VNU Journal of Science: Legal Studies, Vol. 40, No. 3 (2024) 25-37

VNU Journal of Science: Legal Studies

Journal homepage: https://js.vnu.edu.vn/LS

Original Article

# Shortcomings in the Regulations of Criminal Law on Cyber Crime and Recommendations

Nguyen Thi Phuong Hoa*, Tran Thanh Thao

*Ho Chi Minh City University of Law, 2-4 Nguyen Tat Thanh Street, District 4, Ho Chi Minh City, Vietnam*

Received 03 May 2023
Revised 14 March 2024; Accepted 25 September 2024

**Abstract:** In the modern digital space, personal data can be attacked and used for illegal purposes. On 17 April 2023, the Vietnamese Government passed Decree No. 13/2023/ND-CP on Protecting Personal Data. The Criminal Code of Vietnam 2015 (amended in 2017) set up cyber-related crimes to protect the safety of cyber activities in general and personal data in particular. However, there are a number of shortcomings in the Criminal Code in the comparison with the Decree 13/2023/ND-CP and international treaties on cybercrime. This article analyzes these shortcomings and provides recommendations to revise relevant provisions of the Criminal Code.

*Keywords:* Cybercrime, technology crime, computer crime, personal data, personal data protection.

* Corresponding author.
*E-mail address:* nguyenthiphuonghoa@gmail.com

https://doi.org/10.25073/2588-1167/vnuls.4557

# Hạn chế trong quy định của pháp luật hình sự về các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông và kiến nghị

Nguyễn Thị Phương Hoa*, Trần Thanh Thảo

*Trường Đại học Luật Thành phố Hồ Chí Minh, 2-4 Nguyễn Tất Thành, quận 4, Thành phố Hồ Chí Minh, Việt Nam*

Nhận ngày 03 tháng 5 năm 2023
Chỉnh sửa ngày 14 tháng 3 năm 2024; Chấp nhận đăng ngày 25 tháng 9 năm 2024

**Tóm tắt:** Trong môi trường điện tử hiện nay, dữ liệu cá nhân có thể bị "tấn công" và sử dụng vào mục đích bất hợp pháp. Ngày 17/04/2023, Chính phủ đã thông qua Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017) đã quy định về các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông để xử lý các hành vi xâm phạm an toàn của công nghệ thông tin, mạng viễn thông, trong đó có an toàn của dữ liệu cá nhân. Tuy nhiên đối chiếu với quy định của Nghị định số 13/2023/NĐ-CP và một số điều ước quốc tế về tội phạm mạng, quy định của Bộ luật Hình sự vẫn còn một số hạn chế. Bài viết phân tích hạn chế trong quy định của Bộ luật Hình sự về đối tượng tác động và dấu hiệu khách quan của các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông đối với việc bảo vệ dữ liệu cá nhân. Trên cơ sở so sánh với quy định của Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân và các chuẩn mực quốc tế, bài viết đề xuất kiến nghị hoàn thiện quy định liên quan của Bộ luật Hình sự.

*Từ khóa:* Tội phạm công nghệ thông tin, tội phạm mạng, tội phạm máy tính, dữ liệu cá nhân, bảo vệ dữ liệu cá nhân.

## 1. Mở đầu

Ngày 17/04/2023, Chính phủ đã thông qua Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (Nghị định số 13/2023/NĐ-CP). Nghị định cung cấp khái niệm mang tính khái quát về dữ liệu cá nhân: "Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm" (khoản 1 Điều 2). Nghị định cũng khẳng định việc bảo vệ dữ liệu cá nhân bao gồm xử lý các hành vi vi phạm dữ liệu cá nhân (khoản 5 Điều 2). Với vai trò là một công cụ cưỡng chế nghiêm khắc nhất của nhà nước để quản lý xã hội, bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân; luật hình sự bảo vệ dữ liệu cá nhân thông qua tội phạm hóa các hành vi xâm hại đến tính bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu cá nhân [1].[1]

* Tác giả liên hệ.
*Địa chỉ email:* nguyenthiphuonghoa@gmail.com
https://doi.org/10.25073/2588-1167/vnuls.4557

[1] Điều 25 Công ước Liên minh Châu Phi về an ninh và bảo vệ dữ liệu cá nhân năm 2014 (African Union Convention on Cyber Security and Personal Data) cũng nhấn mạnh việc tội phạm hóa các hành vi nguy hiểm để bảo vệ các thuộc tính này của dữ liệu. Ngoài ra, Công ước còn đề cập đến tính "tồn tại" (survival) của dữ liệu.

Mục 2 Chương XXI Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017) (sau đây gọi tắt là BLHS hoặc BLHS năm 2015) quy định về các tội phạm trong trong lĩnh vực công nghệ thông tin, mạng viễn thông. Nghiên cứu từ góc độ dữ liệu cá nhân, các tội phạm trong lĩnh vực này có thể chia thành hai nhóm: *một là,* các tội trực tiếp tác động đến dữ liệu cá nhân và *hai là,* các tội gián tiếp tác động đến dữ liệu cá nhân. Các tội trực tiếp tác động đến dữ liệu cá nhân được quy định tại các điều từ 287 đến 291,[2] các tội này có đối tượng tác động là dữ liệu cá nhân. Các tội gián tiếp tác động đến dữ liệu cá nhân được quy định tại Điều 285, 286, 293, 294[3] và đối tượng tác động của các tội này không phải là dữ liệu cá nhân nhưng hành vi phạm tội xâm hại đến tính bảo mật, tính toàn vẹn, tính khả dụng của dữ liệu cá nhân.

Cần đề cập rằng việc tấn công và sử dụng trái phép dữ liệu cá nhân để thực hiện hành vi trái pháp luật không chỉ bị xử lý bởi các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông đã nêu. Bên cạnh các tội này, BLHS còn quy định những tội phạm khác có tính chất bảo vệ dữ liệu cá nhân, ví dụ: Tội làm nhục người khác, tội lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân... Với phạm vi rộng như vậy, bài viết không thể phân tích hết những vấn đề liên quan, vì vậy bài viết chỉ tập trung vào các quy định của BLHS về các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông có ý nghĩa bảo vệ dữ liệu cá nhân.

Mặt khác, những tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông nêu trên được quy định không chỉ nhằm bảo vệ dữ liệu cá nhân mà còn đấu tranh với các hành vi nguy hiểm xâm hại đến an toàn của công nghệ thông tin và mạng viễn thông nói chung. Bài viết này tập trung vào những vấn đề trực tiếp liên quan bảo vệ dữ liệu cá nhân.

