiền gửi của khách hàng qua mạng máy tính. Theo quy định tại Điều 5, 6 Nghị định 70/2000/NĐ-CP ngày 21/11/2000 của Chính phủ về việc giữ bí mật, lưu trữ và cung cấp các thông tin có liên quan

[119] Xem: khoản 3,4 Điều 2 Nghị định 70/2000/NĐ-CP ngày 21/11/2000 của Chính phủ về việc giữ bí mật, lưu trữ và cung cấp các thông tin có liên quan đến tiền gửi và tài sản gửi của khách hàng.

đến tiền gửi và tài sản gửi của khách hàng, tổ chức tín dụng chỉ được cung cấp các thông tin trên trong 5 trường hợp sau: (1) Theo yêu cầu của khách hàng hoặc người được khách hàng uỷ quyền theo quy định của pháp luật; (2) Phục vụ hoạt động nội bộ của tổ chức nhận tiền gửi và tài sản gửi của khách hàng; (3) Theo yêu cầu bằng văn bản của Tổng Giám đốc tổ chức bảo hiểm tiền gửi khi tổ chức này thực hiện quyền và nghĩa vụ của mình theo quy định của pháp luật; (4) Theo yêu cầu bằng văn bản của các cơ quan Nhà nước trong quá trình thanh tra, điều tra, truy tố, xét xử, thi hành án thuộc thẩm quyền theo quy định của pháp luật; (5) Các tổ chức tín dụng được phép cung cấp cho nhau về các thông tin liên quan đến tiền gửi và tài sản gửi của khách hàng[120]. Việc cung cấp thông tin về tài khoản ngân hàng ngoài các trường hợp trên được coi là công khai hoá trái phép.

Hành vi thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin tài khoản ngân hàng của người khác 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.

---

[120] Xem: Điều 5, Điều 6 Nghị định 70/2000/NĐ-CP ngày 21/11/2000 của Chính phủ về việc giữ bí mật, lưu trữ và cung cấp các thông tin có liên quan đến tiền gửi và tài sản gửi của khách hàng.

Theo Điều 16 Luật tần số vô tuyến điện (2009), tổ chức, cá nhân sử dụng tần số vô tuyến điện, thiết bị vô tuyến điện phải có giấy phép sử dụng tần số vô tuyến điện tương ứng, trừ trường hợp các thiết bị vô tuyến điện hoạt động ở cự ly ngắn, có công suất hạn chế, ít khả năng gây nhiễu có hại theo quy định của pháp luật và thiết bị vô tuyến điện đặt trên tàu biển, tàu bay nước ngoài đi qua lãnh thổ Việt Nam được miễn giấy phép theo thỏa thuận quốc tế, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên. Như vậy, về nguyên tắc cá nhân, tổ chức chỉ được sử dụng tần số vô tuyến điện đã được nhà nước cấp phép. Trong trường hợp khẩn cấp gây nguy hiểm đến tính mạng con người và tài sản, theo Điều 33 Luật tần số vô tuyến điện (2009), tổ chức, cá nhân có thể sử dụng tạm thời tần số và thiết bị vô tuyến điện chưa được cấp giấy phép để phục vụ cho việc gọi cấp cứu nhưng phải thông báo cho cơ quan quản lý chuyên ngành tần số vô tuyến điện. Trường hợp này, cá nhân, tổ chức được phép sử dụng tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn. Ngoài các trường hợp trên, cá nhân sử dụng tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn hoặc cá nhân, tổ chức không được phép mà sử dụng tần số vô tuyến điện dành riêng cho mục đích an ninh, quốc phòng sẽ bị coi là sử dụng trái phép.

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, được chia thành 2 nhóm:

Thứ nhất, tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn. Các tần số này được quy định tại "Phụ lục tần số sử dụng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu nạn", ban hành kèm theo Thông tư 19/2013/TT-BTTTT ngày 02 tháng 12 năm 2013 của Bộ trưởng Bộ Thông tin và Truyền thông quy định tần số cấp cứu, an toàn, tìm

kiếm, cứu nạn trên biển và hàng không dân dụng[121].

Thứ hai, tần số vô tuyến điện danh riêng cho mục đích quốc phòng, an ninh. Loại tần số này sẽ do Bộ quốc phòng, Bộ Công an và Bộ thông tin và Truyền thông phối hợp xác định.

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. 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[122]. Theo quy định của 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 thủ đoạn 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

[121] Xem: Phụ lục 1: Bảng tần số sử dụng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu nạn.

[122] Xem: khoản 13 Điều 3 Luật tần số vô tuyến điện (2009).

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 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 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

Chủ thể của tội phạm trong lĩnh vực CNTT, MVT là cá nhân có năng lực TNHS theo quy định của BLHS năm 2015. Theo đó, cá nhân phải đủ độ tuổi chịu TNHS theo quy định tại Điều 12 và không thuộc tình trạng mất năng lực TNHS theo quy định tại Điều 21 BLHS năm 2015. Thông thường, cá nhân đủ độ tuổi theo quy định tại Điều 12 của BLHS năm 2015 có thể trở thành chủ thể của tội phạm trong lĩnh vực CNTT, MVT, trừ trường hợp có nghi ngờ về khả năng nhận thức hoặc khả năng điều khiển hành vi của người đó. Qua hoạt động giám định pháp y tâm thần, nếu kết quả cho thấy người đó không có khả năng nhận thức hoặc khả năng điều khiển hành vi của mình thì người đó sẽ không thể trở thành chủ thể của tội phạm nói chung và tội phạm trong lĩnh vực CNTT, MVT nói riêng.

Theo quy định tại Điều 12 BLHS năm 2015, người từ đủ 16 tuổi trở lên phải chịu TNHS về mọi tội phạm, do đó, người từ đủ 16 tuổi trở lên sẽ 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 rất nghiêm trọng và đặc biệt nghiêm trọng quy định tại Điều 286, 287, 289 và 290 BLHS năm 2015. Theo quy định về phân loại tội phạm tại Điều 9 BLHS năm 2015, tội phạm rất

nghiêm trọng là tội phạm có tính chất và mức độ nguy hiểm cho xã hội rất lớn mà mức cao nhất của khung hình phạt do BLHS quy định đối với tội ấy là từ trên 07 năm tù đến 15 năm tù; Tội phạm đặc biệt nghiêm trọng là tội phạm có tính chất và mức độ nguy hiểm cho xã hội đặc biệt lớn mà mức cao nhất của khung hình phạt do BLHS quy định đối với tội ấy là từ trên 15 năm tù đến 20 năm tù, tù chung thân hoặc tử hình. Như vậy, người từ đủ 14 tuổi đến dưới 16 tuổi phải chịu trách nhiệm hình sự 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.

Trong thực tiễn, tội phạm trong lĩnh vực CNTT, MVT thường do người nước ngoài thực hiện hoặc do người nước ngoài kết hợp với công dân Việt Nam thực hiện. Địa điểm phạm tội có thể trên lãnh thổ Việt Nam, có thể ở ngoài lãnh thổ Việt Nam. Theo quy định tại Điều 6 BLHS năm 2015, cá nhân là công dân Việt Nam, người nước ngoài đều có thể trở thành chủ thể của loại tội phạm này cho dù địa điểm phạm tội ở đâu, trừ những người được hưởng quyền miễn trừ ngoại giao hoặc lãnh sự theo pháp luật Việt Nam, theo điều ước quốc tế mà Việt Nam là thành viên hoặc tập quán quốc tế. Thực tiễn cho thấy, người phạm tội trong lĩnh vực CNTT, MVT thường là những người có nhiều hiểu biết về CNTT, MVT. Họ sử dụng những hiểu biết đó để thực hiện hành vi phạm tội[123]. Tuy nhiên, những đặc điểm đó không phải là dấu hiệu chủ thể bắt buộc của tội phạm này.

Ở nước ta cũng như trên thế giới, lĩnh vực CNTT, MVT là những lĩnh vực mới, hiện đại và phát triển với tốc độ rất nhanh. Những người trẻ tuổi hiện nay có nhiều điều kiện để tiếp cận, thực hành và trở nên rất giỏi trong lĩnh vực này. Hậu quả tiêu cực kéo theo là tình trạng người phạm tội trong lĩnh vực CNTT, MVT ngày càng "trẻ hoá". Để ngăn chặn tình trạng này,

[123] Xem: Phạm Văn Lợi (2007), Tlđd, tr. 39.

khoản 2 Điều 12 của BLHS năm 2015 đã quy định, người từ đủ 14 tuổi đến dưới 16 tuổi phải chịu TNHS về tội phạm rất nghiệm trọng, tội phạm đặc biệt nghiêm trọng quy định tại một trong 28 điều luật của BLHS năm 2015[124], trong đó có 4 điều luật về tội phạm trong lĩnh vực CNTT, MVT (Điều 286, Điều 287, Điều 289 và Điều 290). Với tỷ lệ 14,2 % số các điều luật trong số những điều luật mà người từ đủ 14 tuổi đến dưới 16 tuổi phải chịu TNHS, cho thấy mức độ quan tâm phòng chống tình trạng "trẻ hoá" của những người thực hiện loại tội phạm này hiện nay của nhà làm luật.

Theo quy định tại Điều 76 của BLHS năm 2015, pháp nhân thương mại không phải là chủ thể của tội phạm trong lĩnh vực CNTT, MVT. Trong số những tội mà pháp nhân thương mại phải chịu TNHS, có một số tội xâm phạm trật tự quản lý kinh tế, một số tội phạm về môi trường và 2 tội xâm phạm an toàn công cộng, trật tự công cộng là tội tài trợ khủng bố (Điều 300) và tội rửa tiền (Điều 324).

Trong khi đó, tại Điều 15 của Công ước Budapest 2001 có quy định về trách nhiệm của pháp nhân. Theo đó, các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để đảm bảo rằng pháp nhân phải chịu trách nhiệm đối với các hành vi phạm tội quy định trong Công ước, được bất cứ cá nhân nào thực hiện vì lợi ích của pháp nhân, nếu cá nhân đó là đại diện hoặc là thành viên trong cơ quan của pháp nhân và nắm vị trí lãnh đạo pháp nhân. Trách nhiệm của pháp nhân sẽ theo các nguyên tắc pháp lý của quốc gia thành viên, có thể là TNHS, dân sự hoặc hành chính. Như vậy, có thể thấy Công ước trên mặc dù quy định về việc các quốc gia thành viên phải xử lý trách nhiệm của pháp nhân đối với những hành vi phạm tội trong lĩnh vực CNTT, MVT, nhưng việc xử lý theo TNHS, dân sự hay hành chính là tuỳ

[124] Bao gồm các điều 123, 134, 141, 142, 143, 144, 150, 151, 168, 169, 170, 171, 173, 178, 248, 249, 250, 251, 252, 265, 266, 286, 287, 289, 290, 299, 303 và 304 BLHS năm 2015.

thuộc vào pháp luật của các quốc gia thành viên, không bắt buộc phải xử lý hình sự.

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

Theo lý luận của khoa học LHS Việt Nam, mặt chủ quan của tội phạm bao gồm lỗi, động cơ và mục đích phạm tội. Theo quy định của BLHS năm 2015, dấu hiệu lỗi là dấu hiệu bắt buộc trong tất cả các cấu thành tội phạm của tội phạm trong lĩnh vực CNTT, MVT.

**** Dấu hiệu lỗi:***

Theo quy định của BLHS năm 2015, cũng như các loại tội phạm khác lỗi là dấu hiệu bắt buộc trong cấu thành tội phạm của tất cả tội phạm trong lĩnh vực CNTT, MVT. Theo đó, 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. Khi thực hiện hành vi phạm tội, người phạm tội nhận thức được hành vi của mình là nguy hiểm cho xã hội, nhận thức được hậu quả nguy hiểm cho xã hội có thể xảy ra (đối với những tội có cấu thành vật chất) nhưng vẫn thực hiện hành vi phạm tội đó và mong muốn hoặc có ý thức bỏ mặc cho hậu quả xảy ra. Trường hợp, hành vi được thực hiện với lỗi vô ý sẽ không bị coi là tội phạm trong lĩnh vực CNTT, MVT. Ví dụ: vô ý truy cập vào mạng máy tính sẽ không bị coi là phạm tội xâm nhập trái phép vào mạng máy tính (Điều 289) hoặc vô ý xoá dữ liệu điện tử trong mạng máy tính cũng sẽ không bị coi là phạm tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính (Điều 287).

Tuy nhiên, ở Việt Nam hiện vẫn còn quan điểm cho rằng, đối với tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính tính, mạng viễn thông, phương tiện điện tử vẫn có thể có lỗi vô ý[125]. Đây là quan điểm không chính

[125] Xem: Trần Văn Hoà (2011), Tlđd, tr. 35.

xác, vì theo hướng dẫn tại khoản 1, 2, 3 Điều 7 Thông tư liên tịch số 10/2012/ TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012, hình thức lỗi trong tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử chỉ là lỗi cố ý. Đây là quy định thống nhất của BLHS năm 1999 và BLHS năm 2015. Quy định này là hợp lý trong bối cảnh của Việt Nam nói riêng và phù hợp với xu hướng chung của các nước trên thế giới.

**** Dấu hiệu động cơ, mục đích phạm tội:***

Động cơ phạm tội là động lực bên trong thúc đẩy người phạm tội thực hiện hành vi phạm tội cố ý[126]. Theo BLHS năm 2015, động cơ phạm tội không phải là dấu hiệu bắt buộc trong cấu thành tội phạm của tội phạm trong lĩnh vực CNTT, MVT. Do đó, động cơ phạm tội trong lĩnh vực CNTT, MVT chỉ có thể là tình tiết tăng nặng TNHS khi quyết định hình phạt.

Mục đích phạm tội là kết quả trong ý thức chủ quan mà người phạm tội đặt ra phải đạt được khi thực hiện hành vi phạm tội cố ý trực tiếp[127]. Theo BLHS năm 2015, mục đích phạm tội được quy định là dấu hiệu định tội của một số tội phạm trong lĩnh vực CNTT, MVT. Cụ thể:

Thứ nhất, "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). Theo Điều 285 BLHS năm 2015, mục đích của 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 là để sử dụng vào mục đích trái pháp luật. Nếu sử dụng vào mục đích hợp pháp như nghiên cứu, học tập, thử

---

[126] Xem: Trường Đại học luật Hà Nội (2017), *Giáo trình luật hình sự Việt Nam (phần chung)*, NXB. Công an nhân dân, tr. 167.

[127] Xem: Trường đại học luật Hà Nội (2017), Tlđd, tr. 168.

nghiệm, áp dụng biện pháp điều tra tố tụng đặc biệt của cơ quan có thẩm quyền không bị coi là tội phạm [128]. Khái niệm "mục đích trái pháp luật" có phạm vi rộng, bao gồm cả mục đích phạm tội và các mục đích vi phạm pháp luật khác như vi phạm pháp luật hành chính, vi phạm luật dân sự. Tham khảo một số văn bản pháp luật quốc tế như Công ước Budapest 2001 hoặc Luật mẫu 2002 tác giả thấy rằng, các văn bản này đều giới hạn ở "mục đích thực hiện các tội trong lĩnh vực CNTT, MVT"[129]. Tác giả cho rằng, quy định của các văn bản pháp luật quốc tế trên là phù hợp. Điều đó sẽ hạn chế được việc xử lý hình sự một cách tràn lan.

Thứ hai, 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 (điểm c, d, đ khoản 1 Điều 290). Đây cũng là dấu hiệu quan trọng giúp chúng ta 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.

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

---

[128] Xem: các biện pháp bí mật ghi âm ghi hình, bí mật theo dõi điện thoại, bí mật thu thập dữ liệu điện tử (được quy định từ Điều 223 đến Điều 228 Chương XVI (Các biện pháp điều tra tố tụng đặc biệt) BLTTHS năm 2015).

[129] Xem: khoản 1 Điều 6 Công ước Budapest 2001 quy định hành vi sử dụng sai lạc các thiết bị là hành vi cố ý của người không có thẩm quyền thực hiện: (a) *"sản xuất, bán, đề nghị sử dụng, nhập khẩu, phân phối hoặc bằng cách thức khác cung cấp: (i) thiết bị, bao gồm chương trình máy tính, được thiết kế hoặc được điều chỉnh để thực hiện hành vi phạm tội nêu từ Điều 2 đến Điều 5"* (tội truy cập bất hợp pháp, tội ngăn chặn bất hợp pháp, tội gây rối dữ liệu và tội gây rối hệ thống).

** Hình phạt tiền*

Hình phạt tiền vừa được sử dụng là hình phạt chính, vừa được sử dụng là hình phạt bổ sung trong tất cả các tội phạm trong lĩnh vực CNTT, MVT, trừ tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện hành vi chiếm đoạt tài sản (Điều 290) chỉ có hình phạt bổ sung là hình phạt tiền. Hầu hết các khung hình phạt trong một điều luật đều có quy định về hình phạt tiền. Ví dụ: cả 3 khung hình phạt chính và hình phạt bổ sung tại Điều 285 đều có quy định hình phạt tiền, Điều 286 có ¾ khung hình phạt có quy định hình phạt tiền, toàn bộ các khung hình phạt của Điều 287 có quy định hình phạt tiền… Mức phạt tiền đối với hình phạt chính, từ 30 triệu đồng đến 1 tỷ đồng; đối với hình phạt bổ sung, từ 5 triệu đồng đến 50 triệu đồng. Như vậy, hình phạt tiền được sử dụng phổ biến trong các tội phạm trong lĩnh vực CNTT, MVT. Theo tác giả Luận án, quy định theo hướng này rất phù hợp, vì động cơ phạm tội trong những tội này thường là động cơ vụ lợi. Do đó, việc áp dụng hình phạt tiền sẽ đạt được mục đích của hình phạt.

** Hình phạt cải tạo không giam giữ*

Cải tạo không giam giữ là hình phạt được áp dụng đối với 7/9 tội phạm trong lĩnh vực CNTT, MVT (trừ Điều 287 và Điều 289). Thời gian cải tạo không giam giữ từ 6 tháng đến 3 năm.

** Hình phạt tù có thời hạn*

Tù có thời hạn được áp dụng đối với tất cả các tội phạm trong lĩnh vực CNTT, MVT. Tuy nhiên đa số các khung hình phạt đều quy định loại hình phạt khác để lựa chọn thay thế hình phạt tù có thời hạn như hình phạt tiền, cải tạo không giam giữ. Chỉ có 8/25 khung hình phạt chính chỉ quy định hình phạt tù có thời hạn (khoản 3 Điều 286, khoản 3 Điều 287, khoản 3 Điều 289, khoản 2,3,4 Điều 290, khoản 2 Điều 293, khoản 2 Điều 294). Mức hình phạt tù có thời hạn phổ biến từ 3 tháng đến 7 năm, cá biệt mới có khung hình phạt

đến 12 năm hoặc 20 năm. Có thể thấy BLHS năm 2015 có xu hướng hạn chế áp dụng hình phạt tù có thời hạn đối với các tội phạm trong lĩnh vực CNTT, MVT. Trường hợp bắt buộc phải áp dụng hình phạt này, mức hình phạt cũng không cao, trừ trường hợp đặc biệt nghiêm trọng hoặc đối với tội phạm có tính chất chiếm đoạt tài sản có giá trị lớn.

** Hình phạt cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định*

Hình phạt cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định là hình phạt bổ sung được áp dụng đối với 7/9 điều luật của tội phạm trong lĩnh vực CNTT, MVT (trừ Điều 293, 294). Mặc dù không phải là dấu hiệu bắt buộc về chủ thể của tội phạm, nhưng người phạm tội này thường phải là người có hiểu biết về CNTT, MVT. Do đó cần phải cấm họ đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc liên quan đến lĩnh vực CNTT, MVT trong một thời gian nhất định, để tránh việc họ lại tiếp tục phạm tội. Do đó, những quy định trên là hoàn toàn hợp lý. Thời gian cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc liên quan đến lĩnh vực CNTT, MVT từ 1 đến 5 năm.

** Hình phạt tịch thu một phần hoặc toàn bộ tài sản*

Tịch thu một phần hoặc toàn bộ tài sản là hình phạt bổ sung chỉ được áp dụng đối với 3 điều luật gồm Điều 285, Điều 290 và Điều 291. Theo quy định tại Điều 45 BLHS năm 2015, hình phạt này được áp dụng đối với tội phạm nghiêm trọng, tội phạm rất nghiêm trọng hoặc tội phạm đặc biệt nghiêm trọng. Do đó, hình phạt này chỉ có thể áp dụng đối với khoản 2, 3 Điều 285, khoản 2, 3, 4 Điều 290 và khoản 3 Điều 291. Khi tịch thu toàn bộ tài sản vẫn để cho người bị kết án và gia đình họ có điều kiện sinh sống.

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:

** Nhóm 1: Các dấu hiệu định khung liên quan đến hành vi phạm tội*

Nhóm dấu hiệu định khung tăng nặng 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 phạm tội có tổ chức, phạm tội từ 2 lần trở lên và phạm tội có tính chất chuyên nghiệp. Cụ thể:

- Dấu hiệu "Phạm tội có tổ chức": là hình thức đồng phạm có sự câu kết chặt chẽ giữa những người cùng phạm tội. Theo Nghị quyết số 02-HĐTP/NQ ngày 16/11/1988 của Hội đồng thẩm phán TAND tối cao, dấu hiệu của sự câu kết chặt chẽ giữa những người đồng phạm trong lĩnh vực CNTT, MVT là một trong những dấu hiệu sau: (1) người đồng phạm đã tham gia vào tổ chức phạm tội trong đó có thực hiện tội phạm trong lĩnh vực CNTT, MVT; (2) những người đồng phạm đã cùng nhau thực hiện tội phạm trong lĩnh vực CNTT, MVT nhiều lần theo kế hoạch đã được thống nhất từ trước; (3) mặc dù chỉ thực hiện tội phạm trong lĩnh vực CNTT, MVT một lần, nhưng trước đó những người đồng phạm đã tính toán kỹ càng, chu đáo về kế hoạch phạm tội. Dấu hiệu "phạm tội có tổ chức" được quy định trong khoản 2 của tất cả các điều luật về tội phạm trong lĩnh vực CNTT, MVT (từ Điều 285 đến Điều 294, trừ Điều 292).

