

HÀI HOÀ HOÁ PHÁP LUẬT TRONG PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO

ĐỖ QUÍ HOÀNG *

Tóm tắt: Xuất phát từ chủ quyền quốc gia, thẩm quyền tài phán đối với các hành vi tội phạm nói chung và tội phạm công nghệ cao nói riêng thuộc về quốc gia có liên quan đến hành vi phạm tội. Đồng thời, cũng xuất phát từ chủ quyền quốc gia, việc quy định hành vi nào là tội phạm cũng như hình phạt tương ứng với hành vi đó thuộc thẩm quyền riêng biệt của quốc gia. Tuy nhiên, sự khác biệt quá lớn giữa hệ thống pháp luật của các quốc gia có thể trở ngại cho hoạt động phòng chống tội phạm, trong đó có tội phạm công nghệ cao. Bài viết phân tích quy định trong các văn kiện pháp lý quốc tế liên quan đến tội phạm công nghệ cao và vấn đề hài hoà hoá pháp luật - một biện pháp để một mặt vẫn tôn trọng chủ quyền quốc gia nhưng đồng thời có thể hạn chế khoảng cách quá lớn giữa các quy định pháp luật các quốc gia, tạo điều kiện tăng cường hoạt động hợp tác quốc tế giữa các quốc gia trong ngăn ngừa, trừng phạt tội phạm. Trên cơ sở đó, bài viết đánh giá thực tiễn thực hiện hài hoà hoá pháp luật trong phòng chống tội phạm công nghệ cao tại Việt Nam.

Từ khoá: Hài hoà hoá; hình sự hoá; tội phạm công nghệ cao.

Nhận bài: 13/5/2020

Hoàn thành biên tập: 29/12/2020

Duyệt đăng: 31/12/2020

THE HAMORNIZATION OF LAWS ON PREVENTION OF HIGH-TECH CRIMES

Abstract: Deriving from national sovereignty, the jurisdiction to crimes in general and high-tech crimes in particular belongs firstly to the state involved in the offense. At the same time, also derived from national sovereignty, the determination of which acts are crimes and the penalties corresponding to those acts are under the exclusive jurisdiction of the state. However, the huge difference among legal systems of countries can hinder the process of crime prevention, including high-tech crimes. The article analyzes the provisions in international legal instruments on cybercrime and the harmonization of laws - a measure which shows respect to national sovereignty but at the same time, limits the large gap between laws of different nations, facilitating international cooperation among countries in crime prevention and punishment. Thereby, the article evaluates the practical implementation of legal harmonization in the prevention of high-tech crimes in Vietnam.

Keywords: Harmonization; criminalization; high-tech crimes

Received: May 13th, 2020; Editing completed: Dec 29th, 2020; Accepted for publication: Dec 31st, 2020

Hài hoà hoá, theo định nghĩa của Từ điển Cambridge 2020 là “làm cho các hệ thống hoặc luật tại các doanh nghiệp, quốc gia khác nhau trở nên giống nhau hoặc

tương tự nhau... để có thể làm việc cùng nhau dễ dàng hơn”.⁽¹⁾ Từ cách tiếp cận này của Từ điển Cambridge có thể hiểu hài hoà hoá pháp luật là quá trình làm giảm bớt sự khác

* Thạc sĩ, Trường Đại học Luật Hà Nội
E-mail: doquihuong@hlu.edu.vn

(1). <https://dictionary.cambridge.org/vi/dictionary/english/harmonize>, truy cập 10/5/2020.

biệt giữa các hệ thống pháp luật khác nhau của các quốc gia. Mức độ hài hoà hoá phụ thuộc vào nhiều yếu tố như cấp độ liên kết giữa các thành viên; mức độ khác biệt giữa các quốc gia về chính sách, pháp luật và mức độ “mở” trong việc tiếp nhận những thay đổi đối với chính hệ thống pháp luật quốc gia khi thực hiện những cam kết về hài hoà hoá.

Trong các văn kiện về phòng chống tội phạm xuyên quốc gia nói chung và tội phạm công nghệ cao nói riêng, hài hoà hoá pháp luật được ghi nhận như một trong những giải pháp nhằm tạo ra sự tương đồng giữa hệ thống pháp luật của các nước, từ đó giảm bớt các rào cản trong việc thực hiện những hoạt động hợp tác cụ thể trong quá trình điều tra, xét xử tội phạm hay tạo kẽ hở để người phạm tội có thể trốn tránh khỏi việc bị pháp luật trừng trị. Chẳng hạn, theo quy định tại Thỏa thuận hợp tác giữa các quốc gia thành viên của Cộng đồng các quốc gia độc lập về chống tội phạm liên quan đến thông tin máy tính năm 2001,⁽²⁾ các bên sẽ cố gắng đảm bảo hài hòa hóa pháp luật quốc gia của mình liên quan đến việc chống lại các hành vi phạm tội liên quan đến thông tin máy tính (Điều 2); hoặc theo quy định tại Công ước của Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân năm 2014, các quốc gia thành viên sẽ đảm bảo rằng những biện pháp pháp lý và/hoặc các quy định được thông qua nhằm chống tội phạm mạng sẽ tăng cường khả năng hài hoà hoá khu vực đối với những biện pháp này và tôn trọng

