BỘ GIÁO DỤC VÀ ĐÀO TẠO **BỘ TƯ PHÁP**

TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

ĐỖ QUÍ HOÀNG

PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO - NHỮNG VẤN ĐỀ ĐẶT RA ĐỐI VỚI VIỆT NAM

LUẬN ÁN TIẾN SỸ LUẬT HỌC

Hà Nội – 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO **BỘ TƯ PHÁP**

TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

ĐỖ QUÍ HOÀNG

PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO - NHỮNG VẤN ĐỀ ĐẶT RA ĐỐI VỚI VIỆT NAM

Chuyên ngành: Luật quốc tế

Mã số: 9 38 01 08

LUẬN ÁN TIẾN SỸ LUẬT HỌC

Người hướng dẫn khoa học: **GS. TS. Trung Tướng. Nguyễn Ngọc Anh**

PGS. TS. Nguyễn Thị Kim Ngân

Hà Nội - 2021

LỜI CAM ĐOAN

* * *

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các số liệu và trích dẫn nêu trong luận án đảm bảo độ tin cậy, chính xác và trung thực. Những kết luận khoa học của luận án chưa được công bố trong bất kỳ công trình nào khác.

TÁC GIẢ LUẬN ÁN

DANH MỤC CÁC TỪ VIẾT TẮT

* * *

ASEAN	: Hiệp hội các nước Đông Nam Á
BLHS	: Bộ luật Hình sự
BLTTHS	: Bộ luật Tố tụng hình sự
CAND	: Công an nhân dân
CNTT	: Công nghệ thông tin
DDOS	: Tấn công từ chối dịch vụ phân tán
ĐƯQT	: Điều ước quốc tế
ICJ	: Tòa án công lý quốc tế Liên hợp quốc
ILC	: Ủy ban Luật quốc tế
INTERPOL	: Tổ chức Cảnh sát hình sự quốc tế
IoT	: Internet of Things – Kết nối vạn vật
LHQ	: Liên hợp quốc
PCTP	: Phòng chống tội phạm
QGTV	: Quốc gia thành viên
TAND	: Tòa án nhân dân
TPCNC	: Tội phạm công nghệ cao
TTTP	: Tương trợ tư pháp
UBND	: Ủy ban nhân dân
USD	: Đô la Mỹ
VKSND	: Viện kiểm sát nhân dân
VPPL	: Vi phạm pháp luật

MỤC LỤC

Trang

MỞ ĐẦU 6
1. Tính cấp thiết của đề tài 6
2. Đối tượng và phạm vi nghiên cứu của luận án 8
3. Mục đích và nhiệm vụ nghiên cứu của luận án 9
4. Phương pháp luận và phương pháp nghiên cứu 9
5. Ý nghĩa khoa học và tính mới của luận án 10
6. Câu hỏi nghiên cứu và giả thuyết nghiên cứu 10
7. Kết cấu của luận án 12
CHƯƠNG 1 TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU NHỮNG VẤN ĐỀ LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN 13
1.1. Nhóm công trình nghiên cứu tổng quan về tội phạm công nghệ cao và nhận diện các loại hình tội phạm công nghệ cao 14
1.1.1. Các công trình nghiên cứu của nước ngoài 14
1.1.2. Các công trình nghiên cứu của Việt Nam 17
1.2. Nhóm công trình nghiên cứu về pháp luật quốc tế và hợp tác đấu tranh phòng chống tội phạm công nghệ cao 18
1.2.1. Các công trình nghiên cứu của nước ngoài 18
1.2.2. Các công trình nghiên cứu của Việt Nam 21
1.3. Nhóm công trình nghiên cứu về pháp luật và thực tiễn đấu tranh phòng chống tội phạm công nghệ cao tại một số quốc gia, khu vực và những vấn đề liên quan đến Việt Nam 22
1.3.1. Các công trình nghiên cứu của nước ngoài 22
1.3.2. Các công trình nghiên cứu của Việt Nam 24
1.4. Đánh giá tình hình nghiên cứu các vấn đề liên quan đến đề tài luận án .. 27
1.5. Những vấn đề cần tiếp tục được nghiên cứu trong luận án 30
TIỂU KẾT CHƯƠNG 1 32
CHƯƠNG 2 MỘT SỐ VẤN ĐỀ LÝ LUẬN VỀ TỘI PHẠM CÔNG NGHỆ CAO VÀ PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO 33
2.1. Khái niệm tội phạm công nghệ cao và hợp tác đấu tranh, phòng chống tội phạm công nghệ cao 33
2.1.1. Khái niệm tội phạm công nghệ cao 33

2.1.2. Khái niệm hợp tác đấu tranh phòng chống tội phạm công nghệ cao. 40
2.2. Lý luận pháp luật quốc tế trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao 52
2.2.1. Định nghĩa và đặc điểm của pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao 52
2.2.2. Nguồn của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao 55
2.2.3. Nguyên tắc của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao 58
2.2.4. Nội dung của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao 63
2.2.5. Vai trò của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao 65
TIỂU KẾT CHƯƠNG 2..... 68
CHƯƠNG 3 NỘI DUNG PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH, PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO VÀ THỰC TIỄN THỰC HIỆN CỦA MỘT SỐ QUỐC GIA 70
3.1. Pháp luật quốc tế quy định nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luậtvà hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao 70
3.1.1. Hài hoà hoá pháp luật của các quốc gia trong phòng chống tội phạm công nghệ cao 70
3.1.2. Xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động ứng phó với tội phạm công nghệ cao 77
3.2. Tương trợ tư pháp hình sự 79
3.2.1. Nội dung tương trợ tư pháp hình sự 79
3.2.2. Thủ tục, thể thức tương trợ tư pháp 83
3.3. Dẫn độ 84
3.3.1. Điều kiện, thể thức dẫn độ 84
3.3.2. Điều kiện dẫn độ, các trường hợp không dẫn độ 88
3.4. Chuyển giao người bị kết án 90
3.5. Xác định thẩm quyền tài phán..... 92
3.6. Thực tiễn thực hiện pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao của một số quốc gia 99

3.6.1. Cộng hòa Liên bang Đức 99
3.6.2. Hoa Kỳ 104
3.6.3. Nhật Bản 108
3.6.4. Một số bài học kinh nghiệm đối với Việt Nam 112
TIỂU KẾT CHƯƠNG 3..... 116
CHƯƠNG 4 PHÁP LUẬT VÀ THỰC TIỄN HỢP TÁC QUỐC TẾ ĐẤU TRANH, PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO CỦA VIỆT NAM 118
4.1. Thực trạng pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao ở Việt Nam 118
4.1.1. Khái quát về tội phạm công nghệ cao ở Việt Nam 118
4.1.2. Nội dung pháp lý cho hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao của Việt Nam 124
4.2. Thực tiễn thực thi pháp luật trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao của Việt Nam 144
4.2.1. Kết quả hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao trong thời gian vừa qua 144
4.2.2. Hạn chế trong hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao 154
4.3. Giải pháp hoàn thiện pháp luật và nâng cao hiệu quả hợp tác quốc tế trong đấu tranh phòng, chống tội phạm công nghệ cao của Việt Nam 159
4.3.1. Giải pháp hoàn thiện pháp luật Việt Nam về đấu tranh phòng chống tội phạm công nghệ cao 159
4.3.2. Hoàn thiện pháp luật Việt Nam trong hợp tác quốc tế trong đấu tranh phòng, chống tội phạm công nghệ cao 161
4.3.3. Nhóm giải pháp nâng cao hiệu quả hợp tác quốc tế phòng chống tội phạm sử dụng công nghệ cao 163
TIỂU KẾT CHƯƠNG 4..... 169
KẾT LUẬN CHUNG 171
DANH MỤC TÀI LIỆU THAM KHẢO
DANH MỤC CÔNG TRÌNH NCKH ĐÃ CÔNG BỐ CÓ LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN TIẾN SĨ

MỞ ĐẦU

* * *

1. Tính cấp thiết của đề tài

Thế kỷ XXI, với sự phát triển của khoa học kỹ thuật, sự bùng nổ của công nghệ cao và những sản phẩm ứng dụng công nghệ mới đã đem lại nhiều tiện ích cho cuộc sống con người, đồng thời thu hẹp khoảng cách giữa các quốc gia một cách nhanh chóng. Đặc biệt, các công nghệ truyền thông Internet cũng như hệ thống thông tin điện tử, trực tuyến, các website của các tổ chức, đơn vị, doanh nghiệp đều được đầu tư mạnh mẽ, góp phần tăng cường mối quan hệ, giao lưu, hợp tác phát triển ở nhiều lĩnh vực, nhất là lĩnh vực kinh tế, văn hóa xã hội, khoa học công nghệ, y tế, giáo dục, giải trí... Có thể nói, sự bùng nổ của khoa học kỹ thuật mặc dù đã đem lại nhiều thuận lợi cho quá trình giao lưu hợp tác quốc tế nhưng cũng tạo điều kiện cho các loại tội phạm phát triển. Sự phát triển của tội phạm không chỉ mở rộng ở phạm vi, mức độ thiệt hại mà hành vi phạm tội cũng ngày một tinh vi hơn khi tội phạm ứng dụng các công nghệ mới trong phương thức thực hiện; điều này gây ảnh hưởng to lớn cũng như gây ra sự lo ngại cho không chỉ một quốc gia mà cho toàn thể cộng đồng quốc tế.

Ngoài tính chất tổ chức chặt chẽ thường thấy, giờ đây cùng với sự phát triển vượt bậc của khoa học công nghệ, phương thức và thủ đoạn phạm tội của loại tội phạm công nghệ cao ngày càng đa dạng hơn, tinh vi hơn, kín đáo hơn và có sự thay đổi liên tục nhằm lẩn tránh sự phát hiện của các cơ quan chức năng. Chưa dừng lại ở đó, tội phạm công nghệ cao diễn ra trên hầu hết các lĩnh vực hợp tác giữa các chủ thể gây ra thiệt hại vô cùng lớn, ảnh hưởng nghiêm trọng đến an ninh mỗi quốc gia cũng như an ninh tập thể.

Thực tiễn hiện nay, pháp luật quốc tế chưa có một cơ sở pháp lý đủ toàn diện và điều chỉnh thống nhất đối với các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao. Tuy nhiên, cộng đồng quốc tế cũng đã bắt đầu nhận thấy sự cần thiết phải có một văn kiện pháp lý quốc tế trong việc tạo ra một khuôn khổ hợp tác chung và hiệu quả trong lĩnh vực hợp tác đấu tranh, phòng chống loại tội phạm nguy hiểm này. Vào năm 2000, tại Palermo, Italia, Công ước của Liên Hợp Quốc về chống tội phạm có tổ chức xuyên quốc gia đã được đàm phán và thông qua vào năm 2000 (Còn được gọi tên là Công ước Palermo năm 2000) và có hiệu lực từ ngày 29 tháng 9 năm 2003. Đây là Công ước quốc tế đầu tiên ở cấp độ đa phương toàn cầu về chống loại tội phạm có tổ chức xuyên quốc gia. Mặc dù Công ước Palermo không trực tiếp điều chỉnh các vấn đề trong hợp tác đấu tranh phòng chống tội

phạm công nghệ cao nhưng ở một góc độ nào đó, giữa tội phạm có tổ chức xuyên quốc gia và tội phạm công nghệ cao đều tồn tại những nét tương đồng nhất định. Chính vì vậy, Công ước Palermo mặc dù chưa thực sự quy định một cách cụ thể nhưng vẫn được coi như là một trong những công cụ pháp lý đầu tiên có đề cập đến vấn đề này.

Cùng với Công ước Palermo, trong Liên minh châu Âu, Công ước về tội phạm mạng (Convention on Cyber Crime), còn được gọi là Công ước Budapest về tội phạm mạng, là văn bản pháp lý quốc tế đầu tiên nhằm giải quyết tội phạm Internet và máy tính bằng cách hài hoà hóa pháp luật mỗi quốc gia thành viên, cải tiến kỹ thuật điều tra và tăng cường hợp tác giữa các quốc gia trong khu vực.

Tại Việt Nam, tội phạm công nghệ cao là loại tội phạm mới xuất hiện trong những năm gần đây nhưng lại có sự gia tăng ngày càng nhanh cả về số lượng, tính chất nguy hiểm và mức độ thiệt hại. Trong lĩnh vực an ninh quốc gia, các thế lực thù địch và phản động quốc tế đã không ngừng lợi dụng kênh truyền thông qua mạng xã hội, mạng Internet để xuyên tạc, vu khống chống phá các chủ trương, đường lối, chính sách, pháp luật của Đảng và Nhà nước; kêu gọi tập hợp lực lượng nhằm mục đích gây rối, nhất là trước và trong các sự kiện chính trị quan trọng của đất nước. Bên cạnh đó, tình trạng tội phạm sử dụng công nghệ cao thông qua mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số để chiếm đoạt tài sản; mua bán các loại thiết bị, phần mềm có chức năng nghe lén cuộc gọi thoại, trộm cắp thông tin cá nhân trong điện thoại di động; tình trạng đánh bạc trực tuyến và cá độ bóng đá qua mạng Internet... diễn biến rất phức tạp, khó lường.

Xuất phát từ thực trạng và những hậu quả mà tội phạm công nghệ cao đã gây ra trên thực tế, có thể nhận thấy, tội phạm công nghệ cao có một số điểm đặc thù, tạo ra sự khác biệt đối với các loại hình tội phạm có tính chất quốc tế khác như: hành vi phạm tội liên quan đến việc sử dụng các thiết bị điện tử có kết nối mạng (chủ yếu là máy tính, thiết bị số...); chủ thể thực hiện hành vi phạm tội là những người có tri thức, có khả năng cập nhật, tiếp cận nhanh và có kỹ năng thành thạo về công nghệ thông tin và đặc biệt, tội phạm công nghệ cao thường gây ra những hậu quả rất nặng nề về mặt kinh tế cũng như khó tính toán được thiệt hại cụ thể về sau... Vì vậy, quá trình hợp tác trong hệ thống an ninh đòi hỏi phải được thực hiện ở một mức độ cao; cùng với đó, yêu cầu trong việc kết nối thông tin, chia sẻ thông tin để nhận diện tội phạm cũng được đặt ra. Sẽ không thể trừng trị được loại tội phạm này nếu như không có sự hợp tác ở một cấp độ toàn diện. Trên thực tế, đa phần các trường hợp xâm phạm dữ liệu an ninh quốc gia đều được tiến hành bởi các phần tử

trước đây đã từng có thời gian phục vụ trong các cơ quan của chính quyền (vụ Edward Snowden hay vụ Wikileaks)[1]. Cùng với đó, trong cơ chế hợp tác, trình độ chuyên môn nghiệp vụ về công nghệ thông tin của đội ngũ phòng chống loại tội phạm này cũng cần phải được nâng cấp và cập nhật thường xuyên; đảm bảo năng lực phòng và chống các loại tội phạm công nghệ cao trong tương lai.

Xuất phát từ những lý do nêu trên nên việc nghiên cứu, làm rõ thêm các quy định của pháp luật quốc tế liên quan đến tội phạm công nghệ cao cũng như hoạt động hợp tác đấu tranh phòng chống loại tội phạm này trên thực tế là việc làm đặc biệt cần thiết, nhất là khi đặt nó trong bối cảnh của cuộc cách mạng công nghiệp 4.0 hiện nay. Để từ đó, rút ra được những giá trị tham khảo đối với Việt Nam trong quá trình hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

2. Đối tượng và phạm vi nghiên cứu của luận án

Đối tượng và phạm vi nghiên cứu của luận án tập trung vào những vấn đề pháp lý quốc tế về tội phạm công nghệ cao cũng như hoạt động hợp tác đấu tranh đối với loại hình tội phạm này. Theo đó:

Đối tượng nghiên cứu của đề tài luận án bao gồm:

- Những vấn đề lý luận về tội phạm công nghệ cao và hoạt động hợp tác đấu tranh, phòng chống loại hình tội phạm công nghệ cao; phân biệt và nhận diện tội phạm công nghệ cao với các tội phạm khác có liên quan.

- Các quy định của pháp luật quốc tế và pháp luật một số quốc gia tiêu biểu về tội phạm công nghệ cao cũng như hoạt động hợp đấu tranh, phòng chống loại hình tội phạm công nghệ cao trong bối cảnh hiện nay.

- Thực trạng tội phạm công nghệ cao trên thế giới cũng như hoạt động hợp tác đấu tranh phòng chống tội phạm công nghệ cao. Qua đó, đề tài luận án cũng sẽ rút ra một số kinh nghiệm và giá trị tham khảo đối với Việt Nam.

- Cơ sở pháp lý và thực tiễn hoạt động hợp tác đấu tranh tội phạm công nghệ cao tại Việt Nam. Một số dự báo, giải pháp, phương hướng cho công tác phòng chống loại hình tội phạm này trong tình hình mới.

Trên cơ sở phân tích nội dung của những đối tượng nghiên cứu nêu trên, phạm vi nghiên cứu của đề tài luận án bao gồm:

- Nhận diện và phân biệt một số thuật ngữ có liên quan đến tội phạm công nghệ cao, đưa ra và phân tích những cách tiếp cận về tội phạm công nghệ cao qua đó xây dựng một định nghĩa chung về tội phạm công nghệ cao, đặc điểm và phân loại loại hình tội phạm này.

[1]Xem https://iuscogens-vie.org/2019/04/15/130/ (truy cập lần cuối ngày 8/5/2020)

- Nội dung các quy định của pháp luật quốc tế và pháp luật một số quốc gia về tội phạm công nghệ cao; các quy định điều chỉnh hoạt động hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

- Thực trạng và pháp luật Việt Nam về tội phạm công nghệ cao và công tác hợp tác đấu tranh phòng chống tội phạm công nghệ cao trong bối cảnh hiện nay. Trên cơ sở đó đưa ra phương hướng, giải pháp đối với Việt Nam trong thời gian tới.

3. Mục đích và nhiệm vụ nghiên cứu của luận án

Mục đích của luận án là làm rõ các vấn đề lý luận-pháp lý của tội phạm công nghệ cao cũng như các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống loại tội phạm này; đồng thời làm rõ các quy định, thực tiễn thực thi của Việt Nam, trên cơ sở đó, đưa ra một số dự báo và đề xuất những giải pháp hoàn thiện pháp luật, nâng cao hiệu quả của hoạt động thực thi pháp luật tại Việt Nam liên quan đến tội phạm công nghệ cao.

Để đạt được những mục đích trên, đề tài sẽ tập trung giải quyết các nhiệm vụ sau:

- Phân tích, nghiên cứu những vấn đề lý luận về tội phạm công nghệ cao và các nội dung, nguyên tắc, vai trò, nguồn của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao;

- Phân tích, đánh giá các quy định của pháp luật quốc tế, việc thực hiện pháp luật quốc tế về tội phạm công nghệ cao ở một số quốc gia. Qua đó, rút ra được một số kinh nghiệm và giá trị tham khảo đối với Việt Nam;

- Bình luận, đánh giá các quy định và thực tiễn quá trình thực thi pháp luật về tội phạm công nghệ cao của Việt Nam, qua đó, đề xuất những giải pháp và phương hướng hoàn thiện pháp luật nhằm tăng cường hiệu quả của hoạt động thực thi pháp luật trong lĩnh vực hợp tác đấu tranh, phòng chống tội phạm công nghệ cao.

4. Phương pháp luận và phương pháp nghiên cứu

Đề tài luận án được thực hiện trên cơ sở phương pháp luận khoa học của chủ nghĩa Mác - Lênin, vận dụng kết hợp các quan điểm của chủ nghĩa duy vật biện chứng và chủ nghĩa duy vật lịch sử. Ngoài ra, các phương pháp nghiên cứu cụ thể cũng được sử dụng trong luận án, ví dụ như: diễn dịch-quy nạp (chương 2 và chương 3), phân tích (chương 2, chương 3 và chương 4), tổng hợp (chương 3 và chương 4), so sánh (chương 2, chương 3 và chương 4), hệ thống hoá-khái quát hoá (chương 2, chương 3 và chương 4)...

Bên cạnh đó, luận án cũng được tiến hành trên cơ sở quán triệt sâu sắc các quan điểm về đường lối lãnh đạo của Đảng Cộng Sản và Nhà nước Cộng hòa xã hội

chủ nghĩa Việt Nam, đặc biệt là quan điểm và định hướng của Đảng đối với công tác phòng, chống tội phạm trong tình hình mới và Chiến lược quốc gia phòng, chống tội phạm đến năm 2020.

5. Ý nghĩa khoa học và tính mới của luận án

Luận án là công trình khoa học nghiên cứu một cách toàn diện các vấn đề lý luận, pháp lý về quá trình hình thành và phát triển của tội phạm công nghệ cao cũng như các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống loại tội phạm này; đồng thời làm rõ các quy định, thực tiễn thực thi của Việt Nam, trên cơ sở đó, đề xuất những giải pháp hoàn thiện pháp luật và nâng cao hiệu quả của hoạt động thực thi pháp luật tại Việt Nam liên quan đến tội phạm công nghệ cao. Luận án đã có những đóng góp mới về mặt khoa học như sau:

- Thứ nhất, luận án đã phân tích, tổng hợp những vấn đề lý luận về tội phạm công nghệ cao và các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao. Qua đó đã xây dựng khái niệm tội phạm công nghệ cao cũng như làm rõ những đặc điểm của loại hình tội phạm này trên cơ sở đối sánh với các thuật ngữ khác có liên quan.

- Thứ hai, luận án đã đánh giá các quy định của pháp luật quốc tế, thực tiễn thực hiện pháp luật quốc tế về tội phạm công nghệ cao của một số quốc gia điển hình. Qua đó, rút ra được một số kinh nghiệm và giá trị tham khảo đối với Việt Nam.

- Thứ ba, luận án đã bình luận, đánh giá các quy định và thực tiễn quá trình thực thi pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao của Việt Nam, qua đó, đề xuất những giải pháp và phương hướng hoàn thiện pháp luật nhằm tăng cường hiệu quả của hoạt động thực thi pháp luật trong lĩnh vực hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao.

6. Câu hỏi nghiên cứu và giả thuyết nghiên cứu

Trước khi triển khai nghiên cứu đề tài luận án tiến sĩ, nghiên cứu sinh đã tự đặt ra một số câu hỏi nghiên cứu, bao gồm:

- Câu hỏi mang tính mô tả: Tội phạm công nghệ cao là gì? Loại tội phạm này được quy định ở những cấp độ và phạm vi nào? Liên quan đến tội phạm công nghệ cao, có những cách tiếp cận và cách thức sử dụng thuật ngữ như thế nào? Thực trạng các loại tội phạm này diễn ra trên thực tế ra sao? Tỷ lệ tương quan giữa các loại tội xảy ra là bao nhiêu? Tần suất của loại tội nào phổ biến trên thực tế; Các nội dung trong hoạt động đấu tranh và hợp tác phòng chống loại tội phạm này là gì? Hiệu quả trên thực tế đến đâu? .v.v...

- Câu hỏi mang tính so sánh và nhân-quả: so sánh để chỉ ra được điểm giống và khác nhau giữa tội phạm công nghệ cao với các loại hình tội phạm khác; sau khi so sánh, tội phạm công nghệ cao có mối liên hệ như thế nào đối với các loại hình tội phạm khác đó? Liệu rằng, đây là một loại hình tội phạm mới hay chỉ là biến thể của các loại hình tội phạm truyền thống? So sánh kinh nghiệm và thực tiễn pháp luật của một số quốc gia phát triển trong vấn đề phòng chống tội phạm công nghệ cao? Rút ra một số bài học kinh nghiệm và liên hệ với Việt Nam? .v.v…

Xuất phát từ những câu hỏi nghiên cứu, nghiên cứu sinh đưa ra một nhận định sơ bộ ban đầu mang tính giả thuyết nghiên cứu, đó là:

- Tội phạm công nghệ cao là một loại hình tội phạm phát sinh trong thời đại công nghệ thông tin, với nhiều đặc điểm tương đồng với các loại tội phạm có tính chất quốc tế hay tội phạm có tổ chức xuyên quốc gia, mức độ nguy hiểm và hậu quả khôn lường hơn rất nhiều so với các loại tội phạm truyền thống. Chính vì vậy, cần thiết trong việc nghiên cứu điều chỉnh và chung tay giải quyết thông qua hợp tác quốc tế (Giả thuyết 1)

- Tội phạm công nghệ cao chỉ là sự biến thể của các loại tội phạm truyền thống nên chỉ cần hoàn thiện các quy định của pháp luật quốc gia để phòng chống loại tội phạm này (Giả thuyết 2)

- Phương thức hợp tác quốc tế có vai trò quyết định trong quá trình đấu tranh phòng chống loại hình tội phạm công nghệ cao (Giả thuyết 3)

Qua quá trình tìm hiểu, nghiên cứu sinh bác bỏ giả thuyết số 2 và tập trung đi vào phát triển và chứng minh Giả thuyết 1 và 3. Đồng thời, nghiên cứu sinh đưa ra Luận đề chính cho Công trình nghiên cứu của mình như sau: "*Trong bối cảnh hiện nay, tội phạm công nghệ cao vừa là một thách thức vừa là một sản phẩm mới của thời đại cùng với những tác động tiêu cực vô cùng lớn tới mỗi cá nhân, pháp nhân, quốc gia hay thậm chí của cả cộng đồng; chính vì thế, cơ sở pháp lý, nội dung và phương thức hợp tác quốc tế trong quá trình đấu tranh loại tội phạm này cũng có nhiều nét đặc thù và rất cần đến sự tận tâm, thiện chí của các chủ thể trên thực tế*".

Xoay quanh luận đề chính, nghiên cứu sinh đã thiết kế hệ thống lập luận để chứng minh cho luận đề chính của mình. Ngoài các lập luận này, nghiên cứu sinh còn sử dụng thêm "lập luận dữ liệu" - đây là những số liệu, bảng biểu, bằng chứng thực tế hay các dẫn chứng thực tiễn và có trích dẫn bằng các nguồn xác thực, đáng tin cậy... Kết hợp tất cả những lập luận này để minh chứng cho luận đề chính của luận án tiến sĩ của mình (xem cụ thể trong các phần sau của luận án).

7. Kết cấu của luận án

Ngoài phần mở đầu và kết luận, cấu trúc của luận án bao gồm 4 chương:

- Chương 1: Tổng quan tình hình nghiên cứu những vấn đề liên quan đến đề tài luận án;

- Chương 2: Một số vấn đề lý luận về tội phạm công nghệ cao và pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

- Chương 3: Nội dung pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao và thực tiễn thực hiện của một số quốc gia.

- Chương 4: Pháp luật và thực tiễn hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao của Việt Nam.

CHƯƠNG 1
TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU NHỮNG VẤN ĐỀ LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN

* * *

Cuộc cách mạng công nghiệp lần thứ 4.0 không chỉ đơn thuần là một xu thế tất yếu mà nó đã trở thành thực tiễn sôi động diễn ra tại hầu khắp các quốc gia trên thế giới cũng như trên phạm vi toàn cầu. Bên cạnh những lợi ích to lớn đưa lại, chính nó cũng đem đến những thách thức an ninh phi truyền thống không hề nhỏ đối với mỗi quốc gia, khu vực. Không giống với các cuộc cách mạng trước đó, cuộc cách mạng công nghiệp lần thứ 4.0 bắt buộc mỗi cá nhân, mỗi quốc gia hay mỗi thể chế phải thay đổi nếu như không muốn bị tụt lại phía sau.

Kể từ cuối những năm 90, đầu những năm 2000 cho đến nay, thuật ngữ "*tội phạm công nghệ cao*" thường xuyên được đề cập đến với tần suất tăng dần trên cả bình diện pháp lý-thực tiễn, trên nhiều cấp độ từ quốc tế, khu vực cho đến quốc gia và đã trở thành đối tượng khảo cứu trong nhiều công trình nghiên cứu khoa học của các tác giả khác nhau ở nước ngoài cũng như tại Việt Nam. Xét về mặt thuật ngữ, tội phạm công nghệ cao được các học giả trong và ngoài nước đề cập tới thông qua một số dạng thức như tội phạm mạng (Cyber crimes); tội phạm máy tính (Computer crimes); tội phạm liên quan đến máy tính (Computer-Related Crimes); tội phạm hình sự công nghệ (Techno-Cyber criminals/Hightech Crimes); tội phạm ảo (Online crimes or E-crimes); tội phạm điện tử (Electronic crimes)...

Về hình thức thể hiện, phạm trù "*tội phạm công nghệ cao*" được nghiên cứu thông qua các thể loại như sách chuyên khảo, luận văn, luận án, các bài báo đăng trên các tạp chí chuyên ngành, đề tài nghiên cứu khoa học hay bài viết hội thảo khoa học... Một cách tổng thể, những công trình này đã bước đầu "xới" lên được một lĩnh vực nghiên cứu còn tương đối mới mẻ và phức tạp do tính chất đa ngành của vấn đề.

Nghiên cứu các công trình liên quan trực tiếp đến đề tài luận án, có thể khái quát hóa thành ba nhóm chính:

Thứ nhất, nhóm công trình nghiên cứu tổng quan về tội phạm công nghệ cao và nhận diện các loại hình tội phạm công nghệ cao;

Thứ hai, nhóm công trình nghiên cứu về pháp luật quốc tế và hợp tác đấu tranh phòng chống tội phạm công nghệ cao;

Thứ ba, nhóm công trình nghiên cứu về pháp luật và thực tiễn đấu tranh phòng chống tội phạm công nghệ cao tại một số quốc gia, khu vực và những vấn đề liên quan đến Việt Nam.

1.1. Nhóm công trình nghiên cứu tổng quan về tội phạm công nghệ cao và nhận diện các loại hình tội phạm công nghệ cao

1.1.1. Các công trình nghiên cứu của nước ngoài

Trong các công trình nghiên cứu của nước ngoài, trước tiên có thể đề cập đến một số cuốn sách tham khảo tiêu biểu về tội phạm công nghệ cao, điển hình là Cuốn sách "*Cybercrime (True Crime)*" của John Townsend (xuất bản năm 2004, nhà xuất bản Raintree Publishers, Oxford, Vương Quốc Anh). Trong tác phẩm của mình, tác giả John Townsend đã đưa ra những khía cạnh cả về pháp lý-kỹ thuật về cách thức mà các loại hình tội phạm công nghệ cao hoạt động và gây thiệt hại cho các cá nhân, công ty hay thậm chí là các quốc gia. Không dừng lại ở đó, cuốn sách đã dành phần lớn dung lượng để đi vào phân loại và phân tích một số loại hình tội phạm cụ thể như: tin tặc (Hacking), tội phạm sử dụng máy tính để lừa đảo (Computer Fraud), tội phát tán vi rút và phần mềm độc hại (Viruses) và gian lận trên mạng (Internet scams)... Cuốn sách là tài liệu bổ trợ tốt cho những ai chưa hiểu rõ cách thức vận hành của những loại hình tội phạm công nghệ cao cụ thể đang hoạt động trên thực tế hiện nay.

Với tiêu đề "*Cybercrime: The Transformation of Crime in the Information Age*" (xuất bản năm 2007 bởi Polity Press, Vương quốc Anh), cuốn sách của tác giả David Wall không chỉ là một cuốn sách chuyên khảo cung cấp các kiến thức đơn thuần về các loại hình tội phạm mạng hay cách thức phòng chống loại hình tội phạm này; thông qua 10 chương của cuốn sách, độc giả sẽ có được những khám phá thực sự về sự biến chuyển cả trong bản chất hành vi cũng như phạm vi, mức độ của tội mạng mạng trong kỷ nguyên công nghệ thông tin. Cuốn sách đi vào lý giải từ những vấn đề cụ thể nhất (như tội phạm mạng là gì, tại sao lại gọi là tội phạm mạng; tội phạm mạng có nguồn gốc từ đâu.v.v...) cho đến những nội dung mang tính chất định hướng như việc đưa ra những dự báo cũng như tính cấp thiết của việc cải cách chính sách, pháp luật của mỗi quốc gia và sự điều chỉnh của luật pháp quốc tế hiện nay đối với loại hình tội phạm này. Cuốn sách cũng khẳng định tội phạm mạng là một dạng thức đã được biến đổi của các loại hình tội phạm truyền thống (new forms of traditional crime) và tội phạm mạng là sản phẩm của con người trong kỷ nguyên công nghệ thông tin (the product of network technologies in the information age).

Một cuốn sách đáng chú ý tiếp theo đó là cuốn "*Encyclopedia of Cybercrime*" của tác giả Samuel C. McQuade (xuất bản năm 2008 bởi nhà xuất bản Greenwood Press, Westport, Connecticut, Hoa Kỳ). Đây có thể được coi là cuốn bách khoa toàn tư đầu tiên về tội phạm mạng - một dạng thức phổ biến của tội phạm công nghệ cao. Đúng với tính chất của một cuốn bách khoa toàn thư, cuốn sách đề cập và phân loại một cách toàn diện các loại hình tội phạm mạng, bao gồm: thuật ngữ, định nghĩa và cấu trúc xã hội của tội phạm mạng; tác giả cũng đề cập đến dạng thức tội phạm khai thác lỗ hổng bảo mật cơ sở hạ tầng quốc gia - một trong những loại hình tội phạm gây thiệt hại đặc biệt nghiêm trọng đối với các lợi ích, an ninh của quốc gia (trong đó cuốn sách có đặc biệt đề cập đến vụ việc Julian Assange - ông trùm của trang web www.Wikileaks.org). Ngoài ra, cuốn sách cũng tập trung làm rõ các loại hình tội phạm tấn công vào máy tính và hệ thống thông tin; các hành vi xâm phạm máy tính và dữ liệu điện tử; những vấn đề mới nổi và gây tranh cãi như nội dung khiêu dâm trực tuyến, hacking và các tác động tiêu cực tiềm tàng của hoạt động trò chơi trực tuyến (games online) và triệu trứng nghiện máy tính của giới trẻ (teenager computer addict)... Mặc dù không đề cập quá sâu nhưng điểm mạnh của cuốn sách đó là có một phạm vi nghiên cứu tương đối rộng, giúp cho người đọc có thêm tri thức về các loại hình tội phạm công nghệ cao hiện nay cũng như các tác động về nhiều mặt nhất là về kinh tế-xã hội của loại hình tội phạm này đối với các quốc gia.

Cuốn sách "*Principles of Cybercrime*" - *Sencond Edition* (nhà xuất bản Cambridge University Press, Vương quốc Anh) của tác giả Jonathan Clough xuất bản năm 2015 là một trong những cuốn sách gần đây nhất đề cập đến những nguyên tắc cơ bản trong hoạt động, sự vận hành và biện pháp triệt phá loại hình tội phạm mạng. Trong lần tái bản thứ hai, cuốn sách đã cập nhật được những xu thế phát triển mới của loại hình tội phạm này cũng như đưa ra những phân tích mang tính học thuyết tổng hợp (*comprehensive doctrinal analysis of cybercrime*) về loại hình tội phạm mạng tại các quốc gia theo truyền thống pháp luật Common Law (Australia, Canada, Vương Quốc Anh và Hoa Kỳ). Một giá trị khác của cuốn sách đó chính là việc bổ sung thêm nhiều loại hình tội phạm mạng mới xuất hiện trong thời gian gần đây cũng như có thêm một chương liên quan đến việc phân định thẩm quyền tài phán đối với loại hình tội phạm này - một trong những nội dung rất ít khi được đề cập trong các công trình nghiên cứu trước đó.

Tiếp đến là một trong những cuốn sách mới được xuất bản trong thời gian gần đây đó là cuốn "*Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*" của các tác giả Joshua B. Hill and Nancy E. Marion (xuất bản

vào năm 2016 bởi nhà xuất bản ABC-CLIO Press, Hoa Kỳ). Cuốn sách đã phân loại và cập nhật thêm một số dạng thức mới của loại hình tội phạm công nghệ cao (từ những loại hình tội phạm cơ bản nhất như trộm cắp, lừa đảo có sử dụng máy tính cho đến hành vi đưa các nội dung khiêu dâm và cờ bạc trực tuyến; lừa đảo trực tuyến hay rửa tiền trên mạng cũng như hành vi lạm dụng bán hàng trực tuyến để trốn thuế...). Bên cạnh đó, cuốn sách này cũng cung cấp một cách toàn diện những thông tin về lịch sử hình thành và phát triển của tội phạm mạng. Không chỉ dừng lại ở đó, cuốn sách cũng đánh giá những nỗ lực của các chủ thể trong công tác phòng chống tội phạm mạng dưới nhiều hình thức, cấp độ khác nhau như phạm vi quốc tế, quốc gia, tiểu bang và địa phương.

Bên cạnh các sách chuyên khảo, vấn đề tội phạm công nghệ cao còn được khảo luận tới thông qua các báo cáo, bài báo, bài viết nghiên cứu riêng biệt... Có thể đề cập đến bài viết "*What is Computer Crime and Why should we care*" của tác giả Michael C. Gemignani (bài viết đăng năm 1986 trên tạp chí Little Rock Law Review, University of Arkansas, Volume 10). Là một trong những bài viết khởi xướng về vấn đề này, bài nghiên cứu bước đầu gợi mở về một dạng thức của tội phạm công nghệ cao, đó chính là tội phạm sử dụng máy tính trong quá trình phạm tội. Mặc dù mới chỉ đề cập được một vài yếu tố nhận dạng chính cũng như phân tích một số vụ việc liên quan đến tội phạm máy tính tại Hoa Kỳ nhưng bài viết đã bắt đầu tạo ra được sự quan tâm của giới nghiên cứu khoa học pháp lý tại Hoa Kỳ về chủ đề này.

Tiếp đến có thể đề cập đến bài viết của David L. Carter "*Computer Crime Categories: How Techno-Criminals Operate*" (được đăng tải trên tạp chí FBI Law Enforcement Bulletin Journal, Volume 64; Issue 7 năm 1995). Trong bài viết, tác giả David L. Carter đã phân biệt bốn dạng thức từ các loại hình tội phạm máy tính, bao gồm: tội phạm chiếm đoạt và kiểm soát máy tính (Computer As the Targe); tội phạm sử dụng máy tính như là công cụ phạm tội (Computer As the Instrumentality of the Crime); các tội phạm có liên quan đến máy tính (Crimes Associated With the Prevalence of Computers) và các loại hình tội phạm xâm phạm đến máy tính và dữ liệu một cách vô thức (Computers Incidental to Other Crimes). Bài viết cũng nhìn nhận vấn đề tội phạm công nghệ dưới cả góc độ pháp lý quốc tế và quốc gia; qua đó đưa ra những nhận định về viễn cảnh sắp tới của loại hình tội phạm này. Tác giả cũng đưa ra quan điểm riêng của mình khi cho rằng "*các quốc gia trên thế giới hiện nay không còn chạy đua bằng vũ khí, năng lượng hay tiền bạc. Cuộc chiến hiện nay*

không được quyết định bởi bên nào có nhiều vũ khí đạn dược hơn mà nó liên quan đến vấn đề quốc gia nào đang nắm giữ nhiều thông tin, bí mật hơn"...

Xuất phát từ tình hình thực tế, các công trình nghiên cứu tổng quan và nhận diện các loại hình tội phạm công nghệ cao được quan tâm khá nhiều. Ngoài những công trình tiêu biểu đã đề cập, những nghiên cứu riêng lẻ khác về tội phạm công nghệ cao có thể nhắc đến như "*The Encyclopedia of High-Tech Crime and Crime-Fighting: From Airport Security to the Zyx Computer Virus*" của Michael Newton và John L French; "*Cybercrime: How to Avoid Becoming a Victim*" của tác giả H. Thomas Milhorn; "*Cybercrime: Criminal Threats from Cyberspace*" của Susan W. Brenner;.... Tuy nhiên, các công trình này đều đưa ra những nhận định tương tự về mặt nội dung cũng như các yếu tố nhận diện tội phạm công nghệ cao và chủ yếu tập trung đánh giá tác động của các loại hình tội phạm công nghệ cao đối với một quốc gia cụ thể, thường là đối với chính quốc gia mà tác giả là công dân.

1.1.2. Các công trình nghiên cứu của Việt Nam

Bài viết "*Nhận diện tội phạm sử dụng công nghệ cao*" của tác giả Đào Văn Vạn (đăng tải trên Tạp chí Khoa học Cảnh sát nhân dân năm số 11/2015) đã chỉ ra sự thiếu nhất quán trong việc sử dụng thuật ngữ về loại hình tội phạm sử dụng công nghệ cao trong cả giới nghiên cứu và thực tiễn. Trên cơ sở phân tích các cách tiếp cận về tội phạm sử dụng công nghệ cao, tác giả đã đưa ra cách tiếp cận của riêng mình cũng như những đặc tính giúp nhận diện tội phạm sử dụng công nghệ cao trên thực tế. Qua đó, tác giả đã phân loại tội phạm có sử dụng công nghệ cao thành hai nhóm, bao gồm: nhóm tội phạm máy tính và mạng máy tính và nhóm tội phạm truyền thống có sử dụng công nghệ cao. Kết luận bài viết, tác giả nhận định rằng, sự thống nhất trong nhận thức về lý luận và thực tiễn sẽ là yếu tố quan trọng đảm bảo hiệu quả cho quá trình phát hiện, điều tra và xử lý tội phạm sử dụng công nghệ cao.

Trong bài viết "*Một số giải pháp phòng ngừa tội phạm sử dụng công nghệ cao*" của Nguyễn Ngọc Thương (Tạp chí Cảnh sát nhân dân, T32, 2017), tác giả đã phân loại một số loại hình tội phạm sử dụng công nghệ cao xuất hiện phổ biến hiện nay. Cụ thể, bài viết đã tập trung xác định rõ tám hình thức tấn công tương ứng với tám loại hình tội phạm có sử dụng công nghệ cao cụ thể, bao gồm: *Hành vi tấn công deface* (truy cập bất hợp pháp vào cơ sở dữ liệu nhằm phá hoại, sửa đổi dữ liệu, trộm cắp dữ liệu và thay đổi giao diện); *Hành vi tấn công DdoS* (làm tắc nghẽn đường truyền bằng cách cài mã điều khiển các máy tính "ma" trong mạng internet hay một địa chỉ trang web đã định trước); *Hành vi phát tán virus, phần mềm gián điệp* (phát tán các mã độc nhằm lây lan vào máy tính cá nhân để lấy thông tin cá

nhân); *Tội phạm trong thương mại điện tử* (lừa đảo qua quảng cáo, bán hàng trực tuyến; lừa đảo trên các sàn giao dịch ảo); *Tội phạm trộm cắp thông tin thẻ tín dụng* (bằng nhiều thủ đoạn có sử dụng công nghệ cao để lấy cắp thông tin cá nhân, thông tin thẻ tín dụng); *Hành vi rút cắp tiền từ thẻ ngân hàng* (thông đồng với nơi chấp nhận thẻ để rút tiền; mua hàng qua mạng bằng thông tin thẻ trộm cắp; rửa tiền với nhiều loại tiền ảo, chuyển tiền từ thẻ tín dụng trộm cắp sang tài khoản ngân hàng; dùng thẻ tín dụng trộm cắp để đánh bạc, cá độ qua mạng...); *Hành vi lừa đảo trong mua bán hàng qua mạng* (gửi thư thông báo tặng quà, hàng giá trị lớn từ nước ngoài với điều kiện phải chuyển trước một khoản phí để làm thủ tục...). Trong bài viết, tác giả cũng dành một mục nhỏ để đưa ra một số giải pháp cụ thể nhằm đấu tranh có hiệu quả với các loại hình tội phạm sử dụng công nghệ cao đang phát triển tại Việt Nam hiện nay.

Một bài nghiên cứu mới xuất hiện khá gần đây đó là bài viết "*Tội phạm mạng trong kỷ nguyên cách mạng 4.0*" của tác giả Lê Thị Hồng Xuân và Nguyễn Thị Thùy Linh được đăng tải trên tạp chí Tòa án nhân dân số 18/2018. Trong bài viết, các tác giả đã đưa ra cách tiếp cận riêng của mình về nhận dạng loại hình tội phạm mạng, tội phạm sử dụng công nghệ cao cũng như những thuộc tính bản chất của loại hình tội phạm này. Không chỉ dừng lại ở đó, bài viết còn đi sâu vào việc phân tích thực trạng, diễn biến tình hình của tội phạm sử dụng công nghệ cao. Ở phần cuối của bài viết, các tác giả kiến nghị một số giải pháp nhằm giảm thiểu và ngăn ngừa tội phạm công nghệ cao trong thời đại công nghệ 4.0 trong đó đặc biệt nhấn mạng đến việc tăng cường hợp tác quốc tế trong lĩnh vực đấu tranh phòng chống tội phạm...

Có thể nhận thấy, tại Việt Nam, các công trình nghiên cứu toàn diện về tội phạm công nghệ cao và nhận diện các loại hình tội phạm công nghệ cao chưa xuất hiện nhiều. Liên quan đến vấn đề này, các công trình hầu như mới chỉ được đề cập dưới dạng các bài viết nghiên cứu chuyên ngành, thể hiện góc nhìn riêng và quan điểm cá nhân của một số tác giả.

1.2. Nhóm công trình nghiên cứu về pháp luật quốc tế và hợp tác đấu tranh phòng chống tội phạm công nghệ cao

1.2.1. Các công trình nghiên cứu của nước ngoài

Trong các công trình nghiên cứu của nước ngoài về pháp luật quốc tế và hợp tác đấu tranh phòng chống tội phạm công nghệ cao, trước tiên có thể đề cập đến một số cuốn sách tham khảo điển hình phân tích chuyên sâu về vấn đề này, tiêu biểu là cuốn "*Cybercrime: A Reference Handbook*" (ấn phẩm nằm trong chuỗi

Contemporary World Issues Series của nhà xuất bản ABC-CLIO Press, Hoa Kỳ) của các tác giả Bernadette Hlubik Schell và Clemens Martin xuất bản năm 2004. Đây có thể coi là một trong những cuốn sách chuyên khảo đầu tiên đề cập một cách tổng quát về loại hình tội phạm mạng và những điều chỉnh của luật pháp đối với loại tội phạm này. Với 7 chương, cuốn sách đã tập trung làm rõ một số khía cạnh cơ bản như lịch sử hình thành và phát triển; các dạng thức của tội phạm mạng; các quy định của pháp luật quốc tế điều chỉnh về loại hình tội phạm này cũng như đưa ra những dự đoán và cảnh báo về chủ nghĩa tấn công mạng rất có thể dẫn đến một trào lưu của một hình thức khủng bố mới trong tương lai không xa. Không chỉ dừng lại ở đó, cuốn sách còn đi sâu hơn nữa vào việc phân tích những thực tiễn tại một số quốc gia mà điển hình là Vương quốc Anh và Hoa Kỳ. Qua đó, tập thể tác giả chỉ ra một số bất cập còn tồn tại trong hệ thống pháp luật của các nước trong quá trình loại bỏ và phòng chống loại hình tội phạm này.

Tiếp đến, phải kể tới cuốn sách "*Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research*" được biên tập bởi Ernesto U. Savona (xuất bản năm 2013 bởi nhà xuất bản Springer). Với 12 chương tương đối đồ sộ, đây cũng là một trong những công trình nghiên cứu tiêu biểu đề cập đến những điều chỉnh pháp lý quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao. Trong tác phẩm của mình, tác giả đã dành tới 3 chương (chương 3, chương 4 và chương 5) để nói về những thách thức đối với các quy định của pháp luật quốc tế khi đấu tranh chống lại tội phạm mạng - một dạng thức của tội phạm công nghệ cao. Tác giả cũng đề cập đến nguồn của pháp luật quốc tế điều chỉnh về vấn đề này cũng như tập trung làm rõ khái niệm tội phạm mạng dưới góc độ của pháp luật quốc tế. Trên cơ sở đó, tác giả đưa ra những đề xuất trong vấn đề cải tổ các quy định của pháp luật quốc gia trên cơ sở phù hợp với pháp luật quốc tế hiện có; đồng thời, đề cao công tác hợp tác quốc tế trong quá trình triệt phá loại hình tội phạm nguy hiểm này.

Cuốn sách "Computer Crime" được biên tập bởi Indira Carr (xuất bản lần đầu năm 2009 bởi Ashgate Publishing, tái bản và bổ sung năm 2016 Routledge Press) cũng là một công trình đáng chú ý. Với 4 phần, cuốn sách tập trung phân tích và làm rõ bản chất pháp lý của một trong những loại hình tội phạm công nghệ cao, đó chính là tội phạm máy tính. Tác giả đã giới thiệu nhiều góc độ của tội phạm máy tính và qua đó tìm ra mối liên hệ giữa loại tội phạm này với các quy định của pháp luật quốc tế, đặc biệt là Công ước của Ủy hội châu Âu về tội phạm mạng và Nghị định thư bổ sung của Công ước này. Trên cơ sở đó, cuốn sách đã tiếp tục đề cập đến một trong những vấn đề hóc búa liên quan đến quá trình điều tra, hợp tác quốc tế,

vấn đề phân định thẩm quyền tài phán và việc định tội loại hình tội phạm máy tính. Ở phần cuối, cuốn sách đưa ra những cảnh báo và sự cần thiết trong việc đấu tranh chống lại loại tội phạm này đặc biệt trong bối cạnh an ninh mạng luôn tiềm ẩn những nguy cơ mất an toàn trong thực tế hiện nay.

Không chỉ dừng lại ở việc thống kê các số liệu, bản báo cáo dài tới 57 trang của Trung tâm tội phạm công nghệ cao của cục Cảnh sát châu Âu Europol "*Hightech Crime within the EU: Old Crimes New Tools, New Crimes New Tools*" (2007) đã đưa ra những nhận dạng và phân loại khá cụ thể đối với loại hình tội phạm công nghệ cao tại các quốc gia của Liên minh châu Âu. Bản báo cáo đã đưa ra những thực tiễn cập nhật về tình hình tội phạm công nghệ cao tại liên minh châu Âu, đồng thời những giải pháp và những khuyến nghị cũng được cân nhắc đối với các quốc gia thành viên trong hoạt động hợp tác, đấu tranh phòng chống tội phạm thời gian tới.

Bài viết "*Cybercrime: National, Transnational, or International?*" của tác giả Ellen S. Podgor (xuất bản năm 2004 bởi Georgia State University College of Law, 50 Wayne L. Rev. 97, Hoa Kỳ) đã lần đầu tiên đặt ra vấn đề phân cấp đối với tội phạm mạng. Tác giả của bài nghiên cứu đã phân tích và đặt tội phạm mạng dưới nhiều cấp độ: cấp độ quốc gia; cấp độ khu vực và cấp độ toàn cầu. Không chỉ đơn thuần đi vào từng cấp độ, bài viết còn tiếp tục làm rõ vấn đề thẩm quyền tài phán đối với loại hình tội phạm này theo quy định tại Điều 22 của Công ước Budapest về tội phạm mạng mà Hoa Kỳ đã tham gia ký cũng như các quy định hiện có của pháp luật quốc tế liên quan đến vấn đề điều chỉnh loại hình tội phạm này.

Bài viết "*Cyber Crime: A Growing Problem*" của Tiến sĩ Rita Esen (đăng tải trên Tạp chí SAGE Journals, Vol 66, Issue 3, 2002) cũng là một công trình đưa ra được những nhận dạng và phân loại một cách tổng quan đối với loại hình tội phạm mạng. Không chỉ dừng lại ở việc phân loại, bài viết của tác giả Rita Esen còn đưa ra được những ví dụ cụ thể cho từng loại hình tội phạm cũng như phân tích những điều chỉnh pháp lý đối với tội phạm mạng theo các quy định của pháp luật Anh-Mỹ. Qua đó, tác giả nhận định rằng, cần "*giải mã*" (decode) được các loại tội phạm công nghệ cao trong đó đặc biệt là tội phạm mạng và đặc biệt nhấn mạnh, điều chỉnh pháp lý quốc tế và hợp tác giữa các quốc gia là chìa khóa cho vấn đề này.

Không giống như các bài nghiên cứu khác, bài viết "*Computer Crime - Traditional and New Values*" (đăng tải trên tạp chí Pécs Journal of International and European Law năm 2004) của tác giả Nagy Zoltan Andras bàn luận về vấn đề những giá trị truyền thống và những giá trị mới sẽ phải đối mặt với một loại hình tội

phạm - đó chính là tội phạm máy tính. Tác giả Nagy Zoltan Andras cho rằng, bên cạnh những giá trị to lớn mà máy tính đưa lại cho công việc của con người thì chính máy tính cũng sản sinh ra một thế hệ chuyên sử dụng máy tính để thực hiện các hành vi tấn công hay phạm tội. Bài viết nghiên cứu quá trình hình thành và phát triển cũng như phân biệt những dạng thức của tội phạm máy tính (Computer crimes). Đặc biệt, bài viết còn đề cập tới những điều chỉnh pháp lý quốc tế được quy định trong Công ước Budapest về tội phạm mạng và pháp luật của một số quốc gia liên quan đến loại tội phạm này (Đức, Áo, Hungary...).

Ngoài những nghiên cứu đã được nhắc đến ở trên, một số công trình khác cũng đã có đề cập về tội phạm công nghệ cao như "*High-technology-crime Investigator's Handbook: Working in the Global Information Environment*" của các tác giả Gerald L. Kovacich, William C. Boni; "*Investigating High-Tech Crime*" của tác giả Michael Knetzger và Jeremy Muraski; "*Cybercrime: The Psychology of Online Offenders*" của Grainne Kirwan, Andrew Power; "*Cybercrime Through an Interdisciplinary Lens*" được biên tập bởi Thomas J. Holt .v.v... Đây đa phần là những công trình nghiên cứu và tiếp cận về tội phạm công nghệ cao dưới giác độ của một số ngành khoa học khác như tội phạm học; khoa học điều tra tội phạm... Khía cạnh pháp lý, đặc biệt là pháp lý quốc tế không được thể hiện một cách thực sự rõ nét tại những công trình này, đa phần các công trình tiếp cận dưới góc độ của pháp luật của các quốc gia là chủ yếu.

1.2.2. Các công trình nghiên cứu của Việt Nam

Tại Việt Nam, liên quan đến vấn đề pháp luật quốc tế và hợp tác đấu tranh phòng chống tội phạm công nghệ cao, các công trình nghiên cứu còn khá khiêm tốn và hạn chế cả về quy mô cũng như mức độ nghiên cứu, chủ yếu thể hiện qua các nghiên cứu riêng lẻ đăng tải trên các trang thông tin điện tử hay các chuyên đề trong các đề tài nghiên cứu khoa học, ví dụ như bài nghiên cứu "*Hợp tác quốc tế trong phòng, chống tội phạm sử dụng công nghệ cao và vấn đề đặt ra trong công tác đào tạo, bồi dưỡng cán bộ*" của tác giả Trần Văn Doanh (trong kỷ yếu hội thảo khoa học "Phòng, chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo", Học viện CSND tháng 11/2014); "*Lịch sử phát triển hoạt động hợp tác quốc tế về nghiên cứu tội phạm học và đấu tranh phòng, chống tội phạm*" của tác giả Nguyễn Minh Đức và Nguyễn Thị Nga (đăng tải trong mục Nghiên cứu, trao đổi pháp luật trên trang thông tin điện tử của học viện cảnh sát nhân dân, truy cập lần cuối 10/10/2018); bài viết "*Khái niệm và các đặc điểm của tội phạm công nghệ thông tin - Sự khác biệt giữa tội phạm công nghệ thông tin và tội phạm thông*

thường" của tác giả Đặng Trung Hà, Vụ Pháp luật quốc tế, Bộ Tư pháp (đăng tải trên cổng thông tin điện tử của Bộ Tư pháp, truy cập lần cuối 10/10/2018)... Về cơ bản, các công trình liên quan đến vấn đề này tại Việt Nam chưa thực sự làm rõ được những khía cạnh pháp lý (đặc biệt là vấn đề pháp lý quốc tế) đối với tội phạm công nghệ cao, chưa đáp ứng được tính cấp thiết của tình hình nghiên cứu và thực tiễn hoạt động của các loại hình tội phạm công nghệ cao hiện nay.

1.3. Nhóm công trình nghiên cứu về pháp luật và thực tiễn đấu tranh phòng chống tội phạm công nghệ cao tại một số quốc gia, khu vực và những vấn đề liên quan đến Việt Nam

1.3.1. Các công trình nghiên cứu của nước ngoài

Trong các công trình nghiên cứu về pháp luật và thực tiễn đấu tranh phòng chống tội phạm công nghệ cao tại một số quốc gia, khu vực và những vấn đề liên quan đến Việt Nam, cuốn sách "*Cyber-Crime: The Challenge in Asia*" của tập thể tác giả Rod Broadhurst và Peter Grabosky (xuất bản năm 2005 bởi Hongkong University Press) là một trong những công trình hiếm hoi đề cập đến loại hình tội phạm mạng và đặt trong mối quan hệ với các quốc gia tại khu vực châu Á. Trong cuốn sách, các tác giả đã tập trung làm rõ những tác động tiêu cực về kinh tế-xã hội của loại tội hình phạm máy tính, tội phạm mạng thông qua thực tiễn tại Trung Quốc, Hồng Kông (đặc khu hành chính của Trung Quốc), Nhật Bản và Singapore. Qua đó, cuốn sách đưa ra những gợi mở đối với các quốc gia khác trong khu vực châu Á Thái Bình Dương, trong đó đặc biệt có đề cập tới các quốc gia tại Đông Nam Á – một khu vực mà cuốn sách đã nhận định là "mảnh đất màu mỡ" của loại hình tội phạm mới này ("*rich land for cybercrime in Asia*")[2]. Cuốn sách cũng đã trực tiếp đề cập tới tình hình tội phạm công nghệ cao ở Việt Nam kể từ những năm 1997 trở lại đây cũng như đưa ra những dự báo tình hình mới cho khu vực châu Á nói chung và khu vực Đông Nam Á nói riêng, trong đó có Việt Nam.

Một cuốn sách khác đó là cuốn "*Cybercrime and Security*" của tập thể tác giả Alan E. Brill, Fletcher N. Baldwin, Robert John Munro (ấn phẩm của Oceana Publications xuất bản năm 1998). Trong cuốn sách, bên cạnh việc tìm hiểu các quy định pháp luật của một số quốc gia trong liên minh châu Âu, các tác giả cũng đã khá nhiều lần nhắc tới những bất cập trong hệ thống pháp luật của các quốc gia châu Á, nhất là tình trạng "thiếu vắng" các quy định về một số nội dung như tội khiêu dâm trẻ em trên mạng; hành vi lan truyền những thông tin thất thiệt và thư rác

[2] Broadhurst, R., & Grabosky, P. (2005). Cyber-crime : The challenge in Asia. Hong Kong: Hong Kong University Press

trên mạng (spams)... Cuốn sách không chỉ nhắc tới Việt Nam mà những quốc gia tại khu vực châu Á cũng được đề cập đến như Nhật Bản, Trung Quốc hay Singapore, Malaysia, Phillipines... trong vấn đề hoàn thiện pháp luật cũng như hợp tác quốc tế nhằm loại bỏ loại hình tội phạm nguy hiểm này.

Cuốn sách "*The History of Cybercrime: 1976-2014*" (xuất bản năm 2014 bởi Cybercrime Research Institute Gmbh, CHLB Đức) của tác giả Stein Schjolberg cũng là một trong những cuốn sách có đề cập tới diễn biến của tội phạm công nghệ cao tại Việt Nam. Với 10 chương và 02 phụ lục, cuốn sách đã đi vào tìm hiểu lịch sử hình thành và phát triển của cả hai dạng thức tội phạm mạng cũng như tội phạm máy tính. Không chỉ dừng lại ở đó, cuốn sách cũng tập trung phân tích những cơ chế và thiết chế hiện nay trong việc đấu tranh phòng chống loại hình tội phạm này thông qua hoạt động của Liên Hợp Quốc, Ủy hội châu Âu, Nato, Interpol, OECD, nhóm G-8 hay các văn bản như Công ước Budapest về tội phạm mạng, Dự thảo Công ước quốc tế Stanford về tăng cường an ninh khỏi tội phạm mạng và khủng bố trên Mạng năm 2000 hay các khuyến nghị của một số tổ chức quốc tế... Liên quan đến Việt Nam, cuốn sách đã nhắc tới những nỗ lực của các quốc gia Đông Nam Á trong việc tiến tới hình thành khung pháp lý cho hoạt động hợp tác và triệt phá tội phạm công nghệ cao của khu vực. Cụ thể, cuốn sách đã đề cập đến Hội nghị Asean lần thứ 13 về tội phạm xuyên quốc gia được tổ chức tại Đà Nẵng của Việt Nam vào năm 2013. Bên cạnh những nỗ lực của Aseanapol, Việt Nam đã đề xuất thành lập những nhóm hoạt động chuyên trách về mảng tội phạm mạng. Những thực tiễn này có thể xem như những bước đi đầu tiên thể hiện quyết tâm cao của Việt Nam và khu vực trong vấn đề đấu tranh phòng chống các loại hình tội phạm công nghệ cao.

Ngoài các công trình đã đề cập, liên quan đến vấn đề pháp luật và thực tiễn đấu tranh phòng chống tội phạm công nghệ cao tại một số quốc gia, khu vực và những vấn đề liên quan đến Việt Nam, có thể kể tới một số công trình của nước ngoài như, "*Prevention and Prosecution of Computer and High Technology Crime*" của tác giả M. Bender (1988); "*Transnational Criminal Organizations, Cybercrime, and Money Laundering*" của tác giả James R. Richards (1999); "*The Internet and Governance in Asia: A Critical Reader*" xuất bản bởi Asian Media Information and Communication Centre (2007); "*Non-Traditional Security in Asia: Issues, Challenges and Framework for Action*" được biên tập bởi Mely Caballero-Anthony, Alistair D.B. Cook (2013)... Tuy nhiên, khía cạnh pháp lý trong những công trình này chưa thực sự rõ nét và chủ yếu đề cập tình hình chung tại các khu vực, những vấn đề liên quan đến Việt Nam cũng ít khi được đề cập.

1.3.2. Các công trình nghiên cứu của Việt Nam

Trong số các công trình nghiên cứu của Việt Nam, trước tiên có thể đề cập đến một số Đề tài nghiên cứu khoa học các cấp được triển khai trong giai đoạn gần đây. Đề tài nghiên cứu khoa học cấp Nhà nước giai đoạn 1996-2000 "*Phòng chống tội phạm trong tình hình mới*" của GS. TS. Nguyễn Phùng Hồng. Trong đề tài, tác giả đã lần đầu tiên nhắc tới sự cần thiết phải tăng cường sự lãnh đạo của Đảng đối với công tác phòng chống tội phạm trong tình hình mới. Tiếp đến, cấp ủy, chính quyền các cấp cần nỗ lực nhiều hơn nữa trong lãnh đạo, chỉ đạo và tăng cường nhận thức của cán bộ, đảng viên và nhân dân. Tác giả nhận định, trong giai đoạn sắp tới, công tác phòng ngừa, điều tra, xử lý các loại tội phạm có tổ chức, hình sự nguy hiểm, kinh tế, tham nhũng, ma túy, tội phạm sử dụng công nghệ cao... cần tập trung và tiến hành quyết liệt hơn, góp phần đảm bảo an ninh quốc gia và giữ gìn trật tự, an toàn xã hội. Với tính chất là một công trình cấp nhà nước, đề tài đã bước đầu cảnh báo về những loại hình tội phạm nguy hiểm trong tình hình mới, đặc biệt là loại hình tội phạm có sử dụng công nghệ cao.

Một đề tài khác là đề tài nghiên cứu khoa học cấp Bộ *"Tội phạm xuyên quốc gia liên quan đến Việt Nam*" do Đại tá Phạm Hỗ (Chánh văn phòng INTERPOL Việt Nam-Tổng cục II Bộ Công an) làm chủ nhiệm đề tài. Đóng góp quan trọng nhất của đề tài đó là đã tiến hành tổng hợp các dữ liệu của Việt Nam liên quan đến tội phạm xuyên quốc gia; trong đó, tác giả đã nhiều lần đề cập và cảnh báo về loại hình tội phạm sử dụng công nghệ cao. Tác giả nhận định, tình hình tội phạm xuyên quốc gia trên thế giới và khu vực có nhiều diễn biến phức tạp. Khi xu hướng toàn cầu hóa bắt đầu xuất hiện, các hình thức tội phạm xuyên quốc gia tăng nhanh chóng, đặc biệt là buôn bán ma túy và các loại tội phạm mang lại lợi nhuận cao như hoạt động buôn bán vũ khí, buôn người, rửa tiền, tội phạm kinh tế quốc tế và tội phạm công nghệ cao... Bên cạnh đó, đề tài cũng đưa ra cảnh báo về thực trạng những dòng người, dòng tiền và hàng hóa di chuyển từ nước này sang nước khác trong bối cảnh toàn cầu hóa và hội nhập kinh tế quốc tế chính là điều kiện thuận lợi để các loại tội phạm mở rộng phạm vi hoạt động.

Ngoài các đề tài nghiên cứu khoa học, có thể kể tới một số cuốn sách chuyên khảo như "*Thực hiện chương trình quốc gia phòng, chống tội phạm trong thời kỳ đẩy mạnh công nghiệp hóa và hiện đại hóa đất nước*" của tác giả Lê Thế Tiệm (nhà xuất bản Công An Nhân Dân năm 2002). Cuốn sách tập trung đi vào làm rõ những tác động tiêu cực của các loại hình tội phạm trong công cuộc công nghiệp hóa - hiện đại hóa của Việt Nam. Tác giả cũng đề cập tới các nội dung, phương hướng trong

chương trình quốc gia phòng, chống tội phạm trong thời kỳ cuộc công nghiệp hóa - hiện đại hóa, trong đó đặc biệt lưu tâm tới các loại hình tội phạm công nghệ cao phát sinh trong giai đoạn mới. Để đạt được hiệu quả cao, tác giả cho rằng, sự phối hợp giữa các bộ ban ngành, các cơ quan phòng, chống tội phạm là yếu tố nền tảng. Ngoài ra, cần đẩy mạnh thực hiện các Chương trình quốc gia phòng, chống tội phạm; chủ động đánh giá thực trạng và dự báo xu thế phát triển của các loại hình tội phạm nói chung và tội phạm sử dụng công nghệ cao tại Việt Nam nói riêng.

Cuốn sách chuyên khảo "*Phòng chống các loại tội phạm ở Việt Nam thời kỳ đổi mới*" của tác giả Nguyễn Xuân Yêm (nhà xuất bản Công An Nhân Dân năm 2005) cũng là một trong những công trình đáng chú ý. Trong cuốn sách, tác giả nhận định, với bối cảnh nước ta chuyển đổi từ nền kinh tế tập trung bao cấp sang nền kinh tế thị trường, bên cạnh những trở ngại về mặt kinh tế thì cũng xuất hiện những vấn đề tiêu cực trong xã hội, nhất là vấn đề tội phạm - một dạng thức hành vi lệch lạc xã hội. Liên quan đến tội phạm công nghệ cao ở Việt Nam, tác giả đã chỉ ra tính phức tạp trong công tác phòng chống đặc biệt trong bối cảnh số lượng, mức độ và diễn biến của tội phạm ngày một phức tạp với các phương thức, thủ đoạn phạm tội mới. Cuốn sách cũng đưa ra dự báo về những khó khăn, thách thức trong giai đoạn sắp tới, tác giả cho rằng sự bùng nổ của công nghệ thông tin trong xu thế phát triển của thế giới sẽ tác động mạnh mẽ đến sự phát triển của mạng Internet, mạng viễn thông tại Việt Nam; chính điều này tạo điều kiện thuận lợi cho tội phạm sử dụng công nghệ cao gia tăng số lượng cùng với phương thức, thủ đoạn ngày càng tinh vi, khó phòng ngừa và đấu tranh hơn.

Đặc biệt, liên quan đến vấn đề tội phạm công nghệ cao tại Việt Nam, sẽ là thực sự thiếu sót nếu như không đề cập tới công trình của Đại tướng, GS. TS. Trần Đại Quang, cuốn sách "*Không gian mạng: Tương lai và Hành động*" (nhà xuất bản Công An Nhân Dân năm 2015). Không chỉ trình bày những vấn đề chung liên quan đến vòng xoáy phát triển không gian mạng tại Việt Nam và thế giới; vấn đề bảo vệ chủ quyền và an ninh-lợi ích quốc gia trên không gian mạng, cuốn sách còn lý giải sự hình thành của không gian mạng với nền tảng là Internet và đi sâu phân tích về bản chất xã hội của không gian mạng, cùng nhiều vấn đề đang là mối quan tâm hàng đầu của Việt Nam như an ninh mạng, gián điệp-tình báo mạng, tội phạm mạng hay thậm chí là chủ nghĩa khủng bố mạng. Dưới cách tiếp cận của mình, tại chương V, tác giả đã đưa ra nhiều giải pháp mang tính định hướng và thực chất đối với Việt Nam gắn chặt với an ninh và vận mệnh quốc gia trong bối cảnh toàn cầu hóa; theo đó, một loạt nhóm giải pháp được đưa ra như, hoàn thiện chủ trương, chính sách,

pháp luật; nâng cao năng lực công nghệ của quốc gia, tránh phụ thuộc vào bên ngoài; tăng cường quản lý và kiểm soát của Nhà nước đối với nội dung thông tin trên mạng; đẩy mạnh phát triển đội ngũ nguồn nhân lực và tổ chức bộ máy; đặc biệt, Đại tướng Trần Đại Quang nhấn mạnh vấn đề ý thức của mỗi người dân khi cho rằng, việc thiếu ý thức của người sử dụng đã tạo ra và thúc đẩy các yếu tố tiêu cực mà ta hay gọi là "mặt trái của Internet".