- Dấu hiệu "Phạm tội từ 2 lần trở lên": là trường hợp phạm tội trong lĩnh vực CNTT, MVT mà trước đó người phạm tội đã phạm tội này ít nhất một lần và chưa bị xét xử, chưa hết thời hiệu truy cứu TNHS. Dấu hiệu này được quy định trong khoản 2 Điều 285 và khoản 2 Điều 290 BLHS năm 2015.

- Dấu hiệu "Có tính chất chuyên nghiệp": là trường hợp thực hiện từ 5 lần trở lên về cùng một tội phạm trong lĩnh vực CNTT, MVT (không phân

biệt đã bị truy cứu TNHS hay chưa, nếu chưa hết thời hiệu truy cứu TNHS hoặc chưa được xoá án tích và người phạm tội đều lấy các lần phạm tội này làm nghề sinh sống và lấy kết quả của việc phạm tội làm nguồn sống chính[130]. Dấu hiệu này được quy định trong khoản 2 Điều 285, khoản 2 Điều 290 và khoản 2 Điều 291 BLHS năm 2015.

** Nhóm 2: Các dấu hiệu định khung liên quan đến hậu quả của tội phạm*

Các dấu hiệu định khung tăng nặng do hậu quả của tội phạm gây ra nặng hơn so với cấu thành tội phạm cơ bản của tội đó. Căn cứ theo loại thiệt hại gây ra, các tình tiết tăng nặng TNHS của tội phạm trong lĩnh vực CNTT, MVT có thể được chia thành các nhóm nhỏ sau:

Thứ nhất, 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, bao gồm:

- Dấu hiệu "Làm đình trệ hoạt động của cơ quan, tổ chức" được quy định tại điểm g khoản 2 và điểm e khoản 3 Điều 287. Tội phạm làm cản trở hoặc gây rối hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử dẫn đến hậu quả trực tiếp làm cho cơ quan, tổ chức đang sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử phải ngừng hoạt động hoặc gián đoạn hoạt động trong thời gian nhất định. Tuỳ theo thời gian bị đình trệ hoạt động, tình tiết này có thể là tình tiết định tội (từ 24 giờ đến dưới 72 giờ) hoặc tình tiết tăng nặng định khung điểm g khoản 2 (từ 72 giờ đến dưới 168 giờ) hoặc điểm e khoản 3 (từ 168 giờ trở lên).

- Dấu hiệu "xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát" được quy định tại điểm đ khoản 2 Điều 288 BLHS năm 2015. Việc phạm

[130] Xem: Mục 5 Nghị quyết số 01/2006/NQ-HĐTP ngày 12/5/2006 của Hội đồng thẩm phán TAND tối cao.

tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông xâm phạm đến "bí mật cá nhân" làm cho nạn nhân có hành vi tự sát là tình tiết tăng nặng TNHS. Khái niệm "bí mật cá nhân" hiện chưa có định nghĩa chính thức. Bí mật cá nhân là một loại thông tin riêng hợp pháp của cá nhân. Đó là tổng thể các quan hệ quá khứ, các thông tin liên quan đến cá nhân mang tính chất chi phối các quan hệ cụ thể của cá nhân mà bị bộc lộ sẽ gây cho cá nhân những bất lợi hoặc dễ gây ra sự hiểu lầm ở các chủ thể khác, mà bản chất của yếu tố bí mật cá nhân không gây ra bất kỳ một thiệt hại nào cho chủ thể khác[131]. Do bí mật cá nhân của mình bị xâm hại mà nạn nhân có hành vi tự kết thúc mạng sống của mình. Hậu quả này chỉ cần nạn nhân có hành vi tự sát, không kể việc chết người có xảy ra hay không.

- Dấu hiệu "Dẫn đến biểu tình" quy định tại điểm g khoản 2 Điều 288 BLHS năm 2015. Pháp luật hiện nay chưa có quy định về khái niệm "biểu tình". Tuy nhiên có thể hiểu biểu tình là hành động tập hợp đông người, có tổ chức và được diễn ra tại nơi công cộng với mục đích là bộc lộ thái độ của người đi biểu tình đối với một vấn đề đang xảy ra trong đời sống chính trị, kinh tế, xã hội ở tầm quốc tế, khu vực, quốc gia hoặc hẹp hơn là một vấn đề chỉ liên quan đến cộng đồng người đang thực hiện biểu tình[132]. Biểu tình thường dẫn đến hậu quả phức tạp về an ninh, xã hội. Do đó, việc phạm tội dẫn đến biểu tình là tình tiết tăng nặng định khung của tội này.

Thứ hai, 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

---

[131] Xem: Phùng Trung Tập, "Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình", *Tạp chí Kiểm sát*, số 02/2018.

[132] Xem: Nguyễn Linh Giang, "Nhu cầu luật hoá quyền biểu tình theo Hiến pháp năm 2013": http://tuphaptamky.gov.vn/2014/news/Gop-y-Hien-phap/Nhu-cau-luat-hoa-quyen-bieu-tinh-theo-Hien-phap-nam-2013-1518.html (ngày truy cập 20/2/2020).

liệu điện tử. Tội phạm gây thiệt hại về tính bí mật, tính toàn vẹn và tính khả dụng của thông tin dữ liệu điện tử mạng máy tính, mạng viễn thông, phương tiện điện tử. Các dấu hiệu này bao gồm:

- Dấu hiệu phản ánh thiệt hại là mất tính bí mật của thông tin dữ liệu điện tử. Thiệt hại này được thể hiện thông qua số lượng thông tin, dữ liệu bị thu thập, tàng trữ, trao đổi, mua bán, công khai trái phép như "thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng của người khác từ 50 tài khoản đến dưới 200 tài khoản (điểm a Khoản 2 Điều 291 BLHS năm 2015) hoặc từ 200 tài khoản trở lên (điểm a Khoản 3 Điều 291 BLHS năm 2015).

- Dấu hiệu phản ánh thiệt hại là mất tính khả dụng của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc dữ liệu điện tử như số thời gian "làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử". Đây là tình tiết định khung tăng nặng tại điểm e khoản 2, điểm d khoản 3 Điều 287 BLHS năm 2015.

Thứ ba, 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 phương tiện hoặc tính theo số người dùng phương tiện đó. Dấu hiệu này được quy tại điểm d khoản 2 Điều 286 (làm lây nhiễm từ 200 phương tiện điện tử đến dưới 500 phương tiện điện tử hoặc hệ thống thông tin có từ 200 người sử dụng đến dưới 500 người sử dụng) và điểm đ khoản 3 Điều 286 (làm lây nhiễm từ 500 phương tiện điện tử trở lên hoặc hệ thống thông tin có từ 500 người sử dụng trở lên).

Thứ tư, 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. Dấu hiệu này được quy định tại 13 trong 15 khung tăng nặng của 7 trong số 9 điều luật (trừ Điều 290, 291) BLHS năm 2015.

Thứ năm, 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. Dấu hiệu này được quy định phổ biến tại 12 trong tổng số 14 khung tăng nặng của 7 trong 9 điều luật trong nhóm tội này (trừ Điều 293, 294) BLHS năm 2015.

** Nhóm 3: Các dấu hiệu định khung liên quan đến nhân thân của người phạm tội*

Các dấu hiệu tăng năng định khung liên quan đến nhân thân người phạm tội làm cho trường hợp phạm tội của họ tăng nặng hơn so với cấu thành cơ bản như: tái phạm nguy hiểm; lợi dụng quyền quản trị mạng máy tính, mạng viễn thông; lợi dụng chức vụ, quyền hạn. Cụ thể:

- Dấu hiệu "tái phạm nguy hiểm": là trường hợp phạm tội đã bị kết án về tội phạm rất nghiêm trọng, tội phạm đặc biệt nghiêm trọng do cố ý, chưa được xóa án tích mà lại thực hiện tội phạm trong lĩnh vực CNTT, MVT thuộc trường hợp tội phạm rất nghiêm trọng, tội phạm đặc biệt nghiêm trọng; hoặc đã tái phạm, chưa được xóa án tích mà lại thực hiện tội phạm trong lĩnh vực CNTT, MVT[133]. Dấu hiệu tái phạm nguy hiểm được quy định tại điểm e khoản 2 Điều 285, điểm đ khoản 2 Điều 286, điểm c khoản 2 Điều 287, điểm e khoản 2 Điều 289, điểm g khoản 2 Điều 290, điểm đ khoản 2 Điều 291, điểm c khoản 2 Điều 293 và điểm c khoản 2 Điều 294 BLHS năm 2015.

- Dấu hiệu "lợi dụng quyền quản trị mạng máy tính, mạng viễn thông" được quy định tại điểm b khoản 2 Điều 287, điểm b khoản 2 Điều 288 BLHS năm 2015. Theo khoản 10 Điều 2 Thông tư 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012, lợi dụng quyền quản trị mạng máy tính, mạng viễn thông là người phạm tội đã sử dụng quyền quản lý, vận hành, khai thác và duy trì hoạt động ổn định hệ thống mạng máy tính,

[133] Xem: Điều 53 BLHS năm 2015.

mạng viễn thông, mạng Internet của mình để thực hiện hành vi phạm tội[134]. Người phạm tội là người có quyền quản lý, vận hành, khai thác và duy trì hoạt động ổn định hệ thống mạng máy tính, mạng viễn thông, mạng Internet của cá nhân, tổ chức, nhưng đã lợi dụng những quyền này để phạm tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287) hoặc tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thong (Điều 288) BLHS năm 2015.

- Dấu hiệu "Lợi dụng chức vụ, quyền hạn": theo khoản 2 Điều 352 BLHS năm 2015, "người có chức vụ là người do bổ nhiệm, do bầu cử, do hợp đồng hoặc do một hình thức khác, có hưởng lương hoặc không hưởng lương, được giao thực hiện một nhiệm vụ nhất định và có quyền hạn nhất định trong khi thực hiện công vụ, nhiệm vụ". Trường hợp này, người phạm tội là người có chức vụ, quyền hạn và người đó đã lợi dụng chức vụ, quyền hạn được giao để phạm tội trong lĩnh vực CNTT, MVT. Dấu hiệu lợi dụng chức vụ, quyền hạn được quy định tại điểm b khoản 2 Điều 289 BLHS năm 2015.

** Nhóm 4: Các dấu hiệu định khung liên quan đến đối tượng tác động của tội phạm*

Mục tiêu tấn công của tội phạm trong lĩnh vực CNTT, MVT có thể là các mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc dữ liệu điện tử nói chung. Nhưng đối với một số mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử có tính chất quan trọng đặc biệt, nếu bị tấn công sẽ gây ra hậu quả rất lớn cho an ninh, trật tự xã hội. Khi tội phạm tác động đến những đối tượng này sẽ làm cho tính chất của tội phạm tăng nặng hơn đáng kể. Do đó, việc tấn công vào các mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc dữ liệu điện tử có tính chất quan trọng được quy

[134] Xem: khoản 4 Điều Điều 7 Thông tư 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012.

định là dấu hiệu định khung tăng nặng TNHS của một số tội. Cụ thể:

- Dấu hiệu "đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh". Hệ thống dữ liệu thuộc bí mật nhà nước là hệ thống thông tin do cơ quan, tổ chức quản lý có chứa những tin về vụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trọng thuộc lĩnh vực chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ, các lĩnh vực khác mà Nhà nước không công bố hoặc chưa công bố và nếu bị tiết lộ thì sẽ gây nguy hại cho Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam và được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước. Hệ thống thông tin phục vụ an ninh là hệ thống thông tin của cơ quan, tổ chức chứa đựng những dữ liệu có liên quan đến việc bảo đảm sự ổn định, phát triển bền vững của chế độ xã hội chủ nghĩa và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, sự bất khả xâm phạm độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc. Hệ thống thông tin phục vụ quốc phòng là hệ thống thông tin của tổ chức, cơ quan nhà nước chứa đựng những dữ liệu có liên quan đến việc bảo vệ đất nước[135]. Dấu hiệu tăng nặng này được quy định tại điểm a khoản 3 Điều 286, điểm a khoản 3 Điều 287, điểm a khoản 3 Điều 289 BLHS năm 2015. Đây đều là khung hình phạt cao nhất của những tội này. Điều đó cho thấy tính chất nguy hiểm rất cao của tình tiết tăng nặng này.

- Dấu hiệu "Đối với 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". Theo Luật công nghệ thông tin (2006), cơ sở hạ tầng thông tin là hệ thống trang thiết bị phục vụ cho việc sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số, bao gồm mạng viễn thông, mạng Internet, mạng máy tính và cơ sở dữ liệu[136]. Theo

[135] Xem: khoản 11, 12, 13 Điều 2 Thông tư 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012.

[136] Xem: khoản 4 Điều 4 Luật công nghệ thông tin (2006).

Thông tư liên tịch số 10/2012/ TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012, hệ thống thông tin điều hành lưới điện quốc gia là hệ thống thông tin phục vụ hoạt động quản lý, vận hành các công trình điện của quốc gia để truyền tải năng lượng điện từ nơi sản xuất điện đến cơ quan, tổ chức, cá nhân sử dụng điện. Hệ thống thông tin điều khiển giao thông là hệ thống thông tin của cơ quan nhà nước phục vụ hoạt động quản lý, vận hành các công trình giao thông nhằm bảo đảm hoạt động giao thông thông suốt, trật tự, an toàn. Hệ thống thông tin tài chính, ngân hàng là hệ thống thông tin chứa đựng cơ sở dữ liệu phục vụ cho một hoặc nhiều hoạt động kỹ thuật nghiệp vụ tài chính, ngân hàng[137]. Dấu hiệu tăng nặng này được quy định điểm b khoản 3 Điều 286; điểm b khoản 3 Điều 287; điểm b khoản 3 Điều 289 của BLHS năm 2015.

- Dấu hiệu "Đối với trạm trung chuyển internet quốc gia, hệ thống cơ sở dữ liệu tên miền và hệ thống máy chủ tên miền quốc gia". Trong đó:

+ Trạm trung chuyển internet quốc gia được hiểu là một hệ thống thiết bị viễn thông được một tổ chức hoặc doanh nghiệp thiết lập để cung cấp dịch vụ kết nối internet. Trạm trung chuyển Internet quốc gia (VNIX) là trạm trung chuyển Internet thuộc Trung tâm Internet Việt Nam do Bộ Thông tin và Truyền thông thành lập[138].

+ Hệ thống cơ sở dữ liệu tên miền gồm một loạt các cơ sở dữ liệu chứa địa chỉ IP và các tên miền tương ứng của nó. Mỗi tên miền tương ứng với một

[137] Xem: Thông tư 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012.

[138] Chức năng của Trạm này là hỗ trợ: a) Bảo đảm an toàn cho hoạt động của toàn bộ mạng Internet Việt Nam trong trường hợp xảy ra sự cố đối với mạng viễn thông trong nước và quốc tế; b) Hình thành mạng thử nghiệm công nghệ IPv6 quốc gia; c) Tham gia kết nối với trạm trung chuyển Internet của khu vực và quốc tế; d) Kết nối các doanh nghiệp cung cấp dịch vụ Internet theo nguyên tắc phi lợi nhuận nhằm nâng cao chất lượng và giảm giá thành dịch vụ.

địa chỉ bằng số cụ thể. Hệ thống tên miền trên mạng Internet có nhiệm vụ chuyển đổi tên miền sang địa chỉ IP và ngược lại từ địa chỉ IP sang tên miền[139].

+ Hệ thống máy chủ tên miền quốc gia được hiểu là hệ thống máy chủ tên miền quốc gia Việt Nam ".vn". Tên miền quốc gia Việt Nam là tập hợp tên miền các cấp dưới tên miền quốc gia Việt Nam cấp cao nhất ".vn" và tên miền các cấp dưới tên miền cấp cao nhất khác thuộc quyền quản lý của Việt Nam. Hệ thống máy chủ tên miền (hệ thống DNS) là tập hợp các cụm máy chủ được kết nối với nhau để trả lời địa chỉ IP tương ứng với một tên miền khi được hỏi đến. Hệ thống DNS quốc gia là hệ thống DNS do VNNIC trực tiếp quản lý phục vụ việc truy vấn địa chỉ IP cho tên miền các cấp dưới tên miền ".vn"[140].

Dấu hiệu này được quy định tại điểm đ khoản 2 Điều 289 BLHS năm 2015. Như vậy, tình tiết này có mức độ giảm nhẹ hơn so với tình tiết "Đối với 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", vì nó được quy định ở khoản 3 của Điều 289 BLHS năm 2015.

Kết luận chương 2

Thông qua sự phân tích, đánh giá quá trình phát triển của các quy định LHS về tội phạm trong lĩnh vực CNTT, MVT có thể rút ra một số kết luận sau:

Thứ nhất, lần đầu tiên BLHS năm 1999 có quy định riêng về tội phạm trong lĩnh vực CNTT, MVT. Các quy định này sửa đổi bổ sung năm 2009 và

---

[139] Xem: Trung tâm Internet Việt Nam (VNNIC), "*Hệ thống tên miền"*, https://www.vnnic.vn/dns/congnghe/h%E1%BB%87-th%E1%BB%91ng-t%C3%AAn-mi%E1%BB%81n (truy cập ngày 15/3/2020).

[140] Xem: khoản 7, 12 Điều 2 Thông tư số 24/2015/TT-BTTTT ngày 18/8/2015 quy định về quản lý và sử dụng tài nguyên internet.

đến BLHS năm 2015 được quy định thành mục riêng. Nội dung các quy định được hoàn thiện và bổ sung dần qua các lần sửa đổi, bổ sung và ban hành BLHS mới.

Thứ hai, BLHS năm 2015 đã quy định về tội phạm trong lĩnh vực CNTT, MVT trong 9 điều luật từ Điều 285 đến Điều 294 (trừ Điều 292). So sánh với các văn bản quốc tế về tội phạm trong lĩnh vực CNTT, MVT hiện nay cho thấy, về cơ bản BLHS năm 2015 đã hình sự hoá hầu hết các hành vi phạm tội trong lĩnh vực CNTT, MVT, phù hợp với xu thế chung của các nước trên thế giới. Tuy nhiên, trong các nội dung cụ thể, BLHS năm 2015 thường có quy định theo hướng hẹp hơn (phạm vi, đối tượng, …) so với quy định chung của các văn bản quốc tế. Mặc dù vậy, đây là cơ sở pháp lý quan trọng để các cơ quan có thẩm quyền đấu tranh có hiệu quả đối với tội phạm này.

Thứ ba, các hình phạt đối với tội phạm trong lĩnh vực CNTT, MVT được quy định trong BLHS năm 2015 khá đa dạng và phong phú, bao gồm: hình phạt tiền; hình phạt cải tạo không giam giữ; hình phạt tù có thời hạn; hình phạt cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm một công việc nhất định; tịch thu một phần hoặc toàn bộ tài sản. Trong đó, hình phạt tiền có xu hướng được quy định áp dụng nhiều hơn trước đây. Đây cũng là cơ sở để cơ quan có thẩm quyền lựa chọn hình phạt phù hợp áp dụng đối với từng trường hợp phạm tội trong lĩnh vực CNTT, MVT cụ thể.

Thứ tư, để phân hoá TNHS đối với tội phạm trong lĩnh vực CNTT, MVT BLHS năm 2015 đã quy định nhiều dấu hiệu định khung tăng nặng khác nhau. Các dấu hiệu định khung tăng nặng này được chia thành 4 nhóm, bao gồm: (1) các dấu hiệu định khung liên quan đến hành vi phạm tội; (2) các dấu hiệu định khung liên quan đến hậu quả của tội phạm; (3) các dấu hiệu định khung tăng nặng liên quan đến nhân thân của người phạm tội; các dấu hiệu định khung tăng nặng liên quan đến đối tượng tác động của tội phạm.

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

Các số liệu tác giả sử dụng để nghiên cứu trong phần này bao gồm: số liệu thống kê án xét xử sơ thẩm đối với tội phạm trong lĩnh vực CNTT, MVT của Toà án nhân dân tối cao từ năm 2009 đến năm 2020 trong phạm vi cả nước; gần 100 bản án hình sự sơ thẩm, phúc thẩm của Toà án các cấp trong cả nước từ năm 2009 được thu thập ngẫu nhiên; số liệu rút ra từ các công trình nghiên cứu, các bài báo khoa học có liên quan. Các số liệu này có tính đại diện để đánh giá thực trạng áp dụng các quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong thời gian qua.

Theo số liêu thống kê tại Bảng 1, trong giai đoạn 2009 - 2020 Toà 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. Đây là con số phản ánh kết quả đạt được trong việc áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT của ngành Tòa án. Kết quả đạt được này thể hiện sự cố gắng và hiệu quả trong việc áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT của Tòa án ngày càng được nâng cao. Số vụ án và số bị cáo bị xét xử sơ thẩm trong những năm gần đây có xu hướng cao hơn những năm trước. Kết quả này góp phần đấu tranh có hiệu quả đối với tội phạm trong lĩnh vực CNTT, MVT đang có xu hướng gia tăng trong những năm gần đây.

Bảng 1.

Số lượng vụ án và bị cáo bị xét xử sơ thẩm về tội phạm trong lĩnh vực CNTT, MVT từ năm 2009 đến năm 2020

Năm	Số vụ án	Số bị cáo	Ghi chú
2009	0	0	
2010	0	0	
2011	5	7	
2012	9	21	
2013	17	51	
2014	47	135	
2015	70	139	
2016	85	202	
2017	63	118	
2018	49	87	
2019	47	73	
2020	53	100	
Tổng số	**445**	**933**	

(Nguồn: Số liệu thống kê của Toà án nhân dân tối cao năm 2009 -2020)

Trong 2 năm đầu của giai đoạn nghiên cứu (2009 - 2010), không có vụ án nào được xét xử. Trước năm 2009, Toà án cả nước cũng chưa xét xử vụ án nào về tội phạm trong lĩnh vực CNTT, MVT. Bên cạnh đó, trong số gần 100 bản án mà tác giả thu thập ngẫu nhiên, không có bản án nào được xét xử trong những năm 2010 trở về trước. Các số liệu trên cho thấy, từ khi tội phạm trong lĩnh vực CNTT, MVT được quy định trong BLHS năm 1999 đến năm 2010, đã hơn 10 năm nhưng trong thực tiễn các quy định này chưa được áp dụng để xét xử tội phạm trong lĩnh vực CNTT, MVT. Trong 2 năm tiếp theo (2011-2012),

quy định của BLHS đã bắt đầu được áp dụng về xét xử tội phạm trong lĩnh vực CNTT, MVT nhưng số lượng rất ít. Cả nước trong 2 năm chỉ xét xử được 14 vụ án với 27 bị cáo. Trung bình mỗi năm xét xử được 7 vụ án với khoảng 14 bị cáo.