nguyên tắc định danh kép (Điều 28).⁽³⁾ Điều này xuất phát từ thực tế là đối với cùng một hành vi, có quốc gia quy định là tội phạm trong luật hình sự của mình nhưng có quốc gia lại không hoặc cũng được quy định là tội phạm nhưng hình phạt tối thiểu tại các quốc gia lại rất khác nhau. Trong trường hợp thứ nhất, sự khác biệt giữa pháp luật hình sự của các quốc gia trong việc xác định một hành vi có phải là tội phạm hay không sẽ tạo ra kẽ hở cho người phạm tội trốn tránh khỏi sự trừng phạt của pháp luật khi phạm tội ở nước này nhưng chạy trốn sang quốc gia khác. Bởi lẽ, theo nguyên tắc “định danh kép”, quốc gia sẽ chỉ tiến hành dẫn độ cá nhân đang hiện diện trên lãnh thổ nước mình cho quốc gia yêu cầu nếu hành vi làm cơ sở để yêu cầu dẫn độ được quy định là tội phạm trong luật hình sự của cả hai bên. Nói cách khác, nếu tại quốc gia mà người chạy trốn đang hiện diện, hành vi mà người đó đã thực hiện tại quốc gia yêu cầu dẫn độ không được quy định là tội phạm trong luật hình sự thì quốc gia được yêu cầu sẽ không tiến hành dẫn độ và người đó sẽ không bị xét xử vì hành vi đã thực hiện đó của mình. Trong trường hợp thứ hai, khi cùng một hành vi phạm tội nhưng các quốc gia lại quy định các khung hình phạt khác nhau thì tại quốc gia quy định hình phạt nhẹ hơn nhiều so với các quốc gia khác, hành vi phạm tội sẽ không được trừng phạt một cách thích đáng và như vậy, sẽ không đảm bảo được tính răn đe để ngăn ngừa các vi phạm tương tự khác trong xã hội.

(2). Thỏa thuận hợp tác giữa các quốc gia thành viên của Cộng đồng các quốc gia độc lập về chống tội phạm liên quan đến thông tin máy tính năm 2001, <https://dig.watch/node/4764>, truy cập 10/5/2020.

(3). Công ước của Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân năm 2014, https://www.opennetafrika.org/?wpfb_dl=4, truy cập 10/5/2020.

Để hạn chế những bất cập này, các văn kiện quốc tế về tội phạm xuyên quốc gia thường quy định vấn đề hài hoà hoá pháp luật ở mức độ phổ biến là hình sự hoá những hành vi nhất định để tạo cơ sở pháp lý cho việc truy cứu trách nhiệm hình sự cũng như tiến hành các hoạt động dẫn độ, tương trợ tư pháp hình sự khi cần thiết. Bên cạnh đó, đối với các trường hợp có cấp độ liên kết cao giữa các thành viên, mức độ hài hoà hoá còn bao gồm cả hài hoà hoá về hình phạt, tức là quy định mức hình phạt tối thiểu đối với mỗi hành vi vi phạm nhất định nhằm tạo ngưỡng chung trong xử lý hình sự những hành vi tội phạm tại tất cả các quốc gia thành viên, điển hình ở mức độ này là Liên minh châu Âu.

1. Hình sự hoá những hành vi vi phạm liên quan đến công nghệ cao

Khuôn mẫu chung của các văn kiện quốc tế về tội phạm công nghệ cao là ghi nhận nghĩa vụ của các quốc gia trong việc quy định ở luật hình sự nước mình những hành vi có ý vi phạm liên quan đến công nghệ cao là tội phạm.⁽⁴⁾

Chẳng hạn, theo quy định tại Công ước Budapest về tội phạm mạng năm 2001 (sau đây gọi tắt là Công ước Budapest), mỗi quốc gia thành viên sẽ ban hành luật và những biện pháp khác khi cần thiết để ghi nhận là tội phạm hình sự theo luật nước mình đối với những hành vi được thực hiện một cách cố ý, bao gồm: 1) nhóm hành vi chống lại sự bí mật, toàn vẹn và sẵn có của dữ liệu máy tính và hệ thống máy tính bao gồm truy cập bất

hợp pháp, ngăn chặn bất hợp pháp, gây rối dữ liệu, gây rối hệ thống, sử dụng sai lạc các thiết bị; 2) những hành vi liên quan đến máy tính gồm hành vi giả mạo liên quan đến máy tính, lừa đảo liên quan đến máy tính; 3) những hành vi liên quan đến các tài liệu khiêu dâm trẻ em; 4) các hành vi xâm phạm quyền tác giả và quyền liên quan và 5) hành vi khuyến khích và hỗ trợ cho việc thực hiện những hành vi trên.⁽⁵⁾ Trong trường hợp hành vi trên do cá nhân thực hiện vì lợi ích của pháp nhân và nếu cá nhân đó là đại diện hoặc giữ vị trí lãnh đạo tại một cơ quan của pháp nhân trên cơ sở thẩm quyền đại diện cho pháp nhân, thẩm quyền ra quyết định nhân danh pháp nhân hoặc thẩm quyền thực hiện việc kiểm soát nội bộ pháp nhân hoặc pháp nhân không thực hiện tốt việc kiểm soát, giám sát những cá nhân đó, dẫn đến việc thực hiện những hành vi trên vì lợi ích của pháp nhân, quốc gia cũng phải ban hành luật và các biện pháp khác khi cần thiết ghi nhận trách nhiệm của pháp nhân, bao gồm cả trách nhiệm hình sự, dân sự hoặc hành chính (Điều 12). Để đảm bảo trừng phạt thích đáng đối với những hành vi tội phạm công nghệ cao, Công ước Budapest cũng quy định nghĩa vụ đối với các quốc gia thành viên phải đảm bảo hệ thống chế tài tương xứng, hiệu quả, có tác dụng răn đe, bao gồm cả việc tước quyền tự do đối với cá nhân và phạt tiền đối với pháp nhân (Điều 13).

Theo quy định tại Công ước Arab về chống tội phạm công nghệ thông tin năm

(4). Schjolberg Stein, "The history of global harmonization on cybercrime legislation—the road to geneva", *Journal of International Commercial Law and Technology*, volume 1.12, 2008, p. 1 - 19.

(5). Nội dung cụ thể của những hành vi này xem Công ước Budapest năm 2001, các điều từ Điều 3 đến Điều 10, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>, truy cập 10/5/2020.