Ngoài ra, các công trình nghiên cứu tại Việt Nam về vấn đề này còn được đề cập tại các bài báo chuyên ngành, thể hiện quan điểm và góc nhìn riêng của các tác giả. Bài viết "*Giải pháp nâng cao hiệu quả đấu tranh với tội phạm sử dụng công nghệ cao trong bối cảnh toàn cầu hóa*" của tác giả Hồ Thế Hòe (đăng tải trên Tạp chí Dân chủ và Pháp luật, Số 6(243), năm 2012) phân tích thực trạng tội phạm sử dụng công nghệ cao trong bối cảnh bùng nổ của công nghệ thông tin và viễn thông. Tác giả cho rằng, ở Việt Nam tội phạm sử dụng công nghệ cao đang gia tăng nhanh chóng, tiếp tục diễn biến phức tạp và gây ra nhiều hậu quả nghiêm trọng. Trước đây, tội phạm sử dụng công nghệ cao xảy ra trên nhiều lĩnh vực như chính trị, kinh tế - xã hội và chủ yếu tập trung tại các thành phố lớn như Hà Nội, Hồ Chí Minh, Đà Nẵng; tuy nhiên, trong giai đoạn hiện nay nó đã lan ra các tỉnh, thành phố khác với quy mô, mức độ và thủ đoạn tinh vi hơn. Không chỉ dừng lại ở đó, tác giả bài viết cũng đưa ra một số kiến nghị nhằm nâng cao hiệu quả trong công tác đấu tranh đối với loại hình tội phạm này tại Việt Nam trong tiến trình hội nhập và toàn cầu hóa, trong đó đặc biệt nhấn mạnh đến công tác rà soát, bổ sung, ban hành mới các quy định của pháp luật. Bên cạnh đó, tác giả cho rằng Việt Nam cũng cần tiếp tục tăng cường hợp tác quốc tế trong lĩnh vực đấu tranh phòng, chống tội phạm sử dụng công nghệ cao, ký kết các thỏa thuận quốc tế, trao đổi thông tin tội phạm, tranh thủ tài trợ các thiết bị kỹ thuật, công nghệ hiện đại và đào tạo cán bộ trình độ cao...

Trong bài viết "*Hoàn thiện cơ sở pháp lý về chứng cứ điện tử trong phòng, chống tội phạm công nghệ cao*" (đăng trên Tạp chí Kiểm sát, số 1, năm 2014) của mình, tác giả Đào Anh Tới không chỉ đề cập tới những khía cạnh pháp lý về tội phạm công nghệ cao mà còn đưa ra những giải pháp trong việc hoàn thiện hồ sơ, chứng cứ điện tử trong công tác xử lý loại hình tội phạm này. Theo tác giả, chứng cứ điện tử có ý nghĩa to lớn không chỉ về mặt pháp lý mà nó còn có một ý nghĩa quan trọng trong công tác điều tra, truy tố và xét xử các vụ án mà 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 (tội phạm công nghệ cao). Tác giả cũng nhận định rằng, chủ thể của tội phạm đều là những người có nhận thức về pháp luật

và hiểu biết sâu về 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. Chính vì vậy, Việt Nam cần gấp rút hoàn thiện cơ sở pháp lý và nâng cấp năng lực của đội ngũ cán bộ trong công tác thu thập chứng cứ điện tử góp phần tăng cường hiệu quả công tác phòng, chống tội phạm nói chung và tội phạm công nghệ cao nói riêng.

Bài viết "*Tính chất của tình hình tội phạm sử dụng công nghệ cao tại Việt Nam, thủ đoạn phạm tội và dự báo*" của tác giả Cao Anh Đức (đăng trên Tạp chí Nghiên cứu lập pháp; số 16 năm 2015) tập trung vào việc nghiên cứu khái niệm và phân tích các đặc tính của tội phạm sử dụng công nghệ cao trong giai đoạn 2010 – 2014 tại Việt Nam. Tác giả chỉ ra rằng, tội phạm sử dụng công nghệ cao là một trong những loại hình tội phạm mới xuất hiện ở Việt Nam. Hiện tại, tình hình tội phạm công nghệ cao đang tiếp tục diễn biến phức tạp, khó lường, xảy ra trên nhiều lĩnh vực như kinh tế, văn hóa-xã hội, an ninh-quốc phòng của đất nước. Dưới góc nhìn của một kiểm sát viên, bài viết được tác giả tiếp cận chủ yếu dưới góc độ của pháp luật quốc gia. Chính vì vậy, những giải pháp mà tác giả đưa ra để khắc phục những hạn chế trong công tác phòng chống tội phạm sử dụng công nghệ cao ở Việt Nam bao gồm: tăng cường sự lãnh đạo và giám sát của các cấp ủy Đảng; chú trọng các biện pháp phòng ngừa xã hội; từng bước nâng cao năng lực của các cơ quan bảo vệ pháp luật và lực lượng chuyên trách; hoàn thiện hệ thống chính sách, pháp luật và tăng cường hợp tác quốc tế...

1.4. Đánh giá tình hình nghiên cứu các vấn đề liên quan đến đề tài luận án

Các công trình nghiên cứu liên quan đến đề tài luận án bước đầu đã có những nhận diện, phân tích và hệ thống hóa ở mức độ nhất định đối với phạm trù "tội phạm công nghệ cao" cũng như những vấn đề đặt ra đối với các quốc gia trong bối cảnh hiện nay, cụ thể:

Về mặt lý luận, mặc dù các công trình đều có những góc độ tiếp cận tương đối khác nhau trong việc nhìn nhận tội phạm công nghệ cao; tuy nhiên, ở một mức độ nhất định, những dấu hiệu pháp lý chung để nhận biết và xác định loại tội phạm này về cơ bản đều khá trùng khớp. Tiếp đó, các công trình đồng loạt đưa ra những cách thức phân loại tội phạm công nghệ cao thành những dạng thức và dựa trên những tiêu chí cụ thể. Một số công trình còn đi sâu hơn vào việc phân tích quá trình hình thành và phát triển của tội phạm công nghệ cao; qua đó, thấy được những sự biến chuyển nhanh chóng và các tác động tiêu cực ngày một tăng lên của loại hình tội phạm này.

Về mặt pháp lý, các công trình nghiên cứu từ bài viết cho đến sách chuyên khảo, bên cạnh việc đề cập đến góc độ kỹ thuật, đều phân tích đến một số khía cạnh pháp lý của loại hình tội phạm công nghệ cao - một loại hình tội phạm chỉ có thể hiểu rõ về mặt pháp lý khi đã nắm chắc được những khía cạnh liên quan đến kỹ thuật của tội phạm. Các công trình đa phần giới thiệu tới những quy định của pháp luật về tội phạm công nghệ cao của một số quốc gia như Mỹ, Canada, Australia, Nhật Bản, Anh, Thụy Điển,... Một số công trình đã bước đầu đề cập tới các văn kiện pháp lý quốc tế điều chỉnh vấn đề tội phạm công nghệ cao như Công ước Budapest về tội phạm mạng; Công ước Palermo về phòng chống tội phạm có tổ chức xuyên quốc gia.

Về mặt thực tiễn, trên cơ sở đưa ra các cách tiếp cận, phân loại và diễn giải các quy định của pháp luật về loại hình tội phạm công nghệ cao, các công trình nghiên cứu đã phân tích tình hình và tác động của tội phạm công nghệ cao tại các quốc gia, mỗi khu vực và trên toàn thế giới; từ đó, đưa ra những dự báo cũng như các giải pháp trong đó đặc biệt lưu tâm đến việc cải thiện công tác lập pháp và nhu cầu tăng cường hợp tác quốc tế giữa các quốc gia trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

Về những vấn đề liên quan đến Việt Nam, có thể nhận định, các công trình nghiên cứu chuyên sâu về tội phạm công nghệ cao thông qua các công trình nghiên cứu ở Việt Nam chưa thực sự được toàn diện và đầy đủ (cả về thể loại và mức độ nghiên cứu) so với tương quan tình hình nghiên cứu trên thế giới cũng như tính cấp thiết của diễn biến tình hình tội phạm công nghệ cao hiện nay. Các công trình chủ yếu tồn tại dưới dạng các bài viết nghiên cứu đơn lẻ, phân tích một số khía cạnh pháp lý của *tội phạm sử dụng công nghệ cao* (cách sử dụng thuật ngữ phổ biến trong giới khoa học pháp lý tại Việt Nam về tội phạm công nghệ cao) đặt trong mối tương quan với các quy định của pháp luật Việt Nam; qua đó, các công trình cũng đưa ra những dự báo và đề ra những giải pháp, đề xuất đối với Việt Nam trong thời gian tới. Ngoài ra, một số khía cạnh khác của tội phạm công nghệ cao cũng được đề cập tới rải rác tại một số đề tài nghiên cứu các cấp, các sách chuyên khảo... Tuy nhiên, các công trình này chủ yếu tiếp cận vấn đề tội phạm công nghệ cao dưới nhiều góc độ của các ngành khoa học khác nhau như: tội phạm học; khoa học điều tra hình sự; công nghệ thông tin.v.v...

Như vậy, về cơ bản, những công trình nghiên cứu hiện có đã cung cấp một "bức tranh" tổng thể để qua đó có thể hình dung được một cách toàn cảnh về tội phạm công nghệ cao là gì; những đặc tính và các dạng thức phổ biến của loại hình

tội phạm công nghệ cao so với các loại tội phạm khác; những tác động của tội phạm công nghệ cao đối với quyền và lợi ích của mỗi cá nhân, pháp nhân cũng như mỗi quốc gia, khu vực trong nhiều lĩnh vực; từ đó, các công trình đã đánh giá và chỉ ra những "khoảng trống" của pháp luật (trong đó có cả pháp luật quốc tế và pháp luật quốc gia) trong việc điều chỉnh đối với loại tội phạm công nghệ cao hiện nay.

Tuy nhiên, qua quá trình phân tích tổng quan, những công trình nghiên cứu hiện có bộc lộ và để ngỏ một số vấn đề sau:

Thứ nhất, các công trình nghiên cứu chủ yếu xoáy sâu vào loại hình tội phạm mạng (Cyber Crimes) - một trong những dạng thức cơ bản của tội phạm công nghệ cao. Mặc dù đã có những công trình ở trong và ngoài nước có nội dung đề cập về tội phạm công nghệ cao nhưng chưa có một công trình nào tiếp cận và nghiên cứu một cách hệ thống, toàn diện và đầy đủ về tội phạm công nghệ cao trên tất cả các bình diện lý luận, pháp lý và thực tiễn (thực tiễn quốc tế và thực tiễn tại Việt Nam).

Thứ hai, yếu tố pháp lý đặc biệt là pháp lý quốc tế được thể hiện tại các công trình hiện có chưa thực sự rõ nét; phần lớn các công trình nghiên cứu về tội phạm công nghệ cao được nghiên cứu trong và ngoài nước được tiếp cận dưới góc độ và bằng phương pháp nghiên cứu của các ngành khoa học như tội phạm học; công nghệ thông tin hay khoa học điều tra tội phạm... Các công trình trong giới luật học chuyên sâu tiếp cận dưới góc độ pháp lý quốc tế hầu như chưa được quan tâm nhiều; các công trình chủ yếu tiếp cận thông qua góc độ luật hình sự quốc gia và thể hiện dưới dạng các bài báo ngắn đăng trên các tạp chí chuyên ngành nên cũng chỉ đề cập được một vài khía cạnh của tội phạm công nghệ cao. Có thể nói rằng, hầu như chưa có công trình khoa học pháp lý nào kể cả ở trong và ngoài nước giải quyết một cách triệt để và có hệ thống các vấn đề pháp lý-thực tiễn về tội phạm công nghệ cao (đặc biệt là thực tiễn quốc tế và thực tiễn tại Việt Nam). Điều này dẫn tới hệ quả tất yếu là những kiến giải, đề xuất được đưa ra tại các công trình hiện có chưa thực sự toàn diện và thiếu đi tính pháp lý thuần khiết (do được tiếp cận bởi các ngành khoa học khác nhau).

Thứ ba, tại Việt Nam, số lượng những công trình nghiên cứu về tội phạm công nghệ cao còn khá khiêm tốn; thiếu vắng những công trình mang tính toàn diện và cập nhật về tình hình tội phạm công nghệ cao đặc biệt trong giai đoạn hiện nay. Tình hình nghiên cứu tại Việt Nam như vậy chưa tương xứng với xu hướng nghiên cứu quốc tế và đặc biệt chưa đáp ứng được yêu cầu của tình hình, tốc độ phát triển cũng như những tác động tiêu cực mà loại hình tội phạm này đưa lại, ảnh hưởng trực tiếp tới quyền lợi của mỗi cá nhân, pháp nhân và Nhà nước. Điều nay dẫn tới

một số hạn chế trong cách tiếp cận mới về tội phạm công nghệ cao, đặc biệt trong giai đoạn hiện nay, khi mà tội phạm công nghệ cao đã biến chuyển và có nhiều dạng thức, thủ đoạn tinh vi hơn so với các phiên bản trước. Thêm vào đó, các công trình nghiên cứu tại Việt Nam hầu như chỉ nhắc đến mà chưa thực sự tiếp cận và phân tích đến các quy định trong Công ước Budapest về tội phạm mạng - một trong những công ước điển hình khi nhắc tới vấn đề điều chỉnh các loại hình tội phạm công nghệ cao hiện nay.

1.5. Những vấn đề cần tiếp tục được nghiên cứu trong luận án

Mặc dù các công trình nghiên cứu quốc tế và tại Việt Nam hiện có đã làm rõ ở những mức độ nhất định đối với một số khía cạnh cơ bản liên quan đến tội phạm công nghệ cao. Tuy nhiên còn nhiều vấn đề lý luận, pháp lý và thực tiễn về tội phạm công nghệ cao cũng như những vấn đề liên quan đến Việt Nam cần được nghiên cứu, làm rõ và tiếp tục làm sâu sắc hơn:

*** Về lý luận:**

Thứ nhất, luận án sẽ tiếp tục khái quát hóa, hệ thống hóa và làm sâu sắc hơn nữa các vấn đề lý luận căn bản trong phạm trù "tội phạm công nghệ cao". Bên cạnh đó, không chỉ tiếp cận bằng những phương cách truyền thống, những vấn đề lý luận cần được soi chiếu và kiểm chứng bằng tình hình phát triển thực tiễn của loại hình tội phạm này, trong đó đặc biệt cần đối chiếu và cập nhật với những diễn biến mới nhất của tội phạm công nghệ cao trong giai đoạn hiện nay.

Thứ hai, luận án sẽ phân định và làm rõ nội hàm của các thuật ngữ đang được sử dụng không thống nhất nhưng có liên quan trực tiếp đến tội phạm công nghệ cao, như: tội phạm mạng; tội phạm không gian ảo; tội phạm máy tính; tội phạm liên quan đến máy tính; tội phạm sử dụng/lợi dụng công nghệ cao.v.v... Qua đó, luận án tiếp tục đúc rút và xây dựng một định nghĩa bao quát về tội phạm công nghệ cao đặc biệt đặt trong bối cảnh và tình hình thực tiễn hiện nay. Cùng với đó, những đặc thù của tội phạm công nghệ cao cũng sẽ được luận án phân tích rõ trong mối tương quan với các loại hình tội phạm khác.

Thứ ba, luận án cũng sẽ tập trung làm rõ những vấn đề lý luận trong hợp tác quốc tế trong đấu tranh, phòng chống tội phạm nói chung và đặc biệt trong công tác phòng chống tội phạm công nghệ cao nói riêng (nguồn luật, nội dung, vai trò và phương thức hợp tác).

*** Về pháp lý:**

Thứ nhất, luận án sẽ tập trung nghiên cứu một cách tổng thể và có hệ thống đối với những vấn đề pháp lý liên quan đến tội phạm công nghệ cao và hợp tác quốc

tế trong công tác phòng chống loại hình tội phạm này, đặc biệt luận án sẽ cố gắng làm sâu sắc hơn yếu tố pháp lý quốc tế được quy định trong một số văn kiện hiện nay mà điển hình là Công ước Budapest về tội phạm mạng của Ủy hội châu Âu cùng các điều ước quốc tế và văn bản khác có liên quan.

Thứ hai, luận án sẽ mở rộng phạm vi tìm hiểu tới việc thực hiện pháp luật quốc tế trong hợp tác đấu tranh phòng, chống tội phạm công nghệ cao của một số quốc gia điển hình; qua đó, đúc rút một số giá trị kinh nghiệm, bài học tham khảo đối với Việt Nam liên quan đến vấn đề này.

*** Về thực tiễn:**

Thứ nhất, luận án sẽ đánh giá thực trạng tình hình và diễn biến cập nhật của các loại hình tội phạm công nghệ cao trên cả phương diện quốc tế và tại Việt Nam; qua đó, đưa ra những dự báo và giải pháp có tính ứng dụng trong quá trình hợp tác đấu tranh, phòng chống tội phạm công nghệ cao hiện nay.

Thứ hai, luận án sẽ tập trung đánh giá hoạt động xây dựng và thực thi pháp luật quốc tế cũng như pháp luật Việt Nam trong lĩnh vực hợp tác đấu tranh phòng chống tội phạm công nghệ cao theo các tiêu chí của nguyên tắc Pacta sunt servanda. Trên cơ sở đó, luận án cũng sẽ tiếp tục nhận định về vấn đề các quy định của pháp luật hiện hành (bao gồm cả pháp luật quốc tế và pháp luật quốc gia) đã đầy đủ cho việc tạo ra một cơ sở pháp lý vững chắc cho các công tác phát hiện, triệt phá, hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao hay chưa; có bảo vệ kịp thời quyền và lợi ích chính đáng của mỗi cá nhân, pháp nhân và mỗi quốc gia hay không. Từ đó, đưa ra những phương hướng, giải pháp toàn diện trên nhiều góc độ nhằm hoàn thiện pháp luật và nâng cao hiệu quả trong công tác hợp tác đấu tranh phòng chống tội phạm công nghệ cao, nhất là tại Việt Nam, đặc biệt đặt trong bối cảnh bùng nổ của cuộc cách mạng công nghiệp lần thứ 4.0 hiện nay.

TIỂU KẾT CHƯƠNG 1

* * *

Trên cả bình diện lý luận, pháp lý và thực tiễn, vấn đề "tội phạm công nghệ cao" thường xuyên được đề cập đến với tần suất tăng dần và đã trở thành đối tượng khảo cứu trong nhiều công trình nghiên cứu khoa học của các tác giả khác nhau ở nước ngoài cũng như tại Việt Nam. Các công trình nghiên cứu liên quan đến đề tài luận án bước đầu đã có những nhận diện, phân tích và hệ thống hóa ở mức độ nhất định đối với phạm trù "tội phạm công nghệ cao" cũng như những vấn đề đặt ra đối với các quốc gia trong bối cảnh hiện nay. Mặc dù các công trình đều có những góc độ tiếp cận tương đối khác nhau trong việc nhìn nhận tội phạm công nghệ cao; tuy nhiên, ở một mức độ nhất định, những dấu hiệu pháp lý chung để nhận biết và xác định loại tội phạm này về cơ bản đều khá trùng khớp. Yếu tố pháp lý đặc biệt là pháp lý quốc tế được thể hiện tại các công trình hiện có chưa thực sự rõ nét; phần lớn các công trình nghiên cứu về tội phạm công nghệ cao được nghiên cứu trong và ngoài nước được tiếp cận dưới góc độ và bằng phương pháp nghiên cứu của các ngành khoa học như tội phạm học; công nghệ thông tin hay khoa học điều tra tội phạm. Các công trình trong giới luật học chuyên sâu tiếp cận dưới góc độ pháp lý quốc tế hầu như chưa được quan tâm nhiều và hầu hết cũng chỉ đề cập được một vài khía cạnh của tội phạm công nghệ cao.

Tại Việt Nam, các công trình nghiên cứu chuyên sâu về tội phạm công nghệ cao thông qua các công trình nghiên cứu chưa thực sự được toàn diện và đầy đủ (cả về thể loại và mức độ nghiên cứu) so với tương quan tình hình nghiên cứu trên thế giới cũng như tính cấp thiết của diễn biến tội phạm công nghệ cao hiện nay; các công trình chủ yếu tồn tại dưới dạng các bài viết nghiên cứu đơn lẻ, phân tích một số khía cạnh pháp lý của tội phạm sử dụng công nghệ cao... Các công trình nghiên cứu tại Việt Nam hầu như chỉ nhắc đến mà chưa thực sự tiếp cận và phân tích đến các quy định trong Công ước Budapest về tội phạm mạng - một trong những công ước điển hình khi nhắc tới vấn đề điều chỉnh các loại hình tội phạm công nghệ cao hiện nay.

Mặc dù, các công trình hiện có đã "xới" lên một lĩnh vực nghiên cứu còn tương đối mới mẻ nhưng đặt trong bối cảnh bùng nổ của khoa học công nghệ thông tin, việc có thêm các công trình nghiên cứu toàn diện và làm rõ hơn khía cạnh pháp lý (đặc biệt là pháp lý quốc tế) là điều vô cùng cấp thiết.

CHƯƠNG 2
MỘT SỐ VẤN ĐỀ LÝ LUẬN VỀ TỘI PHẠM CÔNG NGHỆ CAO VÀ PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO

***

2.1. Khái niệm tội phạm công nghệ cao và hợp tác đấu tranh, phòng chống tội phạm công nghệ cao

Trước khi nghiên cứu về pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao, cần phải làm rõ các nội hàm một số khái niệm như "tội phạm công nghệ cao", "hợp tác đấu tranh" để từ đó có thể thống nhất khái niệm về các quan hệ pháp luật, quy phạm pháp luật điều chỉnh vấn đề này, qua đó xác định cơ sở, nội dung, nguyên tắc, chủ thể, hình thức và các thiết chế trong việc hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

2.1.1. Khái niệm tội phạm công nghệ cao

2.1.1.1. Định nghĩa tội phạm công nghệ cao

Khi nghiên cứu về quá trình hình thành và phát triển, có thể thấy thuật ngữ tội phạm công nghệ cao không xuất hiện ngay từ những thời kì đầu. Những trường hợp tội phạm công nghệ cao đầu tiên được ghi nhận chính là tội ăn cắp dữ liệu thông tin nội bộ khi mà nhân loại đã tìm ra được một hệ thống lưu trữ và chuyển tải thông tin qua máy tính, mạng máy tính và mạng Internet giữa các chính phủ, công ty[3]...

Mặc dù mới chỉ được hình thành và phát triển trong vài thập kỷ gần đây, tuy nhiên, cuộc cách mạng khoa học công nghệ đã khiến cho nhiều ngành kinh tế, khoa học và xã hội phụ thuộc vào các công nghệ mới của nó. Cũng giống như bất kỳ một thành tựu nào của nhân loại, khi mà các phát minh càng được ứng dụng rộng rãi trong đời sống xã hội thì càng dễ bị lợi dụng hoặc là mục tiêu hướng tới của giới tội phạm. Các thành tựu do công nghệ thông tin đem lại cũng không nằm ngoài quy luật đó; chính vì vậy, trong xã hội hiện đại ngày nay đã hình thành một dạng thức mới về tội phạm - tội phạm công nghệ cao. Đây là thuật ngữ mới không chỉ đối với Việt Nam mà còn đối với nhiều quốc gia trên thế giới. Do đó, ngay từ việc sử dụng thuật ngữ cho đến việc đưa ra khái niệm, đặc điểm hay việc sắp xếp những hành vi nguy hiểm cho xã hội nào bị liệt kê vào danh sách của loại tội phạm này cũng còn

---

[3] Akhgar, Babak, Staniforth, Andrew, & Bosco, Francesca. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Rockland, MA: Elsevier Science & Technology Books

có nhiều ý kiến không đồng nhất[4].

Về mặt thuật ngữ, khái niệm "tội phạm công nghệ cao" trong luật pháp của nhiều nước trên thế giới như Australia, Mỹ, Anh… đã có định nghĩa liên quan đến tội phạm này như: tội phạm công nghệ cao (*high-tech crime*); tội phạm mạng (*cybercrime*); tội phạm ảo (*Virtual Crime*); tội phạm máy tính/tội phạm tin học (*computer crime*); tội phạm liên quan đến máy tính (*computer-related crime*); tội phạm được kích hoạt / hỗ trợ bởi công nghệ (*Technologically Enabled/Supported Crime*)... Ví dụ như trong luật hình sự năm 1995 của Australia và phần 10.7 của luật Thịnh vượng chung (Commonwealth Legislation - Part 10.7: Computer Offences), tội phạm công nghệ cao (hi-technology crime) được định nghĩa "*là sự xâm nhập máy tính một cách trái phép; sự sửa đổi trái phép dữ liệu bao gồm việc phá hủy dữ liệu; tấn công từ chối dịch vụ (DoS); Tấn công từ chối dịch vụ phân tán (DdoS) có sử dụng botnets; tạo ra và phân phối phần mềm độc hại*"[5].

Theo Từ điển Luật học Black's Law, tội phạm máy tính (*computer crime*) được định nghĩa là: "*tội phạm đòi hỏi về kiến thức công nghệ máy tính chẳng hạn như phá hoại hoặc ăn cắp dữ liệu máy tính hay sử dụng máy tính để thực hiện một số tội phạm khác*"[6].

Theo cách tiếp cận của Cơ quan Cảnh sát Liên bang Úc (Australian Federal Police AFP) tội phạm công nghệ cao được định nghĩa theo kiểu liệt kê trong luật của Liên bang trong Phần 10.7 - Các tội phạm về máy tính của Đạo luật hình sự năm 1995 bao gồm: xâm nhập máy tính (ví dụ, hacker nguy hiểm); sửa đổi trái phép dữ liệu, bao gồm cả việc hủy dữ liệu các cuộc tấn công từ chối dịch vụ được phân tán (DDoS) sử dụng botnet việc tạo và phân phối phần mềm độc hại (ví dụ như virus, sâu, trojans)[7]...

Theo US. Legal[8]: "*Tội phạm công nghệ cao là những tội ác được thực hiện*

---

[4] GS. TS. Trung Tướng Nguyễn Ngọc Anh - Cục trưởng Cục Pháp chế và cải cách tư pháp V19 - Bộ Công an, mục Nghiên cứu Trao đổi "Một số quy định của pháp luật về tội phạm công nghệ cao"http://csnd.vn/Home/Nghien-cuu-Trao-doi/286/Mot-so-quy-dinh-cua-phap-luat-ve-toi-pham-cong-nghe-cao (truy cập lần cuối ngày 20/3/2020).

[5] Xem *https://www.afp.gov.au/what-we-do/crime-types/cybercrime/high-tech-crime*(truy cập lần cuối ngày 20/3/2020).

[6]Xem*https://legal.thomsonreuters.com/en/products/law-books/blacks-law-dictionary* (truy cập lần cuối ngày 20/3/2020).

[7] Xem *https://www.afp.gov.au/what-we-do/crime-types/cybercrime/high-tech-crime*(truy cập lần cuối ngày 20/3/2020).

[8] US.Legal: là trang hợp pháp cho người tiêu dùng, doanh nghiệp nhỏ, luật sư, công ty và bất kỳ ai quan tâm đến luật pháp, hoặc cần thông tin pháp lý, sản phẩm hoặc dịch vụ.

bằng cách sử dụng công nghệ điện tử và kỹ thuật số mới như internet hoặc sự trợ giúp của máy tính. Những tội phạm này còn được gọi là tội phạm mạng, tội phạm máy tính và tội phạm công nghệ, tùy thuộc vào khu vực mà họ đang thực hiện". Thông thường có hai loại tội phạm công nghệ cao khác nhau; danh mục đầu tiên bao gồm những tội phạm truyền thống được thực hiện thông qua việc sử dụng máy tính. Nó bao gồm bất kỳ tội phạm nào được hỗ trợ bởi máy vi tính như phân phối sách báo khiêu dâm trẻ em, bán hoặc mua thuốc bất hợp pháp, rửa tiền, cờ bạc bất hợp pháp, phân phối tuyên truyền thù địch hoặc các ấn phẩm, phạm tội gian lận internet và sử dụng bất kỳ công nghệ nào để lưu trữ, ẩn hoặc liên lạc với tội phạm và/hoặc các hoạt động hoặc hiệp hội khủng bố. Loại hình tội phạm công nghệ cao thứ hai bao gồm những tội ác nhằm vào máy tính hoặc mạng máy tính. Đây được gọi là tội phạm công nghệ cao tinh khiết và bao gồm các hành vi phạm tội như sử dụng trái phép hệ thống máy tính mà tiêu biểu là tấn công (hack) vào máy tính khác hoặc sử dụng trái phép hay phân phối dữ liệu, tấn công từ chối dịch vụ (DDOS) và phân phối virus máy tính[9].

Theo cách tiếp cận về tội phạm máy tính đã được Bộ Tư pháp Hoa Kỳ đưa ra như sau: "*tội phạm tin học là bất cứ các hành vi vi phạm pháp luật hình sự nào có liên quan đến việc sử dụng các hiểu biết về công nghệ máy tính trong việc phạm tội, điều tra hoặc xét xử*". Theo định nghĩa này thì bất cứ tội phạm nào cũng có thể được xếp vào loại tội phạm máy tính vì chỉ cần trong quá trình điều tra các điều tra viên sử dụng máy tính để tìm kiếm thông tin cũng thuộc phạm vi điều chỉnh của định nghĩa[10]. Cách hiểu tội phạm tin học theo phạm vi rộng vấp phải một vấn đề khó khăn đó là việc cụ thể hoá các hành vi phạm tội cụ thể từ đó xác định tội danh cho các hành vi này. Đây không phải là một công việc dễ dàng vì khi định tội danh, xét về bản chất, nhiều tội danh lại trùng với các tội truyền thống như tội lừa đảo, đánh bạc... điểm khác biệt có khác chăng ở đây là việc sử dụng công cụ thiết bị và mạng máy tính mà thôi.

Tiếp cận ở một giác độ cụ thể hơn, một số nhà nghiên cứu cho rằng tội phạm công nghệ thông tin chỉ là tội phạm được thực hiện và gây hậu quả trong thế giới ảo hay môi trường siêu thực, do thành tựu của khoa học công nghệ tin học đem lại và

[9] Xem *https://definitions.uslegal.com/c/cybercrimes/* (truy cập lần cuối ngày 20/3/2020).
[10] Xem *https://www.justice.gov/criminal-ccips/cybercrime-symposium*(truy cập lần cuối ngày 20/3/2020).

nó hoàn toàn khác so với các loại tội phạm truyền thống trước kia[11]. Trên thế giới hiện nay đã xuất hiện thêm nhiều hành vi được coi là tội phạm công nghệ thông tin khác hiểu theo phạm vi hẹp này như: tội truy cập bằng mật khẩu ăn cắp; tội sao chụp bất hợp pháp các chương trình phần mềm; tội tấn công và đe doạ tấn công hệ thống máy tính... Phương pháp tiếp cận theo phạm vi hẹp này tuy có ưu điểm là định rõ được tội danh cần xử lý nhưng lại có nhược điểm là rất dễ bỏ sót tội phạm, nhất là trong bối cảnh công nghệ thông tin đang phát triển như vũ bão. Một ví dụ điển hình, trên thế giới hiện nay đang tranh cãi về việc có coi hành vi trộm cắp, lừa đảo các tài sản mà người chơi có được khi chơi trò chơi trực tuyến hay không. Nếu nhìn dưới góc độ thế nào là tài sản theo quy định của pháp luật hiện hành, thì các tài sản ảo này là hoàn toàn không giá trị vì nó thực chất không phải là tài sản vì chỉ là những thứ được tạo ra trong thế giới siêu thực do một phần mềm máy tính (những người xây dựng lên trò chơi trực tuyến) tạo ra. Tuy nhiên, nếu xét dưới góc độ giá trị giao dịch thì các tài sản này là do người chơi đã bỏ nhiều công sức để tạo lập được, cùng với tính chất có thể "chiếm hữu, sử dụng và định đoạt" và đặc biệt là những tài sản này có thể quy đổi sang giá trị thực trong giao dịch dân sự (có thể mua bán, trao đổi cho những người chơi khác) thì chúng lại thực sự cần được coi là một tài sản có giá trị thực và cần được pháp luật bảo vệ trước các hành vi như lừa đảo, trộm cắp như đối với các tài sản hữu hình khác.

Mặt khác, nếu chỉ coi tội phạm công nghệ cao giới hạn trong phạm vi thế giới ảo, môi trường điện tử do công nghệ thông tin đem lại thì đối với những *tội phạm truyền thống sử dụng thành tựu công nghệ thông tin* thực hiện hành vi phạm tội, việc truy vết, chính sách ngăn ngừa, hợp tác đấu tranh đối với hành vi này sẽ không có gì khác so với các phương pháp xử lý truyền thống, trong khi về bản chất thì các hành vi phạm tội này khác hẳn, đơn cử như kẻ phạm tội tống tiền trên mạng trong và sau khi thực hiện hoàn toàn có thể xoá sạch toàn bộ dấu vết tội phạm bằng kỹ thuật công nghệ tin học, điều này gây không ít khó khăn cho hoạt động thu thập dấu vết nếu các phương pháp thu thập, bảo quản chứng cứ không được cập nhật và thay đổi phù hợp.

Chính vì mỗi một quan điểm lại có những hạn chế nhất định, nên hiện nay trên thế giới vẫn chưa có một khái niệm thống nhất về tội phạm công nghệ cao. Tại cuộc họp lần thứ 10 của Đại hội đồng Liên hợp quốc về ngăn chặn và xử lý tội phạm được tổ chức tại thành phố Viên (Áo) từ ngày 10 đến ngày 17 tháng 10 năm 2000,

[11] Prasad, R., & Institute of Chartered Financial Analysts of India. (2004). *Cyber crime: An introduction* (1st ed.). Hyderabad, India: Icfai Books

một cuộc hội thảo đã được tổ chức để bàn về vấn đề tội phạm công nghệ thông tin, việc định nghĩa tội phạm này đã được chia ra thành hai dạng tội phạm:

- Thứ nhất, tội phạm công nghệ thông tin theo nghĩa hẹp: được định nghĩa là các hành vi phạm tội sử dụng máy tính và mạng máy tính với mục đích xâm phạm đến an toàn của hệ thống máy tính và quy trình lưu trữ dữ liệu của hệ thống đó. Loại tội phạm theo cách tiếp cận này có thể được hiểu là loại tội phạm mới có quan hệ trực tiếp đến máy tính, mạng máy tính, làm ảnh hưởng và gây thiệt hại cho người sử dụng.

- Thứ hai, tội phạm công nghệ thông tin được hiểu theo nghĩa rộng: được định nghĩa là các hành vi phạm tội sử dụng máy tính hoặc các phương pháp khác có liên quan đến máy tính, mạng máy tính, bao gồm các loại tội phạm như chiếm giữ bất hợp pháp và đe doạ hoặc làm sai lệnh thông tin bằng phương pháp sử dụng mạng máy tính. Loại tội phạm theo định nghĩa này là rất rộng, bao gồm nhiều loại hành vi của tội phạm truyền thống được thực hiện với sự trợ giúp của công cụ máy tính mà phổ biến hiện nay như các hành vi lừa đảo, trốn lậu cước viễn thông, mạo danh...

Định nghĩa này tuy chưa phải là một định nghĩa hoàn chỉnh, vẫn còn hết sức chung chung tuy nhiên nó có một ý nghĩa đặc biệt quan trọng khi mà lần đầu tiên khái niệm thế nào là tội phạm công nghệ thông tin đã được các quốc gia trên thế giới thảo luận và quan tâm. Tội phạm công nghệ thông tin, theo định nghĩa nêu trên, là những tội phạm liên quan đến máy tính và cách mạng thông tin. Định nghĩa thừa nhận tội phạm công nghệ thông tin bao gồm cả các tội phạm mới hình thành trong môi trường của công nghệ thông tin và cả những tội phạm truyền thống nhưng được thực hiện với sự giúp đỡ của các công nghệ thông tin mới[12].

Như vậy, ngay từ cách sử dụng các thuật ngữ khác nhau đã cho thấy tính chất phức tạp của vấn đề. Xét cho cùng, việc sử dụng thuật ngữ nào cần nhất thiết căn cứ vào từng bối cảnh cụ thể cũng như phụ thuộc vào cách tiếp cận theo pháp luật của mỗi quốc gia. Mỗi thuật ngữ đều có những cách tiếp cận riêng và có những hạn chế riêng trong quá trình sử dụng. Đối với nhóm thuật ngữ "*Tội phạm máy tính/tội phạm liên quan đến máy tính/tội phạm do máy tính hay tội phạm xuất phát từ máy tính*", đây là nhóm thuật ngữ nhấn mạnh vào công cụ phạm tội mà trong đó máy tính đóng một vai trò trung tâm quan trọng không thể thiếu. Có thể thấy, đây là

[12] Xem "Lý luận về tội phạm mạng và phương hướng xử lý nếu như có hành vi vi phạm" Bernat, Frances P, and David Makin. "Cybercrime Theory And Discerning If There Is A Crime: The Case Of Digital Piracy" International Review of Modern Sociology, vol. 40, no. 2, 2014, pp. 99–119. JSTOR.

nhóm thuật ngữ được hình thành ngay từ những giai đoạn đầu tiên, sự xuất hiện của nó gắn liền với sự ra đời của máy tính và các thiết bị vi điện tử. Sau khi máy tính ra đời, việc kết nối các mạng LAN nội bộ không đáp ứng được nhu cầu trao đổi dữ liệu và thông tin trên phạm vi toàn cầu. Đó là lý do và là sự tất yếu dẫn tới sự hình thành của mạng Internet - một trong những phát minh vĩ đại và quan trọng bậc nhất làm thay đổi toàn diện cuộc sống của toàn thể cộng đồng nhân loại. Không thể tượng tượng rằng loài người trong giai đoạn hiện nay có thể sống mà thiếu đi kết nối Internet sẽ như thế nào. Đi cùng với sự thịnh hành của máy tính và mạng Internet, một loạt các loại tội phạm đã được phát hiện với quy mô, tần suất, thủ đoạn và mức độ nguy hiểm thiệt hại vô cùng khủng khiếp. Đây cũng là lúc mà một số thuật ngữ cụ thể hơn đã được đưa ra bàn luận như "*tội phạm mạng/ tội phạm tin học/ tội phạm không gian ảo hay tội phạm Internet*". Nhóm thuật ngữ này dùng để chỉ loại hình tội phạm sử dụng mạng Internet cùng với các thủ thuật công nghệ thông tin và gắn chặt với yếu tố "mạng" cũng như được tiến hành trên môi trường số có tính chất ảo. Khi sử dụng nhóm thuật ngữ này, mạng Internet có vai trò tất yếu, quan trọng không thể thiếu trong quá trình thực hiện các hành vi phạm tội. Và trong một số tình huống, khi sử dụng nhóm thuật ngữ này, yếu tố "mạng" đôi lúc còn quan trọng hơn cả yếu tố "máy tính" so với các tiếp cận của nhóm thuật ngữ thứ nhất. Nói một cách khác, nhóm thuật ngữ thứ hai là một biến thể của nhóm thuật ngữ thứ nhất khi mà tội phạm máy tính đã được nâng cấp để chuyển đổi thành phiên bản tội phạm mạng. Và hiện nay, tội phạm mạng đã dần trở thành một xu hướng chính khi các học giả miêu tả về tội phạm máy tính. Chính vì vậy, tội phạm mạng là giao thức cập nhật cho thuật ngữ tội phạm máy tính. Tuy nhiên, điều này không cản trở cũng như không ảnh hưởng tới sự tồn tại và việc sử dụng thuật ngữ tội phạm máy tính trong bối cảnh hiện nay, đặc biệt khi các học giả cũng như các quốc gia đã quá quen thuộc đối với hệ thống nhóm thuật ngữ có liên quan đến "Computer Crimes". Thuật ngữ tội phạm mạng đã bước đầu đạt đến sự chính thức hóa và pháp lý hóa khi nó được ghi nhận một cách rõ ràng trong Công ước của Ủy hội châu Âu về tội phạm mạng hay còn được biết đến với tên gọi là Công ước Budapest về Tội phạm mạng (Council of Europe Convention on Cybercrime (Budapest Treaty 2001). Đây được coi là bước tiến quan trọng trong nhận thức của cộng đồng quốc tế liên quan đến sự ghi nhận và điều chỉnh các loại hình tội phạm mới xuất hiện trong giai đoạn bùng nổ khoa học kỹ thuật hiện nay. Với sự ra đời của Công ước Budapest, lần đầu tiên trong lịch sử pháp luật quốc tế, có một công ước đa phương nhận diện và điều chỉnh một cách tổng quan các vấn đề có liên quan đến tội phạm

mạng nói chung và các loại hình tội phạm công nghệ cao có liên quan, trong đó, công ước này đặc biệt nhấn mạng đến tầm quan trọng của việc hình sự hóa, công tác tương trợ tư pháp khi cho rằng một quốc gia đơn lẻ sẽ không thể đạt được hiệu quả trong vấn đề triệt phá, ngăn ngừa loại hình tội phạm này. Việc loại bỏ các loại hình tội phạm mạng chỉ có thể đạt được hiệu quả cao nhất khi giữa các quốc gia đẩy mạng công tác hợp tác quốc tế đấu tranh, phòng chống tội phạm trên mọi lĩnh vực[13].

Nhóm thuật ngữ thứ ba được sử dụng phổ biến hiện nay là "*Tội phạm công nghệ cao/ tội phạm sử dụng công nghệ cao/ tội phạm kích hoạt công nghệ cao hay tội phạm được hỗ trợ bởi công nghệ cao*". Đây là nhóm thuật ngữ không nhấn mạnh hay xoáy sâu vào bất cứ một yếu tố nào, cho dù là "máy tính" hay "mạng Internet". Nhóm thuật ngữ này sử dụng cách tiếp cận phổ quát trước một loại hình tội phạm liên tục vận động và phát triển; loại hình tội phạm này có sự thích nghi và biến đổi cập nhật theo từng "nhịp sóng" của "làn sóng" khoa học công nghệ. Đây được đánh giá là một cách tiếp cận tương đối phù hợp và chứa đựng tính bao quát, đón đầu được xu thế bùng nổ của khoa học kỹ thuật. Thực tế đã minh chứng rằng, không thể cứ mãi nâng cấp các thuật ngữ bằng việc "theo đuôi" các thành tựu của khoa học công nghệ. Chính vì lý do đó, việc đưa ra một thuật ngữ có tính khái quát cao, bao quát được toàn bộ tiến trình vận động và phát triển của sự vật hiện tượng là điều nên được cân nhắc. Cái hay của nhóm thuật ngữ tội phạm công nghệ cao đó chính là bao quát được tất cả các dạng thức tội phạm có sự dụng những kiến thức và kỹ năng của các ngành khoa học công nghệ (trong đó có công nghệ máy tính và mạng Internet). Và không chỉ dừng lại ở đó, nhóm thuật ngữ này còn mở rộng phạm vi đến cả những thiết bị số cũng như các hoạt động trục lợi, thao túng từ máy tính cho đến điện thoại di động, các thiết bị thông minh kỹ thuật số (Smart Devices) hay bất kỳ một giao thức công nghệ cao bất kỳ đang tồn tại hoặc sẽ xuất hiện trong tương lai... Không phải ngẫu nhiên, trong các chương trình nghị sự của mình, bên cạnh nhóm các thuật ngữ thứ nhất (tội phạm máy tính/tội phạm liên quan đến máy tính) và nhóm thuật ngữ thứ hai (tội phạm mạng), nhóm thuật ngữ thứ ba (tội phạm công nghệ cao) liên tục được nhắc đến và ghi nhận tại các nghị quyết của Đại hội đồng Liên hợp quốc[14]. Điều này thể hiện một sự đón đầu có chủ đích của tổ chức này

---

[13] Alexander Seger (2016), *The Budapest Convention on Cybercrime: a framework for capacity building*, Global Cyber Expertise Magazine, (2).35.

[14] Xem các Nghị quyết tại *https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf* và *https://www.unodc.org/documents/treaties/a_res_57/153e.pdf* (truy cập lần cuối ngày 28/3/2020).

trước bối cảnh sự vận động biến đổi không ngừng của các dạng thức tội phạm trong cuộc cách mạng khoa học công nghệ lần thứ 4.0[15].

Qua nghiên cứu các định nghĩa và các cách tiếp cận trên, hoàn toàn có thể thấy những điểm chung trong nội hàm của các khái niệm này; tất cả đều hướng tới các hành vi liên quan đến việc sử dụng máy tính, thiết bị số, khai thác mạng máy tính, mạng viễn thông một cách bất hợp pháp để gây tổn hại cho lợi ích của các tổ chức, cá nhân và toàn xã hội. Vì vậy, có thể rút ra một định nghĩa chung về tội phạm công nghệ cao như sau: *tội phạm công nghệ cao là một dạng thức tội phạm được tiến hành thông qua việc sử dụng tri thức, kỹ năng, công cụ, phương tiện và thành tựu của công nghệ thông tin ở trình độ cao, tác động một cách bất hợp pháp đến thông tin số và các dữ liệu điện tử được lưu trữ, xử lý, truyền tải trong hệ thống máy tính và các thiết bị công nghệ cao, xâm phạm đến trật tự an toàn thông tin, gây tổn hại nghiêm trọng đến quyền và lợi ích hợp pháp của các cá nhân, tổ chức cũng như của các quốc gia và cộng đồng quốc tế.*

2.1.1.2. Đặc điểm của tội phạm công nghệ cao

Trong xu thế toàn cầu hóa, tội phạm công nghệ cao không chỉ tăng về số lượng hay quy mô mà còn diễn biến ngày càng phức tạp với nhiều thủ đoạn tinh vi hơn. Khác với những tội phạm truyền thống, tội phạm công nghệ cao có những đặc điểm thể hiện sự khác biệt và phức tạp hơn nhiều so với bất kỳ loại hình tội phạm nào.

Thứ nhất, tội phạm công nghệ cao có đầy đủ các tính chất, đặc điểm giống như mọi tội phạm truyền thống khác, nghĩa là cũng được coi là những hành vi nguy hiểm cho xã hội, sự tương đồng trong các cấu thành cơ bản của một tội phạm... Tuy nhiên, điểm khác biệt cốt lõi giữa chúng với tội phạm khác nằm ở khía cạnh "công nghệ thông tin, máy tính và mạng internet" đóng vai trò, mức độ quyết định trong việc thực hiện, che giấu và gây ra những hậu quả khôn lường đối với xã hội của hành vi phạm tội. Nhìn một cách tổng thể, đối với loại tội phạm công nghệ cao, công nghệ máy tính và mạng luôn là một công cụ quan trọng không thể thiếu trong quá trình thực hiện hành vi phạm tội.

Nếu như xem xét dưới góc độ khách thể và công cụ phạm tội, tội phạm công nghệ cao trước tiên xâm phạm, làm ảnh hưởng đến hoạt động bình thường của hệ thống máy tính, mạng kết nối và các thiết bị phụ trợ có liên quan. Sự xâm phạm ở

[15] Kranenbarg, W. M., & Leukfeldt, R. (2021). *Cybercrime in Context: The human factor in victimization, offending, and policing* (Crime and Justice in Digital Society, I) (1st ed. 2021 ed.). Springer

đây được hiểu theo nghĩa rộng, nghĩa là từ các việc làm hỏng hóc, chiếm đoạt, làm sai lệnh thông tin của máy chủ, mạng máy tính và các thiết bị liên quan cũng như các thông tin được chứa đựng bên trong hệ thống máy tính và mạng máy tính. Các khách thể này rất đa dạng, từ chiếc máy tính đơn nhất, các thiết bị chuyển đổi của mạng máy tính... đến các chương trình phần mềm, các thông tin chứa đựng trong hệ thống máy tính và hệ thống mạng. Cùng với đó, máy tính và các thiết bị có liên quan còn là một loại tài sản có giá trị, do vậy nó cũng có thể trở thành đối tượng của các các tội về xâm phạm quyền sở hữu như trộm cắp hay phá hoại tài sản. So với tội phạm thông thường, tội phạm mạng là một loại hình tương đối mới mẻ đi kèm với sự thiệt hại lớn, không thua kém gì so với các loại hình tội phạm truyền thống. Làn sóng tội phạm công nghệ cao với quy mô lớn đầu tiên xuất hiện vào những năm 1980 với sự gia tăng của việc lừa đảo qua email. Với chiêu trò gửi tới hòm thư điện tử của cá nhân những tín hiệu hoặc nội dung lừa đảo, tiêu biểu là vụ Email giả mạo Hoàng tử Nigeria (Fake Nigerian Prince Scam E-mails) kêu gọi trợ giúp thông qua chuyển khoản tiền ủng hộ vào số tài khoản mạo danh[16]... Làn sóng tiếp theo của tội phạm công nghệ cao diễn ra vào đầu những năm 1990, đây là thời điểm thịnh vượng của các trình duyệt Web-browser. Những trình duyệt này là công cụ trung gian lây nhiễm, phát tán các loại virus và mã độc vào máy tính cá nhân của người dùng bất cứ khi nào họ truy cập vào đến các link website nguy hiểm. Một số mã độc thường khiến máy tính chạy chậm đi, hoặc đa phần các mã độc thường khiến các thiết bị truy cập của người dùng tự động phát các đoạn pop-ups quảng cáo không mong muốn... Điều này gây ra rất nhiều phiền nhiễu hoặc trong nhiều trường hợp tồi tệ hơn, những mã độc có thể gây mất thông tin cá nhân hoặc điều hướng thiết bị đến những trang web khiêu dâm hay lừa đảo trá hình...

Thứ hai, về chủ thể của tội phạm, tội phạm công nghệ cao được thực hiện bởi các đối tượng có kiến thức cập nhật và am hiểu sâu về máy tính. Để thực hiện hành vi phạm tội, người phạm tội cần có những kiến thức đủ sâu về máy tính để thực hiện hành vi cũng như che giấu bằng chứng. Tuy nhiên, cũng có trường hợp chủ thể là những người không hiểu biết đầy đủ về các quy định liên quan đến vận hành, khai thác và sử dụng mạng máy tính hoặc các công cụ điện tử dẫn đến những thiệt hại ngoài ý muốn. Một vấn đề nữa đáng lưu ý hiện nay đối với chủ thể của nhóm tội phạm này là tình trạng ngày càng "trẻ hoá" của các tin tặc (hacker). Với sự phát triển của công nghệ thông tin và các chương trình phần mềm mới, giới trẻ luôn là thế hệ nhận biết nhanh nhạy những công nghệ mới, cộng với tính cách còn bồng

[16] Xem *https://www.le-vpn.com/history-cyber-crime-origin-evolution/* (truy cập lần cuối 20/3/2020)

bột, thích tìm tòi, khám phá hay thể hiện mình nên rất dễ dẫn đến việc rơi vào con đường phạm tội với những động cơ và mục đích hết sức đơn giản, ngây thơ, chẳng hạn tạo ra và phát tán virus tin học gây hại chỉ để đùa vui, phá bĩnh hoặc thâm nhập các trang thông tin điện tử chỉ để thể hiện khả năng và thỏa mãn tính hiếu kỳ của bản thân.

Thứ ba, về tính chất của hành vi phạm tội và các hành vi có liên quan đến tội phạm công nghệ cao thường rất tinh vi, tinh xảo. Tính chất này được quyết định bởi rất nhiều yếu tố như: tội phạm công nghệ cao phá huỷ hoạt động của các đối tượng tồn tại dưới dạng phi vật chất, như chương trình máy tính hoặc dữ liệu điện tử, mà không phá huỷ máy tính hoặc phá hủy mạng thông tin hay các linh kiện của chúng, nên sự huỷ hoại này không để lại các dấu vết của sự phá huỷ tồn tại dưới dạng vật thể. Tốc độ thực hiện hành vi phạm tội diễn ra tương đối nhanh, kẻ phạm tội có thể chỉ cần thực hiện hành vi trong nháy mắt, chúng có thể thực hiện hành vi phạm tội chỉ trong vòng một phần nghìn, thậm chí một phần triệu giây bằng các máy tính có tốc độ xử lý siêu tốc hoặc bằng những chiếc USB có chứa siêu mã độc. Hơn nữa, tội phạm không bị hạn chế về thời gian, không gian, chúng có thể thực hiện hành vi phạm tội bất cứ khi nào, bất cứ nơi đâu thậm chí từ từ nước ngoài hoặc một nơi rất xa hiện trường. Chính vì vậy, với công tác đấu tranh phòng chống, loại bỏ loại hình tội phạm này, việc điều tra thu thập dấu vết là cực kỳ khó khăn. Bởi kẻ phạm tội có thể xoá bỏ hoàn toàn các dấu vết của hành vi phạm tội với một chương trình xoá dấu vết đã được cài đặt sẵn khi các mệnh lệnh phạm tội được thực hiện…

Ngoài các đặc điểm khác biệt cơ bản kể trên, cũng có thể thấy một số dấu hiệu đặc thù khác so với các nhóm tội phạm thông thường như tính quốc tế, tính xuyên biên giới của loại tội phạm này; tính chất ngày càng tăng về số lượng và hậu quả, tinh vi về cách thức tiến hành cùng với sự phát triển của cuộc cách mạng khoa học công nghệ... Hiện nay một số cá nhân hacker ưu tú không chỉ có kiến thức về khoa học công nghệ cao mà còn được trang bị bài bản về pháp lý cũng như quan hệ quốc tế giữa các quốc gia hữu quan; qua đó, tận dụng những "khoảng trống, khe hở" trong mối quan hệ giữa các quốc gia như những "tấm lá chắn" để bảo vệ mình. Nhận biết các dấu hiệu này giúp chúng ta dễ dàng hơn trong việc xác định đúng bản chất của các loại tội danh thuộc nhóm tội phạm công nghệ cao để từ đó đề ra những cơ chế hợp tác cũng như các biện pháp ngăn ngừa và xử lý có hiệu quả.

Tóm lại, tội phạm công nghệ cao, hay còn có thể được tiếp cận dưới nhiều tên gọi khác nhau như tội phạm mạng, tội phạm máy tính, tội phạm internet... là những thuật ngữ có thể sử dụng hoán đổi cho nhau nhằm để chỉ một loại hình tội phạm

mới hình thành trong quá trình phát triển của cuộc cách mạng công nghệ thông tin 4.0 vào cuối thế kỷ 20 và được dự báo là sẽ phát triển rất nhanh trong thời gian sắp tới. Có thể nhận định, tội phạm công nghệ cao chính là "*sản phẩm*" của thời đại mà các cá nhân, tổ chức, các quốc gia và cộng đồng quốc tế phải chấp nhận để đổi lấy sự thịnh vượng và phát triển. Hầu hết các nước trên thế giới đều đã và đang xây dựng những quy phạm pháp luật để ngăn ngừa và trừng trị loại tội phạm này. Bộ luật hình sự hiện nay của Việt Nam cũng cho thấy những bước đi đầu của nước ta trong việc hình sự hóa hành vi phạm tội của loại tội phạm công nghệ cao. Cho dù nội dung còn tương đối khái quát và cần phải được cụ thể hoá, chi tiết hoá từng hành vi cụ thể cũng như bổ sung thêm những hành vi tội phạm mới nhưng việc bước đầu tiếp cận và quy định cũng sẽ là một cơ sở nền tảng tốt cho công cuộc đấu tranh, hợp tác ngăn ngừa loại bỏ loại tội phạm mới này.

2.1.1.3. Phân loại tội phạm công nghệ cao

Hiện nay, chưa có bất kỳ một văn bản pháp lý quốc tế nào đề cập đến các tiêu chí phân loại tội phạm công nghệ cao một cách chính thức. Chính vì vậy, việc phân loại ở đây chỉ mang tính chất tương đối và chủ yếu căn cứ trên thực tiễn diễn biến tình hình của loại tội phạm này cũng như thực tiễn pháp luật của một số quốc gia trên thế giới khi tiếp cận và đề cập đến tội phạm công nghệ cao.

Một cách phân loại phổ biến trên thế giới hiện nay là phân loại tội phạm sử dụng công nghệ cao theo cách thức, mục tiêu thực hiện tội phạm; theo đó, tội phạm công nghệ cao bao gồm hai nhóm:

- Nhóm thứ 1: Tội phạm có mục tiêu chính là mạng máy tính và thiết bị bao gồm: Virus máy tính; Tấn công từ chối dịch vụ; mã độc (Crimes that primarily target computer networks or devices include: Computer viruses; Denial-of-service attacks; Malware (malicious code).

- Nhóm thứ 2: Tội phạm sử dụng mạng máy tính hoặc thiết bị để làm công cụ hỗ trợ cho hoạt động phạm tội bao gồm: Đe dọa quấy rối trên mạng; lừa đảo trộm cắp thông tin nhân thân; chiến tranh thông tin; gửi thông điệp lừa đảo[17].

Dựa trên vai trò của máy tính trong hành vi phạm tội thì tội phạm công nghệ cao bao gồm những tội phạm có sự liên can, dính líu của máy tính tới tội phạm với ba vai trò sau:

- Máy tính là mục đích của tội phạm: Những tội phạm này có thể bao gồm

[17] Máy tính và Internet: Dưới góc nhìn tội phạm học, nhóm tác giả Masoud Nosrati, Mehdi Hariri, Alireza Shakarbeygi ("Crimes that use computer networks or devices to advance other ends include: Cyberstalking; Fraud and identity theft; Information warfare; Phishing scams").

trộm cắp dữ liệu, phát tán vi rút hoặc trộm cắp phần cứng.

- Máy tính là công cụ phạm tội: Các máy tính hoạt động như một vũ khí để phạm tội. Tội phạm sử dụng máy tính và công nghệ để thực hiện nhiều loại tội phạm truyền thống.

- Máy tính là vật trung gian để cất giấu, lưu trữ những thứ đã chiếm đoạt được. Máy vi tính cũng hoạt động như một phụ kiện pháp lý, lưu trữ thông tin bắt buộc. Theo quan điểm này thì rất nhiều các loại tội phạm truyền thống cũng đều bị coi là tội phạm công nghệ thông tin hay tội phạm tin học, đặc biệt là những tội sử dụng máy tính, mạng máy tính làm công cụ, phương tiện phạm tội, ví dụ như tội đánh bạc trên mạng, tội cung cấp các dịch vụ mại dâm trực tuyến, tội truyền bá văn hoá phẩm đồi truỵ trên mạng[18]...

Căn cứ vào tính chất hoạt động của hành vi phạm tội, tội phạm công nghệ cao có thể được chia ra làm nhiều dạng thức như:

- Thứ nhất, Hacking (Xâm nhập): Đây là loại hành vi phạm tội có khả năng nắm rõ chương trình trực tuyến một cách tinh vi và sử dụng khả năng của mình để xâm nhập vào hệ thống máy tính, hệ thống dữ liệu của phần mềm bảo mật và truy cập thông tin cá nhân của người dùng. Mục tiêu của tin tặc dạng này thường là lợi dụng thông tin để làm những việc khác nhau. Có thể chỉ đơn giản là đánh cắp thông tin và bán cho người khác, hay thực hiện hoạt động gián điệp công nghiệp, xâm nhập vào hệ thống của các doanh nghiệp và ăn cắp kế hoạch chiến lược kinh doanh, bản quyền sản phẩm....Ngoài ra, việc xâm nhập máy tính còn có thể là dùng để đe dọa hoặc đánh sập hệ thống đó[19].

- Thứ hai, Identity Theft (Mạo danh) Dạng thức này sẽ đánh cắp thông tin danh tính cá nhân của người khác và sử dụng chính thông tin đó cho mình hay đem rao bán ở các diễn đàn ngầm trên mạng. Những thông tin bị đánh cắp này có thể được dùng để rút tiền từ tài khoản trực tuyến, mua hàng qua mạng hay thanh toán, trao đổi cho những hoạt động khác trên Internet.

- Thứ ba, Fraud (Gian lận) Loại hình phạm tội này không cần phải đột nhập vào máy chủ để có được thông tin cá nhân, Hacker và Identity Theft có thể xây dựng những chương trình giả mạo lừa người dùng tự động cung cấp thông tin cá

---

[18] Masoud Nosrati, Mehdi Hariri, Alireza Shakarbeygi (2013), *Computers and Internet: From a Criminological View*, International Journal of Economy, Management and Social Sciences, 2 (4)

[19] Ngày 25-3-2010, tòa án New Jersey, Hoa Kỳ đã tuyên án 20 năm tù giam đối với Albert Gonzalez, kẻ được mệnh danh là "hacker của thế kỷ 21", vì phạm tội đánh cắp dữ liệu của 170 triệu thẻ tín dụng trong khoảng thời gian từ năm 2005 đến năm 2007. Đây là một vụ án lớn nhất trong lịch sử tội phạm cùng loại, gây chấn động dư luận Hoa Kỳ lẫn toàn thế giới do mức độ thiệt hại nặng nề.

nhân cho chúng. Tội phạm dạng thức này sẽ mở một cửa hàng hoặc một dịch vụ giả mạo và yêu cầu nạn nhân tạo một tài khoản với các thông tin cá nhân để có thể sử dụng sản phẩm hay dịch vụ đó. Thủ đoạn thường thấy là gửi lời mời qua email cho nạn nhân về một dịch vụ giá rẻ hoặc miễn phí. Từ những thông tin mà chính người dùng cung cấp, tội phạm mạng dễ dàng đột nhập vào tài khoản cá nhân, tài khoản ngân hàng và thực hiện hành vi phạm tội.

- Thứ tư, Predators (Kẻ săn mồi): Đây là dạng tội phạm mạng chuyên sử dụng mạng xã hội để tìm kiếm nạn nhân và thu thập thông tin. Qua những giao tiếp trực tuyến như nói chuyện, đưa ra tình huống lựa chọn và tạo dựng kịch bản lừa đảo dựa trên những thông tin mà nạn nhân vô tình cung cấp (chẳng hạn như thường vắng nhà khi nào, tìm hiểu thói quen hàng ngày) và chờ thời cơ ra tay. Tội phạm này dựa trên việc muốn mở rộng giao lưu kết bạn với mọi người trên mạng xã hội. Bằng những câu hỏi qua lại, tội phạm chèo lái để lấy được những thông tin cần thiết rồi thực hiện hành vi. Vì vậy, khi giao tiếp trực tuyến với ai đó, bạn cần cân nhắc, cảnh giác và tìm hiểu kĩ mối quan hệ để có thể tự bảo vệ mình.

Tại Việt Nam, Hướng dẫn 16/HD-BCA-C41 ngày 31/12/2013 của Bộ Công an hướng dẫn thực hiện một số quy định trong các Thông tư 18, 19, 20, 21, 22 ngày 01/04/2013 của Bộ trưởng Bộ Công an quy định về công tác nghiệp vụ cơ bản của lực lượng Cảnh sát nhân dân có hướng dẫn việc phân chia các nhóm đối tượng phạm tội có sử dụng công nghệ cao thành hai hệ là: Hệ xâm phạm hoạt động của mạng máy tính, viễn thông và Hệ lợi dụng mạng máy tính, viễn thông để hoạt động bất hợp pháp. Theo đó, tội phạm sử dụng công nghệ cao được phân loại như sau: (i) Tội phạm sử dụng máy tính, thiết bị số, mạng máy tính, mạng viễn thông gây tổn hại tính bảo mật, tính toàn vẹn và tính khả dụng của hệ thống máy tính; và (ii) Tội phạm sử dụng máy tính, thiết bị số, mạng máy tính, mạng viễn thông làm công cụ, phương tiện phạm tội.

2.1.2. Khái niệm hợp tác đấu tranh phòng chống tội phạm công nghệ cao

2.1.2.1. Định nghĩa hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Trước hết, thuật ngữ "hợp tác" trong tiếng Anh là "cooperation" chỉ "*hành động hoặc làm việc cùng nhau cho một mục đích cụ thể*"[20]. Ngày nay, việc hợp tác đã và đang diễn ra trong nhiều lĩnh vực của đời sống xã hội thể hiện sự quyết tâm của cộng đồng quốc tế trong việc giúp đỡ, tạo điều kiện cùng nhau phát triển; cùng

[20]Theo Từ điển Cambridge, xem tại: https://dictionary.cambridge.org/dictionary/english/cooperate, (truy cập lần cuối ngày 28/3/2020)

nhau giải quyết những vấn đề mang tính toàn cầu và để đạt được mục tiêu hoà bình cho toàn thể nhân loại. Theo Đại từ điển tiếng Việt thì "*Hợp tác là cùng chung sức, giúp đỡ lẫn nhau trong một công việc, một lĩnh vực nào đó nhằm một mục đích chung*"[21]. Cơ sở để tiến hành hợp tác đó là sự thống nhất, đồng thuận nhất định về lợi ích giữa các chủ thể trong quan hệ, giải quyết công việc. Các chủ thể có thể hợp tác với nhau khi giữa họ tạo ra được sự thống nhất, đồng thuận về lợi ích và cùng nhau chia sẻ lợi ích với nhau. Do vậy, có thể hiểu rằng, hợp tác được đặt ra nhằm một mục đích nhất định, để giải quyết một nhu cầu chung trong một công việc hay lĩnh vực cụ thể nào đó. Trong tiếng Việt, "*hợp tác quốc tế*" phản ánh bản chất của hoạt động hợp tác trong một lĩnh vực nhất định của đời sống quốc tế, bao gồm các vấn đề về chính trị, kinh tế, văn hoá và xã hội, nó diễn ra giữa các chủ thể của luật quốc tế mang tính chất liên quốc gia, liên chính phủ.

Hợp tác đấu tranh, phòng chống tội phạm công nghệ cao là một trong những nội dung cơ bản của hợp tác quốc tế nói chung và hợp tác quốc tế trong đấu tranh phòng chống tội phạm nói riêng. Hợp tác quốc tế trong đấu tranh phòng chống tội phạm là yêu cầu tất yếu khách quan trong điều kiện hội nhập quốc tế hiện nay, đáp ứng nhanh chóng yêu cầu cấp thiết trong việc đấu tranh, xử lý, phòng chống tội phạm của mỗi quốc gia, hướng tới sự phát triển bền vững của cộng đồng quốc tế. Bên cạnh đó, việc hợp là nhu cầu thiết yếu để giải quyết những vấn đề mang tính toàn cầu. Đối với TPCNC, do có những đặc điểm khác biệt so với các nhóm tội phạm thông thường như tính quốc tế, tính xuyên biên giới của loại tội phạm này; tính chất ngày càng tăng về số lượng và hậu quả; hay tính tinh vi, tinh xảo về cách thức tiến hành cùng với sự phát triển của cuộc cách mạng khoa học công nghệ cũng như số lượng vụ phạm tội ngày càng gia tăng hiện nay thì việc hợp tác để đấu tranh phòng chống TPCNC có ý nghĩa, vai trò đặc biệt quan trọng để ngăn ngừa, trừng trị tội phạm này. Hợp tác quốc tế đấu tranh phòng chống TPCNC bao gồm toàn bộ các hoạt động cần thiết của cộng đồng quốc tế cũng như các quốc gia nhằm ngăn ngừa, trừng trị tội phạm công nghệ cao. Về phạm vi của hoạt động này, có thể tiến hành hợp tác song phương, hợp tác khu vực hoặc hợp tác trên phạm vi toàn cầu. Về nội dung của hoạt động, có thể tiến hành hợp tác trong việc xác định thẩm quyền tài phán đối với TPCNC; hợp tác nhằm thiết lập các thiết chế tài phán quốc tế để tiến hành truy cứu, xét xử, trừng trị tội phạm; hợp tác trong việc xây dựng các văn bản pháp luật quốc tế nhằm điều chỉnh loại tội phạm này…

[21]Đại từ điển tiếng Việt, trang 45

Theo các nhà nghiên cứu pháp lý hình sự ở châu Âu đã sử dụng thuật ngữ "***International cooperation in criminal matters***" (Hợp tác quốc tế về các vấn đề hình sự). Hoạt động hợp tác quốc tế này là hợp tác bao gồm cả về nội dung và hình thức, giữa các cơ quan có thẩm quyền của các quốc gia thuộc EU vì mục đích phòng ngừa, điều tra, truy tố, xét xử, thi hành án hình sự. Cơ sở pháp lý cho hoạt động hợp tác này chính là các công ước của EU và pháp luật các nước thành viên EU[22]. Theo giáo trình Luật quốc tế, trường Đại học Luật Hà Nội thì hợp tác quốc tế đấu tranh chống tội phạm bao gồm toàn bộ các hoạt động cần thiết của thành viên cộng đồng quốc tế, nhằm ngăn ngừa, trừng trị, loại bỏ tội phạm ra khỏi đời sống quốc tế cũng như đời sống quốc gia, bao gồm các hành động cụ thể, được thực hiện trong nhiều lĩnh vực thuộc các hoạt động tư pháp như phân định thẩm quyền xét xử, thoả thuận thành lập toà án quốc tế, tương trợ tư pháp của các quốc gia trong các vụ việc hình sự, dẫn độ tội phạm, chuyển giao phạm nhân để thụ án. Như vậy, có thể hiểu rằng "*Hợp tác đấu tranh phòng chống tội phạm công nghệ cao là việc các quốc gia cũng như các chủ thể khác của luật quốc tế trên cơ sở pháp luật quốc gia, điều ước quốc tế hay các tập quán quốc tế, cũng như các nguyên tắc khác tiến hành phối hợp, giúp đỡ nhau trong xây dựng cơ sở pháp lý và thực hiện tương trợ tư pháp về hình sự, dẫn độ, tiếp nhận, chuyển giao người bị kết án và các hoạt động hợp tác khác nhằm phục vụ cho việc điều tra, truy tố, xét xử, thi hành án và trừng trị tội phạm công nghệ cao*".

2.1.2.2. Đặc điểm hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Trên cơ sở khái niệm hợp tác đấu tranh phòng chống tội phạm công nghệ cao, có thể rút ra một số đặc điểm cơ bản như sau:

Thứ nhất, về chủ thể hợp tác

Trong khoa học pháp lý quốc tế hiện nay đều ghi nhận chủ thể của hợp tác quốc tế chính là chủ thể của luật quốc tế. Bởi lẽ, hoạt động hợp tác đấu tranh phòng chống tội phạm nói chung và hợp tác đấu tranh phòng chống tội phạm công nghệ cao nói riêng là một trong những vấn đề pháp lý cơ bản của Luật hình sự quốc tế. Trong hệ thống pháp luật quốc tế, Luật hình sự quốc tế là một ngành luật độc lập, bao gồm tổng thể các nguyên tắc, các quy phạm pháp lý quốc tế điều chỉnh các vấn đề pháp lý trong hoạt động hợp tác đấu tranh phòng chống tội phạm của cộng đồng

---

[22] Xem: International cooperation in criminal matters, xem tại: https://www.ejtn.eu/Catalogue/Catalogue-20191/International-cooperation-in-criminal-matters/, truy cập lần cuối ngày 28/3/2020

quốc tế. Do vậy, chủ thể trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao là các quốc gia, các tổ chức quốc tế liên chính phủ, các dân tộc đang đấu tranh dành quyền tự quyết và nhóm các chủ thể đặc biệt. Đặc biệt, theo quan niệm trong hợp tác quốc tế hiện nay, các quốc gia là chủ thể chủ yếu và quan trọng nhất của hoạt động hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao. Các quốc gia và các chủ thể khác tham gia vào quá trình hợp tác quốc tế nhằm tạo điều kiện thuận lợi cho quá trình giải quyết vụ án, ngăn ngừa, phòng chống, trừng trị và loại bỏ tội phạm công nghệ cao một cách có hiệu quả. Phạm vi hợp tác của các chủ thể sẽ phụ thuộc vào điều kiện hoàn cảnh cụ thể của từng quốc gia cũng như của các chủ thể khác, đồng thời nó còn phụ thuộc vào yêu cầu của hội nhập quốc tế.

Hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao không chỉ được thực hiện giữa các quốc gia với nhau mà còn được tiến hành với sự tham gia tích cực, năng động trong khuôn khổ của các tổ chức quốc tế với chuyên môn và kỹ thuật cao như Liên hợp quốc, Tổ chức cảnh sát hình sự quốc tế, Hiệp hội Cảnh sát các nước ASEAN, Tổ chức hàng không dân dụng quốc tế và hàng loạt các tổ chức quốc tế chuyên môn của Liên hợp quốc, cũng như các Tổ chức quốc tế phi chính phủ khác. Có thể nói rằng, vị trí và vai trò của các tổ chức quốc tế trong đấu tranh phòng chống tội phạm nói chung và tội phạm công nghệ cao nói riêng là không thể bỏ qua. Sự hợp tác tích cực của các tổ chức quốc tế tạo ra một sức mạnh tổng hợp, sắc bén và đầy chắc chắn trong đấu tranh ngăn ngừa và trừng trị tội phạm công nghệ cao. Trong bối cảnh mà tội phạm công nghệ cao ngày càng gia tăng do sự bùng nổ của khoa học công nghệ trên phạm vi toàn cầu thì cộng đồng quốc tế phải hợp tác chặt chẽ với nhau, không chỉ các quốc gia mà còn cả các tổ chức quốc tế để thống nhất ý chí trong cuộc chiến phòng chống tội phạm công nghệ cao. Bởi đó là nơi tập trung những nhân tài, những con người có chuyên môn cao, cũng như các công cụ, thiết bị và vật lực với kỹ thuật cao và hiệu quả trong đấu tranh phòng chống tội phạm công nghệ cao. Các tổ chức quốc tế này tham gia vào sự nghiệp đấu tranh phòng tội phạm công nghệ cao một cách năng động trong phạm vi mục đích, nhiệm vụ được quy định tại các điều ước quốc tế thành lập tổ chức, cũng như trong các điều ước quốc tế trong quá trình hoạt động của tổ chức.

Ngoài ra, các dân tộc đang đấu tranh dành quyền tự quyết và nhóm các chủ thể đặc biệt cũng tham gia vào quá trình hợp tác đấu tranh phòng chống tội phạm công nghệ cao ở một phạm vi và mức độ nhất định tuỳ vào điều kiện và hoàn cảnh cụ thể.

Thứ hai, về đối tượng hợp tác

Đối tượng của hợp tác đấu tranh phòng chống tội phạm công nghệ cao là các loại tội phạm công nghệ cao xảy ra trên thực tế. Như đã phân tích, tội phạm công nghệ cao là một dạng thức tội phạm sử dụng tri thức, kỹ năng, công cụ, phương tiện và thành tựu của công nghệ thông tin ở trình độ cao, tác động một cách bất hợp pháp đến thông tin số và các dữ liệu điện tử được lưu trữ, xử lý, truyền tải trong hệ thống máy tính và các thiết bị công nghệ cao, xâm phạm đến trật tự an toàn thông tin, gây tổn hại nghiêm trọng đến quyền và lợi ích hợp pháp của các cá nhân, tổ chức cũng như của các quốc gia và cộng đồng quốc tế. Các đối tượng có thể tiến hành tội phạm dưới dạng như: giả danh cán bộ cơ quan Công an, Viện Kiểm sát, Tòa án gọi điện cho người dân để thực hiện hành vi lừa đảo, gây sức ép, yêu cầu khác nhau; lừa đảo qua mạng xã hội nhằm chiếm đoạt tài khoản mạng xã hội cũng như thực hiện các hành vi lừa đảo chiếm đoạt tài sản; tấn công mạng để chiếm đoạt thông tin, tài khoản… và một loạt các hành vi phạm tội khác. Hoạt động phạm tội của các đối tượng này hiện nay có rất nhiều thủ đoạn vô cùng tinh vi và phức tạp, gây rất nhiều khó khăn cho các quốc gia trong việc ngăn ngừa và trừng trị những hành vi phạm tội. Chính vì vậy, đòi hỏi phải có sự hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao.

Thứ ba, mục tiêu hợp tác

Hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao là nhu cầu cần thiết, cấp bách, mang tính tất yếu khách quan xuất phát từ yêu cầu đấu tranh, phòng chống và giải quyết loại tội phạm này trong bối cảnh toàn cầu hoá hiện nay. Chính vì vậy, hợp tác đấu tranh phòng chống tội phạm công nghệ cao hướng tới các mục tiêu chủ yếu sau đây: (1) Hợp tác đấu tranh phòng chống tội phạm công nghệ cao nhằm mục đích giải quyết vụ án về TPCNC một cách nhanh chóng, khách quan, công bằng, hiệu quả không chỉ trong phạm vi một quốc gia mà trên phạm vi toàn cầu. Như đã phân tích, một trong những đặc điểm của TPCNC đó là đối tượng có trình độ công nghệ thông tin chuyên sâu, có những hành vi tinh vi, tinh xảo, có phạm vi hoạt động rộng, dễ cấu kết với nhau, đặc biệt là tính quốc tế, tính xuyên biên giới nên cần phải có sự hợp tác quốc tế trong việc đấu tranh phòng chống loại tội phạm này; (2) Hợp tác đấu tranh phòng chống tội phạm công nghệ cao hướng tới việc bảo vệ chủ quyền của các quốc gia, bảo vệ quốc gia khỏi những tác động tiêu cực trước sự xâm phạm và tấn công của tội phạm diễn ra tại các quốc gia và trên phạm vi toàn cầu. TPCNC thường nhằm vào tính bảo mật, tính toàn vẹn và tính khả dụng của các dữ liệu cũng như làm trầm trọng thêm tình hình các loại tội phạm truyền thống như buôn bán ma tuý, buôn bán người, rửa tiền… Những hậu quả mà

TPCNC gây ra cực kỳ lớn, nó không chỉ ảnh hưởng đến một quốc gia mà thậm chí có liên quan đến rất nhiều quốc gia. Chính vì vậy, chỉ có hợp tác đấu tranh phòng chống tội phạm công nghệ cao mới huy động được sức mạnh của toàn thể cộng đồng quốc tế trong đấu tranh, phòng chống TPCNC hướng tới bảo vệ công lý, bảo vệ hoà bình và an ninh quốc tế, bảo vệ chủ quyền của các quốc gia; (3) Hợp tác đấu tranh phòng chống tội phạm công nghệ cao tăng cường quan hệ hữu nghị, hợp tác giữa các quốc gia đòi hỏi cần có sự nỗ lực, đặc biệt là thiện chí của các quốc gia đối với các hoạt động hợp tác quốc tế trong phòng chống tội phạm. Sự nỗ lực, thiện chí của các quốc gia hữu quan sẽ đưa đến những giải pháp tích cực, hiệu quả kịp thời ngăn chặn tội phạm công nghệ cao, xử lý khách quan, công bằng tội phạm do đó làm cho thỏa thuận đa phương, song phương trong hợp tác quốc tế trong phòng chống tội phạm trở thành hiện thực trong đời sống quốc tế.

Thứ tư, về hình thức hợp tác

Hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao là quá trình các quốc gia và các chủ thể khác của luật quốc tế hợp tác, trao đổi, giúp đỡ lẫn nhau, cũng như xây dựng và thực thi pháp luật quốc tế về đấu tranh phòng chống tội phạm công nghệ cao. Các hình thức hợp tác quốc tế về phòng chống tội phạm công nghệ cao không được quy định cụ thể trong các văn bản quy phạm pháp luật quốc tế mà thông qua nghiên cứu về các văn bản đó thì chúng ta có thể đưa ra các hình thức hợp tác.

Trong thực tế, các hoạt động hợp tác quốc tế được thực hiện bằng con đường tương trợ tư pháp trong việc truy tìm kẻ phạm tội lẩn trốn trên lãnh thổ quốc gia khác, dẫn độ tội phạm cho các quốc gia có liên quan hay chuyển giao người đã bị kết án hoặc tiếp nhận các thông tin, tài liệu cần thiết về vụ việc hình sự…

Từ phương diện hiệu lực theo lãnh thổ thì các hành vi tố tụng hình sự của cơ quan nhà nước có thẩm quyền chỉ có thể được thực hiện trong phạm vi giới hạn lãnh thổ của quốc gia. Tuy nhiên, trong nhiều trường hợp, hoạt động xét xử các vụ việc hình sự chỉ có thể được tiến hành bình thường và đạt được kết quả nếu có sự thực hiện các hành vi tố tụng hình sự trên lãnh thổ của nước khác. Điều này đồng nghĩa với việc phải giải quyết vụ việc hình sự với sự trợ giúp của nước ngoài trong quá trình thực hiện các hành vi tố tụng cần thiết. Song, nguyên tắc chủ quyền quốc gia đã loại bỏ việc thực hiện các hành vi tố tụng của cơ quan nhà nước một quốc gia trên lãnh thổ của quốc gia khác. Vì vậy, việc phòng chống tội phạm hình sự quốc tế nói chung và phòng chống tội phạm sử dụng công nghệ cao nói riêng gặp nhiều khó khăn, đòi hỏi phải có tương trợ tư pháp về hình sự. Sự điều chỉnh của luật quốc tế

đối với hợp tác tương trợ pháp lý về hình sự thường tập trung vào một số vấn đề sau:

(i) Chuyển giao và tiếp nhận các giấy tờ, tài liệu có liên quan đến vụ việc hình sự được thụ lý và giải quyết;

(ii) Cung cấp các thông tin cần thiết về luật pháp hiện hành và thực tiễn tòa án; Thẩm vấn nghi can, người làm chứng, bị cáo và các chuyên gia;

(iii) Tiến hành các hoạt động giám định và khám xét tư pháp, chuyển giao vật chứng; Thực hiện các hoạt động truy cứu hình sự, dẫn độ tội phạm;

(iv) Các hoạt động tương trợ pháp lý khác theo yêu cầu và phù hợp với từng hoàn cảnh, từng trường hợp cụ thể sẽ được thỏa thuận và ghi nhận trong các hiệp định hữu quan giữa các bên thành viên.[23]

Các nội dung tương trợ tư pháp về hình sự này có ý nghĩa cực kỳ quan trọng trong phòng chống tội phạm sử dụng công nghệ cao, vì trong bối cảnh tội phạm này mang đặc điểm không có biên giới, việc thu thập chứng cứ càng trở nên khó khăn nếu không có hợp tác quốc tế.

Trong quan hệ quốc tế, dẫn độ tội phạm cũng là một trong số các nội dung của hợp tác quốc tế chống tội phạm, là hình thức giúp đỡ pháp lý trong việc thực hiện thẩm quyền xét xử tư pháp. Đây là hành vi tương trợ pháp lý, được thỏa thuận giữa các quốc gia hữu quan (quốc gia yêu cầu và quốc gia được yêu cầu dẫn độ) dựa trên cơ sở các quy định của luật quốc tế, trong đó một quốc gia được yêu cầu sẽ thực hiện việc chuyển giao cá nhân đang hiện diện trên lãnh thổ nước mình cho quốc gia có yêu cầu để tiến hành truy cứu trách nhiệm hình sự hoặc thi hành bản án đã có hiệu lực pháp luật đối với cá nhân đó. Theo nguyên tắc chung đã được luật quốc tế công nhận, dẫn độ tội phạm là quyền của quốc gia chứ không phải là nghĩa vụ pháp lý quốc tế của quốc gia. Nói cách khác, dẫn độ tội phạm thuộc thẩm quyền riêng biệt của quốc gia được yêu cầu dẫn độ - nơi tội phạm đang có mặt. Dựa trên cơ sở quyền tối cao đối với lãnh thổ, quốc gia có toàn quyền quyết định tiến hành truy cứu trách nhiệm hình sự đối với các cá nhân đang ở trên lãnh thổ nước mình phù hợp với luật quốc gia. Nghĩa vụ dẫn độ tội phạm chỉ phát sinh trong trường hợp có điều ước quốc tế tương ứng ghi nhận các điều kiện cụ thể cho phép dẫn độ. Chính vì vậy, các quốc gia đã ký kết các điều ước quốc tế song phương hoặc đa phương điều chỉnh các vấn đề có liên quan đến dẫn độ tội phạm trong quan hệ quốc tế. Các điều

[23]Trường Đại học Luật Hà Nội (2019), Giáo trình Luật quốc tế, Nhà xuất bản Công an nhân dân, Hà Nội, tr. 344.

ước quốc tế ký kết giữa các quốc gia được coi là cơ sở pháp lý của dẫn độ tội phạm.[24]

Một hình thức khác của hợp tác quốc tế phòng chống tội phạm sử dụng công nghệ cao là chuyển giao người đã bị kết án về tội phạm này. Đây là việc một quốc gia thực hiện chuyển giao người nước ngoài phạm tội đã bị toà án của quốc gia đó kết án và bản án đã có hiệu lực pháp luật về nước mà người bị kết án là công dân hoặc một nước khác đồng ý tiếp nhận để tiếp tục thi hành bản án trên cơ sở sự đồng ý tự nguyện của người bị kết án hoặc đại diện hợp pháp của họ. Hình thức này tạo điều kiện cho người đang chấp hành hình phạt tù có cơ hội được chấp hành hình phạt tại chính đất nước mà mình mang quốc tịch hay tại chính quê hương của mình, hỗ trợ điều kiện cải tạo tốt nhất, tạo điều kiện thuận lợi cho việc tái hòa nhập cộng đồng thành công, giảm thiểu nguy cơ tái phạm, trở thành người có ích cho xã hội.

Ngoài ra, trong đấu tranh phòng chống tội phạm công nghệ cao không thể thiếu những cơ sở pháp lý quốc tế làm cơ sở cho hoạt động hợp tác quốc tế. Việc ký kết các điều ước quốc tế song phương và đa phương về vấn đề phòng chống tội phạm sử dụng công nghệ cao cũng là một hình thức quan trọng của hợp tác quốc tế trong lĩnh vực này. Mặc dù hiện nay vẫn chưa có điều ước quốc tế quy định riêng về lĩnh vực phòng chống tội phạm sử dụng công nghệ cao nhưng đã có những điều ước quốc tế trong hợp tác đấu tranh phòng chống tội phạm hình sự quốc tế. Qua đó cũng có thể thấy rằng cộng đồng quốc tế đã nhận thức được tầm quan trọng của hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao.

2.2. Lý luận về pháp luật quốc tế trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao

2.2.1. Định nghĩa và đặc điểm của pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao

Trên cơ sở chủ quyền quốc gia và nguyên tắc thẩm quyền theo lãnh thổ, tội phạm thực hiện trên lãnh thổ của quốc gia nào thì quốc gia đó có thẩm quyền xét xử. Hoạt động xét xử và các trình tự thủ tục tố tụng hình sự, về nguyên lý, chỉ được tiến hành bởi các cơ quan có thẩm quyền theo quy định của pháp luật trong phạm vi giới hạn lãnh thổ của quốc gia. Tuy nhiên, nhiều trường hợp, hoạt động tội phạm mang tính chất xuyên biên giới, vượt qua giới hạn lãnh thổ của một quốc gia. Chính vì vậy, trong nhiều trường hợp, hoạt động xét xử các vụ việc hình sự chỉ có thể được tiến hành bình thường và đạt được kết quả nếu có sự thực hiện các hành vi tố

[24]Trường Đại học Luật Hà Nội (2019), Giáo trình Luật quốc tế, Nhà xuất bản Công an nhân dân, Hà Nội, tr. 346-347.

tụng hình sự trên lãnh thổ của nước khác. Hay nói một cách khác, các quốc gia đã chia sẻ bớt một phần chủ quyền của mình để tiến hành hợp tác, hỗ trợ giải quyết vụ việc hình sự đối với các quốc gia hữu quan trong quá trình thực hiện các hành vi tố tụng cần thiết. Như vậy, có thể nhận định, hợp tác quốc tế trong đấu tranh phòng, chống tội phạm nói chung và tội phạm công nghệ cao nói riêng là một nhu cầu cấp thiết mang tính quy luật tất yếu khách quan, đặc biệt trong bối cảnh toàn cầu hóa và bùng nổ phát triển khoa học công nghệ.

Pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao bao gồm tổng thể các nguyên tắc và các quy phạm pháp luật điều chỉnh quan hệ giữa các chủ thể luật quốc tế trong việctiến hành toàn bộ những hoạt động cần thiết giữa các bên, nhằm ngăn ngừa, trừng trị, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế cũng như đời sống quốc gia.

Trước tiên, pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao được coi là một nội dung mới được hình thành và gắn liền với sự phát triển của khoa học công nghệ.Mỗi hệ thống pháp luật cho dù là pháp luật quốc tế hay pháp luật quốc gia đều tỏ ra thận trọng với những vấn đề mới phát sinh, nhất là những lĩnh vực mới với sự manh nha hình thành các công cụ pháp lý quốc tế điều chỉnh mang tính ràng buộc. Ngoài ra, với tính chất là một "sản phẩm" của thời đại, tội phạm công nghệ cao hiện nay đã và đang nhận được sự quan tâm của cộng đồng quốc tế trong việc thiết lập những cơ chế hợp tác toàn diện và thực chất.

Thứ hai, chủ thể của pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao bao gồm các chủ thể của Luật quốc tế (các quốc gia, các tổ chức quốc tế liên chính phủ, các dân tộc đang đấu tranh dành quyền tự quyết và nhóm các chủ thể đặc biệt). Trong đó, các quốc gia và các tổ chức quốc tế liên chính phủ hoạt động trong lĩnh vực hình sự quốc tế là những chủ thể đóng vai trò then chốt trong việc xây dựng khuôn khổ pháp lý cũng như tiến hành toàn bộ các nội dung hợp tác quốc tế ngăn ngừa và loại bỏ tội phạm công nghệ cao.Những chủ thể của pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao vừa tham gia vào quá trình xây dựng nên các nguyên tắc, quy phạm pháp luật, đồng thời cũng chính là những chủ thể chịu sự tác động và thực thi các nguyên tắc và quy phạm này. Xuất phát từ tính chất quyền năng chủ thể luật quốc tế của mỗi chủ thể mà từng chủ thể sẽ có những mức độ và phạm vi tham gia hợp tác khác nhau trong từng trường hợp cụ thể.

Thứ ba, đối tượng điều chỉnh của pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao là các quan hệ giữa các quốc gia và các chủ

thể của luật quốc tế trong việc tiến hành toàn bộ những hoạt động cần thiết giữa các bên, nhằm ngăn ngừa, trừng trị, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế cũng như đời sống quốc gia. Những hoạt động hợp tác này bao gồm những nội dung như: quy định nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luật cũng như xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao; tương trợ tư pháp hình sự; dẫn độ tội phạm; chuyển giao người đã bị kết án và phân định thẩm quyền tài phán hình sự.

Thứ tư, về cơ chế xây dựng và thực thi, các nguyên tắc và quy phạm của luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ caocũng không nằm ngoài cơ chế xây dựng và thực thi chung của luật quốc tế. Đó chính là cơ chế tự thỏa thuận-tự thực thi. Các chủ thể của luật quốc tế sẽ chính là những chủ thể thỏa thuận để xây dựng cũng như thực thi các nguyên tắc và quy phạm. Nét đặc thù trong sự hình thành và áp dụng các nguyên tắc, quy phạm của luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao nằm ở chỗ, các nguyên tắc, quy phạm này chịu ảnh hưởng lớn từ các "làn sóng" phát triển của khoa học công nghệ. Chính vì vậy, các quy định của nó rất khó để có thể đạt được tính ổn định lâu dài. Ngoài ra, việc tạo được một cơ chế đủ toàn diện để thực thi trên thực tế hiện còn gặp nhiều khó khăn khi trình độ phát triển khoa học kỹ thuật của các quốc gia khác nhau sẽ không hoàn toàn giống nhau. Chính vì vậy, việc theo dõi và nắm bắt xu thế phát triển của khoa học công nghệ sẽ có tác động lớn tới cơ chế xây dựng và thực hiệncác nguyên tắc và quy phạm của luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao.

Thứ năm, luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao có mối quan hệ gắn bó mật thiết với các nội dung khác của luật hình sự quốc tế, ví dụ như vấn đề dẫn độ, phân định thẩm quyền tài phánhay đặc biệt là các vấn đề hợp tác quốc tế đấu tranh phòng chống tội phạm có tính chất quốc tế...Trên thực tế, một số nội dung của Luật hình sự quốc tế trong việc xác định thẩm quyền tài phánhay vấn đề dẫn độ cũng như việc thực hiện nghĩa vụ thành viên hoàn toàn có thể áp dụng đối với tội phạm công nghệ cao. Điều này là vô cùng cần thiết khi giữa các loại hình tội phạm đều có mối tương quan nhất định với nhau; bên cạnh đó, việc bổ trợ này cũng góp phần hạn chế bớt những "khoảng trống" trong các quy định của pháp luật quốc tế đối với tội phạm công nghệ cao - một loại hình tội phạm ra đời, gắn liền với các giai đoạn phát triển của khoa học kỹ thuật và công nghệ thông tin.

2.2.2. Nguồn của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Ở phạm vi toàn cầu, đến nay mới chỉ có một điều ước quốc tế điều chỉnh loại tội phạm này là Công ước về tội phạm mạng của Uỷ hội châu Âu năm 2001 (Công ước Budapest). Mặc dù Lời nói đầu của Công ước Budapest ghi nhận việc ký kết Công ước nhằm bổ sung cho những khuôn khổ pháp lý hiện có của Uỷ hội châu Âu trong lĩnh vực đấu tranh phòng chống tội phạm nhưng với điều khoản cho phép các quốc gia không phải thành viên Uỷ hội châu Âu tham gia Công ước, Budapest đã chính thức trở thành một khuôn khổ pháp lý hợp tác quốc tế toàn cầu giữa các quốc gia trong phòng chống tội phạm công nghệ cao với 75 thành viên, trong đó có sự tham gia của 28 quốc gia không phải thành viên của Uỷ hội châu Âu.[25] Công ước ngoài việc quy định cụ thể về tội phạm mạng và các biện pháp đấu tranh phòng ngừa loại tội phạm này thì nó còn thiết lập được một cơ chế hợp tác đồng bộ, thống nhất và tương đối hiệu quả giữa các quốc gia thành viên cũng như giữa các quốc gia với các tổ chức quốc tế hiện nay.

Bên cạnh công ước Budapest, một số nội dung của Công ước Palermo về chống tội phạm có tổ chức liên quốc gia năm 2000 mặc dù không trực tiếp đề cập một cách cụ thể đến các loại hình tội phạm công nghệ cao nhưng Công ước Palermo với 41 điều khoản, luôn được coi là một sự tham khảo cần thiết trong quá trình hợp tác quốc tế đấu tranh phòng chống tội phạm. Có thể nói, Công ước của Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia năm 2000 ra đời vào thời điểm mang tính lịch sử, đó là thời điểm chuyển giao thế kỷ. Công ước là một phương tiện hữu hiệu mở đầu và thúc đẩy cho sự hợp tác sâu rộng hơn, chặt chẽ hơn, toàn diện hơn và hiệu quả hơn trong công cuộc phòng chống loại tội phạm trong quá trình hợp tác quốc tế đấu tranh phòng chống tội phạm có tính chất quốc tế nói chung và tội phạm công nghệ cao nói riêng trên phạm vi toàn cầu.

Ở phạm vi khu vực, một số khuôn khổ pháp lý đã được hình thành làm cơ sở pháp lý cho hoạt động hợp tác giữa các thành viên của một số khu vực trong ngăn ngừa, phòng chống tội phạm công nghệ cao, bao gồm chủ yếu hai loại:

Một là, các điều ước quốc tế khu vực như Thoả thuận của Cộng đồng các quốc gia độc lập về hợp tác trong phòng chống các tội phạm liên quan đến thông tin máy tính năm 2001, Công ước Arab về chống các tội phạm liên quan đến công nghệ

[25] Xem chi tiết các quốc gia thành viên của Công ước về tội phạm mạng của Uỷ hội châu Âu tại https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=eLFlJd5.ffffu -Y, (truy cập lần cuối ngày 13/1/2020)

thông tin năm 2010, Công ước của Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân năm 2014, Thoả thuận của Tổ chức hợp tác Thượng Hải về hợp tác trong lĩnh vực an ninh thông tin quốc tế năm 2010; Nghị định thư của Cộng đồng phát triển Nam Phi về tương trợ tư pháp hình sự và Nghị định của Cộng đồng phát triển Nam Phi về dẫn độ năm 2002; Công ước của Cộng đồng kinh tế các quốc gia Tây Phi về tương trợ tư pháp hình sự, Công ước của Cộng đồng kinh tế các quốc gia Tây Phi về dẫn độ, Hiệp định của ASEAN về tương trợ tư pháp hình sự….

Hai là, các văn bản do những cơ quan có thẩm quyền của các tổ chức quốc tế thông qua, có giá trị pháp lý ràng buộc với các quốc gia thành viên trong ngăn ngừa, phòng chống tội phạm công nghệ cao như Chỉ thị về chống tội phạm mạng do Nghị viện của Cộng đồng kinh tế các quốc gia Tây Phi thông qua năm 2011 hay những văn bản do các thiết chế của Liên minh châu Âu ban hành như Chỉ thị 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, Chỉ thị 2016/1148 của Nghị viện và Hội đồng bộ trưởng ngày 6/7/2016 về những biện pháp nhằm đảm bảo bảo an ninh chung ở mức độ cao của hệ thống mạng và thông tin trên toàn Liên minh, Quyết định 2019/797 của Hội đồng bộ trưởng ngày 17/5/2019 về những biện pháp hạn chế nhằm chống lại các cuộc tấn công mạng đe doạ Liên minh hoặc các quốc gia thành viên…

Ở phạm vi song phương, phổ biến nhất vẫn là các điều ước quốc tế về tương trợ tư pháp hình sự, dẫn độ, chuyển giao người bị kết án được ký kết giữa các quốc gia, làm cơ sở pháp trực tiếp cho việc tiến hành những hoạt động hỗ trợ lẫn nhau giữa các quốc gia trong quá trình giải quyết các vụ án hình sự nói chung và vụ án hình sự liên quan đến tội phạm công nghệ cao nói riêng.

Bên cạnh nguồn thành văn, tập quán quốc tế cũng có vai trò nhất định trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao. Vai trò của tập quán được thể hiện chủ yếu ở những nguyên tắc chung được thừa nhận là tập quán quốc tế trong hoạt động này như nguyên tắc "định danh kép", hay nguyên tắc "hoặc dẫn độ hoặc xét xử" (*aut dedere aut punicare)*.

Cùng với các loại nguồn có giá trị pháp lý ràng buộc như trên, một số các loại nguồn không có giá trị pháp lý ràng buộc, đặc biệt là Nghị quyết mang tính khuyến nghị của các tổ chức quốc tế liên chính phủ và phán quyết của các cơ quan tài phán quốc tế cũng có vai trò quan trọng trong điều chỉnh hoạt động phòng chống tội phạm công nghệ cao.

Có thể thấy, trước năm 2000, vấn đề "an ninh mạng" hay "tội phạm công nghệ cao" hầu như chưa thực sự được quan tâm đề cập đến. Năm 2002, Liên hợp quốc đã

ban hành Nghị quyết số 55/63 và 56/121 về phòng chống hoạt động tội phạm sử dụng công nghệ thông tin. Hai nghị quyết này đã chỉ ra rằng, mạng máy tính và mạng Internet là "nơi ẩn náu an toàn" của những đối tượng tội phạm sử dụng công nghệ thông tin và yêu cầu các quốc gia xây dựng hệ thống quy định pháp luật nhằm ngăn ngừa, đấu tranh và loại bỏ hình thức tội phạm này. Đây được coi là hai văn kiện căn bản nền tảng, góp phần đặt những "viên gạch" đầu tiên trong việc hình thành nhận thức chung của cộng đồng quốc tế về tội phạm công nghệ thông tin cũng như vấn đề phòng chống loại tội phạm mới này[26]. Hay tại ASEAN, trong lĩnh vực phòng chống tội phạm xuyên quốc gia nói chung và tội phạm mạng nói riêng, một số các Tuyên bố chung hay Kế hoạch hành động được thông qua tại các hội nghị bộ trưởng như Tuyên bố Kuala Lumpur về chống tội phạm xuyên quốc gia, Kế hoạch hành động ASEAN về chống tội phạm xuyên quốc gia (2016-2025), Tuyên bố ASEAN về ngăn ngừa và chống tội phạm mạng, Kế hoạch tổng thể về công nghệ thông tin ASEAN năm 2016-2020. Xét về mặt pháp lý, những văn bản này không có giá trị pháp lý ràng buộc nhưng có ý nghĩa rất quan trọng đối với ASEAN trong việc định hình các nội dung hợp tác nói chung và phòng chống tội phạm xuyên quốc gia nói riêng và tội phạm công nghệ cao nói riêng. Bên cạnh đó, một số điều ước quốc tế của ASEAN về tội phạm xuyên quốc gia đã được hình thành từ chính những văn kiện chính trị này như Công ước ASEAN phòng chống khủng bố được nâng cấp từ Tuyên bố ASEAN về hành động chung chống khủng bố 2001, Tuyên bố ASEAN về phòng chống khủng bố 2002 hay Công ước ASEAN về chống buôn bán người, đặc biệt là phụ nữ và trẻ em năm 2015 được nâng cấp từ Tuyên bố ASEAN về chống buôn bán người, đặc biệt là phụ nữ và trẻ em năm 2004. Với xu hướng hoàn thiện pháp luật theo hướng nâng cấp các văn bản từ luật mềm thành các điều ước quốc tế có giá trị pháp lý ràng buộc đang diễn ra khá phổ biến tại ASEAN, trong tương lai, hoàn toàn có khả năng một điều ước quốc tế về chống tội phạm công nghệ cao sẽ được hình thành từ Tuyên bố của ASEAN về ngăn ngừa và chống tội phạm mạng.

Bên cạnh nghị quyết của các tổ chức quốc tế liên chính phủ, phán quyết của các cơ quan tài phán quốc tế, đặc biệt là phán quyết của Toà nhân quyền châu Âu thường được các QGTV của Công ước châu Âu về nhân quyền, đặc biệt là các quốc gia thành viên Liên minh châu Âu viện dẫn khi xem xét các yêu cầu dẫn độ tội phạm của quốc gia yêu cầu liên quan đến các trường hợp không dẫn độ như phán

[26] Xem các Nghị quyết số 55/63 và 56/121 của Liên Hợp Quốc *tại https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf* (truy cập lần cuối ngày 20/3/2020).

quyết trọng các vụ *Abdulazhon Isakov v. Russia, Iskandarov v. Russia, Soering v. United Kingdom…*

2.2.3. Nguyên tắc của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

2.2.3.1. Các nguyên tắc chung của pháp luật quốc tế

Hợp tác quốc tế đấu tranh phòng chống tội phạm nói chung và phòng chống tội phạm công nghệ cao là một trong những hoạt động thuộc đối tượng điều chỉnh của luật quốc tế. Do đó, các nguyên tắc của pháp luật quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao trước tiên cũng bao gồm các nguyên tắc cơ bản của pháp luật quốc tế nói chung, đặc biệt là nguyên tắc bình đẳng tôn trọng về độc lập chủ quyền, không can thiệp vào công việc nội bộ của nhau; nguyên tắc các quốc gia có nghĩa vụ hợp tác và đặc biệt là nguyên tắc Pacta sunt Servanda...

Nguyên tắc tôn trọng độc lập và toàn vẹn lãnh thổ quốc gia, bình đẳng về chủ quyền giữa các quốc gia và không can thiệp vào công việc nội bộ của quốc gia khác được coi là những nguyên tắc tôn chỉ có tính tiên quyết khi tiến hành hợp tác quốc tế đấu tranh phòng chống tội phạm nói chung cũng như tội phạm công nghệ cao nói riêng. Việc hợp tác quốc tế trong phòng chống tội phạm công nghệ cao phải được tiến hành trên cơ sở bình đẳng chủ quyền giữa các quốc gia hữu quan. Khi hợp tác, các bên luôn cam kết đảm bảo vấn đề độc lập, an ninh chủ quyền của quốc gia, tránh những hành vi gây nguy hại đến nền độc lập và toàn vẹn lãnh thổ của các quốc gia khác. Chính vì vậy, trên thực tế, đây được coi là nguyên tắc xuất phát điểm, đóng vai trò nền tảng cho việc thiết lập và triển khai các cấp độ hợp tác từ song phương, khu vực cho đến cấp độ toàn cầu trong đấu tranh phòng chống tội phạm công nghệ cao. Tuy nhiên, nguyên tắc này không có nghĩa là chủ quyền quốc gia là sự tự do tuyệt đối, không có giới hạn trong các hoạt động của các quốc gia trong hợp tác quốc tế. Bởi nếu như các quốc gia quá tuyệt đối hóa chủ quyền của mình thì sẽ rất khó để có thể triển khai các nội dung hợp tác trên cả hai phương diện sâu và rộng. Trong khi việc hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao luôn cần tới sự cởi mở và thiện chí tới từ tất cả các bên. Chính vì vậy, mỗi nội dung hợp tác thuộc chủ quyền của quốc gia luôn phải được đặt trong mối quan hệ với chủ quyền của quốc gia khác để việc triệt phá và loại bỏ loại hình tội phạm này có thể đạt được hiệu quả tối ưu nhất.

Một nguyên tắc xuất hiện từ thời kỳ cổ đại và có lịch sử phát triển lâu đời nhất trong số các nguyên tắc cơ bản của luật quốc tế đó chính là nguyên tắc Pacta sunt Servanda. Dưới góc độ của khoa học pháp lý quốc tế, bản chất của quá trình hợp tác

quốc tế chính là sự thỏa thuận vì vậy toàn bộ quá trình các quốc gia từ khi xây dựng các khuôn khổ hợp tác tới khi tiến hành thực thi các cơ chế để bảo đảm thực hiện hoàn toàn dựa trên sự tự nguyện của các chủ thể mà không dựa trên các cơ chế cưỡng chế áp đặt giống như luật quốc gia. Chính vì vậy, sự tồn tại của nguyên tắc này là cơ sở để ràng buộc quốc gia vào nghĩa vụ pháp lý phải thực hiện những cam kết quốc tế của mình một cách tận tâm, thiện chí và có ý nghĩa đặc biệt quan trọng cho việc duy trì trật tự pháp lý quốc tế cũng như đảm bảo quyền, lợi ích cho mỗi chủ thể khi tham gia hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao.

Đặc biệt, nguyên tắc quốc gia có nghĩa vụ hợp tác cũng là một nguyên tắc có ý nghĩa tối quan trọng trong điều chỉnh quan hệ hợp tác giữa các chủ thể trong phòng chống tội phạm công nghệ cao. Với hai sứ mạng chính là duy trì hòa bình, an ninh quốc tế và thực hiện sự hợp tác quốc tế trên mọi lĩnh vực thì vấn đề hợp tác quốc tế giữa các quốc gia chỉ thực sự được quan tâm và được pháp điển hóa trong các quy định của Hiến chương Liên hợp quốc tại Điều 4 khoản 3. Ngày nay, sự hợp tác này luôn luôn phải được tiến hành trên cơ sở bình đẳng về chủ quyền giữa các quốc gia và trải rộng trên hầu khắp mọi lĩnh vực của đời sống quốc tế trong đó có liên quan trực tiếp đến quá trình đấu tranh phòng chống tội phạm công nghệ cao. Mặc dù nhiều quan điểm cho rằng, nguyên tắc này nên được tiếp cận một cách mở rộng khi coi hợp tác quốc tế vừa là quyền nhưng đồng thời cũng là nghĩa vụ đối với các quốc gia hữu quan. Tuy vậy, cách tiếp cận được chấp nhận rộng rãi hiện nay lại nghiêng nhiều về mặt nghĩa vụ khi mà nhân loại đang ngày càng phải đối mặt với các các vấn đề an ninh phi truyền thống phức tạp mang tính toàn cầu ví dụ như những vấn đề về biến đổi khí hậu, môi trường, tội phạm công nghệ cao, chạy đua vũ trang, khủng hoảng kinh tế, vũ khí hạt nhân, xung đột tôn giáo-sắc tộc hay các dịch bệnh lây lan toàn thế giới... Bên cạnh đó, cho dù có nghiêng về mặt nghĩa vụ nhiều hơn nhưng luật quốc tế không hề quy định nghĩa vụ bắt buộc về các hình thức và cấp độ hợp tác dành cho các quốc gia khi tham gia. Hình thức và mức độ hợp tác này hoàn toàn phụ thuộc vào chính quyết định của các quốc gia xuất phát từ chủ quyền của mình cũng như căn cứ từ tình hình thực tế và năng lực tham gia của mỗi quốc gia. Điều này đặc biệt phù hợp đối với hoạt động hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao, khi mà trình độ phát triển và năng lực ứng phó trong lĩnh vực khoa học kỹ thuật của các quốc gia khác nhau sẽ không hoàn toàn giống nhau. Như vậy có thể nhận thấy, nguyên tắc một mặt đặt ra nghĩa vụ hợp tác cho các quốc gia nhưng đồng thời cũng mở rộng sự thừa nhận hợp tác vừa là quyền của mỗi chủ

thể xuất phát từ khả năng, ý chí và điều kiện cụ thể của mình. Bởi lẽ, xét cho cùng, đứng trước một loại hình tội phạm mới có nhiều đặc tính nguy hiểm thì đây vừa là hợp tác vì sự phát triển, vì lợi ích chung của cả cộng đồng quốc tế nhưng đồng thời nó cũng chính là sự đảm bảo đối với lợi ích và sự phát triển của chính bản thân mỗi quốc gia.

2.2.3.2. Các nguyên tắc đặc thù

Bên cạnh những nguyên tắc chung của luật quốc tế, pháp luật quốc tế trong phòng chống tội phạm công nghệ cao còn được điều chỉnh bởi một số nguyên tắc riêng biệt sau:

***Thứ nhất*,** nguyên tắc có đi có lại

Nguyên tắc có đi có lại thực chất xuất phát từ nguyên tắc bình đẳng về chủ quyền giữa các quốc gia. Theo đó, trên cơ sở bình đẳng về chủ quyền, quốc gia có quyền "ứng xử" với quốc gia khác tương tự như cách thức mà quốc gia đó đã, đang hoặc sẽ "ứng xử" với mình.

Trong luật hình sự quốc tế, các hoạt động hợp tác đấu tranh phòng chống tội phạm được thực hiện trên những cơ sở, *một là* điều ước quốc tế, *hai là* tập quán quốc tế và *ba là* pháp luậtquốc gia. Trong trường hợp có điều ước quốc tế, những vấn đề pháp lý liên quan đến các hoạt động hợp tác cụ thể sẽ được điều chỉnh bằng chính những quy định của điều ước quốc tế đó, ví dụ những vấn đề pháp lý về dẫn độ như các trường hợp dẫn độ, các trường hợp bắt buộc từ chối dẫn độ, các trường hợp cân nhắc để từ chối dẫn độ hay tài liệu cần thiết, chi phí, giải quyết yêu cầu dẫn độ khi có nhiều quốc gia cùng đưa ra yêu cầu… sẽ được ghi nhận cụ thể trong các điều ước về dẫn độ như hiệp định dẫn độ song phương, đa phương, hiệp định tương trợ tư pháp hình sự có phạm vi điều chỉnh cả vấn đề dẫn độ. Khi không có điều ước quốc tế, các hoạt động hợp tác sẽ được thực hiện trên cơ sở tập quán quốc tế hoặc pháp luật quốc gia. Trong trường hợp này, nguyên tắc có đi có lại sẽ trở thành cơ sở vô cùng quan trọng để các quốc gia cân nhắc việc có hay không tiến hành các hoạt động hợp tác theo yêu cầu của quốc gia hữu quan, đặc biệt đối với các yêu cầu về dẫn độ tội phạm và tương trợ tư pháp hình sự. Tập quán quốc tế là hệ thống các quy tắc xử sự được hình thành trong thực tiễn quan hệ quốc tế. Những quy tắc xử sự này đã thể hiện thế mạnh về sự tồn tại lâu đời của nó, có giá trị đối với mọi chủ thể của luật quốc tế. Nguyên tắc có đi có lại là một trong những quy phạm tập quán điều chỉnh về vấn đề dẫn độ tội phạm. Dù đã được pháp điển hóa hay chưa được pháp điển hóa trong các điều ước quốc tế thì nó cũng không làm mất đi giá trị điều chỉnh của tập quán quốc tế trong hoạt động đấu tranh phòng chống tội phạm nói chung và

tội phạm công nghệ cao nói riêng. Ngoài ra, quốc gia được yêu cầu sẽ tiến hành dẫn độ hay tương trợ tư pháp hình sự nếu quốc gia yêu cầu đã từng dẫn độ cho quốc gia được yêu cầu hoặc có căn cứ cho rằng, trong tương lai, quốc gia này sẽ dẫn độ cho quốc gia được yêu cầu.

Trong thực tiễn, dựa trên nguyên tắc này, các quốc gia thường xử sự theo một trong hai cách thức sau khi nhận được yêu cầu hợp tác của các quốc gia khác. Hoặc là quốc gia nhận được yêu cầu tự nguyện hạn chế chủ quyền của mình và thực hiện các hoạt động dẫn độ tội phạm hoặc tương trợ tư pháp hình sự cho quốc gia yêu cầu, nếu như không có các hoàn cảnh đặc biệt loại bỏ các hoạt động này; hoặc là, trên cơ sở chủ quyền quốc gia, quốc gia được yêu cầu từ chối yêu cầu của quốc gia yêu cầu. Việc quốc gia xử sự theo cách thức nào sẽ phụ thuộc vào rất nhiều yếu tố, trong đó một trong những yếu tố quyết định là mối quan hệ giữa quốc gia yêu cầu và quốc gia được yêu cầu.

Nguyên tắc có đi có lại có vai trò vô cùng quan trọng trong hoạt động hợp tác giữa các quốc gia. Không phải trong mọi trường hợp, giữa bên yêu cầu và bên được yêu cầu đều có điều ước quốc tế về hợp tác phòng chống tội phạm. Chẳng hạn, trong lĩnh vực dẫn độ tội phạm, đến nay, chưa có một điều ước quốc tế nào ở phạm vi toàn cầu điều chỉnh riêng biệt về vấn đề dẫn độ; nhiều điều ước quốc tế toàn cầu trong lĩnh vực phòng chống tội phạm mặc dù có điều khoản ghi nhận các quốc gia thành viên có thể viện dẫn chính những điều ước đó làm cơ sở pháp lý để dẫn độ nếu giữa các bên chưa có hiệp định nhưng trên thực tế, không ít các quốc gia, bao gồm cả Việt Nam có xu hướng tuyên bố bảo lưu, loại trừ việc áp dụng điều khoản này. Ở phạm vi khu vực, cũng mới chỉ có một số điều ước quốc tế về dẫn độ được hình thành giữa các quốc gia. Thực tiễn quan hệ quốc tế cho thấy, không phải mọi trường hợp, giữa quốc gia yêu cầu và quốc gia được yêu cầu đều có hiệp định dẫn độ. Trong tình huống này, nguyên tắc có đi có lại chính là cơ sở để quốc gia được yêu cầu xem xét để dẫn độ cho quốc gia yêu cầu, trừ khi việc dẫn độ thuộc các trường hợp không được phép dẫn độ theo quy định của pháp luật quốc gia được yêu cầu. Nói cách khác, nếu chỉ dựa trên điều ước quốc tế, hoạt động hợp tác giữa các quốc gia sẽ trở nên bị hạn chế do bị giới hạn bởi số lượng điều ước nhất định giữa các bên; ngược lại, nguyên tắc có đi có lại sẽ tạo điều kiện cho các quốc gia tiến hành những hoạt động hợp tác khác mặc dù không có điều ước điều chỉnh nhưng vẫn đảm bảo được sự bình đẳng giữa các bên.

Thứ hai, nguyên tắc hợp tác với phạm vi rộng nhất có thể

Nguyên tắc hợp tác với phạm vi rộng nhất có thể được ghi nhận trong Công ước Bundapest với nội dung: Các quốc gia thành viên phải hợp tác với nhau, phù hợp với các quy định trong chương này, và thông qua việc áp dụng các văn bản quốc tế về hợp tác quốc tế trong lĩnh vực hình sự, và luật của quốc gia mình, với phạm vi rộng nhất có thể để phục vụ việc điều tra, tiến hành các hoạt động tố tụng liên quan đến các tội phạm hình sự có liên quan đến hệ thống máy tính và dữ liệu máy tính, hoặc để thu thập chứng cứ dưới hình thức điện tử (Điều 23).

Theo nguyên tắc này, các quốc gia, sẽ tiến hành các hoạt động hợp tác với phạm vi rộng nhất có thể trong quá trình điều tra, thu thập chứng cứ hoặc các hoạt động tố tụng khác trên cơ sở phù hợp với các điều ước quốc tế liên quan và pháp luật quốc gia. Cụm từ "phạm vi rộng nhất có thể" được hiểu theo hai nghĩa. *Một là*, hợp tác trong phạm vi rộng nhất có thể trong khuôn khổ những nội dung hợp tác đã được thiết lập và *hai là*, hợp tác vượt ra ngoài những nội dung đã được ghi nhận nhưng trong phạm vi mà các bên có thể tiến hành, trên cơ sở phù hợp với các điều ước quốc tế và pháp luật quốc gia. Ở trường hợp thứ hai, giới hạn của hoạt động hợp tác không bị bó hẹp trong khuôn khổ các nội dung đã ghi nhận, miễn sao hoạt động đó, không trái với các khuôn khổ pháp lý đã được thiết lập.

Trong hoạt động hợp tác quốc tế về phòng chống tội phạm nói chung và tội phạm công nghệ cao nói riêng, nhu cầu hợp tác trong các lĩnh vực, nội dung cụ thể nào sẽ phụ thuộc vào thực tế của từng vụ việc. Do đó, bản thân các điều ước quốc tế cũng như pháp luật quốc gia không thể liệt kê được hết các nội dung hợp tác quốc tế mà chỉ dừng lại ở việc ghi nhận những nội dung hợp tác phổ biến, cơ bản. Đặc biệt, đối với tội phạm công nghệ cao, sự phát triển từng ngày của khoa học công nghệ khiến cho các thủ đoạn, phương thức phạm tội ngày càng tinh vi, tinh xảo. Vì vậy, nhu cầu hợp tác giữa các quốc gia để cập nhật, chia sẻ và ứng phó đối với loại tội phạm này có thể vượt ngoài những nội dung đang được ghi nhận trong điều ước quốc tế hoặc pháp luật quốc gia. Trong trường hợp này, nếu chỉ căn cứ vào nội dung hợp tác hiện có, hoạt động hợp tác sẽ có thể không đủ hiệu quả để phát hiện, ngăn chặn hoặc xử lý hành vi phạm tội. Ngược lại, nếu một quốc gia, cần sự hỗ trợ từ phía quốc gia khác trong việc thực hiện những hoạt động mà điều ước giữa các bên cũng như pháp luật quốc gia của bên được yêu cầu cũng chưa ghi nhận, thì đề nghị hỗ trợ đó có thể được thực hiện hay không? Nói cách khác, quốc gia được yêu cầu có thể từ chối chỉ vì lý do, nội dung yêu cầu hợp tác chưa được luật hoá trong pháp luật quốc gia và điều ước quốc tế không?

Đó chính là lý do vì sao nguyên tắc hợp tác với phạm vi rộng nhất có thể sẽ có ý nghĩa cực kỳ quan trọng trong trường hợp này. Bởi lẽ, theo nguyên tắc, các bên có thể tiến hành hợp tác trong những hoạt động mà chưa được ghi nhận trong các điều ước liên quan hay pháp luật quốc gia, miễn sao, các hoạt động đó phù hợp với các khuôn khổ pháp lý quốc tế và quốc gia là được. Nói cách khác, trong trường hợp này, điều ước quốc tế hay pháp luật quốc gia không phải là căn cứ duy nhất ghi nhận những nội dung cụ thể nào sẽ tiến hành giữa các bên mà chỉ là ghi nhận những nguyên tắc căn bản điều chỉnh quan hệ giữa các bên trong phòng chống tội phạm để đảm bảo những hoạt động được tiến hành không xâm phạm đến chủ quyền, lợi ích, an ninh của các bên. Thông qua nguyên tắc hợp tác với phạm vi rộng nhất, hoạt động hợp tác quốc tế sẽ được tiến hành một cách thực sự hiệu quả, tránh mang tính hình thức và phù hợp với yêu cầu thực tế của việc đấu tranh, phòng chống tội phạm công nghệ cao.

2.2.4. Nội dung của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao được thực hiện trên cơ sở các điều ước quốc tế, tập quán quốc tế hoặc theo các nguyên tắc của pháp luật quốc tế và quy định khác của pháp luật quốc gia. Phạm vi nội dung hợp tác trong đấu tranh phòng chống tội phạm công nghệ cao bao gồm: tương trợ tư pháp hình sự, dẫn độ tội phạm, chuyển giao người bị kết án, hay phân định thẩm quyền tài phán và các hình thức hợp tác khác. Các hoạt động cụ thể hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao gồm: tiếp nhận, thu giữ, bảo vệ hay chuyển giao tài liệu, dữ liệu liên quan đến tội phạm công nghệ cao; xử lý trường hợp từ chối dẫn độ công dân; trình tự, thủ tục xem xét, xử lý yêu cầu truy cứu trách nhiệm hình sự đối với công dân bị từ chối dẫn độ; trình tự, thủ tục xem xét, yêu cầu thi hành bản án, quyết định hình sự của tòa án nước ngoài đối với công dân bị từ chối dẫn độ; các biện pháp ngăn chặn, bắt tạm giam người bị yêu cầu dẫn độ; phối hợp điều tra tội phạm công nghệ cao... Thực tiễn cho thấy, trong quá trình giải quyết vụ án liên quan đến tội phạm công nghệ cao, do những đặc điểm riêng biệt, đặc thù hơn so với những loại tội phạm thông thường nên quá trình điều tra, thu thập, xác minh chứng cứ, tống đạt giấy tờ, tài liệu tố tụng, truy tìm, bắt giữ người phạm tội mà phải yêu cầu sự hợp tác, tương trợ của các quốc gia khác. Những hoạt động đó được gọi là tương trợ tư pháp về hình sự giữa các quốc gia. Hoạt động này là một yêu cầu, đòi hỏi khách quan, là một xu hướng vận động tất yếu, không thể thiếu được của quá trình hợp tác đấu tranh phòng chống tội phạm

công nghệ cao, nhất là trong bối cảnh toàn cầu hóa và sự bùng nổ của khoa học công nghệ.

Như vậy, nội dung của pháp luật quốc tế trong hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao rất đa dạng như: tương trợ tư pháp hình sự, dẫn độ tội phạm, chuyển giao người bị kết án, phân định thẩm quyền tài phán và hài hòa hóa pháp luật cũng như xây dựng và hoàn thiện cơ sở pháp lý quốc gia.

Một là, pháp luật quốc tế đặt ra và xác định rõ nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luật cũng như xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao:

Hài hoà hoá pháp luật hình sự giữa các quốc gia về tội phạm công nghệ cao là một trong những nghĩa vụ then chốt mà các điều ước quốc tế về đấu tranh, phòng chống tội phạm công nghệ cao đặt ra đối với các quốc gia thành viên, trong đó có Công ước Palermo năm 2000 và Công ước Budapest năm 2001. 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"*.[27] Tương tự như định nghĩa của từ điển Cambridge, hài hoà hoá pháp luật có thể hiểu là quá trình làm giảm bớt sự khác 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. Các nội dung về hài hoà hoá pháp luật hiện nay trong các điều ước quốc tế phổ biến bao gồm hai phương diện, hài hoà hoá hình phạt và hài hoà hoá trong quy định hành vi là tội phạm trong pháp luật hình sự của các quốc gia

Bên cạnh nghĩa vụ hài hòa hóa pháp luật hình sự giữa các quốc gia thành viên, xây dựng cơ sở pháp lý quốc gia cho các hoạt động ứng phó với tội phạm công nghệ cao cũng là một nghĩa vụ mang tính truyền thống trên cơ sở của nguyên tắc Pacta sunt Servanda. Theo đó, một số điều ước quốc tế và văn kiện pháp lý được thông qua trong khuôn khổ của các tổ chức quốc tế khu vực đã ghi nhận cho các QGTV nghĩa vụ chuyển hoá các quy định của điều ước quốc tế vào pháp luật quốc gia để làm cơ sở cho việc tiến hành những hoạt động ứng phó với tội phạm công nghệ cao.

---

[27] Xem https://dictionary.cambridge.org/vi/dictionary/english/harmonize, (truy cập lần cuối ngày 1/2/2020).

Hai là, tương trợ tư pháp hình sự. Xuất phát từ chủ quyền quốc gia, cơ quan tố tụng của quốc gia nào chỉ được thực hiện hoạt động tố tụng trên lãnh thổ của quốc gia đó. Tuy nhiên, trong nhiều trường hợp, việc giải quyết các vụ việc lại vượt ngoài phạm vi biên giới quốc gia. Trong tình huống này, quốc gia sẽ cần đến sự hỗ trợ, hợp tác của cơ quan tố tụng của quốc gia khác để giúp quốc gia trong việc ứng phó với tội phạm như yêu cầu cơ quan tố tụng của quốc gia liên quan tiến hành những biện pháp nhằm kịp thời bảo vệ chứng cứ hoặc kịp thời thu thập thông tin, tạo điều kiện cho việc thực hiện những hoạt động khám xét, điều tra, thu giữ hoặc bảo vệ dữ liệu trước các hành vi phạm tội của tội phạm công nghệ cao.

Ba là, dẫn độ tội phạm. Để trốn tránh khỏi sự trừng phạt của pháp luật, một trong những thủ đoạn mà người phạm tội sử dụng khi có khả năng là chạy trốn khỏi quốc gia mà người đó đã có hành vi phạm tội nhằm không bị truy cứu trách nhiệm hình sự hoặc không phải tiếp tục chấp hành hình phạt tù mà trước đó đã bị toà án có thẩm quyền tuyên phạt. Thông qua việc chuyển giao người phạm tội đang trốn chạy trên lãnh thổ quốc gia cho quốc gia được yêu cầu, quốc gia này mới có thể tiến hành các hoạt động tố tụng để đảm bảo mọi hành vi phạm tội đều phải bị trừng phạt trước pháp luật.

Bốn là, chuyển giao người đã bị kết án ở nước ngoài cho quốc gia mà người đó là công dân để chấp hành hình phạt tù theo bản án mà toà án đã tuyên. Về nguyên tắc, các điều kiện nhất định để chuyển giao người bị kết án được quy định trong các điều ước quốc tế điều chỉnh riêng biệt về chuyển giao người bị kết án, bao gồm cả điều ước song phương và đa phương, trong đó, phổ biến nhất là các hiệp định song phương. Sau khi tiếp nhận phạm nhân, quốc gia thi hành án phải bảo đảm tiếp tục thi hành án phạt phù hợp với luật pháp nước mình, đồng thời dựa trên cơ sở bản án của tòa án nước tuyên án.

Năm là, phân định thẩm quyền tài phán hình sự trên cơ sở một số nguyên tắc là hoạt động để xác định quốc gia có thẩm quyền tài phán đối với tội phạm công nghệ cao trong trường hợp hành vi phạm tội có liên quan đến nhiều quốc gia. Hiện nay, một số nguyên tắc của Luật hình sự quốc tế trong xác định thẩm quyền tài phán hoàn toàn có thể áp dụng đối với tội phạm công nghệ cao như: nguyên tắc lãnh thổ, nguyên tắc quốc tịch,...

2.2.5. Vai trò của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Khi loài người bước vào thời kỳ phát triển của khoa học và công nghệ, xã hội hiện nay ngày càng phụ thuộc nhiều hơn vào máy tính và các kết nối mạng. Hàng

loạt vụ hacker tấn công vào hệ thống thông tin của các Chính phủ, cơ quan nhà nước, hệ thống dữ liệu của doanh nghiệp, ngân hàng, hàng không... đã gây nên những xáo trộn không nhỏ và tạo ra mối quan ngại lớn trên phạm vi toàn cầu. Tuy nhiên, thách thức sẽ còn lớn hơn nữa khi tội phạm công nghệ cao sẽ ngày càng gia tăng cùng với tốc độ phát triển của khoa học - kỹ thuật, ảnh hưởng lớn đến sự tăng trưởng của nền kinh tế. Theo báo cáo của Tổ chức Cảnh sát Hình sự quốc tế, tội phạm công nghệ cao đứng thứ 2 trong các loại tội phạm nguy hiểm nhất, sau tội phạm khủng bố. Và tình hình càng trở nên nghiêm trọng khi bắt đầu xuất hiện sự chuyển hướng mục tiêu đáng kể từ các cá nhân và doanh nghiệp nhỏ sang các tập đoàn lớn, chính phủ và cơ sở hạ tầng quan trọng của khối các cơ quan nhà nước. Thực tiễn cho thấy, càng trong lúc dịch bệnh Covid-19 hoành hành, khoảng 90% các loại tội phạm truyền thống hiện nay đã chuyển sang môi trường mạng hoặc có sử dụng các thiết bị công nghệ cao để hỗ trợ trong quá trình tiến hành hành vi phạm tội[28]. Thế giới đang chứng kiến sự thay đổi to lớn của quá trình chuyển đổi kỹ thuật số trong thời kỳ dịch bệnh Covid-19. Sự xuất hiện của đại dịch Covid-19 làm thay đổi cách thức sinh sống, làm việc của người dân gần như trên toàn thế giới. Các cá nhân, tổ chức phải thích nghi với cách thức làm việc mới: làm việc từ xa, làm việc tại nhà, làm việc trực tuyến trên môi trường mạng (work from home)[29]. Các mối đe dọa về an ninh mạng, tấn công mạng vì thế cũng trở nên gia tăng cả về số lượng cũng như phạm vi, mức độ ảnh hưởng[30]. Trên thực tế, công nghệ số đã mở đường cho việc vận hành và phát triển nền kinh tế một cách bình thường bất chấp những thách thức của dịch Covid-19 đưa lại, tạo ra cơ sở nền tảng cho sự phục hồi của nền kinh tế của mỗi quốc gia cũng như trên toàn cầu. Tuy nhiên, sự phụ thuộc của chúng ta vào khoa học công nghệ cao cũng ngày càng gia tăng; chính vì vậy, việc đảm bảo tính an toàn bảo mật của hệ thống dữ liệu mạng và tăng cường hợp tác quốc tế cũng luôn cần được quan tâm. Do đặc thù của loại tội phạm này là hoạt động trên môi trường mạng, mọi cơ quan, tổ chức, cá nhân có kết nối với mạng internet đều có thể trở thành nạn nhân bất cứ lúc nào. Tội phạm chỉ cần trú ẩn ở một

---

[28] Xem: *https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19*(truy cập lần cuối ngày 6/3/2020).

[29] Lallie, Harjinder Singh, Shepherd, Lynsay A, Nurse, Jason R.C, Erola, Arnau, Epiphaniou, Gregory, Maple, Carsten, & Bellekens, Xavier. (2021). *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*. Computers & Security, 105, 102248.

[30] Bou Sleiman, Mohamed, & Gerdemann, Simon. (2021). *Covid-19: A catalyst for cybercrime?* International Cybersecurity Law Review, 2(1), 37-45.

quốc gia cùng với các thiết bị điện tử thông minh có kết nối mạng và thực hiện hành vi phạm tội tại một quốc gia khác. Chính vì vậy rất khó để phát hiện, đấu tranh, phòng chống và thống kê một cách chính xác, đầy đủ. Bên cạnh những thiệt hại trực tiếp về kinh tế đối với các nạn nhân như trộm cắp tiền trong thẻ hoặc tài khoản ngân hàng, mã hóa tài liệu, chiếm đoạt thông tin bí mật của các cơ quan nhà nước, chính phủ, khống chế, đe dọa dữ liệu của các cá nhân để tống tiền, chúng còn gây ra những thiệt hại gián tiếp như: làm mất uy tín, gián đoạn hoạt động thường xuyên của các cơ quan, tổ chức; hoạt động kinh doanh ổn định của các doanh nghiệp, đặc biệt trong một số trường hợp nghiêm trọng, chúng còn là mối nguy cơ lớn đe dọa đến trật tự an toàn trên mạng Internet của an ninh quốc gia. Không chỉ tội phạm công nghệ cao, các loại tội phạm thông thường cũng đang thể hiện xu hướng thích ứng với làn sóng của thời đại công nghệ. Có lẽ chưa khi nào các loại hình tội phạm lại sử dụng mạng Internet để thực hiện hành vi phạm tội nhiều như hiện nay khi mà thế giới đang bước vào thời đại của cuộc cách mạng công nghiệp 4.0[31].

Đứng trước sự tinh vi phức tạp và những hậu quả nghiêm trọng của tội phạm công nghệ cao, việc hợp tác để đấu tranh, phòng chống tội phạm công nghệ cao giữa các quốc gia ngày càng trở nên cấp thiết hơn bao giờ hết. Pháp luật quốc tế chính là cơ sở để các quốc gia tiến hành những hoạt động hợp tác này. Thông qua các nội dung hợp tác như hình thành các cơ quan, thiết chế quốc tế trong phòng chống tội phạm công nghệ cao; hài hoà hoá pháp luật; tương trợ tư pháp hình sự; dẫn độ; tiến hành phối hợp điều tra… pháp luật quốc tế đã hình thành nên một cơ chế pháp lý chung ở các cấp độ khác nhau, từ song phương, khu vực đến toàn cầu để kết nối hoạt động giữa các quốc gia, từ đó, ứng phó hiệu quả với tội phạm công nghệ cao, góp phần hạn chế, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế.

[31] Faga, Hemen Philip. (2017), *The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century*. Baltic Journal of Law & Politics, 10(1), 1-34

TIỂU KẾT CHƯƠNG 2

* * *

1. Xét về quá trình hình thành và phát triển, thuật ngữ "tội phạm công nghệ cao" không xuất hiện ngay từ những thời kì đầu. Nó ra đời và phát triển gắn liền với các giai đoạn bùng nổ của khoa học công nghệ thông tin. Mặc dù có nhiều tên gọi cũng như có nhiều cách tiếp cận khác nhau nhưng về cơ bản, tội phạm công nghệ cao là một dạng thức tội phạm được tiến hành thông qua việc sử dụng tri thức, kỹ năng, công cụ, phương tiện và thành tựu của công nghệ thông tin ở trình độ cao, tác động một cách bất hợp pháp đến thông tin số và các dữ liệu điện tử được lưu trữ, xử lý, truyền tải trong hệ thống máy tính và các thiết bị công nghệ cao, xâm phạm đến trật tự an toàn thông tin, gây tổn hại nghiêm trọng đến quyền và lợi ích hợp pháp của các cá nhân, tổ chức cũng như của các quốc gia và cộng đồng quốc tế. Tội phạm công nghệ cao chính là "sản phẩm" của thời đại mà các cá nhân, tổ chức, quốc gia và cộng đồng quốc tế phải chấp nhận để đổi lấy sự thịnh vượng và phát triển.

Với sự gia tăng nhanh chóng cả về số lượng, tính chất, mức độ và phạm vi thiệt hại, tội phạm công nghệ cao đã và đang một trong những thách thức đe dọa đến lợi ích của mỗi cá nhân, tổ chức, quốc gia và của cả cộng đồng quốc tế. Sẽ không thể đấu tranh, ngăn ngừa và loại bỏ loại hình tội phạm này nếu như thiếu đi sự chung tay của toàn thể cộng đồng quốc tế. Hay nói một cách khác, hợp tác quốc tế trong đấu tranh phòng, chống tội phạm nói chung và tội phạm công nghệ cao nói riêng là một nhu cầu cấp thiết mang tính quy luật tất yếu khách quan, đặc biệt trong bối cảnh toàn cầu hóa và bùng nổ phát triển khoa học công nghệ.

2. Pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao là hệ thống các nguyên tắc và các quy phạm pháp luật điều chỉnh quan hệ giữa các chủ thể luật quốc tế trong việc tiến hành toàn bộ những hoạt động cần thiết giữa các bên, nhằm ngăn ngừa, trừng trị, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế cũng như đời sống quốc gia. Pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao vừa bao gồm những nội dung chung của luật quốc tế, luật hình sự quốc tế vừa bao gồm những nội dung riêng biệt, cụ thể trong quá trình các chủ thể tiến hành hợp tác đấu tranh, phòng chống tội phạm công nghệ cao. Theo đó, nội dung của pháp quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao bao gồm các hoạt động như tương trợ tư pháp hình sự, dẫn độ tội phạm, chuyển giao người bị kết án, phân định thẩm quyền tài phán và hài hòa hóa pháp luật cũng như xây dựng và hoàn thiện cơ sở pháp lý quốc gia. Những nội

dung trên được điều chỉnh trước tiên và chủ yếu là các điều ước quốc tế đa phương, song phương đặc biệt phải kể đến Công ước Budapest – điều ước quốc tế toàn diện nhất hiện nay điều chỉnh liên quan đến loại tội phạm này. Bên cạnh đó là những điều ước quốc tế, thỏa thuận khu vực đi sâu vào một số dạng thức cụ thể như Thoả thuận của Cộng đồng các quốc gia độc lập về hợp tác trong phòng chống các tội phạm liên quan đến thông tin máy tính năm 2001, Công ước Arab về chống các tội phạm liên quan đến công nghệ thông tin năm 2010, Công ước của Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân năm 2014… Ngoài ra, quá trình hợp tác của các chủ thể còn được điều chỉnh bởi một số loại nguồn khác của luật quốc tế.

Hiện nay, các chủ thể đang trong quá trình tiến hành hoàn thiện và xây dựng pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao để phù hợp với nhu cầu đấu tranh, phòng chống tội phạm công nghệ cao trên thực tiễn và góp phần hạn chế, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế.

CHƯƠNG 3
NỘI DUNG PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH, PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO VÀ THỰC TIỄN THỰC HIỆN CỦA MỘT SỐ QUỐC GIA

* * *

Nhằm tạo ra các khuôn khổ chung trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao, một số văn kiện pháp lý đã được xây dựng ở các cấp độ khác nhau, từ toàn cầu, khu vực cho tới song phương điều chỉnh những vấn đề liên quan đến tội phạm công nghệ cao[32]. Căn cứ vào những văn kiện hiện có, nội dung của hợp tác quốc tế trong đấu tranh, phòng chống tội phạm công nghệ cao bao gồm:Thứ nhất, pháp luật quốc tế quy định nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luật cũng như xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao; Thứ hai, tương trợ tư pháp hình sự; Thứ ba, dẫn độ; Thứ tư, chuyển giao người bị kết án và thứ năm, phân định thẩm quyền tài phán.

3.1. Pháp luật quốc tế quy định nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luật và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao

3.1.1. Hài hoà hoá pháp luật của các quốc gia trong phòng chống tội phạm công nghệ cao

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 nội dung căn bản nhằm tạo ra sự tương đồng giữa hệ thống pháp luật của các nước, từ đó, góp phần 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 tránh việc tạo ra kẽ hở để người phạm tội có thể trốn tránh khỏi việc bị pháp luật trừng trị. 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. Chẳng hạn, theo quy định tại Thoả 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, các Bên sẽ cố gắng đảm bảo hài hòa hóa luật pháp quốc gia của mình liên quan đến việc chống lại các hành vi phạm tội liên quan đến

[32] Mohamed Chawki (2005), A Critical Look at the Regulation of Cybercrime, University of Lyon III, France

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, 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). Điều này xuất phát từ thực tế là cùng một hành vi nhưng có quốc gia quy định là tội phạm trong luật hình sự nhưng có quốc gia lại không hoặc cùng được quy định là tội phạm nhưng hình phạt tối thiểu tại các quốc gia lại rất khác nhau. Sự khác biệt như vậy hoặc sẽ tạo thành kẽ hở cho người phạm tội trốn tránh khỏi việc bị dẫn độ theo nguyên tắc "định danh kép" khi trốn sang quốc gia chưa quy định hành vi này là tội phạm hoặc không đạt được mục đích trừng phạt thích đáng khi mà ở một số quốc gia, hình phạt được quy định nhẹ hơn nhiều so với các quốc gia khác. Do đó, hài hoà hoá pháp luật có thể ngăn chặn việc người phạm tội lợi dụng sự khác biệt trong quy định pháp luật giữa các quốc gia để trốn tránh khỏi sự trừng phạt của pháp luật, đồng thời, tạo điều kiện tăng cường hoạt động hợp tác quốc tế giữa các quốc gia trong ngăn ngừa, trừng phạt tội phạm công nghệ cao, đặc biệt liên quan đến các yêu cầu về dẫn độ, tương trợ tư pháp hình sự.[33]

Để hạn chế những điều này, các văn kiện pháp lý của luật hình sự quốc tế 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 trừng phạt bằng hình luật 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 phạm tội nhất định nhằm tạo một ngưỡng chung trong xử lý hình sự những hành vi tội phạm tại tất cả các thành viên, một ví dụ điển hình ở mức độ này là Liên minh châu Âu.

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

Khuôn mẫu chung của các văn kiện pháp lý quốc tế về tội phạm công nghệ cao là ghi nhận nghĩa vụ đối với các quốc gia quy định trong luật hình sự nước mình những hành vi vi phạm cố ý nhất định liên quan đến công nghệ cao là tội phạm.

