PHÁP LUẬT QUỐC TẾ VỀ TRÁCH NHIỆM HÌNH SỰ ĐỐI VỚI TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN, MẠNG VIỄN THÔNG

NGUYỄN VĂN THẮNG*

Pháp luật quốc tế về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là vấn đề quan trọng, cần được nghiên cứu trong việc hoàn thiện chế định về trách nhiệm hình sự đối với tội phạm này ở Việt Nam. Bài viết phân tích những nội dung trọng tâm của pháp luật quốc tế về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Từ đó, xác định những kinh nghiệm hiệu quả, phù hợp trong quá trình tham khảo hoàn thiện pháp luật ở Việt Nam xoay quanh vấn đề này.

Từ khóa: *Pháp luật quốc tế; trách nhiệm hình sự; tội phạm; công nghệ thông tin; mạng viễn thông.*

International law on criminal liability for crimes in the field of information technology and telecommunications networks is an important issue that needs to be studied in perfecting regulations on criminal liability for these crimes in Vietnam. The article analyzes the key contents of international law on criminal liability for crimes in the field of information technology and telecommunications networks. From there, identify effective and appropriate experiences in the process of consulting to improve the law in Vietnam surrounding this issue.

Keywords: *International law, criminal liability, crime, information technology, telecommunications networks.*

NGÀY NHẬN: 09/4/2024 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 11/5/2024 NGÀY DUYỆT: 17/6/2024

DOI: https://doi.org/10.59394/qlnn.341.2024.890

1. Đặt vấn đề

Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông cũng như trách nhiệm hình sự đặt ra đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là những đối tượng rất quan trọng được điều chỉnh bởi pháp luật quốc tế và luật pháp Việt Nam. Trên phương diện pháp luật quốc tế, bài viết phân tích một số nội dung chủ yếu của các công ước quốc tế và *Bộ luật Hình sự* của một số quốc gia tiêu biểu, như: Hoa Kỳ, Canada, Nga, Trung Quốc về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Từ đó, đưa ra những kinh nghiệm, nội dung phù hợp để nghiên cứu, vận dụng ở nước ta, góp phần nâng cao hiệu quả đấu tranh phòng, chống

* *ThS, Trường Đại học Kỹ thuật - Hậu cần Công an nhân dân*

loại tội phạm này cả ở trong nước và trên thế giới bởi "tính quốc tế" đặc thù của tội phạm công nghệ thông tin, mạng viễn thông.

2. Những nội dung chủ yếu trong quy định của pháp luật quốc tế về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông

2.1. Trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong một số công ước quốc tế

Thứ nhất, Công ước của Hội đồng châu Âu về tội phạm mạng năm 2001 (còn gọi là Công ước Budapest năm 2001) - đây là công ước đầu tiên trên thế giới điều chỉnh hành vi của tội phạm mạng, chia thành 4 nhóm: (1) Những tội phạm chống lại tính bí mật, toàn vẹn và sẵn có của dữ liệu máy tính và hệ thống máy tính; (2) Những tội phạm liên quan đến máy tính; (3) Những tội phạm liên quan đến nội dung; (4) Những tội xâm phạm quyền tác giả và các quyền liên quan.

Tại khoản 1 Điều 12 Công ước thì chủ thể của tội phạm mạng phải chịu trách nhiệm hình sự không chỉ có cá nhân mà còn có cả pháp nhân, rộng hơn cả pháp nhân thương mại ở nước ta, nếu đáp ứng các điều kiện về: hành vi phạm tội do cá nhân thực hiện vì lợi ích của pháp nhân; cá nhân phạm tội là đại diện hoặc là nhân viên của pháp nhân và nắm vị trí lãnh đạo dựa trên cơ sở: có quyền đại diện cho pháp nhân; có thẩm quyền ra quyết định nhân danh pháp nhân; có thẩm quyền thực hiện việc kiểm soát trong nội bộ pháp nhân. Đặc biệt, tại Điều 13 Công ước Budapest xác định "Biện pháp chế tài và biện pháp khác"[1] đối với tội phạm này, theo đó, các quốc gia thành viên phải ban hành luật và các biện pháp cần thiết khác để bảo đảm rằng, các tội phạm được nêu trong Công ước được trừng trị bởi hệ thống chế tài tương xứng, hiệu quả và có tác dụng răn đe, bao gồm cả việc tước quyền tự do cá nhân. Đối với pháp nhân cũng phải chịu trách nhiệm phù hợp và bị áp dụng các biện pháp chế tài hình sự hoặc phi hình sự mang tính tương xứng, hiệu quả và có tính răn đe hoặc các biện pháp khác, bao gồm cả chế tài phạt tiền.