Ngày nay, thế giới đang chứng kiến sự phát triển mạnh mẽ của công nghệ thông tin và viễn thông, sự phát triển trong lĩnh vực này đã và đang ngày càng quan trọng đối với mỗi cá nhân cũng như toàn bộ quá trình phát triển kinh tế, xã hội của các quốc gia. Khoa học - công nghệ nói chung và công nghệ thông tin nói riêng, trên thực tế, đã trở thành nền tảng cho sự phát triển của đất nước và ngày càng trở nên then chốt trong nhiều hoạt động của xã hội [2]. Tính nhanh chóng, tiện lợi của các ứng dụng công nghệ thông tin, mạng viễn thông đã làm cho thành tựu này thâm nhập sâu rộng vào nhiều lĩnh vực, thay thế các phương thức truyền thống trước đây.

Tuy nhiên, điều đáng lo ngại là các hành vi tiêu cực, đe dọa sự an toàn trong sử dụng công nghệ thông tin, mạng viễn thông ở trên thế giới nói chung [3] và Việt Nam nói riêng đang ngày càng nghiêm trọng [4]. Những hành vi nguy hiểm trong lĩnh vực công nghệ thông tin, mạng viễn thông ngày càng đa dạng, không chỉ là hành vi chiếm đoạt tài sản; mà còn những hành vi khác như: hành vi xâm phạm bí mật cá nhân, hành vi xúc phạm nghiêm trọng nhân phẩm, danh dự của con người, hành vi xâm phạm an toàn của hoạt động ngân hàng và hệ thống thanh toán,… Trước thực tiễn đó, BLHS đã sửa đổi, bổ sung quy định về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông để kịp thời bảo vệ sự an toàn của mạng công nghệ thông tin, mạng viễn thông nói chung cũng như dữ liệu cá nhân nói riêng. Việc BLHS đã kịp thời bảo vệ dữ liệu cá nhân trong môi trường điện tử là một kết quả tích cực,

[2] Cụ thể: Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287); Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288); Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289); Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290); Tội thu thập, tàng trữ trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291).

[3] 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 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 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).

phù hợp với cách tiếp cận về quyền, đặc biệt là quyền nhân thân của cá nhân.

Các quy định của BLHS Việt Nam về tội phạm công nghệ thông tin, mạng viễn thông, nhìn chung, đã có sự tương thích nhất định với một số chuẩn mực quốc tế về tội phạm công nghệ thông tin. Có thể kể đến như: Công ước của Hội đồng châu Âu về tội phạm mạng năm 2001, Công ước của Liên minh các nước Ả rập đấu tranh với các tội phạm công nghệ thông tin năm 2012, Công ước của châu Phi về An ninh mạng và dữ liệu cá nhân năm 2014. Cần đề cập rằng, Việt Nam không phải là thành viên của các điều ước quốc tế nêu trên, nhưng những quy định về tội phạm hóa các hành vi nguy hiểm trong lĩnh vực công nghệ thông tin và mạng viễn thông trong các văn bản này là một nguồn tài liệu tham khảo hữu ích khi đề xuất hoàn thiện quy định tương ứng của Việt Nam.

Bên cạnh những kết quả đã nêu, nhìn từ góc độ bảo vệ dữ liệu cá nhân, quy định của BLHS năm 2015 vẫn còn một số hạn chế. Trên cơ sở so sánh với quy định của Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân và các điều ước quốc tế liên quan, bài viết chỉ ra các hạn chế trong quy định hiện hành của BLHS về đối tượng tác động và dấu hiệu khách quan của các tội trong lĩnh vực công nghệ thông tin, mạng viễn thông. Đồng thời, nhằm bảo đảm tính thống nhất trong nội tại hệ thống pháp luật Việt Nam, cũng như tăng cường tính hiệu quả của luật hình sự trong việc bảo vệ dữ liệu cá nhân, bài viết đề xuất một số kiến nghị để khắc phục các hạn chế này.

## 2. Hạn chế trong quy định của Bộ luật Hình sự năm 2015 về đối tượng tác động của các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông và kiến nghị

### *2.1. Hạn chế trong quy định của Bộ luật Hình sự năm 2015 về đối tượng tác động của các tội phạm trực tiếp tác động đến dữ liệu cá nhân và kiến nghị*

BLHS năm 2015 không sử dụng thuật ngữ "dữ liệu cá nhân" khi mô tả đối tượng tác động của các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, mà sử dụng đa dạng các thuật ngữ khác như: "dữ liệu điện tử" (khoản 1 Điều 287), "thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân" (điểm b khoản 1 Điều 288), "thông tin mạng máy tính" (Điều 288), "thông tin về tài khoản, thẻ ngân hàng" (điểm a khoản 1 Điều 290), "tài khoản" (điểm c khoản 1 Điều 290), "tài khoản ngân hàng" (Điều 291). Trong các thuật ngữ này, cụm từ "dữ liệu điện tử" được sử dụng phổ biến nhất.

Theo khoản 1 Điều 99 Bộ luật Tố tụng hình sự (BLTTHS) năm 2015: "Dữ liệu điện tử là ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự được tạo ra, lưu trữ, truyền đi hoặc nhận được bởi phương tiện điện tử". Như vậy, dữ liệu điện tử có nội hàm rộng hơn "dữ liệu cá nhân" tại Nghị định số 13/2023/NĐ-CP vì có thể bao gồm các dữ liệu khác của cơ quan, tổ chức, Nhà nước. Như đã đề cập, các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông không chỉ được quy định nhằm bảo vệ các dữ liệu cá nhân mà còn bảo vệ an toàn trong lĩnh vực công nghệ thông tin, mạng viễn thông nói chung; chính vì vậy việc sử dụng thuật ngữ này là hợp lý.

Về "thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân", Thông tư số 10/2012/TTLT- BCA - BQP - BTP - BTT&TT - VKSNDTC - TANDTC ngày 10/09/2012 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 giải thích rằng đây là "những thông tin thuộc sở hữu của cơ quan, tổ chức, cá nhân được pháp luật bảo vệ". Giải thích này ra đời trong bối cảnh chưa có văn bản pháp luật riêng về bảo vệ dữ liệu cá nhân. Theo quy định của Nghị định số 13/2023/NĐ-CP, "thông tin riêng của cá nhân" có thể hiểu là "dữ liệu cá nhân". Để bảo đảm cho tính thống nhất nội tại của hệ thống pháp luật, đối với các thuật ngữ mà các văn bản khác đã giải thích thì BLHS và các văn bản hướng dẫn thi hành BLHS thường sẽ sử dụng sự giải thích đó và không giới thiệu những nội dung riêng

biệt, trừ những trường hợp đặc thù [5][4]. Do vậy, để bảo đảm tính thống nhất, cụm từ "thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân" đã nêu trong BLHS nên sửa thành "dữ liệu hợp pháp của cơ quan, tổ chức, cá nhân".

Thuật ngữ "thông tin mạng máy tính" xuất hiện trong tên gọi của "Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông". Tuy nhiên, các văn bản luật quan trọng hiện hành về an ninh mạng, an toàn thông tin mạng, viễn thông và công nghệ thông tin không giải thích khái niệm này.