Chẳng hạn, theo quy định tại 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

[33] Council of Europe (2001), *Explanatory Reportto the Convention on Cybercrime*, para 33. *https://rm.coe.int/16800cce5b,* (truy cập lần cuối ngày 1/12/2020).

theo luật nước mình đối với những hành vi được thực hiện một cách cố ý, bao gồm: *Một là,* nhóm hành vi chống lại sự bí mật, toàn vẹn và sẵn có của dữ liệu máy tính và hệ thống máy tính 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; *Hai là,* 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; *Ba là,* những hành vi liên quan đến các tài liệu khiêu dâm trẻ em; *Bốn là*, các hành vi xâm phạm quyền tác giả và quyền liên quan và *năm là,* hành vi nỗ lực và hỗ trợ cho việc thực hiện những hành vi trên.[34] 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 trên, dẫn đến việc thực hiện những hành 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).

Hoặc theo quy định tại Công ước Arab về chống tội phạm công nghệ thông tin, *"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.[35] 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).

Tương tự như hai Công ước trên về nghĩa vụ hình sự hoá hành vi phạm tội liên quan đến công nghệ cao, nhưng cách quy định của 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*

[34] Nội dung cụ thể của những hành vi này xem Công ước Budapest, các điều từ Điều 3→Điều 10.
[35] Nội dung cụ thể của những hành vi này, xem thêm Công ước Arab về chống tội phạm công nghệ thông tin từ Điều 6→Điều 19.

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).

Ngoài các 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 bổ trường châu Âu thông qua hay Chỉ thị của Cộng đồng kinh tế của các quốc gia Tây Phi do Nghị viện thông qua cũng ghi nhận nghĩa vụ của các QGTV 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 doạ 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.[36]

Có thể thấy, mặc dù đều có điểm chung trong việc ghi nhận nghĩa vụ của các QGTV phải hình sự hoá những hành vi phạm tội liên quan đến công nghệ cao nhưng việc xác định những hành vi nào sẽ bị coi là tội phạm ở các văn kiện không giống nhau, ngoài một số những 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. Việc quy định theo hướng liệt kê sẽ dẫn đến việc điều chỉnh không đầy đủ khi luật không phản ánh được kịp thời so với sự phát triển của những hành vi phạm tội trên thực tế. Nói cách khác, nếu một hành vi không thuộc những trường hợp được liệt kê trong các điều ước quốc tế về

[36] Nội dung cụ thể của những hành vi này, xem thêm 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→Điều 23 .

tội phạm công nghệ cao, sẽ có quốc gia quy định đó là tội phạm và quốc gia không. Trong trường hợp cần thiết tiến hành những hoạt động tương trợ tư pháp hình sự hay dẫn độ đối với những hành vi này đòi hỏi phải dựa trên nguyên tắc định danh kép cũng như mục đích của hoạt động trừng trị.

3.1.1.2. Hài hoà hoá hình phạt

Hình sự hoá hành vi phạm tội mới dừng lại ở việc yêu cầu đối với các QGTV 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 và tiêu chuẩn cụ thể liên quan đến hình phạt sẽ áp dụng đối với tội phạm này. Điều này có thể dẫn đến một 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 1 ngày cho đến 12 năm (Điều 5)[37], 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[38] trong khi theo quy định tại Luật tội phạm máy tính năm 2007 của Thái Lan, hình phạt chỉ không quá 6 tháng tù (Điều 5)...[39] 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 hoàn toàn có thể được khắc phục thông qua hài hoà hoá hình phạt. Vấn đề hài 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 với từng hành vi và pháp luật hình sự của các quốc gia phải quy định hình phạt không được thấp hơn ngưỡng hình phạt tối thiểu này.

---

[37] Republic Act No. 10175 *https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/*, (truy cập lần cuối ngày 1/12/2020)

[38] COMPUTER MISUSE ACT *https://www.unodc.org/res/cld/document/computer-misuse-act_html/Brunei_Computer_Misuse.pdf*(truy cập lần cuối ngày 1/12/2020)

[39]Computer Crime Act B.E 2550 (2007) *https://www.samuiforsale.com/law-texts/computer-crime-act.html*(truy cập lần cuối ngày 1/12/2020)

Cấp độ hài hoà hoá hình phạt phổ biến hiện nay là ghi nhận các nguyên tắc chung trong việc xác định hình phạt, còn việc quy định cụ thể sẽ do mỗi quốc gia tự xác định. Theo đó, những nguyên tắc được quy định phổ biến để xác định hình phạt bao gồm: Tương xứng, hiệu quả, có tính răn đe. Nguyên tắc này được ghi nhận tại hầu hết các văn kiện như ở 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 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 không hoàn toàn giống nhau. Điều này bắt nguồn từ đặc điểm nội tại của mỗi quốc gia về thể chế kinh tế, chính trị, xã hội, văn hoá, hệ tư tưởng cũng như đặc điểm lịch sử trong từng giai đoạn phát triển 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, sự thiện chí và mong muốn làm sâu thêm mức độ hợp tác giữa các bên. Hai yếu tố này có mối liên hệ chặt chẽ với nhau. Nếu không có sự tương đồng giữa các thành viên thì 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 thiện chí và bày tỏ mong muốn nâng cao hợp tác thì điều này cũng không thể đạt được.

Điển hình tiêu biểu cho việc đáp ứng được những yếu tố này là Liên minh châu Âu. 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 hay sự khác biệt đáng kể giữa hệ thống pháp luật của các QGTV. 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 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, Chỉ thị 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

Chẳng hạn, theo quy định tại Chỉ thị 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, hình phạt tối thiểu mà các QGTV phải quy định trong pháp luật hình sự của mình đối với những hành vi như sau:

+ 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 phối 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);[40]

+ 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 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);

+ 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).

Hoặc theo quy định tại Chỉ thị 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, 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).

[40] Định nghĩa về những hành vi phạm tội này xem thêm Chỉ thị 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.

3.1.2. Xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động ứng phó với tội phạm công nghệ cao

Theo quy định của luật quốc tế, quốc gia có nghĩa vụ tôn trọng và thực hiện đầy đủ các cam kết quốc tế của quốc gia. Tuy nhiên, nguyên tắc Pacta sunt Servanda chỉ đặt ra nghĩa vụ cho quốc gia phải thực hiện những cam kết quốc tế của mình một cách tận tâm và thiện chí còn việc thực hiện như thế nào và theo cách thức nào, thường do quốc gia tự quyết định trên cơ sở chủ quyền của mình phù hợp với các quy định của pháp luật quốc gia. Nói cách khác, luật quốc tế thường không quy định cụ thể về cách thức thực hiện cam kết quốc tế của quốc gia. Do vậy, quốc gia, trên cơ sở chủ quyền, sẽ quyết định về việc thực hiện cam kết quốc tế theo một trong hai cách thức, hoặc áp dụng trực tiếp các quy định của cam kết quốc tế trên phạm vi lãnh thổ quốc gia hoặc chuyển hoá (nội luật hóa) những quy định của các cam kết quốc tế vào pháp luật quốc gia thông qua việc ban hành các văn bản quy phạm pháp luật mới hay sửa đổi, bổ sung những văn bản hiện hành để đảm bảo sự tương thích với các cam kết quốc tế đó. Tuy nhiên, cũng có một vài ngoài lệ, đó là trường hợp một số điều ước quốc tế trực tiếp quy định nghĩa vụ của quốc gia phải ban hành pháp luật để thực hiện các quy định của điều ước, điển hình như trong lĩnh vực quyền con người, rất nhiều Công ước đã ghi nhận điều khoản với nội dung "*Các quốc gia thành viên phải thực hiện các biện pháp lập pháp nhằm đảm bảo các quyền được ghi nhận trong Công ước*" như Công ước về quyền dân sự chính trị (Điều 2), Công ước về quyền kinh tế, xã hội, văn hoá (Điều 2), Công ước chống tra tấn và các hình thức trừng phạt hay đối xử tàn bạo, vô nhân đạo hoặc hạ thấp nhân phẩm (Điều 2), Công ước về quyền trẻ em (Điều 4)… Trong những trường hợp này, ban hành pháp luật để chuyển hoá quy định của điều ước không phải là cách thức mà quốc gia có thể lựa chọn để thực hiện điều ước mà nó sẽ trở thành nghĩa vụ ràng buộc về mặt pháp lý đối với quốc gia.

Trong luật hình sự quốc tế, nghĩa vụ ban hành pháp luật quốc gia làm cơ sở cho việc tiến hành những hoạt động ứng phó với tội phạm công nghệ cao được ghi nhận trong một loạt các văn kiện, từ Công ước Budapest, Công ước Arab về chống tội phạm công nghệ thông tin, Công ước của Liên minh châu Phi về an ninh mạng và bảo vệ dữ liệu cá nhân cho đến các quy định trong các Chỉ thị của Liên minh châu Âu...

Theo quy định tại những văn bản này, quốc gia thành viên phải ban hành pháp luật để trao quyền cho các cơ quan có thẩm quyền thực hiện những hoạt động nhằm tạo điều kiện cho quá trình điều tra, xử lý hành vi vi phạm, bảo vệ các dữ liệu bị

xâm hại do hành vi tội phạm công nghệ cao như bảo quản dữ liệu máy tính đã được lưu trữ; giám sát khẩn cấp; khám xét và thu giữ dữ liệu máy tính; yêu cầu xuất trình thông tin; chặn dữ liệu nội dung… Chẳng hạn, theo quy định tại các điều từ Điều 16 đến Điều 21 của Công ước Budapest:

+ Các quốc gia thành viên của Công ước phải ban hành luật và các biện pháp cần thiết khác để tạo khả năng cho các cơ quan chức năng ra lệnh hoặc thực hiện các biện pháp tương tự để bảo quản khẩn cấp các dữ liệu máy tính nhất định, bao gồm cả dữ liệu lưu thông, đã được lưu trữ bởi hệ thống máy tính, nhất là khi có căn cứ để cho rằng dữ liệu máy tính này đặc biệt dễ bị mất hoặc thay đổi; QGTV phải ban hành luật hoặc các biện pháp cần thiết khác buộc người giữ gìn dữ liệu máy tính đảm bảo sự bí mật về hành vi tố tụng đó trong một thời hạn được luật của quốc gia mình quy định (Điều 16);

+ QGTV phải ban hành luật hoặc thực hiện các biện pháp cần thiết khác để bảo đảm việc bảo quản khẩn cấp dữ liệu lưu thông là sẵn có; đảm bảo việc tiết lộ nhanh chóng một lượng dữ liệu lưu thông đủ để tạo khả năng cho quốc gia này nhận ra các nhà cung cấp dịch vụ và đường truyền liên lạc đó (Điều 17);

+ QGTV phải ban hành luật hoặc thực hiện các biện pháp cần thiết khác để trao thẩm quyền cho các cơ quan chức năng ra lệnh cho người trong lãnh thổ quốc gia đệ trình dữ liệu máy tính được yêu cầu thuộc sự chiếm hữu, quản lý của người đó hiện đang được lưu trữ trong hệ thống máy tính hoặc phương tiện lưu trữ dữ liệu máy tính hoặc nhà cung cấp dịch vụ đang cung cấp dịch vụ trong lãnh thổ quốc gia đệ trình thông tin về người đăng ký dịch vụ có liên quan đến dịch vụ đang thuộc sự chiếm hữu, quản lý của nhà cung cấp dịch vụ (Điều 18);

+ Quốc gia thành viên Công ước phải ban hành luật hoặc các biện pháp cần thiết khác để trao thẩm quyền cho cơ quan chức năng thực hiện việc khám xét hoặc các biện pháp tương tự đểtruy cập hệ thống máy tính hoặc một phần của hệ thống máy tính và các dữ liệu máy tính được lưu trữ ở trong đó và phương tiện lưu trữ dữ liệu máy tính trong đó dữ liệu máy tính có thể đã được lưu trữ thuộc lãnh thổ của quốc gia mình; Thu thập hoặc ghi lại dữ liệu lưu thông hoặc hợp tác và hỗ trợ cơ quan chức năng trong việc thu thập và ghi lại dữ liệu lưu thông, trong thời gian thực, có gắn với các liên lạc đang được điều tra trong lãnh thổ quốc gia mình được truyền qua hệ thống máy tính; Thu thập hoặc ghi lại việc áp dụng các biện pháp kỹ thuật trên lãnh thổ của quốc gia hoặc buộc nhà cung cấp dịch vụ, trong khả năng kỹ thuật của mình thu thập hoặc ghi lại hoặc hỗ trợ cơ quan chức năng thu thập hoặc ghi lại, dữ liệu nội dung, trong thời gian thực, của các liên lạc cụ thể trong lãnh thổ

quốc gia mình được truyền tải qua hệ thống máy tính việc áp dụng các biện pháp kỹ thuật trên lãnh thổ của quốc gia (Điều 19, Điều 20, Điều 21).

Đặc biệt trong các Chỉ thị của Liên minh châu Âu, QGTV còn được yêu cầu khắt khe hơn khi phải chuyển hoá quy định của Chị thị vào pháp luật quốc gia không được muộn hơn thời hạn được ghi nhận trong từng Chỉ thị liên quan. Chẳng hạn, đối với Chỉ thị 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, QGTV phải ban hành luật, quy định để đảm bảo tuân thủ những quy định của Chị thị trước ngày 4/9/2015. Uỷ ban châu Âu có thẩm quyền giám sát quá trình nội luật hoá này của QGTV. Việc không chuyển hoá quy định của Chỉ thị đúng thời hạn hoặc chuyển hoá không đầy đủ, không chính xác sẽ bị coi là hành vi vi phạm pháp luật của EU. Trong trường hợp này, Uỷ ban châu Âu và/hoặc Toà 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.[41]

3.2. Tương trợ tư pháp hình sự

3.2.1. Nội dung tương trợ tư pháp hình sự

Nguyên tắc tương trợ tư pháp được ghi nhận trong Công ước Budapest là QGTV phải đảm bảo việc cung cấp hoạt động tương trợ tư pháp rộng nhất có thể để phục vụ cho công tác điều tra hoặc tố tụng liên quan đến các tội phạm về máy tính hoặc dữ liệu máy tính hay thu thập các chứng cứ dưới hình thức điện tử về tội phạm. Nói cách khác, ngoài những nội dung được quy định trong các điều ước quốc tế hiện nay, các bên có thể tiến hành những hoạt động tương trợ tư pháp khác miễn là nhận được sự đồng ý của quốc gia hữu quan.

Tương tự như các loại tội phạm khác, nội dung tương trợ tư pháp hình sự đối với tội phạm công nghệ cao cũng bao gồm những hoạt động nhằm hỗ trợ cho các cơ quan tố tụng của các quốc gia trong quá trình tiến hành điều tra, khởi tố hành vi vi phạm. Theo đó, các hoạt động tương trợ tư pháp hình sự phổ biến bao gồm: (i) Trao đổi thông tin như thông tin liên quan đến hành vi phạm tội đang trong quá trình chuẩn bị hoặc đã được thực hiện; thể nhân, pháp nhân liên quan; cách thức, phương tiện phạm tội; cách thức phòng ngừa, phát hiện, điều tra hành vi phạm tội…; (ii) lập kế hoạch, thực hiện các hoạt động phối hợp để ngăn chặn, phát hiện và điều tra hành vi phạm tội; (iii) hỗ trợ đào tạo chuyên gia; (iv) xây dựng hệ thống thông tin

[41] Xem: Phạm Hồng Hạnh (2016), "*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, tr.75-85.

để hỗ trợ hoạt động ngăn chặn, điều tra hành vi phạm tội; (v) trao đổi quy định, tài liệu liên quan đến tội phạm công nghệ cao; (vi) thực hiện các yêu cầu điều tra và yêu cầu tố tụng và các nội dung cụ thể khác theo thoả thuận của các bên.

Ngoài những nội dung phổ biến như trên, một số điều ước quốc tế về tội phạm công nghệ cao như Công ước Budapest, Công ước Arab về chống tội phạm công nghệ thông tin… đã ghi nhận những nội dung tương trợ tư pháp hình sự riêng biệt liên quan đến loại tội phạm này, bao gồm:

(1) Tương trợ tư pháp liên quan đến các biện pháp tạm thời

Về bản chất, các biện pháp tạm thời trong tương trợ tư pháp là những biện pháp mang tính tình thế mà một quốc gia yêu cầu một quốc gia khác thực hiện với mục đích ứng phó với hoàn cảnh khẩn cấp của vụ việc đang giải quyết nhằm kịp thời thu thập chứng cứ, bảo vệ bằng chứng cho quá trình tiến hành các hoạt động tố tụng sau này.

Các biện pháp khẩn cấp tạm thời được ghi nhận trong một số điều ước quốc tế chủ yếu là những biện pháp liên quan đến bảo đảm dữ liệu máy tính nhằm kịp thời bảo vệ chứng cứ hoặc kịp thời thu thập thông tin để tạo điều kiện cho việc thực hiện những hoạt động khám xét, điều tra, thu giữ hoặc bảo vệ dữ liệu như bảo quản khẩn cấp dữ liệu máy tính được lưu trữ, tiết lộ nhanh chóng thông tin trong dữ liệu máy tính đã được bảo quản... Cụ thể, theo quy định tại Công ước Budapest, QGTV có thể yêu cầu quốc QGTV khác ra lệnh hoặc thực hiện những biện pháp cần thiết để bảo quản khẩn cấp các dữ liệu đang được lưu trữ bởi hệ thống máy tính đang nằm trên lãnh thổ quốc gia được yêu cầu (Điều 29). Quốc gia được yêu cầu chỉ có thể từ chối nếu: (i) yêu cầu liên quan đến tội phạm chính trị hoặc tội phạm liên quan đến tội phạm chính trị hoặc (ii) việc thực thi yêu cầu tương trợ có khả năng gây tổn hại tới chủ quyền, an ninh, trật tự công cộng hoặc các lợi ích thiết yếu khác. Đặc biệt, quốc gia được yêu cầu không được viện dẫn nguyên tắc định danh kép đề từ chối thực hiện yêu cầu của QGTV khác. Thời hạn để bảo quản dữ liệu tối thiểu là 60 ngày. Trong quá trình thực hiện yêu cầu bảo quản dữ liệu, nếu quốc gia được yêu cầu phát hiện thấy nhà cung cấp dịch vụ ở quốc gia khác có liên quan đến việc truyền tải liên lạc, quốc gia được yêu cầu sẽ nhanh chóng tiết lộ cho quốc gia yêu cầu lượng dữ liệu lưu thông đủ lớn để nhận diện nhà cung cấp dịch vụ đó và đường truyềnmà liên lạc được truyền tải trừ khi liên quan đến tội phạm chính trị, tội phạm liên quan đến tội phạm chính trị hoặc ảnh hưởng đến chủ quyền, an ninh, trật tự công cộng hoặc lợi ích thiết yếu khác của quốc gia được yêu cầu (Điều 30).

(2) Tương trợ tư pháp trong hoạt động điều tra

Trong quá trình tiến hành hoạt động điều tra, các quốc gia có thể yêu cầu quốc gia khác thực hiện một số hoạt động tương trợ tư pháp liên quan đến truy cập, thu thập dữ liệu hoặc chặn dữ liệu nội dung. Xuất phát từ đặc trưng của tội phạm công nghệ cao, các dữ liệu máy tính được coi là chứng cứ quan trọng nhất trong quá trình điều tra, xác định hành vi phạm tội, tuy nhiên, những dữ liệu này rất dễ bị nghi phạm huỷ bỏ hoặc thay đổi để che dấu hành vi phạm tội. Do đó, để kịp thời cho các cơ quan tố tụng của quốc gia trong quá trình điều tra, một số điều ước quốc tế đã ghi nhận những hoạt động tương trợ tư pháp mà một quốc gia có thể yêu cầu quốc gia thành viên khác tiến hành nhằm thu thập dữ liệu máy tính, phục vụ cho hoạt động điều tra. Cụ thể, theo quy định của Công ước Budapest, những hoạt động này bao gồm:

- Truy cập dữ liệu máy tính được lưu trữ. Theo đó, QGTV có thể yêu cầu QGTV khác tiến hành khám xét hoặc truy cập, thu giữ hoặc các biện pháp tương tự và tiết lộ các dữ liệu đang được lưu trữ bởi hệ thống máy tính đặttrên lãnh thổ của quốc gia được yêu cầu. Yêu cầu sẽ được quốc gia liên quan thực hiện nhanh chóng nếu có căn cứ cho rằng dữ liệu sẽ bị huỷ bỏ hoặc thay đổi và có điều khoản quy định về hỗ trợ nhanh chóng được ghi nhận trong các thoả thuận giữa các bên và pháp luật quốc gia (Điều 31);
- Thu thập dữ liệu lưu thông trong thời gian thực. Cụ thể, các QGTV Công ước sẽ thực hiện các hoạt động tương trợ nhau trong việc thu thập dữ liệu lưu thông trong thời gian thực có liên quan đến liên lạc đang được điều tra trên lãnh thổ của mình được truyền tải qua hệ thống máy tính; ít nhất các quốc gia sẽ thực hiện tương trợ đối với với các tội phạm mà việc thu thập dữ liệu là sẵn có trong hồ sơ vụ việc mà quốc gia đang tiến hành (Điều 33)
- Chặn dữ liệu nội dung. Theo đó, QGTV sẽ thực hiện các hoạt động tương trợ nhau trong việc thu thập hoặc ghi lại dữ liệu nội dung trong thời gian thực có liên quan đến liên lạc đang được điều tra trên lãnh thổ của mình được truyền tải qua hệ thống máy tính trong phạm vi cho phép theo các thoả thuận và pháp luật quốc gia (Điều 34).

(3) Thiết lập Mạng lưới 24/7

Mạng lưới 24/7 là một điểm liên lạc hoạt động 24 giờ một ngày và 7 ngày trong tuần để cung cấp sự hỗ trợ kịp thời trongviệc điều tra hoặc tiến hành các hoạt động tố tụng đối với tội phạm liên quan đến hệ thống máy tính hoặc dữ liệu máy tính, thu thập chứng cứ dưới hình thức điện tử. Nội dung hỗ trợ của mạng lưới bao gồm tạo điều kiện thuận lợi hoặc trong trường hợp được pháp luật hoặc thực tiễn

quốc gia cho phép, sẽ trực tiếp tiến hành cung cấp các tư vấn kỹ thuật; bảo quản dữ liệu và thu thập chứng cứ, cung cấp thông tin pháp lý và địa điểm của nghi phạm.

Để đảm bảo hiệu quả trong hoạt động của Mạng lưới 24/7 cũng như hiệu quả trong việc phối hợp giữa các quốc gia trong quá trình điều tra, Công ước Budapest yêu cầu QGTV phải đảm bảo năng lực thực thi của Mạng lưới với điểm liên lạc của QGTV khác một cách nhanh chóng, đảm bảo sự sẵn có của đội ngũ nhân sự được đào tạo bài bản và trang bị tốt để hỗ trợ hoạt động của Mạng lưới; trong trường hợp điểm liên lạc không thuộc cơ quan chức năng của quốc gia QGTV phải đảm bảo điểm liên lạc đó có thể điều phối với cơ quan chức năng chịu trách nhiệm về hỗ trợ tư pháp (Điều 35).

(4) Truy cập xuyên biên giới dữ liệu máy tính được lưu trữ

Nhằm tạo điều kiện tối đa cho các cơ quan tố tụng trong quá trình điều tra, theo quy định của Công ước Budapestt, QGTV có thể truy cập xuyên biên giới dữ liệu máy tính được lưu trữ với sự nhất trí của QGTV khác (Điều 32).

Tuy nhiên, trong một số trường hợp đặc biệt, QGTV có thể thực hiện hoạt động này mà không cần sự cho phép của quốc gia liên quan. Ngoại lệ này được ghi nhận trong Công ước Budapest, bao gồm:

Một là, truy cập dữ liệu máy tính được lưu trữ sẵn có (nguồn mở) bất kể dữ liệu này đặt tại khu vực nào;

Hai là, truy cập hoặc tiếp nhận, thông qua hệ thống máy tính trên lãnh thổ nước mình, dữ liệu máy tính được lưu trữ đang đặt trên lãnh thổ QGTV khác nếu quốc gia nhận được sự nhất trí một cách hợp pháp và tự nguyện từ người có quyền hợp pháp được tiết lộ dữ liệu cho quốc gia liên quan thông qua hệ thống máy tính đó. Theo Hướng dẫn của Uỷ ban Công ước Budapest, trường hợp này liên quan đến hai tình huống: (i) Email cá nhân có thể được lưu trữ tại QGTV khác bởi nhà cung cấp dịch vụ hoặc một người có thể cố ý lưu trữ dữ liệu tại quốc gia khác. Những người này có thể retrieve dữ liệu với điều kiện là họ có quyền hợp pháp, họ có thể tự nguyện disclose dữ liệu cho cơ quan thực thi pháp luật hoặc cho phép việc tiếp cận chính thức dữ liệu; (ii) Một nghi phạm buôn bán ma tuý bị bắt giữ hợp pháp trong khi hòm thư điện tử của người đó với các bằng chứng tội phạm đang được mở trên bàn, điện thoại thông minh hoặc các phương tiện khác. Nếu nghi phạm tự nguyện nhất trí với việc truy cập của cảnh sát và nếu cảnh sát chắc chắn rằng, dữ liệu của hòm thư điện tử đặt tại QGTV khác, cảnh sát có thể tiếp cận dữ liệu.[42]

[42] Xem: Cybercrime Convention Committee (T-CY) (2014), *T-CY Guidance Note # 3 - Transborder access to data (Article 32*), page.4,5.

Nhằm tránh sự tuỳ tiện của các QGTV trong tiến hành các hoạt động truy cập dữ liệu tại QGTV khác, Hướng dẫn của Uỷ ban Công ước cũng ghi nhận rõ, điều khoản này chỉ áp dụng trong quá trình điều tra, khởi tố một số tội phạm hình sự cụ thể, bao gồm: Các tội phạm công nghệ cao được quy định trong Công ước; các tội phạm hình sự khác được thực hiện bằng hệ thống máy tính; tập hợp bằng chứng theo hình thức điện tử một tội phạm hình sự.[43]

3.2.2. Thủ tục, thể thức tương trợ tư pháp

Thủ tục tương trợ tư pháp đối với tội phạm công nghệ cao vừa được quy định trực tiếp tại các điều ước về tội phạm công nghệ cao cũng như được ghi nhận trong cả các điều ước riêng biệt về tương trợ tư pháp.

Nhìn chung, theo các quy định của các điều ước quốc tế trên, các điều kiện và trình tự thủ tục tương trợ được tiến hành theo những thể thức sau đây:

- Quốc gia yêu cầu sẽ gửi yêu cầu tương trợ tư pháp bằng văn bản đến cơ quan được chỉ định làm cơ quan đầu mối tiếp nhận yêu cầu tương trợ tư pháp của quốc gia được yêu cầu, trong đó, ghi nhận cụ thể các nội dung cần tương trợ tư pháp. Trong trường hợp khẩn cấp, yêu cầu tương trợ tư pháp hoặc các liên lạc có liên quan có thể được tiến hành bằng các phương tiện liên lạc nhanh như fax hoặc thư điện tử… Tập hợp các văn bản yêu cầu và các tài liệu, hồ sơ, giấy tờ kèm theo sẽ được gửi cho quốc gia được yêu cầu theo kênh liên lạc đã được quy định trong điều ước quốc tế hữu quan, có thể là kênh ngoại giao hoặc kênh tư pháp…

- Sau khi đã nhận được yêu cầu tương trợ tư pháp hình sự đúng thủ tục, quốc gia được yêu cầu sẽ nghiên cứu và cho phép tiến hành các hoạt động tương trợ tư pháp theo yêu cầu trên lãnh thổ nước mình. Quá trình thực hiện tương trợ tư pháp hình sự phải tuân thủ theo các quy định tố tụng của luật quốc gia được yêu cầu hoặc quy định của các hiệp định tương trợ tư pháp. Tuy nhiên luật tố tụng hình sự của nước yêu cầu có thể được áp dụng, nếu quốc gia được yêu cầu đồng ý chấp thuận. Đây được coi là ngoại lệ của nguyên tắc Lex fori trong tố tụng pháp lý của cả lĩnh vực hình sự và dân sự quốc tế.

Chi phí cho hoạt động tương trợ tư pháp trên lãnh thổ của quốc gia được yêu cầu thường do quốc gia yêu cầu thanh toán, trừ các trường hợp cụ thể khác do các bên thoả thuận.

Về vấn đề từ chối tương trợ tư pháp, các trường hợp không tương trợ tư pháp được quy định trong các điều ước liên quan như:

---

[43] Xem: Cybercrime Convention Committee (T-CY) (2014), *T-CY Guidance Note # 3 - Transborder access to data (Article 32*), page.5

- Việc thực hiện tương trợ tư pháp hình sự xâm phạm đến chủ quyền quốc gia, an ninh và trật tự công cộng hoặc các lợi ích sống còn quan trọng khác đối với quốc gia;

- Yêu cầu liên quan đến tội phạm chính trị hoặc tội phạm liên quan đến tội phạm chính trị;

- Hoạt động tương trợ tư pháp hình sự không phù hợp với các qui định hiện hành của luật pháp quốc gia hoặc quy định của điều ước giữa các bên được viện dẫn làm căn cứ tương trợ tư pháp;

- Không đáp ứng yêu cầu về "định danh kép" đối với một số tội phạm khi thực hiện một số nội dung tương trợ tư pháp cụ thể theo quy định của quốc gia được yêu cầu trên cơ sở điều ước quốc tế. Cụ thể, một số điều ước quốc tế như Công ước Budapest, Nghị định thư về tương trợ tư pháp hình sự của Cộng đồng Nam Phi có quy định về điều kiện "định danh kép" khi thực hiện tương trợ tư pháp hình sự. Chẳng hạn, theo quy định của Công ước Budapest, trong trường hợp QGTV yêu cầu "định danh kép" là điều kiện để đáp ứng yêu cầu tương trợ tư pháp trong việc khám xét hoặc thực hiện các biện pháp tương tự khác để truy cập, thu giữ hoặc các biện pháp bảo đảm khác hoặc cung cấp thông tin dữ liệu máy tính đang được lưu giữ, quốc gia được yêu cầu có quyền từ chối thực hiện các yêu cầu tương trợ tư pháp nêu trên nếu không đáp ứng được yêu cầu "định danh kép" (Khoản 4 Điều 29).

3.3. Dẫn độ

3.3.1. Điều kiện, thể thức dẫn độ

Về nguyên tắc, dẫn độ là quyền của quốc gia và xuất phát từ chủ quyền quốc gia. Trên cơ sở quyền lực tối cao trong phạm vi lãnh thổ, quốc gia có quyền quyết định có tiến hành chuyển giao hay không cá nhân đang hiện diện trên lãnh thổ nước mình cho quốc gia yêu cầu để tiến hành truy cứu trách nhiệm hình sự. Trong khoa học luật hình sự quốc tế, trường hợp này được coi là "dẫn độ tội phạm không có điều ước quốc tế". Dẫn độ tội phạm trong trường hợp không có điều ước quốc tế tương ứng chỉ có thể được thực hiện theo quan điểm và đường lối riêng của quốc gia được yêu cầu, dựa trên cơ sở pháp lý quan trọng là phápluật của quốc gia. Nhiều quốc gia đã ban hành các đạo luật chuyên biệt về dẫn độ, trong đó ghi nhận một trong những nguyên tắc quan trọng cho phép dẫn độ, đó là dẫn độ được tiến hành trên cơ sở của nguyên tắc có đi có lại. Theo đó, quốc gia được yêu cầu sẽ tiến hành dẫn độ tội phạm nếu quốc gia yêu cầu đã từng tiến hành dẫn độ theo yêu cầu của quốc gia này hoặc quốc gia được yêu cầu nhận thấy được sự bảo đảm chắc chắn từ phía quốc gia yêu cầu rằng, trong trường hợp có yêu cầu dẫn độ tương tự phát sinh

trong tương lai thì quốc gia đó chắc chắn cũng sẽ thực hiện việc dẫn độ tội phạm theo yêu cầu của quốc gia này. Đây là nguyên tắc được ghi nhận trong pháp luật của nhiều quốc gia. Ví dụ Bộ luật Tố tụng hình sự Ba Lan quy định "*Ba Lan sẽ không dẫn độ tội phạm cho quốc gia nước ngoài nào không đảm bảo nguyên tắc có đi có lại trong quan hệ dẫn độ giữa hai quốc gia*". Nguyên tắc có đi có lại thể hiện sự tôn trọng và bình đẳng chủ quyền giữa các quốc gia.Trong trường hợp đồng ý dẫn độ, quốc gia sẽ tiến hành dẫn độ trên cơ sở pháp luật quốc gia. Luật tố tụng nước ngoài (luật nước yêu cầu) trong quá trình dẫn độ có thể được áp dụng nếu có sự thoả thuận của các bên có liên quan, đồng thời đáp ứng mọi điều kiện và yêu cầu được đặt ra.

Dẫn độ tội phạm với tính chất là nghĩa vụ pháp lý quốc tế ràng buộc chỉ phát sinh khi giữa các quốc gia có liên quan tồn tại điều ước quốc tế tương ứng quy định các điều kiện cụ thể cho phép dẫn độ. Tuy nhiên, nghĩa vụ này không phải là tuyệt đối. Bởi lẽ, ngay cả trong trường hợp có điều ước thì dẫn độ cũng chỉ có thể được thực hiện theo đúng các thể thức, điều kiện phù hợp với quy định của điều ước quốc tế đó. Ngay tại Điều 1 Công ước châu Âu về dẫn độ mặc dù có tiêu đề là "Nghĩa vụ dẫn độ" nhưng đã thể hiện rất rõ điều này khi quy định rằng: *"Các bên ký kết tiến hành bắt giữ cho nhau, theo những điều khoản và điều kiện đặt ra trong Công ước này, tất cả những người mà cơ quan có thẩm quyền của quốc gia yêu cầu đang điều tra về hành vi phạm tội hoặc đang bị truy nã bởi cơ quan có thẩm quyền để chấp hành bản án hoặc các quyết định giam giữ"*. Những điều ước quốc tế làm cơ sở pháp lý để dẫn độ tội phạm công nghệ cao hiện nay bao gồm:

(1) Các điều ước chuyên biệt về dẫn độ, trong đó quy định cụ thể các vấn đề pháp lý về dẫn độ như thủ tục dẫn độ, điều kiện dẫn độ, các trường hợp không dẫn độ, chi phí… Phổ biến trong số này là những hiệp định dẫn độ song phương,[44] ngoài ra còn có thể kể đến một số các hiệp định dẫn độ khu vực như Công ước châu Âu về dẫn độ.

(2) Hiệp định tương trợ tư pháp theo nghĩa rộng. Khác với những hiệp định tương trợ tư pháp hình sự không quy định dẫn độ là phạm vi của tương trợ tư pháp hình sự, những hiệp định tương trợ tư pháp theo nghĩa rộng, điều chỉnh chung các vấn đề cả về hình sự, dân sự ghi nhận dẫn độ tội phạm là một trong những nội dung

[44] Chẳng hạn, chỉ tính đến năm 2010, Mỹ đã ký kết hơn 100 hiệp định dẫn độ với các quốc gia và vùng lãnh thổ trên thế giới; tính đến năm 2013, Vương quốc Anh ký kết hơn 130 hiệp định dẫn độ với các quốc gia và vùng lãnh thổ…
Xem: Extradition To and From the United States: Overview of the Law and Recent Treaties *https://fas.org/sgp/crs/misc/98-958.pdf,* (truy cập lần cuối ngày 1/11/2020).
https://www.gov.uk/guidance/extradition-processes-and-review, (truy cập lần cuối 1/11/2020)

của tương trợ tư pháp được điều chỉnh bởi những hiệp định này. Chẳng hạn, các Hiệp định tương trợ tư pháp về hình sự, dân sự được ký kết giữa Việt Nam với Bungari (Điều 5), Liên bang Nga (Điều 5), Lào (Điều 5), Cu Ba (Điều 5)… quy định một trong những nội dung thuộc phạm vi tương trợ tư pháp là dẫn độ tội phạm để xét xử hoặc chấp hành hình phạt tù.[45]

(3) Các điều ước quốc tế về phòng chống tội phạm xuyên quốc gia có điều khoản ghi nhận QGTV có thể viện dẫn điều ước này làm cơ sở pháp lý để tiến hành dẫn độ trong trường hợp giữa các bên hữu quan chưa có điều ước chuyên biệt về dẫn độ, điển hình là Công ước của Liên hợp quốc về phòng chống tội phạm có tổ chức xuyên quốc gia (Công ước Palermo). Điều 16 Công ước quy định rằng: *"Nếu một quốc gia thành viên đưa ra điều kiện dẫn độ trên cơ sở điều ước quốc tế nhận được yêu cầu dẫn độ từ một quốc gia thành viên khác mà giữa các bên chưa có điều ước, quốc gia đó có thể thừa nhận Công ước này là cơ sở pháp lý để dẫn độ đối với bất kỳ tội phạm nào áp dụng điều khoản này"* (Khoản 4)[46]. Trên thực tế, không ít yêu cầu dẫn độ đã được đưa ra và được thực hiện trên cơ sở viện dẫn điều khoản này của Công ước.[47]

Tuy nhiên, để có thể viện dẫn các điều ước về phòng chống tội phạm xuyên quốc gia làm căn cứ để dẫn độ, tội phạm công nghệ cao phải thoả mãn đầy đủ các

---

[45] Ví dụ, theo quy định tại Hiệp định tương trợ tư pháp về dân sự, hình sự Việt Nam – Liên bang Nga, phạm vi tương trợ tư pháp bao gồm: Các bên ký kết thực hiện tương trợ tư pháp cho nhau bằng cách tiến hành các hành vi tố tụng riêng biệt được pháp luật của Bên ký kết được yêu cầu quy định, như lập, gửi và tống đạt giấy tờ, công nhận và thi hành quyết định của Toà án về các vấn đề dân sự, tiến hành khám xét, thu giữ và chuyển giao vật chứng, tiến hành giám định, lấy lời khai của các bên, người làm chứng, người giám định, người bị xác định đã thực hiện hành vi phạm tội, bị cáo và những người khác, tiến hành truy tố hình sự, dẫn độ để truy tố hình sự hoặc để thi hành bản án (Điều 5).
https://lanhsuvietnam.gov.vn/Doc/He%20thong%20VBPQ/Dieu%20uoc%20QT%20song%20phuong/3.HD-TTTP/Russia%20-%20Civil,%20criminal%20matters%20(vn).pdf

[46]Chẳng hạn, trong năm 2009, 2010, sau khi nhận được yêu cầu dẫn độ của Mỹ đối với 3 người là thành viên của một nhóm tội phạm hình sự liên quan đến việc sử dụng máy tính để thực hiện các hành vi gian lận ngân hàng, Estonia đã tiến hành dẫn độ 3 người này trên cơ sở Điều 16 của Công ước; Rumania đã gửi 17 yêu cầu dẫn độ liên quan đến tội phạm công nghệ cao trên cơ sở viện dẫn điều khoản dẫn độ của Công ước đến một loạt quốc gia gồm Australia, Brazil, Jordan, Malaysia, Mexico, New Zealand, Arab Saudi, Tunisia và Liên đoàn các nước Arab.

[47] Xem: Conference of the Parties to the United Nations Convention against Transnational Organized Crime (2010), *Catalogue of cases involving extradition, mutual legal assistance and other forms of international legal cooperation requested on the basis of the United Nations Convention against Transnational Organized Crime*

điều kiện của tội phạm xuyên quốc gia. Theo quy định của Công ước Palermo, tội phạm xuyên quốc gia là tội phạm mà *hành vi phạm tội được thực hiện ở nhiều quốc gia hoặc được thực hiện ở một quốc gia, nhưng phần chủ yếu của việc chuẩn bị, lên kế hoạch, chỉ đạo hay điều khiển việc thực hiện tội phạm lại diễn ra ở một quốc gia khác, hoặc đây là hành vi tội phạm được thực hiện ở một quốc gia nhưng có liên quan đến một nhóm tội phạm có tổ chức tham gia thực hiện các hoạt động tội phạm ở nhiều quốc gia, hoặc tội phạm được thực hiện ở một quốc gia nhưng có ảnh hưởng nghiêm trọng đến một quốc gia khác (Điều 3)*. Nói cách khác, tội phạm công nghệ cao để được coi là tội phạm xuyên quốc gia phải liên quan đến ít nhất hai quốc gia, phải thỏa mãn và được biểu hiện trên một trong các phương diện mà tại Công ước đã trù định:

(i) "nhóm tội phạm có tổ chức" (Organized Criminal Group): Tại khoản (a) Điều 2 của Công ước có quy định : "Nhóm tội phạm có tổ chức là một nhóm có cơ cấu gồm từ ba người trở lên, tồn tại trong một thời gian và hoạt động có phối hợp để thực hiện một hay nhiều tội phạm nghiêm trọng hoặc các hành vi phạm tội được quy định trong Công ước này, nhằm đạt được, trực tiếp hay gián tiếp, lợi ích về tài chính hay vật chất khác". Nhóm có cơ cấu ở đây được hiểu là một nhóm không phải được hình thành một cách ngẫu nhiên để thực hiện một hành vi phạm tội tức thời và không nhất thiết là vai trò của các thành viên trong nhóm phải được xác định rõ ràng mà phải hiểu quan hệ giữa các thành viên phải được duy trì hoặc cơ cấu của nhóm phải được phát triển (theo khoản c Điều 2 Công ước). Mục đích của nhóm tội phạm có tổ chức là vụ lợi về vật chất. Mọi hoạt động của chúng, dù trực tiếp hay gián tiếp, đều hướng tới những lợi ích về tài chính hay vật chất cụ thể nào đó.

(ii) Về "hành vi phạm tội có tính chất xuyên quốc gia" (Transnational Offence): Hành vi phải được thực hiện ở nhiều quốc gia, cụ thể hành vi phạm tội đó phải được thực hiện trên lãnh thổ từ hai quốc gia trở lên (khoản 2 Điều 3). Thêm vào đó, việc chuẩn bị, lên kế hoạch, chỉ đạo hoặc điều khiển hành vi phạm tội đó diễn ra ở nhiều quốc gia hoặc ở một quốc gia nhưng liên quan đến một nhóm tội phạm có tổ chức tham gia các hoạt động tội phạm ở nhiều quốc gia hoặc có ảnh hưởng lớn ở một quốc gia khác...

(4) Các điều ước về tội phạm công nghệ cao có điều khoản về dẫn độ như Công ước Budapest. Điều 24 Công ước ghi nhận các nguyên tắc chung liên quan đến dẫn độ tội phạm công nghệ cao, trong đó có quy định rằng "Nếu một quốc gia thành viên Công ước quy định việc dẫn độ phải có điều kiện là có hiệp định dẫn độ mà hiện tại, giữa các quốc gia thành viên liên quan chưa có hiệp định dẫn độ thì

quốc gia có thể viện dẫn Công ước này làm cơ sở pháp lý dẫn độ các tội phạm công nghệ cao được ghi nhận trong Công ước" (Khoản 3).

3.3.2. Điều kiện dẫn độ, các trường hợp không dẫn độ

Điều kiện dẫn độ phổ biến được quy định là nguyên tắc "định danh kép" kèm theo yêu cầu về thời hạn tù giam. Chẳng hạn, theo quy định tại Công ước Budapest, việc dẫn độ giữa các quốc gia thành viên Công ước được thực hiện với điều kiện là tội phạm đó bị trừng phạt về hình sự theo pháp luật của cả hai quốc gia liên quan với hình phạt tước đoạt tự do tối thiểu 1 năm trở lên hoặc hình phạt nặng hơn (Điều 24). Tuy nhiên, có một ngoại lệ liên quan đến điều kiện "định danh kép" được ghi nhận trong Lệnh bắt giữ châu Âu (EAS) ban hành theo Chỉ thị khung 2002/584/JHA ngày 13/6/2002 của Hội đồng bộ trưởng châu Âu.[48]Lệnh bắt giữ châu Âu là một quyết định tư pháp do một quốc gia thành viên Liên minh châu Âu đưa ra để QGTV khác thực hiện việc bắt giữ vàchuyển giao một người theo yêu cầu nhằm mục đích tiến hành khởi tố hình sự, chấp hành hình phạt tù hoặc chấp hành một yêu cầu giam giữ (Điều 1). Điều 2 EAS đã liệt kê 32 hành vi, trong đó, bao gồm cả tội phạm liên quan đến máy tính và khiêu dâm trẻ em, mà nếu thoả mãn điều kiện (i) được quy định trong luật hình sự của QGTV đưa ra yêu cầu và (ii) hình phạt được quy định trong luật hình sự của quốc gia đó là hình phạt tù hoặc giam giữ với thời hạn tối thiểu ít nhất 3 năm thì QGTV nhận được yêu cầu sẽ tiến hành chuyển giao cho QGTV yêu cầu mà không cần xem xét điều kiện "định danh kép". Nói cách khác, đối với các hành vi tội phạm công nghệ cao, khi một QGTV của Liên minh châu Âu đưa ra Lệnh bắt giữ châu Âu gửi đến một QGTV khác thì ngay cả khi pháp luật của quốc gia được yêu cầu không quy định hành vi đó là tội phạm, quốc gia được yêu cầu không được viện dẫn lý do không thoả mãn điều kiện "định danh kép" để từ chối chuyển giao nếu hình phạt áp dụng với hành vi theo quy định tại luật hình sự của QGTV yêu cầu là hình phạt tù hoặc giam giữ với thời hạn tối thiểu 3 năm.

Liên quan đến các trường hợp không dẫn độ, các căn cứ từ chối dẫn độ tội phạm công nghệ cao nói riêng cũng như tội phạm nói chung thường được quy định phổ biến như:

- Không dẫn độ tội phạm chính trị hoặc không dẫn độ công dân nước mình. Đối với trường hợp người được yêu cầu dẫn độ là công dân của quốc gia được yêu

[48] Xem: Chỉ thị khung 2002/584/JHA ngày 13/6/2002 của Hội đồng bộ trưởng châu Âu về Lệnh bắt giữ châu Âu
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0584&from=en

cầu, xuất phát từ chủ quyền quốc gia, quốc gia có quyền từ chối không dẫn độ, thay vào đó, quốc gia sẽ trực tiếp tiến hành các hoạt động tố tụng đối với công dân nước mình theo nguyên tắc *aut dedere aut punicare (hoặc dẫn độ hoặc xét xử);* ngược lại, xuất phát từ chủ quyền quốc gia, quốc gia vẫn có thể dẫn độ cho quốc gia yêu cầu. Kể cả trong trường hợp sau, việc dẫn độ công dân của mình liên quan đến tội phạm công nghệ cao hay không vẫn là quyền của quốc gia. Nói cách khác, quốc gia có quyền từ chối không dẫn độ công dân nước mình.

Tuy nhiên, có một ngoại lệ đối với trường hợp này được quy định tại Lệnh bắt giữ châu Âu. Theo quy định tại Chỉ thị khung 2002/584/JHA ngày 13/6/2002 của Hội đồng bộ trưởng châu Âu, QGTV nhận được EAS bắt buộc phải từ chối thực hiện EAS nếu (i) Hành vi phạm tội của người bị yêu cầu trong Lệnh bắt giữ thuộc trường hợp được ân xá tại quốc gia được yêu cầu, cũng là quốc gia có thẩm quyền khởi tố theo quy định của pháp luật quốc gia đó; (ii) Người bị yêu cầu đã được xét xử tại một quốc gia thành viên về cùng một hành vi phạm tội đã nêu trong Lệnh bắt giữ hoặc (iii) Người bị yêu cầu chưa đủ tuổi chịu trách nhiệm hình sự theo quy định của pháp luật nước được yêu cầu (Điều 3). Ngoài ra, liên quan đến tội phạm công nghệ cao, QGTV nhận được EAS có thể quyết định từ chối thực hiện EAS nếu thuộc một trong các trường hợp: (i) người bị yêu cầu đã bị khởi tố tại QGTV được yêu cầu về cùng một hành vi được ghi nhận trong EAS; (ii) cơ quan tư pháp của quốc gia được yêu cầu quyết định không khởi tố hoặc đã có phán quyết cuối cùng được thông qua tại một QGTV về cùng một hành vi được ghi nhận trong EAS, trong đó, ngăn chặn các thủ tục tố tụng tiếp theo; (iii) hành vi thuộc thẩm quyền tài phán của quốc gia được yêu cầu theo quy định tại luật hình sự của quốc gia đó; (iv) người bị yêu cầu đã được xét xử tại một quốc gia thứ ba liên quan đến hành vi tương tự được ghi nhận trong EAS với điều kiện là bản án đã được tuyên, bản án đang được chấp hành hoặc đã hết thời hạn chấp hành theo luật của nước tuyên án; (v) người bị yêu cầu đang sống hoặc cư trú hoặc là công dân của nước được yêu cầu trong trường hợp mục đích của EAS nhằm chấp hành hình phạt tù hoặc quyết định giam giữ; (vi) EAS liên quan đến tội phạm mà theo luật của nước được yêu cầu, hành vi đó được thực hiện một phần hoặc toàn bộ trên lãnh thổ của nước được yêu cầu hoặc những vùng lãnh thổ được coi là lãnh thổ của quốc gia được yêu cầu hoặc hành vi đó được thực hiện ngoài lãnh thổ của QGTV đưa ra EAS và luật của quốc gia được yêu cầu không cho phép khởi tố đối với hành vi tương tự được thực hiện bên ngoài lãnh thổ quốc gia (Điều 4).

Như vậy, theo các quy định trên, nếu căn cứ vào luật hình sự của quốc gia đưa ra Lệnh bắt giữ châu Âu (quốc gia yêu cầu), hình phạt đối với tội phạm công nghệ cao tối thiểu là 12 tháng thì QGTV nhận được yêu cầu không được từ chối chuyển giao người bị yêu cầu cho QGTV đã đưa ra EAS để khởi tố chỉ vì lý do người đó là công dân nước mình. QGTV nhận được EAS chỉ có thể viện dẫn lý do người bị yêu cầu là công dân nước mình để từ chối không chuyển giao cho QGTV yêu cầu nếu mục đích của EAS nhằm chấp hành hình phạt tù hoặc giam giữ; trong trường hợp từ chối, quốc gia này sẽ thi hành hình phạt tù hoặc giam giữ đối với người bị yêu cầu phù hợp với pháp luật nước mình.

- Hành vi làm căn cứ yêu cầu dẫn độ đã được xét xử tại quốc gia được yêu cầu *(Nguyên tắc Non bis in idem – Không ai bị xét xử về cùng một hành vi phạm tội)*

- Việc dẫn độ không phù hợp với pháp luật của quốc gia được yêu cầu, xâm phạm chủ quyền quốc gia hoặc trật tự an ninh xã hội;

3.4. Chuyển giao người bị kết án

Cơ sở pháp lý quốc tế phổ biến để tiến hành chuyển giao người bị kết án là các điều ước điều chỉnh riêng biệt về chuyển giao người bị kết án, bao gồm cả điều ước song phương và đa phương, trong đó, phổ biến nhất là các hiệp định song phương. Công ước năm 1954 giữa Lebanon và Arap có thể coi là điều ước song phương đầu tiên trong lĩnh vực này với nội dung cho phép các bên ký kết thi hành các bản án của nhau, trừ trường hợp những bản án ngắn, với điều kiện có sự nhất trí của các bên và người bị kết án. Số lượng ngày càng tăng của các điều ước song phương dẫn đến thực tế là một quốc gia vừa là thành viên của một hiệp định đa phương, vừa là thành viên của nhiều hiệp định song phương khác. Chẳng hạn, Vương quốc Anh vừa là thành viên của Công ước châu Âu về chuyển giao người bị kết án, vừa ký kết các hiệp định song phương với rất nhiều quốc gia và vùng lãnh thổ như Antigua và Barbuda, Barbados, Brazil, Cuba, Dominica, Ai Cập, Ghana, Guyana, Ấn Độ, Lào, Libya,Maroc, Nicaragua, Pakistan, Peru, Saint Lucia, Sri Lanka, Thái Lan, Uganda, Venezuela, Việt Nam, Hong Kong và Trung Quốc; tương tự, Canada vừa là thành viên của Công ước châu Âu về chuyển giao người bị kết án, vừa ký kết các hiệp định song phương với nhiều quốc gia như Argentina, Barbados, Bolivia, Brazil, Cuba, Dominican, Ai Cập, Pháp, Mexico, Mongolia, Morocco, Peru, Thái Lan, Mỹ, Venezuela.

Điều kiện phổ biến để chuyển giao người bị kết án được quy định trong các điều ước bao gồm: (1) Người bị kết án là công dân của nước thi hành án; (2) Bản án

đã tuyên là bản án cuối cùng, chưa còn thủ tục nào chưa giải quyết liên quan đến người bị kết án; (3) Có sự đồng ý của người bị kết án; (4) Vào thời điểm nhận được yêu cầu chuyển giao, thời gian chấp hành hình phạt còn lại theo bản án đã tuyên phải không ít hơn thời gian được quy định trong điều ước quốc tế hoặc pháp luật quốc gia[49]; (5) Đáp ứng điều kiện "định danh kép" theo luật hình sự của các nước tuyên án và nước thi hành án; (6) Nước tuyên án và nước thi hành án đồng ý chuyển giao.

Liên quan đến điều kiện về sự đồng ý của người bị kết án và định danh kép, có các trường hợp ngoại lệ cụ thể đối với hai điều kiện này được quy định trong các văn bản của Liên minh châu Âu. Cụ thể, theo quy định tại Quyết định khung của Hội đồng 2008/909/JHA ngày 27/11/2008 về áp dụng nguyên tắc công nhận lẫn nhau trong các vấn đề hình sự đối với các bản án phạt tù hoặc hình phạt tước tự do nhằm mục đích thi hành tại Liên minh châu Âu[50], điều kiện về sự chấp thuận của người bị kết án sẽ không cần xem xét đến trong trường hợp người bị kết án được chuyển đến QGTV mà người đó là công dân sinh sống; QGTV mà người bị kết án sẽ bị trục xuất sau khi người đó được giải phóng khỏi việc thi hành án trên cơ sở lệnh trục xuất được đưa vào bản án hoặc quyết định tư pháp hoặc quyết định hành chính hoặc QGTV mà người bị kết án đã bỏ trốn hoặc quay trở lại để xem xét các thủ tục tố tụng đối với người đó tại quốc gia kết án (Điều 4). Tương tự, điều kiện "định danh kép" cũng không đặt ra trong trường hợp người bị kết án về tội phạm mạng hoặc khiêu dâm trẻ em nếu người đó bị kết án bằng hình phạt tù hoặc các biện pháp tước tự do với thời hạn tối thiểu 3 năm (Điều 5).

Ngoài những điều kiện phổ biến như trên, hiện nay một số quốc gia còn xem xét đến các điều kiện liên quan đến quyền con người để quyết định có chuyển giao người bị kết án hay không. Toà nhân quyền châu Âu đã áp dụng các quy tắc đối với dẫn độ và trục xuất người nước ngoài tương tự như đối với chuyển giao người bị kết án. Theo đó, trong những trường hợp nhất định, một người nước ngoài không thể bị trục xuất nếu việc trục xuất sẽ làm mất sự tương xứng giữa quyền cá nhân với gia

[49] Ví dụ, theo quy định tại Công ước châu Âu về chuyển giao người bị kết án, một trong những điều kiện để chuyển giao là tại thời điểm nhận được yêu cầu, phần hình phạt còn phải chấp hành của người bị kết án tối thiểu phải là 6 tháng (Điều 3) trong khi theo quy định tại Hiệp định về chuyển giao người bị kết án Việt Nam – Liên bang Nga, thời hạn này tối thiểu là 1 năm 9 (Điều 3)

[50] Xem: COUNCIL FRAMEWORK DECISION 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0909&from=EN

đình hoặc cuộc sống riêng tư (Điều 8 Công ước châu Âu về bảo vệ quyền con người và tự do cơ bản). Thực tế là, khi quốc gia kết án tìm cách đưa một người đã bị kết án đi mà không có sự đồng ý của người đó, quốc gia kết án phải đảm bảo rằng việc chuyển giao không phương hại đến những quyền con người cơ bản có liên quan đến người đó. Điều này cũng có thể đòi hỏi phải được sự đảm bảo của quốc gia thi hành án sẽ không xâm hại những quyền con người cơ bản của người bị kết án.[51] Trong một số trường hợp, nội dung này có thể được ghi nhận cụ thể trong các điều ước song phương. Chẳng hạn, Hiệp định về chuyển giao người bị kết án giữa Uganda và Vương quốc Anh quy định rằng: "*Mỗi bên sẽ đối xử với tất cả những người bị chuyển giao theo Hiệp định này phù hợp với những nghĩa vụ quốc tế về quyền con người"*.

Sau khi tiếp nhận phạm nhân, quốc gia thi hành án phải bảo đảm tiếp tục thi hành án phạt phù hợp với luật pháp nước mình, đồng thời dựa trên cơ sở bản án của tòa án nước tuyên án. Nếu theo luật pháp của nước thi hành án, thời hạn tối đa của hình phạt đã thực hiện ít hơn thời hạn đã ấn định trong bản án, thì tòa án của nước thi hành án sẽ quyết định thời hạn tối đa theo luật nước mình. Quyết định đối với việc thi hành án phạt bổ sung sẽ được nước thi hành án thực hiện nếu luật nước này cũng qui định như vậy. Ở mức độ nhất định, các vấn đề pháp lý về giảm án, ân xá, thay đổi án phạt, xem xét lại bản án đều được ghi nhận trong luật hình sự quốc tế, nhìn chung theo quan điểm sau: mỗi bên đều có quyền giảm án, ân xá, đặc xá hoặc thay đổi án phạt phù hợp với luật pháp nước mình, còn vấn đề kháng án, xem xét lại bản án chỉ nước kết án mới có quyền giải quyết. Sau khi chuyển giao người bị kết án sẽ không bị truy cứu trách nhiệm hoặc bị xét xử tại nước thi hành án về cùng hành vi phạm tội mà nước tuyên án đã có bản án trừng phạt. Vấn đề chấm dứt thi hành án sẽ được thực hiện, khi nước tuyên án gửi quyết định xác nhận hình phạt không phải thực thi nữa cho quốc gia thi hành án.

3.5. Xác định thẩm quyền tài phán

Từ góc độ lý luận, khoa học luật quốc tế xác định thẩm quyền tài phán của quốc gia được hiểu theo hai nghĩa. Theo nghĩa rộng, thẩm quyền tài phán của một quốc gia cụ thể được hiểu là quyền riêng biệt của mỗi quốc gia trong các lĩnh vực hoạt động của quốc gia, cụ thể là trong lĩnh vực lập pháp, hành pháp và tư pháp. Như vậy, thẩm quyền tài phán quốc gia được cấu thành từ quyền lập pháp, hành

[51] Xem: The United Nations Office on Drugs and Crime (2012), Handbook on the International Transfer of Sentenced Persons, page.87

pháp và tư pháp của quốc gia và đây chính là quyền lực tối cao của một nhà nước trong phạm vi lãnh thổ của mình, một nội dung quan trọng của chủ quyền quốc gia.

Theo nội dung này, trong phạm vi lãnh thổ của mình, quốc gia có quyền lực tối cao trong việc thực hiện quyền và nghĩa vụ trong lĩnh vực lập pháp, tư pháp và hành pháp mà không có bất kì sự can thiệp nào từ bên ngoài, có quyền thông qua các quyết định về mọi vấn đề chính trị, kinh tế, văn hóa và xã hội của đất nước với mục đích tối thượng là bảo vệ quyền và lợi ích của nhân dân, an ninh và ổn định của đất nước. Thẩm quyền tài phán hiểu theo nghĩa này được xây dựng trên nền tảng nguyên tắc bình đẳng chủ quyền quốc gia và không can thiệp vào công việc nội bộ của quốc gia khác.

Theo nghĩa hẹp của thuật ngữ này (thẩm quyền tài phán quốc gia), khoa học luật quốc tế xác định thẩm quyền tài phán quốc gia đơn giản chỉ là thẩm quyền xét xử và giải quyết các vụ việc thuộc phạm vi điều chỉnh của luật quốc gia. Như vậy, hiểu theo nghĩa hẹp, thẩm quyền tài phán nằm trong phạm vi giới hạn của hoạt động tư pháp nhà nước. Căn cứ vào tiêu chí bản chất vụ việc cần giải quyết, thẩm quyền bao gồm: thẩm quyền tài phán trong lĩnh vực hình sự, thẩm quyền tài phán trong lĩnh vực dân sự và thẩm quyền tài phán trong lĩnh vực hành chính cũng như thẩm quyền tài phán đối với các vụ việc khác phát sinh trong đời sống xã hội của quốc gia.

Từ góc độ pháp lý, thẩm quyền tài phán hình sự quốc gia là tổng thể các quyền cho phép hoặc nghiêm cấm, quyền xét xử và thi hành án trong các vụ án hình sự. Quyền cho phép hoặc nghiêm cấm là những quyền cho phép chủ thể luật được thực hiện những hành vi mà luật pháp không cấm hoặc không được thực hiện các hành vi mà luật pháp không cho phép. Quyền này thường được quy định trong luật hình sự và tố tụng hình sự quốc gia; còn quyền xét xử là thẩm quyền được thực hiện nhằm truy tố, xét xử và trừng phạt của cơ quan tài phán hình sự quốc gia đối với các chủ thể phạm tội được quy định tại các văn bản quy phạm pháp luật hình sự và tố tụng hình sự của mỗi nước; còn quyền thi hành không phải đơn giản chỉ là quyền thi hành phán quyết mà là quyền thực hiện các hoạt động tư pháp chuyên môn của mỗi nước trong phạm vi lãnh thổ của mình. Quyền này không thể được thi hành ở nước ngoài nếu không có sự chấp nhận của quốc gia nước ngoài. Quyền thi hành được xây dựng trên nền tảng nguyên tắc bình đẳng chủ quyền quốc gia và không can thiệp vào công việc của quốc gia khác.

Tội phạm hình sự truyền thống, ngay cả tội phạm xuyên quốc gia cũng không có đặc điểm của "tính ảo" và tính "mở rộng không giới hạn" như tội phạm công

nghệ cao vì mục tiêu của các tội phạm này là hữu hình và các đối tượng được cấu thành bởi không gian ba chiều thực sự. Ví dụ, một số cựu sinh viên Đức đã xâm chiếm Bộ Quốc phòng Hoa Kỳ qua Internet với mục đích đánh cắp bí mật quân sự cho Nga, các sinh viên lần đầu đăng nhập vào máy chủ tại Nhật Bản thông qua mạng của Đức trong khi sử dụng dữ liệu mạng của Nhật Bản và hệ thống tín hiệu để chuyển đến một trường đại học ở Hoa Kỳ và cuối cùng xâm chiếm máy tính của Bộ Quốc phòng Hoa Kỳ thông qua hệ thống mạng lưới trường đại học Hoa Kỳ này và đánh cắp các bí mật quân sự quan trọng của Hoa Kỳ. Trong trường hợp này, một số hành vi tội phạm của học sinh kéo dài từ Đức, Nhật Bản và Hoa Kỳ. Liệu tất cả các quốc gia có thẩm quyền tài phán hình sự đối với trường hợp này hay không và liệu Nhật Bản có quyền tài phán không?

Từ đó, có thể nhận thấy một số nguyên tắc của Luật hình sự quốc tế trong xác định thẩm quyền tài phán hoàn toàn áp dụng đối với tội phạm công nghệ cao, bao gồm:

- ***Nguyên tắc lãnh thổ***

Nguyên tắc lãnh thổ được ghi nhận trong Công ước Budapest với nội dung, QGTV ban hành luật và các biện pháp cần thiết khác để thực hiện thẩm quyền tài phán đối với *các hành vi tội phạm được thực hiện trên lãnh thổ nước mình*. Chẳng hạn, một toà án ở Pháp đã thừa nhận quyền thẩm quyền tài phán đối với Yahoo, một nhà cung cấp nội dung nhắn tin trực tuyến của Mỹ và ra lệnh gỡ bỏ các trang web tại Pháp hiển thị bản ghi nhớ của Đức quốc xã. Trong một vụ việc khác, một toà án Anh đã tuyên rằng một công dân Anh phải chịu trách nhiệm đối với việc đăng tải những bức ảnh bị coi là tục tĩu ở Anh lên một trang web có máy chủ đặt tại Mỹ; tương tự, một công dân Mỹ đã bị toà án nước này tuyên phải chịu trách nhiệm đối với hoạt động của một công ty đánh bạc có trụ sợ đặt tại Antigua nhận tiền đặt cược của các công dân Mỹ thông qua Internet.

Xuất phát từ tính "ảo" của các loại hình tội phạm trên không gian mạng nên không dễ để xác định chính xác nơi hành vi thực sự diễn ra. Việc công khai một trang web có nội dung phạm pháp như khiêu dâm trẻ em hoặc ngôn từ kích động thù địch, có thể được coi là diễn ra tại nơi nội dung được tải lên. Nhưng hành động tải lên có thể liên quan đến một số quốc gia, nếu nhà cung cấp nội dung ở tại quốc gia A trong khi nhà cung cấp dịch vụ lưu trữ ở tại quốc gia B, trong trường hợp đó, hành động tải lên được bắt đầu ở A và chấm dứt ở B và thậm chí có thể được coi như diễn ra ở các nước trung gian thông qua dữ liệu được vận chuyển. Tuy nhiên, việc công bố một website có thể được xem như diễn ra tại vị trí của máy chủ vì việc

công bố website là một hành động liên tục diễn ra từ thời điểm tải lên trở đi. Trong trường hợp này, hành vi tội phạm chỉ có thể diễn ra tại quốc gia đặt máy chủ. Một lập luận khác cho rằng việc công bố website xảy ra ở bất kỳ nơi nào mà nội dung có thể tiếp nhận và xem được, mặc dù có nhiều khả năng đây là nơi bị tác động hơn là nơi thực hiện hành vi.[52]

Trên thực tế, nguyên tắc lãnh thổ được các quốc gia quy định thành những căn cứ khác nhau để xác định thẩm quyền tài phán, bao gồm:

Một là, nơi thực hiện hành vi.

Chẳng hạn tại Hoa Kỳ, một số bang có cách tiếp cận rất rộng trong xác định vấn đề này. Ví dụ, theo quy định tại bang Arkansas, bang Akansas có thẩm quyền đối với bất kỳ hành vi tội phạm công nghệ cao nào được quy định ở chương này nếu việc truyền tải cấu thành hành vi phạm tội được bắt nguồn từ bang này hoặc được nhận tại bang này"; theo quy định tại Bắc Carolina, tội phạm mạng được coi là thực hiện tại bang này nếu thông tin liên lạc điện tử được gửi đi hoặc được nhận tại Bắc Carolina; luật của bang Utah có quy định khá chi tiết trong việc xác định thẩm quyền tài phán của bang. Theo đó, một người sẽ bị khởi tố tại bang Utah do hành vi phạm tội của người đó, bất kể trong hay ngoài bang Utah do hành vi của người đó hoặc của người mà anh ta phải chịu trách nhiệm pháp lý nếu: (i) hành vi phạm tội được thực hiện một phần hoặc toàn bộ tại bang này; (ii) hành vi được thực hiện ngoài bang nhưng cấu thành nỗ lực để thực hiện hành vi phạm tội tại bang này; (iii) hành vi bên ngoài bang nhưng tạo thành một âm mưu phạm tội tại bang và hành động sau đó được thực hiện tại bang này.

Tại Đức, Bộ luật hình sự Đức quy định rằng, một hành vi được coi là thực hiện trên lãnh thổ Đức nếu: (1) Hành vi được thực hiện tại bất kỳ địa điểm nào trên lãnh thổ Đức mà thủ phạm đã hành động hoặc trong trường hợp có nghĩa vụ phải hành động nhưng thiếu sót không hành động hoặc tại lãnh thổ Đức, xuất hiện hậu quả là một yếu tố của hành vi phạm tội; (2) Hành vi khuyến khích, xúi giục hoặc đồng phạm được thực hiện không chỉ tại nơi hành vi được thực hiện mà còn tại bất kỳ nơi nào trên lãnh thổ Đức. Nếu việc khuyến khích, xúi giục hoặc đồng phạm được thực hiện tại Đức nhằm xúi giục hoặc đồng phạm với hành vi diễn ra ở nước

[52] Xem: Susan W. Brenner & Bert-Jaap Koops (2004), "Approaches to Cybercrime Jurisdiction", *Journal of high technology law,* Vol. IV No. 1. Page 3- 44.

ngoài, luật hình sự Đức vẫn sẽ áp dụng, ngay cả khi hành vi đó không bị trừng phạt theo luật của nơi thực hiện hành vi này.[53]

Hai là, nơi đặt máy tính. Một số bang của Hoa Kỳ, chẳng hạn như Connecticut, có các đạo luật ghi nhận thẩm quyền tài phán cho bang trong các vụ án tội phạm công nghệ cao vì hệ quả của hành vi phạm tội ảnh hưởng đến một máy tính tại bang đó. Tương tự, Luật của Singapore cũng quy định thẩm quyền của nước này đối với tội phạm công nghệ cao nếu "máy tính, dữ liệu hoặc chương trình tại Singapore".