2010, “mỗi quốc gia thành viên cam kết hình sự hóa các hành vi được quy định trong chương này theo các luật và đạo luật của quốc gia” (Điều 5), bao gồm: truy cập bất hợp pháp; ngăn chặn bất hợp pháp; gây rối dữ liệu; lạm dụng phương tiện công nghệ thông tin; giả mạo; lừa đảo; hành vi liên quan đến khiêu dâm; hành vi xâm phạm quyền riêng tư; khủng bố bằng hình thức công nghệ thông tin; hành vi liên quan đến phạm tội có tổ chức bằng hình thức công nghệ thông tin; hành vi xâm phạm quyền tác giả và quyền liên quan; sử dụng trái phép công cụ thanh toán điện tử và các hành vi nỗ lực; trợ giúp cho việc thực hiện những hành vi trên.⁽⁶⁾ Trên cơ sở tính đến pháp luật quốc gia, mỗi quốc gia sẽ ban hành quy định ghi nhận trách nhiệm hình sự đối với pháp nhân trong trường hợp hành vi được thực hiện bởi người đại diện của pháp nhân hoặc vì lợi ích của pháp nhân (Điều 20).

Theo quy định tại Thỏa thuận hợp tác giữa các quốc gia thành viên của Cộng đồng các quốc gia độc lập về chống tội phạm liên quan đến thông tin máy tính năm 2001, theo quy định của pháp luật nước mình, các bên kí kết sẽ quy định những hành vi được thực hiện có ý sau đây là tội phạm trong luật hình sự của mỗi nước: 1) truy cập bất hợp pháp vào thông tin máy tính được pháp luật bảo vệ, trong đó hành vi đó dẫn đến việc phá hủy, ngăn chặn, sửa đổi hoặc sao chép thông tin hoặc làm gián đoạn hoạt động của máy

tính, hệ thống máy tính hoặc các mạng liên quan; 2) tạo ra, sử dụng hoặc phân phối phần mềm độc hại; 3) vi phạm các quy định quản lý việc sử dụng máy tính, hệ thống máy tính hoặc mạng liên quan của người có quyền truy cập vào máy tính, hệ thống hoặc mạng đó, dẫn đến việc phá hủy, chặn hoặc sửa đổi thông tin máy tính được pháp luật bảo vệ, hành vi gây ra thiệt hại đáng kể hoặc hậu quả nghiêm trọng; 4) sử dụng bất hợp pháp phần mềm máy tính và cơ sở dữ liệu được bảo vệ bằng bản quyền, hoặc vi phạm bản quyền phần mềm mà hành vi đó gây ra thiệt hại đáng kể (Điều 3).

Tương tự như các công ước trên về nghĩa vụ hình sự hoá hành vi phạm tội liên quan đến công nghệ cao nhưng Công ước Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân lại không ghi nhận theo hướng liệt kê những hành vi cần được hình sự hoá mà chỉ quy định ngắn gọn: “Mỗi quốc gia thành viên sẽ thông qua luật và/hoặc quy định khi cần thiết để thừa nhận là tội phạm hình sự đối với những hành vi tác động đến tính bảo mật, toàn vẹn, sẵn có và sống còn của hệ thống công nghệ và thông tin, dữ liệu, cơ sở hạ tầng mạng” (Điều 25).⁽⁷⁾

Ngoài điều ước quốc tế, một số văn bản có giá pháp lý ràng buộc do các cơ quan có tổ chức quốc tế thông qua như các chỉ thị của Liên minh châu Âu do Nghị viện, Hội đồng bộ trưởng châu Âu thông qua hay Chỉ thị của Cộng đồng kinh tế các quốc gia Tây Phi do

(6). Công ước Arab về chống tội phạm công nghệ thông tin, từ Điều 6 đến Điều 19. <https://dig.watch/instruments/arab-convention-combating-technology-offences>, truy cập 10/5/2020.

(7). Bande Lewis, “Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities”, *International Journal of Cyber Criminology*, 2018, volume 05.

Nghị viện thông qua cũng ghi nhận nghĩa vụ của các quốc gia thành viên phải ban hành luật trong nước để quy định những hành vi được liệt kê trong văn kiện này là tội phạm hình sự. Chẳng hạn, theo quy định tại Chỉ thị C/DIR.1/08/11 về chống tội phạm mạng trong khuôn khổ Cộng đồng kinh tế của các quốc gia Tây Phi, những hành vi sau đây là tội phạm: truy cập trái phép hệ thống máy tính; xâm hại tính toàn vẹn của hệ thống máy tính; tiếp cận trái phép dữ liệu của hệ thống máy tính; ngăn chặn trái phép dữ liệu máy tính; thay đổi trái phép dữ liệu máy tính; giả mạo dữ liệu máy tính, thu lợi từ máy tính do sự gian lận, chiếm đoạt dữ liệu cá nhân; sử dụng dữ liệu giả mạo; chiếm đoạt công cụ để phạm các tội về tội phạm mạng được ghi nhận trong Chỉ thị; tham gia vào một hiệp hội hoặc thoả thuận về tội phạm máy tính; các hành vi liên quan đến khiêu dâm trẻ em như sản xuất, giới thiệu, nhập khẩu, xuất khẩu, sở hữu, tiếp cận các sản phẩm khiêu dâm trẻ em; sở hữu các tranh ảnh, tài liệu bằng văn bản về phân biệt chủng tộc hoặc bài ngoại thông qua hệ thống máy tính; đe dọa thông qua hệ thống máy tính, lạm dụng thông qua hệ thống máy tính; bao biện hoặc biện minh hoặc phạm tội ác chống loài người bằng hệ thống máy tính.⁽⁸⁾ Theo quy định tại Chỉ thị 2013/40/EU của Nghị viện và Hội đồng Bộ trưởng ngày 12/8/2013 về những hành vi tấn công chống lại hệ thống thông tin

và thay thế Quyết định khung 2005/222/JHA, các quốc gia thành viên có nghĩa vụ phải quy định những hành vi được thực hiện cố ý sau đây là tội phạm hình sự, ít nhất trong các trường hợp mà người thực hiện không phải là người chưa thành niên, bao gồm: 1) tiếp cận bất hợp pháp hệ thống thông tin; 2) can thiệp bất hợp pháp; 3) can thiệp dữ liệu bất hợp pháp; 4) ngăn chặn bất hợp pháp; 5) sử dụng, nhập khẩu, phân phối hoặc những hành vi khác để tạo điều kiện cho việc sử dụng các công cụ để thực hiện các hành vi tiếp cận bất hợp pháp hệ thống thông tin, can thiệp bất hợp pháp, can thiệp dữ liệu bất hợp pháp, ngăn chặn bất hợp pháp cũng như những hành vi xúi giục, hỗ trợ việc thực hiện những hành vi trên (Điều 3, Điều 4, Điều 5, Điều 6, Điều 7 và Điều 8).⁽⁹⁾