Lưu ý rằng khác với Việt Nam, Công ước châu Âu về tội phạm công nghệ thông tin năm 2001 (Công ước Budapest), đối tượng tác động của nhiều tội phạm trong Công ước này là, "dữ liệu máy tính" (computer data). "Dữ liệu máy tính" được hiểu 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" (Điều 1(b)) [6]. Công ước của Liên minh châu Phi về An ninh mạng và Bảo vệ dữ liệu cá nhân năm 2014 (Công ước châu Phi) [1] sử dụng thuật ngữ "dữ liệu được máy tính hóa" (computerized data, Điều 1) với nội dung có nhiều điểm tương đồng với Công ước Budapest.

So với khái niệm "dữ liệu điện tử" sử dụng trong luật Việt Nam, khái niệm "dữ liệu máy tính" của các Công ước có sự tương đồng nhưng cũng có điểm khác biệt. Về sự tương đồng, dạng tồn tại của những dữ liệu này khá đa dạng và chúng tương thích với hoạt động của hệ thống máy tính. Về sự khác biệt, "dữ liệu điện tử" trong luật Việt Nam được hiểu rộng hơn "dữ liệu máy tính". Theo khoản 2 Điều 99 BLTTHS năm 2015, dữ liệu điện tử "được thu thập từ phương tiện điện tử, mạng máy tính, mạng viễn thông, trên đường truyền và các nguồn điện tử khác". Như vậy, dữ liệu điện tử không chỉ là các dữ liệu tương thích với hoạt động của hệ thống máy tính mà còn tương thích với hoạt động viễn thông. Chính vì sự khác biệt đó, cân nhắc giữa các cụm từ: "thông tin mạng máy tính" (đang sử dụng trong BLHS và chưa được giải thích), "dữ liệu máy tính" (đang sử dụng trong các Công ước) và "dữ liệu điện tử" (đã được giải thích trong BLTTHS), Chúng tôi kiến nghị sử dụng cụm từ "dữ liệu điện tử". Việc dùng cụm từ này phù hợp với mục đích của nhà làm luật Việt Nam, bảo đảm sự thống nhất nội tại trong quy định về các tội phạm trong lĩnh vực này và đồng bộ với thuật ngữ đang sử dụng trong BLTTHS. Từ đó, tên gọi của "Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông" cần sửa đổi thành "Tội đưa hoặc sử dụng trái phép dữ liệu điện tử".

### *2.2. Hạn chế trong quy định của Bộ luật Hình sự năm 2015 về đối tượng tác động của các tội phạm gián tiếp tác động đến dữ liệu cá nhân và kiến nghị*

Theo quy định của BLHS năm 2015, đối tượng tác động của nhiều tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là "mạng viễn thông", "mạng máy tính". Tuy nhiên, các văn bản luật quan trọng hiện hành về viễn thông, công nghệ thông tin, an ninh mạng, an toàn thông tin mạng không giải thích khái niệm "mạng máy tính". Trước đây, theo khoản 3 Điều 2 Thông tư số 10/2012, "mạng máy tính" được hiểu là "tập hợp nhiều máy tính kết nối với nhau, có thể chia sẻ dữ liệu cho nhau".

Đối chiếu với quy định của Công ước Budapest, đối tượng tác động của nhiều tội phạm trong Công ước này là "hệ thống máy tính" (computer system). "Hệ thống máy tính" được hiểu là "một thiết bị hoặc một nhóm thiết bị kết nối với nhau, trên cơ sở của một chương trình một hoặc nhiều hơn các thiết bị đó thực hiện việc xử lý dữ liệu một cách tự động" (Điều 1(a)) [6]. Khái niệm này cũng được sử dụng trong Luật mẫu của Cộng đồng Phát triển Nam châu Phi và

[4] Ví dụ: cách hiểu về "tài sản" trong quy định của BLHS về đối tượng tác động của các tội xâm phạm sở hữu có tính chất chiếm đoạt không đồng nhất với khái niệm "tài sản" trong quy định của Bộ luật Dân sự.

Luật mẫu của Khối thịnh vượng (Para 7 Definition Part I Preliminary HIPPSA) [7, 8].

So sánh với quy định hiện hành của Việt Nam về "mạng máy tính", khái niệm "hệ thống máy tính" sử dụng trong Công ước có tính bao quát cao hơn, bởi vì "hệ thống máy tính" có thể hiểu là một máy tính hoặc một nhóm máy tính kết nối với nhau. Trên thực tế đã có hành vi của hacker xâm nhập vào một máy chủ để thực hiện các hành vi bất hợp pháp [9]. Nếu theo định nghĩa "mạng máy tính" của Việt Nam, hành vi tấn công này không thỏa mãn tội "Cản trở hoặc gây rối loạn hoạt động của mạng máy tính", bởi lẽ hành vi này không tấn công vào "mạng máy tính" mà chỉ là "một máy tính". Ngoài ra, nếu coi máy tính là "phương tiện điện tử" thì hành vi này phạm vào tội cản trở hoặc gây rối loạn hoạt động của phương tiện điện tử. Điều này không phản ánh đúng bản chất nguy hiểm của hành vi. Vì vậy, chúng tôi kiến nghị sửa thuật ngữ và khái niệm "mạng máy tính" của Việt Nam theo cách hiểu của Công ước để có cơ sở chuẩn xác trong việc truy cứu trách nhiệm hình sự đối với các hành vi phạm tội. Việc sửa đổi này cũng tạo ra sự tương thích giữa luật Việt Nam với các nước thành viên Công ước để thuận lợi trong hoạt động hợp tác quốc tế đấu tranh với loại tội phạm [10].

Ngoài ra, việc BLHS năm 2015 quy định đối tượng tác động của một số tội phạm chỉ là "mạng viễn thông, mạng máy tính, phương tiện điện tử" là chưa đầy đủ và cần được bổ sung thêm đối tượng tác động là dữ liệu điện tử. Ví dụ: xem xét hành vi nguy hiểm: nghe lén trên đường truyền (sniffing attack), sau đó sửa dữ liệu của gói tin và gửi cho nạn nhân hoặc chỉ can thiệp vào đường truyền để đánh cắp dữ liệu [11]. Hiện nay, với định nghĩa "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", tội "xâm nhập trái phép vào mạng viễn thông" không hàm chứa hành vi đã nêu và thể hiện hạn chế cần khắc phục. Do vậy, để bao quát cả trường hợp này, các Điều 286, 289 BLHS năm 2015 cần bổ sung đối tượng tác động là "dữ liệu điện tử". Do vậy, tên các điều luật này sửa lại như sau: "Tội phát tán chương trình tin học gây hại cho dữ liệu điện tử, hoạt động của hệ thống máy tính, mạng viễn thông, phương tiện điện tử"; "Tội xâm nhập trái phép hệ thống máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử của người khác". Đối với "Tội cản trở hoặc gây rối loạn cho hoạt động của mạng máy tính mạng viễn thông phương tiện điện tử", đối tượng tác động của tội này đã bao gồm dữ liệu điện tử (khoản 1 Điều 287 BLHS năm 2015). Tuy nhiên, tên gọi của tội phạm này chưa thể hiện đầy đủ đối tượng tác động của tội phạm, vì vậy chúng tôi kiến nghị sửa tên gọi của điều luật này như sau: "Tội cản trở hoặc gây rối loạn hoạt động của hệ thống máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử" [12][5].