Trong các năm tiếp theo cho đến khi BLHS năm 2015 có hiệu lực (2013 - 2017) có sự gia tăng đột biến về số vụ án được xét xử về tội phạm trong lĩnh vực CNTT, MVT. Tổng số vụ án được xét xử trong giai đoạn này là 282 vụ với 645 bị cáo. Trung bình mỗi năm cả nước xét xử được 56 vụ án với 129 bị cáo. Nếu so sánh với giai đoạn 2011 - 2012, trung bình số vụ án được xét xử đã tăng 8 lần. Đây là điểm rất đáng chú ý vì bắt đầu giai đoạn này Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10 tháng 9 năm 2012 được ban hành.

Giai đoạn từ năm 2018 - 2020 là thời gian áp dụng quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT. Mặc dù quy định của BLHS năm 2015 đã kế thừa và bổ sung nhiều quy định mới so với BLHS năm 1999 nhưng việc áp dụng các quy định này có xu hướng giảm so với giai đoạn 2013 - 2017. Cụ thể, trong 3 năm (2018 - 2020) cả nước xét xử được 149 vụ án với 260 bị cáo. Trung bình mỗi năm xét xử được 49 vụ án với 86 bị cáo. So với giai đoạn trước trung bình mỗi năm giảm 7 vụ án.

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. Theo Bảng 2. (Số lượng vụ án về tội phạm trong lĩnh vực CNTT, MVT Tòa án đã thụ lý, trả hồ sơ điều tra bổ sung và còn tồn đọng từ năm 2009 đến năm 2020), 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 đó, tỷ lệ số vụ án được xét xử sơ thẩm đạt 73,2% số vụ án được giải quyết, số vụ án phải trả hồ sơ cho VKS chiếm 26,9% số vụ án được giải quyết.

Bảng 2. Số lượng vụ án về tội phạm trong lĩnh vực CNTT, MVT Tòa án đã thụ lý, trả hồ sơ điều tra bổ sung và còn tồn đọng từ năm 2009 đến năm 2020

Năm	Số vụ án phải giải quyết	Số vụ án được giải quyết				Số vụ án tồn đọng	
		Số vụ án trả hồ sơ cho VKS		Số vụ án được xét xử			
		Số lượng	Tỷ lệ số vụ trả hồ sơ trên số vụ án được giải quyết (%)	Số lượng	Tỷ lệ số vụ xét xử sơ thẩm trên số vụ án được giải quyết (%)	Số lượng	Tỷ lệ số vụ tồn đọng so với số vụ án phải giải quyết (%)
2009							
2010							
2011	10	2	28,5	5	71,5	3	30
2012	10	0	0	9	100	1	10
2013	45	10	37	17	63	18	40
2014	94	24	33,8	47	66,2	23	24,4
2015	122	25	26,3	70	73,6	27	22,1
2016	136	35	29,1	85	69,9	16	11,7
2017	106	27	30	63	70	16	15
2018	72	14	22,2	49	77,8	9	12,5
2019	75	14	22,9	47	77,1	14	18,6
2020	68	12	18,4	53	81,6	3	4,4
Tổng cộng	**738**	**163**	**26,8**	**445**	**73,2**	**130**	**17,6**

(Nguồn: Số liệu thống kê của Toà án nhân dân tối cao năm 2009 - 2020)

Theo Bảng số liệu trên, tỷ lệ số vụ án tồn đọng so với số vụ án phải giải quyết của Tòa án có xu hướng giảm dần. Tỷ lệ số vụ án tồn đọng trung bình trong giai đoạn (2011 - 2017) khi thực hiện BLHS năm 1999 là 21,8 %. Trong khi đó, giai đoạn 2018 - 2020, khi thực hiện BLHS năm 2015 giảm xuống còn 11,8 %. Đồng thời, tỷ lệ số vụ án mà Tòa án phải trả hồ sơ cho VKS trên số vụ án giải quyết cũng có xu hướng giảm dần. Trong giai đoạn 2011 - 2017 tỷ lệ này là 26,3 %, còn trong giai đoạn 2018 - 2020 là 21,1 %. Các số liệu trên cho thấy hiệu quả trong việc áp dụng quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT của Tòa án ngày càng được nâng lên. Tuy nhiên, tỷ lệ số án tồn đọng trên số vụ án cần giải quyết và tỷ lệ số vụ án mà Tòa án trả hồ sơ cho VKS trên số vụ án đã giải quyết còn cao. Điều đó cũng cho thấy việc áp dụng quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT còn nhiều khó khăn, vướng mắc.

Kết quả áp dụng quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT của Tòa án còn được thể hiện trong từng quy định cụ thể. Trong mỗi giai đoạn, kết quả này cũng có sự thay đổi, khác nhau. Điều đó được thể hiện qua Bảng 3 (Số lượng vụ án và bị cáo đã xét xử sơ thẩm về tội phạm trong lĩnh vực CNTT, MVT theo từng điều luật từ năm 2009 đến năm 2020) dưới đây:

Bảng 3. Số lượng vụ án và bị cáo đã xét xử sơ thẩm về tội phạm trong lĩnh vực CNTT, MVT theo từng điều luật từ năm 2009 đến năm 2020

*** Giai đoạn 2009 – 2017 (BLHS năm 1999 có hiệu lực)**

Năm		**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Điều 224	Vụ									
	Bị cáo									
Điều 225	Vụ			1	1			1	1	
	Bị cáo			1	1			1	2	

Điều 226	Vụ			4	6	2	8	12	10	7
	Bị cáo			6	16	9	21	19	17	10
Điều 226a	Vụ				1	1	1	1	1	5
	Bị cáo				2	2	2	1	2	16
Điều 226b	Vụ				1	14	38	56	73	51
	Bị cáo				2	40	112	118	181	92

*** Giai đoạn 2018 – 2020 (BLHS năm 2015 có hiệu lực**

Năm		**2018**	**2019**	**2020**
Điều 285	Vụ	1	1	
	Bị cáo	2	3	
Điều 286	Vụ			
	Bị cáo			
Điều 287	Vụ	1	1	
	Bị cáo	1	1	
Điều 288	Vụ			3
	Bị cáo			3
Điều 289	Vụ	5	1	1
	Bị cáo	7	1	1
Điều 290	Vụ	42	44	48
	Bị cáo	77	68	95
Điều 291	Vụ			1
	Bị cáo			1
Điều 293	Vụ			
	Bị cáo			
Điều 294	Vụ			
	Bị cáo			

(Nguồn: Số liệu thống kê của Toà án nhân dân tối cao năm 2009 - 2020)

Số liệu trên cho thấy một số điều luật thường xuyên được áp dụng để xét xử tội phạm trong lĩnh vực CNTT, MVT như tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện việc chiếm đoạt tài sản (Điều 226b BLHS năm 1999 và Điều 290 BLHS năm 2015), tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 226a BLHS năm 1999 và Điều 289 BLHS năm 2015), tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 226 BLHS năm 1999 và Điều 288 BLHS năm 2015). Ngược lại, một số quy định chưa được áp dụng hoặc ít khi được áp dụng như: Điều 224 BLH năm 1999, Điều 286 BLHS năm 2015; Điều 291, Điều 293, Điều 294 BLHS năm 2015. Các điều luật còn lại như Điều 285 BLHS năm 2015; Điều 225 BLHS năm 1999, Điều 287 BLHS năm 2015 ít khi được áp dụng.

Kết quả áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT để quyết định hình phạt của Tòa án được thể hiện trong Bảng 4 (Tình hình áp dụng loại và mức hình phạt đối với bị cáo bị xét xử về tội phạm trong lĩnh vực CNTT, MVT từ năm 2009 đến năm 2020). Đối với hình phạt chính, đa số bị cáo bị áp dụng hình phạt tù chiếm 94,3 % tổng số bị cáo, hình phạt tiền chiếm 3,6%, hình phạt cải tạo không giam giữ chiếm 1,7% và hình phạt cảnh cáo chiếm 0,4%. Trong số những bị cáo bị áp dụng hình phạt tù, mức phạt tù phổ biến nhất là từ 3 năm tù trở xuống, chiếm 49,8%, mức phạt tù trên 3 năm tù đến 7 năm tù chiếm 24,9%, mức phạt tù trên 7 năm tù đến 15 năm tù chiếm 17,4% và mức phạt tù trên 15 năm tù đến 20 năm tù chiếm 2,2%. Điều đáng chú ý là Tòa án đã cho hưởng án treo với tỷ lệ rất cao, chiếm 21,6% trên tổng số bị cáo. Nếu chỉ tính riêng số bị cáo bị áp dụng mức phạt tù từ 3 năm trở xuống, tỷ lệ hưởng án treo đạt 43,4% (202 bị cáo được hưởng án treo trên tổng số 465 bị cáo bị phạt tù từ 3 năm trở xuống). Hình phạt bổ sung ít được áp dụng đối với bị cáo phạm tội trong lĩnh vực CNTT, MVT. Trong số các

hình phạt bổ sung được quy định có thể áp dụng với các bị cáo, hình phạt tiền được áp dụng với tỷ lệ 4,6 % số bị cáo bị xét xử; trục xuất được áp dụng với tỷ lệ 0,8%.

Bảng 4. Tình hình áp dụng loại và mức hình phạt đối với bị cáo bị xét xử về tội phạm trong lĩnh vực CNTT, MVT từ năm 2009 đến năm 2020

TT	Hình phạt	Số bị cáo	Tỷ lệ (%) trên tổng số bị cáo bị (933)
I	**Hình phạt chính**		
1	Cảnh cáo	1	0,4
2	Phạt tiền	34	3,6
3	Cải tạo không giam giữ	16	1,7
4	Trục xuất	0	0
5	Tù từ 3 năm trở xuống	465	49,8
6	Tù trên 3 -7 năm	233	24,9
7	Tù từ trên 7-15 năm	163	17,4
8	Tù từ trên 15 năm đến 20 năm	21	2,2
II	**Hình phạt bổ sung**		
1	Tịch thu tài sản	0	0
2	Phạt tiền	42	4,6
4	Trục xuất	8	0,8
III	**Án treo**	202	21,6

(Nguồn: Số liệu thống kê của Toà án nhân dân tối cao năm 2009 -2020)

Kết quả nghiên cứu gần 100 bản án về tội phạm trong lĩnh vực CNTT, MVT mà tác giả thu thập được cho thấy, đa số các bản án về tội sử dụng

mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản quy định tại Điều 226b BLHS năm 1999 và Điều 290 BLHS năm 2015, chiếm 83%. Việc áp dụng khung hình phạt đối với tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản quy định tại Điều 226b BLHS năm 1999 và Điều 290 BLHS năm 2015 trong các bản án: 20% áp dụng khoản 1 có mức phạt tiền từ 10 triệu đồng đến 100 triệu đồng hoặc phạt tù từ 1 năm đến 5 năm; 54% áp dụng khoản 2 có mức phạt tù từ 3 năm đến 7 năm; 18% áp dụng khoản 3 có mức phạt tù từ trên 7 năm đến 15 năm và 8% áp dụng khoản 4 có mức phạt tù trên 15 năm đến 20 năm hoặc tù chung thân. Đối với tội xâm nhập trái phép mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 226a BLHS năm 1999) có 66% áp dụng khoản 3 có mức phạt từ từ 5 năm đến 12 năm; còn lại 34% áp dụng khoản 1 mức phạt tiền từ 20 triệu đến 200 triệu đồng hoặc phạt tù từ 1 năm đến 5 năm. Như vậy, các tội phạm này đa số áp dụng hình phạt tù có mức hình phạt từ 3 năm đến 7 năm.

Thực tiễn xét xử cho thấy một điểm đáng chú ý là người nước ngoài phạm tội trong lĩnh vực CNTT, MVT tại Việt Nam chiếm tỷ lệ cao. Theo Bảng 5 (Số lượng bị cáo là người nước ngoài bị xét xử sơ thẩm về tội phạm trong lĩnh vực CNTT, MVT từ năm 2009 đến năm 2020), trung bình tỷ lệ bị cáo là người nước ngoài trên tổng số bị cáo bị xét xử sơ thẩm về tội phạm trong lĩnh vực CNTT, MVT là 9%. Giai đoạn từ năm 2013 đến 2015 tỷ lệ này rất cao, có năm lên đến 35,29%. Tuy những năm gần đây, tỷ lệ này có xu hướng giảm nhưng vẫn cao hơn nhiều so với những tội phạm khác. Nguyên nhân các vụ án về tội phạm trong lĩnh vực CNTT, MVT có tỷ lệ bị cáo là người nước ngoài cao là do đặc điểm của tội phạm này. Tội phạm này có tính chất quốc tế cao do việc thực hiện tội phạm không bị giới hạn về không gian địa lý và biên giới quốc gia. Bên cạnh đó, đây cũng là tội phạm có liên quan đến lĩnh vực công nghệ, kỹ thuật hiện đại đã được phát triển và ứng dụng rộng rãi ở nước ngoài.

Bảng 5. Số lượng bị cáo là người nước ngoài bị xét xử sơ thẩm về tội phạm trong lĩnh vực CNTT, MVT từ năm 2009 đến năm 2020

Năm	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Tổng số bị cáo	7	21	51	135	139	202	118	87	73	100
Số bị cáo là người nước ngoài	0	0	18	14	19	8	4	8	2	11
Tỷ lệ %	0	0	35,29	10,37	13,66	3,96	3,38	6,89	2,7	11

(Nguồn: Số liệu thống kê của Toà án nhân dân tối cao năm 2009 - 2020)

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

Thông qua việc nghiên cứu thực tiễn áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong thời gian qua (2009 - 2020), có thể rút ra một số kết luận về những hạn chế, khó khăn, vướng mắc trong thực tiễn như 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:

Có thể có trường hợp BLHS đã có quy định về một tội phạm nhưng quy định đó chưa bao giờ được áp dụng do tội phạm chưa xảy ra trong thực tế. Nhưng nếu BLHS đã có quy định và tội phạm đó đã xảy ra trên thực tế mà

các điều luật đó lại không áp dụng để xử lý được thì đó là một tồn tại, hạn chế. Qua các số liệu khảo sát cho thấy trong 12 năm (2009 - 2020), TAND cả nước chỉ xét xử được 445 vụ án với 933 bị cáo. Trung bình mỗi năm xét xử được khoảng 37 vụ án với 77 bị cáo. Trong khi đó, theo đánh giá của các cơ quan chức năng, thực tế trong xã hội loại tội phạm này đang diễn ra phổ biến. Theo số liệu báo cáo của Cục cảnh sát phòng chống tội phạm sử dụng công nghệ cao thì trong cả nước đã xác minh hàng trăm đầu mối vụ việc có dấu hiệu tội phạm và đã khởi tố điều tra: năm 2011 số vụ việc loại này là 120 vụ; năm 2012 là 214 vụ; năm 2013 là 282 vụ. Trong đó hành vi sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản chiếm tỷ lệ cao nhất (hàng năm vào khoảng 50% đến 60% tổng số vụ việc). Thực trạng về tội phạm trong lĩnh vực CNTT, MVT thường được các chuyên gia nhận định là "báo động đỏ" của an ninh mạng Việt Nam với rất nhiều vụ tấn công, phá hoại, lây nhiễm vi - rút, phầm mềm gián điệp, mã tin học độc hại..., nhằm vào hệ thống mạng của cơ quan, doanh nghiệp, tập đoàn kinh tế của Nhà nước với mức độ, tính chất ngày càng nghiêm trọng, làm rối loạn hoạt động của hệ thống và lộ lọt thông tin[141]. Có chuyên gia còn cho rằng Việt Nam đang là "chỗ trũng" về tội phạm công nghệ từ các cuộc tấn công mạng theo phương thức cổ điển tới những hình thức mới xuất hiện[142]. Theo thống kê từ hệ thống giám sát vi - rút của Bkav, hơn 1,6 triệu lượt máy tính tại Việt Nam bị mất dữ liệu trong năm 2018; thiệt hại do virus máy tính

---

[141] Xem: Hồ Thế Hòe, *"Giải pháp nâng cao hiệu quả đấu tranh với tội phạm sử dụng công nghệ cao trong bối cảnh toàn cầu hóa"*: http://tks.edu.vn/thong-tin-khoa-hoc/chi-tiet /79/687 (truy cập ngày 15/1/2020).

[142] Xem: Thu Trang, *"Khó khăn trong xử lý tội phạm công nghệ cao"* http://nguoibaovequyenloi.com/User/ThongTin_ChiTiet.aspx?MaTT=18220155314078972&MaMT=24 (truy cập ngày 15/1/2020).

gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 14.900 tỷ đồng, tương đương 642 triệu USD, nhiều hơn 21% so với mức thiệt hại của năm 2017[143]. Tuy nhiên, số lượng vụ án về tội phạm trong lĩnh vực CNTT, MVT trong giai đoạn 2011 - 2013 được TAND xét xử chỉ có 31 vụ án. Trong đó, tội phát tán chương trình tin học gây hại (Điều 224 BLHS năm 1999 và Điều 286 BLHS năm 2015) chưa có vụ án nào được đưa ra xét xử. Từ khi BLHS năm 2015 có hiệu lực (01/01/2018), các quy định này cũng không được áp dụng nhiều. Trong 3 năm (2018 - 2020) đã xét xử được 149 vụ án với 260 bị cáo; trung bình mỗi năm xét xử được khoảng 50 vụ án với 86 bị cáo. Tình trạng các cơ quan có thẩm quyền gặp khó khăn khi áp dụng quy định của BLHS để xử lý tội phạm trong lĩnh vực CNTT, MVT là một tồn tại, hạn chế cần được khắc phục trong thời gian tới.

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

Trong quá trình điều tra, truy tố, xét xử tội phạm trong lĩnh vực CNTT, MVT, còn nhiều trường hợp giữa CQĐT, VKS và TAND áp dụng quy định của LHS chưa thống nhất. Điều đó phần nào được thể hiện thông qua số con số các vụ án mà TAND trả hồ sơ lại cho VKS để điều tra bổ sung. Tỷ lệ số vụ án mà TAND thụ lý sau đó phải trả hồ sơ cho VKS luôn trong khoản từ 20% - 25%. So với tỷ lệ TAND trả hồ sơ cho VKS để điều tra bổ sung đối với các vụ án khác tỷ lệ này là rất cao. Ví dụ: tỷ lệ TAND trả hồ sơ cho VKS để điều tra đối với các vụ án xâm phạm sở hữu chỉ có 5,5%[144]. Đối với các vụ án hình

---

[143] Xem: http://m.bkav.com.vn/tin_tuc_noi_bat/-/chi_tiet/601424/tong-ket-an-ninh-mang nam-2018-va-du-bao-xu-huong-2019 (truy cập ngày 15/1/2020).

[144] Số liệu thống kê của TAND tối cao năm 2014 đối với các tội xâm phạm sở hữu: Tổng số vụ án cần giải quyết 28.159, số vụ án trả hồ sơ cho VKS là 1572 vụ, số vụ án xét xử sơ thẩm 26.094, số vụ án tồn đọng 425 vụ.

sự nói chung, tỷ lệ trả hồ sơ thường không quá 10%. Như vậy, tỷ lệ TAND trả hồ sơ cho VKS để điều tra bổ sung khi giải quyết vụ án về tội phạm trong lĩnh vực CNTT, MVT đã gấp 2,0 đến 2,5 lần các vụ án khác. Có vụ án khi TAND trả hồ sơ cho VKS nhưng VKS không nhất trí.

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:

Đây là một khó khăn của các cơ quan tiến hành tố tụng khi giải quyết các vụ án về tội phạm trong lĩnh vực CNTT, MVT. Loại tội phạm này luôn xuất hình những hành vi mới, chưa được quy định cụ thể trong BLHS, đòi hỏi các cơ quan tiến hành tố tụng phải vận dụng các quy định hiện có để giải quyết. Điều này cũng sẽ dẫn đến các quan điểm giải quyết không thống nhất, còn nhiều ý kiến khác nhau sau khi xét xử. Ví dụ: Do BLHS năm 1999 chưa quy định cụ thể về hành vi lắp đặt, thuê kênh riêng, sử dụng dịch vụ viễn thông để chiếm đoạt tiền cước viễn thông nên việc xử lý hành vi này có nhiều quan điểm khác nhau. Có quan điểm cho rằng, rằng, hành vi này phạm tội kinh doanh trái phép (Điều 159 BLHS năm 1999)[145]; Quan điểm khác lại cho rằng, hành vi này phạm tội vi phạm các quy định về nghiên cứu, thăm dò, khai thác tài nguyên (Điều 172 BLHS năm 1999) hoặc phạm tội sử dụng trái phép tài sản (Điều 142 BLHS năm 1999)[146]; Có quan điểm lại cho rằng, hành vi này phạm tội trộm cắp tài sản (Điều 138 BLHS năm 1999)[147]. Trên thực tế, đa số các bản án của TAND đều xét xử hành vi này về tội trộm cắp tài sản.

[145] Xem: Trần Vũ Hải (2004), "Lắp đặt, sử dụng thiết bị viễn thông để thu lợi cước điện thoại trái phép - Có thể bị truy tố về tội kinh doanh trái phép", *Tạp chí Tòa án nhân dân*, số 22 (tháng 11/2004).

[146] Xem: Phạm Văn Lợi (2007), Tlđd, tr.101 - 102.