Ba là, nơi bị tác động của hành vi phạm tội. Theo căn cứ này, quốc gia sẽ thực hiện thẩm quyền tài phán đối với các hành vi xảy ra ngoài khu vực thuộc thẩm quyền tài phán của quốc gia nhưng ảnh hưởng có hại đến lãnh thổ quốc gia đó. Trong vụ *UnitedStatesvs. Nippon Paper Industries Co., Ltd*, Toà án bang Massachusetts đã khẳng định rằng: *"Quốc gia có thẩm quyền tài phán đối với hành vi xảy ra bên ngoài lãnh thổ quốc gia nhưng có tác động đáng kể hoặc nhằm tạo ra tác động đáng kể đối với lãnh thổ của quốc gia liên quan"*.[54]

- ***Nguyên tắc quốc tịch***

Sau nguyên tắc lãnh thổ, nguyên tắc quốc tịch của người phạm tội (quốc tịch chủ động) là nguyên tắc phổ biến thứ hai để xác định thẩm quyền tài phán của quốc gia đối với tội phạm công nghệ cao. Theo quy định của Công ước Budapest, quốc gia có thẩm quyền tài phán đối với người phạm tội mang quốc tịch của quốc gia nếu hành vi đó bị trừng phạt theo luật hình sự của quốc gia nơi hành vi đó được thực hiện hoặc hành vi được thực hiện ngoài lãnh thổ của bất kì quốc gia nào (Điểm (d) Khoản 1 Điều 22). Luật hình sự của nhiều quốc gia đã ghi nhận nguyên tắc này để xác định thẩm quyền tài phán quốc gia. Chẳng hạn, luật hình sự Đức quy định rằng, Đức có thẩm quyền tài phán đối với cả các hành vi phạm tội do công dân Đức thực hiện ở nước ngoài nếu hành vi đó bị trừng phạt theo luật hình sự của quốc gia nơi hành vi đó được thực hiện hoặc không thuộc thẩm quyền tài phán hình sự của quốc gia nơi hành vi đó được thực hiện. Tương tự, luật hình sự Hà Lan cũng quy định

---

[53] Đơn cử, một người gửi một email từ Đức với chương trình tạo virus dưới dạng tệp đính kèm và nếu người nhận ở Benin, một quốc gia ở Tây Phi, sử dụng virus này ở quốc gia của mình, anh ta phải chịu trách nhiệm hình sự ở Đức về tội lây lan virus , bất kể việc lan truyền virus có phải là tội phạm ở Benin hay không.

[54] Xem: **U.S. District Court for the District of Massachusetts,** *United States v. Nippon Paper Industries Co., Ltd., 62 F. Supp. 2d 173 (D. Mass. 1999)* https://law.justia.com/cases/federal/district-courts/FSupp2/62/173/2410334/

thẩm quyền tài phán của nước này đối với hành vi giả mạo, bao gồm cả giả mạo bằng máy tính, do các nhân viên trong Chính chủ Hà Lan hoặc nhân viên của các tổ chức quốc tế có trụ sở tại Hà Lan thực hiện ở nước ngoài nếu hành vi đó bị trừng phạt theo luật hình sự của quốc gia nơi hành vi đó được thực hiện; hành vi khiêu dâm trẻ em do công dân Hà Lan thực hiện. Đặc biệt, luật của Hà Lan quy định thẩm quyền tài phán hình sự của nước này trên cơ sở quốc tịch ngay cả trong trường hợp một người trở thành công dân Hà Lan chỉ sau khi đã thực hiện hành vi phạm tội.

Ngoài quốc tịch của người phạm tội như quy định của Công ước Budapest, một số quốc gia cũng quy định quốc tịch của nạn nhân như một căn cứ để xác định thẩm quyền tài phán. Chẳng hạn, luật hình sự của Hà Lan quy định rằng, Hà Lan có thẩm quyền tài phán đối với hành vi phá hoại máy tính hoặc gây thiệt hại dữ liệu để chống lại một công dân Hà Lan nếu hành vi đó thuộc phạm vi của Điều 2 Công ước quốc tế về ngăn ngừa khủng bố bằng bom hoặc Công ước về ngăn ngừa tài trợ khủng bố; hoặc theo quy định tại Bộ luật hình sự Hoa Kỳ, Hoa Kỳ có thẩm quyền tài phán đối với các hành vi chống lại chính phủ liên bang, ví dụ, Hoa Kỳ có thẩm quyền đối với bất kì người nào cố ý, không được sự cho phép của cơ quan có thẩm quyền, truy cập bất kì máy tính nào của các cơ quan của Mỹ (Mục 1030 (a) (3) Điều 18). Với nguyên tắc này, một quốc gia có thể yêu cầu thẩm quyền tài phán nếu máy tính của công dân quốc gia đang cư trú ở nước ngoài bị ảnh hưởng do hành vi phát tán virus.

- ***Nguyên tắc quốc tịch của tàu thuyền, phương tiện bay***

Theo quy định của Công ước Budapest, quốc gia sẽ có thẩm quyền tài phán đối với tội phạm công nghệ cao nếu hành vi được thực hiện trên tàu thuyền treo cờ của quốc gia hoặc phương tiện bay đăng ký tại quốc gia (Điểm b, c Khoản 1 Điều 22).

Dưới góc độ lý luận, một số học giả cho rằng thẩm quyền phương tiện bay hoặc tàu thuyền được coi là thẩm quyền cạnh tranh với thẩm quyền lãnh thổ. Trong thực tiễn quan hệ quốc tế, đã phát sinh nhiều trường hợp xung đột pháp luật về thẩm quyền tài phán giữa quốc gia, nơi phương tiện bay hay tàu thuyền đang lưu trú với quốc gia mà các phương tiện giao thông này mang quốc tịch. Để giải quyết vấn đề pháp lý này các quốc gia đã có sự thừa nhận chung nguyên tắc thẩm quyền hỗn hợp để xử lý, theo đó quốc gia có thẩm quyền tài phán đối với các hành vi tội phạm được thực hiện trên phương tiện bay hay tàu thuyền là quốc gia đăng tịch các phương tiện này với điều kiện hành vi xâm phạm đó và hậu quả của nó không gây ra hoặc đe dọa gây ra thiệt hại cho an ninh và chủ quyền quốc gia sở tại. Nếu vượt

quá giới hạn này, quốc gia nơi tàu thuyền và phương tiện bay đang lưu trú sẽ có thẩm quyền tài phán. Nội dung của nguyên tắc này đã được ghi nhận trong các điều ước quốc tế hữu quan cũng như luật hàng hải và hàng không của các quốc gia. Chẳng hạn, theo quy định của Công ước luật biển 1982, nếu tội phạm công nghệ cao được thực hiện trên tàu thuyền nước ngoài khi con tàu đang đi qua lãnh hải của quốc gia ven biển, quốc gia mà tàu mang cờ sẽ thực hiện thẩm quyền tài phán đối với hành vi vi phạm trừ các trường hợp sau, thẩm quyền tài phán sẽ thuộc về quốc gia ven biển, bao gồm: (i) Hậu quả của hành vi vi phạm mở rộng đến quốc gia ven biển; (ii) Hành vi vi phạm đe doạ đến hoà bình của quốc gia ven biển hoặc an ninh, trật tự trong lãnh hải; (iii) Thuyền trưởng hoặc viên chức ngoại giao, lãnh sự của quốc gia mà tàu mang cờ yêu cầu hỗ trợ (Khoản 1 Điều 27).

Trong trường hợp tàu thuyền hay phương tiện bay đang vận hành trên các vùng lãnh thổ quốc tế thì thẩm quyền tàu thuyền hay phương tiện bay sẽ là thẩm quyền duy nhất được áp dụng, ngoại trừ các ngoại lệ được qui định.

Ngoài những nguyên tắc phổ biến như trên, nguyên tắc thẩm quyền phổ quát mặc dù không được ghi nhận trong Công ước Budapest nhưng cũng được quy định trong luật hình sự của một số quốc gia để xác định thẩm quyền tài phán đối với một số loại hình tội phạm công nghệ cao cụ thể, như trường hợp của Bỉ và Đức, hai quốc gia này thừa nhận nguyên tắc thẩm quyền phổ quát đối với hành vi khiêu dâm trẻ em.

Đối với tội phạm công nghệ cao, hoàn toàn có thể xảy ra tình trạng xung đột thẩm quyền tài phán, tức là tình trạng nhiều hơn một quốc gia đều tuyên bố thực hiện thẩm quyền tài phán hình sự đối với cùng một hành vi tội phạm công nghệ cao. Xuất phát từ đặc điểm của loại tội phạm này, người phạm tội có thể thực hiện hành vi thông qua các không gian ảo trải rộng trên một số hoặc hàng chục quốc gia mà không tiếp xúc gần với các đối tượng cụ thể và hậu quả của hành vi phạm tội lớn hơn nhiều so với các loại tội phạm khác. Chẳng hạn, một công dân Hà Lan sử dụng máy tính tại Bỉ để xâm nhập một máy tính ở Utah, trong trường hợp này, ít nhất Hà Lan, Bỉ và Utah đều có thể tuyên bố thực hiện thẩm quyền tài phán đối với hành vi này, đặc biệt nếu người phạm tội tiến hành truyền dữ liệu thông qua lãnh thổ của Singapore hay Mỹ thì các quốc gia này cũng có thể tuyên bố thực hiện thẩm quyền tài phán. Trên thực tế, đối với trường hợp virus "love bug" hay "Blaster worm", nhiều quốc gia đã cùng tuyên bố thẩm quyền tài phán trên cơ sở tác động của những virus này đến các quốc gia trên hay trường hợp một website đăng ký tại bang Wyoming (Mỹ) truyền dẫn những hình ảnh, clip khiêu dâm trẻ em trên một số

website tại Bỉ, Đức, ngoài tuyên bố thẩm quyền tài phán của ba quốc gia này trên cơ sở hành vi vi phạm thực hiện trên lãnh thổ nước mình, một số quốc gia châu Âu khác cũng tuyên bố thẩm quyền tài phán với hành vi trên với lý do, website đã khuyến khích, trợ giúp cho các hành vi phạm tội liên quan đến khiêu dâm trẻ em tại những quốc gia đó. Công ước Budapest cũng như các điều ước về tội phạm công nghệ cao đều không có quy định giải quyết trực tiếp vấn đề xung đột thẩm quyền tài phán này. Công ước Budapest chỉ đưa ra một quy định mang tính nguyên tắc *"Khi có nhiều hơn một quốc gia đều đưa ra yêu cầu thẩm quyền tài phán trên cơ sở phù hợp với Công ước này, các bên liên quan sẽ, khi thích hợp, tham vấn nhằm mục đích xác định thẩm quyền tài phán thích hợp nhất để khởi tố"* (Khoản 5 Điều 22). Tuy nhiên, Báo cáo giải thích của Công ước lại ghi nhận rằng, tham vấn không phải là nghĩa vụ. Theo đó, "nếu một quốc gia thành viên cho rằng tham vấn không cần thiết, ví dụ quốc gia thành viên đó nhận được xác nhận rằng quốc gia thành viên khác không có kế hoạch tiến hành tham vấn, hoặc nếu một quốc gia thành viên cho rằng, tham vấn có thể ảnh hưởng đến quá trình điều tra, khởi tố của họ, quốc gia thành viên đó có thể trì hoãn hoặc huỷ bỏ việc tham vấn".[55] Mặt khác, đến nay, cả trên phương diện lý luận cũng như pháp lý, chưa có quy tắc để xác định thế nào là "thẩm quyền tài phán thích hợp nhất". Nói cách khác, không có thứ bậc ưu tiên giữa các nguyên tắc xác định thẩm quyền tài phán. Điều này dẫn đến thực tế, trong trường hợp có tranh chấp phát sinh giữa các quốc gia liên quan đến thẩm quyền tài phán, không có những quy tắc thống nhất để giải quyết tranh chấp này. Do đó, việc xác định thẩm quyền tài phán thuộc về quốc gia nào, phụ thuộc phần lớn vào cơ quan giải quyết tranh chấp.

3.6. Thực tiễn thực hiện pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao của một số quốc gia

3.6.1. Cộng hòa Liên bang Đức

Cộng hòa Liên bang Đức đã phê chuẩn Công ước Budapest vào năm 2009 và cũng đã tiến hành sửa đổi Bộ luật Hình sự ngay sau khi phê chuẩn Công ước[56]. Theo đó, Bộ luật Hình sự của Đức bao gồm tất cả các điều khoản tương đối toàn diện và tương thích với quy định cơ bản của Công ước về tội phạm máy tính và tội

[55] Xem: Explanatory Report to the Convention on Cybercrime (Báo cáo giải thích của Công ước Budapest)

[56] Chart of signatures and ratifications of Treaty 185 - Convention on Cybercrime, xem tại: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true (truy cập lần cuối ngày 03/6/2021)

phạm mạng[57]. Tương tự như vậy, Bộ luật Tố tụng hình sự của nước này cũng đề cập đến hầu hết các quyền tố tụng có liên quan đã được nêu trong Công ước, tuy nhiên có loại trừ một số điều khoản (sẽ được đề cập ở các phần tiếp theo).

Với việc thực hiện nghĩa vụ đối với quốc gia thành viên trong việc hình sự hóa hành vi phạm tội và nghĩa vụ hoàn thiện hệ thống pháp luật quốc gia, Bộ luật Hình sự Đức tại các điều khoản từ Điều 202 đến Điều 206 quy định các hành vi phạm tội được tạo ra do vi phạm quyền riêng tư thông qua lừa đảo, gián điệp, ăn cắp dữ liệu (*data espionage*), hành vi chuẩn bị dữ liệu cho hoạt động gián điệp cũng như các hành vi chuẩn bị cho hoạt động gián điệp. Tội phạm mạng như được quy định trong Bộ luật Hình sự Đức liên quan đến một số hành vi tội phạm nhất định được truyền bá thông qua việc sử dụng các hệ thống máy tính[58].

Tại Điều 303b quy định về hành vi phá hoại hệ thống máy tính và các chương trình phần mềm máy tính (*computer sabotage*). Theo quy định này, bất kỳ ai can thiệp vào các hoạt động xử lý dữ liệu bằng cách xóa, ngăn chặn, hiển thị dữ liệu không sử dụng được hoặc thay đổi hoặc bằng cách nhập hoặc truyền dữ liệu với ý định gây thiệt hại cho người khác sẽ phải chịu hình phạt tiền hoặc hình phạt tù lên đến ba năm[59]. Điều tương tự cũng áp dụng cho việc phá hủy, làm hỏng, làm cho không sử dụng được, loại bỏ hoặc thay đổi hệ thống xử lý dữ liệu hoặc phương tiện truyền dữ liệu. Ngoài ra Bộ luật này còn quy định các hành vi khuyến khích phạm tội nghiêm trọng đe dọa toàn vẹn lãnh thổ, phân phối, mua lại và sở hữu các tài liệu khiêu dâm, các buổi biểu diễn thông qua phát sóng,[60] đánh chặn dữ liệu (*data interception*),[61] rình rập, gian lận, phá hoại, tổ chức và tham gia đánh bạc bất hợp pháp cũng như vi phạm bí mật thông tin cá nhân và vi phạm bí mật chính thức (*breach of official secrets*).[62]

Tính đến nay Cộng hòa Đức đã ban hành một số lượng khá lớn văn bản luật pháp liên quan trong lĩnh vực an ninh thông tin, bao gồm văn bản được ban hành ở cấp độ Luật, Đạo luật. Đạo luật chính liên quan đến an ninh mạng ở Đức là Đạo luật An ninh mạng (*IT-Sicherheitsgesetz*) chính thức có hiệu lực vào ngày 25 tháng 7

[57] German Criminal Code - "Strafgesetzbuch" (StGB), xem tại: https://www.gesetze-im-internet.de/englisch_stgb/ (truy cập lần cuối ngày 02/6/2020)
[58] Section 202-206 of the German Criminal Code, xem tại: https://www.gesetze-im-internet.de/englisch_stgb/ (truy cập lần cuối ngày 02/6/2020)
[59] Section 303 of the German Criminal Code, xem tại: https://www.gesetze-im-internet.de/englisch_stgb/ (truy cập lần cuối ngày 02/6/2020)
[60] German Criminal Code (note above) Sect 184.
[61] German Criminal Code (note above) Sect 202b.
[62] German Criminal Code (note above) Chap 15.

năm 2015. Ngoài ra, Đức cũng đã sửa đổi một số đạo luật, đặc biệt là Đạo luật Truyền thông công nghệ Telemedia(*Telemediengesetz*), Đạo luật Viễn thông (*Telekommunikationsgesetz*), Quy định bảo vệ dữ liệu chung của EU (*Datenschutz-Grundverordnung*), Đạo luật Bảo vệ dữ liệu liên Bang (*Bundesdatenschutzgesetz*) và Đạo luật Văn phòng liên Bang về bảo mật thông tin (*Gesetz uber das Bundesamt fur Sicherheit in der Informationstechnik*). Bên cạnh đó, những quy định cụ thể của lĩnh vực bảo đả an toàn an ninh mạng được điều chỉnh bởi Đạo luật về Ngân hàng (*Kreditwesengesetz*) và Đạo luật liên quan đến lĩnh vực giao dịch chứng khoán (*Wertpapierhandelsgesetz*)[63]...Pháp luật về an ninh mạng của Đức nhằm buộc các nhà khai thác cơ sở hạ tầng quan trọng cung cấp bảo mật CNTT tốt hơn và báo cáo về các rủi ro cũng như các mối đe dọa có nguy cơ hiện hữu, đặc biệt trong bối cảnh các cuộc tấn công mạng diễn ra liên tiếp trên phạm vi toàn cầu gần đây.

Đạo luật Văn phòng liên Bang về Bảo mật thông tin (BSI) quy định các nghĩa vụ cụ thể đối người vận hành, khai thác các sản phẩm, dịch vụ thiết yếu về bảo mật công nghệ thông tin được đề cập trong Đạo luật[64], bao gồm tất cả các phương tiện kỹ thuật để xử lý hoặc truyền tải thông tin phải:

- Thực hiện các biện pháp phòng ngừa về tổ chức và kỹ thuật thích hợp để tránh làm gián đoạn tính khả dụng, tính toàn vẹn, tính xác thực và tính bảo mật của các hệ thống công nghệ thông tin, hoặc bất kỳ thành phần hay quy trình nào gắn liền với chức năng của các cơ sở hạ tầng quan trọng;

- Chứng minh sự tuân thủ các yêu cầu của Văn phòng liên bang về Bảo mật thông tin bằng các phương pháp kiểm tra, đánh giá hoặc chứng nhận bảo mật ít nhất hai năm một lần đối với Văn phòng liên bang về Bảo mật thông tin;

- Chỉ định một đầu mối liên hệ với Văn phòng liên bang về Bảo mật thông tin trong vòng sáu tháng, phải sẵn sàng 24/7; và

- Báo cáo ngay các sự cố cho Văn phòng liên bang về Bảo mật thông tin qua người liên hệ

---

[63] Germany enacts IT-Security Act, xem tại: https://www.twobirds.com/en/news/articles/2015/germany/july/germany-enacts-it-security-act, truy cập lần cuối ngày 22/6/2020

[64] Act on the Federal office for Information Security (BSI Act – BSIG), xem tại: https://www.gesetze-im-internet.de/englisch_bsig/englisch_bsig.html (truy cập lần cuối ngày 02/6/2020)

Về thủ tục tố tụng, truy tố các hành vi phạm tội công nghệ cao, được quy định trong Bộ luật Tố tụng hình sự Đức (StPO).[65] Các cuộc điều tra tội phạm sẽ do cảnh sát đảm nhiệm hoặc theo yêu cầu của cơ quan công tố. Cảnh sát có nghĩa vụ thực hiện yêu cầu đó, cơ quan công tố chịu trách nhiệm về việc thực hiện thủ tục hình sự. Các biện pháp tố tụng/cưỡng chế được xác định bởi Công ước Budapest được quy định trong StPO và do đó có thể áp dụng cho các cuộc điều tra của cơ quan thực thi pháp luật Đức đối với bất kỳ tội phạm nào thuộc thẩm quyền của họ, như được quy định trong Điều 14 Công ước Budapest. Tuy nhiên, các biện pháp sơ bộ theo Công ước Budapest (Điều 16 và 17) không được quy định trong StPO, vì khái niệm thu giữ dữ liệu máy tính, bao gồm cả việc tiết lộ dữ liệu, được thực hiện bằng cách áp dụng khái niệm thu giữ người mang dữ liệu liên quan, như được quy định cho các đồ vật để làm chứng cứ tại Điều 94 của StPO[66].

Trong lĩnh vực tương trợ tư pháp hình sự, Đức có thể cung cấp, hỗ trợ pháp lý dựa trên hai căn cứ: một hiệp ước/công ước hoặc trên cơ sở không có điều ước (có đi có lại). Với điều kiện cốt lõi là các nguyên tắc cơ bản của luật pháp Đức không bị vi phạm. Luật pháp quốc gia của Đức cho phép, trên cơ sở nguyên tắc có đi có lại, có thể thực hiện các yêu cầu tương trợ tư pháp trong tương lai mà không có thỏa thuận song phương hoặc đa phương đã được thực hiện theo luật pháp quốc tế[67]. Vấn đề tương trợ tư pháp này áp dụng cho: yêu cầu kiểm tra người làm chứng, yêu cầu thu giữ và giao nộp tài liệu, yêu cầu cung cấp thông tin, yêu cầu cung cấp hồ sơ, yêu cầu thu giữ và giao nộp tiền, cũng như yêu cầu dẫn độ, yêu cầu quá cảnh và yêu cầu tiếp quản việc thi hành án. Nếu tương trợ tư pháp không thuộc phạm vi điều chỉnh của một hiệp định quốc tế thì việc hỗ trợ sẽ dựa trên Luật hỗ trợ pháp lý quốc tế trong các vấn đề hình sự (IRG) của Đức năm 1982 (đặc biệt là thực hiện theo các Điều 59-67a của IRG)[68]. Các yêu cầu từ các nhà chức trách nước ngoài phải tuân theo các yêu cầu về thủ tục tương tự như các yêu cầu áp dụng cho một cuộc điều tra hình sự của Đức. Tương tự, trong vấn đề dẫn độ tội phạm; chuyển giao người bị kết án, Luật hỗ trợ pháp lý quốc tế trong các vấn đề hình sự quy định: "*Trong chừng*

---

[65] German Code of Criminal Procedure, xem tại: https://www.gesetze-im-internet.de/englisch_stpo/ (truy cập lần cuối ngày 02/6/2020)

[66] Section 94 of German Code of Criminal Procedure, xem tại: https://www.gesetze-im-internet.de/englisch_stpo/ (truy cập lần cuối ngày 02/6/2020)

[67] Section 76, Act on International Mutual Assistance in Criminal Matters, xem tại: http://www.gesetze-im-internet.de/englisch_irg/ (truy cập lần cuối ngày 03/6/2020)

[68] Act on International Mutual Assistance in Criminal Matters, xem tại: http://www.gesetze-im-internet.de/englisch_irg/ (truy cập lần cuối ngày 03/6/2020)

mực các hiệp định đã trở thành luật áp dụng trực tiếp trong nước, các quy định của các hiệp định theo luật quốc tế sẽ được ưu tiên hơn các quy định của Đạo luật này". Tuy nhiên, luật này yêu cầu điều kiện dẫn độ và thi hành án, đó là nguyên tắc "định danh kép", có nghĩa "việc dẫn độ chỉ được cho phép nếu hành vi phạm tội cũng là hành vi trái pháp luật Đức đáp ứng các yếu tố của điều khoản hình sự hoặc nếu nó cấu thành một hành vi tương tự như vậy" và "dẫn độ vì mục đích truy tố chỉ được phép nếu hành vi phạm tội bị trừng phạt theo luật của Đức tước đoạt tự do tối thiểu 1 năm"[69]. Như vậy, có thể thấy các quy định về tương trợ tư pháp hình sự, dẫn độ tội phạm hay chuyển giao người bị kết án của Đức khá tương thích với quy định của các Công ước quốc tế, đặc biệt là Công ước Budapest, Công ước châu Âu về dẫn độ, Công ước Palermo…

Về việc phân định thẩm quyền tài phán đối với tội phạm công nghệ cao, việc áp dụng các quy định của pháp luật Đức để truy tố các hành vi phạm tội phụ thuộc vào "*nơi thực hiện hành vi phạm tội*". Theo Điều 9 Bộ luật hình sự Đức, một hành vi phạm tội được coi là đã được thực hiện ở một nơi mà người phạm tội đã hành động hoặc nơi mà hậu quả xảy ra theo ý định của người phạm tội. Do đó, các hành vi phạm tội công nghệ cao sẽ được áp dụng nếu người phạm tội thực hiện trên lãnh thổ nước Đức và trong trường hợp hành vi phạm tội ảnh hưởng đến hệ thống CNTT đươc đặt hoặc sử dụng cho các dịch vụ được cung cấp tại Đức nơi người phạm tội thực hiện ngoài lãnh thổ Đức. Điều 5 Bộ luật này quy định *không bất cứ luật nào được áp dụng* tại nơi xảy ra hành vi vi phạm bí mật kinh doanh hoặc bí mật thương mại của một doanh nghiệp thực tế nằm trong phạm vi lãnh thổ của quy chế này hoặc của một doanh nghiệp có trụ sở ở nước ngoài.

Tóm lại, các đạo luật về an ninh mạng của Đức đã có những quy định cụ thể các điều kiện về bảo đảm các tiêu chuẩn an ninh mạng đối với các sản phẩm, dịch vụ mạng thiết yếu; quy định về trách nhiệm bảo vệ và các hoạt động bảo mật, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; quy định về quyền và trách nhiệm pháp lý cho các doanh nghiệp lưu trữ web và nhà cung cấp truy cập cho các vi phạm bản quyền xảy ra trên hệ thống của họ... Nhìn chung, luật pháp về vấn đề hợp tác đấu tranh phòng chống tội phạm trong lĩnh vực công nghệ thông tin ở Đức phù hợp với những tiêu chuẩn quốc tế trong lĩnh vực này, đặc biệt là Công ước Budapest năm 2001.

[69] Section 3(1),(2), Act on International Mutual Assistance in Criminal Matters

3.6.2. Hoa Kỳ

Pháp luật Hoa Kỳ từ lâu đã được biết đến là một trong những hệ thống pháp luật toàn diện, lâu đời và hiệu quả nhất trên thế giới về bảo toàn an ninh mạng cũng như hợp tác phòng ngừa tội phạm công nghệ cao. Trên cả bình diện pháp lý và thực tiễn, Hoa Kỳ luôn xác định mối đe dọa về an ninh mạng là mối đe doạ hàng đầu đối với an ninh quốc gia. Chính vì vậy, trong Luật An ninh nội địa Hoa Kỳ (2002) quy định: *Nguy cơ an ninh mạng là các mối đe dọa và lỗ hổng của thông tin hoặc các hệ thống thông tin và bất kỳ hậu quả liên quan nào bị gây ra bởi hoặc là kết quả của việc truy cập trái phép, sử dụng, tiết lộ, làm suy giảm, gián đoạn, chỉnh sửa hoặc phá hoại các thông tin hoặc các hệ thống thông tin này, bao gồm hậu quả liên quan bởi các hành vi tấnc công và/hoặc khủng bố mạng; không bao gồm bất kỳ hành động nào chỉ liên quan đến việc vi phạm điều khoản hoặc thỏa thuận hợp đồng với khách hàng*[70]. Đạo luật cũng đã thành lập thiết chế có tên gọi "Bộ An ninh nội địa Hoa Kỳ" (DHS), với thẩm quyền hoạt động như một bộ phận điều hành tối cáo vấn đề an ninh mạng của Hoa Kỳ. Nhiệm vụ chính của cơ quan này là ngăn chặn các cuộc tấn công khủng bố, giảm thiểu nguy cơ vũ trang và phi vũ trang đối với quốc gia, giảm thiểu thiệt hại từ các cuộc tấn công và tăng khả năng phục hồi quốc gia.

Khi phát hiện nguy cơ đe dọa an ninh mạng, Điều 105 Đạo luật chia sẻ thông tin an ninh mạng (*Cybersecurity Information Sharing Act* - CISA)[71] của Mỹ quy định về báo cáo đối với các nguy cơ đe dọa an ninh mạng. Theo đó, báo cáo này phải được đệ trình lên Ủy ban Tình báo Thượng viện (*Select Committee on Intelligence of the Senate*) và Ủy ban Tình báo Hạ viện (*Permanent Select Committee on Intelligence of the House*)[72]. Đạo luật này được thiết kế nhằm hai mục đích chính: Thứ nhất, chia sẻ thông tin về các mối đe dọa an ninh mạng, bao gồm cả việc thực hiện các biện pháp bảo vệ trên hệ thống riêng của các công ty sản xuất và khai thác công nghệ; Thứ hai, khuyến khích việc chia sẻ thông tin về mối đe dọa an ninh mạng giữa Chính phủ Mỹ và các công ty, tập đoàn công nghệ. Có thể thấy rằng, CISA hiện nay vừa là công cụ quan trọng nhưng cũng vừa là cơ sở phối

---

[70] Homeland Security Act of 2002, xem tại: https://www.dhs.gov/homeland-security-act-2002 (truy cập lần cuối ngày 03/6/2020)

[71] Section 105(c)(1)(B), Cybersecurity Information Sharing Act 2015, xem tại: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf (truy cập lần cuối ngày 03/6/2020)

[72] Report of Congress: https://www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf (truy cập lần cuối ngày 03/6/2020)

hợp giữa Chính phủ Mỹ và các tập đoàn công nghệ trong việc bảo vệ những cơ sở hạ tầng thông tin quan trọng của nước này.

Luật về Lạm dụng và Gian lận máy tính (*Computer Fraud and Abuse Act* - CFAA) là công cụ chủ đạo trong công tác đấu tranh, truy tố và trừng trị tội phạm công nghệ cao với đầy đủ các chế tài về hình sự và dân sự. CFAA nghiêm cấm việc cố ý truy cập trái phép (Hacking) vào một máy tính mà không có sự cho phép hoặc vượt quá sự cho phép, làm hỏng máy tính do cố ý hoặc vượt quá sự cho phép; buôn bán mật khẩu; truyền các mối đe dọa, cụ thể là các mối đe dọa làm hỏng máy tính được bảo vệ và các mối đe dọa lấy cắp thông tin hoặc xâm phạm tính bảo mật của thông tin; tống tiền liên quan đến nhu cầu về tiền bạc hoặc tài sản. Tùy theo tội danh cụ thể mà hình phạt có thể từ 01 năm đến 20 năm tù.[73] Bên cạnh đó luật này còn quy định các hành vi phạm tội công nghệ cao khác như tấn công DOS - cố ý gây thiệt hại thông qua việc truyền tải, bị phạt tù lên đến 10 năm[74]; lừa đảo hoặc gian lận có thể bị phạt tù lên đến 20 năm[75]; lây nhiễm các phần mềm độc hại gây thiệt hại bị phạt tù lên đến 10 năm[76]; trộm cắp danh tính hoặc gian lận danh tính[77]; lấy cắp thông tin điện tử;[78] bất kỳ hoạt động nào khác ảnh hưởng xấu hoặc đe dọa đến an ninh, tính bảo mật, tính toàn vẹn hoặc tính khả dụng của hệ thống công nghệ thông tin, cơ sở hạ tầng, mạng truyền thông, thiết bị hoặc dữ liệu điện tử[79]…

Bên cạnh đó, một số văn bản pháp luật khác có liên quan như Luật bảo vệ thông tin liên lạc điện tử (*Electronic Communications protection Act* - ECPA) cũng cung cấp bổ sung thêm các biện pháp bảo vệ thông tin liên lạc trong quá trình lưu trữ và chuyển tiếp. Một đạo luật phái sinh khác của ECPA là Luật Lưu trữ Truyền thông (*Stored Communications Act* - SCA) quy định việc cố tình truy cập mà không được phép (hoặc vượt quá quyền truy cập được phép) là hành vi vi phạm hình sự đối với cơ sở cung cấp dịch vụ liên lạc điện tử, có thể bao gồm nhà cung cấp dịch vụ email hoặc người sử dụng lao động cung cấp địa chỉ email cho nhân viên của mình. Các hành vi vi phạm có thể bị phạt tù từ 01 năm nếu vi phạm lần đầu hoặc lên

---

[73] 18 U.S.C. Section 1030, Computer Fraud and Abuse Act, xem tại: http://its.famu.edu/images/pdfs/ComputerFraudAbuseAct.pdf (truy cập lần cuối ngày 03/6/2020)
[74] 18 U.S.C Section 1030(a)(5)(A), Computer Fraud and Abuse Act
[75] 18 U.S.C Section 1030(a)(5)(A) hoặc 18 U.S.C Section 2702, Computer Fraud and Abuse Act
[76] 18 U.S.C Section 1030(a)(5)(A), Computer Fraud and Abuse Act
[77] 18 U.S.C Section 1028, Computer Fraud and Abuse Act
[78] 18 U.S.C Section 1030(a)(2), Computer Fraud and Abuse Act
[79] 18 U.S.C Section 1030(a)(2) hoặc 18 U.S.C Section 2702, Computer Fraud and Abuse Act

đến 10 năm nếu vi phạm nhiều lần[80]. Với việc cố ý chặn, tiết lộ thông tin liên lạc điện tử khi giao tiếp bằng miệng hay bất kỳ thiết bị điện tử nào khác tuyệt đối bị ngăn cấm theo các quy định của Luật nghe lén (*Wiretap Act*), hình phạt cho các vi phạm có thể bao gồm hình phạt tù đến 05 năm.[81]

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 cao trên cơ sở phù hợp với tình hình của mỗi bang. Đây hầu hết là những văn bản luật có quy định chi tiết và cụ thể hơn so với luật chung của Liên 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 04 năm tù hoặc các hình phạt khác lên đến 15 năm tù tùy theo mức độ vi phạm.[82]

Trong các hoạt động tương trợ tư pháp, cơ quan ở cấp trung ương hoặc có thẩm quyền của nước ngoài có thể yêu cầu hỗ trợ từ Hoa Kỳ trong việc thu thập bằng chứng cho các cuộc điều tra hình sự, truy tố và tố tụng liên quan đến tội phạm công nghệ cao nói riêng và các loại tội phạm khác nói chung. Tất cả các yêu cầu, cho dù đó là yêu cầu theo hiệp ước song phương hay đa phương, thư yêu cầu hỗ trợ tư pháp (yêu cầu từ Tòa án nước ngoài thông qua kênh ngoại giao) hoặc thư yêu cầu phi hiệp ước, sẽ được trình lên Văn phòng Các vấn đề Quốc tế của Phòng Hình sự của Bộ Tư pháp (OIA) của Hoa Kỳ. Theo Hiến pháp Hoa Kỳ, các yêu cầu hỗ trợ pháp lý theo hiệp ước tương trợ tư pháp được thực hiện theo đúng các điều khoản của hiệp ước và luật pháp trong nước của Hoa Kỳ[83]. Theo đó, quốc gia này sẽ tận tâm, thiện chí để nỗ lực hỗ trợ pháp lý với phạm vi rộng nhất có thể đối với các quốc gia yêu cầu hỗ trợ. Việc hỗ trợ pháp lý có thể được cung cấp ở giai đoạn điều tra của thủ tục tố tụng, ví dụ như cung cấp bản sao hồ sơ của chính phủ hoặc công ty; thực hiện phỏng vấn nhân chứng; hay cung cấp mẫu chữ viết tay...[84]

---

[80] 18 U.S.C Section 2702, Stored Communications Act, xem tại: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121, truy cập lần cuối ngày 03/6/2020

[81] 18 U.S.C Section 2511, Wiretap Act, xem tại:https://www.law.cornell.edu/uscode/text/18/2515, truy cập lần cuối ngày 03/6/2020

[82] Section 156.10, 156.05, 156.20, New York Penal Law, https://www.nysenate.gov/legislation/laws/PEN/P3TJA156, truy cập lần cuối ngày 03/6/2020

[83] Title 28 Section 3512 và Section 1782, United States Code, xem tại: https://www.law.cornell.edu/uscode/text/28, truy cập lần cuối ngày 04/6/2020

[84] Title 28 Section 1733, United States Code

Trong vấn đề dẫn độ tội phạm nói chung trong đó có tội phạm công nghệ cao, Hoa Kỳ hiện có hiệp ước dẫn độ với hơn 100 quốc gia[85], hầu hết đều là các hiệp ước trên cơ sở "định danh kép", đối với các hành vi đều bị coi là tội phạm ở hai quốc gia. Nhìn chung, theo luật của Hoa Kỳ, dẫn độ chỉ có thể được thực hiện trên cơ sở một hiệp ước, tuy nhiên, Hoa Kỳ vẫn có thể dẫn độ dựa trên nguyên tắc "có đi có lại" nếu quốc gia nước ngoài đã dẫn độ cho Hoa Kỳ trong quá khứ hoặc thực hiện yêu cầu dẫn độ trong tương lai trong trường hợp không có hiệp ước[86]. Dẫn độ tội phạm còn có thể được thực hiện thông qua kênh ngoại giao, thường là từ Đại sứ quán của quốc gia nước ngoài ở Washington đến Bộ Ngoại giao và được thực hiện theo đúng trình tự thủ tục được quy định tại Điều 3190 Tiêu đề 18 của Hiến pháp Hoa Kỳ. Tương trợ tư pháp hình sự, dẫn độ tội phạm hay chuyển giao người bị kết án liên quan đến tội phạm công nghệ cao còn được thực hiện trên cơ sở Công ước Budapest, bởi công ước này cung cấp một kim chỉ nam để Hoa Kỳ xây dựng và hài hòa hóa một cách toàn diện luật pháp quốc gia về tội phạm mạng, đồng thời đây cũng là thỏa thuận hợp tác khu vực ràng buộc về tội phạm mạng mà Hoa Kỳ đã tham gia là thành viên.[87] Bên cạnh đó, Công ước Palermo cũng là một cơ chế ràng buộc pháp lý khác khi mà Hoa Kỳ là thành viên kể từ khi được phê chuẩn vào năm 2005. Mặc dù Công ước này nhằm ngăn ngừa và phòng chống tội phạm có tổ chức xuyên quốc gia, nhưng chính phủ Hoa Kỳ đã cho rằng các điều khoản của nó đôi khi có thể được sử dụng để tạo điều kiện hợp tác trong các trường hợp tội phạm mạng.[88]

Như vậy, Luật An ninh mạng của Hoa Kỳ tồn tại và được thiết kế kép ở cả cấp độ liên bang và từng tiểu bang. Bên cạnh những yêu cầu chung của pháp luật liên bang, từng tiểu bang được tạo điều kiện để đặt ra những quy định cụ thể và chi tiết hơn, đáp ứng sát với tình hình tại địa phương. Nhìn chung, pháp luật về an ninh mạng của Hoa Kỳ được đánh giá rất toàn diện và đồng bộ, có độ tương thích cao đối với các tiêu chuẩn quốc tế, đặc biệt là các quy định trong Công ước Budapest về tội phạm mạng. Về thực tiễn, pháp luật về an ninh mạng của Hoa Kỳ hiện đảm bảo

[85] Treaties and agreements, U.S. Department of State, xem tại: https://www.state.gov/2019-TIAS/?results=1000, truy cập lần cuối ngày 03/6/2020

[86] Title 18 Section 3184

[87] Chart of signatures and ratifications of Treaty 185 - Convention on Cybercrime, xem tại: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true, truy cập lần cuối ngày 03/6/2020

[88] US Global Cybercrime Cooperation: A Brief Explainer, xem tại: https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer, truy cập lần cuối ngày 04/6/2020

tốt vai trò là công cụ pháp lý trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao, góp phần quan trọng vào việc bảo vệ quyền lợi của cá nhân, tổ chức cũng như cơ sở hạ tầng công nghệ quan trọng của quốc gia và duy trì được an toàn an ninh mạng.

3.6.3. Nhật Bản

An ninh mạng nói chung và vấn đề ngăn chặn tội phạm trên không gian mạng nói riêng đã và đang trở thành một vấn đề phổ biến ở Nhật Bản; có thể coi đây là một trong những mối đe dọa hàng đầu đối với an ninh của quốc gia này. Vào tháng 11 năm 2001, chính phủ Nhật Bản đã ký tham gia Công ước Budapest về tội phạm mạng của Ủy hội châu Âu. Ngay sau khi ký, từ năm 2004 đến 2006, Chính phủ Nhật Bản đã đệ trình ba dự luật lên Quốc hội để phê chuẩn Công ước. Tuy nhiên, cả ba dự luật đều đã bị bãi bỏ trong quá trình này vì nhiều lý do khách quan.[89] Phải mất tới hơn 10 năm sau đó, một dự luật cuối cùng đã được Quốc hội thông qua và dẫn đến việc phê chuẩn Công ước vào ngày 3 tháng 7 năm 2012.[90] Theo đó, Nhật Bản đã tiến hành sửa đổi Bộ luật Hình sự và Bộ luật Tố tụng hình sự để tăng tính tương thích trong việc điều chỉnh phù hợp với các quy định của Công ước Budapest. Cùng với đó, Nhật Bản đã ban hành Luật bảo vệ thông tin cá nhân (*Personal Information Protection Act*) năm 2003 để bảo vệ dữ liệu, thông tin cá nhân và các dạng thức danh tính khác. Đặc biệt, Luật cơ bản về An ninh mạng của Nhật Bản (2014) còn mở rộng việc quy định xây dựng các tiêu chuẩn chung về các biện pháp đảm bảo an toàn an ninh mạng cho các cơ quan hành chính quốc gia và các tổ chức liên quan. Hiện tại, Nhật Bản cũng có các đạo luật khác cũng có quy định liên quan đến tội phạm công nghệ cao như Bộ luật Hình sự Nhật Bản[91] (*Penal Code*), Luật chống cạnh tranh không công bằng (*Unfair Competition Prevention Act*), Luật cấm truy cập máy tính trái phép (*Act on the Prohibition of Unauthorised*

---

[89] Cyberdefense Report, Japan's National Cybersecurity and Defense Posture, xem tại: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf (truy cập lần cuối ngày 03/06/2020)

[90] Chart of signatures and ratifications of Treaty 185 - Convention on Cybercrime, xem tại: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true (truy cập lần cuối ngày 03/6/2020)

[91] Penal Code, xem tại: http://www.japaneselawtranslation.go.jp/law/detail/?id=3581&vm=04&re=01, (truy cập lần cuối ngày 03/6/2020)

Computer Access – UCAL)[92], Luật bán trả góp (*Instalment Sales Act*), Luật bảo vệ bí mật được chỉ định đặc biệt (*Specially Designated Secret Protection Act*) và Luật an ninh xã hội và mã số thuế (*Social Security and Tax Number Act 2013*). Trên cơ sở các văn bản pháp luật của Nhật Bản quy định, có thể xác định một số hành vi phạm tội công nghệ cao cơ bản như:

- Lấy cắp dữ liệu hay truy cập trái phép (Hacking). UCAL nghiêm cấm các hành động sau: truy cập trái phép (Điều 3); lấy mã nhận dạng của người dùng được ủy quyền để thực hiện truy cập trái phép (Điều 4); cung cấp mã nhận dạng của người dùng được ủy quyền cho bên thứ ba không phải là quản trị viên quyền truy cập hoặc người dùng được ủy quyền (Điều 5); giữ mã nhận dạng của người dùng được ủy quyền đã bị lấy bất hợp pháp để thực hiện truy cập trái phép (Điều 6) và thực hiện các hành khác nhằm mạo danh quản trị viên đồng ý truy cập vào mã nhận dạng (Điều 7). Bộ luật Hình sự quy định hình phạt chính cho các hành vi trên tại Điều 168(2) và Điều 168(3). Ngoài ra là một số hình phạt bổ sung tại các Điều 234(2), 246(2) và 161(2).

- Điều 7 của UCAL nghiêm cấm hành vi lừa đảo (Phishing), trong khi Điều 4 UCAL cấm bất kỳ mã nhận dạng nào thông qua việc lừa đảo. Người nào thu lợi bất chính bằng cách sử dụng mã số nhận dạng có được từ lừa đảo sẽ bị phạt tù đến 10 năm[93].

- Với hành vi lây nhiễm hệ thống CNTT với phần mềm độc hại bao gồm ransomware (mã độc tống tiền), spyware (phần mềm gián điệp), trojan (một loại phần mềm ác tính), worm và virus được quy định hình phạt giống với hành vi lấy cắp dữ liệu/ truy cập trái phép. Việc phân phối, bán hoặc chào bán phần cứng, phần mềm hoặc các công cụ khác được sử dụng để thực hiện tội phạm mạng có thể bị phạt tù đến 03 năm hoặc bị phạt tiền lên đến 500.000 JPY[94].

- Bên cạnh các hành vi nêu trên, còn một số hành vi khác như: sở hữu hoặc sử dụng phần cứng, phần mềm hoặc các công cụ khác được sử dụng để thực hiện tội phạm mạng[95]; đánh cắp danh tính hoặc gian lận danh tính (Computer Fraud)[96]; ăn

---

[92] Act on the Prohibition of Unauthorised Computer Access , xem tại: https://www.npa.go.jp/cyber/english/legislation/uca_Tentative.pdf, (truy cập lần cuối ngày 03/6/2020)

[93] Article 246(2), Penal Code, xem tại: http://www.japaneselawtranslation.go.jp/law/detail/?id=3581&vm=04&re=01, (truy cập lần cuối ngày 03/6/2020)

[94] Article 168(2), Penal Code

[95] Article 168(3), Penal Code

cắp điện tử[97]; hay bất kỳ hoạt động nào khác ảnh hưởng xấu hoặc đe dọa đến an ninh, bảo mật, tính toàn vẹn hoặc tính khả dụng của bất kỳ hệ thống CNTT, cơ sở hạ tầng, mạng truyền thông, thiết bị hoặc dữ liệu nào[98]…

Năm 2018, Quốc hội Nhật Bản tiếp tục thông qua dự luật sửa đổi Luật cơ bản về An ninh mạng năm 2014 (Basic Act on Cybersecurity)[99]. Theo đó, an ninh mạng đề cập trong Luật sửa đổi được gắn liền với các biện pháp để quản lý dữ liệu một cách an toàn, chẳng hạn như ngăn chặn vi phạm bảo mật, mất mát hoặc hư hỏng dữ liệu; đảm bảo sự an toàn và độ tin cậy của hệ thống mạng thông tin viễn thông[100]... Luật này cũng đã làm rõ trách nhiệm của Chính phủ quốc gia Nhật Bản, chính quyền địa phương và các tổ chức liên quan khác. Giống với cơ chế của Hoa Kỳ, Nhật Bản cũng cho triển khai một thiết chế chỉ đạo-tham mưu có tên gọi "*Ban chiến lược an ninh mạng*" nhằm mục đích thúc đẩy một cách hiệu quả và toàn diện các chính sách an ninh mạng. Không chỉ dừng lại ở trách nhiệm của các cơ quan công quyền, Luật An ninh mạng còn mở rộng trách nhiệm đối với các doanh nghiệp có trách nhiệm trong việc cài đặt, khai thác, thiết lập và thúc đẩy các biện pháp an ninh mạng phù hợp (Điều 7). Theo đó, Luật đặc biệt lưu ý các thực thể kinh doanh liên quan đến không gian mạng, chẳng hạn như những chủ thể liên quan đến việc bảo trì Internet và các mạng viễn thông tiên tiến khác. Những thực thể này khi tiến hành việc khai thác và sử dụng công nghệ thông tin-viễn thông; hoặc tham gia vào hoạt động kinh doanh liên quan đến an ninh mạng, phải đảm bảo an ninh mạng một cách tự nguyện và chủ động trong hoạt động kinh doanh của mình; trách nhiệm này không loại trừ việc hợp tác với các biện pháp về an ninh mạng nếu như Chính phủ quốc gia hoặc chính quyền địa phương có yêu cầu phối kết hợp để giải quyết các vụ việc trong từng trường hợp cụ thể[101].

Đối với vấn đề tương trợ tư pháp, trên cơ sở của nguyên tắc "có đi có lại", Nhật Bản có thể hỗ trợ cung cấp bằng chứng cần thiết trong quá trình điều tra vụ án

---

[96] Article 246(2), Penal Code

[97] Article 21, paragraph 1,2; Unfair Competition Prevention Act, xem tại: https://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html, (truy cập lần cuối ngày 03/6/2020)

[98] Article 21; Unfair Competition Prevention Act

[99] Basic Act on Cybersecurity, xem tại: http://www.japaneselawtranslation.go.jp/law/detail/?printID=&ft=2&re=02&dn=1&yo=Basic+Act+on+Cybersecurity&ia=03&ph=&x=52&y=22&ky=&page=1&vm=02, (truy cập lần cuối ngày 03/6/2020)

[100] Article 2, Basic Act on Cybersecurity

[101] Article 7, Basic Act on Cybersecurity

hình sự và chuyển giao người bị kết án khi có yêu cầu từ nước ngoài theo đúng các trình tự thủ tục được quy định trong Luật Hỗ trợ quốc tế trong điều tra các vấn đề liên quan đến tội phạm công nghệ cao nói riêng và các loại tội phạm khác nói chung (Đạo luật số 69 năm 1980)[102], và có thể thông qua các kênh ngoại giao nếu như một quốc gia nước ngoài chưa ký hiệp định tương trợ với Nhật Bản. Điều này cũng cho phép Nhật Bản nhận được bằng chứng cần thiết để điều tra một vụ án hình sự từ nước ngoài miễn là có thể trong phạm vi luật pháp của họ. Với các yêu cầu hỗ trợ không dựa trên hiệp ước, dựa trên quy định của Luật Hỗ trợ quốc tế, ngoài nguyên tắc "có đi có lại" thì hoạt động tương trợ cần thỏa mãn các điều kiện sau: việc hỗ trợ là cần thiết cho cuộc điều tra tội phạm ở quốc gia yêu cầu; tội phạm không phải là tội phạm chính trị và yêu cầu hỗ trợ không nhằm mục đích điều tra hành vi phạm tội chính trị[103]; nguyên tắc "định danh kép" – hành vi cấu thành tội được yêu cầu hỗ trợ sẽ cấu thành tội phạm theo quy định của pháp luật Nhật Bản[104]; liên quan đến yêu cầu kiểm tra nhân chứng hoặc cung cấp các bằng chứng, Nhật Bản yêu cầu chứng minh rõ ràng bằng văn bản rằng bằng chứng là cần thiết cho cuộc điều tra[105]; và Bộ trưởng Bộ Tư pháp đồng ý yêu cầu hỗ trợ là phù hợp[106]. Trong trường hợp dẫn độ tội phạm, Luật dẫn độ của Nhật Bản cũng quy định các điều kiện dẫn độ tương tự như điều kiện tương trợ tư pháp và chuyển giao người bị kết án. Tuy nhiên, với nguyên tắc "định danh kép", Nhật Bản không xem xét yêu cầu một cách "*hời hợt*" bằng cách so sánh cấu thành tội phạm của cả hai nước mà còn có thể xem xét thêm các yếu tố khác như: quốc tịch, hình phạt hay nơi thực hiện hành vi phạm tội[107]...

---

[102] Section 3 Mutual Legal/Judicial Assistance in Criminal Matters, xem tại: http://hakusyo1.moj.go.jp/en/61/nfm/n_61_2_2_6_3_1.html (truy cập lần cuối ngày 04/6/2020)

[103] Article 2(1), Act on International Assistance in Investigation and Other Related Matters, xem tại:https://www.imolin.org/doc/amlid/Japan/Japan_Act_on_International_Assistance_in_Investigation_and_Other_Related_Matters_1980.pdf (truy cập lần cuối ngày 04/6/2020)

[104] Article 2(2), Act on International Assistance in Investigation and Other Related Matters

[105] Article 2(3), Act on International Assistance in Investigation and Other Related Matters

[106] Article 3(2), Act on International Assistance in Investigation and Other Related Matters

[107] Điều 2 Luật dẫn độ Nhật Bản quy định nước này có thể từ chối dẫn độ trong các trường hợp: *Khi hành vi bị yêu cầu dẫn độ không bị trừng phạt bằng án tử hình, hoặc tù chung thân hoặc án tù với khung hình phạt cao nhất từ 3 năm hoặc trên 3 năm theo quy định của luật, điều lệ hoặc pháp lệnh của quốc gia yêu cầu; Khi hành vi cấu thành tội phạm bị yêu cầu dẫn độ, theo luật, điều lệ hoặc pháp lệnh của Nhật Bản, sẽ không bị trừng phạt bằng án tử hình hoặc tù chung thân kèm hoặc không kèm cưỡng bức lao động hoặc án tù với khung hình phạt cao nhất từ 3 năm hoặc trên 3 năm nếu hành vi này đã được thực hiện ở Nhật Bản; Khi hành vi phạm tội được thực hiện tại Nhật Bản hoặc một tòa án của Nhật Bản đã tiến hành xét xử hành vi này; Khi cá nhân bị yêu cầu dẫn độ là công dân Nhật Bản...*

Nguyên tắc lãnh thổ là nguyên tắc hàng đầu trong các vấn đề liên quan đến việc phân định thẩm quyền tài phán. Điều 1 của Bộ luật Hình sự quy định rằng bộ luật này sẽ áp dụng cho bất cứ cá nhân nào phạm tội trong lãnh thổ Nhật Bản, và điều khoản này cũng sẽ áp dụng cho một người phạm tội trên tàu thuyền hoặc máy bay của Nhật Bản khi họ đang ở bên ngoài lãnh thổ của Nhật Bản. Tuy nhiên, với các hành vi phạm tội công nghệ cao xảy ra ngoài phạm vi lãnh thổ Nhật Bản cũng có thể bị áp dụng quy định pháp luật này; cụ thể, Điều 4-2 của Bộ luật Hình sự quy định rằng Bộ luật này cũng sẽ áp dụng đối với những người đã vi phạm, vượt quá giới hạn lãnh thổ của Nhật Bản, ngay cả khi những tội phạm ngay được thực hiện bên ngoài lãnh thổ Nhật Bản.

3.6.4. Một số bài học kinh nghiệm đối với Việt Nam

Bên cạnh việc đều là thành viên của Công ước Budapest, Cộng hòa Liên bang Đức, Nhật Bản, Hoa Kỳ cũng là những quốc gia có hệ thống pháp luật tiên tiến và toàn diện trong hợp tác quốc tế phòng chống tội phạm công nghệ cao cũng như vấn đề đảm bảo an toàn an ninh mạng. Qua một số khía cạnh pháp lý và thực tiễn thực hiện pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao của ở các quốc gia này, có thể đưa ra một số nhận định:

Thứ nhất, các quốc gia trên đều nhận thức rõ được tính chất, mức độ nguy hiểm của tội phạm công nghệ cao đối với trật tự an toàn xã hội, an ninh quốc gia và đặc biệt là vấn đề hợp tác quốc tế trong việc ngăn ngừa, triệt phá và loại bỏ loại hình tội phạm này. Chính vì vậy, các quốc gia đềuđã ban hành nhiều đạo luật, các văn bản có liên quan điều chỉnh về tội phạm công nghệ cao căn cứ trên những cơ sở pháp lý là các công ước quốc tế mà những quốc gia này đã tham gia là thành viên. Đồng thời, do đều là thành viên của Công ước Budapest, Công ước Palermo và một số công ước khác có liên quan đến tội phạm công nghệ cao nên các quốc gia đều đang có xu hướng tiến hành thay đổi, sửa đổi, bổ sung các quy định của pháp luật trong nước để tăng tính phù hợp, tương thích với các quy phạm của Công ước khi thực hiện nghĩa vụ thành viên của mình. Pháp luật Nhật Bản đã bước đầu phản ánh được những vấn đề của xã hội hiện đại và bắt kịp với các tiêu chuẩn, quy định quốc tế về bảo vệ dữ liệu cá nhân, thông tin cá nhân; trong khi đó, Mỹ chú trọng phòng ngừa, phát hiện nguy cơ đe dọa an ninh mạng từ sớm để ngăn chặn triệt để những tiềm ẩn nguy hại đến an ninh quốc gia; còn Đức lại có yêu cầu sát sao đối với người sử dụng, qua đó hạn chế tính ẩn danh của không gian mạng, nhằm dễ dàng quản lý và truy soát tốt hơn... Bên cạnh đó, các quốc gia đã thiết lập các cơ quan đầu mối ở cấp trung ương mang tính chỉ đạo-tham mưu trong việc tiến hành xây dựng các quy

tắc, tiêu chuẩn, quy chuẩn về an ninh mạng. Tội phạm công nghệ cao ở các quốc gia này đều được cấu thành từ một tập hợp của nhiều đạo luật khác nhau, hầu như không có một luật lệ duy nhất nào có thể điều chỉnh được tất cả mọi thứ trong lĩnh vực này.

Thứ hai, nhận thức được mức độ nguy hiểm của tội phạm công nghệ cao, cả ba quốc gia đều xác định rõ trọng tâm và dành những sự quan tâm đặc biệt đến các nội dung hợp tác quốc tế trong đấu tranh, phòng chống tội phạm công nghệ cao như việc đáp ứng nghĩa vụ thành viên trong hài hòa hóa và hoàn thiện pháp luật,vấn đề tương trợ tư pháp hình sự, dẫn độ tội phạm và chuyển giao người bị kết án. Đa phần các quốc gia đều quy định những nội dung này trong từng văn bản pháp luật chuyên ngành cụ thể như Luật Dẫn độ của Nhật Bản; Luật Hỗ trợ Quốc tế trong Điều tra và các vấn đề liên quan khác của Nhật Bản;Luật hỗ trợ pháp lý quốc tế trong các vấn đề hình sự của Đức; Hiến pháp Hoa Kỳ và một loạt văn bản cụ thể hóa khác đi kèm theo... Về nguyên tắc chung, các quốc gia trên đều tiến hành các hoạt động tương trợ tư pháp trên cơ sở quy định của một công ước/hiệp định hoặc trên cơ sở không có điều ước; và thực hiện trên cơ sở các nguyên tắc được ghi nhận tại các công ước quốc tế và thực tiễn thực hiện trên thế giới trong đó đặc biệt lưu tâm nguyên tắc "định danh kép", nguyên tắc "có đi có lại" hay không dẫn độ công dân nước mình; không dẫn độ tội phạm chính trị. Trên cơ sở đó, các vấn đề cơ bản về thẩm quyền, trình tự, thủ tục thực hiện hoạt động tương trợ tư pháp, dẫn độ tội phạm hay chuyển giao người bị kết án được quy định rõ ràng, cụ thể tại luật pháp trong nước, bao gồm cả các quy định liên quan đến việc xây dựng các yêu cầu tương trợ tư pháp, dẫn độ hay chuyển giao người bị kết án từ Hoa Kỳ, Nhật Bản, Đức và các quy định về việc các quốc gia khác gửi yêu cầu tới Hoa Kỳ, Nhật Bản, Đức.

Thứ ba, nguyên tắc "lãnh thổ" hay "nơi thực hiện hành vi phạm tội" là những nguyên tắc xác định thẩm quyền tài phán phổ biến của các quốc gia đối với tội phạm công nghệ cao. Từ phương diện hiệu lực theo lãnh thổ thì các hành vi tố tụng hình sự của cơ quan nhà nước có thẩm quyền chỉ có thể được thực hiện trong phạm vi giới hạn lãnh thổ của quốc gia. Tuy nhiên, trong nhiều trường hợp, hoạt động xét xử các vụ việc hình sự chỉ có thể được tiến hành bình thường và đạt được kết quả nếu có sự thực hiện các hành vi tố tụng hình sự trên lãnh thổ của nước khác. Bởi tội phạm công nghệ cao dù thực hiện ngoài lãnh thổ quốc gia nhưng lại vẫn có thể gây ảnh hưởng đến hệ thống CNTT, an toàn an ninh mạng, xâm phạm đến quyền lợi chính đáng của cá nhân, tổ chức cũng như các quốc gia khác. Chính vì vậy, các quốc gia đều đã có những quy định cụ thể trong pháp luật của mình nhằm xác định

thẩm quyền tài phán đối với những hành vi phạm tội công nghệ cao xảy ra ngoài phạm vi lãnh thổ quốc gia, có thể bị áp dụng quy định pháp luật về nội dung và trình tự thủ tục xét xử của quốc gia.

Từ những nhận định, pháp luật của Việt Nam hoàn toàn có thể đúc rút ra một số kinh nghiệm giá trị mang cả tính tham khảo cũng như tính ứng dụng trong quá trình hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao như sau:

Thứ nhất, việc xây dựng, ban hành các quy định của pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao và vấn đề an ninh mạng của nước ta trong giai đoạn hiện nay là điều vô cùng cấp bách và khẩn thiết. Để thực hiện được vấn đề này, quá trình xây dựng pháp luật cần bám sát các tiêu chuẩn quốc tế trong các văn kiện pháp lý quốc tế hiện hành để tạo ra sự phù hợp, tương thích với các quy chuẩn quốc tế và bảo đảm các điều kiện khi hợp tác, hội nhập quốc tế về an ninh mạng. Việt Nam nên cân nhắc vấn đềtham gia và nội luật hóa một số quy định của Công ước Budapest. Đây là việc làm có thể giúp cho việc đồng bộ hóa hệ thống pháp luật hiện hành với các quy chuẩn quốc tế đã được thiết lập trong Công ước từ nghĩa vụ hình sự hóa các hành vi phạm tội trong lĩnh vực an ninh mạng đến cách thức tổ chức bộ máy, vận hành, hoạt động công vụ, biện pháp hợp tác quốc tế, trình tự thủ tục bắt giữ, xử lý tội phạm cũng nhưtạo ra mối liên kết giữa các luật liên quan như Bộ luật hình sự 2015, Luật an toàn thông tin mạng 2015, Luật Công nghệ thông tin 2006, Luật Giao dịch điện tử năm 2006….

Thứ hai, mặc dù hiện nay Việt Nam đã có Luật An ninh mạng năm 2018 với những quy định cụ thể nhằm bảo vệ hệ thống thông tin quan trọng của quốc gia và trên không gian mạng. Tuy nhiên, những quy định của Luật An ninh mạng đôi khi vẫn đưa đến những cách hiểu không thống nhất do vẫn chưa hề có bất kỳ một nghị định hay thông tư hướng dẫn thi hành cho luật này. Chính vì vậy, Việt Nam cần sớm hoàn chỉnh khung pháp lý cần thiết liên quan đến các hoạt động trên không gian mạng, trong đó đặc biệt lưu tâm tới vấn đề ban hành các văn bản hướng dẫn liên quan trong vấn đề này.

Thứ ba, liên quan đến các hoạt động tương trợ tư pháp hình sự, thực tiễn cho thấy, quá trình giải quyết các vụ án, vụ việc hình sự trong nước phát sinh ngày càng nhiều yêu cầu hợp tác với nước ngoài trong việc thực hiện hỗ trợ tư pháp về hình sự. Quá trình tương trợ tư pháp hình sự thường mất nhiều thời gian trong khi việc giải quyết các vụ án, vụ việc hình sự phải tuân thủ thời hạn, trình tự thủ tục luật định. Việc chậm có kết quả tương trợ, kết quả tương trợ chưa đáp ứng kịp thời yêu cầu hoặc thậm chí không có kết quả tương trợ đã làm ảnh hưởng đến chất lượng,

tiến độ giải quyết các vụ án, vụ việc hình sự. Trong khi đó, hiện nay, tình hình tội phạm công nghệ cao ngày càng diễn ra với một tốc độ nhanh hơn, mức độ phức tạp tinh vi hơn. Chính vì vậy, cần tăng tính phản hồi nhanh chóng của các văn bản pháp luật riêng biệt để điều chỉnh kịp thời và có hiệu quả khi tiến hành các hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao ở Việt Nam hiện nay.

Thứ tư, chủ động thực hiện phòng, chống tội phạm công nghệ cao ngay từ trong an ninh nội địa và tăng cường chất lượng của các hoạt động hợp tác quốc tế phòng, chống tội phạm công nghệ cao. Đội ngũ cán bộ có năng lực chuyên môn, trình độ ngoại ngữ, có kinh nghiệm, được đào tạo kiến thức, kỹ năng công nghệ chuyên sâu, am hiểu luật pháp trong nước và quốc tế là yếu tố quan trọng để nâng cao chất lượng hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao trên thực tế. Bên cạnh đó, cần có các đề án chuyên biệt để đào tạo, bồi dưỡng, tập huấn về pháp luật quốc tế, về kỹ thuật nghiệp vụ chuyên sâu để cập nhật và đáp ứng sự thay đổi liên tục trong phương thức, thủ đoạn cũng như các công cụ, phương tiện ngày một hiện đại của tội phạm công nghệ cao.

TIỂU KẾT CHƯƠNG 3

* * *

Nhằm tạo ra các khuôn khổ chung trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao, một số văn kiện pháp lý đã được xây dựng ở các cấp độ khác nhau, từ toàn cầu, khu vực cho tới song phương điều chỉnh những vấn đề liên quan đến tội phạm công nghệ cao. Căn cứ vào những văn kiện hiện có, pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao hiện nay quy định một số nội dung đối với các quốc gia hữu quan bao gồm: Thứ nhất, pháp luật quốc tế quy định nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luật cũng như xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao; Thứ hai, tương trợ tư pháp hình sự; Thứ ba, dẫn độ; Thứ tư, chuyển giao người bị kết án và thứ năm, phân định thẩm quyền tài phán. Việc thực hiện những nội dung hợp tác này hoàn toàn có thể sử dụng bổ trợ các điều ước quốc tế đa phương hoặc song phương có liên quan, trong đó đặc biệt là Công ước Budapest năm 2001 và Công ước Palermo năm 2000.

Cùng với đó, chương 3 của luận án cũng đã đánh giá thực tiễn thực hiện pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao của một số quốc gia. Bên cạnh sự cân nhắc lựa chọn các quốc gia tiêu biểu theo từng khu vực địa lý, việc lựa chọn cả ba quốc gia đều là thành viên của Công ước Budapest góp phần nhìn nhận rõ nét và thực tế hơn việc thực hiện các quy định của pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao. Từ đó, luận án cũng rút ra được những bài học kinh nghiệm đối với Việt Nam trong tình hình mới như sau:

Thứ nhất, xây dựng, ban hành các quy định của pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao và vấn đề an ninh mạng của nước ta trong giai đoạn hiện nay. Để thực hiện được vấn đề này, quá trình xây dựng pháp luật cần bám sát các tiêu chuẩn quốc tế trong các văn kiện pháp lý quốc tế hiện hành để tạo ra sự phù hợp, tương thích với các quy chuẩn quốc tế và bảo đảm các điều kiện khi hợp tác, hội nhập quốc tế về an ninh mạng. Việt Nam nên cân nhắc vấn đềtham gia và nội luật hóa một số quy định của Công ước Budapest.

Thứ hai, Việt Nam cần sớm hoàn chỉnh khung pháp lý cần thiết liên quan đến các hoạt động trên không gian mạng, trong đó đặc biệt lưu tâm tới vấn đề ban hành các văn bản hướng dẫn liên quan trong vấn đề này.

Thứ ba, cần tăng tính phản hồi nhanh chóng của các văn bản pháp luật riêng biệt để điều chỉnh kịp thời và có hiệu quả khi tiến hành các hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao ở Việt Nam hiện nay.

Thứ tư, chủ động thực hiện phòng, chống tội phạm công nghệ cao ngay từ trong an ninh nội địa và tăng cường chất lượng của các hoạt động hợp tác quốc tế phòng, chống tội phạm công nghệ cao.

CHƯƠNG 4
PHÁP LUẬT VÀ THỰC TIỄN HỢP TÁC QUỐC TẾ ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO CỦA VIỆT NAM

* * *

4.1. Thực trạng pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao ở Việt Nam

4.1.1. Khái quát về tội phạm công nghệ cao ở Việt Nam

4.1.1.1. Tình hình tội phạm công nghệ cao ở Việt Nam

Tính đến hết năm 2018, Việt Nam đã có hơn 58 triệu người dùng Internet nói chung (chiếm 70% dân số), tỷ lệ hộ gia đình có kết nối Internet tại Việt Nam chiếm 47% và hơn 36 triệu người sử dụng Internet trên các thiết bị di dộng, cao hơn mức trung bình của thế giới, nằm trong số những quốc gia và vùng lãnh thổ có số lượng người dùng Internet cao nhất châu Á[108]. Việt Nam hiện đang có 115 triệu thuê bao điện thoại di động, 15 triệu thuê bao điện thoại cố định[109]. Sự phát triển của CNTT, viễn thông trong những năm gần đây bên cạnh những thành tựu đạt được thì cũng tạo ra những nguy cơ khi CNTT trở thành một lĩnh vực trọng điểm mà các đối tượng tập trung khai thác, lợi dụng để thực hiện tội phạm.

Các hành vi do tội phạm công nghệ cao thực hiện trên thế giới hiện nay diễn biến rất phức tạp. Vì đặc thù của loại tội phạm này là tính quốc tế và hội nhập nhanh, do đó, điều này đã tác động mạnh đến tình hình tội phạm công nghệ cao thực hiện tại Việt Nam. Tội phạm công nghệ cao ở các nước xâm nhập vào Việt Nam rất nhanh, thậm chí nhiều đối tượng người nước ngoài nhập cảnh vào Việt Nam để tổ chức hoạt động tội phạm. Việt Nam đã được dự báo có thể là một trong những khu vực nóng về tội phạm công nghệ cao. Số liệu của hãng bảo mật Symantec cho thấy, Việt Nam hiện đang đứng thứ 11 trên toàn cầu về các hoạt động đe dọa tấn công mạng (năm 2018)[110]. Những hoạt động đe dọa nhắm vào cơ quan, doanh nghiệp, tổ chức tại Việt Nam bao gồm, tấn công có chủ đích, các mối đe dọa trên thiết bị di động, phát tán mã độc, virus và đánh cắp dữ liệu. Các tội phạm công

---

[108] Bộ Thông tin và Truyền thông (2019), Sách trắng Công nghệ thông tin và truyền thông VIệt Nam năm 2019, chttps://mic.gov.vn/Upload_Moi/FileBaoCao/Sach-Trang2019-Final.pdf (truy cập lần cuối ngày 19/6/2020).

[109]Bộ Thông tin và Truyền thông (2019), Sách trắng Công nghệ thông tin và truyền thông VIệt Nam năm 2019, chttps://mic.gov.vn/Upload_Moi/FileBaoCao/Sach-Trang2019-Final.pdf (truy cập lần cuối ngày 19/6/2020).

[110] Xem https://www.cybercrimejournal.com/LuongetalVol13Issue2IJCC2019.pdf (truy cập lần cuối 20/12/2020)

nghệ cao thường tập trung tại một số tỉnh, thành phố lớn, nơi có sự giao lưu hội tụ của nhiều lĩnh vực khoa học công nghệ, tài chính ngân hàng hoặc nơi có nhiều người nước ngoài sinh sống...