## 3. Hạn chế trong quy định của Bộ luật Hình sự năm 2015 về dấu hiệu khách quan của các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông và kiến nghị

### *3.1. Hạn chế trong quy định của Bộ luật Hình sự năm 2015 về dấu hiệu khách quan của các tội phạm trực tiếp tác động đến dữ liệu cá nhân và kiến nghị*

Quy định của BLHS năm 2015 về dấu hiệu khách quan của các tội phạm trực tiếp xâm hại dữ liệu cá nhân có một số hạn chế sau đây.

*Một là*, về Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290). Căn cứ vào điểm k khoản 3 và điểm h khoản 4 Điều 2 Nghị định số 13/2023, tội này trực tiếp xâm hại đến dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm. Khi quy định về tội phạm này, nhà làm luật đã đưa ra yêu cầu về "loại trừ" trong định tội danh, cụ thể: hành vi sử dụng mạng máy tính, mạng

[5] Về vấn đề này, trong Luận án tiến sỹ, Tác giả Nguyễn Quý Khuyến đề xuất 2 phương án là tách tội danh hoặc hoàn thiện tên gọi.

viễn thông hoặc phương tiện điện tử để chiếm đoạt tài sản của người khác chỉ cấu thành tội này nếu không cấu thành Tội trộm cắp tài sản (Điều 173) hoặc Tội lừa đảo chiếm đoạt tài sản (Điều 174). Quy định nêu trên không hợp lý vì hành vi khách quan của tội phạm tại Điều 290 BLHS năm 2015 được thực hiện với phương thức đặc trưng sau:

- Sử dụng thông tin về tài khoản, thẻ ngân hàng của cơ quan, tổ chức, cá nhân để chiếm đoạt tài sản của chủ tài khoản, chủ thẻ hoặc thanh toán hàng hóa, dịch vụ. Người phạm tội sử dụng những cách thức khác nhau để có được những thông tin về tài khoản, thẻ ngân hàng của cơ quan, tổ chức, cá nhân, chẳng hạn như: dùng thủ đoạn lừa đảo thông qua các cuộc gọi, email giả mạo, tin nhắn giả mạo, trang web giả mạo để lấy các thông tin tài khoản, thẻ ngân hàng; mua hoặc có được thông tin từ người khác,… Sau khi người phạm tội có được dữ liệu nhạy cảm là thông tin về tài khoản, thông tin về thẻ ngân hàng, người phạm tội sử dụng trái phép các thông tin đó để chiếm đoạt tài sản của chủ tài khoản, chủ thể bằng cách rút tiền mặt, chuyển khoản tiền mặt hoặc thanh toán các chi phí khác.

- 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. Đây là trường hợp người phạm tội sau khi có được thông tin thẻ ngân hàng của người khác đã tạo ra thẻ ngân hàng giả dựa trên thông tin đó hoặc cố ý tàng trữ, mua bán, sử dụng, lưu hành thẻ ngân hàng giả có chứa thông tin của chủ thẻ thật nhằm mục đích chiếm đoạt tài sản.

- Truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản. Người phạm tội cố ý vượt qua cảnh báo, mã truy cập, tường lửa hoặc sử dụng mã truy cập của người khác mà không được sự cho phép của người đó để truy cập vào tài khoản không phải của mình nhằm mục đích chiếm đoạt tài sản của nạn nhân hoặc sử dụng chính tài khoản bị truy cập bất hợp pháp để lừa đảo chiếm đoạt tài sản của người khác.

- 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. Người phạm tội đưa ra các thông tin gian dối trong các lĩnh vực này thông qua mạng máy tính, mạng viễn thông, phương tiện điện tử làm nạn nhân tin tưởng và giao tài sản. Trong lĩnh vực thanh toán điện tử, thông thường người phạm tội đưa ra thông tin gian dối làm cho nạn nhân tin tưởng mà cung cấp các thông tin liên quan đến việc thanh toán 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.

- Thiết lập, cung cấp trái phép dịch vụ viễn thông, internet nhằm chiếm đoạt tài sản. Đây là hành vi thiết lập, cung cấp dịch vụ viễn thông, internet mà không được các cơ quan có thẩm quyền cho phép hoặc thực hiện không đúng với nội dung đã được cấp phép nhằm mục đích chiếm đoạt tài sản của người khác.

Như vậy, trong khi hành vi phạm tội quy định tại Điều 173 và 174 BLHS năm 2015 chỉ xâm phạm đến khách thể duy nhất là quyền sở hữu tài sản, hành vi sử dụng mạng máy tính, mạng viễn thông hoặc phương tiện điện tử để chiếm đoạt tài sản của người khác không chỉ xâm phạm đến quyền sở hữu tài sản mà còn xâm phạm đến sự an toàn trong lĩnh vực công nghệ thông tin, mạng viễn thông, trong đó có an toàn của dữ liệu cá nhân. Vì vậy, nhà làm luật quy định thành một tội mới và xếp vào chương "Các tội xâm phạm an toàn công cộng, trật tự công cộng". Với vị trí của tội này có thể thấy rằng nhà làm luật xác định khách thể chính của tội phạm là an toàn trong lĩnh vực công nghệ thông tin, mạng viễn thông. Tuy nhiên, chúng tôi cho rằng khách thể trực tiếp mà người phạm tội mong muốn xâm phạm là quan hệ sở hữu.