[147] Xem: Đỗ Văn Chỉnh (2004), "Xác định tội trộm cắp tài sản đối với người lắp đặt thiết bị thu phát viễn thông để thu lợi bất chính là có căn cứ", *Tạp chí Tòa án nhân dân*, số 19 (tháng 10/2004).

Tuy nhiên, nhiều quan điểm cũng cho rằng, đây là loại hành vi nguy hiểm cho xã hội mới xuất hiện, cần được quy định cụ thể trong BLHS. Tác giả cho rằng đây là quan điểm chính xác. Hành vi mới này cần được quy định cụ thể trong BLHS để việc áp dụng được chính xác và thống nhất.

Trong quá trình giải quyết vụ án hình sự về tội phạm trong lĩnh vực CNTT, MVT các cơ quan tiến hành tố tụng đã gặp khó khăn khi phải xử lý những hành vi phạm tội mới xuất hiện trong khi BLHS chưa quy định cụ thể. Ví dụ: Theo bản án hình sự phúc thẩm số 361/2017/HS-PT ngày 20/7/2017 của TAND cấp cao tại Thành phố Hồ Chí Minh, Đ đã có hành vi mua, sau đó bán phần mềm nghe lén, theo dõi điện thoại trên các thiết bị di động cho các khách hàng. Khách hàng nào không biết cài đặt thì Đ cài đặt hộ và hướng dẫn cách sử dụng. Trong khoảng thời gian từ 2012 - 2015, Đ đã bán cho rất nhiều khách hàng khác nhau. Trong vụ án này, bản chất hành vi phạm tội của Đ là hành vi mua bán trái phép phần mềm để sử dụng vào mục đích trái pháp luật. Nhưng tại thời điểm từ năm 2012 - 2015, BLHS năm 1999 không quy định về tội này nên các cơ quan tiến hành tố tụng buộc phải chứng minh Đ có hành vi cài đặt phần mềm này cho khách hàng để vận dụng xử vào tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng internet hoặc thiết bị số của người khác (Điều 226b). Giả sử Đ chỉ bán phần mềm mà không hỗ trợ cài đặt hộ cho khách thì sẽ không xử vào tội này được.

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:

Đối với hành vi sử dụng CNTT, MVT để thực hiện tội phạm dễ bị nhầm lẫn giữa tội phạm trong lĩnh vực CNTT, MVT với tội phạm "truyền thống". Chẳng hạn nhầm lẫn giữa tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 290) với tội trộm cắp tài sản (Điều 173) hoặc tội lừa đảo chiếm đoạt tài sản (Điều 174) BLHS năm 2015.

Ví dụ: A và B cùng thuê trọ chung phòng với nhau. B đã lấy trộm thẻ ATM của A. Do biết được thông tin tài khoản và mật khẩu nên B đã sử dụng thẻ ATM của A để rút tiền với số tiền 16,5 triệu đồng. Việc xử lý hành vi của B và những hành vi tương tự như vậy có 2 quan điểm khác nhau:

Quan điểm thứ nhất cho rằng, B phạm tội trộm cắp tài sản theo Điều 173 BLHS năm 2015. Quan điểm này được thể hiện trong bản án số 46/2018/HSST ngày 17/5/2018 của Tòa án nhân dân TX. Phổ Yên, tỉnh Thái Nguyên, xét xử bị cáo G về tội trộm cắp tài sản theo khoản 1 Điều 173 (Tội trộm cắp tài sản)[148]. Quan điểm này cũng được thể hiện trong Cáo trạng số 57/KSĐT-KT ngày 11/9/2017 VKSND huyện Bình Xuyên truy tố Lê Thị H về tội trộm cắp tài sản (khoản 1 Điều 138 BLHS năm 1999)[149].

Quan điểm thứ hai cho rằng, B phạm 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 hoặc Điều 226b BLHS năm 1999). Quan điểm này được thể hiện trong bản án số 11/2018/HS-ST ngày 19/1/2018 của Tòa án nhân dân quận 3, TP. Hồ Chí Minh xét xử Nguyễn Ngọc Anh Quốc về hành vi trộm cắp 2 thẻ tín dụng, sau đó thanh toán hàng hóa đã mua với số tiền 115.000.000 đồng theo điểm đ khoản 2 Điều 290 BLHS năm 2015; Bản án số 290/2017/HSPT ngày 20/4/2017 của Tòa án nhân dân Hà Nội; Bản án số 59/2017/HSST ngày 28/9/2017 của TAND huyện Bình Xuyên, tỉnh Vĩnh Phúc.

Có thể thấy, trong các hành vi trên các đối tượng đã sử dụng thông tin tài khoản là thông tin và mật khẩu của thẻ ATM của nạn nhân để chiếm đoạt tài sản. Việc lấy trộm được thẻ ATM của nạn nhân chỉ là bước đầu để có được thông tin tài khoản chứ chưa chiếm đoạt được tài sản của nạn nhân. Do đó,

---

[148] Xem: Bản án 46/2018/HSST ngày 17/5/2018 của TAND TX. Phổ Yên, Thái Nguyên;

[149] Xem: Bản án số 59/2017/HSST ngày 28/9/2017 của TAND huyện Bình Xuyên, tỉnh Vĩnh Phúc.

việc xác định các đối tượng trên đã sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản theo Điều 290 BLHS năm 2015 là chính xác.

Việc xác định tội danh đối với hành vi dùng thẻ ngân hàng giả để rút tiền của người khác tại các ngân hàng cũng có nhiều quan điểm khác nhau. Quan điểm thứ nhất cho rằng hành vi này phạm tội trộm cắp tài sản theo Điều 138 BLHS năm 1999[150]. Quan điểm thứ hai cho rằng hành vi này phạm tội lừa đảo chiếm đoạt tài sản theo Điều 139 BLHS năm 1999[151]. Tác giả cho rằng, quan điểm thứ hai có nhiều điểm hợp lý hơn. Người phạm tội đã sử dụng thẻ giả để giao dịch với ngân hàng nhưng ngân hàng không phát hiện ra mà giao tiền cho người phạm tội. Tuy nhiên, xét về bản chất, đây là hành vi nguy hiểm cho xã hội mới xuất hiện, cần phải có quy định của BLHS cụ thể để tội phạm hóa hành vi này. Do đó, BLHS năm 2015 đã quy định về hành vi sử dụng thẻ ngân hàng giả tại Điều 291.

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

Điều đó được thể hiện thông qua việc áp dụng không chính xác, không thống nhất các căn cứ quyết định hình phạt, cũng như việc quyết định hình phạt cụ thể. Cụ thể:

- Đối với tình tiết "Phạm tội nhiều lần" (theo BLHS năm 1999) hoặc "phạm tội từ 2 lần trở lên" (theo BLHS năm 2015):

Trong số những bản án mà tác giả thu thập, vẫn còn một số bản án áp dụng tình tiết tăng nặng TNHS "phạm tội nhiều lần" hoặc "phạm tội từ 2 lần

---

[150] Xem: Lê Đăng Doanh (2006), "Về tội danh đối với hành vi làm, sử dụng, thẻ tín dụng giả hay các thẻ khác để mua hàng hóa hoặc rút tiền tại máy trả tiền tự động của các ngân hàng", *Tạp chí Tòa án nhân dân*, số 6/2006, tr.24.

[151] Xem: Lê Đăng Doanh (2006), Tlđd, tr.26.

trở lên" không đúng pháp luật. Có vụ án người phạm tội đã thực hiện tội phạm rất nhiều lần trong thời gian dài, đối với nhiều nạn nhân khác nhau nhưng TAND lại không áp dụng tình tiết tăng nặng TNHS "phạm tội nhiều lần". Ví dụ: từ tháng 12/2012 đến tháng 4/2015 Đ đã bán phần mềm theo dõi điện thoại cho khách hàng, đồng thời hỗ trợ cài đặt phần mềm đó vào điện thoại của khách hàng. Tổng số có 87 lượt khách hàng mua và cài đặt phần mềm. Nhưng bản bản án số 361/2017/HS-PT ngày 20/7/2017 của TAND cấp cao tại TP. Hồ Chí Minh vẫn không áp dụng tình tiết tăng nặng TNHS "phạm tội nhiều lần". Việc không áp dụng tình tiết tăng nặng TNHS "phạm tội nhiều lần" trong trường hợp này là không đúng pháp luật. Trong khi đó, có nhiều bản án đã áp dụng đúng pháp luật đối với tình tiết này. Ví dụ: P là nhân viên của Công ty Bảo Nam. Do bị cho nghỉ việc nên P đã nhiều lần xâm nhập vào trang mạng của công ty khác để phá hoại gây thiệt hại cho công ty gần 9 triệu đồng. Hành vi của P đã bị TAND huyện Hóc Môn, TP. Hồ Chí Minh kết án phạm tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng internet hoặc thiết bị số của người khác (Điều 226a BLHS năm 1999) và áp dụng tình tiết tăng nặng TNHS "phạm tội nhiều lần" tại điểm g khoản 1 Điều 48 BLHS năm 1999. Việc Toà án áp dụng tình tiết tăng nặng TNHS "phạm tội nhiều lần" trong trường hợp này là đúng pháp luật.

- Đối với tình tiết giảm nhẹ TNHS "phạm tội lần đầu" thuộc khoản 2 Điều 46 BLHS năm 1999 cũng có bản án áp dụng sai. Ví dụ: Bị cáo phạm tội sử dụng mạng máy tính, mạng viễn thông, mạng internet thực hiện hành vi chiếm đoạt tài sản (Điều 226b) 4 lần với 4 nạn nhân khác nhau vào ngày 08/9/2016, 29/9/2016, 3/10/2016 và đầu tháng 10/2016. Tuy nhiên, trong bản án số 26/2017/HSST ngày 27/9/2017 của TAND huyện Nghi Xuân, Hà Tĩnh, Hội đồng xét xử đã nhận định *"bị cáo phạm tội lần đầu, ...đây không phải là tình tiết giảm nhẹ nhưng cũng cần thiết xem xét khi lượng hình phù hợp với*

khoản 2 Điều 46 BLHS năm 1999”. Việc nhận định và áp dụng tình tiết “phạm tội lần đầu” trong trường hợp này là không chính xác. Theo hướng dẫn của TAND Tối cao tại văn bản giải đáp nghiệp vụ số 01/2017/GĐ-TANDTC ngày 07/4/2017, nếu trước đó đã phạm tội và chưa bị kết án, chưa hết thời hiệu truy cứu TNHS, nay bị truy cứu TNHS trong cùng lần phạm tội sau thì không được coi là phạm tội lần đầu.

- Một số bản án áp dụng Điều 47 (Quyết định hình phạt nhẹ hơn quy định của Bộ luật) không đúng, do không áp dụng tình tiết tăng nặng TNHS “phạm tội nhiều lần” hoặc “phạm tội từ 2 lần trở lên”, đồng thời lại áp dụng tình tiết giảm nhẹ TNHS tại khoản 2 Điều 48 BLHS năm 1999 sai. Ví dụ: Trong bản án số 361/2017/HS-PT ngày 20/7/2017 của TAND cấp cao tại Thành phố Hồ Chí Minh, bị cáo có hành vi bán phần mềm theo dõi điện thoại cho khách hàng, đồng thời hỗ trợ cài đặt phần mềm đó vào điện thoại của khách hàng trong suốt thời gian từ tháng 12/2012 đến tháng 4/2015. Tổng cộng có 87 lượt khách hàng mua và cài đặt phần mềm. Bị cáo bị tuyên phạm tội “Truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng internet hoặc thiết bị số của người khác”, áp dụng điểm c khoản 3 Điều 226a; điểm b, p khoản 1 Điều 46; Điều 47 của BLHS năm 1999. Như vậy, vì có 2 tình tiết giảm nhẹ và không có tình tiết tăng nặng TNHS nên Hội đồng xét xử đã áp dụng Điều 47 của BLHS năm 1999. Tuy nhiên, bản án đã sai khi không áp dụng tình tiết tăng nặng TNHS “phạm tội nhiều lần” nên dẫn đến áp dụng Điều 47 là không phù hợp. Vì nếu có 2 tình tiết giảm nhẹ TNHS và 1 tình tiết tăng nặng TNHS sẽ không thể áp dụng Điều 47 BLHS năm 1999.

Bên cạnh đó, vẫn còn có trường hợp áp dụng không đúng tinh thần của Điều 47 BLHS năm 1999. Theo điểm c khoản 10 Nghị quyết số 01/2000/NQ-HĐTP ngày 04/8/2000 hướng dẫn áp dụng một số quy định phần chung BLHS năm 1999, những trường hợp nếu không có nhiều tình tiết giảm nhẹ thì

bị cáo bị xử phạt ở mức cao của khung hình phạt, thì (khi có nhiều tình tiết giảm nhẹ) TAND có thể quyết định một hình phạt ở mức thấp của khung hình phạt mà bị cáo bị xét xử, không thể áp dụng hình phạt ở dưới khung. Nhưng một số bản án đã không áp dụng đúng tinh thần này. Ví dụ: Trong bản án số 41/2017/HSST ngày 27/12/2017 của TAND tỉnh Quảng Trị, bị cáo D phạm tội "sử dụng mạng internet thực hiện hành vi chiếm đoạt tài sản" 3 lần với 3 nạn nhân khác nhau. Tổng giá trị tài sản chiếm đoạt là 274 triệu đồng. D bị áp dụng điểm a khoản 3 Điều 226b BLHS năm 1999. Tội này có khung hình phạt từ 7 đến 15 năm đối với trường hợp chiếm đoạt tài sản có giá trị từ 200 triệu đến dưới 500 triệu. Bị cáo D có 2 tình tiết giảm nhẹ và 01 tình tiết tăng nặng TNHS nhưng TA vẫn áp dụng Điều 47 để quyết định hình phạt dưới mức thấp nhất của khung hình phạt là 3 năm tù. Việc áp dụng Điều 47 trong trường hợp này là không phù hợp vì D có 2 tình tiết giảm nhẹ nhưng lại có 1 tình tiết tăng nặng TNHS. Hơn nữa, với số tiền chiếm đoạt 274 triệu đồng là ở mức cao của khung hình phạt tại điểm a khoản 3 Điều 226b BLHS năm 1999.

- Trong khi xét xử TAND đã cho các bị cáo phạm tội trong lĩnh vực CNTT, MVT hưởng án treo nhiều, chiếm tới 28% tổng số bị cáo bị xét xử. Tuy nhiên việc áp dụng cho hưởng án treo không thống nhất. Có trường hợp tội nặng lại cho hưởng án treo. Ví dụ trường hợp bị cáo D phạm tội "sử dụng mạng internet thực hiện hành vi chiếm đoạt tài sản" chiếm đoạt 274 triệu của 3 người khác nhau, bị áp dụng điểm a khoản 3 Điều 226b BLHS 1999, bị phạt 3 năm tù và cho hưởng án treo[152]. Trong khi đó, bị cáo H cũng phạm tội "sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt" của 1 nạn nhân 2,2 triệu đồng, bị áp dụng khoản 1 Điều 290 BLHS năm 2015, có 3 tình tiết giảm nhẹ, không có tình tiết tăng nặng TNHS

[152] Bản án số 41/2017/HSST ngày 27/12/2017 của TAND tỉnh Quảng Trị.

nào, bị phạt tù giam 6 tháng, nhưng không cho hưởng án treo[153].

Việc áp dụng hình phạt đối với tội phạm trong lĩnh vực CNTT, MVT còn nhẹ, hình phạt bổ sung ít được áp dụng. Đa số các bị cáo bị áp dụng khoản 1 hoặc khoản 2 của các tội trong lĩnh vực CNTT, MVT, theo đó mức phạt không quá 7 năm tù. So với tính chất và mức độ nguy hiểm cho xã hội của loại tội phạm này, mức hình phạt trên được coi là nhẹ. Đây cũng là nhận định của tác giả Trần Cảnh Hưng[154]. Bên cạnh đó, hình phạt bổ sung, nhất là hình phạt tiền ít được áp dụng. BLHS năm 2015 quy định nhiều loại hình phạt bổ sung đối với tội phạm trong lĩnh vực CNTT, MVT nhất là hình phạt tiền và tịch thu tài sản. Tuy nhiên, hình phạt tịch thu tài sản chưa được áp dụng. Còn hình phạt tiền mặc dù được quy định rất nhiều trong BLHS năm 2015 nhưng cũng được áp dụng không nhiều, chỉ có 2 bị cáo bị áp dụng hình phạt tiền là hình phạt chính và 74 bị cáo bị áp dụng hình phạt tiền là hình phạt bổ sung.

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

Trong các vụ án về tội phạm trong lĩnh vực CNTT, MVT, số bị cáo là người nước ngoài chiếm tỷ lệ khá cao. Trung bình tỷ lệ bị cáo là người nước ngoài trong giai đoạn 2009 - 2020 là 9%. Tuy nhiên, có năm tỷ lệ này rất cao như năm 2013 tỷ lệ bị cáo là người nước ngoài chiếm 35,2%. Trong khi đó, tỷ lệ này ở các tội xâm phạm sở hữu chỉ chiếm 0,04%[155]. Điều này gây ra những khó khăn không nhỏ cho các cơ quan tiến hành tố tụng. Bởi vì việc điều tra, xử lý gặp khó khăn; bên cạnh đó việc xử lý liên quan đến pháp luật quốc tế,

---

[153] Bản án số 59/2017/HSST ngày 28/9/2017 của TAND huyện Bình Xuyên, Vĩnh Phúc.

[154] Xem: Trần Cảnh Hưng (2003), "Một số vấn đề lý luận và thực tiễn về tội phạm máy tính", *Tạp chí Kiểm sát*, số 1/2003, tr. 27.

[155] Theo số liệu thống kê của TAND tối cao năm 2014, đối với các vụ án xâm phạm sở hữu trong năm 2014 có 41.920 bị cáo trong đó có 20 bị cáo là người nước ngoài.

luật quốc gia mà người đó là công dân, đến hoạt động và phối hợp của lực lượng cảnh sát quốc tế, của cơ quan tư pháp quốc tế.

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 quy định của Bộ luật hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

Bộ luật hình sự là công cụ sắc bén để đấu tranh chống và phòng ngừa tội phạm nói chung và tội phạm trong lĩnh vực CNTT, MVT nói riêng. Các quy định của BLHS đã góp phần không nhỏ vào thành công của công tác đấu tranh phòng chống tội phạm trong lĩnh vực CNTT, MVT. Tuy nhiên, so với yêu cầu các quy định này còn những bất cập nhất định. Đây chính là một trong những nguyên nhân gây ra những khó khăn, vướng mắc trong thực tiễn áp dụng. Những bất cập trong các quy định của BLHS bao gồm một số nội dung sau:

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:

Hiện nay, các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT đã được bổ sung, từng bước hoàn thiện. Tuy nhiên có thể thấy, so với yêu cầu thực tiễn của cuộc đấu tranh phòng chống loại tội phạm này, cũng như so với các văn bản pháp luật quốc tế, còn nhiều hành vi sử dụng CNTT, MVT để thực hiện tội phạm chưa được quy định trong BLHS[156]. Thực tiễn thi hành BLHS trong những năm qua đã chứng minh rằng, việc thiếu các quy định cụ thể để xử lý những hành vi phạm tội mới phát sinh đã gây ra nhiều

[156] Xem: Phụ lục 1. Bảng so sánh giữa các văn bản pháp luật quốc tế về tội phạm trong lĩnh CNTT, MVT

khó khăn cho các cơ quan tiến hành tố tụng khi giải quyết vụ án. Có tội dù đã được BLHS quy định nhưng lại quy định thiếu hành vi khách quan cụ thể. Ví dụ: Điều 285 BLHS năm 2015 đã quy định 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 nhưng chưa quy định về hành vi "chiếm hữu, sở hữu nhằm cho người khác sử dụng" hoặc "đề nghị người khác sử dụng, nhập khẩu" công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật. Trong thời gian tới, nếu những hành vi này không được kịp thời nghiên cứu kỹ để bổ sung quy định trong BLHS sẽ dẫn đến những khó khăn trong thực tế khi xử lý những hành vi này.

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

Lĩnh vực CNTT, MVT là lĩnh vực kỹ thuật cao, các khái niệm thường khó hiểu đối với những người không có chuyên môn sâu về lĩnh vực này. Các quy định của BLHS quy định về lĩnh vực CNTT, MVT vốn đã phức tạp, thêm vào đó các quy định này lại chung chung, không cụ thể. Do đó, nhiều nội dung nếu không được giải thích rõ sẽ khó áp dụng. Ví dụ, nếu không được hướng dẫn cụ thể, sẽ không xác định được phạm vi của "mạng máy tính" hay "gây hậu quả nghiêm trọng", "gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng" là gì để định tội và quyết định hình phạt. Những nội dung này đã được hướng dẫn tại Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012. Từ khi ban hành Thông tư liên tịch trên, các hạn chế, vướng mắc trong việc áp dụng quy định của BLHS năm 1999 mới dần được tháo gỡ, tạo thuận lợi cho các cơ quan tiến hành tố tụng.

Hiện nay, BLHS năm 2015 đã khắc phục phần nào hạn chế của BLHS năm 1999 bằng cách quy định cụ thể, rõ ràng hơn. Tuy nhiên, BLHS năm 2015 vẫn còn một số nội dung cần có sự hướng dẫn mới thực hiện được như: "công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, mạng viễn

thông hoặc phương tiện điện tử", "mục đích trái pháp luật" tại khoản 1 Điều 285; "thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân" tại khoản 1 Điều 288 và "dẫn đến biểu tình" tại điểm g khoản 2 Điều 288. Thời gian tới nếu các nội dung trên không có giải thích, hướng dẫn cụ thể sẽ gây khó khăn trong quá trình áp dụng của các cơ quan có thẩm quyền.