Thứ hai, Công ước Ả Rập về phòng, chống tội phạm công nghệ thông tin năm 2010. Công ước Ả Rập năm 2010 có sự khác biệt về tên gọi "tội phạm công nghệ thông tin", không giống tên gọi "tội phạm mạng" trong Công ước Budapest năm 2001 nêu trên và không có sự phân chia nhóm mà quy định theo cách liệt kê, với 13 loại tội phạm cụ thể, liên quan. Về trách nhiệm hình sự, Điều 21 Công ước Ả Rập yêu cầu các quốc gia thành viên phải cam kết về việc tăng nặng trách nhiệm hình sự đối với trường hợp thực hiện tội phạm truyền thống nhưng người phạm tội sử dụng công nghệ thông tin để thực hiện tội phạm. Bên cạnh đó, Điều 20 của Công ước này quy định các quốc gia thành viên phải cam kết việc quy định trách nhiệm hình sự đối với pháp nhân trong trường hợp hành vi phạm tội do người đại diện của pháp nhân thực hiện nhân danh pháp nhân hoặc vì lợi ích pháp nhân và việc truy cứu trách nhiệm hình sự đối với pháp nhân cũng không làm ảnh hưởng đến việc áp dụng hình phạt đối với cá nhân thực hiện hành vi phạm tội[2].

Thứ ba, Công ước của Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân năm 2014, từ đó nhằm mục đích thiết lập khung pháp lý cơ bản về an ninh mạng và bảo vệ dữ liệu cá nhân, trực tiếp góp phần chống lại tội phạm công nghệ thông tin. Theo Công ước này, tội phạm trong lĩnh vực công nghệ thông tin được phân thành 4 nhóm: (1) Các tội phạm tấn công hệ thống máy tính; (2) Các tội xâm phạm dữ liệu máy tính; (3) Các tội phạm liên quan đến nội dung; (4) Các tội xâm phạm tài sản có liên quan đến công nghệ thông tin và truyền thông. Về vấn đề trách nhiệm hình sự, khoản 1 Điều 30 Công ước châu Phi yêu cầu các quốc gia thành viên phải hình sự hóa các hành vi xâm phạm đến quyền sở hữu tài sản có liên quan đến dữ liệu máy tính, bao gồm: trộm cắp, lừa đảo, tiêu thụ tài sản trộm cắp, lạm dụng tín nhiệm, cưỡng đoạt tài sản. Đối với tình tiết sử dụng công

nghệ thông tin và truyền thông để thực hiện hành vi phạm tội nêu trên và hành vi khủng bố, rửa tiền, các quốc gia phải coi đó là tình tiết tăng nặng trách nhiệm hình sự. Bên cạnh đó, khoản 2 Điều 30 Công ước này thì pháp nhân phải chịu trách nhiệm hình sự về những hành vi phạm tội được quy định nếu hành vi đó do đại diện của pháp nhân thực hiện nhân danh pháp nhân[3].

Như vậy, có thể thấy điểm chung của cả 3 công ước nêu trên là đều quy định về trách nhiệm hình sự của pháp nhân đối với tội phạm công nghệ thông tin khi hành vi phạm tội do cá nhân thực hiện vì lợi ích của pháp nhân hoặc nhân danh pháp nhân và cá nhân phạm tội là người đại diện của pháp nhân đó. Việc truy cứu trách nhiệm hình sự đối với pháp nhân sẽ không loại trừ trách nhiệm hình sự của cá nhân trực tiếp thực hiện tội phạm trong lĩnh vực này.

2.2. Trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo pháp luật của một số quốc gia

(1) Trong pháp luật của Hoa Kỳ: tại *Bộ luật số 18* thuộc *Bộ tổng luật Hoa Kỳ* (viết tắt *18 USC*) không có điều khoản riêng quy định về chủ thể của tội phạm nói chung cũng như các tội liên quan đến công nghệ thông tin, viễn thông nói riêng[4]. Nhiều tài liệu về *Luật Hình sự* của Hoa Kỳ cũng đề cập rằng chủ thể của tội phạm có thể là thể nhân, tổ chức hoặc cả hai[5]. Khi cân nhắc quyết định truy cứu trách nhiệm hình sự đối với tổ chức, công tố viên phải tuân thủ các nguyên tắc về truy cứu đối với tổ chức[6].