Việc quy định loại trừ như hiện nay dẫn đến "bối rối" và không thống nhất trong thực tiễn định tội danh đối với hành vi xâm phạm đến dữ liệu cá nhân của nạn nhân để chiếm đoạt tài sản qua mạng máy tính, mạng viễn thông, phương tiện điện tử. Điển hình là trường hợp sau: Bản án hình sự sơ thẩm số 89/2022/HS-ST ngày 08/9/2022 của Tòa án nhân dân huyện BB, tỉnh BD tuyên bố hành vi truy cập bất hợp pháp vào tài khoản cá nhân (tài khoản ví điện tử) của bị

hại, thực hiện chuyển tiền từ tài khoản ứng dụng MoMo sang tài khoản ngân hàng, chiếm đoạt tài sản của bị hại là hành vi "lén lút lấy tài sản của người khác" nên phạm vào tội "Trộm cắp tài sản" quy định tại Điều 173 BLHS năm 2015. Sau đó, Bản án này bị kháng nghị theo hướng sửa đổi thành tội "Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản" tại điểm b khoản 2 Điều 290 BLHS năm 2015. Bản án hình sự phúc thẩm số 05/2023/HS-PT ngày 10/01/2023 của Tòa án nhân dân tỉnh BD xác định hành vi phạm tội đủ yếu tố cấu thành tội "Sử dụng hệ thống máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản" [13]. Trong vụ án này, người phạm tội đã thực hiện hành vi "truy cập bất hợp pháp vào tài khoản cá nhân và chiếm đoạt tài sản của nạn nhân". Hành vi này không chỉ xâm phạm quyền sở hữu tài sản mà còn xâm phạm đến dữ liệu cá nhân của nạn nhân (thông tin tài khoản số của cá nhân). Do đó, hành vi cần phải bị truy cứu trách nhiệm hình sự theo quy định tại Điều 290 BLHS năm 2015. Tuy nhiên, khi sửa đổi toàn diện các quy định của BLHS năm 2015 về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông cần cân nhắc kỹ lưỡng về vị trí của tội này để bảo đảm xác định đúng khách thể trực tiếp, phản ánh đầy đủ nhất bản chất nguy hiểm của hành vi.

Ngoài ra, đối với hành vi lén lút sử dụng trái phép mật khẩu tài khoản của người khác chiếm đoạt tài sản, việc định tội danh còn chưa thống nhất, có tòa án xử lý về tội "Trộm cắp tài sản", có tòa án lại xử lý về tội "Sử dụng hệ thống máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản". Ví dụ, Bản án hình sự sơ thẩm số 24/2022/HS-ST ngày 21/07/2022 của Tòa án nhân dân Huyện TT, Tỉnh LA xác định hành vi đăng nhập trái phép tài E-mobile Banking trên điện thoại di động của nạn nhân chiếm đoạt tài sản phạm vào tội "Trộm cắp tài sản" [14]. Trong khi đó, Bản án hình sự sơ thẩm số 11/2023/HS-ST của Tòa án nhân dân Huyệt CH, Thành phố HP ngày 28/04/2023 xác định truy cập trái phép vào tài khoản ứng dụng ngân hàng trực tuyến trên điện thoại di động của nạn nhân chiếm đoạt tài sản phạm vào tội "sử dụng hệ thống máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản" [15].

Để phản ánh đúng bản chất nguy hiểm của hành vi phạm tội, đồng thời bảo đảm tính thống nhất trong định tội danh đối với hành vi xâm phạm đến dữ liệu cá nhân của nạn nhân để chiếm đoạt tài sản qua mạng máy tính, mạng viễn thông, phương tiện điện tử, cần thiết cấu trúc lại quy định của điều luật, bỏ dấu hiệu "nếu không thuộc một trong các trường hợp quy định tại Điều 173 và Điều 174 của Bộ luật này" tại khoản 1 Điều 290 BLHS năm 2015. Vì vậy, chúng tôi đề xuất sửa đổi nội dung Điều 290 BLHS năm 2015 như sau: "Người nào sử dụng hệ thống máy tính, mạng viễn thông hoặc phương tiện điện tử thực hiện một trong những hành vi sau đây thì bị phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:..."

Bên cạnh đó, quy định tại Điều 290 BLHS năm 2015 đề cập đến việc sử dụng thông tin về "tài khoản, thẻ ngân hàng"; "tài khoản" để chiếm đoạt tài sản. Theo chúng tôi, việc quy định như hiện nay là chưa đầy đủ. Về pháp luật, Nghị định số 101/2012/NĐ-CP ngày 22/11/2012 của Chính phủ về thanh toán không dùng tiền mặt (sửa đổi, bổ sung năm 2016, 2019) sử dụng thuật ngữ "tài khoản thanh toán" để đề cập đến các tải khoản khác không dùng tiền mặt (Điều 1 Văn bản hợp nhất số 10/VBHN-NHNN ngày 22/02/2019), ví dụ: tài khoản ví điện tử. Trong khi đó Luật An ninh mạng năm 2018 và Nghị định số 13/2023/NĐ-CP sử dụng thuật ngữ "tài khoản số" (điểm k khoản 3 Điều 2). Theo Luật An ninh mạng năm 2018, tài khoản số được hiểu là "thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng" (khoản 11 Điều 2). Thuật ngữ này bao quát cả tài khoản thanh toán, tài khoản ngân hàng. Trên thực tế, khi thực hiện hành vi chiếm đoạt tài sản, người phạm tội không chỉ sử dụng tài khoản ngân hàng, mà còn sử dụng tài khoản thanh toán hoặc tài khoản định danh khác [16]. Chính vì vậy, chúng tôi kiến nghị sửa đổi thuật ngữ "thông tin về tài khoản, thẻ ngân hàng" tại điểm a khoản 1 Điều 290 thành "dữ liệu về thẻ, tài khoản thanh toán"; thuật ngữ "tài khoản" tại

điểm c khoản 1 Điều 290 thành "tài khoản số". Mặt khác, thuật ngữ "tài khoản ngân hàng" tại Điều 291 cũng cần sửa đổi thành "tài khoản thanh toán".

*Hai là*, so sánh quy định pháp luật hình sự Việt Nam và một số điều ước quốc tế về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, có thể nhận thấy quy định pháp luật hình sự Việt Nam vẫn còn tồn tại hạn chế trong việc bảo vệ dữ liệu cá nhân của trẻ em, đặc biệt là những dữ liệu cá nhân nhạy cảm mang tính khiêu dâm. Hầu hết các điều ước quốc tế đều coi "tài liệu khiêu dâm trẻ em" là dữ liệu cá nhân và bắt buộc các quốc gia thành viên Công ước phải tội phạm hóa hành vi cố ý sản xuất, truyền tải, phát tán tài liệu khiêu dâm trẻ em qua hệ thống máy tính.