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:

Một số điều luật ít được áp dụng hoặc chưa được áp dụng để xử lý tội phạm đã xảy ra trong thực tiễn như Điều 286, Điều 287, Điều 291, Điều 293, Điều 294 BLHS năm 2015. Các điều luật này thường có quy định dấu hiệu hậu quả trong cấu thành tội phạm cơ bản. Khi không xác định được hậu quả của tội phạm sẽ không xử lý tội phạm đó được. Trong khi đó, tội phạm trong lĩnh vực CNTT, MVT thường để lại hậu quả, chứng cứ ở dạng chứng cứ điện tử, nạn nhân nhiều khi không biết mình bị thiệt hại. Việc xác định hậu quả của tội phạm này rất khó khăn. Điều đó dẫn đến thực tế là đã có hành vi phạm tội xảy ra trong thực tiễn, nhưng các cơ quan có thẩm quyền không biết, không xác định được hậu quả của tội phạm. Theo các quy định trên để xử lý hình sự đối với tội phạm này bắt buộc phải xác định được dấu hiệu hậu quả. Thực tế có nhiều trường hợp mới chỉ có hành vi phạm tội dù hậu quả chưa xảy ra nhưng đã rất nguy hiểm cho xã hội. Nếu những hành vi như vậy không được xử lý hình sự sẽ làm cho hiệu quả công tác đấu tranh phòng chống loại tội phạm này bị hạn chế.

Hiện nay, BLHS năm 2015 đã khắc phục một phần hạn chế này bằng cách, vẫn quy định dấu hiệu hậu quả nhưng quy định song song các dấu hiệu khác như "đã bị xử phạt hành chính về hành vi này hoặc đã bị kết án về tội

này chưa được xoá án tích mà còn vi phạm". Cách này được sử dụng phổ biến tại 6 trong tổng số 9 điều luật về tội phạm trong lĩnh vực CNTT, MVT[157]. Điều này làm tăng khả năng áp dụng các quy định này trên thực tế dù chưa chứng minh được hậu quả của tội phạm. Tuy nhiên, việc sửa đổi này vẫn còn hạn chế, chưa triệt để. Vì nếu người phạm tội trước đó chưa bị xử phạt hành chính hoặc bị kết án mà lại chưa chứng minh được hậu quả của tội phạm thì không xử lý được. Trong khi đó, có nhiều trường hợp do tính chất quan trọng của đối tượng bảo vệ, mới có hành vi phạm tội chưa chứng minh được hậu quả hoặc hậu quả chưa xảy ra đã rất nguy hiểm (dù trước đó chưa vi phạm hành chính hoặc phạm tội). Ví dụ: hành vi cản trở hoặc gây rối loạn đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh.

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:

(1) Quy định về dấu hiệu "để sử dụng vào mục đích trái pháp luật" tại khoản 1 Điều 285 BLHS năm 2015 (tội sản xuất, mua bán, trao đổi tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật) không phù hợp, bởi vì "mục đích trái pháp luật" có phạm vi rất rộng. Do đó, nếu áp dụng sẽ dẫn đến việc xử lý hình sự tràn lan. Quy định này không phù hợp với văn bản pháp luật quốc tế và xu hướng chung của các nước trên thế giới. Các văn bản pháp luật quốc tế quy định về điều luật này đều chỉ giới hạn mục đích của hành vi sản xuất, mua bán công cụ, thiết bị, phần mềm là để thực hiện tội phạm trong lĩnh vực CNTT, MVT. Như vậy, vấn đề này đã được pháp luật quốc tế quy định rất cụ thể và hạn chế, không rộng như quy định tại Điều 285 BLHS năm 2015.

[157] Bao gồm: Điều 286, Điều 287, Điều 288, Điều 291, Điều 293, Điều 294 BLHS năm 2015

(2) Dấu hiệu 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" không hợp lý và khó hiểu. Bởi vì bản thân hành vi sản xuất, mua bán, trao đổi tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật chưa thể gây ra thiệt hại về tài sản, mà phải thông qua hành vi của người sử dụng. Khi đó, người sử dụng công cụ, thiết bị, phần mềm sẽ phải chịu trách nhiệm pháp lý đối với hậu quả thiệt hại gây ra. Không thể bắt người sản xuất, mua bán, trao đổi tặng cho công cụ, thiết bị, phần mềm phải chịu trách nhiệm về hậu quả do người dùng công cụ, thiết bị, phần mềm đó gây ra, nếu họ không phải là đồng phạm với nhau.

(3) Điểm e khoản 2, điểm đ khoản 3 Điều 287 là "làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử … từ 10 lần đến 50 lần trong thời gian 24 giờ" trùng với điểm c khoản 1 Điều 287 "làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử … từ 3 lần đến dưới 10 lần trong thời gian 24 giờ". Hai dấu hiệu này trùng nhau vì trong thời gian 24 giờ mà mạng máy tính, mạng viễn thông, phương tiện điện tử bị tê liệt, gián đoạn, ngừng trệ từ 3 lần đến 10 lần thì coi như bị mất tối đa 24 giờ. Trường hợp, trong 24 giờ mà mạng máy tính, mạng viễn thông, phương tiễn điện tử bị tê liệt, gián đoạn, ngưng trệ từ 10 lần đến 50 lần thì cũng chỉ mất tối đa 24 giờ. Như vậy, 2 trường hợp này bằng nhau, không thể quy định tại 2 khoản khác nhau được.

(4) Tội danh quy định tại Điều 287 (tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử) chưa phản ánh hết nội dung của điều luật. Điều luật quy định có 2 đối tượng tác động của tội phạm khác nhau là hệ thống máy tính, mạng viễn thông, phương tiện điện tử và dữ liệu điện tử. Trong khi tên của điều luật lại chỉ phản ánh 1 đối tượng tác động là mạng máy tính, mạng viễn thông, phương tiện điện tử.

(5) Dấu hiệu tăng nặng "tái phạm nguy hiểm" được sử dụng ở tất cả các điều luật, nhưng lại không được sử dụng trong Điều 288 là không thống nhất. Điều 288 cũng giống như các điều luật khác trong nhóm, vẫn sử dụng được dấu hiệu định khung tăng nặng "tái phạm nguy hiểm". Việc không sử dụng dấu hiệu "tái phạm nguy hiểm" trong điều luật này làm giảm khả năng phân hoá TNHS của điều luật.

(6) Hình phạt của Điều 290 nhẹ hơn so với hình phạt tại Điều 174 của BLHS năm 2015. Theo khoản 4 Điều 174, hình phạt cao nhất đối với tội lừa đảo chiếm đoạt tài sản là tù chung thân. Trong khi đó, theo khoản 4 Điều 290 hình phạt cao nhất đối với tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản chỉ là 20 năm tù. Điều này không phù hợp, vì cùng chiếm đoạt từ 500 triệu đồng trở lên nhưng tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản có tính chất nguy hiểm hơn. Trong khi đó, thông thường các quy định của BLHS năm 2015 luôn coi dấu hiệu sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử là dấu hiệu tăng nặng định khung trong các tội tương ứng[158]. Một số văn bản quốc tế cũng quy định theo hướng này, coi việc sử dụng CNTT, MVT để thực hiện tội phạm là tình tiết tăng nặng TNHS[159].

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

---

[158] Ví dụ: tội khủng bố nhằm chống chính quyền nhân dân (điểm đ khoản 2 Điều 113); tội làm nhục người khác (điểm e khoản 2 Điều 155); tội vu khống (điểm e khoản 2 Điều 156); tội khủng bố (điểm d khoản 2 Điều 299); tội đánh bạc (điểm c khoản 2 Điều 321); tội tổ chức đánh bạc hoặc gá bạc (điểm c khoản 2 Điều 322).

[159] Xem: Điều 21 Công ước phòng chống tội phạm công nghệ thông tin các nước Ả -rập: http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information Technology Offences (truy cập ngày 18/8/2019).

Việc quy định nội dung loại trừ tại khoản 1 Điều 290 "nếu không thuộc trường hợp quy định tại Điều 173 và Điều 174" là không cần thiết, nhiều khi còn gây ra hiểu nhầm trong việc định tội. Bởi vì Điều 290 so với Điều 173 và Điều 174 đều là điều luật riêng so với điều luật chung. Theo nguyên tắc áp dụng pháp luật, trường hợp vừa thoả mãn cấu thành tội phạm của tội chung và cấu thành tội phạm của tội riêng thì áp dụng điều luật riêng. Ngược lại, nếu chỉ thoả mãn cấu thành tội phạm của điều luật chung, không thoả mãn cấu thành tội phạm của tội riêng thì áp dụng điều luật chung. Quy định trên lại quy định ngược lại, nếu không thuộc trường hợp của điều luật chung sẽ áp dụng điều luật riêng.

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 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. Thực tiễn cho thấy, trước khi có Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10 tháng 9 năm 2012, các cơ quan tiến hành tố tụng gần như không xét xử được vụ án nào. Kể từ khi có văn bản hướng dẫn này, các vụ án về tội phạm trong lĩnh vực CNTT, MVT mới được xét xử nhiều hơn. Hiện nay, BLHS năm 2015 đã có những quy định mới cụ thể hơn nhưng vẫn còn một số nội dung cần có sự giải thích, hướng dẫn để việc áp dụng thuận lợi hơn như: thuật ngữ "công cụ, thiết bị, phần mềm có khả năng tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử" tại khoản 1

Điều 285; "thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân" tại khoản 1 Điều 288; "gây dư luận xấu" tại khoản 1 Điều 288; "dẫn đến biểu tình" điểm g khoản 2 Điều 288; … Những vấn đề này nếu không được giải thích, hướng dẫn kịp thời, trong thời gian tới sẽ gây ra những khó khăn không nhỏ cho các 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

Công tác tổ chức thực hiện quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT ảnh hưởng không nhỏ đến hiệu quả áp dụng các quy định này. Trong những năm qua, công tác tổ chức thực hiện quy định này còn một số bất cập, làm giảm hiệu quả của việc áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT. Điều đó được thể hiện qua một số khía cạnh sau:

Thứ nhất, nhân lực thực hiện công tác đấu tranh chống và phòng ngừa tội phạm trong lĩnh vực CNTT, MVT còn hạn chế:

Để giải quyết vụ án hình sự về tội phạm trong lĩnh vực CNTT, MVT, ngoài kiến thức về pháp luật, người tiến hành tố tụng phải có kiến thức, hiểu biết nhất định về lĩnh vực CNTT, MVT. Trong khi hiện nay, người tiến hành tố tụng còn hạn chế về trình độ chuyên môn sâu trong lĩnh vực CNTT, MVT. Điều đó gây ra những khó khăn rất lớn trong quá trình áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT. Hiện nay, mặc dù trình độ và khả năng về CNTT, MVT của người tiến hành tố tụng đã được cải thiện, nhưng vẫn chưa đáp ứng được yêu cầu đấu tranh đối với loại tội phạm này.

Không chỉ hạn chế về trình độ CNTT, MVT mà kinh nghiệm đấu tranh đối với tội phạm trong lĩnh vực CNTT, MVT của người tiến hành tố tụng còn thiếu. Với số lượng vụ án về tội phạm trong lĩnh vực CNTT, MVT ít như

những năm qua cho thấy, có nhiều TAND cấp huyện, thậm trí cả TAND cấp tỉnh cũng chưa xét xử vụ án nào về tội phạm này. Khi người tiến hành tố tụng không có kinh nghiệm giải quyết loại án này sẽ gặp nhiều lúng túng, khó khăn.

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:

Trong các vụ án thuộc lĩnh vực CNTT, MVT, việc phát hiện, thu thập, bảo quản dấu vết, chứng cứ phạm tội thường là các chứng cứ điện tử. Các đối tượng phạm tội thường lợi dụng những kỹ thuật, thiết bị mới nhất, hiện đại để phạm tội. Do đó, các cơ quan tiến hành tố tụng cần phải được trang bị những thiết bị hiện đại, phù hợp để phòng ngừa tội phạm bằng giải pháp kỹ thuật; phát hiện ra tội phạm, thu thập và bảo quản chứng cứ điện tử. Trong khi đó thực tế hiện nay, các cơ quan tiến hành tố tụng chưa được trang bị công cụ, thiết bị cần thiết trong việc phát hiện, xử lý loại tội phạm này. Không chỉ thiếu về số lượng, các trang thiết bị, kỹ thuật của các cơ quan tiến hành tố tụng còn lạc hậu[160]. Tình trạng này vốn đã tồn tại từ trước đây, tuy nhiên đến nay vẫn chưa được cải thiện đáng kể. Điều đó góp phần dẫn đến những khó khăn trong việc phát hiện, xử lý tội phạm trong lĩnh vực CNTT, MVT trong những năm qua.

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:

Theo số liệu thống kê về số bị cáo là người nước ngoài bị xét xử về tội phạm trong lĩnh vực CNTT, MVT trong những năm qua, chiếm tỷ lệ khá cao so với các loại tội phạm khác (khoảng 9 %). Tội phạm trong lĩnh vực CNTT, MVT có tính quốc tế cao vì không bị giới hạn bởi biên giới quốc gia. Do đó, tỷ lệ người phạm tộ là người nước ngoài hoặc có liên quan đến nước ngoài cao (khoảng 9 %). Điều này gây nên những khó cho các cơ quan tiến hành tố

[160] Xem: Phạm Văn Lợi (2007), Sđd, tr. 119.

tụng. Bởi vì trong quá trình giải quyết các vụ án này, yêu cầu cao hơn về năng lực, trình độ, nhất là trình độ ngoại ngữ của cán bộ. Đồng thời, phải thực hiện các hoạt động tương trợ tư pháp, hợp tác quốc tế. Đó là những hợp động khó khăn, phức tạp hiện nay. Hơn thế nữa, còn thiếu cơ sở pháp lý cho các cơ quan có thẩm quyền thực hiện hoạt động hợp tác quốc tế. Cụ thể, Việt Nam chưa tham gia các các công quốc tế về tội phạm trong lĩnh vực CNTT, MVT. Đây cũng là nguyên nhân hạn chế hiệu quả hoạt động hợp tác quốc tế trong lĩnh vực này.

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

Cơ sở để xây dựng các giải pháp hoàn thiện BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT là kết quả nghiên cứu lý luận, các quy định và thực tiễn áp dụng quy định của BLHS của Luận án và tham khảo quy định của pháp luật quốc tế. Các giải pháp cụ thể:

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):

Với quy định như hiện nay, Điều 285 BLHS năm 2015 chỉ quy định các hành vi "sản xuất, mua bán, trao đổi, tặng cho" công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật là tội phạm. Còn các hành vi "chiếm hữu, sở hữu nhằm cho người khác sử dụng" hoặc "đề nghị người khác sử dụng, nhập khẩu" công cụ, thiết bị, phần mềm để sử dụng vào mục đích phạm tội không bị coi là tội phạm. Thực tế những hành vi này cũng nguy hiểm

không kém gì so với hành vi mua bán, trao đổi, tặng cho quy định tại Điều 185 BLHS năm 2015. Hơn nữa, trong thực tế những hành vi như vậy đã và sẽ ngày càng nhiều. Việc 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 tạo cơ sở pháp lý cho việc xử lý đối với những hành vi nguy hiểm này. Đồng thời, việc bổ sung này cũng phù hợp với các văn bản pháp luật quốc tế hiện nay như Công ước Budapest 2001, Luật mẫu 2002 đều có quy định về các hành vi này[161]. Khi bổ sung thêm 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 vào Điều 185 BLHS năm 2015, tên của điều luật này cũng phải sửa đổi, bổ sung theo. Theo đó, tội danh tại Điều 185 BLHS năm 2015 sẽ là "Tội lạm dụng cộng cụ, thiết bị, phần mềm để sử dụng vào mục đích phạm tội".

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

Thực tế hiện nay có những hành vi vi phạm pháp luật trong lĩnh vực CNTT, MVT nhưng các cơ quan tiến hành tố tụng không xử lý hình sự được. Tình trạng này có phần do nguyên nhân từ quy định của BLHS năm 2015. Trong đó, có nhiều tội quy định dấu hiệu hậu quả trong cấu thành tội phạm cơ bản như Điều 286, Điều 287 và Điều 288 BLHS năm 2015. Khi hành vi phạm tội xảy ra nếu không xác định được hậu quả sẽ không xử lý hình sự được. Trong khi đó, do đặc điểm của loại tội phạm này rất khó xác định hậu quả của tội phạm. Điều đó dẫn đến bỏ lọt tội phạm. Để xử lý tội phạm triệt để, tránh bỏ lọt tội phạm cần sửa đổi, bổ sung các quy định của BLHS theo hướng: đối với những hành vi thực sự nguy hiểm cho xã hội thì phải xử lý hình sự kể cả

[161] Xem: Điều 6 Công ước Busdapest 2001 và Điều 9 Luật mẫu 2002.

khi hậu quả chưa xảy ra hoặc không xác định được hậu quả. Cụ thể, đối với Điều 286, Điều 287 và Điều 288 của BLHS năm 2015 chỉ cần có hành vi tác động đến những đối tượng có tính quan trọng đặc biệt như hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh; 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 đã thể hiện đầy đủ tính nguy hiểm cho xã hội của hành vi phạm tội. Do đó, tội phạm sẽ được coi là hoàn thành kể từ khi có hành vi phạm tội, không kể hậu quả đã xảy ra hay chưa. Trường hợp, các hành vi phạm tội đã gây ra hậu quả thì việc xâm hại đến những đối tượng trên được coi là dấu hiệu tăng nặng định khung của tội phạm đó. Theo hướng này, tác giả đề xuất sửa đổi, bổ sung về cấu thành tội phạm của các tội sau đây:

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. Như vậy, chỉ cần người phạm tội cố ý phát tán chương trình tin học gây hại cho "hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh" là tội phạm đã hoàn thành, chưa cần phải gây ra hậu quả hoặc đã bị xử phạt vi phạm hành chính hay có bị kết án trước đó. Trường hợp, phạm tội đối với những đối tượng này mà đã gây ra hậu quả hoặc trước đó đã bị xử phạt hành chính hay bị kết án sẽ bị coi là dấu hiệu tăng nặng TNHS tại khoản 3 Điều 286. Theo đó, Điều 286 sẽ được sửa đổi, bổ sung như sau:

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

1. Người nào cố ý phát tán chương trình tin học gây hại cho mạng máy

tính, mạng viễn thông, phương tiện điện tử thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 50.000.000 đồng đến 200.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:

Các điểm (a), (b), (c) và (d): giữ nguyên

đ) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh;

2. *Giữ nguyên*

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 12 năm:

a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh nếu thuộc một trong các trường hợp quy định tại điểm a, b, c, d khoản 1 Điều này.

Các điểm (b), (c), (d) và (d) giữ nguyên

4. Giữ nguyên

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.*** Theo đó, người phạm tội chỉ cần có hành vi cản trở hoặc gây rối loạn hoạt động đối với các đối tượng này thì tội phạm phạm đã hoàn thành, không kể hậu quả của tội phạm có xảy ra hay chưa. Trường hợp hậu quả của tội phạm đã xảy ra hoặc người phạm tội trước đó đã bị xử phạt hành chính hoặc đã bị kết án về tội này mà chưa được xoá án tích, việc xâm phạm tới các đối tượng trên được coi là tình tiết tăng nặng TNHS tại khoản 3. Sau khi sửa đổi, bổ sung Điều 287 BLHS năm 2015 sẽ có nội dung sau:

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

1. Người nào tự ý xóa, 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 thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng hoặc phạt tù từ 06 tháng đến 03 năm:

Các điểm (a), (b), (c), (d), (đ): giữ nguyên

e) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh;

g) Đối với 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;

2. *Giữ nguyên*

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 12 năm:

a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh nếu thuộc một trong các trường hợp quy định từ điểm a đến điểm đ khoản 1 Điều này;

b) Đối với 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 nếu thuộc một trong các trường hợp quy định từ điểm a đến điểm đ khoản 1 Điều này;

Các điểm (c), (d), (đ) và (e): giữ nguyên

4. *Giữ nguyên*

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. Như vậy, Điều 288 BLHS năm 2015 sẽ được sửa đổi, bổ sung như sau:

Điều 288. Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông

1. Người nào thực hiện một trong các hành vi sau đây, thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng hoặc gây thiệt hại từ 100.000.000 đồng đến dưới 500.000.000 đồng hoặc gây dư luận xấu làm giảm uy tín của Cơ quan, tổ chức, cá nhân hoặc ***đối với những thông tin có tác hại lớn cho xã hội*** thì bị phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc bị phạt tù từ 06 tháng đến 03 năm:

Các điểm (a), (b), (c): giữ nguyên

Các khoản 2, 3: g*iữ nguyên*

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), cần sửa đổi một số nội dung sau:

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. Theo Điều 285 hiện nay, đối tượng của tội phạm là "công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật" có phạm vi rất rộng,

bao gồm cả vi phạm hành chính, vi phạm dân sự. Điều đó dẫn đến phạm vi xử lý hình sự đối với tội phạm này rộng. Tham khảo các văn bản pháp luật quốc tế hiện nay, đa số đều quy định đối tượng phạm tội của tội này là các công cụ, thiết bị, phần mềm để sử dụng vào mục đích phạm tội trong lĩnh vực CNTT, MVT[162]. Do đó, việc sửa đổi để thu hẹp phạm vi đối tượng tác động của tội phạm này là cần thiết và phù hợp với xu hướng chung của quốc tế.

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***). Dấu hiệu này có nội dung khó hiểu và không có khả năng áp dụng trên thực tế. Bởi vì việc sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật không thể gây thiệt hại cho về tài sản cho người khác được. Chỉ có người sử dụng công cụ, thiết bị, phần mềm vào mục đích trái pháp luật mới có thể gây thiệt hại về tài sản cho người khác. Nhưng khi đó thì người nào sử dụng công cụ, thiết bị, phần mềm đó phải chịu trách nhiệm chứ không phải là người sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm đó.

Ba là, bổ sung quy định để truy cứu TNHS đối với pháp nhân thương mại về tội này. Theo quy định tại Điều 76 BLHS năm 2015, pháp nhân thương mại không phải chịu TNHS về tội phạm trong lĩnh vực CNTT, MVT. Tuy nhiên, với quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT như hiện nay, trong tương lai cần bổ sung theo hướng truy cứu TNHS pháp nhân thương mại đối với một số tội phạm trong lĩnh vực CNTT, MVT như tội sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích phạm tội (Điều 285). Việc bổ sung này là cần thiết vì các lý do sau: (1) nếu pháp nhân thương mại thực hiện tội này sẽ gây ra hậu quả rất lớn vì số lượng công cụ, thiết bị, phần mềm được sản xuất, mua

[162] Xem: khoản 1 Điều 6 Công ước Budapest 2001.

bán sẽ rất lớn; (2) động cơ phạm tội của tội này thường là động cơ vụ lợi, trong khi đó pháp nhân thương mại là tổ chức hoạt động nhằm mục đích lợi nhuận nên có thể thực hiện tội phạm này; (3) hiện một số văn bản quốc tế như Công ước Budapest 2001 tuy không quy định bắt buộc nhưng cũng đề cập đến việc xử lý trách nhiệm của pháp nhân đối với tội này, kể cả biện pháp xử lý hình sự[163].