Có thể thấy, mặc dù đều có điểm chung trong việc ghi nhận nghĩa vụ của các quốc gia thành viên phải hình sự hoá những hành vi phạm tội liên quan đến công nghệ cao nhưng việc xác định hành vi nào sẽ bị coi là tội phạm ở các văn kiện không giống nhau, ngoài một số hành vi chung như truy cập bất hợp pháp, gây rối dữ liệu, giả mạo hay các hành vi liên quan đến khiêu dâm trẻ em trên mạng. Sở dĩ có điều này là vì hiện nay chưa có văn kiện nào định nghĩa về tội phạm công nghệ theo hướng chỉ ra các đặc điểm chung để nhận diện mà chỉ tiếp cận theo hướng liệt kê các hành vi bị coi là tội phạm công nghệ cao.

(8). Chỉ thị C/DIR.1/08/11 về chống tội phạm mạng trong khuôn khổ Cộng đồng kinh tế của các quốc gia Tây Phi từ Điều 4 đến Điều 23, <https://issafrica.org/ctafrika/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS.pdf>, truy cập 10/5/2020.

(9). Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>, truy cập 16/5/2020.

2. Hải hoà hoá hình phạt

Hình sự hoá hành vi phạm tội mới dừng lại ở yêu cầu đối với các quốc gia thành viên phải quy định những hành vi nhất định là tội phạm trong luật hình sự, nhằm tạo cơ sở cho các hoạt động hợp tác giữa các cơ quan tư pháp, cơ quan thực thi pháp luật giữa các quốc gia trong ngăn ngừa, phòng chống tội phạm công nghệ cao nhưng lại không đặt ra những quy tắc cụ thể liên quan đến hình phạt sẽ áp dụng đối với tội phạm này. Điều này có thể dẫn đến thực tế là mặc dù cùng quy định là tội phạm trong luật hình sự nhưng hình phạt áp dụng giữa các nước sẽ có sự khác biệt. Chẳng hạn, hành vi truy cập bất hợp pháp một phần hay toàn bộ hệ thống máy tính, ngoài phạt tiền, theo quy định tại Luật số 1075 năm 2012 về ngăn ngừa tội phạm mạng của Philippines, có thể bị phạt tù từ 6 năm 01 ngày cho đến 12 năm (Điều 5),⁽¹⁰⁾ theo quy định tại Luật Sử dụng sai máy tính của Brunei bị phạt tù tối đa 2 năm, hoặc 3 năm trong trường hợp tái phạm.⁽¹¹⁾ Trong khi đó, theo quy định tại Luật Tội phạm máy tính năm 2007 của Thái Lan, hình phạt chỉ không quá 6 tháng tù (Điều 5).⁽¹²⁾

Sự khác nhau này có thể khiến cho hình phạt không đủ hiệu quả trong trừng trị người phạm tội cũng như không đủ tính răn đe để ngăn ngừa những hành vi phạm tội trong

tương lai tại những quốc gia mà hình phạt nhẹ hơn nhiều so với các quốc gia khác.

Hệ quả trên có thể khắc phục được thông qua hải hoà hoá hình phạt. Vấn đề hải hoà hoá hình phạt được quy định trong các văn kiện quốc tế về tội phạm công nghệ cao có thể chia thành hai cấp độ: *Một là* ghi nhận quy tắc chung trong xác định hình phạt tại các quốc gia; *hai là* quy định ngưỡng hình phạt tối thiểu đối từng hành vi và pháp luật hình sự của các quốc gia phải quy định hình phạt không được thấp hơn ngưỡng hình phạt này.⁽¹³⁾

Cấp độ hải hoà hoá hình phạt phổ biến hiện nay là ghi nhận nguyên tắc chung trong xác định hình phạt, còn việc quy định cụ thể ra sao sẽ do mỗi quốc gia tự quy định. Theo đó, những nguyên tắc được quy định phổ biến để xác định hình phạt bao gồm: Tương xứng, hiệu quả và có tính răn đe (Điều 13 Công ước Budapest, Điều 31 Công ước của Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân, Điều 28 Chỉ thị về chống tội phạm mạng do Nghị viện của Cộng đồng kinh tế các quốc gia Tây Phi...). Tuy nhiên, nội dung của những nguyên tắc này sẽ do mỗi quốc gia tự xác định. Điều này dẫn đến hệ quả là mặc dù có những nguyên tắc chung trong quy định hình phạt nhưng vẫn có thể xảy ra thực tế là hình phạt giữa các nước có sự khác biệt đáng kể bởi lẽ mức độ nặng nhẹ của hình phạt trước hết được xác định thông qua sự đánh giá mức độ nguy hiểm cho xã hội của hành vi phạm tội. Nói cách khác, sự khác nhau trong hình phạt của các quốc gia

(10). Republic Act No. 10175, <https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/>, truy cập 10/5/2020.

(11). Computer Misuse Act, https://www.unodc.org/res/cld/document/computer-misuse-act_html/Brunei_Computer_Misuse.pdf, truy cập 10/5/2020.