Theo Điều 9(1) Công ước Budapest, các quốc gia thành viên phải ban hành luật để quy định các hành vi sau đây là tội phạm: "Sản xuất tài liệu khiêu dâm trẻ em để phát tán qua hệ thống máy tính; Đề nghị cung cấp hoặc cung cấp tài liệu khiêu dâm trẻ em qua hệ thống máy tính; Phát tán hoặc truyền tải tài liệu khiêu dâm trẻ em qua hệ thống máy tính". Đối với các hành vi "Mua tài liệu khiêu dâm trẻ em cho mình hoặc cho người khác thông qua hệ thống máy tính; Sở hữu tài liệu khiêu dâm trẻ em trong hệ thống máy tính hoặc trong phương tiện lưu trữ dữ liệu máy tính" thì các quốc gia thành viên có quyền bảo lưu không áp dụng toàn bộ hay một phần các nội dung này [6]. Cũng theo quy định này, "tài liệu khiêu dâm trẻ em" bao gồm bất cứ tài liệu nào bằng hình ảnh mô tả: "Trẻ em thực hiện hành vi tình dục hoặc người giống trẻ em thực hiện hành vi tình dục hoặc hình ảnh thực tế diễn tả trẻ em thực hiện hành vi tình dục". "Trẻ em" theo quy định tại Điều 9(4) của Công ước này được hiểu là "người dưới 18 tuổi". Tuy nhiên, các quốc gia thành viên có thể giới hạn độ tuổi của trẻ em thấp hơn, nhưng phải bao gồm trẻ em dưới 16 tuổi [6].

Điều 29 của Công ước châu Phi cũng quy định các quốc gia thành viên phải tội phạm hóa các hành vi liên quan đến tài liệu khiêu dâm trẻ em, bao gồm: "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 tài liệu khiêu dâm trẻ em thông qua hệ thống máy tính; Sở hữu tài liệu 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" [1].

Việt Nam đã phê chuẩn Công ước về quyền trẻ em năm 1989 (Công ước về quyền trẻ em) vào ngày 20/2/1990 [17] và Nghị định thư không bắt buộc bổ sung Công ước quyền trẻ em về việc buôn bán trẻ em, mại dâm trẻ em và văn hóa khiêu dâm trẻ em năm 2000 (Nghị định thư) vào ngày 20/12/2001 [18]. Các văn bản này yêu cầu các quốc gia thành viên việc bảo vệ trẻ em nói chung và bảo vệ trẻ em khỏi các hành vi xâm hại tình dục nói riêng. Theo quy định tại Điều 34 Công ước về quyền trẻ em thì: "Các quốc gia thành viên cam kết bảo vệ trẻ em khỏi mọi hình thức bóc lột và lạm dụng tình dục. Vì những mục đích này, các Quốc gia thành viên đặc biệt phải thực hiện tất cả các biện pháp thích hợp để ngăn chặn: a) Việc xúi giục hoặc ép buộc trẻ em tham gia vào bất kỳ hoạt động tình dục bất hợp pháp; b) Việc sử dụng có mục đích bóc lột trẻ em trong hoạt động mại dâm hoặc các hành vi tình dục bất hợp pháp khác; c) Việc sử dụng có mục đích bóc lột trẻ em trong các buổi biểu diễn và tài liệu khiêu dâm". Bên cạnh đó, theo quy định tại Điều 1 Nghị định thư, "các quốc gia thành viên phải nghiêm cấm việc buôn bán trẻ em, mại dâm trẻ em và khiêu dâm trẻ em theo quy định của Nghị định thư này". Đồng thời, Điều 3 Nghị định thư quy định nghĩa vụ của các quốc gia thành viên Nghị định thư phải tội phạm hóa trong pháp luật hình sự quốc gia đối với hành vi "sản xuất, phân phối, phổ biến, nhập khẩu, xuất khẩu, chào bán hoặc sở hữu nội dung khiêu dâm trẻ em,…".

Quy định của BLHS năm 2015 và một số văn bản hướng dẫn thi hành đã điều chỉnh một số hành vi xâm hại tình dục trẻ em, bao gồm: Hiếp dâm người dưới 16 tuổi (Điều 142), Cưỡng dâm người từ đủ 13 tuổi đến dưới 16 tuổi (Điều 144), Giao cấu hoặc thực hiện hành vi quan hệ tình dục khác với người từ đủ 13 tuổi đến dưới 16 tuổi (Điều 145), Dâm ô đối với người dưới 16 tuổi (Điều 146), Sử dụng người dưới 16 tuổi vào mục

đích khiêu dâm (Điều 147) Như vậy, quy định về trẻ em trong BLHS năm 2015 là "người dưới 16 tuổi", đồng bộ với Luật Trẻ em năm 2016. Tuy nhiên, có thể nhận thấy BLHS Việt Nam năm 2015 vẫn chưa tội phạm hóa cụ thể hành vi "phổ biến tài liệu khiêu dâm trẻ em qua hệ thống máy tính, mạng viễn thông hay phương tiện điện tử", ảnh hưởng rất lớn đến việc bảo vệ dữ liệu cá nhân của trẻ em cũng như không đáp ứng các nghĩa vụ được đặt ra trong các Điều ước quốc tế mà Việt Nam là thành viên. Trong trường hợp một người thực hiện hành vi này thì chỉ có thể áp dụng Điều 326 BLHS năm 2015 về Tội truyền bá văn hóa phẩm đồi trụy để truy cứu trách nhiệm hình sự đối với họ dù hành vi phổ biến tài liệu khiêu dâm trẻ em qua mạng máy tính, mạng viễn thông hay phương tiện điện tử có tính chất nguy hiểm cho xã hội cao hơn do xâm phạm trực tiếp đến danh dự, nhân phẩm của trẻ em.

Do đó, nhằm phù hợp với các chuẩn mực quốc tế về truy cứu trách nhiệm hình sự đối với các hành vi về tội phạm mạng liên quan đến khiêu dâm trẻ em cũng như có thêm cơ sở pháp lý bảo vệ quyền lợi trẻ em một cách tốt nhất, cần bổ sung tội danh "Phổ biến tài liệu khiêu dâm trẻ em qua mạng máy tính, mạng viễn thông hay phương tiện điện tử" trong BLHS năm2015. Bên cạnh đó, nhằm đảm bảo đồng bộ với Luật Trẻ em năm 2016 và các tội danh xâm hại tình dục trẻ em đang quy định trong BLHS năm 2015, đối tượng tác động của tội phạm "trẻ em" trong trường hợp này là "người dưới 16 tuổi. Từ những lập luận trên, kiến nghị bổ sung tội danh "Phổ biến tài liệu khiêu dâm người dưới 16 tuổi qua mạng máy tính, mạng viễn thông, phương tiện điện tử" với nội dung cụ thể như sau:

"Người nào làm ra, sao chép, lưu hành, vận chuyển, mua bán, tàng trữ tài liệu có nội dung khiêu dâm của người dưới 16 tuổi qua hệ thống máy tính, mạng viễn thông hay phương tiện điện tử thì bị phạt tù từ 06 tháng đến 03 năm".