(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, Điều 287 đang có sự bất cập về tội danh (Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử) không bao gồm hết các đối tượng điều chỉnh trong nội dung của điều luật. Cụ thể, theo tội danh chỉ có đối tượng là "mạng máy tính, mạng viễn thông, phương tiện điện tử" nhưng nội dung điều chỉnh thì có thêm đối tượng là "***dữ liệu điện tử***". Do đó, chúng ta có 2 phương án sửa đổi như sau:

+ Phương án 1: sửa tội danh của Điều 287 để tội danh bao gồm hết các đối tượng điều chỉnh trong điều luật (mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử).

+ Phương án 2: tách Điều luật này thành 2 điều luật riêng gồm: (1) Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; (2) Tội cản trở hoặc gây rối loạn dữ liệu điện tử.

Theo tác giả việc lựa chọn phương án 1 sẽ đơn giản hơn. Chúng ta chỉ cần sửa đổi tội danh của Điều 287 là có thể chấp nhận được, mà không phải quy định thành một tội riêng. Trên thế giới, các nước lựa chọn hai phương án trên theo tỷ lệ cân bằng, tương đương nhau. Do đó, tội danh của Điều 287 sẽ sửa đổi 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".***

[163] Xem: Điều 12 Công ước Budapest 2001.

Hai là, sửa đổi điểm e khoản 2 Điều 287 và điểm d khoản 3 Điều 287 vì 2 điểm này trùng với điểm c khoản 1 Điều 287. Đây là một sai sót lớn của BLHS năm 2015 cần phải được khắc phục. 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".*** Như vậy, việc làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 10 đến 50 lần trong thời gian từ 24 giờ đến 168 giờ cũng sẽ tương đương với việc làm mạng máy tính, mạng viễn thông, phương tiện điện tử tê liệt, gián đoạn, ngưng trệ hoàn toàn trong thời gian từ 24 giờ đến 168 giờ. Điều đó tránh việc trùng với điểm c khoản 1 Điều 287, đồng thời làm cho các dấu hiệu quy định trong cùng một điểm tăng nặng tương đương nhau.

+ Đối với điểm đ 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. Dấu hiệu "tái phạm nguy hiểm" được sử dụng là dấu hiệu định khung tăng nặng tại khoản 2 của tất cả các tội, trừ Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288).

Việc quy định như vậy chưa đảm bảo tính thống nhất. Trong khi đó, quy định dấu hiệu này là tình tiết định khung tăng nặng tại khoản 2 Điều 288 cũng sẽ có tác dụng phân hoá TNHS tốt hơn.

(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***". Cụm từ này vừa không cần thiết, vừa quy định ngược. Bởi vì tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290) được coi là điều luật riêng cụ thể so với tội trộm cắp tài sản (Điều 173) và tội lừa đảo chiếm đoạt tài sản (Điều 174). Nếu người phạm tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để chiếm đoạt tài sản thuộc một trong các trường hợp quy định từ điểm a đến điểm đ khoản 1 Điều 290 thì xử lý về tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản. Nếu không thoả mãn yếu tố cấu thành của tội này nhưng thoả mãn cấu thành tội phạm tại Điều 173 hoặc Điều 174 thì xử lý về tội trộm cắp tài sản hoặc tội lừa đảo chiếm đoạt tài sản. Do đó, không thể quy định ngược là nếu không thuộc trường hợp quy định tại Điều 173 và Điều 174 mới xử lý theo Điều 290 được.

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. Mức cao nhất của khung hình phạt đối với tội này hiện nay là 20 năm tù (khoản 4 Điều 290). Trong khi đó, hành vi phạm tội này cũng được xếp vào tội phạm có tính chất chiếm đoạt như tội trộm cắp tài sản, tội lừa đảo chiếm đoạt tài sản. Hơn thế nữa, giữa tội và tội trộm cắp tài sản (Điều 173), tội lừa đảo chiếm đoạt tài sản (Điều 174) chỉ khác nhau cơ bản về công cụ thực hiện tội phạm là CNTT, MVT. Việc sử

dụng CNTT, MVT để thực hiện tội phạm làm cho tính chất của tội phạm nguy hiểm hơn so với tội phạm thông thường. Trong các văn bản pháp luật quốc tế cũng quy định coi việc sử dụng CNTT, MVT để thực hiện tội phạm là tình tiết tăng nặng TNHS so với trường hợp khác[164]. Tuy nhiên, BLHS năm 2015 lại quy định hình phạt của tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290) nhẹ hơn tội lừa đảo chiếm đoạt tài sản (Điều 174). Bởi vì mức hình phạt cao nhất của tội lừa đảo chiếm đoạt tài sản là tù chung thân (khoản 4 Điều 174). Điều đó không phù hợp với tính chất nguy hiểm của hành vi phạm tội trong lĩnh vực CNTT, MVT. Do đó, tác giả đề nghị sửa đổi hình phạt tại khoản 4 Điều 290 lên mức cao nhất là tù chung thân.

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

Hiện nay, BLHS năm 2015 đã khắc phục được một số hạn chế của BLHS năm 1999 bằng cách các nội dung đã được quy định chi tiết cụ thể hơn. Tuy nhiên, một số quy định vẫn cần được cơ quan có thẩm quyền giải thích, hướng dẫn chính thức, nếu không sẽ gây khó khăn cho việc áp dụng các quy định này. Do chưa có văn bản hướng dẫn mới nên Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10 tháng 9 năm 2012 vẫn được sử dụng. Tuy nhiên, một số nội dung hướng dẫn trong Thông tư này cũng cần phải được sửa đổi cho phù hợp. Trong thời gian tới, các cơ quan có thẩm quyền cần giải thích, hướng dẫn một số nội dung sau:

** 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

[164] Xem: Điều 21 Công ước phòng chống tội phạm công nghệ thông tin các nước Ả -rập: http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (truy cập ngày 18/8/2019).

tính, mạng viễn thông, phương tiện điện tử" tại khoản 1 Điều 285. Thực tế, các công cụ, thiết bị, phần mềm thường có thể sử dụng vào nhiều mục đích khác nhau. Do đó, cần phải giới hạn phạm vi khái niệm "công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử" không bị xử lý tràn lan. Theo đó, "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. Hiện chưa có khái niệm thế nào là "thông tin riêng hợp pháp". Các văn bản hiện nay đều không có quy định trực tiếp. Ví dụ: theo khoản 4 Điều 6 Luật viễn thông (2009), "thông tin riêng liên quan đến người sử dụng dịch vụ viễn thông" bao gồm: tên, địa chỉ, số máy gọi, số máy được gọi, vị trí máy gọi, vị trí máy được gọi, thời gian gọi và thông tin riêng khác mà người sử dụng đã cung cấp khi giao kết hợp đồng với doanh nghiệp. Theo điểm a khoản 2 Điều 72 Luật công nghệ thông tin (2006), tổ chức, cá nhân không được xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường không gian mạng. Trong khi đó, theo khoản 2 Điều 9 của Luật công nghệ thông tin (2006), tổ chức, cá nhân khi hoạt động kinh doanh trên môi trường mạng phải thông báo công khai trên môi trường mạng những thông tin có liên quan, bao gồm: tên, địa chỉ địa lý, số điện thoại, địa chỉ thư điện tử; thông tin về quyết định thành lập, giấy phép hoạt động hoặc giấy chứng nhận đăng ký kinh doanh (nếu có); tên cơ quan quản lý nhà cung cấp (nếu có); thông tin về giá, thuế, chi phí vận chuyển (nếu có) của hàng hóa, dịch vụ. Theo khoản 16 Điều 3 Nghị định 72/2013/NĐ-CP ngày

15/7/2013 quy định về quản lý, cung cấp và sử dụng dịch vụ internet và thông tin trên mạng, "thông tin cá nhân" là thông tin gắn liền với việc xác định danh tính, nhân thân của cá nhân bao gồm tên, tuổi, địa chỉ, số chứng minh nhân dân, số điện thoại, địa chỉ thư điện tử và thông tin khác theo quy định của pháp luật. Trong đó, thông tin được chia làm 2 loại là thông tin công cộng và thông tin riêng. Theo khoản 14, 15 Điều 3 Nghị định 72/2013/NĐ-CP ngày 15/7/2013 quy định về quản lý, cung cấp và sử dụng dịch vụ internet và thông tin trên mạng, thông tin công cộng là "thông tin trên mạng của một tổ chức, cá nhân được công khai cho tất cả các đối tượng mà không cần xác định danh tính, địa chỉ cụ thể của các đối tượng đó". Thông tin riêng là "thông tin trên mạng của một tổ chức, cá nhân mà tổ chức, cá nhân đó không công khai hoặc chỉ công khai cho một hoặc một nhóm đối tượng đã được xác định danh tính, địa chỉ cụ thể".

Qua các quy định trên có thể xác định một số đặc điểm của thông tin riêng hợp pháp của tổ chức, cá nhân như sau: (1) thông tin riêng hợp pháp của cá nhân, cơ quan, tổ chức là những thông tin gắn liền với mỗi cá nhân, cơ quan, tổ chức đó (bao gồm cả thông tin điện tử của cá nhân); (2) Thông tin cá nhân bao gồm bất kể thông tin nào liên quan đến việc xác định hoặc nhận dạng cá nhân (thông tin có thể trực tiếp hoặc gián tiếp nhận dạng cá nhân như thông tin về thể chất, sinh lý, tâm thần, kinh tế, văn hóa hoặc xã hội)[165]; (3) thông tin riêng hợp pháp của cá nhân, cơ quan, tổ chức có thể là thông tin bí mật, cũng có thể không phải là thông tin bí mật nhưng cá nhân, tổ chức đó *"không công khai hoặc chỉ công khai cho một hoặc một nhóm đối tượng đã được xác định danh tính, địa chỉ cụ thể"*[166]*;* (4) thông tin riêng hợp pháp của cá nhân, cơ quan, tổ chức là thông tin dữ liệu điện tử.

[165] Xem: điểm a Điều 2 Chỉ thị số 95/46/EC ngày 24/11/1995 của Hội đồng Châu Âu.

[166] Xem: khoản 14, 15 Điều 3 Nghị định 72/2013/NĐ-CP ngày 15/7/2013.

Từ những phân tích trên có thể kết luận, "Thông tin riêng hợp pháp của cơ quan, tổ chức, các nhân" 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. Hiện tại nước ta chưa có quy định của pháp luật về biểu tình nên chưa có khái niệm chính thức về biểu tình. Tuy nhiên, có thể hiểu "dẫn đến biểu tình" là dẫn đến tụ tập đông người để bày tỏ ý chí, nguyên 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:

Giữa 3 loại tội phạm trên có thể có cùng thủ đoạn và hậu quả, nhưng khác nhau về mục đích và nhận thức. Người thực hiện hành vi phát tán chương trình tin học gây hại không nhận thức và xác định trước được đối tượng (nạn nhân) bị tấn công, trong khi đó để thực hiện hành vi cản trở hoặc gây rối hay hành vi xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử, người phạm tội phải xác định rõ từ trước đối tượng mà mình sẽ tấn công. Để cản trở hoặc gây rối hoạt động mạng máy tính, mạng viễn thông hoặc phương tiện điện tử người phạm tội có thể xâm nhập trái phép, sau đó thay đổi, huỷ hoại dữ liệu của mạng máy tính, mạng viễn thông hoặc phương tiện điện tử đó. Điểm khác nhau của các hành vi này là ở mục đích của việc xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử. Nếu mục đích là để gây rối hoặc cản trở hoạt động của

mạng máy tính, mạng viễn thông, phương tiện điện tử thì thuộc Điều 287, nếu mục đích là chiếm đoạt tài sản sẽ thuộc Điều 290, còn lại sẽ thuộc Điều 289. Trong mối quan hệ giữa Điều 286, 287 và 289 thì Điều 286 và Điều 289 là điều luật chung, còn Điều 287 là điều luật cụ thể.

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

Giữa các tội này cơ bản khác nhau về hành vi khách quan của tội phạm. Trong đó, tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290) là tội có tính chất riêng, đặc thù. Cụ thể, tội phạm này sử dụng công cụ trực tiếp là mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện việc chiếm đoạt tài sản. Nếu không có các công cụ đó sẽ không chiếm đoạt được tài sản của nạn nhân. Hơn nữa, việc chiếm đoạt tài sản được thực hiện theo một trong các trường hợp quy định từ điểm a đến điểm đ khoản 1 Điều 290 BLHS năm 2015. Trường hợp, không thoả mãn các dấu hiệu cấu thành của tội này, nhưng thoả mãn dấu hiệu cấu thành của tội trộm cắp tài sản (Điều 173) hoặc tội lừa đảo chiếm đoạt tài sản (Điều 174) sẽ bị xử lý theo các tội này.

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:*

Hạn chế về trình độ chuyên môn và kinh nghiệm của người tiến hành tố tụng là nguyên nhân của những khó khăn trong khi giải quyết các vụ án về tội phạm trong lĩnh vực CNTT, MVT đã được xác định rõ. Để khắc phục hạn chế này, cần có giải pháp đồng bộ và lâu dài. Những giải pháp này bao gồm:

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.

Để làm được điều này cần tăng cường nghiên cứu, trao đổi về lý luận và thực tiễn, giúp nhận thức chung của cán bộ về tội phạm này được nâng cao và thống nhất.

Hai là, tích cực đào tạo, bồi dưỡng kiến thức về CNTT, MVT pháp lý cho người tiến hành tố tụng. Trình độ về CNTT, MVT có lẽ là điểm yếu của cán bộ trong các cơ quan tiến hành tố tụng hiện nay. Hiện tại chỉ một số đơn vị nghiệp vụ chuyên trách của ngành Công an là được đào tạo chuyên sâu về CNTT, MVT để đấu tranh với loại tội phạm này. Còn lại, đa số điều tra viên, cán bộ điều tra, kiểm sát viên, thẩm phán chưa được đào tạo chuyên sâu về CNTT, MVT. Do đó, để đấu tranh, phòng ngừa có hiệu quả loại tội phạm này, cần thiết phải đào tạo, bồi dưỡng về CNTT, MVT pháp lý cho những người tiến hành tố tụng.

Theo kinh nghiệm của các nước trên thế giới, những người tiến hành tố tụng không cần phải được đào tạo như một chuyên gia trong lĩnh vực CNTT, MVT[167]. Nhưng họ cần được đào tạo, bồi dưỡng về CNTT, MVT để phục vụ cho hoạt động điều tra, truy tố, xét xử loại tội phạm này. Những kiến thức chung cần cung cấp như cơ chế hoạt động của máy tính, cơ chế hoạt động của mạng máy tính, mạng viễn thông, kỹ thuật máy tính có thể làm gì và không thể làm gì, đặc biệt là thủ đoạn sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện tội phạm như thế nào. Trên cơ sở đó, Điều tra viên, Kiểm sát viên, Thẩm phán sẽ được đào tạo, bồi dưỡng các nội dung khác nhau. Chẳng hạn, Điều tra viên cần được đào tạo, bồi dưỡng để phát hiện ra tội phạm, biết được cách thức đối tượng đã thực hiện tội phạm thế nào, phát hiện, thu thập, bảo quản và sử dụng chứng cứ điện tử; tìm ra, khôi phục, mã hóa, giải mã dữ liệu điện tử; đọc, giải thích, kiểm tra những tệp tài liệu hoặc các sự việc được khám phá ra… Đối với Kiểm sát viên, Thẩm phán cần được đào tạo, bồi dưỡng để hiểu ý nghĩa của từng loại chứng cứ điện tử và sử

[167] Xem: Debra Littlejohn Shinder (2010), Tlđd, tr.38 - 39.

dụng tốt nhất chứng cứ điện tử tại phiên tòa.

Về hình thức đào tạo, bồi dưỡng, cần tổ chức lớp theo từng đối tượng cụ thể với mục đích phù hợp. Đào tạo, bồi dưỡng theo từng chuyên đề trong những khóa học ngắn ngày. Các chuyên đề có thể theo từng tội phạm trong lĩnh vực CNTT, MVT đã được quy định trong BLHS năm 2015.

Ba là, thường xuyên tập huấn, phổ biến kinh nghiệm đấu tranh đối với tội phạm trong lĩnh vực CNTT, MVT. Hiện nay, ở nhiều nơi người tiến hành tố tụng còn thiếu kinh nghiệm điều tra, truy tố, xét xử tội phạm trong lĩnh vực CNTT, MVT. Bởi vì số lượng vụ án về tội phạm trong lĩnh vực này còn ít, chủ yếu tập trung tại một số địa phương như Hà Nội, TP. Hồ Chí Minh, Đà Nẵng, Quảng Trị. Nhiều địa phương từ trước đến nay chưa có vụ án nào về tội phạm trong lĩnh vực CNTT, MVT. Do thiếu kinh nghiệm xử lý loại tội phạm này nên khi vụ án xảy ra sẽ gặp lúng túng, khó khăn. Để khắc phục vấn đề này, các cơ quan có thẩm quyền trong phạm vi quản lý của mình cần tổ chức nhiều lớp tập huấn, phổ biến kinh nghiệm đấu tranh đối với loại tội phạm này của những địa phương có nhiều án. Khi có những thủ đoạn phạm tội mới cần thông tin, giới thiệu nhanh nhất đến người tiến hành tố tụng để cập nhật thông tin, kịp thời phát hiện và xử lý tội phạm.

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. Việc phát hiện và xử lý đối với tội phạm trong lĩnh vực CNTT, MVT là công tác khó khăn, phức tạp, cần những cán bộ giỏi không chỉ về chuyên môn, trình độ pháp luật, mà còn am hiểu lĩnh vực CNTT, MVT. Thực tế, không phải cán bộ nào cũng đáp ứng được các yêu cầu đó. Theo kinh

nghiệm của một số nước trên thế giới[168], các cấp quản lý cần quan tâm lựa chọn những cán bộ ưu tú có đủ các các điều kiện trên để giao thụ lý giải quyết các vụ án về tội phạm trong lĩnh vực CNTT, MVT. Với trình độ, kinh nghiệm của mình những cán bộ này sẽ hoàn thành tốt nhiệm vụ. Đồng thời, họ còn có thể hướng dẫn, trực tiếp đào tạo những cán bộ mới tiếp cận.

** 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:*

Loại tội phạm này đa số được thực hiện trong môi trường không gian mạng, không thể phát hiện bằng mắt thường, mà phải sử dụng công cụ, phương tiện chuyên dùng. Hơn nữa, lĩnh vực CNTT, MVT là lĩnh vực công nghệ cao, trình độ hiện đại, có sự phát triển rất nhanh. Do đó, các thủ đoạn phạm tội ngày càng tinh vi, khó phát hiện. Nếu không được trang bị những thiết bị, công cụ tiên tiến nhất sẽ khó lòng phát hiện, đấu tranh có hiệu quả đối với loại tội phạm này. Do đó, việc 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 là yêu cầu bắt buộc. 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. Giá thành những sản phẩm này thường rất đắt đỏ, nhưng chúng ta buộc phải đầu tư mua sắm.

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

Tội phạm trong lĩnh vực CNTT, MVT có tính quốc tế rất cao, nên hiện nay, vấn đề về tội phạm này không phải là vấn đề của riêng quốc gia nào.

---

[168] Xem: Nguyễn Đức Hà, "Kinh nghiệm truy tố tội phạm sử dụng công nghệ cao của Viện Công tố Singapore", https://kiemsat.vn/kinh-nghiem-truy-to-toi-pham-su-dung-cong-nghe-cao-cua-vien-cong-to-singapore-50807.html (truy cập ngày 02/3/2020).

Trong môi trường không gian mạng toàn cầu, đối tượng phạm tội có thể thực hiện tội phạm ở bất cứ đâu trên thế giới mà không bị giới hạn bởi thời gian, khoảng cách địa lý hay biên giới quốc gia. Thực tế ở Việt Nam, tỷ lệ bị cáo người nước ngoài bị xét xử về tội phạm này chiếm khoảng 8,7%. Đó là một tỷ lệ khá cao, so với những nhóm tội phạm khác. Để đấu tranh có hiệu quả đối với loại tội phạm này, các quốc gia buộc phải hợp tác với nhau trong cuộc chiến chống lại loại tội phạm này. Trong thời gian tới, chúng ta cần hợp tác với các quốc gia khác để đấu tranh với loại tội phạm này theo một số lĩnh vực sau:

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. Hiện nay, Công Budapest 2001 được rất nhiều nước tham gia. Công ước này được mở cho cả các nước khác ngoài khu vực châu Âu tham gia. Qua nghiên cứu, tác giả thấy quy định của LHS Việt Nam về tội phạm trong lĩnh vực CNTT, MVT cũng khá tương thích, phù hợp với nội dung của Công ước này. Do đó, chúng ta cần nghiên cứu khả năng gia nhập Công ước này. Điều này sẽ giúp hoàn thiện hơn nữa hệ thống pháp luật của Việt Nam, giúp hệ thống pháp luật của chúng ta tương thích hơn với pháp luật của các nước khác trên thế giới. Điều đó sẽ tạo thuận lợi cho việc hợp tác quốc tế đấu tranh đối với loại tội phạm này.

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. Các vụ án về tội phạm trong lĩnh vực CNTT, MVT thường có đối tượng phạm tội là người nước ngoài. Do đó nhiều trường hợp cần có các hoạt động tương trợ tư pháp của các nước khác mới xử lý hình sự các đối tượng này.