(12). Computer Crime Act B.E 2550 (2007) <https://www.samuiforsale.com/law-texts/computer-crime-act.html>, truy cập 10/5/2020.

(13). Schjolberg, Judge Stein, and Amanda M. Hubbard, "Harmonizing National Legal Approaches on Cybercrime", *International Telecommunication Union*, volume (1 July 2005).

đối với cùng một hành vi phản ánh sự khác nhau trong đánh giá mức độ nguy hiểm của hành vi đó đối với xã hội, từ đó dẫn đến mức độ cưỡng chế, trừng phạt khác nhau. Điều này xuất phát từ đặc điểm nội tại của mỗi quốc gia về kinh tế, chính trị, xã hội, văn hoá, hệ tư tưởng cũng như đặc điểm lịch sử trong từng giai đoạn của quốc gia đó.

So với cấp độ đầu tiên, việc quy định ngưỡng hình phạt tối thiểu đã thể hiện một cấp độ cao hơn trong hợp tác. Để đạt được điều này, đòi hỏi phải thoả mãn đồng thời hai yếu tố: *một là* sự tương đồng giữa các thành viên; *hai là* quyết tâm chính trị, mong muốn làm sâu thêm mức độ hợp tác. Hai yếu tố này có mối liên hệ chặt chẽ với nhau. Nếu không có sự tương đồng giữa các thành viên sẽ không có cơ sở để nâng cấp mức độ hợp tác. Ngược lại, cho dù giữa các thành viên có sự tương đồng lớn nhưng nếu không có mong muốn nâng cao hợp tác thì điều này cũng không diễn ra.

Diễn hình cho việc đáp ứng được những yếu tố này là Liên minh châu Âu (EU).⁽¹⁴⁾ Trong lĩnh vực hình sự, EU đang tiến hành hài hoà hoá pháp luật hình sự của các quốc gia thành viên thông qua việc quy định một mức hình phạt tối thiểu chung đối với một số loại tội phạm, trong đó có tội phạm công nghệ cao nhằm đảm bảo tính hiệu quả, tương xứng, khả năng ngăn ngừa của hình phạt, qua đó hạn chế những ảnh hưởng tiêu cực đến hiệu quả của hoạt động phòng chống tội

phạm do khoảng cách, sự khác biệt đáng kể giữa các hệ thống pháp luật của các quốc gia thành viên. Đến nay, EU đã ban hành một số văn bản liên quan đến tội phạm công nghệ cao dưới dạng chỉ thị do Nghị viện và Hội đồng bộ trưởng thông qua, trong đó ghi nhận những hình phạt tối thiểu đối với từng hành vi phạm tội cụ thể như Chỉ thị số 2013/40 của Nghị viện và Hội đồng Bộ trưởng châu Âu ngày 12/8/2013 về các cuộc tấn công chống lại hệ thống thông tin (sau đây gọi tắt là Chỉ thị số 2013/40), Chỉ thị số 2011/92 của Nghị viện và Hội đồng Bộ trưởng ngày 13/12/2011 về chống lạm dụng tình dục, bạo hành tình dục trẻ em và khiêu dâm liên quan đến trẻ em (sau đây gọi tắt là Chỉ thị số 2011/92).

Chẳng hạn, theo quy định tại Chỉ thị số 2013/40, hình phạt tối thiểu mà các quốc gia thành viên phải quy định trong pháp luật hình sự của mình đối với những hành vi, bao gồm:

Thứ nhất, tối thiểu 2 năm tù đối với các hành vi tấn công hệ thống thông tin bất hợp pháp; can thiệp bất hợp pháp vào hệ thống; can thiệp bất hợp pháp dữ liệu; ngăn chặn trái phép; cố ý sản xuất, bán, mua sắm để sử dụng, nhập khẩu, phân khối hoặc cung cấp chương trình máy tính, mật khẩu máy tính, mã truy cập hoặc dữ liệu của hệ thống thông tin để thực hiện các hành vi can thiệp bất hợp pháp vào hệ thống, can thiệp bất hợp pháp dữ liệu hoặc ngăn chặn trái phép (khoản 2 Điều 9);⁽¹⁵⁾

Thứ hai, tối thiểu 3 năm tù đối với hành vi cố ý tấn công hệ thống thông tin bất hợp pháp; can thiệp bất hợp pháp vào hệ thống nếu một số lượng đáng kể hệ thống thông tin

(14). Shkempi, Aldo, Indrit Shtupi, and Arjan Qafa, "The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation", *Academic Journal of Interdisciplinary Studies*, volume 5.1, 2016.

(15). Định nghĩa về những hành vi phạm tội này xem thêm Chỉ thị số 2013/40.

đã bị ảnh hưởng do việc sử dụng một trong những công cụ gồm chương trình máy tính, mật khẩu máy tính, mã truy cập hoặc dữ liệu của hệ thống thông tin được tạo ra nhằm thực hiện các hành vi trên (khoản 3 Điều 9);

Thứ ba, tối thiểu 5 năm tù nếu hành vi do tội phạm có tổ chức thực hiện; gây ra thiệt hại nghiêm trọng hoặc chống lại hệ thống thông tin cơ sở hạ tầng quan trọng (khoản 4 Điều 9).