*3.2. Hạn chế trong quy định của Bộ luật Hình sự năm 2015 về dấu hiệu khách quan của các tội phạm gián tiếp tác động đến dữ liệu cá nhân và kiến nghị*

Trong các quy định của BLHS năm 2015 về các tội gián tiếp tác động đến dữ liệu cá nhân cần lưu ý đến quy định về 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 này được xác định 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 máy tính, thiết bị viễn thông, thiết bị số.[6] Chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử mà người phạm tội sử dụng để thực hiện tội phạm thường là các loại virus máy tính hay các phần mềm độc hại như worms, trojan horses, ransomware, spyware, malvertising, rogue software, wiper, keyloggers,… [19] Khi thực hiện hành vi này, người phạm tội có thể sao chép được dữ liệu điện tử hoặc làm biến dạng hay xóa bỏ dữ liệu điện tử của người sử dụng được lưu trữ trên máy tính, thiết bị viễn thông hoặc thiết bị số.

Qua số liệu thống kê công tác xét xử của Tòa án, hành vi này hiếm khi bị xử lý hình sự dù trên thực tế đã gây nhiều thiệt hại cho người khác[7]. Có nhiều nguyên nhân dẫn đến hạn chế này, trong đó nguyên nhân chủ yếu xuất phát từ khó khăn trong việc chứng minh hậu quả và thiệt hại cụ thể do hành vi phạm tội được quy định tại Điều 286 BLHS gây ra. Mức độ thiệt hại cụ thể của hành vi phát tán chương trình tin học có tính năng gây hại trên mạng máy tính, mạng viễn thông hay phương tiện điện tử rất khó xác định vì một chương trình tin học có tính năng gây hại có thể lan truyền đến hàng trăm, hàng ngàn phương tiện điện tử khác nhau và một phương

[6] Khoản 1 Điều 6 Thông tư liên tịch số 10/2012.

[7] Từ năm 2016 đến năm 2022, tổng số vụ án được Tòa án đưa ra xét xử là 03 vụ (Căn cứ số liệu thống kê công tác xét xử của Tòa án từ năm 2016 đến năm 2022).

tiện điện tử bị thiệt hại có thể là do tác động của nhiều loại chương trình tin học có tính năng gây hại. Vì vậy, để xác định được mức độ thiệt hại do hành vi phát tán chương trình tin học có tính năng gây hại gây ra trong từng trường hợp cụ thể là điều rất khó thực hiện trong khi Điều 286 BLHS đòi hỏi phải chứng minh được hành vi phát tán "gây thiệt hại từ 50.000.000 đồng đến dưới 300.000.000 đồng" hoặc người thực hiện hành vi phát tán "thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng" từ việc thực hiện hành vi thì mới cấu thành tội phạm này.

Bên cạnh đó, khoản 1 Điều 286 BLHS quy định dấu hiệu: "Làm lây nhiễm từ 50 phương tiện điện tử đến dưới 200 phương tiện điện tử hoặc hệ thống thông tin có từ 50 người sử dụng đến dưới 200 người sử dụng" là một trong những dấu hiệu cấu thành tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. Việc quy định như trên là không hợp lý vì với sự phát triển của mạng máy tính, mạng viễn thông hiện nay, khi một chương trình tin học gây hại được phát tán trên mạng thì tốc độ lây nhiễm diễn ra rất nhanh với số lượng phương tiện điện tử bị lây nhiễm rất lớn. Chẳng hạn, chương trình virus tin học Slammer sau khi được phát tán đã làm lây nhiễm đến 75 nghìn máy tính chỉ trong thời gian 10 phút hay chương trình độc hại Storm Worm khiến hơn 10 triệu máy tính bị lây nhiễm [20]. Do đó, theo quan điểm của các tác giả thì việc quy định số lượng phương tiện điện tử bị lây nhiễm hoặc hệ thống thông tin bị ảnh hưởng chỉ từ 50 phương tiện hoặc từ 50 người sử dụng là dấu hiệu định tội thật sự không cần thiết vì khi một chương trình tin học gây hại được phát tán trên mạng máy tính, mạng viễn thông thì số lượng phương tiện điện tử bị lây nhiễm hoặc số người bị ảnh hưởng sẽ lớn hơn rất nhiều.

Vì vậy, chúng tôi đề xuất sửa đổi quy định tại Điều 286 BLHS năm 2015 theo hướng bỏ dấu hiệu hậu quả (thiệt hại về tài sản), dấu hiệu thu lợi bất chính và quy mô lây nhiễm. Đối với tội phạm này, rất khó xác định mức độ thiệt hại cụ thể trong từng trường hợp nên quy định pháp luật hình sự của một số quốc gia trên thế giới, trong đó có Cộng hòa Pháp, không quy định về việc chứng minh hậu quả của tội phạm. Do đó, chỉ nên quy định tội phạm tại Điều 286 BLHS năm 2015 là tội phạm có cấu thành hình thức, ngay khi người phạm tội thực hiện hành vi khách quan thì tội phạm được coi là hoàn thành. Khoản 1 Điều 286 BLHS năm 2015 sau khi được sửa đổi sẽ có nội dung như sau: "Người nào cố ý phát tán chương trình tin học gây hại cho hệ thống máy tính, mạng viễn thông, phương tiện điện tử 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".

## 4. Kết luận và kiến nghị

Nhìn từ góc độ bảo vệ dữ liệu cá nhân, quy định của BLHS năm 2015 vẫn còn nhiều hạn chế và chưa thống nhất với các quy định mới về bảo vệ dữ liệu cá nhân và các quy định về an ninh mạng. Ngoài ra, so sánh với quy định của một số điều ước quốc tế về tội phạm mạng (cyber crime), quy định của BLHS năm 2015 bộc lộ những hạn chế nhất định về xác định đối tượng tác động và dấu hiệu khách quan của tội phạm. Để khắc phục các hạn chế đã nêu, Bài viết đưa ra một số kiến nghị cụ thể sau:

*Thứ nhất*, sửa đổi một số cụm từ, thuật ngữ để bảo đảm tính thống nhất với Nghị định số 13/2023/NĐ-CP của Chính phủ cũng như các văn bản pháp luật có liên quan. Các cụm từ "thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân" tại điểm b khoản 1 Điều 288, "thông tin mạng máy tính" trong tên gọi của Điều 288, "thông tin về tài khoản, thẻ ngân hàng" tại điểm a khoản 1 Điều 290, "tài khoản" tại điểm c khoản 1 Điều 290, "tài khoản ngân hàng" tại Điều 291 cần sửa lại tương ứng là "dữ liệu hợp pháp của cơ quan, tổ chức, cá nhân", "dữ liệu điện tử", "dữ liệu về thẻ, tài khoản thanh toán", "tài khoản số" và "tài khoản thanh toán".

*Thứ hai*, bổ sung đối tượng tác động là "dữ liệu điện tử" vào các tội quy định tại Điều 286, 289 BLHS năm 2015, không sử dụng cụm từ "mạng máy tính" mà sử dụng cụm từ "hệ thống máy tính" để bảo đảm tính chính xác của thuật ngữ, đồng thời tương đồng với thuật ngữ dùng

phổ biến trong các điều ước quốc tế đấu tranh với tội phạm mạng. Tên các điều luật này sửa lại như sau: "Tội phát tán chương trình tin học gây hại cho dữ liệu điện tử, hoạt động của hệ thống máy tính, mạng viễn thông, phương tiện điện tử"; "Tội xâm nhập trái phép hệ thống máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử của người khác".