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 cực CNTT, MVT thông qua việc tổ chức các hội thảo, hội nghị quốc tế. Thông qua hợp

tác quốc tế, chúng ta cũng có thể trạng bị, mua sắm, sử dụng hiệu quả các trang thiết bị chuyên dùng trong đấu tranh đối với loại tội phạm này.

Kết luận chương 3

Đánh giá quá trình áp dụng các quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong 12 năm qua (2009 - 2020) cho thấy, các quy định của BLHS thực sự là công cụ sắc bén, là cơ sở pháp lý để các cơ quan có thẩm quyền đấu tranh với tội phạm trong lĩnh vực CNTT, MVT. Trong giai đoạn này, các Toà án cả nước đã xét xử được tổng số 445 vụ án với 933 bị cáo. Trung bình mỗi năm xét xử được khoảng 37 vụ án với 77 bị cáo. Trong quá trình áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT để định tội và quyết định hình phạt, các cơ quan tiến hành tố tụng nói chung và Toà án nói riêng đã đạt được những kết quả nhất định.

Bên cạnh đó, trong quá trình áp dụng các quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT những năm qua cũng cho thấy những hạn chế, khó khăn, vướng mắc như: (1) 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; (2) 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; (3) 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; (4) các cơ quan tiến hành tố tụng còn nhầm lẫn khi định tội danh đối với tội phạm trong lĩnh vực CNTT, MVT; (5) việc quyết định hình phạt đối với tội phạm trong lĩnh vực CNTT, MVT còn chưa chính xác và thống nhất; (6) khó khăn của các cơ quan tiến hành tố tụng khi phải giải quyết vụ án liên quan đến người nước ngoài.

Những hạn chế, khó khăn, vướng mắc trên là do 3 nguyên nhân cơ bản sau:(1) Nguyên nhân từ những tồn tại, bất cập trong các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT; (2) Nguyên nhân từ sự chậm trễ, thiếu giải thích, hướng dẫn của cơ quan có thẩm quyền để áp dụng quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT;(3) Nguyên nhân từ những hạn chế trong công tác tổ chức thực hiện quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT.

Trên cơ sở kết quả nghiên cứu của các nội dung lý luận, quy định và thực tiễn áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong thời gian qua, Luận án xây dựng một số giải pháp nâng cao hiệu quả áp dụng các quy định này trong thời gian tới. Các nhóm giải pháp cơ bản của luận án là: (1) giải pháp hoàn thiện quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT; (2) giải pháp về giải thích, hướng dẫn áp dụng quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT; (3) giải pháp hoàn thiện, đổi mới công tác tổ chức, thực hiện quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT.

PHẦN KẾT LUẬN

Trong bối cảnh hiện nay, khi CNTT, MVT đang phát triển rất nhanh và được ứng dụng rộng rãi trong mọi lĩnh vực của đời sống xã hội, tội phạm trong lĩnh vực CNTT, MVT cũng diễn ra hết sức nghiêm trọng và phức tạp. Trong khi đó, quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT và thực tiễn áp dụng các quy định này còn hạn chế, vướng mắc. Nhiều vấn đề lý luận về tội phạm trong lĩnh vực CNTT, MVT còn chưa rõ ràng và thống nhất. Do đó, cần phải có sự nghiên cứu một cách tổng thể về tội phạm trong lĩnh vực CNTT, MVT theo LHS Việt Nam. Đó là lý do tác giả lựa chọn đề tài "*Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo Luật hình sự Việt Nam*" làm đề tài luận án nghiên cứu sinh của mình. Thông qua việc nghiên cứu đề tài này, 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. Có thể thấy rằng, các nghiên cứu về tội phạm trong lĩnh vực CNTT, MVT đã xây dựng được hệ thống lý luận phong phú và đa dạng; tổng kết đánh giá thực tiễn áp dụng quy định của LHS để chỉ ra những hạn chế, khó khăn, vướng mắc, đồng thời đề xuất giải pháp khắc phục. Tuy nhiên, trong giai đoạn hiện nay, còn nhiều vấn đề cần phải tiếp tục nghiên cứu như: nhận thức về tội phạm trong lĩnh vực CNTT, MVT chưa thống nhất; do sự phát triển của lĩnh vực CNTT, MVT nên nhiều hành vi phạm tội mới cần được xử lý; BLHS năm 2015 mới ra đời, chưa có nhiều nghiên cứu, đánh giá về thực tiễn áp dụng. Điều đó, đòi hỏi luận án cần tiếp tục nghiên cứu nhằm đề xuất một số giải pháp nâng cao hiệu quả áp dụng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT trong thời gian tới.

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

một trong những tội phạm liên quan đến CNTT, MVT. Khái niệm tội phạm trong lĩnh vực CNTT, MVT được hiểu 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*".

Căn cứ theo khái niệm trên, Luận án đã phân tích làm rõ các đặc điểm của tội phạm trong lĩnh vực CNTT, MVT 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.

Luận án đã thực hiện việc phân loại tội phạm trong lĩnh vực CNTT, MVT theo các tiêu chí sau:

(1) Dựa vào tính chất, mức độ nguy hiểm cho xã hội của hành vi phạm tội, tội phạm trong lĩnh vực CNTT, MVT được chia thành bốn loại, bao gồm: tội phạm ít nghiệm trọng, tội phạm nghiêm trọng, tội phạm rất nghiêm trọng và tội phạm đặc biệt nghiêm trọng.

(2) Dựa vào vai trò của CNTT, MVT đối với tội phạm, tội phạm trong lĩnh vực CNTT, MVT được chia thành hai loại: tội phạm trong lĩnh vực CNTT, MVT trong đó mạng máy tính, mạng viễn thông, phương tiện điện tử,

dữ liệu điện tử trở thành mục tiêu tấn công của tội phạm; tội phạm trong lĩnh vực CNTT, MVT trong đó người phạm tội sử dụng CNTT, MVT thực hiện tội phạm trong môi trường không gian mạng.

(3) Dựa vào vai trò của CNTT, MVT và mục đích phạm tội, tội phạm trong lĩnh vực CNTT, MVT được chia thành bốn loại, bao gồm: 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; tội phạm trong lĩnh vực CNTT, MVT trong đó người phạm tội có mục đích chiếm đoạt tài sản; 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; 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.

Trên cơ sở hệ thống lý luận của tội phạm trong lĩnh vực CNTT, MVT, chúng ta thấy hoàn toàn có cơ sở để quy định về tội phạm này trong BLHS.

Những vấn đề lý luận trên đã được minh chứng thông qua các phân tích của về quy định của pháp luật quốc tế về tội phạm trong lĩnh vực CNTT, MVT như Công ước Budapest 2001, Luật mẫu (2002, Công ước của các nước Châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân (2014), Công ước của các nước Ả - rập về chống tội phạm công nghệ thông tin.

Thứ ba, Luận án đã phân tích, đánh giá thực trạng quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT; đồng thời tổng kết, đánh giá thực tiễn áp dụng các quy định này của Tòa án trong giai đoạn 2009 - 2020. Qua đó thấy rằng, nội dung quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT từng bước được xây dựng và hoàn thiện phù hợp với xu thế chung của các văn bản pháp luật quốc tế. Tuy nhiên, vẫn còn có những tồn tại, hạn chế cần được tiếp tục nghiên cứu hoàn thiện hơn nữa trong thời gian tới. Trong

quá trình áp dụng quy định này còn xuất hiện không ít những hạn chế, khó khăn, vướng mắc. Trong đó, có 6 hạn chế, khó khăn, vướng mắc cơ bản sau: (1) 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; (2) 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; (3) 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; (4) các cơ quan tiến hành tố tụng còn nhầm lẫn khi định tội danh đối với tội phạm trong lĩnh vực CNTT, MVT; (5) việc quyết định hình phạt đối với tội phạm trong lĩnh vực CNTT, MVT còn chưa chính xác và thống nhất; (6) khó khăn của các cơ quan tiến hành tố tụng khi phải giải quyết vụ án liên quan đến người nước ngoài.

Những hạn chế, khó khăn, vướng mắc trên các nguyên nhân cơ bản như: các quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT còn có tồn tại, bất cập; Công tác giải thích, hướng dẫn áp dụng quy định của BLHS của cơ quan có thẩm quyền còn thiếu, trậm trễ; Công tác tổ chức thực hiện quy định của LHS về tội phạm trong lĩnh vực CNTT, MVT còn nhiều bất cập, vướng mắc.

Thứ tư, trên cơ sở kết quả nghiên cứu về lý luận, quy định của BLHS và thực tiễn áp dụng các quy định về tội phạm trong lĩnh vực CNTT, MVT trong 12 năm qua, Luận án xây dựng các giải pháp nâng cao hiệu quả áp dụng quy định của BLHS trong thời gian tới như sau: (1) Tiếp tục nghiên cứu hoàn thiện quy định của BLHS năm 2015 về tội phạm trong lĩnh vực CNTT, MVT; (2) tăng cường công tác giải thích, hướng dẫn áp dụng quy định của BLHS về tội phạm trong lĩnh vực CNTT, MVT của cơ quan nhà nước có thẩm quyền; (3) đổi mới và hoàn thiện công tác tổ chức, thực hiện quy định của LHS về tội

phạm trong lĩnh vực CNTT, MVT.

Với những kết quả đạt được trên, Luận án này sẽ góp phần vào sự thành công của công tác đấu tranh, phòng chống tội phạm trong lĩnh vực CNTT, MVT trong thời gian tới.

DANH MỤC TÀI LIỆU

DANH MỤC VĂN BẢN PHÁP LUẬT

Văn bản pháp luật của Việt Nam

1. Bộ luật hình sự 1999

2. Bộ luật hình sự 2015

3. Bộ luật tố tụng hình sự năm 2015

4. Luật Công nghệ thông tin 2006

5. Luật công nghệ cao 2008

6. Luật an toàn thông tin mạng 2015

7. Luật viễn thông 2009

8. Luật tần số vô tuyến điện 2009

9. Luật an ninh mạng 2018

10. Nghị quyết số 49-NQ/TW của Bộ Chính trị ngày 26/5/2005 về Chiến lược cải cách tư pháp đến năm 2020.

11. Nghị định 70/2000/NĐ-CP của Chính phủ ngày 21/11/2000 về việc giữ bí mật, lưu trữ và cung cấp các thông tin có liên quan đến tiền gửi và tài sản gửi của khách hàng.

12. Nghị định 52/2013/NĐ-Cp ngày 15/5/2013 về thương mại điện tử.

13. Nghị định 40/2018/NĐ-CP ngày 12/3/2018 của Chính phủ quy định về kinh doanh theo phương thức đa cấp.

14. Nghị định 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ quy định về quản lý, cung cấp và sử dụng dịch vụ internet và thông tin trên mạng.

15. Thông tư số 19/2013/TT-BTTTT ngày 02/12/2013 của Bộ trưởng Bộ thông tin và truyền thông quy định tần số cấp cứu, an toàn, tìm kiếm, cứu nạn trên biển và hàng không dân dụng.

16. Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012 của Chính phủ hướng dẫn một số quy định của BLHS năm 1999 về tội phạm công nghệ thông tin, viễn thông.
17. Nghị quyết số 01/2006/NQ-HĐTP ngày 12/5/2006 của Hội đồng thẩm phán toà án nhân dân tối cao.
18. Thông tư số 24/2015/TT-BTTTT ngày 18/8/2015 quy định về quản lý và sử dụng tài nguyên internet.

Văn bản pháp luật quốc tế và nước ngoài

19. Công ước Châu Âu về tội phạm mạng 2001.
20. Luật mẫu về tội phạm máy tính của các nước thuộc khối thịnh vượng chung (Anh, Úc, Newziland, Canada…) 2002.
21. Công ước Châu Phi về tội phạm mạng.
22. Công ước của các nước Ả Rập về xét xử tội phạm công nghệ thông tin.
23. Một số văn bản của Hội đồng châu Âu về tội phạm mạng.
24. Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders: https://www.unodc.org/documents/congress//Previous_ Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_ Computer_Networks.pdf (truy cập ngày 2/3/2020).
25. ITU/CARICOM/CTU Model Legilative Texts, Art.14: https://www.itu.int /ITUD/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf (truy cập ngày 8/4/2018).
26. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: https://rm.coe.int/CoERMPublicCommonSearchServices/ DisplayDCTMContent?documentId=090000168008160f (truy cập ngày 10/4/2019).

27. Luật sửa đổi, bổ sung Luật bảo vệ thông tin cá nhân của Nhật Bản (2017) (*Amended Act on the Protection of Personal Information*):https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf (truy cập ngày 20/2/2020).

DANH MỤC BẢN ÁN ĐÃ SỬ DỤNG

28. Bản án số 59/2017/HSST ngày 28/9/2017 TAND Bình Xuyên, Vĩnh Phúc.

29. Bản án số 97/2017/HSST ngày 25/12/2017 TAND Đan Phượng, Hà Nội.

30. Bản án số 701/2017/HS-PT ngày 22/9/2017 TAND TP. Hà Nội.

31. Bản án số 41/2017/HS-ST ngày 27/12/2017 TAND tỉnh Quảng Trị.

32. Bản án số 169/2018/HS-PT ngày 17/4/2018 TAND cấp cao tại TP. Hồ Chí Minh.

33. Bản án số 245/2018/HS-PT ngày 23/4/2018 TAND cấp cao tại TP. Hồ Chí Minh.

34. Bản án số 46/2018/HSST ngày 17/5/2018 của TAND thị xã Phổ Yên, Thái Nguyên.

35. Bản án số 11/2018/HS-ST ngày 19/1/2018 của TAND quận 3, TP. Hồ Chí Minh

36. Bản án số 290/2017/HSPT ngày 20/4/2017 của TAND TP. Hà Nội.

37. Bản bản án số 361/2017/HS-PT ngày 20/7/2017 của TAND cấp cao tại TP. Hồ Chí Minh.

38. Bản án số 26/2017/HSST ngày 27/9/2017 của TAND huyện Nghi Xuân, Hà Tĩnh

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng việt

Sách, luận văn, luận án

39. Lại Kiên Cường (2010), *Phòng ngừa tội phạm trong lĩnh vực thương mại điện tử của lực lượng cảnh sát nhân dân*, Luận án tiến sỹ, Học viện cảnh sát nhân dân, Hà Nội.

40. Lê Đăng Doanh - Cao Thị Oanh (2016), *Bình luận khoa học Bộ luật hình sự 2015*, NXB. Hồng Đức, Hà Nội.

41. Đại học Nông Lâm Huế, *Giáo trình công nghệ thông tin cơ bản* http://ciffl.huaf.edu.vn/uploads/page/giao_trinh_cntt.pdf (truy cập 02/2/2020)

42. Nguyễn Văn Hương, "Đánh giá tính thống nhất giữa BLHS năm 2015 với Luật công nghệ thông tin" thuộc đề tài cấp Bộ (2016), *Nghiên cứu tính thống nhất giữa Bộ luật hình sự trong việc quy định các tội phạm với các luật khác trong hệ thống pháp luật Việt nam*, Bộ tư pháp, do GS.TS. Nguyễn Ngọc Hòa làm chủ nhiệm đề tài.

43. Nguyễn Ngọc Hoà (2018), *Bình luận khoa học Bộ luật hình sự năm 2015, được sửa đổi, bổ sung năm 2017 (Phần các tội phạm)*, quyển 2, NXB. Tư pháp, Hà Nội.

44. Trần Văn Hòa (2011), *An toàn thông tin và công tác phòng chống tội phạm sử dụng công nghệ cao*, NXB. Công an nhân dân, Hà Nội.

45. Phạm Văn Lợi (2007), *Tội phạm trong lĩnh vực công nghệ thông tin*, NXB. Tư pháp, Hà Nội.

46. Trần Thị Hồng Lê (2009), *Các tội phạm trong lĩnh vực tin học theo Luật hình sự Việt Nam*, Luận văn thạc sỹ luật học, khoa Luật, Đại học Quốc gia Hà Nội.

47. Nguyễn Đức Mai (2013), *Bình luận khoa học Bộ luật hình sự 1999 (Phần các tội phạm)*, NXB. Chính trị quốc gia, Hà Nội.

48. Nguyễn Văn Ngọc (2012), *Từ điển kinh tế học*, NXB. Đại học kinh tế quốc dân, Hà Nội.

49. Trường Đại học kiểm sát Hà Nội (2016), *Giáo trình Luật hình sự Việt Nam Tập 2*, NXB. Đại học quốc gia Hà Nội, Hà Nội.

50. Trường Đại học luật Hà Nội (2015), *Giáo trình Luật hình sự Việt Nam* (Tập II), NXB. Công an nhân dân, Hà Nội.

51. Trường Đại học luật Hà Nội (2017), *Giáo trình luật hình sự (Phần chung)*, NXB. Công an nhân dân, Hà Nội.
52. Trần Thanh Thảo (2013), *Tội phạm công nghệ thông tin trong Bộ luật hình sự Việt Nam*, Luận văn thạc sỹ luật học, Trường Đại học luật Thành phố Hồ Chí Minh, Thành phố Hồ Chí Minh.
53. Viện chiến lược và khoa học công an (2007), *Tội phạm trong lĩnh vực bưu chính- viễn thông và giải pháp phòng ngừa, đấu tranh*, NXB. Công an nhân dân, Hà Nội.
54. Viện khoa học pháp lý (2006), *Từ điển luật học*, NXB. Từ điển bách khoa và NXB. Tư pháp, Hà Nội.

Tạp chí chuyên ngành

55. Nguyễn Hòa Bình (2003), "Tội phạm máy tính - Khái niệm, đặc trưng và một số giải pháp phòng, chống", *Tạp chí Công an nhân dân*, tháng 8/2003.
56. Mai Thế Bảy (2002), "Về việc xác định tội danh đối với một số hành vi vi phạm trong lĩnh vực viễn thông", *Tạp chí Nhà nước và Pháp luật*, số 3/2002.
57. Bùi Quang Nhơn & Phạm Văn Beo (2005), "Cần tội phạm hóa và cụ thể hóa các hành vi nguy hiểm liên quan đến máy tính", *Tạp chí Dân chủ & Pháp luật*, số 3/2005.
58. Đỗ Văn Chỉnh (2004), "Xác định tội trộm cắp tài sản đối với người lắp đặt thiết bị thu phát viễn thông để thu lợi bất chính là có căn cứ", *Tạp chí toà án nhân dân*, số 19/2004.
59. Lê Đăng Doanh (2006), "Về định tội danh đối với hành vi làm, sử dụng thẻ tín dụng giả hay các loại thẻ khác để mua hàng hóa hoặc rút tiền tại các máy trả tiền tự động của các ngân hàng", *Tạp chí Toà án nhân dân*, số 17/2006.
60. Lê Đăng Doanh (2006), "Về định tội danh đối với hành vi làm, sử dụng thẻ tín dụng giả hay các loại thẻ khác để mua hàng hóa hoặc rút tiền tại máy trả tiền tự động của các ngân hàng", *Tạp chí Toà án nhân dân*, số 3/2006.

61. Nguyễn Minh Đức (2008), "Viện kiểm sát nhân dân trước những khó khăn, thách thức của các tội phạm về công nghệ thông tin", *Tạp chí kiểm sát*, số 19 (tháng 10/2008).

62. Cao Anh Đức (2015), "Tính chất của tình hình tội phạm sử dụng công nghệ cao tại Việt Nam - Thủ đoạn và dự báo", *Tạp chí Nghiên cứu lập pháp*, http://lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid=208465 (truy cập ngày 15/10/2019).

63. Nguyễn Minh Đức (2014), "Đặc điểm tội phạm học của tội phạm sử dụng công nghệ cao và giải pháp nâng cao hiệu quả phòng ngừa, đấu tranh", *Kỷ yếu hội thảo "Phòng chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo"*, Học viện cảnh sát nhân dân, tháng 11/2014.

64. Đặng Trung Hà (2009), "Khái niệm và đặc điểm của tội phạm công nghệ thông tin - Sự khác nhau giữa tội phạm công nghệ thông tin và tội phạm thông thường", *Tạp chí Dân chủ và Pháp luật*, số 3/2009.

65. Nguyễn Văn Hoàn (2010), "Cần sớm có văn bản hướng dẫn thực hiện luật sửa đổi, bổ sung một số điều của Bộ luật hình sự về các tội phạm trong lĩnh vực công nghệ thông tin", *Tạp chí Kiểm sát*, số 4 (tháng 2/2010).

66. Trần Cảnh Hưng (2003), "Một số vấn đề lý luận và thực tiễn về tội phạm máy tính", *Tạp chí kiểm sát*, số 1/2003.

67. Dương Tuyết Miên, Nguyễn Ngọc Khanh (2000), "Tội phạm máy tính", *Tạp chí Toà án nhân dân*, số 5/2000.

68. Nguyễn Quý Khuyến (2017), "Tội 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 theo BLHS năm 2015", Tạp chí Toà án nhân dân, số 1/2017.

69. Nguyễn Quý Khuyến (2017), "Dấu hiệu định lượng thiệt hại của các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo BLHS năm 2015", *Tạp chí kiểm sát*, số 18/2017.

70. Nguyễn Quý Khuyến (2020), "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.

71. Phùng Trung Tập (2018), "Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình", *Tạp chí Kiểm sát*, số 02/2018.

72. Nguyễn Mạnh Toàn (2002), "Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học", *Tạp chí Nhà nước và Pháp luật*, số 3/2002.

73. Phạm Minh Tuyên (2012), "Quy định của BLHS và các văn bản hướng dẫn thi hành luật sửa đổi, bổ sung BLHS năm 2009 về tội phạm trong lĩnh vực CNTT và viễn thông ở Việt Nam", *Tạp chí Kiểm sát*, số 19/2012.

74. Phạm Minh Tuyên (2013), "Một số vướng mắc và biện pháp xử lý tội phạm trong lĩnh vực CNTT, viễn thông ở Việt Nam", *Tạp chí Kiểm sát*, số 23/2013.

Tiếng nước ngoài

Sách

75. Bryan A. Garner (1996), *Black's Law Dictionary*, West Publishing Co.

76. Debra Littejohn Shinder (2002), *Scene of the Cybercrime*, Syngress Publishing, Inc.

77. Daniel T. Kuehl (2009), *From Cyberspace to Cyberpower: Defining the Problem*, Washing, D.C. National Defense University Press.