Theo quy định tại Chỉ thị số 2011/92, hành vi đề nghị, bằng công nghệ thông tin, một đứa trẻ chưa đến tuổi chấp thuận tình dục, để gặp đứa trẻ đó nhằm thực hiện hành vi quan hệ tình dục với trẻ em hoặc đặt hàng, cung cấp các nội dung khiêu dâm, nếu đề nghị đó được tiếp tục bằng những hành vi thực tế để dẫn đến một cuộc gặp như vậy sẽ bị phạt tù tối thiểu 1 năm (Điều 6); hành vi cố ý truy cập thông tin, nội dung khiêu dâm trẻ em bằng công nghệ, bị phạt tù tối thiểu 1 năm (Điều 5). Quốc gia thành viên có nghĩa vụ chuyển hoá những quy định về hình phạt trong các chỉ thị này vào pháp luật quốc gia trong thời hạn do chỉ thị quy định. Nói cách khác, quốc gia phải ban hành những quy định trong luật hình sự quốc gia, trong đó quy định những hành vi trên là tội phạm và hình phạt tối thiểu đối với những tội này không được thấp hơn hình phạt mà chỉ thị ghi nhận. Ủy ban châu Âu có thẩm quyền giám sát quá trình nội luật hoá này của quốc gia thành viên. Việc không chuyển hoá quy định của chỉ thị đúng thời hạn hoặc chuyển hoá không chính xác sẽ bị coi là hành vi vi phạm pháp luật của Liên minh châu Âu (EU). Trong trường hợp này, Ủy ban châu Âu và/hoặc Tòa công lý Liên minh châu Âu sẽ có thẩm quyền thực hiện những biện pháp mang tính

chất hành chính, tư pháp theo quy định của pháp luật EU để đảm bảo nghĩa vụ chuyển hoá chính xác của quốc gia vi phạm.⁽¹⁶⁾

Trong lĩnh vực hình sự, chủ quyền quốc gia được thể hiện rất rõ thông qua thẩm quyền riêng biệt của mỗi quốc gia trong việc xác định tội phạm và hình phạt. Tuy nhiên, điều này có thể trở thành kẻ hở trong việc ngăn ngừa, trừng trị hành vi phạm tội nếu tồn tại sự khác biệt quá lớn giữa pháp luật của các nước. Do đó, hài hoà hoá pháp luật được coi như một biện pháp hữu ích để thu hẹp khoảng cách này trong khi vẫn đảm bảo tôn trọng chủ quyền của mỗi quốc gia.

3. Vấn đề hài hoà hóa pháp luật về tội phạm công nghệ cao ở Việt Nam

Liên quan đến các nội dung về hài hoà hoá pháp luật về phòng chống tội phạm công nghệ cao, thực tiễn của Việt Nam mới chỉ thực hiện được nội dung thứ nhất về hình sự hóa các hành vi vi phạm liên quan đến công nghệ cao, còn nội dung thứ hai về hài hoà hóa hình phạt vẫn đang được thực hiện một cách hạn chế.

Đối với yêu cầu về hình sự hóa hành vi vi phạm liên quan đến công nghệ cao, Bộ luật Hình sự Việt Nam năm 2015 sửa đổi, bổ sung năm 2017 đã có các quy định về các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông với 9 tội danh, từ Điều 285 đến Điều 294.⁽¹⁷⁾ Ngoài ra, quy định tại Bộ

(16). Phạm Hồng Hạnh, “Cơ chế đảm bảo thực thi pháp luật của Liên minh châu Âu và một số kinh nghiệm đối với ASEAN”, *Tạp chí Luật học*, số 9/2016, tr. 75 - 85.

(17). Quy định trong Bộ luật Hình sự Việt Nam 2015 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 phát tán chương

luật Hình sự Việt Nam năm 2015 được hướng dẫn tại Nghị định số 25/2014/NĐ-CP ngày 07/4/2014 của Chính phủ quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao và Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC ngày 10/9/2012 của liên ngành Bộ Công an, Bộ Quốc phòng, Bộ Tư pháp, Bộ Thông tin và Truyền thông, Viện kiểm sát nhân dân tối cao, Tòa án nhân dân tối cao hướng dẫn áp dụng một số quy định của Bộ luật Hình sự về một số tội phạm trong lĩnh vực công nghệ thông tin, viễn thông.

Tội phạm sử dụng công nghệ cao được điều chỉnh cũng có đầy đủ các đặc điểm của các loại tội phạm truyền thống khác: là những hành vi nguy hiểm cho xã hội và có bốn yếu tố cấu thành tội phạm (khách thể, mặt khách quan, chủ thể và mặt chủ quan).

- Về khách thể: Để thực hiện các hành vi phạm tội sử dụng công nghệ cao, thủ phạm sử dụng máy tính và mạng máy tính làm công cụ để xâm phạm lợi ích của cá nhân, pháp nhân, tổ chức; ảnh hưởng đến trật tự công cộng, an toàn công cộng (là loại tội phạm không biên giới, có thể xâm hại quyền

lợi người bị hại ở các quốc gia khác nhau). Đây là loại tội phạm có khách thể rất rộng và liên quan đến các tội phạm truyền thống nhưng đã sử dụng các thành tựu của công nghệ thông tin để thực hiện hành vi phạm tội.

- Về mặt khách quan: Các hành vi của tội phạm công nghệ cao rất đa dạng và phức tạp, được quy định trong Bộ luật Hình sự Việt Nam năm 2015 sửa đổi, bổ sung năm 2017 gồm 9 tội danh quy định từ Điều 285 đến Điều 292.

Hậu quả của hành vi trong tội phạm công nghệ cao gây nên rất khó định lượng. Những thiệt hại trực tiếp của nó có thể nhỏ nhưng hậu quả gián tiếp có thể rất lớn. Theo Điều 3 Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTTTT-VKSNDTC-TANDTC, hậu quả đó có thể là thiệt hại về vật chất (như tiền, máy móc, phần mềm kỹ thuật hoặc thiệt hại do hỏng máy móc, phần mềm kỹ thuật dẫn đến thiệt hại về hoạt động sản xuất) hoặc thiệt hại phi vật chất như gây ảnh hưởng xấu đến việc thực hiện đường lối, chính sách của Đảng, pháp luật của Nhà nước; gây ảnh hưởng xấu về an ninh quốc gia, trật tự, an toàn xã hội; xâm phạm danh dự, nhân phẩm con người, uy tín của cơ quan, tổ chức...