Ngoài các luật chung của Liên bang, pháp luật Hoa Kỳ còn tạo điều kiện cho từng tiểu bang thông qua những sắc luật riêng để phòng, chống tội phạm công nghệ thông tin, mạng viễn thông trên cơ sở phù hợp với tình hình của mỗi bang. Ví dụ, New York nghiêm cấm việc sử dụng các công cụ, thiết bị công nghệ cao với mục đích truy cập vào các tài liệu trong máy tính một cách bất hợp pháp (xâm phạm máy tính), với hành vi vi phạm trên có thể áp dụng hình phạt lên đến 4 năm tù hoặc các hình phạt khác lên đến 15 năm tù tùy theo mức độ vi phạm[7].

Về dấu hiệu định khung tăng nặng trách nhiệm hình sự theo quy định *Luật Hình sự Hoa Kỳ* thì "tiền án" cũng được là một dấu hiệu. Tuy nhiên, đối với trị giá tài sản liên quan đến hành vi phạm tội thì pháp luật Hoa Kỳ còn đưa thêm một dấu hiệu để xác định đó là giới hạn thời gian. Điểm lưu ý tiếp theo là hình phạt, cụ thể: hình phạt áp dụng đối với thể nhân là hình phạt tiền hoặc hình phạt tù (gồm tù có thời hạn hoặc tù chung thân) hoặc cả hai. Đối với từng tội phạm cụ thể, *Luật Hình sự Hoa Kỳ* không quy định mức phạt tù tối thiểu mà chỉ giới hạn mức phạt tối đa, do vậy, *18 USC* cũng chỉ quy định hình phạt tối đa được áp dụng đối với mỗi loại tội phạm và mỗi trường hợp phạm tội liên quan đến công nghệ thông tin, mạng viễn thông. Theo *Luật Hình sự Hoa Kỳ*, hình phạt cao nhất đối với tội phạm này là tù chung thân đối với một số trường hợp hành vi phạm tội xâm hại dữ liệu liên quan đến an ninh, quốc phòng hoặc vị thế chính trị hoặc quan hệ ngoại giao của Hoa Kỳ với các nước khác.

(2) Trong pháp luật của Canada. Bộ luật Hình sự của Canada có 28 phần, trong đó có 10 phần quy định về tội phạm cụ thể, nhưng không có phần hay mục nào quy định riêng về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông[8]. Các hành vi phạm tội liên quan đến lĩnh vực này được quy định đan xen trong các phần liên quan. Theo *Luật Hình sự Canada*, trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông được đặt ra đối với cả thể nhân và tổ chức. Trong đó, đối với thể nhân, độ tuổi chịu trách nhiệm hình sự là từ 12 tuổi (nhỏ hơn so với quy định của pháp luật hình sự Việt Nam) và quy định rõ ràng về suy đoán đương nhiên có trách nhiệm hình sự và "Việc người phạm tội thiếu hiểu biết pháp luật không phải là lý do được chấp thuận để họ thực hiện tội phạm" (s19). *Bộ luật Hình sự Canada* phân loại 2 trường hợp mà tổ chức phải chịu trách

nhiệm hình sự về tội phạm với lỗi cẩu thả và lỗi không phải do cẩu thả. Tội phạm liên quan đến công nghệ thông tin trong *Bộ luật Hình sự Canada* đều có lỗi cố ý (nghĩa là không có lỗi vô ý do cẩu thả). Bộ luật này không quy định dấu hiệu định khung tăng nặng riêng đối với các tội phạm liên quan đến công nghệ thông tin, mạng viễn thông.

Về hình phạt đối với tội phạm này trong *Bộ luật Hình sự Canada*, gồm: phạt tiền, phạt tù có thời hạn và phạt tù chung thân, được phân hóa theo tội phạm với 3 loại là: tội phạm ít nghiêm trọng, tội phạm nghiêm trọng và tội phạm hỗn hợp. Khi áp dụng hình phạt tiền, Tòa án phải nêu rõ số tiền phạt, cách thức nộp tiền phạt, thời hạn nộp phạt, những loại tài sản nào được chấp nhận cho việc nộp phạt. Điểm rất đặc biệt là Canada cho phép quy đổi từ phạt tiền sang phạt tù nếu người phạm tội vi phạm nghĩa vụ nộp phạt (nghĩa là chưa nộp đầy đủ tiền phạt theo thời hạn quy định). Tòa án có thể áp dụng đồng thời hình phạt tiền và hình phạt tù đối với người phạm tội. Nếu phạm tội ít nghiêm trọng có thể bị áp dụng hình phạt tiền không quá 5.000 USD hoặc hình phạt tù dưới 2 năm hoặc cả hai. Nếu phạm tội nghiêm trọng, hình phạt tù phổ biến là không quá 10 năm. Quy định đó chứng minh quan điểm của nhà làm luật Canada xác định tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là những tội nghiêm trọng ở mức trung bình. Đối với tổ chức, *Bộ luật Hình sự Canada* chỉ quy định hình phạt tiền.