78. Marco Gercke (2012), *"Understanding cybercrime: phenomena, challenges and legal response"*, ITU.

79. Scott Eltringham (2007), *Prosecuting Computer Crime:* http://www.steptoecyberblog.com/files/2012/11/ccmanual1.pdf

80. Whittle, B. David (1996), *Cyber space: The Human Dimension*, W.H. Freeman Co., New York.

81. M.E. Kabay, *A Brief History of Computer Crime: An Introduction for Students*: http://www.mekabay.com/overviews/history.pdf .

82. Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (2013), *Comprehensive Study On Cybercrime,* United Nations (UNODC): https://www.unodc.org/...**crime**/ ...**2013**/**CYBERCRIME_STUDY**_210213.pdf

Tạp chí chuyên ngành:

83. Aaron Burstein (2003), "A servey of Cybercrime in the United States", *Berkeley Technology Law Journal*, Volume 18/Issue 1/Article 20.

84. Bettina Weisser, "Cyber Crime - The Information Society and Related Crime": http://www.penal.org/sites/default/files/files/RM-8.pdf

85. Chawki, M (2005), *"A Critical Look at the Regulation of Cybercrime"*, *The ICFAI Journal of Cyberlaw*: http://www.findarticles.com/p/articles/mi_m2194/is_8_70/ai_78413303>

86. Frank Easterbrook (2007), "Cyberspace and the Law of the Horse", *CHI.Legal F*. 2007.

Webste

87. http://tuphaptamky.gov.vn/2014/news/Gop-y-Hien-phap/Nhu-cau-luat-hoa-quyen-bieu-tinh-theo-Hien-phap-nam-2013-1518.html

88. https://vnexpress.net/so-hoa/luong-nguoi-dung-internet-can-moc-mot-nua-dan-so-the-gioi-3851569.html

89. https://vnetwork.vn/news/cac-so-lieu-thong-ke-internet-viet-nam-2019

90. https://www.baomoi.com/canh-giac-voi-loai-hinh-toi-pham-nguoi-nuoc-ngoai-su-dung-cong-nghe-cao-chiem-doat-tai-san/c/22260395.epi

91. http://pup.edu.vn/index.php/news/Nghien-cuu-Trao-doi/Mot-so-trao-doi-ve-toi-pham-su-dung-Cong-nghe-cao-theo-quy-dinh-cua-phap-luat-Viet-Nam-657.html

92. http://cpd.vn/news/detail/tabid/77/newsid/1306/seo/Chang-duong-phat-trien-cua-nganh-Ky-thuat-May-tinh/Default.aspx

93. http://vietnamnet.vn/vn/kinh-doanh/bi-an-phong-may-tinh-ve-chien-tranh-viet-nam-234670.html
94. http://tiasang.com.vn/-khoa-hoc-cong-nghe/chuyen-ve-chiec-may-vi-tinh-dau-tien-cua-viet-nam-1044
95. https://nld.com.vn/thoi-su-trong-nuoc/hacker-trung-quoc-gay-su-co-tai-san-bay-noi-bai-tan-son-nhat-20160729210104008.htm
96. https://baotintuc.vn/phap-luat/hack-he-thong-du-lieu-nang-diem-cho-71-sinh-vien-20140825140005350.htm
97. https://vietnamnet.vn/vn/phap-luat/ho-so-vu-an/nam-thanh-nien-nghi-xam-nhap-xoa-sach-du-lieu-cua-ubnd-huyen-443941.html
98. https://vnexpress.net/kinh-doanh/2-chieu-lua-pho-bien-tren-thi-truong-chung-khoan-2715571.html
99. https://nld.com.vn/phap-luat/xet-xu-vu-trom-cap-cuoc-vien-thong-lon-nhat-tu-truoc-toi-nay-222158.htm
100. https://thanhnien.vn/thoi-su/phap-luat/toi-pham-trung-quoc-trom-cuoc-vien-thong-o-ha-noi-267710.html
101. https://www.vnnic.vn/dns/congnghe/h%E1%BB%87-th%E1%BB%91ng-t%C3%AAn-mi%E1%BB%81n
102.http://nguoibaovequyenloi.com/User/ThongTin_ChiTiet.aspx?MaTT=182201553140789 72&MaMT=24
103. http://m.bkav.com.vn/tin_tuc_noi_bat/-/chi_tiet/601424/tong-ket-an-ninh-mang-nam-2018-va-du-bao-xu-huong-2019
104. http://congantravinh.gov.vn/ch12/178-Canh-bao-toi-pham-Cong-nghe-cao.html
105. https://vnexpress.net/kinh-doanh/ngan-hang-dong-loat-canh-bao-toi-pham-the-bung-phat-cuoi-nam-3864236.html
106. http://congan.com.vn/vu-an/mat-may-tinh-chua-20000-so-do-khien-nguoi-dan-hoang-mang_64120.html

107. http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2018-08-13/toi-pham-cong-nghe-cao-trong-linh-vuc-tien-te-gia-tang-60921.aspx
108. https://kiemsat.vn/kinh-nghiem-truy-to-toi-pham-su-dung-cong-nghe-cao-cua-vien-cong-to-singapore-50807.htmla

PHỤ LỤC

Phụ lục 1:
Bảng so sánh giữa các văn bản pháp luật quốc tế về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thong

Hành vi phạm tội	Công ước của Hội đồng Châu Âu về tội phạm mạng (2001)	Luật mẫu về tội phạm máy tính và liên quan đến máy tính của Khối thịnh vương chung	Công ước của các nước Châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân năm 2014	Công ước của các nước Ả-rập về chống tội phạm công nghệ thông tin
Tội truy cập bất hợp pháp	Điều 2	Điều 5, 7	Điểm a. b, c khoản 1 Điều 29	Điều 6
Tội truy cập trái phép, ngăn chặn, chặn bắt bất hợp pháp dữ liệu máy tính	Điều 2, 3	Điều 5, 8	Điểm d khoản 1, điểm a khoản 2 Điều 29	Điều 6, 7, 18
Tội gây rối dữ liệu	Điều 4	Điều 6	Điểm d, e, f khoản 1, điểm a, b khoản 2 Điều 29	Điều 8
Tội gây rối hệ thống	Điều 5	Điều 7		Điều 6
Tội lạm dụng các thiết bị	Điều 6	Điều 9	Điểm g, h khoản 1 Điều 29	Điều 9

Tội xâm phạm bí mật đời tư				
Tội giả mạo liên quan đến máy tính	Điều 7		Điểm c, d khoản 2 Điều 29, Điểm b khoản 1 Điều 30	Điều 10, 18
Tội lừa đảo liên quan đến máy tính	Điều 8			Điều 11
Tội phạm về công cụ thanh toán điện tử liên quan đến máy tính				Điều 18
Tội phạm liên quan đến thông tin cá nhân				
Tội phạm liên quan đến sở hữu trí tuệ	Điều 10			Điều 17
Gửi thư rác				
Tội liên quan đến quấy rối, đe doạ hoặc các hành vi gây hại cho con người				
Tội liên quan đến phân biệt chủng tộc, bài ngoại	Điều 2, 3 Nghị định thư bổ sung năm 2003		Điểm e, f, g, h khoản 3 Điều 29	

Tội phạm liên quan đến việc cổ suý diệt chủng hoặc tội phạm chống loài người	Điều 6 Nghị định thư bổ sung năm 2003			
Tội liên quan đến tài liệu khiêu dâm trẻ em	Điều 9	Điều 10	Điểm a, b, c, d khoản 3 Điều 29	Điều 12
Tội phạm liên quan đến lừa gạt, dụ dỗ trẻ em				
Tội phạm liên quan đến hành vi tài trợ khủng bố				Điều 15
Tội phạm liên quan đến rửa tiền				Điều 15
Tội phạm liên quan đến buôn người				Điều 16
Tội phạm liên quan đến hành vi chống đối trật tự công cộng, đạo đức, an ninh				Điều 12, 13, 14, 15

Phụ lục 2:

Bảng tần số sử dụng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu nạn

(*Ban hành kèm theo Thông tư 19/2013/TT-BTTTT ngày 02 tháng 12 năm 2013 của Bộ trưởng Bộ Thông tin và Truyền thông)*

BẢNG 1: TẦN SỐ DƯỚI 30 MHz

Tần số (kHz)	Quy định sử dụng
490	Tần số 490 kHz là tần số dành riêng cho thông tin an toàn hàng hải (MSI) sử dụng phương thức điện báo in trực tiếp băng hẹp.
518	Tần số 518 kHz là tần số dành riêng cho hệ thống phát và thu tự động thông tin an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
2174,5	Tần số 2174,5 kHz là tần số dành riêng cho phát bản tin cứu nạn và an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
2182	Tần số 2182 kHz là tần số cấp cứu hàng hải quốc tế sử dụng phương thức điều chế biên độ đơn biên với sóng mang nén (J3E). Tần số này cũng được sử dụng để: - Gọi và bắt liên lạc theo quy trình quy định tại Điều 57-Thể lệ vô tuyến điện của Liên minh viễn thông Quốc tế. - Phát thông báo hoặc phát danh sách liên lạc như khuyến nghị ITU-R M.1171. Sử dụng trong hoạt động tìm kiếm, cứu nạn hàng không dân dụng và trên biển.
2187,5	Tần số 2187,5 kHz là tần số dành riêng cho các cuộc gọi cấp cứu và an toàn hàng hải sử dụng phương thức gọi chọn số.
3023	Tần số 3023 kHz được sử dụng như sau: - Các đài di động tham gia hoạt động tìm kiếm và cứu nạn sử dụng cho

	mục đích cấp cứu và an toàn hàng không bằng phương thức thoại. - Dùng để thông tin liên lạc giữa các đài di động tham gia vào hoạt động tìm kiếm và cứu nạn, và giữa các đài này với các đài mặt đất tương ứng theo quy định của Phụ lục 27 – Thể lệ thông tin vô tuyến điện của Liên minh viễn thông Quốc tế bằng phương thức thoại.
4125	Tần số 4125 kHz là tần số phát thông tin cấp cứu và an toàn hàng hải bằng phương thức thoại. Các đài tàu bay cũng có thể sử dụng để liên lạc với các đài thuộc nghiệp vụ Di động hàng hải với mục đích cấp cứu và an toàn, bao gồm cả tìm kiếm và cứu nạn với công suất bao đỉnh không vượt quá 1kW và phải có khả năng thu và phát loại phát xạ J3E.
4177,5	Tần số 4177,5 kHz là tần số dành riêng cho phát bản tin cứu nạn và an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
4207,5	Tần số 4207,5 kHz là tần số dành riêng cho gọi cấp cứu và an toàn hàng hải bằng phương thức gọi chọn số.
4209,5	Tần số 4209,5 kHz được sử dụng dành riêng cho hệ thống phát và thu tự động thông tin an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
4210	Tần số 4210 kHz là tần số dành riêng cho truyền dẫn bản tin an toàn hàng hải (MSI) ở các vùng biển xa, chiều từ bờ tới tàu, bằng phương thức điện báo in trực tiếp băng hẹp.
5680	Tần số 5680 kHz được sử dụng như sau: - Các đài di động tham gia hoạt động tìm kiếm và cứu nạn sử dụng cho mục đích cấp cứu và an toàn hàng không bằng phương thức thoại. - Dùng để thông tin liên lạc giữa các đài di động tham gia vào hoạt động tìm kiếm và cứu nạn, và giữa các đài này với các đài mặt đất tương ứng theo quy định của Phụ lục 27 – Thể lệ thông tin vô tuyến điện của Liên minh viễn thông Quốc tế bằng phương thức thoại.

6215	Tần số 6215 kHz được sử dụng như sau: - Phát thông tin cấp cứu và an toàn hàng hải bằng phương thức thoại. - Gọi, bắt liên lạc bằng phương thức thoại đơn biên với công suất bao đỉnh không vượt quá 1 kW.
6268	Tần số 6268 kHz là tần số dành riêng cho phát bản tin cứu nạn và an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
6312	Tần số 6312 kHz là tần số dành riêng cho các cuộc gọi cấp cứu và an toàn hàng hải bằng phương thức gọi chọn số.
6314	Tần số 6314 kHz là tần số dành riêng cho truyền dẫn bản tin an toàn hàng hải (MSI) ở các vùng biển xa, chiều từ bờ tới tàu, bằng phương thức điện báo in trực tiếp băng hẹp
6973	Tần số 6973 kHz là tần số liên lạc giữa Đồn Biên phòng và tàu thuyền bằng phương thức thoại.
7903	Tần số 7903 kHz là tần số cấp cứu hàng hải quốc gia sử dụng phương thức thoại đơn biên. Tàu thuyền được phép gọi bắt liên lạc trên tần số này.
7906	Tần số 7906 kHz là tần số phát thông tin an toàn hàng hải (MSI) và các thông báo liên quan đến phòng chống thiên tai, an toàn, an ninh trên biển; thông tin phục vụ công tác quản lý Nhà nước bằng phương thức thoại.
8291	Tần số 8291 kHz là tần số phát thông tin cấp cứu và an toàn hàng hải bằng phương thức thoại.
8294	Tần số 8294 kHz là tần số phát thông tin về áp thấp nhiệt đới, bão, lũ bằng phương thức thoại.
8376,5	Tần số 8376,5 kHz là tần số dành riêng cho phát bản tin cứu nạn và an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
8364	Tần số 8364 kHz là tần số dành cho hoạt động tìm kiếm, cứu nạn hàng không dân dụng sử dụng phương thức thoại.

8414,5	Tần số 8414,5 kHz là tần số dành riêng cho các cuộc gọi cấp cứu và an toàn hàng hải sử dụng phương thức gọi chọn số.
8416,5	Tần số 8416,5 kHz là tần số dành riêng cho truyền dẫn bản tin an toàn hàng hải (MSI) ở các vùng biển xa, chiều từ bờ tới tàu bằng phương thức điện báo in trực tiếp băng hẹp.
9339	Tần số 9339 kHz là tần số liên lạc giữa Đồn Biên phòng và tàu thuyền bằng phương thức thoại.
12251/13098	12251/13098 kHz là cặp tần số phát/thu giữa tàu – bờ và ngược lại để liên lạc giữa Đài canh dân sự Hải quân và tàu thuyền bằng phương thức thoại.
12290	Tần số 12290 kHz là tần số phát thông tin cấp cứu và an toàn hàng hải bằng phương thức thoại.
12520	Tần số 12520 kHz là tần số dành riêng cho phát bản tin cứu nạn và an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
12577	Tần số 12577 kHz là tần số dành riêng cho các cuộc gọi cấp cứu và an toàn hàng hải bằng phương thức gọi chọn số.
12579	Tần số 12579 kHz là tần số dành riêng cho truyền dẫn bản tin an toàn hàng hải (MSI) ở các vùng biển xa, chiều từ bờ tới tàu bằng phương thức điện báo in trực tiếp băng hẹp.
13434	Tần số 13434 kHz là tần số phát thông tin an toàn hàng hải (MSI) và các thông báo liên quan đến phòng chống thiên tai, an toàn, an ninh trên biển; thông tin phục vụ công tác quản lý Nhà nước bằng phương thức thoại.
16420	Tần số 16420 kHz là tần số phát thông tin cấp cứu và an toàn hàng hải bằng phương thức thoại.
16695	Tần số 16695 kHz là tần số dành riêng cho phát bản tin cứu nạn và an toàn hàng hải bằng phương thức điện báo in trực tiếp băng hẹp.
16804,5	Tần số 16804,5 kHz là tần số dành riêng cho các cuộc gọi cấp cứu và an

	toàn hàng hải bằng phương thức gọi chọn số.
16806,5	Các tần số này là tần số dành riêng cho truyền dẫn bản tin an toàn hàng hải (MSI) ở các vùng biển xa, chiều từ bờ tới tàu, bằng phương thức điện báo in trực tiếp băng hẹp.
19680,5	
22376	
26100,5	

Chú thích:

MSI: Thông tin an toàn hàng hải (MSI) gồm các cảnh báo hàng hải và cảnh báo khí tượng, dự báo thời tiết biển, thông tin tìm kiếm cứu nạn và các thông báo liên quan đến an toàn và khẩn cấp khác.

BẢNG 2: TẦN SỐ TRÊN 30 MHz

Tần số (MHz)	Quy định sử dụng
121,500	Tần số 121,500 MHz là tần số sử dụng cho mục đích cấp cứu và khẩn cấp hàng không bằng phương thức thoại. - Tần số này cũng có thể sử dụng cho các đài cứu nạn. Phao vô tuyến chỉ báo vị trí khẩn cấp sử dụng tần số này cho mục đích cấp cứu và khẩn cấp theo quy định của Liên minh viễn thông Quốc tế. - Tần số này cũng được các đài di động tham gia vào hoạt động tìm kiếm, cứu nạn sử dụng cho mục đích cấp cứu và an toàn. - Tần số này cũng được sử dụng để liên lạc giữa đài di động thuộc nghiệp vụ Di động hàng hải với các đài thuộc nghiệp vụ Di động hàng không với mục đích cấp cứu và khẩn cấp, sử dụng phương thức phát điều chế biên độ song biên (A3E). -Tàu bay quân sự Việt Nam sử dụng tần số 121,500 MHz với phương thức phát điều biên để liên lạc hai chiều với tàu thuyền trên biển cho mục đích tìm kiếm và cứu nạn.
123,100	Tần số 123,100 MHz là tần số phụ của tần số cấp cứu, khẩn cấp hàng không 121,500 MHz.

	- Tần số này cũng có thể sử dụng cho các đài thuộc nghiệp vụ di động hàng không, các đài mặt đất và đài di động khác khi tham gia vào hoạt động phối hợp tìm kiếm và cứu nạn. - Tần số này cũng được các đài di động tham gia vào hoạt động tìm kiếm, cứu nạn sử dụng cho mục đích cấp cứu và an toàn. - Các đài di động thuộc nghiệp vụ di động hàng hải có thể liên lạc với các đài thuộc nghiệp vụ di động hàng không trên tần số 123,100 MHz cho hoạt động phối hợp tìm kiếm và cứu nạn, sử dụng loại phát xạ A3E.
156,300	Tần số 156,300 MHz là tần số sử dụng cho thông tin liên lạc trong hoạt động tìm kiếm và cứu nạn hàng không dân dụng và trên biển. Tần số này cũng có thể được tàu bay sử dụng để liên lạc với các tàu thuyền cho mục đích an toàn.
156,425	Tần số 156,425 MHz là tần số liên lạc giữa Đài canh dân sự Hải quân và tàu thuyền bằng phương thức thoại.
156,525	Tần số 156,525 MHz là tần số gọi cấp cứu và an toàn hàng hải được sử dụng trong nghiệp vụ Di động hàng hải bằng phương thức gọi chọn số.
156,650	Tần số 156,650 MHz là tần số liên lạc giữa tàu thuyền với tàu thuyền liên quan đến an toàn hàng hải sử dụng phương thức thoại.
156,800	Tần số 156,800 MHz là tần số sử dụng cho thông tin liên lạc cấp cứu và an toàn hàng hải bằng phương thức thoại. Ngoài ra, tần số 156,8 MHz có thể được các đài tàu bay sử dụng chỉ cho mục đích an toàn.
161,500	Tần số 161,500 MHz là tần số phát thông tin an toàn hàng hải (MSI) bằng phương thức thoại của Hệ thống đài thông tin duyên hải Việt Nam.
161,975	Tần số 161,975 MHz là tần số AIS1, được sử dụng đối với các máy phát AIS tìm kiếm và cứu nạn (AIS-SART) trong hoạt động tìm kiếm và cứu nạn.
162,025	Tần số 162,025 MHz là tần số AIS 2, được sử dụng đối với các máy phát

	tìm kiếm và cứu nạn AIS (AIS-SART) trong hoạt động tìm kiếm và cứu nạn.
406-406,1	Băng tần số này được dành riêng cho phao vô tuyến chỉ báo vị trí khẩn cấp qua vệ tinh (EPIRB) công suất thấp hướng từ trái đất đến vũ trụ.
1530-1544	Ngoài việc sử dụng cho thông tin liên lạc, băng tần (1530-1544) MHz còn được sử dụng cho các mục đích cấp cứu và an toàn hàng hải chiều từ vũ trụ tới trái đất trong nghiệp vụ di động hàng hải qua vệ tinh. Thông tin cấp cứu, khẩn cấp và an toàn hàng hải GMDSS phải được ưu tiên trong băng tần này.
1544-1545	Việc sử dụng băng tần 1544-1545 MHz (chiều từ vũ trụ tới trái đất) được hạn chế cho các hoạt động cấp cứu và an toàn, bao gồm các đường tiếp sóng của các vệ tinh cần phải chuyển tiếp các phát xạ của pha vô tuyến chỉ báo vị trí khẩn cấp tới các đài trái đất và các đường thông tin băng hẹp (chiều từ vũ trụ tới trái đất) từ các đài không gian đến các đài di động.
1626,5-1645,5	Ngoài việc sử dụng cho thông tin liên lạc, băng tần (1626,5-1645,5) MHz được sử dụng cho mục đích cấp cứu và an toàn hàng hải theo chiều từ trái đất tới vũ trụ trong nghiệp vụ Di động hàng hải qua vệ tinh. Thông tin cấp cứu, khẩn cấp và an toàn hàng hải GMDSS được ưu tiên trong băng tần này.
1645,5-1646,5	Việc sử dụng băng tần (1645,5-1646,5) MHz chiều từ trái đất tới vũ trụ được giới hạn cho các hoạt động cấp cứu và an toàn.
9200-9500	Băng tần số này được các bộ phát đáp Ra – đa (SARTS) sử dụng nhằm tạo thuận lợi cho việc tìm kiếm và cứu nạn.

Chú thích:

AIS: là hệ thống nhận dạng tự động hàng hải để trao đổi thông tin giữa tàu thuyền với tàu thuyền và giữa tàu thuyền với bờ.

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

1. Nguyễn Quý Khuyến, "Về tội sản suất, 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 Toà án nhân dân*, số 3/2017;

2. Nguyễn Quý Khuyến, "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 Khuyến - Mục 2 Chương XXI: Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông)*;

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