Việc xác định hậu quả là thiệt hại về tài sản để coi là yếu tố định tội hoặc định khung hình phạt không được căn cứ vào giá trị tài sản bị chiếm đoạt, vì giá trị tài sản này đã được quy định thành tình tiết định khung riêng biệt. Hậu quả phải là thiệt hại về tài sản xảy ra ngoài giá trị tài sản bị chiếm đoạt. Thiệt hại về tài sản do tội phạm gây ra bao gồm thiệt hại trực tiếp và thiệt hại gián tiếp. Thiệt hại trực tiếp là thiệt hại do hành vi phạm tội trực tiếp gây ra, bao gồm thiệt hại

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 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); Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông (Điều 292).

về phần mềm, phần cứng, thiết bị số... Thiệt hại gián tiếp là thiệt hại thuộc về hệ quả của thiệt hại trực tiếp.

- Về mặt chủ quan: Chủ thể thực hiện hành vi phạm tội phạm công nghệ cao thường thực hiện do lỗi cố ý. Trong trường hợp tuy hành vi vi phạm chưa gây ra hậu quả nghiêm trọng nhưng trước đó đã bị xử phạt hành chính về hành vi này mà còn vi phạm thì vẫn cấu thành tội phạm. Các yếu tố về động cơ, mục đích của vi phạm pháp luật trong lĩnh vực công nghệ thông tin thường không phải là dấu hiệu bắt buộc mà yếu tố quan trọng để xác định hành vi có cấu thành tội phạm là hậu quả xảy ra. Động cơ, mục đích của tội phạm máy tính có thể đơn giản nhưng lại có thể gây ra những hậu quả rất nghiêm trọng.

- Về chủ thể thực hiện hành vi phạm tội:

Đối với tội phạm công nghệ cao, trách nhiệm hình sự áp dụng với người từ đủ 16 tuổi trở lên. Đối với người từ đủ 14 tuổi trở lên nhưng chưa đủ 16 tuổi chỉ phải chịu trách nhiệm hình sự về tội phạm rất nghiêm trọng, tội phạm đặc biệt nghiêm trọng quy định 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); 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); Điều 287 (tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử); Điều 289 (tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác); Điều 290 (tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản).

Bên cạnh các quy định về cấu thành tội phạm công nghệ cao, một trong những quy định phục vụ có hiệu quả cho yêu cầu đấu tranh phòng chống tội phạm công nghệ cao, đó là quy định về nguồn chứng cứ - dữ liệu điện tử (chứng cứ điện tử). Đây là quy định tạo tiền đề cho việc giải quyết đúng đắn các vụ án hình sự trong lĩnh vực công nghệ cao, những vụ án có sử dụng công nghệ thông tin là công cụ, phương tiện phạm tội. Dữ liệu điện tử - với tư cách là một nguồn chứng cứ, được định nghĩa là *“kí 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”*.⁽¹⁸⁾ Khi các dữ liệu điện tử được thu thập theo những biện pháp do Bộ luật Tố tụng hình sự quy định, thỏa mãn các thuộc tính của chứng cứ thì các dữ liệu điện tử được coi là chứng cứ điện tử.

Chứng cứ trong vụ án hình sự nói chung và trong vụ án thực hiện tội phạm công nghệ cao nói riêng có ý nghĩa lớn không chỉ về mặt pháp lý để chứng minh hành vi phạm tội mà nó còn có một ý nghĩa vô cùng quan trọng khi vận dụng để thu thập, phân tích, chuyển hóa chứng cứ điện tử sang chứng cứ truyền thống để phục vụ công tác điều tra, truy tố và xét xử các vụ án mà các đối tượng phạm tội đã sử dụng, lạm dụng những thành tựu khoa học, kỹ thuật tiên tiến làm công cụ, phương tiện để thực hiện hành vi phạm tội. Một trong những nguồn chứng cứ quan trọng trong các vụ án sử dụng công nghệ cao để phạm tội là những vật chứng thu giữ tại nơi tội phạm xảy ra, mang dấu vết tội phạm như: “cookies”, “URL”, web server logs, email logs... (đây là những thông tin do máy tính

(18). Điều 99 Bộ luật Tố tụng hình sự Việt Nam năm 2015.

tạo ra) hoặc cũng có thể là những thông tin điện tử do con người tạo ra được lưu giữ trong máy tính hoặc các thiết bị điện tử khác như các văn bản, bảng biểu, các hình ảnh, thông tin được lưu giữ dưới dạng tin hiệu điện tử. Hầu hết đối tượng sử dụng công nghệ cao để phạm tội đều có nhận thức về pháp luật và hiểu biết công nghệ cao và khi thực hiện hành vi phạm tội đều có những thủ đoạn tinh vi để che giấu thông tin phạm tội, khi phát hiện nguy cơ bại lộ, chúng nhanh chóng xóa bỏ các dấu vết để chối tội (như xóa các dữ liệu có liên quan; đánh sập các trang web), vì vậy việc thu thập, phục hồi, chuyển hoá chứng cứ điện tử thành chứng cứ truyền thống để chứng minh hành vi phạm tội của các đối tượng là vô cùng quan trọng, nó quyết định sự thành công hay thất bại của hoạt động đấu tranh.

- Về hình phạt đối với tội phạm công nghệ cao: Pháp luật Việt Nam quy định bảy hình phạt chính và bảy hình phạt bổ sung đối với người phạm tội.⁽¹⁹⁾ Hình phạt chính là phạt tiền hoặc tù có thời hạn. Bên cạnh các hình phạt chính, người phạm tội còn có thể bị phạt tiền, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm; tịch thu một phần hoặc toàn bộ tài sản.

Như vậy, từ các phân tích trên cho thấy, quan điểm của Việt Nam về hình sự hoá hành vi phạm liên quan đến công nghệ cao là phù hợp và tương thích với các điều ước quốc tế đa phương về tội phạm công nghệ cao. Hình thức quy định về loại tội phạm này cũng theo cách thức liệt kê là chủ yếu.