Số lượng vụ án về tội phạm công nghệ cao được phát hiện và xử lý có tỷ lệ không nhiều so với các loại hình tội phạm khác nhưng lại có sự gia tăng rất nhanh về số lượng. Trong giai đoạn năm 2010-2014, tổng số vụ và bị cáo tội phạm công nghệ cao là 156 vụ với 612 bị cáo, với tổng số tiền các bị cáo chiếm đoạt hơn 859 tỷ đồng. Năm 2019, lực lượng Công an phát hiện 287 vụ, 437 đối tượng phạm tội, vi phạm pháp luật trong lĩnh vực viễn thông, tin học (nhiều hơn 3,24% so với cùng kỳ năm 2018), trong đó, đã khởi tố 127 vụ, 258 bị can (tăng 4,96% số vụ và giảm 5,84% bị can so với cùng kỳ năm 2018)[111], đặc biệt Việt Nam đã triệt phá nhiều đường dây tội phạm cờ bạc, cá độ bóng đá qua mạng Internet; tội phạm người nước ngoài sử dụng công nghệ cao tại Việt Nam. Trung bình mỗi năm ở Việt Nam xảy ra 31 vụ án với 122 bị cáo là tội phạm công nghệ cao, mỗi vụ án có khoảng 4 bị cáo tham gia và số tiền bị tội phạm công nghệ cao chiếm đoạt mỗi năm là 172 tỷ đồng[112]. Tội phạm công nghệ cao thường xuyên thay đổi phương thức, thủ đoạn phạm tội nên gây khó khăn cho việc điều tra, phát hiện tội phạm, do đó những vụ việc chưa bị tố giác của tội phạm này là rất lớn, mức độ nguy hiểm và hậu quả của tội phạm gây ra chưa thể thống kê, đánh giá được một cách thực sự chính xác.

Phương thức thực hiện của tội phạm công nghệ cao thường là đồng phạm và có tổ chức chặt chẽ. Trong giai đoạn 2010 đến 2014, tội phạm công nghệ cao được thực hiện dưới hình thức đồng phạm chiếm 48,18%, phạm tội có tổ chức chiếm 44,87%, đây là tỷ lệ rất cao so với các loại tội phạm thông thường[113]. Tội phạm công nghệ cao thường sử dụng các thủ đoạn sau: tạo, phát tán vi rút tin học, phần mềm tin học độc hại; sử dụng thẻ ATM giả thanh toán dịch vụ, mua hàng hóa; mua thông tin thẻ tín dụng bị hacker chiếm đoạt rao bán trên các trang web, để sử dụng đặt mua hàng trực tuyến chuyển về Việt Nam tiêu thụ (ship hàng); truy cập trái phép mạng viễn thông để nối ghép lập trạm thu phát tín hiệu trái phép, nhằm ăn cắp

[111] Bộ Công An: Phát hiện 287 vụ vi phạm pháp luật về CNTT và viễn thông; https://ictnews.vietnamnet.vn/cuoc-song-so/bo-cong-an-phat-hien-287-vu-vi-pham-phap-luat-ve-cntt-va-vien-thong-36195.html (truy cập lần cuối ngày 20/12/2020)

[112] Báo cáo về tình hình tội phạm sử dụng công nghệ cao diễn ra tại địa phương giai đoạn 2005 đến 2014, của 63 Viện kiểm sát nhân dân tỉnh, thành phố, theo Công văn số 2176/VKSTC-V1 ngày 11/7/2014 của Viện Kiểm sát nhân dân tối cao

[113] Báo cáo về tình hình tội phạm sử dụng công nghệ cao diễn ra tại địa phương giai đoạn 2005 đến 2014, của 63 Viện kiểm sát nhân dân tỉnh, thành phố, theo Công văn số 2176/VKSTC-V1 ngày 11/7/2014 của Viện Kiểm sát nhân dân tối cao

cước phí viễn thông; tấn công email của cá nhân, doanh nghiệp, sử dụng thông tin của nạn nhân để chiếm đoạt tài sản; lập trang web mua bán trực tuyến để chiếm đoạt tài sản; lập trang web để lừa đảo bán các gian hàng ảo này dưới hình thức bán hàng đa cấp; sử dụng tài khoản chat của người khác để lừa đảo lấy tiền; làm quen qua chat rồi lừa đảo chiếm đoạt tài sản, cưỡng đoạt tài sản; lợi dụng chat để thực hiện các hành vi cưỡng đoạt tài sản, mại dâm, mua bán người; đưa thông tin lên mạng Internet để truyền bá văn hóa phẩm đồi trụy; mua bán mại dâm; mua bán chất ma túy; mua bán phụ nữ, trẻ em; đánh bạc; tổ chức đánh bạc; tài trợ cho khủng bố, rửa tiền; sử dụng mạng máy tính, mạng Internet tuyên truyền tư tưởng chống phá Nhà nước, chính quyền nhân dân; sử dụng mạng máy tính, mạng viễn thông, mạng Internet đưa thông tin lên mạng để thực hiện các hoạt động tống tiền; xâm phạm nhân phẩm, tự do cá nhân khác.

Về độ tuổi thực hiện hành vi phạm tội, tội phạm công nghệ cao tập trung chủ yếu ở độ tuổi từ 18 đến 30 (chiếm 54,23%). So sánh với số liệu thống kê của Liên hiệp quốc thì tội phạm công nghệ cao trên thế giới tập trung chủ yếu ở độ tuổi dưới 25 chiếm 45% tổng số loại tội phạm này[114]; nhưng ở Việt Nam chiếm 55,27% tuổi từ 25 đến 35. Như vậy, so với thế giới, tuổi tội phạm công nghệ cao của Việt Nam cao hơn với mặt bằng chung của thế giới từ 5 đến 10 tuổi.

Về giới tính và trình độ học vấn: tội phạm công nghệ cao chủ yếu là nam giới (chiếm 95,51%; nữ giới chỉ có 4,49%) trong nhiều vụ án không có nữ giới tham gia. Điều này có thể giải thích do đặc thù của loại hình tội phạm này cần sử dụng thành thạo công nghệ thông tin nên nữ giới thường là nạn nhân chứ không phải là người thực hiện. Về trình trình độ học vấn, không phải tội phạm công nghệ cao đều có trình độ học vấn cao (73,92% bị cáo trình độ văn hóa phổ thông trung học; tuy nhiên, chỉ có 11,57% bị cáo tốt nghiệp đại học và có tới 4,09% bị cáo có văn hóa là tiểu học). Tội phạm công nghệ cao chủ yếu là các đối tượng thất nghiệp, nghề nghiệp không ổn định, các đối tượng này chiếm 41,79% và mỗi năm trung bình tăng khoảng 50%[115].

Về địa bàn thực hiện hành vi phạm tội của tội phạm công nghệ cao trong những năm qua chủ yếu tại hai thành phố trực thuộc trung ương là Hà Nội và TP.

---

[114] Báo cáo về tình hình tội phạm sử dụng công nghệ cao diễn ra tại địa phương giai đoạn 2005 đến 2014, của 63 Viện kiểm sát nhân dân tỉnh, thành phố, theo Công văn số 2176/VKSTC-V1 ngày 11/7/2014 của Viện Kiểm sát nhân dân tối cao

[115] Báo cáo về tình hình tội phạm sử dụng công nghệ cao diễn ra tại địa phương giai đoạn 2005 đến 2014, của 63 Viện kiểm sát nhân dân tỉnh, thành phố, theo Công văn số 2176/VKSTC-V1 ngày 11/7/2014 của Viện Kiểm sát nhân dân tối cao

Hồ Chí Minh (chiếm 64,05%), còn lại là ở các thành phố lớn (22,39%), nông thôn (7,35%), huyện lỵ (4,09%), thị xã (2,12%).

Đặc điểm bị hại của tội phạm công nghệ cao chủ yếu bị hại là cá nhân (chiếm 97,28%); doanh nghiệp chỉ chiếm 2,72%[116].

Về quốc tịch của bị cáo, 95,85% bị cáo tội phạm công nghệ cao có quốc tịch Việt Nam, bị cáo có quốc tịch nước ngoài chiếm 4,15%, gồm: Trung Quốc, Malaysia, Hàn Quốc, Nigeria, Rumania, Pakistan. Từ năm 2010 đến năm 2017, tội phạm sử dụng công nghệ cao trong lĩnh vực CNTT gia tăng, diễn biến rất phức tạp, các loại tội phạm truyền thống có xu hướng cấu kết với tội phạm công nghệ cao để thực hiện hành vi phạm tội gây thiệt hại nghiêm trọng hơn. Nổi lên trong thời gian gần đây là một số loại tội phạm như: Người nước ngoài (chủ yếu là người Trung Quốc, Đài Loan - Trung Quốc) cấu kết với các đối tượng trong nước thiết lập tổng đài gọi điện trên nền tảng Internet (VoIP) thực hiện các cuộc gọi giả mạo các cơ quan thực thi pháp luật như Công an, Viện Kiểm sát, Tòa án để đe dọa người bị hại có liên quan đến các vụ án đặc biệt quan trọng như lừa đảo, rửa tiền, buôn bán ma túy…Qua đó, các đối tượng yêu cầu người bị hại chuyển tiền đến các tài khoản ngân hàng do các đối tượng chỉ định với lý do để kiểm tra có liên quan đến các hành vi phạm tội. Ngay sau khi bị hại chuyển tiền các đối tượng tổ chức việc rút tiền và chiếm đoạt tài sản trong thời gian ngắn.

Các đối tượng bằng thủ đoạn tạo ra các website có giao diện gần giống giao diện các website của các ngân hàng hoặc của các mạng xã hội lừa người dùng đăng nhập để thu thập trái phép thông tin đăng nhập của người dùng (Phishing). Chúng sử dụng quyền đăng nhập vào tài khoản để nhắn tin lừa bạn bè, người thân trong danh bạ của chủ tài khoản để nhờ chuyển tiền, mua thẻ cào điện thoại, thẻ game…qua đó chiếm đoạt tài sản. Theo số liệu khảo sát của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, từ năm 2015 đến tháng 4/2017 phát hiện 136 vụ lừa đảo chiếm đoạt tài sản qua mạng Internet do các đối tượng trú tại Quảng Nam, Quảng Trị, Hà Tĩnh thực hiện, trong đó khởi tố 52 vụ/103 bị can gây thiệt hại về tài sản hàng chục tỷ đồng. Nguy hiểm hơn, trong thời gần đây đã phát hiện nhiều phương thức, thủ đoạn phạm tội mới ngày càng tinh vi, xảo quyệt và liên tục có sự thay đổi nhằm che giấu, lẩn tránh sự phát hiện của cơ quan Công an.

---

[116] Báo cáo về tình hình tội phạm sử dụng công nghệ cao diễn ra tại địa phương giai đoạn 2005 đến 2014, của 63 Viện kiểm sát nhân dân tỉnh, thành phố, theo Công văn số 2176/VKSTC-V1 ngày 11/7/2014 của Viện Kiểm sát nhân dân tối cao

Trong lĩnh vực thẻ ngân hàng, tình trạng đối tượng là người Trung Quốc và một số nước châu Phi nhập cảnh vào Việt Nam, làm giả thẻ và móc nối với một số cơ quan, tổ chức chấp nhận thanh toán thẻ (POS), tiến hành giao dịch khống để rút tiền mặt, hoặc mua hàng hóa tại các cửa hàng, siêu thị, gây thiệt hại hàng triệu USD; nhiều đối tượng còn lắp đặt thiết bị tại các ATM hoặc máy POS để ăn cắp thông tin thẻ ngân hàng. Trong lĩnh vực viễn thông, nhiều đối tượng là người Trung Quốc vào Việt Nam lắp đặt thiết bị kỹ thuật, giả mạo cơ quan thực thi pháp luật của nước ngoài để lừa đảo, chiếm đoạt tiền của công dân Trung Quốc kinh doanh tại Việt Nam. Bên cạnh đó, các đối tượng là người Trung Quốc nhập cảnh Việt Nam, lắp đặt thiết bị phát sóng không dây (wifi) xuyên biên giới tại các tỉnh biên giới của Việt Nam như: Quảng Ninh, Tây Ninh tạo thành hệ thống tổ chức đánh bạc qua mạng cho công dân Trung Quốc nhằm trốn tránh sự phát hiện của cơ quan chức năng Trung Quốc.

4.1.1.2. Dự báo về tình hình tội phạm công nghệ cao tại Việt Nam và xu hướng hợp tác quốc tế trong đấu tranh, phòng chống tội phạm công nghệ cao tại Việt Nam

Tội phạm sử dụng công nghệ cao ở Việt Nam trong những năm tới được dự báo sẽ diễn ra phức tạp với nhiều phương thức, thủ đoạn phạm tội mới, hoạt động có tính chất xuyên quốc gia và xảy ra trên nhiều lĩnh vực, trong đó, các lĩnh vực được tội phạm công nghệ cao tập trung thực hiện các hành vi phạm tội như:

- Phát tán virus, đăng tải thông tin xuyên tạc, sai sự thật nhằm bôi nhọ danh dự, uy tín của lãnh đạo Đảng, Nhà nước trên các diễn đàn, trang mạng xã hội tiếp tục diễn ra phức tạp hơn, nhằm tác động xấu đến an ninh trật tự và dư luận xã hội; xuất hiện những chủng loại virus mới rất khó kiểm soát và ngăn chặn.

- Tấn công vào website, cơ sở dữ liệu, hạ tầng thông tin của các cơ quan chính phủ, ngân hàng và các doanh nghiệp lớn để lấy cắp và phá hoại dữ liệu, đặc biệt là dữ liệu liên quan đến an ninh quốc gia, quốc phòng.

- Tình trạng lừa đảo, chiếm đoạt tài sản qua mạng Internet dưới hình thức kinh doanh đa cấp gây thiệt hại lớn về tài sản sẽ diễn ra ngày càng nhiều, sẽ tăng số lượng người bị hại lên đến hàng chục nghìn người, trên nhiều địa bàn khác nhau. Những vụ như MB24 có đến 50 chi nhánh ở 32 tỉnh, thành phố với số tiền đưa vào hệ thống lên đến 700 tỷ, trong tương lai có thể được các đối tượng phạm tội lợi dụng với các thủ đoạn tương tự nhằm chiếm đoạt tài sản. Trong tương lai, khi tiền ảo phát triển mạnh tại Việt Nam thì việc đổi tiền thật lấy tiền ảo trên các website… với mạng lưới đầu tư đa cấp sẽ lan rộng. Việc lôi kéo người đầu tư trên các trang

website, hưởng lãi suất theo điểm tích lũy, thì dù bị cáo có hay không biết website trên là thật hay giả cũng đủ cấu thành tội lừa đảo.

Diễn biến của tình hình tội phạm do tội phạm công nghệ cao thực hiện tại Việt Nam sẽ ngày càng phức tạp cả về số vụ, số đối tượng phạm tội; số vụ án tội phạm công nghệ cao sẽ tăng liên tục hàng năm (trên 50% mỗi năm). Về cơ cấu tình hình tội phạm theo đơn vị hành chính, tội phạm công nghệ cao không chỉ xuất hiện, tập trung tại các thành phố lớn như thành phố Hồ Chí Minh, Hà Nội mà sẽ còn rộng ra nhiều tỉnh, thành phố khác (giai đoạn 2010-2014 chỉ xuất hiện ở 26 tỉnh, thành phố), mở rộng trên quy mô cả nước; cũng không chỉ tập trung ở các đô thị mà phát triển về các vùng thôn quê.

Tình trạng người nước ngoài sử dụng thẻ tín dụng giả để chiếm đoạt tài sản sẽ có xu hướng mở rộng cả về số vụ và diện đối tượng (không chỉ tập trung tại các quốc gia gần với Việt Nam như Trung Quốc hay Malaysia mà sẽ mở rộng ra các nước phương Tây như Anh, Pháp, Tây Ban Nha...) và việc gây thiệt hại về tài sản sẽ lớn hơn so với các vụ việc được phát hiện trong những năm qua. Những vướng mắc trong việc lần theo thông tin trên các thẻ ATM giả, khi các đối tượng xâm nhập vào website bán hàng trực tuyến ở nước ngoài lấy thông tin thẻ tín dụng của khách rồi in vào thẻ ATM giả sau đó rút tiền từ các ATM. Cơ quan điều tra khó xác định được cá nhân, tập thể nào là nạn nhân của vụ án. Mọi rủi ro tài chính từ các giao dịch này sẽ chuyển về cho các ngân hàng phát hành thẻ ở nước ngoài.

Hiện tượng cá độ bóng đá xuyên quốc gia qua mạng Internet sẽ gia tăng, các đối tượng lợi dụng đường truyền Internet tốc độ cao truyền hình trực tuyến từ các sòng bạc về Việt Nam để tổ chức đánh bạc. Bởi hoạt động này sẽ làm khó cho lực lượng điều tra của Việt Nam phát hiện hành vi vi phạm cho đến xử lý do thiếu hướng dẫn cụ thể. Các cán bộ tố tụng cho rằng, không dễ phát hiện đường dây đánh bạc trên mạng, khi phát hiện thì việc triệt phá tận gốc cũng rất khó bởi hình thức đánh bạc này tổ chức theo hình kim tự tháp. Sự phân cấp này giúp người vi phạm có khả năng trốn tránh sự phát hiện của cơ quan pháp luật. Nếu có bị phát hiện, thông thường chỉ có những mắt xích nhỏ sa lưới, còn người tổ chức mạng cá độ thì khó mà lần ra.[117]

Về cơ cấu theo phương thức, thủ đoạn phạm tội: số vụ án do TPCNC thực hiện dưới hình thức đồng phạm và đồng phạm có tổ chức sẽ gia tăng trong thời gian tới. Hầu hết các vụ án TPCNC thực hiện dưới hình thức đồng phạm, phạm tội có tổ

[117] Trần Đoàn Hạnh (2016), *Những vướng mắc trong đấu tranh, xử lý vi phạm pháp luật về tội phạm công nghệ cao*, Tạp chí nghiên cứu lập pháp.

chức; xu thế hình thành ổ nhóm TPCNC hoạt động mang tính quốc tế, có sự phân công vai trò cụ thể, chặt chẽ sẽ ngày càng phổ biến. Theo INTERPOL, xu hướng mới trong TPCNC đang nhập lại làm một và gây tốn kém cho nền kinh tế toàn cầu nhiều tỷ đô la. Nếu như trước đây, tội phạm sử dụng công nghệ cao chủ yếu là do các cá nhân hoặc nhóm nhỏ thì ngày nay các tổ chức tội phạm đã hình thành các mạng lưới tội phạm ảo liên kết các cá nhân từ khắp nơi trên thế giới trong thời gian thực để phạm tội trên một quy mô lớn. Bên cạnh đó, các tổ chức tội phạm đang chuyển sang Internet để tạo thuận lợi cho hoạt động.

Nếu vấn đề an ninh mạng không được giải quyết kịp thời, lĩnh vực thương mại điện tử của Việt Nam sẽ rơi vào tình trạng trì truệ, trở thành một rào cản đối với phát triển kinh tế, xã hội. Hiện nay đã xuất hiện một số mạng máy tính ma (botnet) do các hacker Việt Nam phát triển và mở rộng đã gây tác hại lớn đối với an ninh mạng nói chung và thương mại điện tử nói riêng. Ngoài ra, xu hướng gửi thư rác quy mô lớn, lừa đảo qua phishing, cài keylogger, lấy cắp thông tin, rửa tiền bằng tiền ảo… đang ngày càng phát triển. Việt Nam đã từng được xếp vào 1 trong 10 nước có lượng spam email lớn nhất thế giới, vào trong số các spam email được gửi đi từ Việt Nam rất ít nội dung bằng tiếng Việt. Điều này cho thấy các spam email này được gửi từ mạng botnet do nước ngoài kiểm soát.

Các quốc gia sẽ ngày càng thấy rõ hơn tính nguy hại của tội phạm sử dụng công nghệ cao, thấy rõ hơn đặc điểm mang tính toàn cầu của loại tội phạm này do vậy sẽ tăng cường hợp tác quốc tế trong lĩnh vực đấu tranh phòng chống tội phạm công nghệ cao. Đặc biệt, trong thời gian gần đây, với sự xuất hiện của loại tội phạm sử dụng công nghệ cao để rửa tiền đã gia tăng hoạt động HTQT trong lĩnh vực phòng chống rửa tiền tại Việt Nam. Trong thời gian tới, hoạt động đấu tranh với loại tội phạm công nghệ cao sẽ là nội dung hợp tác trọng tâm được đưa vào chương trình hợp tác giữa các quốc gia và nhiều tổ chức đa phương và song phương. Đáp ứng nhu cầu này, thời gian tới sẽ có thêm nhiều Hiệp định TTTP và dẫn độ được ký kết giữa Việt Nam và nhiều quốc gia trong đó có các nội dung tượng trợ tư pháp hình sự và dẫn độ trong đấu tranh phòng, chống tội phạm công nghệ cao.

4.1.2. Nội dung pháp lý cho hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao của Việt Nam

Việt Nam đã xây dựng các cơ sở pháp lý tương đối đầy đủ trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao, bao gồm các quy định do Việt Nam ban hành và các điều ước quốc tế mà Việt Nam ký kết hoặc tham gia. Các quy

định do Việt Nam ban hành trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao gồm có:

- Luật Công nghệ thông tin 2006 quy định về hoạt động ứng dụng và phát triển CNTT, các biện pháp bảo đảm ứng dụng và phát triển CNTT, quyền và nghĩa vụ của cơ quan, tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển CNTT. Tại Điều 12 quy định các hành vi bị nghiêm cấm; Điều 77 quy định xử lý VPPL về CNTT: "*Cá nhân có hành vi vi phạm pháp luật về công nghệ thông tin thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật*"

- Luật an toàn thông tin mạng 2015 quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng. Tại Điều 7 quy định 6 nhóm hành vi bị nghiêm cấm trong lĩnh vực bảo đảm an toàn thông tin mạng; Điều 8 quy định về xử lý VPPL về an toàn thông tin mạng: "*Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật*".

- Luật an ninh mạng 2018 quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan trong đó xác định hai nguyên tắc cơ bản trong bảo vệ an ninh mạng là chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng; mọi hành vi VPPL về an ninh mạng phải được xử lý kịp thời, nghiêm minh. Đây cũng là văn bản đầu tiên đưa ra định nghĩa về hoạt động "tấn công mạng". Theo đó, "*tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử*" (khoản 8 Điều 2). Thêm vào đó, tại Điều 8 quy định 6 nhóm hành vi bị nghiêm cấm; Điều 9 quy định về xử lý VPPL về an ninh mạng: *Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử*

lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật. Theo Điều 30, "Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng". Luật An ninh mạng cũng quy định cụ thể cơ chế phối hợp phòng, chống tấn công mạng của các bộ, ngành chức năng, xác định trách nhiệm cụ thể của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ trong phòng, chống tấn công mạng.

- Bộ luật hình sự 2015 quy định tội phạm sử dụng công nghệ cao không phải là một tội danh độc lập mà nó là tổng hợp của những tội phạm sử dụng tri thức về công nghệ cao để xâm phạm các quan hệ xã hội được pháp luật hình sự bảo vệ. Các tội phạm trong lĩnh vực CNTT, mạng viễn thông với 10 tội danh từ điều 285 đến điều 294 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 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); 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).

- Bộ luật Tố tụng hình sự 2003 trước đây chưa có quy định về chứng cứ điện tử, phương pháp thu thập, chuyển hóa chứng cứ[118]... Bộ luật Tố tụng hình sự 2015 quy định về dữ liệu điện tử được ghi nhận tại các Điều 87, 88, 99, 107. Ngoài ra khoản 3 Điều 223 Bộ luật Tố tụng hình sự 2015 cũng đề cập đến việc "thu thập bí mật dữ liệu điện tử" với tư cách là một biện pháp điều tra tố tụng đặc biệt. Đây là các quy định pháp lý tạo cơ sở cho hoạt động đấu tranh và xử lý với TPCNC bằng hoạt động tố tụng hình sự;

- Nghị định số 25/2014/NĐ-CP quy định về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao. Nghị định này quy định về hoạt động phòng ngừa, phát hiện, xử lý tội phạm và VPPL khác có sử dụng công nghệ cao; hợp tác quốc tế

[118] Cũng vì hạn chế này, từ khi Bộ luật Hình sự 1999 ra đời, qua một số lần sửa đổi, bổ sung hoàn thiện nhưng chỉ xử lý được rất ít, hoặc chưa xử lý được một trường hợp nào.

trong phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; trách nhiệm của cơ quan, tổ chức, doanh nghiệp và cá nhân trong phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao.

Nghị định cũng quy định 09 nội dung hợp tác quốc tế về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao, có thể chia thành ba nội dung chính bao gồm trao đổi thông tin về tội phạm, dẫn độ và tổ chức thi hành án, bồi dưỡng huấn luyện nghiệp vụ về phòng chống tội phạm công nghệ cao[119]. Đồng thời Nghị định cũng quy định trường hợp từ chối hợp tác quốc tế theo đó cơ quan được giao nhiệm vụ phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao và các cơ quan, tổ chức có liên quan của Việt Nam có quyền từ chối yêu cầu hợp tác khi các yêu cầu đó có nội dung gây phương hại đến chủ quyền, an ninh quốc gia, lợi ích của Nhà nước hoặc có nội dung không phù hợp với quy định của pháp luật Việt Nam và các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.[120]

-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, VKSNDTC, TANDTC, hướng dẫn áp dụng một số quy định của BLHS về một số tội phạm trong lĩnh vực CNTT, viễn thông.

Đặc biệt, gần đây nhất, trong Văn kiện Đại hội XIII, Đảng ta nêu rõ: "Tích cực, chủ động… giữ vững chủ quyền số quốc gia trên không gian mạng trong mọi tình huống". Đây là một nội dung lần đầu tiên được ghi trong một Văn kiện Đại hội, phản ánh sự nhận thức sâu sắc của Đảng ta về tính chất của thời đại dưới góc độ khoa học – công nghệ, bởi cuộc Cách mạng Công nghiệp lần thứ tư sẽ chuyển dịch toàn bộ thế giới từ thế giới thực sang thế giới số. Đồng thời, Đại hội XIII của Đảng xác định: "Củng cố quốc phòng, an ninh, bảo vệ vững chắc Tổ quốc Việt Nam xã hội chủ nghĩa là nhiệm vụ trọng yếu, thường xuyên của Đảng, Nhà nước, hệ thống chính trị và toàn dân, trong đó Quân đội nhân dân và Công an nhân dân là nòng cốt". Văn kiện Đại hội XIII nhấn mạnh điểm mới là: "Tiếp tục triển khai thực hiện toàn diện, đồng bộ Chiến lược bảo vệ Tổ quốc, Chiến lược quốc phòng, Chiến lược quân sự, Chiến lược bảo vệ an ninh quốc gia, Chiến lược bảo vệ biên giới quốc gia,

[119] Điều 16 Nghị định 25/2014/NĐ-CP của Chính phủ quy định về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao

[120] Điều 17 Nghị định 25/2014/NĐ-CP của Chính phủ quy định về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao

Chiến lược bảo vệ Tổ quốc trên không gian mạng, Chiến lược an ninh mạng quốc gia và các chiến lược quốc phòng, an ninh chuyên ngành khác".

Bên cạnh các quy định do Việt Nam ban hành, thực hiện chính sách đa phương hóa, đa dạng hóa và tích cực, chủ động hội nhập quốc tế, là thành viên có trách nhiệm trong cộng đồng quốc tế, tính đến tháng 9/2017, Việt nam là thành viên của 22 điều ước quốc tế đa phương về TTTP về hình sự, dẫn độ, chuyển giao người bị kết án phạt tù và 27 Hiệp định TTTP về dân dự và hình sự với các quốc gia. Trong các Hiệp định này đều có các quy định về TPCNC hoặc các tội phạm xuyên quốc gia có yếu tố công nghệ cao. Trong số 22 điều ước quốc tế đa phương, Việt Nam tuyên bố không coi 10/22 điều ước quốc tế đa phương là cơ sở pháp lý trực tiếp về dẫn độ như Công ước về trừng trị việc chiếm giữ bất hợp pháp tàu bay năm 1970, Công ước thống nhất về các chất ma túy năm 1961, Công ước của Liên hợp quốc về chống tham nhũng năm 2003, Công ước của Liên hợp quốc về chống tra tấn và các hình thức đối xử hoặc trừng phạt tàn bạo vô nhân đạo hoặc hạ nhục con người…

Hiện nay Việt Nam kí 12 Hiệp định song phương chuyên biệt về dẫn độ với các quốc gia như Hàn Quốc, Ấn Độ, Angieri, Astraylia, Indonesia, Campuchia, Hungari, Xrilanca, Tây Ban Nha, Trung Quốc, Pháp, Kazakhstan. Hiệp định thứ 13 với Cộng hòa Nam Phi được đàm phán từ năm 2012 vẫn chưa được các bên ký kết, và tính đến tháng 7/2017 thì các Hiệp định chuyên biệt về dẫn độ với Trung Quốc, Pháp và Kazakhstan vẫn chưa có hiệu lực.

- *Các điều ước quốc tế về TTTP về hình sự*

Việt Nam hiện là thành viên của 22 điều ước quốc tế đa phương và 22 điều ước quốc tế song phương có quy định về TTTP về hình sự. Trong số này có 01 điều ước quốc tế đa phương quy định về TTTP về hình sự là Hiệp định TTTP về hình sự giữa các quốc gia ASEAN năm 2004 (có hiệu lực tại Việt Nam ngày 20/9/2005). Việt Nam đã kí 11 Hiệp định về TTTP về hình sự với các quốc gia như Hàn Quốc, Ấn Độ, Vương quốc Anh và Ailen, Angieria, Indonesia, Astraylia, Tây Ban Nha, Pháp, Hungaria, Campuchia, Kazakhstan, Nam Phi. Khác với các điều ước về dẫn độ, các điều ước quốc tế đa phương có quy định về TTTP về hình sự đều được Việt Nam coi là cơ sở pháp lý trực tiếp về TTTP về hình sự, hay nói cách khác, tất cả các quốc gia thành viên của các điều ước quốc tế đa phương này, nếu chưa có hiệp định TTTP về hình sự song phương với Việt Nam, có thể gửi yêu cầu TTTP về hình sự trên cơ sở điều ước quốc tế đa phương.

- *Các điều ước quốc tế về chuyển giao người bị kết án phạt tù*

Tính đến tháng 9/2017, Việt Nam đã gia nhập 03 điều ước quốc tế đa phương là Công ước quốc tế về chống buôn bán bất hợp pháp năm 1988 (có hiệu lực tại Việt Nam ngày 4/11/1997), Công ước của Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia năm 2000 (có hiệu lực tại Việt Nam từ 8/11/2012) và Công ước của Liên hợp quốc về chống tham nhũng năm 2003 (hiệu lực tại Việt Nam ngày 18/9/2009). Các quy định về chuyển giao người đang chấp hành hình phạt tù trong các công ước này chỉ quy định mang tính nguyên tắc, có tính khuyến nghị các nước thành viên tăng cường hợp tác về chuyển giao người bị kết án phạt tù về các tội nêu trong Công ước mà không có những quy định cụ thể để có thể áp dụng trực tiếp.

Thực hiện cam kết quốc tế trong các điều ước quốc tế nêu trên và đặc biệt sau khi có Luật TTTP, Việt Nam đã kí 12 điều ước quốc tế song phương có quy định về chuyển giao người đang chấp hành hình phạt tù. Trong đó có 10 hiệp định chuyên biệt về chuyển giao người bị kết án phạt tù với các nước: Anh và Bắc Ailen, Australia, Hàn Quốc, Thái Lan, Nga, Hungari (ký năm 2014), Ấn Độ, Xrilanca, Tây Ban Nha, Campuchia và 02 hiệp định TTTP về các vấn đề dân sự, hôn nhân, gia đình và hình sự có quy định về chuyển giao người bị kết án phạt tù với Hungaria (kí năm 1985) và Ba Lan (kí năm 1993). Hiện nay, Việt Nam đang đàm phán để ký các hiệp định về chuyển giao người bị kết án phạt tù đối với các quốc gia như Séc, Malysia, Nhật Bản, Hồng Kông-Trung Quốc, Singapore, Lào, Hoa Kỳ, Trung Quốc, Philippines, Pháp, Đức…

Các quy định trong các điều ước quốc tế song phương về chuyển giao người đang chấp hành hình phạt tù mà Việt Nam ký kết với các nước đều quy định cụ thể về các vấn đề trong hoạt động chuyển giao người bị kết án và thông thường gồm các quy định về giải thích từ ngữ; các nguyên tắc chung; cơ quan trung ương; điều kiện chuyển giao; thủ tục chuyển giao; yêu cầu và trả lời yêu cầu; sự đồng ý và việc xác nhận; hiệu lực của việc chuyển giao đối với Nước nhận; tiếp tục thi hành hình phạt; xem xét lại phán quyết và đặc xá, đại xá hoặc giảm án; chấm dứt việc thi hành án; thông tin về việc thi hành hình phạt; quá cảnh; chi phí; ngôn ngữ; phạm vi áp dụng; giải quyết bất động; bàn giao người bị kết án; sửa đổi, bổ sung; điều khoản cuối cùng.

Trên đây là tổng hợp những văn bản quy phạm pháp luật và các điều ước quốc tế mà Việt Nam đã tham gia có đề cập về tội phạm công nghệ cao. Trên cơ sở đó, nội dung cơ bản của pháp luật về tội phạm công nghệ cao cũng như công tác hợp tác quốc tế đấu tranh phòng chống loại hình tội phạm này bao gồm những vấn đề chủ đạo sau đây:

4.1.2.1. Các quy định về phòng ngừa tội phạm công nghệ cao

Việc phòng ngừa tội phạm công nghệ cao hiện nay bên cạnh thuộc trách nhiệm của cơ quan chuyên trách phòng, chống TPCNC (là các đơn vị nghiệp vụ trong Công an nhân dân – Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Quân đội nhân dân được giao nhiệm vụ chuyên trách tham mưu, tổ chức, trực tiếp thực hiện nhiệm vụ đấu tranh phòng, chống TPCNC) còn có sự tham gia của các cá nhân, tổ chức, doanh nghiệp và cơ quan thông tin đại chúng.

Hoạt động phòng ngừa TPCNC của các Cơ quan chuyên trách bao gồm[121]: tổ chức, triển khai các biện pháp nghiệp vụ theo quy định của pháp luật để thu thập thông tin, tài liệu về tình hình có liên quan tại các địa bàn, lĩnh vực phụ trách nhằm phục vụ việc phòng ngừa, ngăn chặn tội phạm và VPPL khác có sử dụng công nghệ cao; tổng hợp, phân tích, đánh giá, dự báo tình hình, đề xuất các chủ trương, biện pháp phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; hướng dẫn các cơ quan, đơn vị có liên quan thực hiện các biện pháp phòng ngừa, ngăn chặn tội phạm và VPPL khác có sử dụng công nghệ cao; thông tin, tuyên truyền, giáo dục pháp luật phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao.

Trong phòng ngừa TPCNC, cá nhân có trách nhiệm[122]: tham gia các hoạt động phòng ngừa chung; bảo vệ mật khẩu, khóa mật khẩu, cơ sở dữ liệu, thông tin cá nhân, thông tin tài khoản và hệ thống thiết bị công nghệ cao của mình; phát hiện, kịp thời tố giác tội phạm và VPPL khác có sử dụng công nghệ cao với cơ quan Công an hoặc chính quyền cơ sở gần nhất; phối hợp chặt chẽ với Cơ quan chuyên trách trong quá trình xác minh làm rõ tội phạm và VPPL khác có sử dụng công nghệ cao, cung cấp các thông tin, tài liệu cần thiết có liên quan cho Cơ quan chuyên trách khi được yêu cầu theo quy định của pháp luật.

Các cơ quan, tổ chức, doanh nghiệp tham gia phòng ngừa TPCNC có trách nhiệm[123]: Thực hiện quy định của pháp luật về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; chấp hành quy định của pháp luật về thời hạn bảo quản, lưu trữ, cung cấp thông tin, dữ liệu điện tử phục vụ công tác phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; cung cấp thông tin, tài liệu, số liệu, dữ liệu, đồ vật liên quan đến tội phạm và VPPL khác có sử dụng công nghệ cao cho

[121] Điều 8 Nghị định 25/2014/NĐ-CP quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao.

[122] Điều 9 Nghị định 25/2014/NĐ-CP quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao.

[123] Điều 10 Nghị định 25/2014/NĐ-CP quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao.

Cơ quan chuyên trách khi có yêu cầu; phối hợp chặt chẽ với Cơ quan chuyên trách, các cơ quan nhà nước có thẩm quyền trong việc phát hiện, phòng ngừa, ngăn chặn tội phạm và VPPL khác có sử dụng công nghệ cao.

Đối với cơ quan thông tin đại chúng, trách nhiệm tham gia phòng ngừa TPCNC bao gồm[124]: Đưa tin kịp thời, chính xác chủ trương, chính sách, pháp luật về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; phản ánh tình hình, kết quả công tác phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; nêu gương các điển hình tiên tiến, mô hình có hiệu quả trong phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; lồng ghép nội dung phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao với các chương trình thông tin, tuyên truyền khác.

Việc phòng ngừa TPCNC còn bao gồm các hoạt động: thông tin, tuyên truyền, giáo dục về phòng, chống TPCNC; thực hiện quản lý hành chính về an ninh, trật tự và các hoạt động chuyên môn của cơ quan chuyên trách.

Về biện pháp thông tin, tuyên truyền, giáo dục về phòng, chống TPCNC: các nội dung tuyên truyền bao gồm chính sách, pháp luật về phòng, chống TPCNC; vị trí, vai trò, tầm quan trọng của công tác phòng, chống TPCNC trong việc bảo vệ và giữ gìn an ninh, trật tự; Phương thức, thủ đoạn và nguy cơ, tác hại của TPCNC; Kiến thức, kỹ năng tự phòng, chống các nguy cơ của TPCNC; kỹ năng ứng phó khi bị tấn công, xâm nhập trái phép vào hệ thống thông tin, cơ sở dữ liệu; Biện pháp, kinh nghiệm phòng, chống TPCNC; Trách nhiệm của cá nhân, cơ quan, tổ chức, doanh nghiệp trong phòng, chống TPCNC; Các nội dung khác có liên quan đến phòng, chống TPCNC;

Hình thức thông tin, tuyên truyền, giáo dục bao gồm: Gặp gỡ, trao đổi, đối thoại, thảo luận trực tiếp; thông qua các phương tiện thông tin đại chúng; thông qua hoạt động tại các cơ sở giáo dục, đào tạo; thông qua các cuộc thi tìm hiểu pháp luật, sinh hoạt cộng đồng; các hình thức khác phù hợp với quy định của pháp luật. Công tác thông tin, tuyên truyền, giáo dục đặc biệt được tăng cường đối với các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ Internet, viễn thông; các doanh nghiệp hoạt động trong lĩnh vực tài chính, ngân hàng, thanh toán điện tử và thương mại điện tử; tầng lớp thanh niên, thiếu niên, học sinh, sinh viên trong nhà trường phổ thông và các cơ sở giáo dục, đào tạo khác liên quan đến công nghệ cao; các hiệp

[124] Điều 11 Nghị định 25/2014/NĐ-CP quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao.

hội, câu lạc bộ trong lĩnh vực công nghệ cao và những địa bàn xảy ra nhiều vụ việc VPPL có sử dụng công nghệ cao.

Về biện pháp quản lý hành chính về an ninh, trật tự: Cơ quan thực hiện chức năng quản lý hành chính về an ninh, trật tự thông qua hoạt động của mình có trách nhiệm chủ động phát hiện kịp thời nguyên nhân, điều kiện, phương thức, thủ đoạn hoạt động của TPCNC và có biện pháp xử lý phù hợp. Các biện pháp phòng ngừa tội phạm sử dụng công nghệ cao thông qua quản lý hành chính về an ninh, trật tự, bao gồm: Theo dõi nhân khẩu, hộ khẩu thông qua công tác quản lý cư trú, kiểm tra nhân khẩu thường trú, tạm trú, lưu trú, tạm vắng trên địa bàn; quản lý hồ sơ, tàng thư, căn cước phục vụ công tác phòng, chống TPCNC; quản lý nhập cảnh, xuất cảnh, quá cảnh và các biện pháp quản lý hành chính nhà nước về an ninh, trật tự khác theo quy định của pháp luật.

4.1.2.2. Các quy định về đấu tranh, triệt phá tội phạm công nghệ cao

Thứ nhất, quy định về phát hiện, xử lý tội phạm công nghệ cao

Cá nhân có trách nhiệm tố giác về TPCNC với cơ quan Công an, Ủy ban nhân dân xã, phường, thị trấn hoặc với bất kỳ cơ quan, tổ chức nào[125]. Cơ quan, tổ chức khi phát hiện hoặc nhận được tố giác, tin báo về TPCNC có trách nhiệm xử lý theo thẩm quyền hoặc thông báo ngay với Cơ quan điều tra, Cơ quan chuyên trách theo quy định của pháp luật[126].

Việc phát hiện TPCNC thông qua hoạt động thanh tra, kiểm tra được xử lý như sau[127]: Cơ quan, tổ chức, doanh nghiệp có trách nhiệm thường xuyên tự kiểm tra việc thực hiện chức năng, nhiệm vụ của mình; trường hợp phát hiện TPCNC thì phải xử lý theo thẩm quyền hoặc kiến nghị xử lý theo quy định của pháp luật; cơ quan thanh tra chuyên ngành, Cơ quan chuyên trách thông qua hoạt động thanh tra chủ động phát hiện, xử lý hoặc kiến nghị xử lý TPCNC. Trong trường hợp cần thiết, cơ quan thanh tra chuyên ngành đề nghị Cơ quan chuyên trách phối hợp tiến hành thanh tra, xử lý vi phạm đối với các cơ quan, tổ chức, doanh nghiệp, cá nhân nhằm phòng ngừa TPCNC.

Thứ hai, về các biện pháp tổ chức, đấu tranh chống TPCNC của Cơ quan chuyên trách bao gồm[128]:

---

[125] Khoản 1 Điều 12 Nghị định 25/2014/NĐ-CP

[126] Khoản 2 Điều 12 Nghị định 25/2014/NĐ-CP

[127] Điều 13 Nghị định 25/2014/NĐ-CP

[128] Điều 14 Nghị định 25/2014/NĐ-CP

+ Áp dụng các biện pháp nghiệp vụ theo quy định của pháp luật để thu thập thông tin, tài liệu, xác minh, làm rõ TPCNC;

+ Sử dụng phương tiện kỹ thuật nghiệp vụ để kiểm tra, giám sát, phát hiện, thu thập, phục hồi và phân tích thông tin, tài liệu, dữ liệu điện tử phục vụ phát hiện, điều tra, xử lý TPCNC;

+ Yêu cầu cá nhân, cơ quan, tổ chức cung cấp thông tin, tài liệu, đồ vật, phương tiện liên quan đến TPCNC;

+ Yêu cầu ngân hàng, tổ chức tín dụng cung cấp thông tin, tài liệu về hoạt động của tài khoản và thông tin, tài liệu khác phục vụ công tác phát hiện, điều tra, xử lý TPCNC theo quy định của pháp luật;

+ Yêu cầu các doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet bố trí mặt bằng, cổng kết nối, các điều kiện kỹ thuật cần thiết để Cơ quan chuyên trách triển khai các phương tiện, biện pháp kỹ thuật kiểm tra, giám sát, thu thập dữ liệu điện tử; yêu cầu doanh nghiệp viễn thông, doanh nghiệp CNTT, doanh nghiệp ứng dụng CNTT cung cấp thông tin, tài liệu về hoạt động của chủ thuê bao và thông tin, tài liệu khác phục vụ công tác phát hiện, điều tra, xử lý TPCNC;

+ Trực tiếp hoặc phối hợp với cơ quan nhà nước có thẩm quyền yêu cầu các doanh nghiệp cung cấp dịch vụ Internet, doanh nghiệp viễn thông ngăn chặn, đình chỉ việc truy nhập hệ thống thiết bị, mạng lưới, sử dụng và cung cấp dịch vụ;

+ Thực hiện các nhiệm vụ, quyền hạn khác theo quy định của pháp luật.

Thứ ba, quy định về hình sự hóa đối với các hành vi sử dụng công nghệ cao để gây tổn hại đến quyền lợi chính đáng của cá nhân, tổ chức và nhà nước

Theo đó, pháp luật hình sự Việt Nam hiện nay coi tội phạm sử dụng công nghệ cao 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 4 yếu tố cấu thành tội phạm (khách thể, mặt khách quan, chủ thể và mặt chủ quan).

+ *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 CNTT, để thực hiện hành vi phạm tội.

+ *Mặt khách quan*

Các hành vi của tội phạm công nghệ cao rất đa dạng và phức tạp. Các hành vi này cũng phát triển, thay đổi không ngừng cùng với sự phát triển của công nghệ mới. Đó là hành vi được quy định trong Bộ luật hình sự 2015 sửa đổi, bổ sung 2017 gồm 8 tội danh quy định từ Điều 285 đến Điều 292.

Hậu quả của hành vi trong TPCNC 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 hướng dẫn áp dụng quy định của Bộ luật Hình sự về một số tội phạm trong lĩnh vực CNTT và viễn thông thì 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.

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. Ví dụ: Tài khoản của B ở Ngân hàng T có số tiền là năm triệu đồng. A truy cập bất hợp pháp vào tài khoản của B chiếm đoạt số tiền năm triệu đồng. Quá trình truy cập bất hợp pháp vào tài khoản của B, hệ thống mạng của Ngân hàng T bị tổn hại và Ngân hàng T khắc phục sự cố này hết năm mươi triệu đồng. Trường hợp này, hậu quả thiệt hại do hành vi của A gây ra là năm mươi triệu đồng.

Ví dụ về thiệt hại trực tiếp hoặc thiệt hại gián tiếp. A phát tán virus làm cho mạng máy tính điều hành sản xuất của Công ty B ngừng hoạt động trong thời gian 2 giờ. Công ty B phải chi trả số tiền là bảy triệu đồng để khắc phục sự cố của mạng máy tính công ty trở lại nguyên trạng như trước khi bị virus do A phát tán xâm nhập. Do mạng máy tính của Công ty B ngừng hoạt động trong hai giờ dẫn đến hoạt động sản xuất của Công ty B bị đình trệ gây thiệt hại hai trăm triệu đồng. Trường hợp này, thiệt hại do hành vi phát tán vi rút của A gây ra đối với Công ty B là hai trăm linh bảy triệu đồng (bao gồm thiệt hại trực tiếp là bảy triệu đồng và thiệt hại gián tiếp là hai trăm triệu đồng).

+ *Mặt chủ quan:* Chủ thể TPCNC 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 VPPL trong lĩnh vực CNTT thường không phải là dấu hiệu bắt buộc mà yếu tố quan trọng để xác định hành vi có cấu thành VPPL 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.

+ *Chủ thể:* Đối với TPCNC, 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). Nhưng pháp nhân thương mại không phải chịu trách nhiệm hình sự về các tội phạm trong lĩnh vực CNTT[129]. Do vậy, tội phạm trong lĩnh vực CNTT chỉ là người có năng lực trách nhiệm hình sự.

Một trong những quy định phục vụ có hiệu quả cho yêu cầu đấu tranh phòng chống TPCNC đó là quy định về nguồn chứng cứ - dữ liệu điện tử (chứng cứ điện tử).[130] Khi các dữ liệu điện tử được thu thập theo những biện pháp do BLTTHS quy định, thỏa mãn các thuộc tính của chứng cứ, thì các dữ liệu điện tử được coi là chứng cứ điện tử. 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 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 tín hiệu điện tử. Hầu hết các 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 rất 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 hóa 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.

---

[129] Điều 76 Bộ luật Hình sự 2015, sửa đổi, bổ sung năm 2017

[130] Điều 99 BLTTHS 2015

Thứ tư, quy định về hình phạt đối với TPCNC

Pháp luật hình sự Việt Nam quy định về 7 hình phạt chính và 7 hình phạt bổ sung đối với người phạm tội[131]. Đối với các TPCNC, 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 01 năm đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

4.1.2.3. Các quy định về chủ thể trong hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao

Chủ thể trực tiếp thực hiện các hoạt động hợp tác quốc tế trong phòng, chống TPCNC là Bộ Công an[132]. Bên cạnh đó, theo quy định tại Điều 65 của Luật TTTP năm 2007, Bộ Công an là cơ quan có trách nhiệm tiếp nhận, chuyển giao, xem xét, giải quyết các yêu cầu của nước ngoài về dẫn độ, chuyển giao người đang chấp hành hình phạt tù; xem xét và chuyển hồ sơ cho VKSND, TAND và thực hiện hoạt động TTTP theo thẩm quyền. Bộ Công an đề xuất việc ký kết, gia nhập và thực hiện điều ước quốc tế về dẫn độ và chuyển giao người đang chấp hành hình phạt tù; kiến nghị sửa đổi, bổ sung và hoàn thiện pháp luật Việt Nam về TTTP. Định kỳ sáu tháng và hàng năm Bộ công an phải thông báo với Bộ Tư pháp tình hình thực hiện yêu cầu dẫn độ và chuyển giao người đang chấp hành hình phạt tù.

Trong hoạt động phòng chống TPCNC của Bộ Công an, lực lượng đóng vai trò nòng cốt là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao A05. Bên cạnh các hoạt động chuyên môn, nghiệp vụ, để thực hiện có hiệu quả chức năng hợp tác quốc tế trong phòng chống TPCNC, Cục còn phối hợp với Văn phòng INTERPOL Việt Nam. Ngoài ra, còn có các cơ quan tiến hành tố tụng hình sự của Việt Nam như Cơ quan VKSND gồm VKSNDTC và VKSND cấp tỉnh; Cơ quan TAND gồm TANDTC và TAND cấp tỉnh;

Các chủ thể phối hợp tham gia thực hiện hợp tác quốc tế trong phòng, chống tội phạm gồm có:

- Bộ Tư pháp: Với tư cách là cơ quan quản lý nhà nước về TTTP, Bộ Tư pháp có trách nhiệm phối hợp với Bộ Công an, VKSNDTC, TANDTC, Bộ Ngoại giao soạn thảo các văn bản quy phạm pháp luật hướng dẫn thực thi Luật TTTP; tham gia đàm phán, góp ý, thẩm định các hiệp định TTTP về hình sự, dẫn độ và chuyển giao

[131] Điều 32 Bộ Luật hình sự năm 2015, sửa đổi, bổ sung năm 2017

[132] Khoản 19 Điều 15 Luật Công an nhân dân năm 2018

người chấp hành án phạt tù. Bên cạnh đó, Bộ Tư pháp cũng phối hợp với Bộ Công an và VKSNDTC xử lý những yêu cầu ủy thác phức tạp và nhạy cảm.

- Bộ Ngoại giao: Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Tư pháp, TANDTC, Bộ Công an, VKSNDTC trong công tác xây dựng pháp luật về TTTP, phối hợp thực hiện các hoạt động trong hợp tác quốc tế trong đấu tranh phòng chống tội phạm trên nguyên tắc có đi có lại.

4.1.2.4. Các quy định về dẫn độ tội phạm công nghệ cao

Quy định về dẫn độTPCNC tại Việt Nam áp dụng chung như các trường hợp dẫn độ tội phạm khác.[133]

Thứ nhất, Quy định về thẩm quyền thực hiện dẫn độ.

Các cơ quan có thẩm quyền về dẫn độ TPCNC gồm có Bộ Công an, Tòa án, Viện Kiểm sát, Bộ Ngoại giao.

Bộ Công an trực tiếp thực hiện các hoạt động dẫn độ TPCNC. Bộ Công an tiếp nhận yêu cầu dẫn độ và các tài liệu kèm theo từ cơ quan có thẩm quyền của Việt Nam và cơ quan có thẩm quyền của nước ngoài.Kiểm tra tính hợp lệ của hồ sơ, sự phù hợp với các hiệp định, điều ước quốc tế song phương hoặc đa phương về dẫn độ (nếu có). Trường hợp cần áp dụng nguyên tắc có đi có lại thì chuyển cho Bộ Ngoại giao để chủ trì việc xem xét áp dụng nguyên tắc này.

Trường hợp yêu cầu dẫn độ được chuyển trực tiếp qua kênh INTERPOL, ASEANAPOL Việt Nam thuộc Cục Đối ngoại, Bộ Công an, thì phối hợp thực hiện theo quy chế tại Điều lệ các tổ chức trên. Kết quả việc thực hiện được gửi cho cơ quan đầu mối là Cục Đối ngoại của Bộ Công an để theo dõi, tổng hợp chung.

TANDTC có trách nhiệm hướng dẫn TAND các cấp xem xét, quyết định dẫn độ; xem xét, quyết định các vụ việc về dẫn độ theo thẩm quyền khi có kháng cáo, kháng nghị; định kỳ sáu tháng và hằng năm thông báo với Bộ Tư pháp tình hình thực hiện các vụ việc dẫn độ thuộc thẩm quyền. Tòa án nhân dân cấp tỉnh có trách nhiệm xem xét, quyết định dẫn độ hoặc từ chối dẫn độ theo quy định của Luật TTTP và báo cáo kết quả thực hiện dẫn độ cho TANDTC.

Viện Kiểm sát nhân dân các cấp: Có trách nhiệm thực hiện kiểm sát hoạt động dẫn độ theo thẩm quyền.

Bộ Ngoại giao: Có trách nhiệm chủ trì phối hợp với các bộ, ngành có liên quan xem xét, quyết định áp dụng nguyên tắc có đi có lại trong dẫn độ với nước hữu quan; định kỳ sáu tháng và hằng năm thông báo với Bộ Tư pháp tình hình áp dụng nguyên tắc có đi có lại trong dẫn độ với nước hữu quan.

---

[133] Khoản 1, Điều 32 Luật Tương trợ tư pháp ra đời năm 2007

Thứ hai, Quy định về các trường hợp bị dẫn độ, từ chối dẫn độ và dẫn độ kèm theo một số điều kiện

- Trường hợp bị dẫn độ:

+ Trường hợp cơ quan có thẩm quyền tiến hành tố tụng của Việt Nam yêu cầu cơ quan có thẩm quyền tương ứng của nước ngoài dẫn độ thì đối tượng bị dẫn độ (đang cư trú ở nước ngoài) là người có hành vi phạm tội hoặc bị kết án hình sự mà bản án đã có hiệu lực pháp luật. Trường hợp này, người bị dẫn độ có thể là người Việt Nam hoặc người nước ngoài.

+ Trường hợp cơ quan có thẩm quyền tiến hành tố tụng của nước ngoài yêu cầu cơ quan có thẩm quyền tương ứng của Việt Nam thực hiện việc dẫn độ thì đối tượng bị dẫn độ phải là người nước ngoài có hành vi phạm tội hoặc bị kết án hình sự mà bản án đã có hiệu lực pháp luật hiện đang cư trú trên lãnh thổ Việt Nam (xuất phát từ nguyên tắc chủ quyền quốc gia, thì cơ quan có thẩm quyền của Việt Nam từ chối dẫn độ nếu người bị yêu cầu dẫn độ là người có quốc tịch Việt Nam). Người nước ngoài bị yêu cầu dẫn độ ở đây được hiểu là người mang quốc tịch của nước yêu cầu dẫn độ đã phạm tội hoặc gây thiệt hại cho quốc gia có yêu cầu dẫn độ hoặc người mang quốc tịch của quốc gia khác, người không quốc tịch đã thực hiện tội phạm ở quốc gia yêu cầu dẫn độ hoặc gây thiệt hại cho quốc gia đó. Quốc tịch của cá nhân bị yêu cầu dẫn độ thường được các quốc gia thoả thuận xác định vào thời điểm tiếp nhận quyết định dẫn độ.

- Trường hợp đương nhiên từ chối và có thể từ chối dẫn độ cho nước ngoài. Không phải yêu cầu dẫn độ nào của nước ngoài cũng được Cơ quan tiến hành tố tụng có thẩm quyền của Việt Nam chấp thuận. Việc từ chối dẫn độ trong trường hợp này được chia thành các trường hợp sau: Trường hợp đương nhiên từ chối dẫn độ[134]; trường hợp có thể từ chối dẫn độ[135].

- Trường hợp dẫn độ kèm theo một số điều kiện nhất định:

Trường hợp Việt Nam là nước được yêu cầu dẫn độ thì việc dẫn độ chỉ được thực hiện khi nước yêu cầu dẫn độ cam kết không truy cứu trách nhiệm hình sự người bị dẫn độ về hành vi phạm tội khác ngoài hành vi phạm tội đã được nêu trong yêu cầu dẫn độ, không dẫn độ người đó cho nước thứ ba, trừ trường hợp được sự đồng ý bằng văn bản của Việt Nam[136].

4.1.2.5.Tương trợ tư pháp về hình sự

---

[134] Khoản 1 Điều 35 Luật Tương trợ tư pháp 2007

[135] Khoản 2 Điều 35 Luật Tương trợ tư pháp 2007

[136]khoản 2 Điều 34 Luật Tương trợ tư pháp 2007

Tại Việt Nam, TTTP về hình sự đối với TPCNC được thực hiện theo quy định các điều ước quốc tế song phương hoặc đa phương mà Việt Nam ký kết hoặc tham gia và pháp luật có liên quan đến TTTP về hình sự như Luật TTTP (Điều 24), Bộ luật TTHS 2015 (Điều 178, 184…) Bộ luật hình sự và các quy định của một số luật khác như Luật Phòng chống rửa tiền 2012, Luật Phòng chống tham nhũng 2018, Luật Phòng chống khủng bố 2013… và các văn bản hướng dẫn thi hành có quy định về HTQT trong đấu tranh phòng chống TPCNC.

Căn cứ vào quy định của Luật TTTP 2007, Bộ luật TTHS năm 2015 và thực tiễn áp dụng hoạt động TTTP về hình sự giữa Việt Nam với các quốc gia, phạm vi TTTP về hình sự bao gồm[137]: tống đạt giấy tờ, hồ sơ, tài liệu liên quan đến TTTP về hình sự; triệu tập người làm chứng, người giám định; thu thập, cung cấp chứng cứ; truy cứu trách nhiệm hình sự; trao đổi thông tin; các yêu cầu tương trợ tư pháp khác về hình sự. Ngoài ra, Bộ luật TTHS quy định TTTP về hình sự là một trong các hoạt động hợp tác quốc tế trong tố tụng hình sự (Điều 491), theo đó, các hoạt động TTTP về hình sự cụ thể như: Xác định giá trị pháp lý của tài liệu, đồ vật thu thập được (Điều 494); Quy định về việc tiến hành tố tụng của người có thẩm quyền của Việt Nam ở nước ngoài và người có thẩm quyền của nước ngoài ở Việt Nam được thực hiện theo điều ước quốc tế mà Việt Nam là thành viên hoặc theo nguyên tắc có đi có lại (Điều 495); cho người làm chứng, người giám định, người đang chấp hành án phạt tù tại nước được đề nghị có mặt ở Việt Nam để phục vụ việc giải quyết vụ án hình sự hoặc có thể cho phép người làm chứng, người giám định, người đang chấp hành án phạt tù tại Việt Nam có mặt ở nước ngoài để phục vụ việc giải quyết vụ án hình sự (Điều 469); truy tìm, tạm giữ, kê biên, phong tỏa, tịch thu, xử lý tài sản do phạm tội mà có để phục vụ yêu cầu điều tra, truy tố, xét xử và thi hành án hình sự (Điều 507); phong tỏa tài khoản có thể được áp dụng nếu có căn cứ cho rằng số tiền trong tài khoản đó liên quan đến hành vi phạm tội của người bị buộc tội (Điều 129); phối hợp điều tra hoặc áp dụng các biện pháp điều tra tố tụng đặc biệt (Điều 508);

4.1.2.6. Các quy định về chuyển giao người đang chấp hành hình phạt tù

Việc chuyển giao người đang chấp hành hình phạt tù mang tính nhân đạo và tái hoà nhập cộng đồng xã hội. Vì vậy, trong các quy định của điều ước quốc tế mà Việt Nam là thành viên về chuyển giao người đang chấp hành hình phạt tù và Luật TTTP năm 2007, điều kiện bắt buộc là được chính người bị kết án hoặc người đại diện hợp pháp của họ đồng ý một cách tự nguyện và công khai. Về hậu quả pháp lý,

[137] Điều 17 Luật TTTP 2007

thời hạn chấp hành hình phạt mà người bị kết án phải tiếp tục thi hành là phần hình phạt chưa được thực hiện tại quốc gia chuyển giao (nơi tòa án có thẩm quyền đã tuyên bản án).

Thứ nhất, căn cứ tiếp nhận, chuyển giao người đang chấp hành án phạt tù.

Về căn cứ chuyển giao người đang chấp hành hình phạt tù được thực hiện theo quy định tại khoản 2 Điều 49, Điều 50 Luật TTTP năm 2007 và Điều 6 Thông tư liên tịch số 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC.

Về điều kiện tiếp nhận người từ nước ngoài về: Người đó phải là công dân Việt Nam; có nơi thường trú cuối cùng ở Việt Nam; hành vi phạm tội mà người đó bị kết án ở nước ngoài cũng cấu thành tội phạm theo quy định của pháp luật Việt Nam. Điều kiện này nhằm tạo cơ sở cho việc xem xét chuyển đổi hình phạt để có thể tiếp tục chấp hành bản án tại Việt Nam; vào thời điểm tiếp nhận yêu cầu chuyển giao thời hạn chưa chấp hành án phạt tù phải còn ít nhất là 01 năm; trong trường hợp đặc biệt, thời hạn này còn ít nhất là 06 tháng. Quy định này có ý nghĩa giáo dục, cải tạo người đó, tạo điều kiện cho họ tái hoà nhập cộng đồng khi chấp hành bản án tại Việt Nam; bản án đối với người được đề nghị chuyển giao về Việt Nam đã có hiệu lực pháp luật và không còn thủ tục tố tụng nào đối với người đó tại nước chuyển giao; nước chuyển giao và người bị kết án đều đồng ý với việc chuyển giao (trong trường hợp người bị kết án phạt tù là người chưa thành niên, người có nhược điểm về thể chất hoặc tâm thần thì phải có sự đồng ý của người đại diện hợp pháp của người đó); ngoài ra, Tòa án có thẩm quyền của Việt Nam có quyết định đồng ý tiếp nhận đã có hiệu lực pháp luật.

Về điều kiện chuyển giao người đang chấp hành hình phạt tù ra nước ngoài: Người đó là công dân (có quốc tịch) của nước tiếp nhận hoặc là người được phép cư trú không thời hạn hoặc có người thân thích tại nước tiếp nhận chuyển giao; có đủ các điều kiện quy định tại khoản 1 Điều 50 Luật TTTP năm 2007 thuộc trường hợp đã nêu ở trên và đã thực hiện xong phần trách nhiệm dân sự, hình phạt bổ sung là phạt tiền, tịch thu tài sản và các trách nhiệm pháp lý khác trong bản án. Nước tiếp nhận và người bị kết án đều đồng ý với việc chuyển giao. Trong trường hợp người bị kết án phạt tù là người chưa thành niên, người có nhược điểm về thể chất hoặc tâm thần thì phải có sự đồng ý của người đại diện hợp pháp của người đó, Tòa án có thẩm quyền của Việt Nam có quyết định đồng ý chuyển giao đã có hiệu lực pháp luật.

Thứ hai, các trường hợp từ chối chuyển giao người đang chấp hành án phạt tù.

Việc từ chối chuyển giao người đang chấp hành hình phạt tù tại Việt Nam cho nước ngoài khi:[138] có căn cứ cho rằng người được chuyển giao có thể bị tra tấn, trả thù hoặc truy bức tại nước tiếp nhận chuyển giao; việc chuyển giao có thể phương hại đến chủ quyền, an ninh quốc gia của Việt Nam.

Thứ ba, lưu ý về việc tiếp nhận, chuyển giao người đang chấp hành hình phạt tù

Khi thỏa mãn điều kiện được chuyển giao, Công dân Việt Nam phạm tội và bị kết án phạt tù có thể làm đơn thể hiện nguyện vọng được chuyển giao về Việt Nam để tiếp tục chấp hành phần hình phạt còn lại thông qua Bộ Công an nước Cộng hòa xã hội chủ nghĩa Việt Nam hoặc cơ quan đại diện Việt Nam ở nước ngoài. Trình tự, thủ tục nhận yêu cầu chuyển giao và xem xét, quyết định việc tiếp nhận được quy định tại Điều 9 Thông tư liên tịch số 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC. Bộ Công an sẽ phải xác minh người đó có đồng ý một cách tự nguyện và với nhận thức đầy đủ về những hệ quả pháp lý của việc chuyển giao hay không.[139]

Thông báo quyền được yêu cầu chuyển giao cho người đang chấp hành án phạt tù.Theo quy định của pháp luật TTTP 2007 và Điều 12 Thông tư liên tịch số 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC, Tòa án nhân dân đã xét xử sơ thẩm, phúc thẩm có trách nhiệm thông báo cho bị cáo thuộc diện quy định biết về quyền được yêu cầu chuyển giao. Hàng năm, Bộ Công an thực hiện việc thông báo biết về quyền được yêu cầu chuyển giao.

Bộ Công an có trách nhiệm lập hồ sơ đề nghị tiếp nhận và chuyển giao cho Bộ Ngoại giao xem xét, quyết định áp dụng nguyên tắc có đi có lại. Tại các quốc gia có điều ước quốc tế mà Việt Nam là thành viên thì khi có đơn xin chuyển giao, bản tuyên bố của người này về việc họ hiểu biết đầy đủ về hệ quả của việc chuyển giao và các quyền, nghĩa vụ của việc chuyển giao. Khi đó Bộ trưởng Bộ Công an quyết định cho phép nước tiếp nhận cử đại diện sang Việt Nam để xác minh sự đồng ý chuyển giao của người đang chấp hành án phạt tù.[140]

4.1.2.7. Một số nội dung khác trong hợp tác quốc tế về phòng chống tội phạm công nghệ cao

Thứ nhất, hoạt động thu thập, trao đổi thông tin và truy nã tội phạm thông qua vai trò của Cơ quan INTERPOL Việt Nam.

---

[138] Điều 51 Luật TTTP 2007

[139] Điều 10 Thông tư liên tịch số Số: 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC

[140] Điều 14 Thông tư liên tịch số Số: 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC

Thông qua kênh hợp tác INTERPOL - Văn phòng INTERPOL Việt Nam, lực lượng Công an nhân dân (lực lượng cảnh sát) đã có những thông tin kịp thời về tình hình hoạt động của các tổ chức tội phạm quốc tế; tiếp nhận và xử lý trao đổi thông tin về tội phạm có tổ chức xuyên quốc gia, tội phạm có yếu tố nước ngoài trong việc sử dụng công nghệ cao để thực hiện hành vi phạm tội. Thông qua Cơ quan Interpol Việt Nam, phía Công an Việt Nam đã phối hợp thực hiện các yêu cầu về tương trợ tư pháp hình sự với nước ngoài và ngược lại, hoạt động bắt tội phạm truy nã khi đối tượng tìm cách trốn ra nước ngoài hoặc từ nước ngoài vào Việt Nam.

Thứ hai, hoạt động đẩy trả, trục xuất

Bên cạnh hình thức dẫn độ, trong hoạt động truy bắt tội phạm bỏ trốn hoặc các hình thức đấu tranh phòng chống tội phạm khác còn có các hình thức tương tự như dẫn độ là đẩy trả, trục xuất. Đây là các biện pháp áp dụng cho những đối tượng và những trường hợp khác nhau. Nhưng thực tế, nhiều khi chúng ta lại có sự nhầm lẫn giữa các biện pháp này. Đôi khi cùng một trường hợp, có người gọi là dẫn độ, có người gọi là đẩy trả... Để tránh sự nhầm lẫn đó, cần phải có sự phân biệt các biện pháp này.

Trục xuất là hành vi đưa người nước ngoài ra khỏi lãnh thổ nước mình bằng hành động đơn phương của cơ quan chức năng của nước mà người đó đang cư trú. Trục xuất thường được áp dụng đối với người nước ngoài vi phạm pháp luật của nước sở tại. Vì mục đích bảo đảm an ninh, trật tự xã hội của mình, một nước có quyền trục xuất người nước ngoài vi phạm pháp luật ra khỏi lãnh thổ của mình mà không cần thông báo trước cho nước mà người bị trục xuất mang quốc tịch. Như vậy, trục xuất có nhiều điểm khác biệt với dẫn độ.

Đẩy trả là biện pháp thường được áp dụng đối với những đối tượng phạm tội ở nước ngoài, sau đó lẩn trốn ở lại nước đó. Nói chung đối tượng của đẩy trả về hình thức tương tự như đối tượng của dẫn độ, nhưng trong trường hợp xem xét các khía cạnh về lợi ích quốc gia và yêu cầu phòng, chống tội phạm mà các bên có thể lựa chọn áp dụng biện pháp đẩy trả. Trong thực tiễn, đẩy trả được coi như là một biện pháp áp dụng chủ yếu giữa các nước chưa có luật trong nước quy định về dẫn độ; chủ yếu dựa trên quan hệ thân thiết giữa các quốc gia. Thủ tục đẩy trả đơn giản hơn thủ tục dẫn độ, cụ thể là: nước đẩy trả áp giải đối tượng tới địa điểm đã thoả thuận để trao trả cho cơ quan chức năng của nước tiếp nhận đẩy trả. Tại đó, nước tiếp nhận đọc lệnh bắt đối tượng và tiến hành các thủ tục cần thiết để tiếp nhận đối tượng. Việc đẩy trả thường được tiến hành ở những địa phương giáp biển trên cơ sở mối quan hệ giữa cơ quan Cảnh sát hai địa phương của hai nước.

Thứ ba, hoạt động phối hợp công an các tỉnh biên giới tại các quốc gia trong đấu tranh, phòng chống TPCNC

Công an các tỉnh biên giới (Công an cấp tỉnh của Việt Nam: với Cơ quan tương ứng cấp tỉnh của nước láng giềng) hợp tác quốc tế trong phòng, chống tội phạm gồm các hoạt động:

+ Hợp tác quốc tế trong điều tra khám phá các vụ án hình sự mà hai bên có trách nhiệm cùng nhau giải quyết.

+ Hợp tác quốc tế trong truy bắt, dẫn giải và chuyển giao đối tượng phạm tội hình sự.

+ Hợp tác quốc tế trong tiếp nhận, giải cứu nạn nhân của tội phạm hình sự. Chủ yếu thông qua các cơ quan đầu mối trung ương, lực lượng cảnh sát nước láng giềng chuyển giao các nạn nhân của các tội phạm xuyên quốc gia cho Công an cấp tỉnh biên giới Việt Nam tại các sân bay và cửa khẩu giữa hai nước.