*Thứ ba*, xóa bỏ dấu hiệu "nếu không thuộc một trong các trường hợp quy định tại Điều 173 và Điều 174 của Bộ luật này" trong cấu thành cơ bản của Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản tại khoản 1 Điều 290 BLHS năm 2015 nhằm đảm bảo tính thống nhất cho việc định tội danh, đồng thời phản ánh đúng bản chất nguy hiểm của hành vi phạm tội.

*Thứ tư*, bổ sung "Tội phổ biến tài liệu khiêu dâm người dưới 16 tuổi qua mạng máy tính, mạng viễn thông, phương tiện điện tử" nhằm bảo vệ dữ liệu cá nhân của trẻ em nói riêng và bảo vệ danh dự, nhân phẩm của trẻ em nói chung. Việc bổ sung tội danh này cũng giúp đảm bảo sự phù hợp giữa quy định của BLHS Việt Nam với các chuẩn mực quốc tế về truy cứu trách nhiệm hình sự đối với các hành vi liên quan đến tuyên truyền, phổ biến các tài liệu khiêu dâm trẻ em cũng như có cơ sở pháp lý bảo vệ quyền lợi trẻ em một cách tốt nhất.

*Thứ năm*, sửa đổi quy định tại khoản 1 Điều 286 BLHS năm 2015 về Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử theo hướng bỏ đi dấu hiệu hậu quả (thiệt hại về tài sản), bỏ dấu hiệu thu lợi bất chính và số phương tiện bị lây nhiễm là dấu hiệu bắt buộc nhằm đảm bảo cho việc áp dụng điều luật được khả thi trên thực tế. Khoản 1 Điều 286 BLHS năm 2015 sau khi sửa đổi sẽ có nội dung: "Người nào cố ý phát tán chương trình tin học gây hại cho hệ thống máy tính, mạng viễn thông, phương tiện điện tử 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".

## Tài liệu tham khảo


[1] African Union Convention on Cyber Security and Personal Data, 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed on: March 15th, 2023).

[2] Văn kiện Đại hội XII của Đảng (năm 2016).

[3] Group IB, High-Tech Crime Trend 2017, Global Cyber Security Company, pp. 10.

[4] L. T. Tam, P. T. T. Thao, High-Tech Crime Against the Vietnamese Banking Industry in the Context of the Fourth Industrial Revolution: Current Situation and some Policy Recommendations, Banking Science and Education Journal, Issue 192, May 2018, pp. 2-3 (in Vietnamese).

[5] N. N. Hoa, The Discrete Content and Harmonization of the Criminal Code in the Vietnamese Legal System, Journal on State and Law, No 11/2015, 2015, pp. 35-42 (in Vietnamese).

[6] Council of Europe, Convention on Cybercrime, 2001, https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf (accessed on: March 15th, 2023).

[7] Harmonization of Information and Communication Technologies Policies in Sub-Saharan Africa of the Southern African Community, Model Law on Computer and Computer-related Crime, 2013, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf (accessed on: March 12th, 2023).

[8] Office of Civil and Criminal Justice Reform, Model Law on Computer and Computer-related Crime, 2017, https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf, (accessed on: March 15th, 2023).

[9] K. An, The FBI's Server Was Hacked, Sending Emails to More Than 100,000 People, Youth Newspaper, 2021, https://thanhnien.vn/may-chu-cua-fbi-bi-tin-tac-tan-cong-gui-email-den-hon-100-000-nguoi-1851401128.htm (accessed on: April 12th, 2023) (in Vietnamese).

[10] Đ. Q. Hoang, Harmonization of Laws in the Fight Against Cybercrimes, Journal of Legal Studies, No 08/2020, 2020, pp. 30-40 (in Vietnamese).

[11] Đ. Quang, Sending Fraudulent SMS Messages Using the Bank's Names, Finance Journal, 2022 https://tapchitaichinh.vn/chieu-thuc-phat-tan-tin-nhan-sms-mao-danh-ngan-hang.html (accessed on: April 15th, 2023) (in Vietnamese).

[12] N. Q. Khuyen, Crimes in the Area of Information Technology, Telecommunication Network, Ph.D Thesis, Hanoi Law University, Hanoi, 2021 (in Vietnamese).

[13] Official Website of the Supreme People's Court, Appeal Judgment No. 05/2023/HS-PT Dated January 15th, 2023 of the Provincial People's Court of BD Province, 2023, https://congbobanan.toaan.gov.vn/2ta1114814t1cvn/chi-tiet-ban-an (in Vietnamese) (accessed on: April 15th, 2023).

[14] Bản án: số 24 ngày 21/07/2022 của TAND huyện Thủ Thừa, tỉnh Long An Phạm Thị Thanh H (trộm cắp tài sản) - phạm tội trộm cắp tài sản (điều 173 Luật sửa đổi, bổ sung một số điều của BLHS năm 2015) - Phạm Thị Thanh H (trộm cắp tài sản) Tội trộm cắp tài sản (toaan.gov.vn) (in Vietnamese) (accessed on: November 29th, 2023).

[15] Official Website of the Supreme People's Court, Fist-instance Judgment No. 11/2023/HS-ST Dated April 28th, 2023 of the CB District People's Court, HP City, 2023, https://congbobanan.toaan.gov.vn/0tat1cvn/ban-an-quyet-dinh (in Vietnamese) (accessed on: November 30th, 2023).

[16] N. Q. Khuyen, Using Computer Network, Telecommunication Network to Appropriate Property, Procuration Journal No. 9, 2020, pp. 37-42 (in Vietnamese).

[17] United Nations Convention on the Rights of the Child, 1989, https://www.unicef.org/vietnam/vi/c%C3%B4ng-%C6%B0%E1%BB%9Bc-li%C3%AAn-h%E1%BB%A3p-qu%E1%BB%91c-v%E1%BB%81-quy%E1%BB%81n-tr%E1%BA%BB-em (in Vietnamese) (accessed on: March 15th, 2023).

[18] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, 2000, https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child (accessed on: March 15th, 2023).

[19] R. Tahir, A Study on Malware and Malware Detection Techniques, International Journal of Education and Management Engineering No. 2018-8(2), 2018, pp. 20-30, Doi: 10.5815/ijeme.2018.02.03 (accessed on: March 15th, 2023).

[20] B. Nga, The Most Dangerous Computer Viruses Ever, Network Administration, 2021, https://quantrimang.com/cong-nghe/10-virus-may-tinh-nguy-hiem-nhat-tu-truoc-toi-nay-69255 (in Vietnamese) (accessed on: April 15th, 2023).