(19). Điều 32 Bộ luật Hình sự Việt Nam năm 2015, sửa đổi, bổ sung năm 2017.

Đối với yêu cầu thứ hai về hài hoà hoá hình phạt, tính đến tháng 12/2020, Việt Nam chưa tham gia điều ước quốc tế nào trực tiếp liên quan đến phòng chống tội phạm công nghệ cao cả ở phạm vi song phương, khu vực cũng như toàn cầu. Trong quá trình đấu tranh hợp tác quốc tế phòng chống tội phạm nói chung và tội phạm công nghệ cao nói riêng, Việt Nam đã là thành viên của các điều ước quốc tế đa phương và song phương về tương trợ tư pháp về hình sự, dẫn độ, chuyển giao người bị kết án phạt tù và các hiệp định tương trợ tư pháp về dân sự và hình sự với các quốc gia, trong đó có một số nội dung liên quan đến phòng chống tội phạm công nghệ cao thông qua các hoạt động hợp tác quốc tế về dẫn độ tội phạm, tương trợ tư pháp về hình sự, chuyển giao người bị kết án phạt tù, không có nội dung cam kết liên quan đến hình phạt đối với loại hình tội phạm này. Tính đến tháng 9/2019, Việt Nam là thành viên của 22 điều ước quốc tế đa phương quy định về tương trợ tư pháp về hình sự, dẫn độ và chuyển giao người bị kết án phạt tù. Trong số này có 01 hiệp định chuyên biệt tương trợ tư pháp về hình sự là Hiệp định tương trợ tư pháp về hình sự giữa các quốc gia ASEAN năm 2004 (có hiệu lực tại Việt Nam từ ngày 20/9/2005).⁽²⁰⁾

Trong lĩnh vực hợp tác quốc tế phòng, chống tội phạm nói chung và tội phạm công nghệ cao nói riêng, Việt Nam đã kí kết nhiều điều ước quốc tế song phương với từng quốc gia khác nhau trên cơ sở mức độ quan hệ ngoại giao và tùy thuộc nhu cầu về phạm vi,

(20). Văn phòng Quốc hội, “Hài hòa pháp luật trong xây dựng Cộng đồng Asean – Những vấn đề đặt ra với Việt Nam qua kinh nghiệm từ EU”, Ki yếu Hội thảo quốc tế, tháng 7/2015.

nội dung hợp tác quốc tế trong phòng, chống tội phạm của của mỗi nước. Hiện nay, Việt Nam đã kí 45 hiệp định song phương với các quốc gia, trong đó có 12 hiệp định tương trợ tư pháp chung, bao gồm cả dân sự, gia đình và hình sự với các quốc gia, 11 hiệp định chuyên biệt về tương trợ tư pháp về hình sự, 12 hiệp định chuyên biệt về dẫn độ và 10 hiệp định chuyên biệt về chuyển giao người bị kết án phạt tù.⁽²¹⁾ Các điều ước quốc tế song phương hiện hành là cơ sở pháp lí hợp tác quốc tế trong phòng, chống tội phạm cụ thể.

Như vậy, cần lưu ý rằng, trong khu vực ASEAN, Hiệp định tương trợ tư pháp về hình sự giữa các quốc gia ASEAN năm 2004 là điều ước quốc tế đa phương đầu tiên về tương trợ tư pháp trong lĩnh vực hình sự giữa các quốc gia Đông Nam Á, thể hiện sự quyết tâm chung của các nước ASEAN trong hợp tác phòng, chống tội phạm trong khu vực, nhất là tội phạm mang tính chất quốc tế, tội phạm xuyên quốc gia nhưng trong đó chưa đề cập các nội dung về hài hoà hoá hình phạt giống như cách thức của EU. Chính vì vậy, trong thời gian tới, với vai trò Chủ tịch ASEAN, Việt Nam cần chủ động nỗ lực bàn bạc, thảo luận, đề xuất các giải pháp khả thi và đưa ra sáng kiến với các nước thành viên ASEAN để điều chỉnh vấn đề này./.

TÀI LIỆU THAM KHẢO

1. Bande Lewis, “Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities”, *International Journal of Cyber Criminology*, volume 05, 2018.
2. Computer Misuse Act, https://www.unodc.org/res/cld/document/computer-misuse-act_html/Brunei_Computer_Misuse.pdf
3. Computer Crime Act B.E 2550 (2007), <https://www.samuihorsale.com/law-texts/computer-crime-act.html>
4. Phạm Hồng Hạnh, “Cơ chế đảm bảo thực thi pháp luật của Liên minh châu Âu và một số kinh nghiệm đối với ASEAN”, *Tạp chí Luật học*, số 9/2016.
5. <https://dictionary.cambridge.org/vi/dictionary/english/harmonize>
6. Republic Act No. 10175, <https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/>
7. Schjolberg Stein, “The history of global harmonization on cybercrime legislation—the road to geneva”, *Journal of International Commercial Law and Technology*, volume 1.12, 2008.
8. Schjolberg, Judge Stein, and Amanda M. Hubbard, “Harmonizing National Legal Approaches on Cybercrime”, *International Telecommunication Union*, volume (1 July 2005) 6.
9. Shkempi, Aldo, Indrit Shtupi, and Arjan Qafa, “The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation”, *Academic Journal of Interdisciplinary Studies*, volume 5.1, 2016.
10. Văn phòng Quốc hội, “Hài hòa pháp luật trong xây dựng Cộng đồng Asean – Những vấn đề đặt ra với Việt Nam qua kinh nghiệm từ EU”, Kỷ yếu Hội thảo quốc tế, tháng 7/2015.

(21). Danh mục các hiệp định xem tại: <https://lanhsuvietnam.gov.vn/Lists/BaiViet/B%C3%A0i%20vi%E1%BA%Bf/DispForm.aspx?List=dc7c7d75%2D6a32%2D4215%2Dafeb%2D47d4bee70eee&ID=414>, truy cập 13/12/2020.