Thứ tư, hợp tác quốc tế trong việc traođổi, cung cấp thông tin về tội phạm với các tổ chức cảnh sát trong khu vực và toàn cầu

- Trao đổi thông tin ra nước ngoài[141]: Khi các lực lượng nghiệp vụ cảnh sát nhân dân có yêu cầu, các bộ phận chuyên trách sẽ có nhiệm vụ chuyển nội dung thông tin cần trao đổi, xác minh đối với nước ngoài đến Văn phòng INTERPOL Việt Nam; trong đó ghi rõ địa chỉ, nội dung cụ thể, thời hạn, mục đích cần đạt được, tính hợp pháp (pháp lý); sau đó INTERPOL Việt Nam căn cứ vào phạm vi hợp tác sẽ dịch ra tiếng Anh, chuyển yêu cầu đến địa chỉ và có nhiệm vụ thường xuyên nhắc nhở, theo quy trình. Sau khi đối tác gửi kết quả, INETERPOL dịch và khẩn trương gửi kết quả về đơn vị nghiệp vụ có yêu cầu ban đầu; đưa ra những khuyến nghị và tham mưu hướng giải quyết cho các đơn vị theo thông lệ quốc tế, cũng như pháp luật quốc gia của nước đối tác.

- Trao đổi thông tin từ phía nước ngoài: Văn phòng INTERPOL Việt Nam là đơn vị đầu mối của Bộ Công an Việt Nam, có nhiệm vụ tiếp nhận thông tin và các yêu cầu khác về đấu tranh phòng, chống tội phạm, trong phạm vi của mình dịch các thông tin (hoặc không) ra tiếng Việt sau đó báo cáo lãnh đạo có thẩm quyền chuyển cho các đơn vị nghiệp vụ thực hiện nhiệm vụ xác minh thông tin hoặc tự xác minh thông tin; sau đó tiếp nhận, dịch ra tiếng Anh kết quả xác minh trả lời và gửi trả lời kết quả cho đối tác.

Thực tế, hình thức trao đổi thông tin về tội phạm trong khuôn khổ hợp tác INTERPOL và ASEAN/ASEANAPOL là những khuôn khổ hoạt động có hiệu quả

[141]Điều 5 Điều lệ tổ chức INTERPOL

và được sử dụng thường xuyên nhất trong hợp tác quốc tế trao đổi thông tin về phòng, chống tội phạm nói chung và TPCNC nói riêng.

Thứ năm, trao đổi kinh nghiệm đào tạo và chuyển giao công nghệ

Trong khuôn khổ, phạm vi đã ký kết tại điều ước quốc tế song phương hoặc đa phương, Bộ Công an, VKSNDTC, TANDTC có thể tổ chức các hội nghị, quốc tế để trao đổi kinh nghiệm, tổng kết công tác hợp tác đấu tranh phòng, chống tội phạm giữa các bên.

Thứ sáu, hợp tác quốc tế đấu tranh phòng, chống tội phạm giữa lực lượng Cảnh sát nhân dân Việt Nam với lực lượng Cảnh sát các nước

Cơ chế hợp tác quốc tế trong phòng, chống tội phạm liên quan đến Việt Nam, lực lượng cảnh sát nhân dân Việt Nam thường chủ yếu thực hiện theo những khuôn khổ hợp tác đó là: Thông qua khuôn khổ hợp tác INTERPOL; thông qua khuôn khổ hợp tác ASEAN/ASEANAPOL; qua kênh hợp tác với Văn phòng Sỹ quan liên lạc Cảnh sát các nước tại Việt Nam và trong khu vực Đông Nam Á; qua kênh hợp tác trực tiếp với một số cơ quan thi hành pháp luật khác như Cục điều tra Liên hang Hoa Kỳ (FBI); Cơ quan Bài trừ ma tuý Liên bang Hoa Kỳ (DEA); các Trung tâm chống tội phạm xuyên quốc gia trong mạng lưới Trung tâm chống tội phạm xuyên quốc gia Châu Á - Thái Bình Dương,...

Hoặc cơ chế hợp tác song phương phòng, chống tội phạm nói chung và với một số loại tội phạm nói riêng giữa Công an các tỉnh biên giới của Việt Nam với các đối tác tương ứng của nước ngoài dưới hình thức hợp tác giữa các tỉnh biên giới, hoặc bằng hình thức kết nghĩa đối với những tỉnh chưa ký kết thỏa thuận quốc tế phòng, chống tội phạm cấp tỉnh.

4.2. Thực tiễn thực thi pháp luật trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao của Việt Nam

4.2.1. Kết quả hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao trong thời gian vừa qua

4.2.1.1. Về đàm phán, ký kết, gia nhập điều ước quốc tế trong phòng chống tội phạm công nghệ cao:

- Các điều ước quốc tế đa phương về phòng, chống tội phạm:

Theo thống kê của Bộ Công an, tính đến tháng 9/2019, Việt Nam là thành viên của 22 điều ước quốc tế đa phương quy định về TTTP về hình sự, dẫn độ và chuyển giao người bị kết án phạt tù. Trong số này có 01 Hiệp định chuyên biệt TTTP 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 ngày 20/9/2005). Có 03 điều ước quốc tế đa phương

có quy định về chuyển giao người bị kết án phạt tù và các điều ước quốc tế đa phương còn lại đều quy định về dẫn độ *(xem thêm tại Phụ lục 01 và tiểu mục 4.1.2.2)*.

Trong số các điều ước quốc tế đa phương mà Việt Nam là thành viên quy định về HTQT trong đấu tranh, phòng chống tội phạm thì có điều ước quốc tế điều chỉnh HTQT trong lĩnh vực phòng chống TPCNC như.

+ Công ước của Liên Hợp quốc về chống tội phạm có tổ chức xuyên quốc gia (Transnational Organized Crime - gọi tắt tiếng là TOC) thông qua ngày 12 đến ngày 15/12/2000 tại thành phố Palermo, Cộng hòa Ý, dưới sự chủ trì của Liên hợp quốc, đại diện 124 nước trong đó có Việt Nam đã ký Công ước của Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia. Công ước này đã và sẽ thúc đẩy sự hợp tác giữa các quốc gia trên thế giới để ngăn ngừa và trừng phạt tội phạm có tổ chức xuyên quốc gia một cách hiệu quả, đồng thời tăng cường năng lực của các nước thành viên trong việc phòng, chống tội phạm có tổ chức xuyên quốc gia.

+ Hiệp định TTTP về hình sự giữa các nước ASEAN, được các quốc gia ASEAN ký vào ngày 29/11/2004 tại thủ đô Kuala Lumpur, Liên bang Malaysia gồm đại diện của 08 nước là Brunei, Campuchia, Indonesia, Lào, Malaysia, Philippines, Singapore và Việt Nam. Tiếp đó, ngày 17/1/2006, 02 nước thành viên ASEAN còn lại là Thái Lan và Myamnar đã ký. Hiệp định là điều ước quốc tế đa phương đầu tiên về TTTP 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.

- *Các điều ước quốc tế song phương (Hiệp định) về hợp tác quốc tế trong đấu tranh, phòng chống tội phạm nói chung và TPCNC nói riêng*

Trong lĩnh vực hợp tác quốc tế phòng, chống tội phạm nói chung và TPCNC nói riêng, Việt Nam đã ký 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 vào nhu cầu về phạm vi, nội dung hợp tác quốc tế trong phòng, chống tội phạm của của mỗi nước. Các điều ước quốc tế song phương về hợp tác quốc tế trong phòng, chống tội phạm giữa Việt Nam với các nước thường là các hiệp định TTTP. Các hiệp định về dẫn độ; các hiệp định về tiếp nhận, chuyển giao người đang chấp hành án phạt tù (trường hợp đặc biệt có nội dung khác như: Hiệp định giữa Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam và Chính phủ Cộng hòa Pháp về hợp tác trong lĩnh vực giữ gìn trật tự, an toàn xã hội ký ngày 12/11/2009); các thỏa thuận hoặc bản ghi

nhớ về hợp tác quốc tế trong phòng, chống tội phạm giữa một cơ quan cấp Bộ hay cấp tỉnh và tương đương trên một lĩnh vực hay một phạm vi nhất định. Các điều ước quốc tế song phương hiện hành là cơ sở pháp lý hợp tác quốc tế trong phòng, chống tội phạm cụ thể.

Hiện nay, Việt Nam đã kí 45 Hiệp định song phương với các quốc gia, trong đó có 12 Hiệp định TTTP chung (bao gồm cả dân sự, gia đình và hình sự với các quốc gia), 11 Hiệp định chuyên biệt về TTTP 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.

Ngoài ra, trong lĩnh vực hợp tác quốc tế phòng, chống TPCNC còn có những Hiệp định song phương giữa Chính phủ Việt Nam và Chính phủ các quốc gia hữu quan điều chỉnh trực tiếp đấu tranh phòng, chống các loại tội phạm mà Việt Nam cũng đã ký kết, gia nhập (xem Phụ lục 02).

4.2.1.2.Về phối hợp phát hiện, ngăn chặn và điều tra, xử lý tội phạm sử dụng công nghệ cao theo quy định của pháp luật và các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

Trong thời gian qua, các cơ quan thực thi pháp luật của Việt Nam đã chủ động phối hợp phát hiện, ngăn chặn và điều tra, xử lý nhiều đối tượng tội phạm sử dụng công nghệ cao có yếu tố nước ngoài trên lãnh thổ Việt Nam hoặc đối tượng ở nước ngoài nhưng xâm hại lợi ích của cá nhân, tổ chức trên lãnh thổ Việt Nam. Theo báo cáo của Hiệp hội An toàn thông tin Việt Nam tại Hội thảo triển lãm quốc gia an ninh bảo mật năm 2013, trong 100 Website thuộc Chính phủ (có phần mở rộng là gov.vn) có đến 78% có thể bị tấn công toàn diện. Trong giai đoạn từ năm 2012 đến năm 2013 (tăng 39 vụ việc có liên quan đến người nước ngoài phạm tội sử dụng công nghệ cao). Cùng với đó, số đối tượng là người nước ngoài bị khởi tố về các tội danh liên quan đến lĩnh vực công nghệ cao năm sau cao hơn năm trước.

Phối hợp trong việc thu thập, xác minh thông tin tài liệu phục vụ công tác phát hiện, điều tra TPSDCNC là một trong những yêu cầu hợp tác thông thường giữa lực lượng Công an nhân dân Việt Nam với Công an các nước. Đó có thể là xác minh các địa chỉ IP mà đối tượng phạm tội sử dụng vào hoạt động phạm tội như Chuyên án 126S: Đấu tranh chống tội phạm trộm cắp thông tin thẻ tín dụng đế bán cho tội phạm nước ngoài. Thực hiện yêu cầu xác minh của Cơ quan điều tra tội phạm nguy hiểm của Vương quốc Anh (SOCA) đối với đối tượng Nguyễn Ngọc Lâm và Nguyễn Ngọc Thành với tài sản trộm cắp 4 tỷ đồng. Năm 2012, theo yêu cầu của Cảnh sát Hàn Quốc, lực lượng Công

an Việt Nam đã cung cấp thông tin và dữ liệu ổ cứng máy tính liên quan đến một số địa chỉ IP của Việt Nam có hành vi tấn công website của chính phủ Hàn Quốc…

Trong thời gian từ năm 2010 đến 2014, lực lượng Cảnh sát phòng chống TPSDCNC đã tiếp nhận và xử lý gần 100 thông tin liên quan đến TPSDCNC. Như trường hợp, ngày 11/06/2010, C50 nhận được công văn yêu cầu hỗ trợ của văn phòng AFP, Cảnh sát Liên bang Úc điều tra vụ trộm cắp 182 máy tính Apple ở Úc về tiêu thụ ở Việt Nam. Với sự hợp tác của hai bên, phía Việt Nam đã xác minh và thu thập được chứng cứ liên quan một số đối tượng móc nối tạo dựng một đường dây vận chuyển hàng hóa từ Úc về Việt Nam không khai báo, trốn thuế với số lượng lớn. Bên phía Úc thông tin đường dây này có sự tham gia của nhân viên hải quan, an ninh sân bay và tiếp viên hàng không của Việt Nam Airline, đưa thông tin lượng hàng nhập lậu về Việt Nam gồm 820 máy tính xách tay các loại và nhiều linh kiện điện tử với số tiền vận chuyển khoảng 2 triệu đô la Úc.[142]

Phối hợp trong việc phát hiện và điều tra các vụ án lừa đảo nhằm chiếm đoạt tài sản, đánh bạc bằng công nghệ cao trên lãnh thổ Việt Nam.

Từ năm 2010 đến năm 2017, lực lượng Công an Việt Nam đã phát hiện và điều tra làm rõ gần 200 vụ án lừa đảo nhằm chiếm đoạt tài sản bằng cách sử dụng công nghệ cao, các đối tượng chủ yếu là người Trung Quốc thực hiện trên lãnh thổ Việt Nam. Có thể kể đến 02 vụ việc điển hình diễn ra trên lãnh thổ Việt Nam về việc phối hợp phát hiện, ngăn chặn và điều tra, xử lý tội phạm sử dụng công nghệ cao theo quy định của pháp luật và các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên:

Vụ thứ nhất[143]: Tháng 5-2019, qua công tác nắm tình hình, lực lượng Công an phát hiện tại khu đô thị Our City (quận Dương Kinh, TP Hải Phòng) có số đối tượng lớn người Trung Quốc thuê nhà (gần 400 người) và thuê đường truyền với dung lượng rất lớn. Qua theo dõi, số đối tượng này truy cập hơn 100 website và xây dựng 99 trang web khác tổ chức cho công dân Trung Quốc đánh bạc trực tuyến qua

---

[142] Trần Văn Doanh (2014), Hợp tác quốc tế trong phòng, chống tội phạm sử dụng công nghệ cao và vấn đề đặt ra trong công tác đào tạo, bồi dưỡng cán bộ, *Kỷ yếu hội thảo khoa học* ***"Phòng, chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo"****, Học viện CSND tháng 11/2014*

[143] Vụ 395 người Trung Quốc đánh bạc ở Hải Phòng: Việt Nam không thiệt hại gì! https://nld.com.vn/chinh-tri/vu-395-nguoi-trung-quoc-danh-bac-o-hai-phong-viet-nam-khong-thiet-hai-gi-20190904103959592.htm (truy cập lần cuối ngày 21/12/2020)

mạng internet (có máy chủ đặt tại nước ngoài) để chơi xổ số, cá cược. Sau khi nắm bắt thông tin, Bộ Công an lập tức xác lập chuyên án đấu tranh, trao đổi thông tin với Bộ Công an Trung Quốc. Sau khi nắm được thông tin, Bộ Công an Trung Quốc cũng cho biết đang tổ chức điều tra nhóm đối tượng này và đó là nhóm đối tượng có liên quan đến hoạt động tội phạm tại cả Trung Quốc và Việt Nam. Sau khi xác định rõ nhóm đối tượng trên có hành vi đánh bạc thì lực lượng công an tiến hành bắt quả tang, thu giữ gần 2.000 điện thoại di động thông minh, 533 máy tính các loại, nhiều thẻ ngân hàng, tiền mặt cùng nhiều đồ vật, tài liệu liên quan đến vụ án. Cùng với đó, số tiền mà tổ chức cờ bạc này đã giao dịch trên hệ thống là trên 3,6 tỉ nhân dân tệ, tương đương hơn 12.000 tỉ đồng. Sau khi bắt giữ số đối tượng trên, dựa vào Thoả thuận về hợp tác phòng chống tội phạm giữa Việt Nam - Trung Quốc, Hiệp định định TTTP về hình sự giữa Việt Nam - Trung Quốc cũng như có sự phối hợp thường xuyên trong nhiều năm qua và đối tượng phạm tội đều là người Trung Quốc không có đối tượng phạm tội và bị hại là người Việt Nam nên Bộ Công an đã giao lại các đối tượng cho phía Trung Quốc tiếp nhận, xử lý theo đúng quy định. Đây có thể nói là vụ việc điển hình của công tác hợp tác quốc tế trong phòng chống TPCNC. Suốt trong quá trình phối hợp, hoạt động phát hiện, ngăn chặn và điều tra, xử lý tội phạm sử dụng công nghệ cao phát sinh những vấn đề gì phía Việt Nam cần thì phía Trung Quốc đều có trả lời đầy đủ, đồng thời giữa hai bên đều có những thỏa thuận và hiệp định đầy đủ nên việc xử lý đều nhanh chóng, hiệu quả và đúng quy định.

Vụ thứ hai: Năm 2013, Vương Huy Long (27 tuổi, trú tại xã Tân Thạnh Tây, huyện Củ Chi, TP Hồ Chí Minh) tạo ra diễn đàn với hơn 1.000 thành viên tham gia, có nội dung hướng dẫn tấn công website để trộm cắp thông tin thẻ tín dụng và xác định, có khoảng 1 triệu thẻ tín dụng đã bị hack (trộm cắp). Qua các thông tin thẻ tín dụng hack được, Vương Huy Long cùng đồng bọn tạo ra những người mua hàng là công dân của các bang trên nước Mỹ, hoặc một số nước khác để đi mua hàng, thuê vận chuyển về Việt Nam để chiếm đoạt tiền của các khách hàng. Đối tượng mà Long nhắm tới thường là công dân Mỹ và một số nước kinh tế phát triển khác. Thậm chí, Long còn phối hợp với một đối tượng người Nigeria thành lập công ty "ma" tại Mỹ, chuyên kinh doanh trên mạng, có tên gọi *bp.jobinc.com*, đến năm 2011 đổi thành *savinglogistics.com*. Công ty của Long đã tuyển dụng được 20 nhân viên là những người thất nghiệp, đang cần việc làm trên đất Mỹ. Những người này gọi là Dropper, chỉ làm mỗi việc là đưa địa chỉ cư trú cho Long, để chúng đưa hàng mua được bằng các tài khoản tín dụng trộm cắp về. Sau đó, các Dropper có nhiệm

vụ vận chuyển về Việt Nam cho Long qua các công ty vận chuyển hàng hóa lớn như DHL, Fedex, UPS... và sẽ được trả 10% giá trị hàng hóa. Phương thức Long thanh toán tiền công cho các Dropper là thông qua các giao dịch tiền điện tử LR.

Sau khi thu thập đầy đủ chứng cứ, cơ sở dữ liệu về hoạt động của Long, dựa vào các Thỏa thuận hợp tác giữa hai bên, Bộ Công an Việt Nam đã phối hợp với Bộ An ninh nội địa Hoa Kỳ đấu tranh với hoạt động phạm tội do đối tượng Vương Huy Long cầm đầu. Tháng 7-2013, trang web giao dịch tiền điện tử mà Long trả tiền cho Dropper đã bị các cơ quan chức năng Mỹ đánh sập, do liên quan đến các hoạt động "rửa tiền". Cho đến khi Cơ quan CSĐT Bộ Công an sang Mỹ phối hợp lấy lời khai của các Dropper này, họ vẫn nghĩ mình đang làm việc cho một công ty hợp pháp, mà không hề biết rằng đã tiếp tay cho hành vi phạm tội của bọn Vương Huy Long. Đến tháng 9/2013, Bộ Công an Việt Nam đã phối hợp với Bộ An ninh nội địa Hoa Kỳ đấu tranh với các đối tượng trong diễn đàn tội phạm mạng với hơn 1.000 thành viên do đối tượng Vương Huy Long cầm đầu, thu giữ 29.000 thông tin thẻ tín dụng được đưa lên diễn đàn, xác định tổng số tài sản các đối tượng này chiếm hưởng trái phép hơn 15 tỷ đồng và 280.000 USD. Cơ quan CSĐT, Bộ Công an Việt Nam đã xác định và trao đổi thông tin về hàng trăm đối tượng trong đường dây tội phạm ở 23 bang của Hoa Kỳ, Vương quốc Anh, Đức cho Cảnh sát các nước. Các đối tượng đã gây thiệt hại cho phía chủ thẻ hàng trăm triệu USD. Chuyên án thành công, được lực lượng cảnh sát các nước đánh giá rất cao, nâng uy tín của Cảnh sát Việt Nam trên trường quốc tế. Đây được coi là vụ án triệt phá đường dây trộm cắp thẻ tín dụng lớn nhất từ trước đến nay để mua hàng, nhằm chiếm đoạt hàng trăm nghìn USD của người nước ngoài.

4.2.1.3. Kết quả công tác dẫn độ, tương trợ tư pháp về hình sự về tội phạm sử dụng công nghệ cao trong tương quan với các loại hình tội phạm khác

- Kết quả công tác dẫn độ trong việc điều tra, truy tố, xét xử và thi hành án:

Trong Báo cáo tổng kết công tác thi hành pháp luật về dẫn độ đối với tội phạm nói chung của Bộ Công an năm 2019, số đối tượng có lệnh truy nã đỏ của Interpol có thông tin lẩn trốn vào Việt Nam là 317 đối tượng, nhưng rất ít trường hợp nước ngoài yêu cầu dẫn độ về TPCNC. Đến năm 2017, Bộ Công an đã tiếp nhận và xử lý 23 yêu cầu dẫn độ của nước ngoài (12 yêu cầu dẫn độ theo các hiệp định song phương về dẫn độ, 11 yêu cầu dẫn độ theo nguyên tắc có đi có lại) và từ chối 03 yêu cầu dẫn độ không hợp lệ. Có khoảng 1.200 đối tượng phạm tội tại Việt Nam bỏ trốn ra nước ngoài, trong đó có 235 đối tượng đã bị INTERPOL ra lệnh truy nã đỏ,

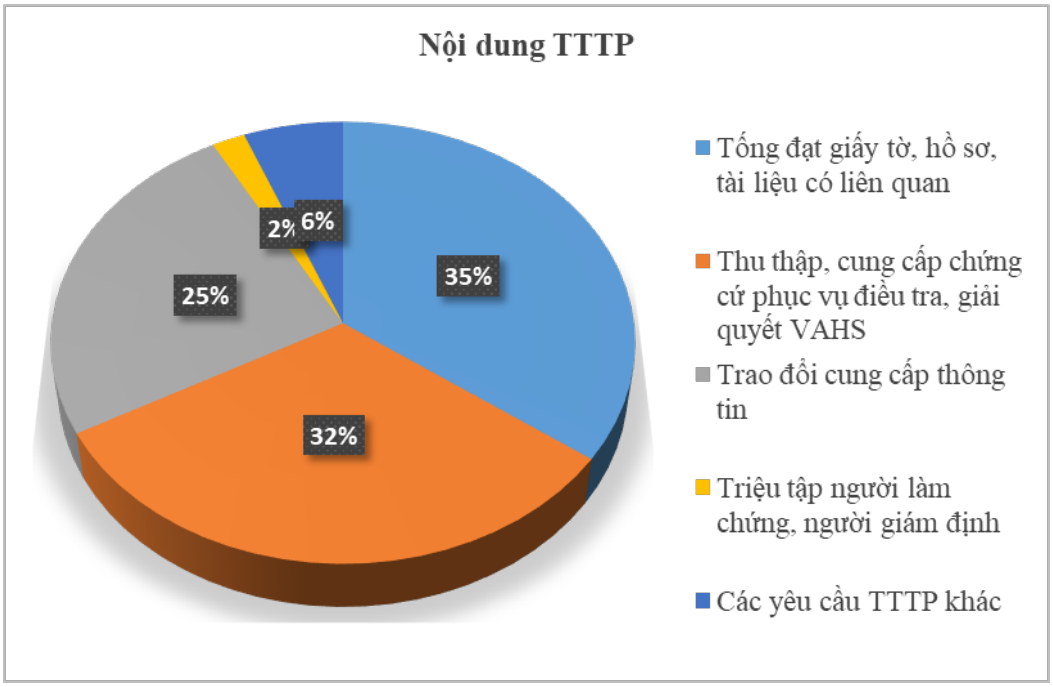
nhiều đối tượng phạm tội đặc biệt nghiêm trọng, trong đó có TPCNC[144]. Bộ Công an đã lập và chuyển 35 hồ sơ yêu cầu dẫn độ đến cơ quan có thẩm quyền của nước ngoài (đến năm 2017), gồm 21 yêu cầu dẫn độ theo các hiệp định song phương và 14 yêu cầu dẫn độ theo nguyên tắc có đi có lại.

- Kết quả tương trợ tư pháp về hình sự trong việc điều tra, truy tố, xét xử:

Trong giai đoạn từ 1/7/2008 đến hết 31/5/2017 thì VKSNDTC đã tiếp nhận 627 yêu cầu TTTPHS của nước ngoài, trong đó Văn phòng Cơ quan CSĐT Bộ Công an thực hiện 512 yêu cầu (chiếm 81,7%), chuyển các cơ quan khác (Bộ ngoại giao, Tòa án, Cục lãnh sự BNG, VKSND…) thực hiện 115 yêu cầu (chiếm 18,3%). Các nội dung yêu cầu TTTP về hình sự mà nước ngoài đề nghị Việt Nam thực hiện chủ yếu là tống đạt giấy tờ, hồ sơ, tài liệu có liên quan.

Cũng trong thời gian trên, các cơ quan có thẩm quyền của Việt Nam (Cơ quan điều tra trong CAND, TAND, VKSND…) đã yêu cầu phía nước ngoài thực hiện tổng số 660 yêu cầu TTTPHS, trong đó phía Cơ quan điều tra trong CAND có 554 yêu cầu (chiếm 83,9%) và các cơ quan khác có thẩm quyền đề nghị 116 yêu cầu (chiếm 16,1%)[145]. Trong đó có khoảng 78% yêu cầu liên quan đến các nước đã ký Hiệp định với Việt Nam. Trong đó, nội dung yêu cầu do cơ quan điều tra trong Công an nhân dân đề nghị nước ngoài thực hiện thì thu thập chứng cứ chiếm 68% và xác minh lý lịch tư pháp chiếm 32%, việc lấy lời khai chiếm 17% trong tổng số nội dung thu thập chứng cứ[146].

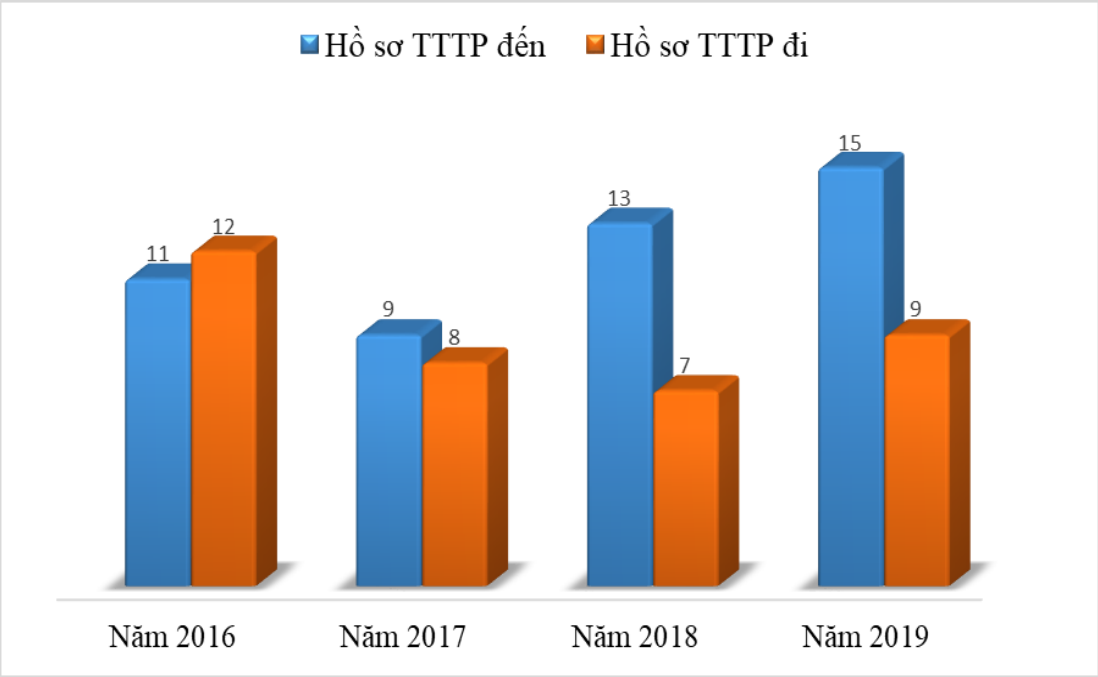
[144] Báo cáo tổng kết thi hành pháp luật về dẫn độ vào năm 2019 của , Bộ Công an
[145] Báo cáo tổng kết thi hành pháp luật về dẫn độ vào năm 2019 của , Bộ Công an
[146] Báo cáo tổng kết thi hành pháp luật về dẫn độ vào năm 2019 của , Bộ Công an



Biểu đồ 4.1. Yêu cầu tương trợ tư pháp về hình sự của nước ngoài[147]

Trong Báo cáo tuân thủ kỹ thuật (Báo cáo TC) và Báo cáo tính hiệu quả (Báo cáo IO) của Việt Nam gửi Hiệp hội phòng chống rửa tiền Châu Á – Thái BÌnh Dương (APG) năm 2019 cho thấy, hoạt động tương trợ tư pháp về hình sự trong đấu tranh đối với tội phạm sử dụng công nghệ cao để thực hiện hành vi rửa tiền giữa Việt Nam với các quốc gia có xu hướng gia tăng trong giai đoạn 2016-2019, cụ thể:

[147] Viện Kiểm sát Nhân dân tối cao (2017), Báo cáo Tổng kết 10 năm triển khai thi hành Luật tương trợ tư pháp năm 2007



Biểu đồ 4.2. Số vụ tương trợ tư pháp về hình sự giữa Việt Nam và các quốc gia đối với tội phạm sử dụng công nghệ cao để rửa tiền[148]

4.2.1.4. Công tác tổ chức hội nghị, hội thảo trao đổi thông tin, kinh nghiệm và phối hợp đào tạo, bồi dưỡng, huấn luyện nghiệp vụ:

Theo cơ cấu, biên chế đến năm 2020 để đơn vị đấu tranh chống TPCNC trên cả nước cần khoảng 2.500 cán bộ, chiến sĩ có trình độ chuyên môn tin học và nghiệp vụ. Trong biên chế của Cục C50 cũ nay là Cục An ninh mạng cần khoảng 500 cán bộ, chiến sĩ. Mỗi địa phương có khoảng 20-40 cán bộ, chiến sĩ. Mỗi cán bộ phải thông thạo ít nhất một ngoại ngữ, tỷ lệ về trình độ chuyên môn tin học và nghiệp vụ là 70/30, bên cạnh đó mục tiêu đào tạo, bồi dưỡng 100% cán bộ, chiến sĩ giỏi về chuyên môn tin học và nắm chắc nghiệp vụ điều tra. Vì vậy, bên cạnh nhu cầu tuyển dụng cán bộ, chiến sĩ trong đấu tranh, phòng chống TPCNC thì cần chú ý đến công tác phát triển cán bộ trực tiếp làm công tác HTQT trong đấu tranh phòng, chống TPCNC vì hiện nay lực lượng này đang thiếu và chưa có lực lượng chuyên trách. Vì vậy, thời gian qua, Bộ Công an đã cử nhiều đoàn đi nghiên cứu và học tập kinh nghiệm ở các nước có nền khoa học CNTT tiên tiến và hiện đại như Mỹ, Nhật, Úc, Hàn Quốc… để trao đổi về công tác đấu tranh phòng, chống TPCNC trong tình hình mới.

[148] Việt Nam (2019), Báo cáo tuân thủ kỹ thuật (Báo cáo TC) và Báo cáo tính hiệu quả (Báo cáo IO).

Bộ Công an Việt Nam với vai trò nòng cốt trong phòng chống tội phạm sử dụng công nghệ cao đã phối hợp với các tổ chức quốc tế, cảnh sát các quốc gia thường xuyên tiến hành các hội nghị, hội thảo về an ninh, an toàn thông tin cũng như phòng chống tội phạm sử dụng công nghệ cao. Năm 2017, Bộ Công an Việt Nam phối hợp cùng Tập đoàn Dữ liệu Quốc tế (IDG), Bộ Thông tin & Truyền thông cùng Ban Cơ yếu Chính phủ tổ chức Hội thảo - Triển lãm Quốc gia về An ninh Bảo mật 2017 (Security World 2017) lần thứ 12 với chủ đề "Bảo đảm an ninh mạng, an ninh thông tin trong thời kỳ cách mạng công nghiệp lần thứ 4". Tại đây, các nhà lãnh đạo Việt Nam đã truyền đi thông điệp: "*...cần có sự chung tay của các nước trong khu vực và thế giới, thông qua cơ chế, khuôn khổ pháp lý song phương, đa phương, thiết lập quan hệ hợp tác chặt chẽ trên lĩnh vực bảo đảm an ninh mạng, phòng chống tội phạm công nghệ cao*".

Đồng thời, Bộ Công an cũng thường xuyên cử lực lượng tham gia các hội nghị, hội thảo do lực lượng INTERPOL quốc tế và các ủy ban của Liên Hợp Quốc tổ chức trong phòng chống tội phạm nói chung và phòng chống tội phạm sử dụng công nghệ cao nói riêng. Minh chứng là vào tháng 01/2019, tại Lyon, Pháp, INTERPOL và Trung tâm Phòng, chống khủng bố của Liên Hợp Quốc (UNCCT) đã phối hợp tổ chức Hội thảo về "*Nâng cao năng lực của các quốc gia thành viên trong việc sử dụng phương tiện truyền thông xã hội để ngăn chặn và chống lại các phần tử khủng bố quốc tế*". Tại Hội nghị có sự tham gia của đại diện INTERPOL Việt Nam và đoàn Việt Nam cũng có bài tham luận tại Hội thảo này. Bài hội thảo đã được cảnh sát các nước đánh giá cao về các kinh nghiệm và thành công của Việt Nam trong ngăn chặn và chống lại các phần tử khủng bố quốc tế;

Ngoài ra, với đầu mối trao đổi thông tin về tội phạm quốc tế, Văn phòng INTERPOL Việt Nam đóng vai trò cung cấp cảnh báo của các tổ chức cảnh sát, an ninh quốc gia cũng như quốc tế trong phòng chống TPCNC. Đầu năm 2020, khi INTERPOL quốc tế ban hành một cảnh báo cho các tổ chức đang ở tuyến đầu phòng, chống dịch có nguy cơ trở thành mục tiêu của các vụ tấn công bằng mã độc nhằm đòi tiền chuộc. Tội phạm công nghệ cao đang sử dụng mã độc để kiểm soát về mặt kỹ thuật số các bệnh viện và các dịch vụ y tế, khống chế không cho họ truy cập vào các hồ sơ và hệ thống cho đến khi trả một khoản tiền chuộc nhất định. Để đối phó với mối đe dọa này, INTERPOL đã ban hành một Thông báo tím cảnh báo Cảnh sát ở khắp 194 quốc gia thành viên về thủ đoạn tấn công bằng mã độc này[149].

[149] *Tội phạm công nghệ cao nhằm vào các cơ sở y tế trọng yếu để đòi tiền chuộc*; http://bocongan.gov.vn/interpol/Pages/list.aspx?Cat=3&ItemID=207 (truy cập lần cuối 20/12/2020)

Dựa vào cảnh báo này, các cơ quan thực thi pháp luật của Việt Nam đã tăng cường các biện pháp để phòng ngừa và ngăn chặn TPCNC vào các cơ sở y tế trọng điểm của Việt Nam.

4.2.2. Hạn chế trong hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao

4.2.2.1. Vướng mắc, hạn chế từ quy định của Luật Tương trợ tư pháp lien quan đến hợp tác quốc tế phòng chống tội phạm sử dụng công nghệ cao

Sau gần 15 năm áp dụng Luật TTTP, một số quy định trong Luật TTTP chưa tương thích hoặc chưa có quy định, trong đó có nhiều nội dung phức tạp, nhạy cảm, dẫn đến khó khăn trong việc triển khai tổ chức thực hiện các hoạt động HTQT phòng chống tội phạm nói chung và TPCNC nói riêng, cụ thể:

Quy định liên quan đến dẫn độ

Về cơ quan Trung ương của Việt Nam. Theo 11 Hiệp định TTTP có quy định về dẫn độ mà Việt Nam ký với các quốc gia trước đây, VKSNDTC là cơ quan đầu mối về dẫn độ của Việt Nam. Nhưng Luật TTTP lại quy định Bộ Công an là cơ quan đầu mối về dẫn độ, chuyển giao người đang chấp hành hình phạt tù. Sự không thống nhất này đã gây khó khăn cho quá trình thực hiện chức năng của Bộ Công an trong dẫn độ. Vì muốn thay đổi cơ quan trung ương của Việt Nam về dẫn độ thì phải sửa đổi các Hiệp định. Nên thời gian tới Việt Nam sẽ tách các nội dung về dẫn độ thành một Hiệp định riêng và kí lại với các quốc gia.

Về vấn đề cam kết không áp dụng án tử hình. Một số Hiệp định về dẫn độ giữa Việt Nam và các nước có quy định về cam kết không áp dụng án tử hình (như Hiệp định với Cộng hòa Bê-la-rút (Điều 70), với Nga và Austraylia…), theo đó, việc dẫn độ sẽ bị từ chối trong trường hợp tội phạm bị yêu cầu dẫn độ bị án tử hình theo pháp luật của Bên ký kết yêu cầu, nhưng bên ký kết yêu cầu không đảm bảo chắc chắn cho bên ký kết được yêu cầu rằng sẽ không thi hành bản án tử hình đó. Pháp Luật Việt Nam vẫn còn quy định nhiều loại tội phạm có quy định hình phạt tử hình và không hạn chế việc dẫn độ đối với người có thể bị kết án tử hình. Điều này gây khó khăn cho Việt Nam khi đàm phán các Hiệp định về dẫn độ với các quốc gia châu Âu (nơi mà pháp luật tại nhiều quốc gia không có án tử hình). Vì vậy, thời gian tới, cần nghiên cứu bổ sung quy định về cam kết không áp dụng thủ tục hình phạt tử hình với người bị yêu cầu dẫn độ.

Hiện nay, Luật TTTP mới chỉ quy định trường hợp từ chối dẫn độ để truy cứu trách nhiệm hình sự, cụ thể, VKSNDTC xem xét yêu cầu của cơ quan có thẩm quyền của nước ngoài về việc tiếp tục truy cứu trách nhiệm hình sự đối với công dân Việt

Nam phạm tội ở nước ngoài đang có mặt tại Việt Nam[150]. Như vậy, quy định của Luật TTTP đã bỏ lọt trường hợp từ chối dẫn độ phạm nhân (hoặc người đã bị kết án bằng bản án hình sự có hiệu lực pháp luật) bỏ trốn để tiếp tục thi hành án hình sự. Như vậy, khi có yêu cầu với trường hợp này, Việt Nam phải từ chối dẫn độ. Tuy nhiên, Việt Nam cũng không thể truy cứu trách nhiệm hình sự của người bị yêu cầu dẫn độ vì không ai bị kết án hai lần vì một tội danh. Điều này đã được Bộ luật TTHS năm 2015 quy định về cho thi hành bản án, quyết định hình sự của Tòa án nước ngoài đối với công dân Việt Nam bị từ chối dẫn độ. Nên cần phải sửa đổi Luật TTTP sao cho phù hợp với quy định trong Bộ luật TTHS 2015 nhằm tránh bỏ lọt tội phạm.

Quy định liên quan đến thực hiện công tác chuyển giao người đã bị kết án phạt tù

Về thời hạn còn lại phải chấp hành án của người được chuyển giao. Luật TTTP quy định người bị kết án phạt tù còn phải chấp hành ít nhất 01 năm, trong trường hợp đặc biệt còn ít nhất 06 tháng. Tuy nhiên, trong hầu hết các Hiệp định song phương về chuyển giao người bị kết án phạt tù mà Việt Nam đã ký kết đều quy định người bị kết án phạt tù còn phải chấp hành ít nhất 01 năm hoặc do các bên thống nhất.

Cần có sự đồng ý của người bị kết án phạt tù còn nhiều vướng mắc. Hiện nay Luật TTTP quy định người đang chấp hành hình phạt tù ở nước ngoài có thể được tiếp nhận về Việt Nam để thi hành hình phạt tù thì cần phải có sự đồng ý của người được chuyển giao[151]. Như vậy, trong trường hợp nhiều người Việt Nam phạm tội ở nước ngoài (đặc biệt là phạm tội liên quan đến ma túy) sẽ không muốn về Việt Nam để thi hành hình phạt tù. Điều này dẫn đến trường hợp khi quốc gia hữu quan đề nghị chuyển giao công dân Việt Nam phạm tội tại nước ngoài về Việt Nam sẽ khó thực thi và cần có hướng kí văn bản thỏa thuận riêng. Bên cạnh đó, trong một số trường hợp phía nước ngoài đề nghị Việt Nam cam kết không tuyên hình phạt tử hình hoặc có tuyên nhưng không thi hành hình phạt tử hình đối với người đang chấp hành án phạt tù đồng thời là đối tượng truy nã của Việt Nam sau khi được chuyển giao về Việt Nam. Tuy nhiên, pháp luật Việt Nam chưa có quy định này.

Về chi phí, Luật TTTP quy định chi phí về chuyển giao người đang chấp hành hình phạt tù do Bên yêu cầu chi trả[152]. Nhưng các Hiệp định TTTP Việt Nam đã kí lại quy định là chi phí do Bên nhận chi trả trừ chi phí phát sinh hoàn toàn trong lãnh

[150] Điều 29 Luật TTTP
[151] Điểm g Khoản 1 Điều 50 Luật TTTP năm 2007
[152] Điều 60 Luật TTTP 2007

thổ Bên chuyển giao. Ví dụ, trong Hiệp định giữa Nhật Bản và Việt Nam về chuyển giao người bị kết án phạt tù có quy định rằng: Chi phí phát sinh trong việc áp dụng Hiệp định này sẽ do Bên nhận chi trả trừ những chi phí phát sinh hoàn toàn trong phạm vi lãnh thổ của Bên chuyển giao hay trong hiệp định giữa Việt Nam và cộng hòa Séc cũng quy định tương tự như trên. Như vậy, khi Việt Nam là bên nhận mà Việt Nam chưa có nguồn kinh phí cho các hoạt động tiếp nhận phạm nhân là người Việt Nam đang chấp hành hình phạt tù tại nước ngoài về Việt Nam tiếp tục chấp hành hình phạt tù thì lúc này việc tiến hành chuyển giao sẽ không được tiếp tục, trừ khi có thỏa thuận khác giữa Việt Nam và bên chuyển giao.

Quy định thực hiện công tác TTTP về hình sự

Để thực hiện yêu cầu TTTP, các nước yêu cầu không áp dụng án tử hình. Tuy nhiên, Luật TTTP chưa có quy định về trình tự, thủ tục cam kết không áp dụng hình phạt tử hình trong hoạt động TTTP về hình sự.

Phạm vi TTTP về hình sự quy định tại Điều 17 Luật TTTP còn hạn chế, chưa phù hợp với các cam kết quốc tế của Việt Nam. Luật TTTP vẫn chưa có quy định về việc cho phép người tiến hành tố tụng của Bên yêu cầu được tham gia một số hoạt động trong quá trình thực hiện TTTP tại Bên được yêu cầu, tổ chức cho người tại Bên được yêu cầu đến Bên yêu cầu để hỗ trợ điều tra hoặc cung cấp chứng cứ, liên kết điều tra, phối hợp điều tra…đây là những nội dung được quy định trong các điều ước quốc tế song phương và đa phương trong lĩnh vực tư pháp hình sự mà Việt Nam đã ký kết và tham gia và đã phát sinh trên thực tiễn.

Chưa có quy định cụ thể về trình tự, thủ tục thực hiện một số yêu cầu tương trự như triệu tập người làm chứng, người giám định, dẫn giải người chấp hành hình phạt tù ra nước ngoài để hỗ trợ điều tra hoặc cung cấp chứng cứ; chuyển giao truy cứu trách nhiệm hình sự công dân Việt Nam tại Việt Nam….

4.2.2.2. Khó khăn từ thực tiễn áp dụng pháp luật trong đấu tranh, phòng chống tội phạm sử dụng công nghệ cao

Một là, việc hợp tác quốc tế trong trao đổi thông tin về TPCNC còn chưa đầy đủ. Mặc dù giữa Việt Nam và nhiều quốc gia đã xây dựng được kênh liên lạc trực tiếp, nhưng các kênh này chỉ thực hiện khi có yêu cầu giải quyết cụ thể, do đó dẫn đến không chủ động trong công tác đấu tranh phòng, chống TPCNC. Ngoài ra, vấn đề bất đồng ngôn ngữ cũng là nguyên nhân khiến việc tiếp xúc, trao đổi thông tin còn gặp nhiều khó khăn. Các tài liệu trong hồ sơ yêu cầu TTTP về hình sự có những bản dịch chưa đúng từ ngữ pháp luật, chưa logic về mặt ngữ pháp, gây khó hiểu cho cơ quan thụ lý thực hiện. Tên đối tượng hoặc tên địa chỉ khi không rõ ràng nên

không xác định con người cụ thể, mất thời gian hoặc không xác định được để gửi lại thông tin cho Bên yêu cầu.

Ngoài ra, việc tiếp nhận thông tin yêu cầu phối hợp qua "đường dây nóng" được một số quốc gia như Trung Quốc, các quốc gia ASEAN… triển khai có hiệu quả, tuy nhiên, trong một số vụ việc, Công hàm, Lệnh truy nã, Lệnh tạm giam được chuyển chậm, gây khó khăn cho hoạt động phối hợp xác minh, điều tra, truy bắt tội phạm.

Trong lĩnh vực phòng, chống TPCNC, công tác phối hợp, trao đổi, cung cấp thông tin giữa các cơ quan phòng, chống tội phạm các nước còn chậm, không đầy đủ trong khi TPCNC diễn ra rất nhanh, các đối tượng sau khi rút tiền sẽ nhanh chóng tẩu thoát do đó kết quả đấu tranh với tội phạm này vẫn còn nhiều hạn chế. Đặc biệt, việc thu thập, xác minh địa chỉ IP để xác định vị trí, địa điểm, đối tượng hoạt động gặp rất nhiều khó khăn và kéo dài.

Hai là, *việc hợp tác với các cơ quan thực thi pháp luật nước ngoài thường bị kéo dài*. Nguyên nhân của việc kéo dài là do thông tin về tội phạm muốn trao đổi với cơ quan có thẩm quyền nước ngoài phải báo cáo qua nhiều cấp có thẩm quyền dẫn đến chậm, không còn tính chiến đấu. Hay có những yêu cầu TTTP từ phía nước bạn yêu cầu Việt Nam với những tên văn bản đi kèm lệnh, quyết định đó không có hiệu lực thi hành trên lãnh thổ Việt Nam nên cần thời gian để cơ quan tiến hành tố tụng Việt Nam triển khai bằng các văn bản, quyết định theo quy định của pháp luật trong nước. Việc này cũng làm chậm quá trình điều tra vụ án TPCNC. Ngoài ra, việc chậm có kết quả yêu cầu TTTP về hình sự còn có nguyên nhân là các Hiệp định mà Việt Nam đã ký với các nước chưa quy định rõ thời hạn thực hiện yêu cầu TTTP về hình sự, mà thời hạn này phụ thuộc vào pháp luật quốc gia được yêu cầu. Nên từ việc chậm có kết quả thực hiện yêu cầu tương trợ ảnh hưởng đến tiến độ giải quyết vụ án.

Công tác phối hợp tổ chức hội đàm, trao đổi giữa Bộ Công an Việt Nam với cơ quan an ninh, cảnh sát các quốc gia khác còn hạn chế, chỉ thực hiện ở một số địa bàn, lĩnh vực và thời điểm. Công an cấp tỉnh (các phòng nghiệp vụ) có chung đường biên giới với Trung Quốc, Lào, Campuchia ít có điều kiện tổ chức hội đàm, trao đổi trực tiếp đã ảnh hưởng đến công tác phòng ngừa và đấu tranh phòng, chống TPCNC giữa các bên có chung đường biên giới.

Ba là, *các quy định của luật chưa dự báo điều chỉnh hết các trường hợp sẽ phát sinh và chưa phù hợp với điều kiện tại Việt Nam*. Như quy định về dẫn độ, khi mà TPCNC có hành vi được thực hiện tại nhiều quốc gia hay tội phạm do tổ chức

tội phạm xuyên quốc gia thực hiện, thì sẽ dẫn đến trường hợp Bộ Công an nhận được văn bản của hai hoặc nhiều nước yêu cầu dẫn độ một người về cùng một tội phạm hoặc nhiều tội phạm khác nhau thì Bộ Công an chủ trì phối hợp với Bộ Ngoại giao, Bộ Tư pháp, VKSNDTC, TANDTC xem xét, quyết định đáp ứng yêu cầu dẫn độ cho một trong các nước yêu cầu và chuyển hồ sơ yêu cầu dẫn độ cho Tòa án nhân dân cấp tỉnh xem xét, quyết định dẫn độ[153]. Tuy nhiên, trên thực tế, các yêu cầu dẫn độ của các nước khác nhau thường không được gửi đến Bộ Công án cùng một thời điểm. Mà thời hạn yêu cầu kiểm tra hồ sơ trong 20 ngày, nên sẽ có trường hợp Bộ Công an gửi đến TAND cấp tỉnh có thẩm quyền để thụ lý, giải quyết thì Bộ Công an lại nhận được yêu cầu dẫn độ tại quốc gia thứ hai. Trường hợp này, TAND cấp tỉnh đã thụ lý yêu cầu dẫn độ thứ nhất phải trả lại hồ sơ cho Bộ Công an để xem xét, quyết định việc đáp ứng yêu cầu. Nhưng Luật chưa quy định việc trả hồ sơ yêu cầu dẫn độ sau khi đã thụ lý. Nên điều này sẽ mất thời gian và gây lãng phí, chưa kể đến có nhiều hơn hai nước yêu cầu dẫn độ cùng một người thì cần có cách giải quyết phù hợp.

Bốn là, vẫn còn hiện tượng né tránh, đùn đẩy trách nhiệm của các lực lượng thực thi pháp luật tại Việt Nam trong việc xử lý các vụ việc có yếu tố nước ngoài nói chung và các vụ việc có dấu hiệu VPPL hình sự liên quan đến việc sử dụng công nghệ cao nói riêng liên quan đến áp dụng ĐƯQT về phòng chống tội phạm mà Việt Nam là thành viên. Nhiều trường hợp, Công an các đơn vị địa phương nhận được thông tin đối tượng phạm tội đã bỏ trốn ra nước ngoài thì cơ quan điều tra ngay lập tức đình chỉ điều tra và đóng hồ sơ mà không có cơ sở pháp lý trong nước; hoặc chuyển cho cơ quan truy nã hoặc đơn vị hợp tác quốc tế thực hiện việc áp dụng ĐƯQT… Khi Công an một số đơn vị, địa phương cho rằng thủ tục liên quan đến TTTP về hình sự, yêu cầu dẫn độ, yêu cầu chuyển giao người bị kết án phạt tù quá phức tạp nên không thực hiện các thủ tục này, dẫn đến bỏ lọt tội phạm hoặc không bảo vệ được quyền lợi hợp pháp của các bên liên quan hay của người bị kết án phạt tù[154].

Năm là, các chế tài và hình phạt xử lý tội phạm sử dụng công nghệ cao còn nhẹ, chưa đủ sức răn đe phục vụ công tác đấu tranh, phòng ngừa tội phạm. Tại Việt Nam, theo Cục Cảnh sát PCTP sử dụng công nghệ cao (C50) nay được đổi tên thành Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05)

[153] Điều 39 Luật TTTP 2007

[154] Nguyễn Thị Quế Thu (2017), Điều ước quốc tế- Lý luận và thực tiễn áp dụng điều ước quốc tế về phòng, chống tội phạm tại Việt nam, Sách chuyên khảo, Nxb Công an nhân dân.

trực thuộc Bộ Công an, từ năm 2010 đến tháng 6/2014 lực lượng Cảnh sát PCTP sử dụng công nghệ cao trên cả nước đã phát hiện và xác minh 11.476 đầu mối vụ việc có dấu hiệu VPPL liên quan đến yếu tố công nghệ cao với 3.220 đối tượng, trong đó 823 vụ việc và 1.990 đối tượng là do C50 phát hiện; 450 vụ việc và 1.230 đối tượng là do Công an các địa phương phát hiện; tổng thiệt hại do loại tội phạm trong lĩnh vực này gây ra lên tới hàng chục ngàn tỷ đồng. Nhưng số vụ án các loại này đưa ra xét xử rất ít. Đây cũng là nguyên nhân mà cơ quan lập pháp bổ sung các điều luật quy định về loại tội phạm sử dụng công nghệ cao trong BLHS năm 2015, sửa đổi, bổ sung năm 2017. Do mới được ban hành nên số lược vụ án hình sự được xét xử tại Tòa án về loại tội phạm sử dụng công nghệ cao chiếm tỷ trọng ít so với các vụ án hình sự khác.

Sáu là, công tác tuyên truyền, phổ biến giáo dục, pháp luật chưa được quan tâm đúng mức dẫn đến nhiều người dân biết các đối tượng nước ngoài mượn, thuê địa điểm với mục đích không minh bạch nhưng vẫn chấp nhận cho thuê hoặc đối với các quốc gia có chung biên giới, việc tuần tra, kiểm soát bảo vệ đường biên giới chưa được thường xuyên, trong bối cảnh tình hình bất ổn chính trị, kinh tế thế giới, khu vực tác động lên một số nhân dân biên giới bị tội phạm dụ dỗ, lừa gạt, mua chuộc… tham gia hoạt động phạm tội.

4.3. Giải pháp hoàn thiện pháp luật và nâng cao hiệu quả hợp tác quốc tế trong đấu tranh phòng, chống tội phạm công nghệ cao của Việt Nam

4.3.1. Giải pháp hoàn thiện pháp luật Việt Nam về đấu tranh phòng chống tội phạm công nghệ cao

Thứ nhất, về mặt văn bản pháp luật cần thiết phải có những quy định rõ ràng, cụ thể về việc thu thập, kiểm tra, đánh giá chứng điện tử cũng như ban hành văn bản hướng dẫn về đường lối xử lý đối với các TPCNC trong Bộ luật hình sự năm 2015, sửa đổi, bổ sung năm 2017. Ngoài ra, cần có quy định chặt chẽ về trách nhiệm thậm chí là chế tài xử lý đối với cá nhân, tổ chức (cơ quan thứ 3) trong việc chậm trễ cung cấp dữ liệu điện tử, giám định dữ liệu điện tử làm ảnh hưởng tới tiến trình giải quyết vụ án. Điều này xuất phát từ việc trong hệ thống pháp luật hiện hành, dữ liệu điện tử vừa được quy định trong Luật giao dịch điện tử năm 2006 nhưng với tư cách là một nguồn chứng cứ, dữ liệu điện tử cũng được ghi nhận trong Bộ luật Tố tụng hình sự 2015 tại các Điều 87, 88, 99, 107. Ngoài ra khoản 3 Điều 223 Bộ luật Tố tụng hình sự cũng đề cập đến việc "thu thập bí mật dữ liệu điện tử" với tư cách là một biện pháp điều tra tố tụng đặc biệt. Hiện tại, chưa có văn bản dưới luật hướng dẫn chi tiết về vấn đề này. Bên cạnh các quy định đặc thù về thu

thập phương tiện điện tử, dữ liệu điện tử (Điều 107), các nội dung khác như: việc kiểm tra, đánh giá, bảo quản, niêm phong.... đối với chứng cứ điện tử được thực hiện theo quy định chung hiện hành. Tuy nhiên, chứng cứ điện tử có những đặc điểm khác biệt với các chứng cứ truyền thống cần phải có những quy định chặt chẽ của pháp luật về quy trình thu giữ và phục hồi đối với loại chứng cứ này nhằm bảo vệ tính toàn vẹn của dữ liệu, giữ nguyên giá trị chứng cứ của dữ liệu; cũng như quy định về trách nhiệm của các cá nhân trong việc sử dụng, bảo quản loại chứng cứ đặc thù này; đặc biệt là đối với việc "thu thập bí mật dữ liệu điện tử" còn liên quan đến quyền con người, quyền công dân. Việc chưa có hướng dẫn cụ thể dẫn đến việc cơ quan điều tra đang áp dụng một cách tùy nghi, tương tự.

Bên cạnh đó, trong các quy định của Bộ luật Tố tụng hình sự cũng đã bộc lộ những điểm chưa thống nhất, cụ thể: Điều 107 Bộ luật Tố tụng hình sự 2015 quy định về việc thu thập phương tiện điện tử, dữ liệu điện tử nhưng tại khoản 1 của Điều luật này lại quy định "phương tiện điện tử phải được thu giữ kịp thời, đầy đủ…" và "trường hợp không thể thu giữ phương tiện lưu trữ điện tử thì cơ quan có thẩm quyền tiến hành tố tụng sao lưu dữ liệu điện tử đó…". Có thể thấy, dường như nhà làm luật đang đồng nhất khái niệm "thu thập phương tiện điện tử" và "thu giữ phương tiện điện tử". Bởi vì chúng ta chỉ nên đặt ra vấn đề thu thập đối với dữ liệu điện tử vì dữ liệu điện tử mới là một nguồn chứng cứ, còn phương tiện điện tử chỉ là nơi mà dữ liệu điện tử được chứa đựng. Đây cũng cần các cơ quan có thẩm quyền quan tâm khắc phục để nâng cao hiệu quả đấu tranh phòng chống TPCNC.

Theo cách tiếp cận của Interpol, tội phạm công nghệ cao được phân chia thành 3 loại: *tấn công phần cứng và phần mềm máy tính* (ví dụ: phần mềm độc hại và xâm nhập mạng…); *tội phạm tài chính* (ví dụ: lừa đảo trực tuyến, xâm nhập của các dịch vụ tài chính trực tuyến và lừa đảo); *lạm dụng, đặc biệt là những trẻ em* (ví dụ: truyền bá ảnh, phim đồi trụy, khiêu dâm về trẻ em trên mạng). Nhưng trong pháp luật Việt Nam hiện nay mới chỉ đang điều chỉnh TPCNC về tấn công phần cứng và phần mềm máy tính và tội phạm tài chính, còn loại TPCNC về lạm dụng trẻ em thì đang nằm rải rác trong các văn bản pháp luật khác với các chế tài chưa tương xứng với tính chất, mức độ nguy hiểm của hành vi tội phạm này. Vì vậy, cũng cần thiết phải bổ sung thêm tội danh về lạm dụng trẻ em trong nhóm các TPCNC của Bộ luật hình sự.

Thứ hai, những người tiến hành tố tụng cần nâng cao kiến thức cơ bản về dữ liệu điện tử, về CNTT (am hiểu nhất định về đối tượng đang được khai thác)... Để làm tốt điều đó, cần xác định phương hướng cho hoạt động thu thập dữ liệu điện tử

đó là: (i) Phải xuất phát từ những thông tin, tài liệu, chứng cứ ban đầu về vụ án đã thu thập được, đây là cơ sở đầu tiên giúp cho cơ quan có thẩm quyền xác định phương hướng thu thập dữ liệu điện tử; (ii) Xuất phát từ quy luật dấu vết điện tử có điểm riêng biệt so với dấu vết hình sự khác, căn cứ vào nguồn gốc hình thành và đặc điểm của vật mang dấu vết điện tử (phương tiện điện tử, mạng máy tính, mạng viễn thông hoặc trên đường truyền); (iii) Quy luật hoạt động của các đối tượng phạm tội đối với các hệ, loại đối tượng là khác nhau, chẳng hạn như: Quy luật hoạt động của các đối tượng sử dụng công nghệ cao xâm phạm an ninh quốc gia sẽ có những điểm đặc trưng so với quy luật hoạt động của các đối tượng sử dụng CNTT để hoạt động lừa đảo chiếm đoạt tài sản....

Thứ ba, cần thiết phải có những tổng kết khoa học và thực tiễn về thu thập, đánh giá, sử dụng chứng cứ điện tử trong các vụ án hình sự. Mặt khác, dữ liệu điện tử là nguồn chứng cứ phi truyền thống, tồn tại trên không gian mạng, sự tồn tại đó có thể vượt ra khỏi phạm vi của một quốc gia và loại tội phạm để lại dấu vết này cũng thường mang tính chất xuyên quốc gia. Do vậy, cơ quan có thẩm quyền cần tăng cường hợp tác quốc tế trong đấu tranh với loại tội phạm này.

4.3.2. Hoàn thiện pháp luật Việt Nam trong hợp tác quốc tế trong đấu tranh phòng, chống tội phạm công nghệ cao

Hiện nay, Luật TTTP 2007 điều chỉnh nhiều hoạt động hợp tác quốc tế trong đấu tranh, phòng chống tội phạm, trong khi đó mỗi lĩnh vực có những đặc thù riêng. Trong thời gian qua, Bộ Công an nhiều lần trao đổi với Bộ Tư pháp đề nghị báo cáo Chính phủ về việc sửa đổi Luật TTTP theo hướng tách thành 04 luật riêng điều chỉnh các lĩnh vực TTTP về dân sự, TTTP về hình sự, dẫn độ và chuyển giao người bị kết án phạt tù là phù hợp với chỉ đạo của Bộ Chính trị tại Nghị quyết số 48-NQ/TW. Từ sự lúng túng của các cơ quan tiến hành tố tụng, mặc dù Bộ luật TTHS năm 2015 (có hiệu lực từ ngày 01/1/2018) đã có những quy định cụ thể hơn về các nội dung HTQT trong tố tụng hình sự. Tuy nhiên, cần có những hướng dẫn cụ thể để áp dụng trên thực tiễn. Lấy Luật TTHS làm văn bản luật gốc, có tính định hướng để xây dựng các đạo luật mang tính chuyên biệt như Luật TTTP về hình sự, Luật dẫn độ.

- *Về công tác dẫn độ:* Quốc hội sớm ban hành đạo luật chuyên biệt về dẫn độ trên cơ sở tách quy định về dẫn độ trong Luật TTTP năm 2007. Đạo luật về dẫn độ cần bảo đảm các yêu cầu về chính trị, ngoại giao, pháp luật; nội luật hoá các quy định của ĐƯQT về dẫn độ mà Việt Nam đã ký kết hoặc tham gia; đồng bộ hoá các quy định về dẫn độ giữa đạo luật về dẫn độ với các quy định của pháp luật liên

quan, nhất là trong BLHS và BLTTHS; xây dựng cơ chế phối hợp hiệu quả trong hoạt động dẫn độ và xác định, phân định lại cơ quan quản lý nhà nước về dẫn độ; bảo đảm các điều kiện về cơ sở vật chất và bố trí cán bộ làm công tác dẫn độ... Đồng thời, Nhà nước cần tiếp tục đàm phán, ký kết và triển khai thực hiện có hiệu quả các hiệp định hợp tác song phương về dẫn độ; trong đó, ưu tiên đàm phán, ký kết với các quốc gia là đối tác chiến lược toàn diện, đối tác chiến lược, đối tác toàn diện, các nước có truyền thống quan hệ lịch sử và thiện chí với Việt Nam và các nước có yêu cầu hợp tác đấu tranh phòng, chống tội phạm với Việt Nam. Ngoài ra, các cơ quan có thẩm quyền cần tăng cường áp dụng nguyên tắc có đi có lại trong giải quyết vụ việc dẫn độ khi Việt Nam chưa ký kết hiệp định hợp tác song phương về dẫn độ với nước ngoài, tránh việc người phạm tội lợi dụng "kẽ hở" của pháp luật và trong hợp tác quốc tế để trốn tránh sự trừng phạt của pháp luật dẫn đến bỏ lọt tội phạm...

- *Về tương trợ tư pháp về hình sự:* thực tiễn thực hiện các yêu cầu TTTP hình sự cho thấy hiện tượng do pháp luật TTTP hình sự Việt Nam chưa có quy định về sự tham gia của người tiến hành tố tụng tại nước được yêu cầu, các quy định hỗ trợ điều tra hoặc cung cấp chứng cứ, liên kết, phối hợp điều tra; chưa quy định cụ thể trong việc phong tỏa, kê biên, thu giữ, tịch thu và xử lý tài sản do phạm tội mà có…[155] dẫn đến hệ quả là thiếu cơ sở để đáp ứng các yêu cầu TTTP hình sự của nước ngoài, nhưng nếu không thực hiện thì Việt Nam đi ngược với các nghĩa vụ mà mình cam kết. Vì vậy, việc bổ sung các nội dung như: xác minh, giải quyết tin báo, tố giác tội phạm; liên kết điều tra, phối hợp điều tra; quy định cho phép sử dụng các phương tiện kỹ thuật áp dụng công nghệ cao (thư điện tử, fax...) trong việc gửi, tiếp nhận hồ sơ ủy thác tư pháp và thực hiện một số hoạt động TTTP[156]...là cần thiết. Ngoài ra quy định về trường hợp từ chối thực hiện ủy thác tư pháp về hình sự của nước ngoài tại Điều 21 Luật TTTP 2007 sẽ giới hạn trường hợp TTTP tại khoản 6 Điều 17 Luật TTTP 2007, nên nhu cầu loại bỏ khoản 2, 3 Điều 21 cũng cần được quan tâm khi xây dựng Luật mới hoặc ban hành Luật sửa đổi, bổ sung Luật TTTP 2007. Cần xem xét sửa đổi, bổ sung căn cứ từ chối TTTP theo hướng phân biệt giữa những trường hợp "bắt buộc" phải từ chối và "có thể" từ chối.

Năm 2018, VKSNDTC đã tổ chức xây dựng và thực hiện Đề án cải cách tư pháp *"Thực tiễn thi hành và kiến nghị hoàn thiện quy định của pháp luật về tương*

---

[155] Viện kiểm sát nhân dân tối cao, Vụ 13 (2017), Chuyên đề "*Thực trạng và giải pháp hoạt động TTTP về hình sự; Một số kiến nghị, sửa đổi, bổ sung Luật TTTP năm 2007"*, Hà Nội, tr.34

[156] Viện kiểm sát nhân dân tối cao, Vụ 13 (2017), Chuyên đề, tr.34

trợ tư pháp hình sự đáp ứng nhu cầu cải cách tư pháp". Vì vậy, xây dựng Luật Tương trợ tư pháp về hình sự tách khỏi Luật TTTP 2007 vừa là xu thế vừa là nhu cầu thực tiễn.

- *Về hoạt động chuyển giao người đang chấp hành án phạt tù,* trong thời gian tới, các cơ quan có thẩm quyền cần cần sớm ban hành 01 đạo luật riêng biệt về chuyển giao người đang chấp hành án phạt tù trên cơ sở tách từ Luật TTTP năm 2007 để phân biệt rõ giữa các hoạt động mang bản chất nhân đạo với các hoạt động mang tính cưỡng chế cao như dẫn độ, TTTP về hình sự của Luật TTTP hiện hành. Các nội dung quy định trong dự thảo Luật chuyển giao người đang chấp hành án phạt tù sẽ tạo cơ sở pháp lý mới đầy đủ, toàn diện hơn trong việc thực hiện chuyển giao người đang chấp hành án phạt tù ở Việt Nam, góp phần bảo đảm chính sách nhân đạo của Đảng và Nhà nước CHXHCN Việt Nam, bảo đảm hiệu quả công tác thi hành án hình sự và tái hoà nhập xã hội thành công.. Đồng thời, cần tăng cường đàm phán, ký kết ĐƯQT về chuyển giao người đang chấp hành án phạt tù với các quốc gia và vùng lãnh thổ nơi có nhiều công dân Việt Nam đang làm việc, sinh sống, lao động, học tập hoặc các quốc gia có nhiều công dân hiện đang sinh sống, làm việc tại Việt Nam; các quốc gia láng giềng có chung đường biên giới trên đất liền, trong cùng ASEAN... Mặt khác cũng cần tiến hành khảo sát, thống kê, đánh giá thực trạng, tình hình người Việt Nam đang chấp hành án tại nước ngoài và nhu cầu được chuyển giao về Việt Nam để tiếp tục chấp hành án. Đồng thời, khảo sát khả năng đáp ứng yêu cầu tiếp nhận của các trại giam tại Việt Nam trong trường hợp tất cả các công dân Việt Nam đang chấp hành án tại nước ngoài mong muốn được trở về Việt Nam để chấp hành án.

4.3.3. Nhóm giải pháp nâng cao hiệu quả hợp tác quốc tế phòng chống tội phạm sử dụng công nghệ cao

4.3.3.1. Giải pháp chung

Các cơ quan có thẩm quyền của Việt Nam cần tiếp tục mở rộng quan hệ đối ngoại và tăng cường hợp tác quốc tế về phòng, chống tội phạm sử dụng công nghệ cao. Việc mở rộng hợp tác quốc tế về an toàn thông tin trong đó có nội dung phòng chống TPCNC phải trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với pháp luật Việt Nam và điều ước quốc tế mà Việt Nam tham gia ký kết;

Nhà nước cần huy động sức mạnh của cả hệ thống chính trị, tăng cường sự lãnh đạo của cấp ủy đảng, hiệu quả quản lý, điều hành của chính quyền, phát huy vai trò của Mặt trận Tổ quốc, các đoàn thể quần chúng các cấp trong công tác phòng, chống TPCNC. Hiện nay, cơ bản hợp tác quốc tế chỉ diễn ra trên mặt trận

ngoại giao nhà nước mà chưa phát huy được mặt trận đối ngoại Đảng và đối ngoại nhân dân trong trao đổi về CNTT và phòng chống TPCNC. Đồng thời, tăng cường công tác kiểm tra, giám sát, phát hiện và xử lý đối với tổ chức, cá nhân vi phạm quy định về trách nhiệm phòng, chống TPCNC, không để các đối tượng nước ngoài lợi dụng để thực hiện các hành vi phạm tội sử dụng công nghệ cao trên lãnh thổ Việt Nam như thời gian qua.