(3) Trong pháp luật của Nga. Bộ luật Hình sự Liên bang Nga xác định đối với các tội phạm trong lĩnh vực này là tội phạm trong lĩnh vực thông tin, máy tính. Trước hết, *Bộ luật Hình sự Liên bang Nga* xác định chủ thể của các tội phạm trong lĩnh vực thông tin, máy tính là cá nhân và hầu hết là chủ thể thường. Duy chỉ có tội phạm được quy định tại Điều 274.2 (Tội vi phạm các quy tắc quản lý tập trung các phương tiện kỹ thuật để chống lại các mối đe dọa đối với sự ổn định, an ninh và toàn vẹn hoạt động của mạng thông tin và viễn thông "internet" và mạng truyền thông công cộng trên lãnh thổ Liên bang) là chủ thể đặc biệt - người có chức vụ thực hiện.

Nghiên cứu các quy định của *Bộ luật Hình sự Liên bang Nga* về chế tài áp dụng đối với các tội phạm trong lĩnh vực thông tin, máy tính cho thấy, Nga sử dụng nhiều hình phạt chính không tước tự do, như: phạt tiền, lao động cải tạo, hạn chế tự do, cưỡng bức lao động. Bên cạnh đó, tất cả các tội phạm trong lĩnh vực thông tin, máy tính đều dự liệu đến việc áp dụng hình phạt tù mà mức tối đa có thể là 3 năm tù, 5 năm tù, thậm chí đến 8 năm tù. *Bộ luật Hình sự Nga* còn quy định các hình phạt bổ sung như phạt tiền, hạn chế tự do, cấm đảm nhiệm chức vụ, một số công việc nhất định. Các quy định này chứng tỏ Nga có sự phân hóa rất rõ ràng trong chính sách hình sự đối với các trường hợp phạm tội cụ thể[9].

(4) Trong pháp luật của Trung Quốc. Bộ luật Hình sự của Trung Quốc không quy định tên riêng cho các tội phạm liên quan đến mạng máy tính, mạng viễn thông mà quy định tại mục 1, Chương VI. Theo đó, các tội phạm liên quan đến mạng máy tính, mạng viễn thông có thể do cá nhân hoặc pháp nhân thực hiện. Điều 30, *Bộ luật Hình sự Trung Quốc* quy định: công ty, doanh nghiệp, cơ quan, tổ chức công cộng thực hiện hành vi nguy hại cho xã hội mà hành vi đó được quy định là tội phạm thì phải chịu trách nhiệm hình sự, nghĩa là không giới hạn phạm vi pháp nhân và giới hạn nhóm hay loại tội phạm mà pháp nhân phải chịu trách nhiệm hình sự. Quy định về tội phạm liên quan đến mạng máy tính, mạng viễn thông tại Điều 285, 286, 286-1, 287-1, 287-2 *Bộ luật Hình sự* chỉ rõ: trường hợp đơn vị phạm tội quy định tại khoản 1 thì đơn vị đó bị phạt tiền, người phụ trách trực tiếp và những người chịu trách nhiệm trực tiếp khác bị xử phạt theo quy định tại khoản 1.

Về hình phạt quy định đối với các tội phạm liên quan đến mạng máy tính, mạng viễn thông theo quy định của *Bộ luật Hình sự* Trung Quốc chủ yếu là hình phạt tù có thời

hạn, giam giữ ngắn hạn và hình phạt tiền[10]. Xu thế chung của pháp luật hình sự Trung Quốc là ngày càng trừng phạt nghiêm khắc hơn nữa các tội phạm này.

3. Kinh nghiệm cho Việt Nam trong xây dựng, hoàn thiện chế định về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin và mạng viễn thông

Trên cơ sở pháp luật quốc tế về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông đã nêu trên, có thể rút ra một số kinh nghiệm của pháp luật quốc tế cho Việt Nam như sau:

Thứ nhất, có thể bổ sung quy định về việc pháp nhân thương mại phải chịu trách nhiệm hình sự về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong *Bộ luật Hình sự*. Các công ước quốc tế hiện nay đều yêu cầu các nước thành viên phải truy cứu trách nhiệm hình sự đối với pháp nhân khi có tội phạm công nghệ thông tin do cá nhân thực hiện vì lợi ích của pháp nhân hoặc nhân danh pháp nhân và cá nhân phạm tội là người đại diện của pháp nhân đó. Thực tiễn ở nước ta đã xảy ra nhiều trường hợp pháp nhân được thành lập chỉ nhằm mục đích thực hiện một số tội phạm công nghệ thông tin nhưng do *Bộ luật Hình sự* năm 2015 chưa quy định pháp nhân thương mại là chủ thể của tội phạm này, dẫn đến, cơ quan chức năng không thể đấu tranh, xử lý được.

Thứ hai, điều chỉnh, bổ sung các tình tiết tăng nặng trách nhiệm hình sự đối với một số loại tội phạm trong khung cấu thành tội phạm, đặc biệt là với tình tiết:"Sử dụng mạng Internet, mạng máy tính, mạng viễn thông, phương tiện điện tử để phạm tội" (Điều 321 *Bộ luật Hình sự* năm 2015), nhất là với các tội: rửa tiền, đánh bạc, mua bán người, mua bán bộ phận cơ thể người, mua bán trái phép vũ khí quân dụng, xâm phạm quyền tác giả, quyền trẻ em,... Bởi việc sử dụng các công cụ, phương tiện là mạng internet, mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện tội phạm sẽ làm gia tăng tính chất, mức độ nguy hiểm, tạo thêm tính phức tạp trong vụ án và trên thực tế luôn chứa đựng khả năng gây hậu quả, thiệt hại lớn hơn so với phương thức truyền thống không sử dụng các công cụ, phương tiện này.

Ba là, cần làm rõ và phân hóa hơn nữa trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông trong pháp luật hình sự hiện nay. Pháp luật hình sự nói chung và *Bộ luật Hình sự Việt Nam* nói riêng cần làm rõ và phân hóa cao độ trách nhiệm hình sự đối với từng loại tội phạm cụ thể trong lĩnh vực công nghệ thông tin, mạng viễn thông với xu hướng đa dạng hóa các loại hình phạt chính, hình phạt bổ sung và biện pháp tư pháp áp dụng đối với chủ thể phạm tội, mở rộng thêm các hình phạt không tước tự do nhưng vẫn cần thể hiện tính răn đe, trấn áp nghiêm minh của Nhà nước. Đồng thời, chú trọng xu thế nhân đạo, khắc phục triệt để hậu quả, thiệt hại do tội phạm gây ra và khắc phục nguyên nhân, điều kiện của tội phạm trong lĩnh vực này. Mục đích của trách nhiệm hình sự đối với tội phạm này không phải và không chỉ là trừng trị mà quan trọng là bảo đảm công lý, công bằng xã hội và làm tốt công tác phòng ngừa tội phạm.

Thứ tư, cần có sự điều chỉnh độ rộng của khung hình phạt cải tạo không giam giữ, phạt tiền và phạt tù có thời hạn áp dụng đối với chủ thể phạm tội trong lĩnh vực công nghệ thông tin, mạng viễn thông bảo đảm cân đối, hợp lý, dễ áp dụng, tránh dẫn đến sự tùy tiện và thể hiện được sự công bằng. Theo đó, *Bộ luật Hình sự* cần giới hạn định mức tối thiểu và tối đa của khung hình phạt phù hợp với tính chất, mức độ nguy hiểm của tội phạm, nhân thân người phạm tội và các tình tiết tăng nặng, giảm nhẹ trách nhiệm hình sự của chủ thể phạm tội trong từng vụ án cụ thể. Riêng đối với hình phạt tiền nên định lượng theo trị giá tài sản, thiệt hại gây ra hoặc chiếm đoạt được dùng làm căn cứ quyết định mức phạt. Bên cạnh đó, nên tham khảo kinh nghiệm của Canada trong việc quy đổi từ phạt tiền sang phạt tù khi người phạm tội vi phạm quy định

về nộp phạt tiền. Đặc biệt, rất cần lưu ý nâng mức phạt tù có thời hạn lên mức tù chung thân đối với một số tội phạm cụ thể trong lĩnh vực công nghệ thông tin, mạng viễn thông mà gây hậu quả, thiệt hại rất lớn cho các quan hệ xã hội được *Luật Hình sự* bảo vệ, ví dụ: hệ thống thông tin quan trọng về an ninh quốc gia, tài sản của cơ quan, tổ chức, cá nhân.

Thứ năm, pháp luật hình sự Việt Nam cần quy định rõ trong *Bộ luật Hình sự* về việc suy đoán đương nhiên có trách nhiệm hình sự đối với chủ thể là cá nhân phạm tội nói chung, phạm tội trong lĩnh vực công nghệ thông tin, mạng viễn thông nói riêng theo kinh nghiệm của Canada. Đồng thời, phải xác định nghĩa vụ, trách nhiệm của Nhà nước mà đại diện là các cơ quan chức năng có thẩm quyền tiến hành tố tụng trong quá trình truy cứu trách nhiệm đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Cần xác định rõ vai trò, nghĩa vụ và trách nhiệm của Nhà nước, cụ thể là các cơ quan nhà nước trong việc phải bảo đảm truy cứu trách nhiệm hình sự một cách đúng đắn, khách quan, trên tinh thần "thượng tôn pháp luật".

Thứ sáu, Việt Nam cần sớm hoàn chỉnh khung pháp lý cần thiết liên quan đến các hoạt động trên không gian mạng, trong đó tiếp tục xác định rõ ràng, chặt chẽ những quy định về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Trong đó chú ý vấn đề ban hành các văn bản hướng dẫn liên quan đến các hoạt động trên không gian mạng, các vi phạm pháp luật nói chung, tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông nói riêng và chế tài xử lý đối với các vi phạm đó, bảo đảm cụ thể, chi tiết, phù hợp và dễ áp dụng trong thực tiễn. Để thực hiện tốt vấn đề này, chúng ta cần tham khảo việc nội luật hóa một số quy định trong các văn bản pháp luật quốc tế, như: Công ước Budapest năm 2001 hay tham khảo kinh nghiệm lập pháp của một số nước tiên tiến, như: Hoa Kỳ, Canada về chế định trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

4. Kết luận

Trên cơ sở những nội dung chủ yếu trong quy định của pháp luật quốc tế về trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông cho thấy, nhiều giá trị tiến bộ, phù hợp và rất khả thi để nước ta tham khảo, điều chỉnh chính sách và quy định của pháp luật hình sự liên quan vấn đề này. Thiết nghĩ, *Bộ luật Hình sự* và một số các văn bản pháp lý khác ở Việt Nam cần có sự tiếp thu, vận dụng trong những lần sửa đổi, bổ sung trong thời gian tới, góp phần hoàn thiện chế định trách nhiệm hình sự đối với tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, đáp ứng yêu cầu trong tình hình mới❐

Chú thích:

1. Hội đồng châu Âu (2001). *Công ước về tội phạm mạng* năm 2001.

2. Liên đoàn Ả Rập (2010). *Công ước về phòng, chống tội phạm công nghệ thông tin* năm 2010.

3. Liên minh châu Phi (2014). *Công ước về an ninh mạng và bảo vệ dữ liệu cá nhân* năm 2014.

4. Nguyễn Thị Phương Hoa (2020). *Bàn về mối quan hệ giữa trách nhiệm hình sự của cá nhân với trách nhiệm hình sự của pháp nhân và một số kiến nghị*. Tạp chí Khoa học Pháp lý Việt Nam, số 139 (9/2020), tr. 60.

5, 6. Nguyễn Thị Phương Hoa (2024). *Quy định của Bộ tổng luật Hoa Kỳ về tội phạm liên quan đến công nghệ thông tin, mạng viễn thông*/Kỷ yếu Hội thảo "Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông: Những hạn chế trong quy định, thực tiễn áp dụng pháp luật và giải pháp khắc phục". Trường Đại học Luật TP. Hồ Chí Minh, tr. 114, 114.

7. *Section 156.10, 156.05, 156.20, New York Penal Law*. https://www.nysenate.gov/legislation/laws/PE/ 3TJA156, truy cập ngày 03/6/2020.

8. *Bộ luật Hình sự Canada* (1985). http://www.justice.gc.ca

9. *Bộ luật Hình sự Liên bang Nga* (1996). http://www.kremlin.ru/acts/bank/9555.

10. *Bộ luật Hình sự Trung Quốc* (2015). http://www.criminallaw.com.cn.