Nhà nước từng bước nâng cao năng lực phòng, chống tội phạm sử dụng công nghệ cao của các cơ quan bảo vệ pháp luật và các lực lượng chuyên trách đặc biệt là nâng cao năng lực và chất lượng hợp tác quốc tế. Ưu tiên đầu tư ngân sách, mua sắm, cung ứng vật tư, phương tiện một cách hợp lý, từng bước đáp ứng yêu cầu hậu cần - kỹ thuật cho hoạt động của các cơ quan tư pháp và lực lượng chuyên trách trong đấu tranh với loại tội phạm này;

Đảng và Nhà nước cần tập trung lãnh đạo, chỉ đạo công tác rà soát, xây dựng, hoàn thiện hệ thống pháp luật về phòng, chống TPCNC, trong đó chú trọng cần nghiên cứu sửa đổi, bổ sung Bộ luật hình sự, Bộ luật Tố tụng hình sự, pháp luật về các biện pháp phòng, chống tội phạm sử dụng công nghệ cao và một số đạo luật có liên quan khác. Trong đó, trước mắt, cần tập trung nghiên cứu bổ sung kịp thời các chế định về các hành vi vi phạm pháp luật, tội phạm mới nảy sinh, chứng cứ điện tử trong Bộ luật Hình sự, Bộ luật Tố tụng hình sự đảm bảo hành lang pháp lý đủ mạnh và đủ sức răn đe tội phạm sử dụng công nghệ cao. Đề xuất tăng thẩm quyền pháp lý cho các cơ quan chuyên trách phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an và Bộ Quốc phòng đảm bảo đủ cơ sở pháp lý để tiến hành các hoạt động phòng ngừa, ngăn chặn, điều tra, xử lý các loại tội phạm sử dụng công nghệ cao.

Việt Nam cần mở rộng không gian phòng thủ của quốc gia, tranh thủ nguồn lực, tài trợ và tận dụng kinh nghiệm của các nước tiên tiến nhằm nâng cao hiệu quả đấu tranh phòng, chống tội phạm sử dụng công nghệ cao.

4.3.3.2. Giải pháp cụ thể

Thứ nhất, đẩy mạnh hợp tác quốc tế nhằm phòng ngừa từ xa đối với tội phạm sử dụng công nghệ cao.

Cần tăng cường đàm phán, ký kết, gia nhập các điều ước quốc tế về phòng, chống tội phạm nói chung, về TPSDCNC nói riêng, trọng tâm là với các nước đối tác chiến lược, đối tác toàn diện, các nước có quan hệ truyền thống, các nước láng giềng, các nước có đông người Việt Nam sinh sống, các nước có hợp tác kinh tế - đầu tư phát triển với Việt Nam.

Hợp tác theo cách này là kênh chia sẻ thông tin, kinh nghiệm và hỗ trợ lẫn nhau trong phòng chống tội phạm và cả trong đào tạo, phát triển các giải pháp an ninh mạng. Ngoài ra, Việt Nam cần thiết lập một cơ chế pháp lý cho mối quan hệ phối hợp giữa các lực lượng chuyên trách về phòng, chống TPCNC giữa Việt Nam và các quốc gia. Cùng với đó, cần xây dựng một cơ quan điều phối quan hệ phối hợp có trách nhiệm liên kết lực lượng chuyên trách phòng, chống tội phạm sử dụng công nghệ cao giữa các quốc gia với nhau để các nước có thể thường xuyên, nhanh chóng tạo ra được sự liên hệ chặt chẽ với nhau trong đấu tranh, phòng chống TPCNC.

Tiếp tục triển khai có hiệu quả kế hoạch thực hiện các Hiệp định, Thỏa thuận về hợp tác trong công tác đấu tranh phòng, chống tội phạm giữa Chính phủ, Bộ Công an Việt Nam và Chính phủ, Bộ Công an các nước có số lượng lớn người phạm các tội về sử dụng công nghệ cao trên lãnh thổ Việt Nam; đồng thời cần tăng cường ngoại giao để thỏa thuận tiến tới ký kết các Hiệp định, Thỏa thuận về hợp tác trong công tác đấu tranh phòng, chống tội phạm tội phạm nói chung và TPCNC nói riêng với các quốc gia mà Việt Nam chưa ký kết các Hiệp định TTTP về hình sự, Hiệp định dẫn độ, Hiệp định về hợp tác phòng, chống tội phạm;

Thứ hai, tranh thủ nguồn nhân lực và học hỏi kinh nghiệm các quốc gia

Các cơ quan thực thi pháp luật trong phòng chống TPCNC cần tranh thủ nguồn nhân lực và học hỏi kinh nghiệm của các nước trong đấu tranh PCTP sử dụng công nghệ cao, kinh nghiệm về quản trị, vận hành hệ thống mạng. Tiếp tục nghiên cứu tranh thủ các dự án tài trợ về trang bị, phương tiện; các khóa tập huấn, hội nghị, hội thảo quốc tế về phòng, chống tội phạm sử dụng công nghệ cao để chia sẻ thông tin và phối hợp PCTP sử dụng công nghệ cao hiệu quả. Đặc biệt cần chủ động và tích cực tham gia các khuôn khổ hợp tác song phương và đa phương, các tổ chức, hiệp hội thực thi pháp luật quốc tế như INTERPOL, ASEANAPOL, Cơ quan về phòng chống ma túy và tội phạm Liên hợp quốc (UNODC)...

Thứ ba, nâng cao năng lực cho lực lượng chuyên trách đấu tranh, phòng ngừa TPCNC

Một trong những vấn đề cốt lõi để nâng cao vai trò và đảm bảo cho hoạt động đấu tranh, phòng chống tội phạm sử dụng công nghệ cao có hiệu quả là nâng cao năng lực cho các cơ quan chuyên trách. Nhằm nâng cao năng lực phòng ngừa, điều tra khám phá TPCNC, Chính phủ cần có các đề cán để đào tạo, bồi dưỡng, tập huấn tập huấn (kể cả trong và ngoài nước) về pháp luật quốc tế, về kỹ thuật nghiệp vụ và về ngôn ngữ để đáp ứng sự thay đổi của phương thức, thủ đoạn tội phạm sử dụng

công nghệ cao. Cần tập trung phát huy tốt hơn vai trò và tăng cường hoạt động của lực lượng nòng cốt trong phòng chống tội phạm sử dụng công nghệ cao là Văn phòng INTERPOL Việt Nam và lực lượng an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao.

Chính phủ cần định hướng chiến lược xây dựng và phát triển đội ngũ cán bộ chuyên trách ngang tầm nhiệm vụ trong tình hình mới, có đủ kiến thức về pháp luật, nghiệp vụ và công nghệ thông tin. Nhà nước cần có chính sách hợp lý để khuyến khích, thu hút, tuyển chọn những cán bộ trình độ cao về khoa học công nghệ và năng lực đấu tranh chống TPCNC phục vụ trong các cơ quan chuyên trách.

Thứ tư, xây dựng trang thiết bị, công nghệ tiên tiến trong công tác đấu tranh, phòng ngừa TPCNC.

Bởi lẽ, đặc thù của TPCNC luôn sử dụng thiết bị, máy móc công nghệ thông tin trong hoạt động phạm tội do đó đòi hỏi cơ quan chuyên trách như Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao, Cục An ninh mạng (Bộ Công an) cần được quan tâm đầu tư mạnh mẽ về trang thiết bị chuyên dụng hiện đại và xây dựng được một đội ngũ cán bộ có trình độ cao. Hiện nay, mặc dù đã được Đảng, Nhà nước quan tâm đầu tư trang thiết bị, máy móc, nhưng trên đường đua ứng dụng khoa học công nghệ để phòng chống TPCNC thì chỉ có thể chiến thắng nếu có đủ trang thiết bị kỹ thuật, phương tiện, phần mềm chuyên dụng hiện đại. Vì vậy, Chính phủ cần tiếp tục ban hành các Đề án đầu tư mua sắm trang thiết bị cho các cơ quan chuyên trách bên cạnh Đề án 5 thuộc Chương trình Quốc gia phòng chống tội phạm về "Đấu tranh, phòng chống tội phạm sử dụng công nghệ cao" đã được thông qua.

Thứ năm, thiết lập và duy trì các kênh thông tin trao đổi

Nghiên cứu lựa chọn cơ chế trao đổi thông tin phù hợp với từng quốc gia thông qua các hình thức: Đường dây nóng, văn phòng sĩ quan liên lạc về phòng, chống tội phạm hay đại diện Bộ Công an đặt tại nước sở tại… Thiết lập và duy trì "đường dây nóng" hoặc kênh thông tin trao đổi (sĩ quan liên lạc) làm cơ sở trao đổi thông tin giữa lực lượng phòng chống TPCNC giữa Việt Nam và một số quốc gia đã thường xuyên hợp tác trong đấu tranh phòng chống tội phạm nói chung và tội phạm nói riêng để nhanh chóng trao đổi thông tin đáp ứng đòi hỏi với tính chất nhanh chóng, thuận tiện và chính xác của cuộc đấu tranh này.

Thứ sáu, hợp tác quốc tế đấu tranh phòng chống tội phạm sử dụng công nghệ cao cần có trọng tâm, trọng điểm.

Các cơ quan thi hành pháp luật cần xác định địa bàn, yếu tố quốc tịch các đối tượng để đưa ra các nội dung trọng tâm, trọng điểm trong HTQT để phòng ngừa,

đấu tranh với TPCNC. Trong đó lưu ý với Trung Quốc. Cần tiếp tục xác định hợp tác phòng chống TPCNC giữa Bộ Công an hai nước là một nội dung quan trọng trong tổng thể quan hệ hữu nghị Việt Nam - Trung Quốc, tiếp tục thúc đẩy quan hệ hợp tác dựa trên nội dung các thỏa thuận đã thống nhất, đặc biệt là Biên bản Hội nghị hợp tác phòng, chống tội phạm lần thứ tư trên cơ sở tôn trọng lẫn nhau, bình đẳng, cùng có lợi, góp phần phát triển bền vững, ổn định quan hệ đối tác hợp tác chiến lược toàn diện Việt Nam - Trung Quốc. Tiếp tục tăng cường trao đổi đoàn các cấp từ Trung ương đến địa phương để trao đổi thông tin, kinh nghiệm, ký kết các thỏa thuận hợp tác mà hai bên cùng quan tâm, tạo tiền đề hỗ trợ giúp đỡ phối hợp nâng cao hiệu quả công tác, bảo vệ vững chắc an ninh của mỗi nước. Tổ chức có hiệu quả các cuộc gặp gỡ song phương luân phiên hằng năm giữa đơn vị phòng chống TPCNC.

Thứ bảy, đề cao vai trò của ASEANPOL và INTERPOL trong hợp tác quốc tế đấu tranh phòng chống TPCNC.

Việt Nam với vai trò Chủ tịch ASEAN năm 2020 cần nỗ lực bàn bạc, thảo luận, đề xuất các giải pháp khả thi nhất để lực lượng Cảnh sát các nước thành viên ASEANAPOL và các đối tác có sự hợp tác chặt chẽ và toàn diện hơn nữa trong phòng, chống các loại tội phạm nói chung và tội phạm phòng sử dụng công nghệ cao nói riêng, trên tinh thần trách nhiệm, đoàn kết, tin tưởng lẫn nhau nhằm gìn giữ khu vực ngày một an toàn hơn. Cảnh sát giữa các nước cần tăng cường hợp tác trong chia sẻ thông tin; thực hiện các chiến dịch, chương trình đấu tranh với các loại tội phạm xuyên quốc gia trong đó có tội phạm sử dụng công nghệ cao; vận dụng linh hoạt các quy định của pháp luật để việc phối hợp trong điều tra, khám phá các chuyên án, các vụ án có hiệu quả hơn. Đồng thời, lực lượng Cảnh sát các nước thành viên ASEANAPOL và các đối tác cần đạt được tiếng nói chung và có sự ủng hộ lẫn nhau tại các diễn đàn quốc tế khác nhằm thể hiện được sự đoàn kết, thống nhất theo đúng tinh thần chung của hợp tác ASEAN.

Đối với Văn phòng INTERPOL Việt Nam cần thực hiện có hiệu quả việc hỗ trợ cho các đơn vị nghiệp vụ ở Trung ương và Công an các đơn vị, địa phương trong cả nước phối hợp điều tra, giải quyết thành công nhiều vụ án nghiêm trọng có yếu tố nước ngoài liên quan đến an ninh, trật tự. Đặc biệt cần nâng cao việc hướng dẫn và trực tiếp thực hiện nhiều yêu cầu về TTTP về hình sự và dẫn độ của các cơ quan chức năng trong và ngoài nước, đảm bảo thành công trong đấu tranh phòng, chống TPCNC, nâng cao vị thế của lực lượng Công an nhân dân nói chung và lực lượng Cảnh sát nhân dân nói riêng trên trường quốc tế. Hoạt động của Văn phòng

INTERPOL Việt Nam cần tập trung vào thu thập, phân tích, xử lý thông tin về TPCNC nhằm tham mưu về chiến lược, kế hoạch hợp tác quốc tế trong đấu tranh phòng, chống tội phạm; nghiên cứu cơ bản, dự báo tình hình tội phạm xuyên quốc gia cũng như đề xuất những biện pháp cụ thể để tăng cường hoạt động hợp tác quốc tế trong phòng, chống TPCNC vừa thực hiện các hoạt động phối hợp cụ thể trong xử lý các yêu cầu điều tra vụ án, truy tìm, truy nã tội phạm và những vấn đề TTTP hình sự và dẫn độ trong các vụ án, nhất là với những nước Việt Nam chưa ký kết các Hiệp định TTTP về hình sự, Hiệp định dẫn độ, Hiệp định về hợp tác phòng, chống tội phạm.

TIỂU KẾT CHƯƠNG 4

* * *

1. Các hành vi do tội phạm công nghệ cao thực hiện trên thế giới hiện nay diễn biến rất phức tạp. Vì đặc thù của loại tội phạm này là tính quốc tế, thực hiện trên môi trường ảo và ứng dụng nhanh thành tựu của khoa học công nghệ, do đó, điều này đã tác động mạnh đến tình hình tội phạm công nghệ cao thực hiện tại Việt Nam. Tội phạm sử dụng công nghệ cao ở Việt Nam trong những năm tới được dự báo sẽ diễn ra phức tạp với nhiều phương thức, thủ đoạn phạm tội mới, hoạt động có tính chất xuyên quốc gia và xảy ra trên nhiều lĩnh vực.

2. Việt Nam hiện đã bước đầu tạo dựng được khung pháp lý làm cơ sở cho hoạt động hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao, bao gồm các quy định của pháp luật quốc gia do Việt Nam ban hành và các điều ước quốc tế mà Việt Nam tham gia là thành viên. Các quy định của pháp luật trong nước về phòng ngừa, đấu tranh, triệt phá cũng như việc thực hiện hình sự hóa đối với các hành vi sử dụng công nghệ cao để gây tổn hại đến quyền lợi chính đáng của cá nhân, tổ chức và nhà nước... đã được Việt Nam hết sức quan tâm. Bên cạnh đó, những nội dung hợp tác tương trợ tư pháp, dẫn độ tội phạm, chuyển giao người bị kết án và phân định thẩm quyền tài phán cũng được Việt Nam đặc biệt chú trọng. Theo thống kê, tính đến tháng 9/2019, Việt Nam là thành viên của 22 điều ước quốc tế đa phương quy định về TTTP về hình sự, dẫn độ và chuyển giao người bị kết án phạt tù. Một số điều ước quốc tế đa phương điển hình điều chỉnh hợp tác quốc tế trong lĩnh vực phòng chống tội phạm công nghệ cao như Công ước của Liên Hợp quốc về chống tội phạm có tổ chức xuyên quốc gia, Hiệp định tương trợ tư pháp về hình sự giữa các nước ASEAN. Ngoài ra, Việt Nam đã ký 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 vào nhu cầu về phạm vi, nội dung hợp tác quốc tế trong phòng, chống tội phạm của của mỗi nước chủ yếu là các hiệp định tương trợ tư pháp.

Trong quá trình hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao, các cơ quan thực thi pháp luật của Việt Nam cũng đã chủ động phối hợp phát hiện, ngăn chặn và điều tra, xử lý nhiều đối tượng tội phạm sử dụng công nghệ cao có yếu tố nước ngoài trên lãnh thổ Việt Nam hoặc đối tượng ở nước ngoài nhưng xâm hại lợi ích của cá nhân, tổ chức trên lãnh thổ Việt Nam; phối hợp trong việc phát hiện và điều tra các vụ án lừa đảo nhằm chiếm đoạt tài sản, đánh bạc bằng công nghệ cao trên lãnh thổ Việt Nam.

3. Cùng với những nỗ lực hiện có, để nâng cao hiệu quả hợp tác đấu tranh phòng chống tội phạm công nghệ cao, trước tiên cần hoàn thiện hệ thống pháp luật Việt Nam trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao. Pháp luật Việt Nam cần tiếp tục tháo gỡ những vướng mắc, hạn chế từ một số quy định của luật thực định trong đó đặc biệt là Luật Tương trợ tư pháp, Luật Tố tụng hình sự... liên quan đến vấn đề hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao. Ngoài ra, liên tục tranh thủ cập nhật tri thức, thiết bị mới về khoa học công nghệ cao và học hỏi kinh nghiệm các quốc gia trên thế giới cũng là một vấn đề mà Việt Nam cần thực sự đầu tư hơn nữa để hỗ trợ cho công tác hợp tác quốc tế phòng chống tội phạm công nghệ cao hiện nay.

KẾT LUẬN CHUNG

* * *

1. Cuộc cách mạng công nghiệp lần thứ 4.0 không chỉ đơn thuần là một xu thế tất yếu mà nó đã trở thành thực tiễn sôi động diễn ra tại hầu khắp các quốc gia trên thế giới cũng như trên phạm vi toàn cầu. Bên cạnh những lợi ích to lớn đưa lại, chính nó cũng đem đến những thách thức an ninh phi truyền thống không hề nhỏ đối với mỗi quốc gia, khu vực. Không giống với các cuộc cách mạng trước đó, cuộc cách mạng công nghiệp lần thứ 4.0 bắt buộc mỗi cá nhân, mỗi quốc gia hay mỗi thể chế phải thay đổi nếu như không muốn bị tụt lại phía sau.

2. Tội phạm công nghệ cao, hay còn có thể được tiếp cận dưới nhiều tên gọi khác nhau như tội phạm mạng, tội phạm máy tính, tội phạm internet... là những thuật ngữ có thể sử dụng hoán đổi cho nhau nhằm để chỉ một loại hình tội phạm mới hình thành trong quá trình phát triển của cuộc cách mạng công nghệ thông tin 4.0 vào cuối thế kỷ 20 và được dự báo là sẽ phát triển rất nhanh trong thời gian sắp tới. Có thể nhận định, tội phạm công nghệ cao chính là "sản phẩm" của thời đại mà các cá nhân, tổ chức, các quốc gia và cộng đồng quốc tế phải chấp nhận để đổi lấy sự thịnh vượng và phát triển. Ở phạm vi toàn cầu, đến nay mới chỉ có một điều ước quốc tế điều chỉnh loại tội phạm này là Công ước về tội phạm mạng của Uỷ hội châu Âu năm 2001 (Công ước Budapest). Ngoài ra, ở phạm vi song phương, các điều ước quốc tế về tương trợ tư pháp hình sự, dẫn độ, chuyển giao người bị kết án được ký kết giữa các quốc gia chính là cơ sở pháp trực tiếp cho việc tiến hành những hoạt động hỗ trợ lẫn nhau giữa các quốc gia trong quá trình giải quyết các vụ án hình sự nói chung và vụ án hình sự liên quan đến tội phạm công nghệ cao nói riêng.

Đứng trước sự tinh vi phức tạp và những hậu quả nghiêm trọng của tội phạm công nghệ cao, việc hợp tác để đấu tranh, phòng chống tội phạm công nghệ cao giữa các quốc gia ngày càng trở nên cấp thiết hơn bao giờ hết. Pháp luật quốc tế chính là cơ sở để các quốc gia tiến hành những hoạt động hợp tác này. Thông qua các nội dung hợp tác như hình thành các cơ quan, thiết chế quốc tế trong phòng chống tội phạm công nghệ cao; hài hoà hoá pháp luật; tương trợ tư pháp hình sự; dẫn độ; tiến hành phối hợp điều tra… pháp luật quốc tế đã hình thành nên một cơ chế pháp lý chung ở các cấp độ khác nhau, từ song phương, khu vực đến toàn cầu để kết nối hoạt động giữa các quốc gia, từ đó, ứng phó hiệu quả với tội phạm công nghệ cao, góp phần hạn chế, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế.

3. Trên cơ sở những quy định của pháp luật quốc tế Việt Nam đã và đang tiến hành nhiều hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao. Về thực tiễn, Việt Nam đã phối hợp phát hiện, ngăn chặn và điều tra, xử lý nhiều đối tượng tội phạm sử dụng công nghệ cao có yếu tố nước ngoài trên lãnh thổ Việt Nam hoặc đối tượng ở nước ngoài nhưng xâm hại lợi ích của cá nhân, tổ chức trên lãnh thổ Việt Nam hay các vụ án lừa đảo nhằm chiếm đoạt tài sản, đánh bạc bằng công nghệ cao trên lãnh thổ Việt Nam. Về pháp lý, Việt Nam tiến hành ký kết rất nhiều các điều ước quốc tế cũng như các thỏa thuận quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao. Việt Nam đã ban hành hệ thống các văn bản pháp luật chung và chuyên ngành để điều chỉnh trực tiếp những nội dung hợp tác đấu tranh phòng chống tội phạm công nghệ cao như Luật Công nghệ thông tin 2006, Luật an toàn thông tin mạng 2015, Luật an ninh mạng 2018, Bộ luật hình sự 2015, Bộ luật Tố tụng hình sự 2015, Nghị định số 25/2014/NĐ-CP quy định về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao, Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC 10/9/2012 của liên ngành Bộ Công an, Bộ Quốc phòng, Bộ Tư pháp, Bộ Thông tin và Truyền thông, VKSNDTC, TANDTC, hướng dẫn áp dụng một số quy định của BLHS về một số tội phạm trong lĩnh vực CNTT, viễn thông…

Đại hội XIII của Đảng xác định: "*Củng cố quốc phòng, an ninh, bảo vệ vững chắc Tổ quốc Việt Nam xã hội chủ nghĩa là nhiệm vụ trọng yếu, thường xuyên của Đảng, Nhà nước, hệ thống chính trị và toàn dân, trong đó Quân đội nhân dân và Công an nhân dân là nòng cốt*". Đồng thời, nhấn mạnh: "*Tiếp tục triển khai thực hiện toàn diện, đồng bộ Chiến lược bảo vệ Tổ quốc, Chiến lược quốc phòng, Chiến lược quân sự, Chiến lược bảo vệ an ninh quốc gia, Chiến lược bảo vệ biên giới quốc gia, Chiến lược bảo vệ Tổ quốc trên không gian mạng, Chiến lược an ninh mạng quốc gia và các chiến lược quốc phòng, an ninh chuyên ngành khác*". Do vậy, bên cạnh việc hoàn thiện hệ thống pháp luật, tăng cường hợp tác với các quốc gia trên thế giới thì Việt Nam phải liên tục cập nhật tri thức, thiết bị mới về khoa học công nghệ cao từ các tổ chức quốc tế chuyên môn cũng như các quốc gia phát triển để bảo vệ vững chắc chủ quyền của Việt Nam trước những thách thức của tội phạm công nghệ cao./.

DANH MỤC TÀI LIỆU THAM KHẢO

* * *

TIẾNG VIỆT

1. Đảng cộng sản Việt Nam (1996), Văn kiện Đại hội đại biểu toàn quốc lần thứ VIII, Nxb. Chính trị quốc gia, Hà Nội.
2. Đảng Cộng sản Việt Nam (2001), Văn kiện Đại hội đại biểu toàn quốc lần thứ IX, Nxb Chính trị Quốc gia, Hà Nội.
3. Đảng Cộng sản Việt Nam (2006), Văn kiện Đại hội đại biểu toàn quốc lần thứ X, Nxb Chính trị quốc gia, Hà Nội.
4. Đảng Cộng sản Việt Nam (2007), Văn kiện Nghị quyết Hội nghị lần thứ tư Ban Chấp hành Trung ương Đảng khóa X.
5. Đảng Cộng sản Việt Nam (2011), Văn kiện Đại hội đại biểu toàn quốc lần thứ XI, Nxb Chính trị quốc gia, Hà Nội.
6. Đảng Cộng sản Việt Nam (2021), Văn kiện Đại hội Đại biểu toàn quốc lần thứ XIII, Tập I, NXB Chính trị quốc gia, sự thật, Hà Nội
7. Luật Công an nhân dân năm 2018.
8. Luật Tương trợ tư pháp 2007.
9. Bộ luật hình sự năm 2015.
10. Bộ luật tố tụng hình sự năm 2015.
11. Nghị định số 25/2014/NĐ-CP quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao.
12. Nghị quyết số 07-NQ/TW của Bộ Chính trị ngày 27/11/2001 về hội nhập kinh tế quốc tế.
13. Nghị quyết số 22-NQ/TW của Bộ Chính trị ngày 10 /04 /2013 về hội nhập quốc tế.
14. Nghị quyết số 31/NQ–CP của Chính phủ ngày 13/05/2014 về Ban hành Chương trình hành động của Chính phủ thực hiện Nghị quyết số 22-NQ/TW của Bộ Chính trị về hội nhập quốc tế.
15. Nghị quyết số 48-NQ/TW của Bộ Chính trị ngày 24/05/2005 về Chiến lược xây dựng và hoàn thiện hệ thống pháp luật Việt Nam đến năm 2010, định hướng đến năm 2020.

16. Nghị quyết số 49-NQ/TW của Bộ chính trị ngày 02/06/2005 về Chiến lược cải cách tư pháp đến năm 2020.
17. Thông tư liên tịch số 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC
18. Công ước Budapest của Ủy Hội Châu Âu về tội phạm mạng năm 2001 và báo cáo giải thích công ước.
19. Công ước của Liên Hợp Quốc về chống tội phạm có tổ chức xuyên quốc gia năm 2000 và các Nghị định thư bổ sung.
20. Điều lệ tổ chức INTERPOL.
21. Báo cáo về tình hình tội phạm sử dụng công nghệ cao diễn ra tại địa phương giai đoạn 2005-2014, của 63 Viện kiểm sát nhân dân tỉnh, thành phố, theo Công văn số 2176/VKSTC-V1 ngày 11/7/2014 của Viện Kiểm sát nhân dân tối cao.
22. Bộ Công an (2019), Báo cáo tổng kết thi hành pháp luật về dẫn độ.
23. Bộ Thông tin và Truyền thông (2019), *Sách trắng Công nghệ thông tin và truyền thông VIệt Nam năm 2019*.
24. Cao Anh Đức (2015), "*Tính chất của tình hình tội phạm sử dụng công nghệ cao tại Việt Nam, thủ đoạn phạm tội và dự báo"*, Tạp chí Nghiên cứu lập pháp số 16.
25. Đinh Thế Hưng, Lê Thị Hồng Xuân (2019), "*Tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng ở Việt Nam hiện nay"*, Tạp chí Tòa án nhân dân. Số 7.
26. Hiệp định tương trợ tư pháp về dân sự, gia đình và hình sự giữa nước CHXHCN Việt Nam với các nước ngoài, Nxb. Pháp lý, Hà Nội, 1990.
27. Hồ Thế Hòe, *Giải pháp nâng cao hiệu quả đấu tranh với tội phạm sử dụng công nghệ cao trong bối cảnh toàn cầu hóa*, (Đại học An ninh nhân dân, TP. Hồ Chí Minh)
28. Hoàng Việt Quỳnh (2016), "*Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định của pháp luật Việt Nam"*, Tạp chí Khoa học giáo dục Cảnh sát nhân dân số 79.
29. Kết luận số 01-KL/TW ngày 04/04/2016 của Bộ Chính trị về việc tiếp tục thực hiện Nghị quyết số 48-NQ/TW của Bộ Chính trị khóa IX về Chiến lược xây dựng và hoàn thiện hệ thống pháp luật Việt Nam đến năm 2010, định hướng đến năm 2020.

30. Kết luận số 92-KL/TW ngày 12/03/2014 của Bộ Chính trị về việc tiếp tục thực hiện Nghị quyết số 49-NQ/TW ngày 02/06/2005 của Bộ chính trị về Chiến lược cải cách tư pháp đến năm 2020.
31. Kết luận số 01-KL/TW ngày 04/04/2016 của Bộ Chính trị về việc tiếp tục thực hiện Nghị quyết số 48-NQ/TW của Bộ Chính trị khóa IX về Chiến lược xây dựng và hoàn thiện hệ thống pháp luật Việt Nam đến năm 2010, định hướng đến năm 2020.
32. Kết luận số 92-KL/TW ngày 12/03/2014 của Bộ Chính trị về việc tiếp tục thực hiện Nghị quyết số 49-NQ/TW ngày 02/06/2005 của Bộ chính trị về Chiến lược cải cách tư pháp đến năm 2020.
33. Nguyễn Mạnh Toàn (2002), "*Đặc điểm và các dạng hành vi cơ bản của tội phạm tin học"*, Tạp chí Nhà nước và Pháp luật số 3.
34. Nguyễn Ngọc Anh, *Một số quy định của pháp luật về tội phạm công nghệ cao* (website Bộ Công an).
35. Nguyễn Thị Kim Ngân, Nguyễn Đức Phúc (2008), "*Hiệp hội cảnh sát các nước ASEAN – Mô hình hợp tác quốc tế đấu tranh chống tội phạm xuyên quốc gia*", Tạp chí Luật học số 9.
36. Nguyễn Thị Quế Thu (2017), "*Điều ước quốc tế - Lý luận và thực tiễn áp dụng điều ước quốc tế về phòng, chống tội phạm tại Việt Nam"*, Sách chuyên khảo, Nxb Công an nhân dân.
37. Phạm Hồng Hạnh (2016), "*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.
38. Trần Đoàn Hạnh (2016), "*Những vướng mắc trong đấu tranh, xử lý vi phạm pháp luật về tội phạm công nghệ cao"*, Tạp chí nghiên cứu lập pháp.
39. Trần Văn Doanh (2014), *Hợp tác quốc tế trong phòng, chống tội phạm sử dụng công nghệ cao và vấn đề đặt ra trong công tác đào tạo, bồi dưỡng cán bộ,Kỷ yếu hội thảo khoa học "Phòng, chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo",*Học viện CSND tháng 11/2014.
40. Trường Đại học Luật Hà Nội (2020), *Giáo trình Luật Quốc tế,* Nxb. Công an nhân dân, Hà Nội.
41. Viện Kiểm sát Nhân dân tối cao (2017), Báo cáo Tổng kết 10 năm triển khai thi hành Luật tương trợ tư pháp năm 2007.

42. Viện kiểm sát nhân dân tối cao, Vụ 13 (2017), Chuyên đề "*Thực trạng và giải pháp hoạt động TTTP về hình sự; Một số kiến nghị, sửa đổi, bổ sung Luật TTTP năm 2007"*, Hà Nội.
43. Viện ngôn ngữ học (2010), *Từ điển Tiếng Việt*, Hoàng Phê chủ biên,
44. Việt Nam (2019), Báo cáo tuân thủ kỹ thuật (Báo cáo TC) và Báo cáo tính hiệu quả (Báo cáo IO).

TIẾNG ANH

45. Akhgar, Babak, Staniforth, Andrew, & Bosco, Francesca (2014), *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Rockland, MA: Elsevier Science & Technology Books.
46. Alexander Seger (2016), *The Budapest Convention on Cybercrime: a framework for capacity building*, Global Cyber Expertise Magazine, (2).35.
47. ASEAN (2017), *ASEAN Declaration to prevent and combat cybercrime*, Manila.
48. Bernat, Frances P, and David Makin (2014), *Cybercrime Theory And Discerning If There Is A Crime: The Case Of Digital Piracy*, International Review of Modern Sociology, vol. 40, no. 2.
49. Bou Sleiman, Mohamed, & Gerdemann, Simon. (2021), *Covid-19: A catalyst for cybercrime?,* International Cybersecurity Law Review, 2(1), 37-45.
50. Broadhurst, R., & Grabosky, P. (2005), *Cyber-crime: The challenge in Asia*. Hong Kong: Hong Kong University Press.
51. Council of Europe (2003), *Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems*, Strasbourg.
52. Council of Europe (2007), *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, Lanzarote.
53. European Parliament (2016), *General Data Protection Regulation (GDPR*), Brussels.
54. European Parliament (2016), *The Directive on security of network and information systems (NIS Directive)*, Brussels.
55. Faga, Hemen Philip (2017), *The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between*

Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. Baltic Journal of Law & Politics, 10(1), 1-34.

56. Jonathan Clough (2015), "*Principles of cybercrime*", Cambridge University Press, Second Edition.
57. Kranenbarg, W. M., & Leukfeldt, R. (2021), *Cybercrime in Context: The human factor in victimization, offending, and policing* (Crime and Justice in Digital Society, I) (1st ed. 2021 ed.). Springer.
58. Kshetri, Nir (2010), *The Global Cybercrime Industry* (1. Aufl. ed.). Berlin, Heidelberg: Springer-Verlag.
59. Lallie, Harjinder Singh, Shepherd, Lynsay A, Nurse, Jason R.C, Erola, Arnau, Epiphaniou, Gregory, Maple, Carsten, & Bellekens, Xavier (2021). *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*. Computers & Security, 105, 102248.
60. Masoud Nosrati, Mehdi Hariri, Alireza Shakarbeygi (2013), *Computers and Internet: From a Criminological View*, International Journal of Economy, Management and Social Sciences, 2 (4).
61. Mohamed Chawki (2005), *A Critical Look at the Regulation of Cybercrime*, University of Lyon III, France.
62. Prasad, R., & Institute of Chartered Financial Analysts of India (2004), *Cyber crime: An introduction* (1st ed.). Hyderabad, India: Icfai Books.
63. Roger Brownsword, Eloise Scotford và Karen Yeung (2017), *The Oxford Handbook of Law, Regulation and Technology*, United Kingdom. Oxford University Press.
64. Roth, M. (2010), *Global organized crime: A reference handbook* (Contemporary world issues). Santa Barbara, Calif.: ABC-CLIO.
65. Susan W. Brenner & Bert-Jaap Koops (2004), "*Approaches to Cybercrime Jurisdiction*", Journal of high technology law, Vol. IV No. 1.
66. The United Nations Office on Drugs and Crime (2012), Handbook on the International Transfer of Sentenced Persons.
67. Tsagourias, N., & Buchan, R. (2015), *Research handbook on international law and cyberspace (Research handbooks in international law)*, Cheltenham, England; Northampton, Massachusetts: Edward Elgar Publishing.

68. Twede, Jason, & Marion, Nancy E. (2020). *Cybercrime: An Encyclopedia of Digital Crime*. ABC-CLIO.
69. United Nations (2001), Resolution 55/63 - Combating the criminal misuse of information technologies, New York.
70. United Nations (2002), Resolution 56/121 - Combating the criminal misuse of information technologies, New York.

WEBSITE

http://bocongan.gov.vn/
http://canhsatnhandan.vn/
http://hudoc.echr.coe.int/eng
http://legal.un.org/
https://definitions.uslegal.com/c/cybercrimes/
https://dictionary.cambridge.org/
https://eur-lex.europa.eu/
https://fas.org/sgp/
https://ictnews.vietnamnet.vn/
https://iuscogens-vie.org/
https://lanhsuvietnam.gov.vn/
https://law.justia.com/
https://legal.thomsonreuters.com/
https://nld.com.vn/chinh-tri/
https://reports.weforum.org/
https://rm.coe.int/
https://unis.unvienna.org/
https://www.afp.gov.au/
https://www.cybercrimejournal.com/
https://www.gov.uk/
https://www.interpol.int/
https://www.itu.int/
https://www.justice.gov/
https://www.le-vpn.com/
https://www.officialgazette.gov.ph/

https://www.samuiforsale.com/
https://www.unodc.org/
https://www.unodc.org/

DANH MỤC CÔNG TRÌNH NGHIÊN CỨU KHOA HỌC ĐÃ CÔNG BỐ CỦA NGHIÊN CỨU SINH CÓ LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN TIẾN SĨ

* * *

*** Các công trình khoa học đã được công bố trên các Tạp chí chuyên ngành trong thời gian Nghiên cứu sinh thực hiện Luận án tiến sĩ:**

1. "*Hài hòa hóa pháp luật trong phòng chống tội phạm công nghệ cao*", Tạp chí Luật học, số 8 năm 2020.
2. "*Khung pháp lý về cơ chế hợp tác phòng chống tội phạm mạng trong khu vực ASEAN*", Tạp chí Luật học, số 12 năm 2020.
3. "*Nhận diện tội phạm công nghệ cao trong pháp luật quốc tế và một số kinh nghiệm đối với Việt Nam trong tình hình mới*", Tạp chí Giáo dục và xã hội, số đặc biệt năm 2020.

BỘ GIÁO DỤC VÀ ĐÀO TẠO **BỘ TƯ PHÁP**

TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

***

THÔNG TIN VỀ NHỮNG KẾT LUẬN MỚI CỦA LUẬN ÁN TIẾN SĨ

Đề tài luận án: Pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao – Những vấn đề đặt ra đối với Việt Nam.

Chuyên ngành: Luật quốc tế **Mã số: 9 38 01 08**

Cơ sở đào tạo: Trường Đại học Luật Hà Nội

Người hướng dẫn khoa học: 1) GS. TS. Trung tướng Nguyễn Ngọc Anh;

2) PGS. TS. Nguyễn Thị Kim Ngân

TÓM TẮT NHỮNG KẾT LUẬN MỚI CỦA LUẬN ÁN

Luận án là công trình khoa học nghiên cứu một cách toàn diện các vấn đề lý luận, pháp lý về quá trình hình thành và phát triển của tội phạm công nghệ cao cũng như các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống loại tội phạm này; đồng thời làm rõ các quy định, thực tiễn thực thi của Việt Nam, trên cơ sở đó, đề xuất những giải pháp hoàn thiện pháp luật và nâng cao hiệu quả của hoạt động thực thi pháp luật tại Việt Nam liên quan đến tội phạm công nghệ cao. Luận án đã có những đóng góp mới về mặt khoa học như sau:

- **Thứ nhất**, luận án đã phân tích, tổng hợp những vấn đề lý luận về tội phạm công nghệ cao và các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao. Qua đó đã xây dựng khái niệm tội phạm công nghệ cao cũng như làm rõ những đặc điểm của loại hình tội phạm này trên cơ sở đối sánh với các thuật ngữ khác có liên quan.

- **Thứ hai**, luận án đã đánh giá một cách toàn diện các quy định của pháp luật quốc tế, thực tiễn thực hiện pháp luật quốc tế về tội phạm công nghệ cao của một số quốc gia điển hình. Qua đó, rút ra được một số kinh nghiệm và tham khảo có giá trị đối với Việt Nam.

- **Thứ ba**, luận án đã bình luận, đánh giá các quy định và thực tiễn quá trình thực thi pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao của Việt Nam, qua đó, đề xuất những giải pháp và phương hướng hoàn thiện pháp luật nhằm tăng cường hiệu quả của hoạt động thực thi pháp luật trong lĩnh vực hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao./.

MINISTRY OF EDUCATION AND TRAINING **MINISTRY OF JUSTICE**

HANOI LAW UNIVERSITY

*** * ***

INFORMATION ON NEW CONCLUSIONS OF THE DOCTORAL THESIS

Doctoral thesis topic: INTERNATIONAL LAW IN COOPERATION TO FIGHT HIGH-TECH CRIME – ISSUES FOR VIETNAM.

Specialization: International Law **Code: 9 38 01 08**

The work was completed at: Hanoi Law University

Science instructor: 1) Prof. Dr. Lieutenant General. Nguyen Ngoc Anh;

2) AssocProf. Dr. Nguyen Thi Kim Ngan

SUMMARY OF NEW CONCLUSIONS OF THE DOCTORAL THESIS

The doctoral thesis is a scientific work that comprehensively studies theoretical and legal issues about the formation and development of high-tech crimes as well as the provisions of international law in international cooperation to prevent this type of crime; At the same time, clarify Vietnam's regulations and enforcement practices, on that basis, propose solutions to improve the law and improve the efficiency of law enforcement activities in Vietnam related to high technology crime. The thesis has made new scientific contributions as follows:

- Firstly, the thesis has analyzed and synthesized theoretical issues on high-tech crime and the provisions of international law in cooperation in the fight against high-tech crime. Thereby, the concept of high-tech crime was developed as well as clarified the characteristics of this type of crime on the basis of comparison with other related terms.

- Second, the thesis has evaluated the provisions of international law, the practice of implementing international law on high-tech crimes of some typical countries. Thereby, drawing some experience and reference values for Vietnam.

- Thirdly, the thesis has commented and evaluated the regulations and practices of law enforcement in international cooperation in the fight against and prevention of high-tech crimes in Vietnam, thereby, proposing solutions, methods and directions for perfecting the law in order to enhance the effectiveness of law enforcement activities in the field of international cooperation in the fight against high-tech crime./.

BỘ GIÁO DỤC VÀ ĐÀO TẠO **BỘ TƯ PHÁP**
TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

ĐỖ QUÍ HOÀNG

PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO – NHỮNG VẤN ĐỀ ĐẶT RA ĐỐI VỚI VIỆT NAM

Chuyên ngành: Luật quốc tế
Mã số: 9 38 01 08

TÓM TẮT LUẬN ÁN TIẾN SỸ LUẬT HỌC

Hà Nội - 2021

Công trình được hoàn thành tại:

Trường Đại học Luật Hà Nội

Người hướng dẫn khoa học:

1. GS.TS. Trung tướng. Nguyễn Ngọc Anh

2. PGS.TS. Nguyễn Thị Kim Ngân

Phản biện 1:

Phản biện 2:

Phản biện 3:

Luận án sẽ được bảo vệ trước Hội đồng chấm Luận án cấp Trường họp tại Trường Đại học Luật Hà Nội vào hồi… giờ ngày…. tháng….năm

Có thể tìm hiểu Luận án tại:

1. Thư viện Quốc gia
2. Thư viện Trường Đại học Luật Hà Nội

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Thế kỷ XXI, sự bùng nổ của khoa học kỹ thuật mặc dù đã đem lại nhiều thuận lợi cho quá trình giao lưu hợp tác quốc tế nhưng cũng tạo điều kiện cho các loại tội phạm phát triển. Sự phát triển của tội phạm không chỉ mở rộng ở phạm vi, mức độ thiệt hại mà hành vi phạm tội cũng ngày một tinh vi hơn khi tội phạm ứng dụng các công nghệ mới trong phương thức thực hiện; điều này gây ảnh hưởng to lớn cũng như gây ra sự lo ngại cho không chỉ một quốc gia mà cho toàn thể cộng đồng quốc tế.

Ngoài tính chất tổ chức chặt chẽ thường thấy, giờ đây cùng với sự phát triển vượt bậc của khoa học công nghệ, phương thức và thủ đoạn phạm tội của loại tội phạm công nghệ cao ngày càng đa dạng hơn, tinh vi hơn, kín đáo hơn và có sự thay đổi liên tục nhằm lẩn tránh sự phát hiện của các cơ quan chức năng. Chưa dừng lại ở đó, tội phạm công nghệ cao diễn ra trên hầu hết các lĩnh vực hợp tác giữa các chủ thể gây ra thiệt hại vô cùng lớn, ảnh hưởng nghiêm trọng đến an ninh mỗi quốc gia cũng như an ninh tập thể.

Thực tiễn hiện nay, pháp luật quốc tế chưa có một cơ sở pháp lý đủ toàn diện và điều chỉnh thống nhất đối với các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao. Tuy nhiên, cộng đồng quốc tế cũng đã bắt đầu nhận thấy sự cần thiết phải có một văn kiện pháp lý quốc tế trong việc tạo ra một khuôn khổ hợp tác chung và hiệu quả trong lĩnh vực hợp tác đấu tranh, phòng chống loại tội phạm nguy hiểm này.

Tại Việt Nam, tội phạm công nghệ cao là loại tội phạm mới xuất hiện trong những năm gần đây nhưng lại có sự gia tăng ngày càng nhanh cả về số lượng, tính chất nguy hiểm và mức độ thiệt hại. Trong lĩnh vực an ninh quốc gia, các thế lực thù địch và phản động quốc tế đã không ngừng lợi dụng kênh truyền thông qua mạng xã hội, mạng Internet để xuyên tạc, vu khống chống phá các chủ trương, đường lối, chính sách, pháp luật của Đảng và Nhà nước.

Xuất phát từ những lý do nêu trên nên việc nghiên cứu, làm rõ thêm các quy định của pháp luật quốc tế liên quan đến tội phạm công nghệ cao cũng như hoạt động hợp tác đấu tranh phòng chống loại tội phạm này trên thực tế là việc làm đặc biệt cần thiết, nhất là khi đặt nó trong bối cảnh của cuộc cách mạng công nghiệp 4.0 hiện nay. Để từ đó, rút ra được những giá trị tham khảo đối với Việt Nam trong quá trình hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

2. Đối tượng và phạm vi nghiên cứu của luận án

Đối tượng và phạm vi nghiên cứu của luận án tập trung vào những vấn đề pháp lý quốc tế về tội phạm công nghệ cao cũng như hoạt động hợp tác đấu tranh đối với loại hình tội phạm này. Theo đó:

Đối tượng nghiên cứu của đề tài luận án bao gồm:

- Những vấn đề lý luận về tội phạm công nghệ cao và hoạt động hợp tác đấu tranh, phòng chống loại hình tội phạm công nghệ cao; phân biệt và nhận diện tội phạm công nghệ cao với các tội phạm khác có liên quan.

- Các quy định của pháp luật quốc tế và pháp luật một số quốc gia tiêu biểu về tội phạm công nghệ cao cũng như hoạt động hợp đấu tranh, phòng chống loại hình tội phạm công nghệ cao trong bối cảnh hiện nay.

- Thực trạng tội phạm công nghệ cao trên thế giới cũng như hoạt động hợp tác đấu tranh phòng chống tội phạm công nghệ cao. Qua đó, đề tài luận án cũng sẽ rút ra một số kinh nghiệm và giá trị tham khảo đối với Việt Nam.

- Cơ sở pháp lý và thực tiễn hoạt động hợp tác đấu tranh tội phạm công nghệ cao tại Việt Nam. Một số dự báo, giải pháp, phương hướng cho công tác phòng chống loại hình tội phạm này trong tình hình mới.

Trên cơ sở phân tích nội dung của những đối tượng nghiên cứu nêu trên, phạm vi nghiên cứu của đề tài luận án bao gồm:

- Nhận diện và phân biệt một số thuật ngữ có liên quan đến tội phạm công nghệ cao, đưa ra và phân tích những cách tiếp cận về tội phạm công nghệ cao qua đó xây dựng một định nghĩa chung về tội phạm công nghệ cao, đặc điểm và phân loại loại hình tội phạm này.

- Nội dung các quy định của pháp luật quốc tế và pháp luật một số quốc gia về tội phạm công nghệ cao; các quy định điều chỉnh hoạt động hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

- Thực trạng và pháp luật Việt Nam về tội phạm công nghệ cao và công tác hợp tác đấu tranh phòng chống tội phạm công nghệ cao trong bối cảnh

hiện nay. Trên cơ sở đó đưa ra phương hướng, giải pháp đối với Việt Nam trong thời gian tới.

3. Mục đích và nhiệm vụ nghiên cứu của luận án

Mục đích của luận án là làm rõ các vấn đề lý luận-pháp lý của tội phạm công nghệ cao cũng như các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống loại tội phạm này; đồng thời làm rõ các quy định, thực tiễn thực thi của Việt Nam, trên cơ sở đó, đưa ra một số dự báo và đề xuất những giải pháp hoàn thiện pháp luật, nâng cao hiệu quả của hoạt động thực thi pháp luật tại Việt Nam liên quan đến tội phạm công nghệ cao.

Để đạt được những mục đích trên, đề tài sẽ tập trung giải quyết các nhiệm vụ sau:

- Phân tích, nghiên cứu những vấn đề lý luận về tội phạm công nghệ cao và các nội dung, nguyên tắc, vai trò, nguồn của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao;

- Phân tích, đánh giá các quy định của pháp luật quốc tế, việc thực hiện pháp luật quốc tế về tội phạm công nghệ cao ở một số quốc gia. Qua đó, rút ra được một số kinh nghiệm và giá trị tham khảo đối với Việt Nam;

- Bình luận, đánh giá các quy định và thực tiễn quá trình thực thi pháp luật về tội phạm công nghệ cao của Việt Nam, qua đó, đề xuất những giải pháp và phương hướng hoàn thiện pháp luật nhằm tăng cường hiệu quả của hoạt động thực thi pháp luật trong lĩnh vực hợp tác đấu tranh, phòng chống tội phạm công nghệ cao.

4. Phương pháp luận và phương pháp nghiên cứu

Đề tài luận án được thực hiện trên cơ sở phương pháp luận khoa học của chủ nghĩa Mác - Lênin, vận dụng kết hợp các quan điểm của chủ nghĩa duy vật biện chứng và chủ nghĩa duy vật lịch sử. Ngoài ra, các phương pháp nghiên cứu cụ thể cũng được sử dụng trong luận án, ví dụ như: diễn dịch-quy nạp (chương 2 và chương 3), phân tích (chương 2, chương 3 và chương 4), tổng hợp (chương 3 và chương 4), so sánh (chương 2, chương 3 và chương 4), hệ thống hoá-khái quát hoá (chương 2, chương 3 và chương 4)...

Bên cạnh đó, luận án cũng được tiến hành trên cơ sở quán triệt sâu sắc các quan điểm về đường lối lãnh đạo của Đảng Cộng Sản và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, đặc biệt là quan điểm và định hướng của Đảng đối với công tác phòng, chống tội phạm trong tình hình mới và Chiến lược quốc gia phòng, chống tội phạm đến năm 2020.

5. Ý nghĩa khoa học và tính mới của luận án

Luận án là công trình khoa học nghiên cứu một cách toàn diện các vấn đề lý luận, pháp lý về quá trình hình thành và phát triển của tội phạm công nghệ cao cũng như các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống loại tội phạm này; đồng thời làm rõ các quy định, thực tiễn thực thi của Việt Nam, trên cơ sở đó, đề xuất những giải pháp hoàn thiện pháp luật và nâng cao hiệu quả của hoạt động thực thi pháp luật tại Việt Nam liên quan đến tội phạm công nghệ cao. Luận án đã có những đóng góp mới về mặt khoa học như sau:

- Thứ nhất, luận án đã phân tích, tổng hợp những vấn đề lý luận về tội phạm công nghệ cao và các quy định của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao. Qua đó đã xây dựng khái niệm tội phạm công nghệ cao cũng như làm rõ những đặc điểm của loại hình tội phạm này trên cơ sở đối sánh với các thuật ngữ khác có liên quan.

- Thứ hai, luận án đã đánh giá các quy định của pháp luật quốc tế, thực tiễn thực hiện pháp luật quốc tế về tội phạm công nghệ cao của một số quốc gia điển hình. Qua đó, rút ra được một số kinh nghiệm và giá trị tham khảo đối với Việt Nam.

- Thứ ba, luận án đã bình luận, đánh giá các quy định và thực tiễn quá trình thực thi pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao của Việt Nam, qua đó, đề xuất những giải pháp và phương hướng hoàn thiện pháp luật nhằm tăng cường hiệu quả của hoạt động thực thi pháp luật trong lĩnh vực hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao.

6. Câu hỏi nghiên cứu và giả thuyết nghiên cứu

Trước khi triển khai nghiên cứu đề tài luận án tiến sĩ, nghiên cứu sinh đã tự đặt ra một số câu hỏi nghiên cứu, bao gồm:

- Câu hỏi mang tính mô tả: Tội phạm công nghệ cao là gì? Loại tội phạm này được quy định ở những cấp độ và phạm vi nào? Liên quan đến tội

phạm công nghệ cao, có những cách tiếp cận và cách thức sử dụng thuật ngữ như thế nào? Thực trạng các loại tội phạm này diễn ra trên thực tế ra sao? Tỷ lệ tương quan giữa các loại tội xảy ra là bao nhiêu? Tần suất của loại tội nào phổ biến trên thực tế; Các nội dung trong hoạt động đấu tranh và hợp tác phòng chống loại tội phạm này là gì? Hiệu quả trên thực tế đến đâu? .v.v...

- Câu hỏi mang tính so sánh và nhân-quả: so sánh để chỉ ra được điểm giống và khác nhau giữa tội phạm công nghệ cao với các loại hình tội phạm khác; sau khi so sánh, tội phạm công nghệ cao có mối liên hệ như thế nào đối với các loại hình tội phạm khác đó? Liệu rằng, đây là một loại hình tội phạm mới hay chỉ là biến thể của các loại hình tội phạm truyền thống? So sánh kinh nghiệm và thực tiễn pháp luật của một số quốc gia phát triển trong vấn đề phòng chống tội phạm công nghệ cao? Rút ra một số bài học kinh nghiệm và liên hệ với Việt Nam? .v.v…

Xuất phát từ những câu hỏi nghiên cứu, nghiên cứu sinh đưa ra một nhận định sơ bộ ban đầu mang tính giả thuyết nghiên cứu, đó là:

- Tội phạm công nghệ cao là một loại hình tội phạm phát sinh trong thời đại công nghệ thông tin, với nhiều đặc điểm tương đồng với các loại tội phạm có tính chất quốc tế hay tội phạm có tổ chức xuyên quốc gia, mức độ nguy hiểm và hậu quả khôn lường hơn rất nhiều so với các loại tội phạm truyền thống. Chính vì vậy, cần thiết trong việc nghiên cứu điều chỉnh và chung tay giải quyết thông qua hợp tác quốc tế (Giả thuyết 1)

- Tội phạm công nghệ cao chỉ là sự biến thể của các loại tội phạm truyền thống nên chỉ cần hoàn thiện các quy định của pháp luật quốc gia để phòng chống loại tội phạm này (Giả thuyết 2)

- Phương thức hợp tác quốc tế có vai trò quyết định trong quá trình đấu tranh phòng chống loại hình tội phạm công nghệ cao (Giả thuyết 3)

Qua quá trình tìm hiểu, nghiên cứu sinh bác bỏ giả thuyết số 2 và tập trung đi vào phát triển và chứng minh Giả thuyết 1 và 3. Đồng thời, nghiên cứu sinh đưa ra Luận đề chính cho Công trình nghiên cứu của mình như sau: "Trong bối cảnh hiện nay, tội phạm công nghệ cao vừa là một thách thức vừa là một sản phẩm mới của thời đại cùng với những tác động tiêu cực vô cùng lớn tới mỗi cá nhân, pháp nhân, quốc gia hay thậm chí của cả cộng đồng; chính vì thế, cơ sở pháp lý, nội dung và phương thức hợp tác quốc tế trong quá trình đấu tranh loại tội phạm này cũng có nhiều nét đặc thù và rất cần đến sự tận tâm, thiện chí của các chủ thể trên thực tế".

Xoay quanh luận đề chính, nghiên cứu sinh đã thiết kế hệ thống lập luận để chứng minh cho luận đề chính của mình. Hệ thống những lập luận đi kèm những số liệu, bảng biểu, bằng chứng thực tế hay các dẫn chứng thực tiễn và có trích dẫn bằng các nguồn xác thực, đáng tin cậy... Kết hợp tất cả những lập luận này để minh chứng cho luận đề chính của luận án tiến sĩ của mình (xem cụ thể trong các phần sau của luận án).

7. Kết cấu của luận án

Ngoài phần mở đầu và kết luận, cấu trúc của luận án gồm 4 chương:

- Chương 1: Tổng quan tình hình nghiên cứu những vấn đề liên quan đến đề tài luận án;

- Chương 2: Một số vấn đề lý luận về tội phạm công nghệ cao và pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

- Chương 3: Nội dung pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao và thực tiễn thực hiện của một số quốc gia.

- Chương 4: Pháp luật và thực tiễn hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao của Việt Nam.

CHƯƠNG 1
TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU NHỮNG VẤN ĐỀ LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN

* * *

Cuộc cách mạng công nghiệp lần thứ 4.0 không chỉ đơn thuần là một xu thế tất yếu mà nó đã trở thành thực tiễn sôi động diễn ra tại hầu khắp các quốc gia trên thế giới cũng như trên phạm vi toàn cầu. Bên cạnh những lợi ích to lớn đưa lại, chính nó cũng đem đến những thách thức an ninh phi truyền thống không hề nhỏ đối với mỗi quốc gia, khu vực. Kể từ cuối những năm 90, đầu những năm 2000 cho đến nay, thuật ngữ "*tội phạm công nghệ cao*" thường xuyên được đề cập đến với tần suất tăng dần trên cả bình diện pháp lý-thực tiễn, trên nhiều cấp độ từ quốc tế, khu vực cho đến quốc gia và đã trở thành đối tượng khảo cứu trong nhiều công trình nghiên cứu khoa học của các tác

giả khác nhau ở nước ngoài cũng như tại Việt Nam và được đề cập tới thông qua một số dạng thức như tội phạm mạng; tội phạm máy tính; tội phạm liên quan đến máy tính; tội phạm hình sự công nghệ; tội phạm ảo; tội phạm điện tử. Tuy nhiên, các công trình nghiên cứu chủ yếu xoáy sâu vào loại hình tội phạm mạng hoặc chưa tiếp cận và nghiên cứu một cách hệ thống, toàn diện và đầy đủ về tội phạm công nghệ cao trên tất cả các bình diện lý luận, pháp lý và thực tiễn. Hay các công trình tiếp cận dưới góc độ pháp lý quốc tế hầu như chưa được quan tâm nhiều; các công trình chủ yếu tiếp cận thông qua góc độ luật hình sự quốc gia và thể hiện dưới dạng các bài báo ngắn đăng trên các tạp chí chuyên ngành nên cũng chỉ đề cập được một vài khía cạnh của tội phạm công nghệ cao. Trên cơ sở đối chiếu với mục đích, nhiệm vụ nghiên cứu của luận án và những hạn chế của các công trình đã thực hiện, luận án sẽ làm rõ những vấn đề sau để làm sáng tỏ dưới các góc độ lý luận, pháp lý và thực tiễn hợp tác đấu tranh phòng chống tội phạm công nghệ cao trong pháp luật quốc tế và Việt Nam bao gồm:

*** Về lý luận:** luận án sẽ phân định và làm rõ nội hàm của các thuật ngữ đang được sử dụng không thống nhất nhưng có liên quan trực tiếp đến tội phạm công nghệ cao, từ đó đúc rút và xây dựng một định nghĩa bao quát về tội phạm công nghệ cao đặc biệt đặt trong bối cảnh và tình hình thực tiễn hiện nay và những vấn đề lý luận trong hợp tác quốc tế trong đấu tranh, phòng chống tội phạm nói chung và đặc biệt trong công tác phòng chống tội phạm công nghệ cao nói riêng (nguồn luật, nội dung, vai trò và phương thức hợp tác).

*** Về pháp lý:** luận án sẽ tập trung nghiên cứu một cách tổng thể và có hệ thống đối với những vấn đề pháp lý liên quan đến tội phạm công nghệ cao và hợp tác quốc tế trong công tác phòng chống loại hình tội phạm này, đặc biệt là quy định trong một số văn kiện hiện nay mà điển hình là Công ước Budapest về tội phạm mạng của Ủy hội châu Âu cùng các điều ước quốc tế và văn bản khác có liên quan. Luận án cũng sẽ mở rộng phạm vi tìm hiểu tới việc thực hiện pháp luật quốc tế trong hợp tác đấu tranh phòng, chống tội phạm công nghệ cao của một số quốc gia điển hình; qua đó, đúc rút một số giá trị kinh nghiệm, bài học tham khảo đối với Việt Nam liên quan đến vấn đề này.

*** Về thực tiễn:** luận án sẽ đánh giá thực trạng tình hình và diễn biến cập nhật của các loại hình tội phạm công nghệ cao trên cả phương diện quốc tế và tại Việt Nam; qua đó, đưa ra những dự báo và giải pháp có tính ứng dụng trong quá trình hợp tác đấu tranh, phòng chống tội phạm công nghệ cao hiện nay. Ngoài ra, luận án sẽ tập trung đánh giá hoạt động xây dựng và thực thi pháp luật quốc tế cũng như pháp luật Việt Nam trong lĩnh vực hợp tác đấu tranh phòng chống tội phạm công nghệ cao theo các tiêu chí của nguyên tắc Pacta sunt servanda. Trên cơ sở đó, luận án cũng sẽ tiếp tục nhận định về vấn đề các quy định của pháp luật hiện hành để đưa ra những phương hướng, giải pháp toàn diện trên nhiều góc độ nhằm hoàn thiện pháp luật và nâng cao hiệu quả trong công tác hợp tác đấu tranh phòng chống tội phạm công nghệ cao, nhất là tại Việt Nam, đặc biệt đặt trong bối cảnh bùng nổ của cuộc cách mạng công nghiệp lần thứ 4.0 hiện nay.

CHƯƠNG 2
MỘT SỐ VẤN ĐỀ LÝ LUẬN VỀ TỘI PHẠM CÔNG NGHỆ CAO VÀ PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO

***

2.1. Khái niệm tội phạm công nghệ cao và hợp tác đấu tranh, phòng chống tội phạm công nghệ cao

Trước khi nghiên cứu về pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao, cần phải làm rõ các nội hàm một số khái niệm như "tội phạm công nghệ cao", "hợp tác đấu tranh" để từ đó có thể thống nhất khái niệm về các quan hệ pháp luật, quy phạm pháp luật điều chỉnh vấn đề này, qua đó xác định cơ sở, nội dung, nguyên tắc, chủ thể, hình thức và các thiết chế trong việc hợp tác đấu tranh phòng chống tội phạm công nghệ cao.

2.1.1. Khái niệm tội phạm công nghệ cao

2.1.1.1. Định nghĩa tội phạm công nghệ cao

Về mặt thuật ngữ, khái niệm "tội phạm công nghệ cao" trong luật pháp của nhiều nước trên thế giới như Australia, Mỹ, Anh… đã có định nghĩa liên

quan đến tội phạm này như: tội phạm công nghệ cao (*high-tech crime*); tội phạm mạng (*cybercrime*); tội phạm ảo (*Virtual Crime*); tội phạm máy tính/tội phạm tin học (*computer crime*); tội phạm liên quan đến máy tính (*computer-related crime*); tội phạm được kích hoạt / hỗ trợ bởi công nghệ (*Technologically Enabled/Supported Crime*)...

Qua nghiên cứu các định nghĩa và các cách tiếp cận trên, hoàn toàn có thể thấy những điểm chung trong nội hàm của các khái niệm này; tất cả đều hướng tới các hành vi liên quan đến việc sử dụng máy tính, thiết bị số, khai thác mạng máy tính, mạng viễn thông một cách bất hợp pháp để gây tổn hại cho lợi ích của các tổ chức, cá nhân và toàn xã hội. Vì vậy, có thể rút ra một định nghĩa chung về tội phạm công nghệ cao như sau: *tội phạm công nghệ cao là một dạng thức tội phạm được tiến hành thông qua việc sử dụng tri thức, kỹ năng, công cụ, phương tiện và thành tựu của công nghệ thông tin ở trình độ cao, tác động một cách bất hợp pháp đến thông tin số và các dữ liệu điện tử được lưu trữ, xử lý, truyền tải trong hệ thống máy tính và các thiết bị công nghệ cao, xâm phạm đến trật tự an toàn thông tin, gây tổn hại nghiêm trọng đến quyền và lợi ích hợp pháp của các cá nhân, tổ chức cũng như của các quốc gia và cộng đồng quốc tế.*

2.1.1.2. Đặc điểm của tội phạm công nghệ cao

Thứ nhất, tội phạm công nghệ cao là những hành vi nguy hiểm cho xã hội, sự tương đồng trong các cấu thành cơ bản của một tội phạm... Tuy nhiên, điểm khác biệt cốt lõi giữa chúng với tội phạm khác nằm ở khía cạnh "công nghệ thông tin, máy tính và mạng internet" đóng vai trò, mức độ quyết định trong việc thực hiện, che giấu và gây ra những hậu quả khôn lường đối với xã hội của hành vi phạm tội.

Thứ hai, về chủ thể của tội phạm, tội phạm công nghệ cao được thực hiện bởi các đối tượng có kiến thức cập nhật và am hiểu sâu về máy tính. Tuy nhiên, cũng có trường hợp chủ thể là những người không hiểu biết đầy đủ về các quy định liên quan đến vận hành, khai thác và sử dụng mạng máy tính hoặc các công cụ điện tử dẫn đến những thiệt hại ngoài ý muốn.

Thứ ba, về tính chất của hành vi phạm tội và các hành vi có liên quan đến tội phạm công nghệ cao thường rất tinh vi, tinh xảo.

Ngoài các đặc điểm khác biệt cơ bản kể trên, cũng có thể thấy một số dấu hiệu đặc thù khác so với các nhóm tội phạm thông thường như tính quốc tế, tính xuyên biên giới của loại tội phạm này; tính chất ngày càng tăng về số lượng và hậu quả, tinh vi về cách thức tiến hành cùng với sự phát triển của cuộc cách mạng khoa học công nghệ...

2.1.1.3. Phân loại tội phạm công nghệ cao

Một cách phân loại phổ biến trên thế giới hiện nay là phân loại tội phạm sử dụng công nghệ cao theo cách thức, mục tiêu thực hiện tội phạm; theo đó, tội phạm công nghệ cao bao gồm hai nhóm:

- Nhóm thứ 1: Tội phạm có mục tiêu chính là mạng máy tính và thiết bị
- Nhóm thứ 2: Tội phạm sử dụng mạng máy tính hoặc thiết bị để làm công cụ hỗ trợ cho hoạt động phạm tội

Dựa trên vai trò của máy tính trong hành vi phạm tội thì tội phạm công nghệ cao bao gồm những tội phạm có sự liên can, dính líu của máy tính tới tội phạm với ba vai trò sau:

- Máy tính là mục đích của tội phạm
- Máy tính là công cụ phạm tội
- Máy tính là vật trung gian để cất giấu, lưu trữ những thứ đã chiếm đoạt được

Căn cứ vào tính chất hoạt động của hành vi phạm tội, tội phạm công nghệ cao có thể được chia ra làm nhiều dạng thức như:

- Thứ nhất, Hacking (Xâm nhập):
- Thứ hai, Identity Theft (Mạo danh).
- Thứ ba, Fraud (Gian lận).
- Thứ tư, Predators (Kẻ săn mồi): Đây là dạng tội phạm mạng chuyên sử dụng mạng xã hội để tìm kiếm nạn nhân và thu thập thông tin.

Tại Việt Nam, Hướng dẫn 16/HD-BCA-C41 ngày 31/12/2013 của Bộ Công an hướng dẫn thực hiện một số quy định trong các Thông tư 18, 19, 20, 21, 22 ngày 01/04/2013 của Bộ trưởng Bộ Công an quy định về công tác nghiệp vụ cơ bản của lực lượng Cảnh sát nhân dân có hướng dẫn việc phân chia các nhóm đối tượng phạm tội có sử dụng công nghệ cao thành hai hệ là: Hệ xâm phạm hoạt động của mạng máy tính, viễn thông và Hệ lợi dụng mạng

máy tính, viễn thông để hoạt động bất hợp pháp. Theo đó, tội phạm sử dụng công nghệ cao được phân loại như sau: (i) Tội phạm sử dụng máy tính, thiết bị số, mạng máy tính, mạng viễn thông gây tổn hại tính bảo mật, tính toàn vẹn và tính khả dụng của hệ thống máy tính; và (ii) Tội phạm sử dụng máy tính, thiết bị số, mạng máy tính, mạng viễn thông làm công cụ, phương tiện phạm tội.

2.1.2. Khái niệm hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Hợp tác đấu tranh phòng chống tội phạm công nghệ cao là việc các quốc gia cũng như các chủ thể khác của luật quốc tế trên cơ sở pháp luật quốc gia, điều ước quốc tế hay các tập quán quốc tế, cũng như các nguyên tắc khác tiến hành phối hợp, giúp đỡ nhau trong xây dựng cơ sở pháp lý và thực hiện tương trợ tư pháp về hình sự, dẫn độ, tiếp nhận, chuyển giao người bị kết án và các hoạt động hợp tác khác nhằm phục vụ cho việc điều tra, truy tố, xét xử, thi hành án và trừng trị tội phạm công nghệ cao.

2.1.2.2. Đặc điểm hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Trên cơ sở khái niệm hợp tác đấu tranh phòng chống tội phạm công nghệ cao, có thể rút ra một số đặc điểm cơ bản như sau:

Thứ nhất, về chủ thể hợp tác

Thứ hai, về đối tượng hợp tác

Thứ ba, mục tiêu hợp tác

Thứ tư, về hình thức hợp tác

2.2. Lý luận về pháp luật quốc tế trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao

2.2.1. Định nghĩa và đặc điểm của pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao

Pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao bao gồm tổng thể các nguyên tắc và các quy phạm pháp luật điều chỉnh quan hệ giữa các chủ thể luật quốc tế trong việc tiến hành toàn bộ những hoạt động cần thiết giữa các bên, nhằm ngăn ngừa, trừng trị, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế cũng như đời sống quốc gia.

2.2.2. Nguồn của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Ở phạm vi toàn cầu, đến nay mới chỉ có một điều ước quốc tế điều chỉnh loại tội phạm này là Công ước về tội phạm mạng của Uỷ hội châu Âu năm 2001 (Công ước Budapest). Bên cạnh công ước Budapest, một số nội dung của Công ước Palermo về chống tội phạm có tổ chức liên quốc gia năm 2000 mặc dù không trực tiếp đề cập một cách cụ thể đến các loại hình tội phạm công nghệ cao nhưng Công ước Palermo với 41 điều khoản, luôn được coi là một sự tham khảo cần thiết trong quá trình hợp tác quốc tế đấu tranh phòng chống tội phạm.

Ở phạm vi khu vực, một số khuôn khổ pháp lý đã được hình thành làm cơ sở pháp lý cho hoạt động hợp tác giữa các thành viên của một số khu vực trong ngăn ngừa, phòng chống tội phạm công nghệ cao, bao gồm chủ yếu hai loại: các điều ước quốc tế khu vực và các văn bản do những cơ quan có thẩm quyền của các tổ chức quốc tế thông qua, có giá trị pháp lý ràng buộc với các quốc gia thành viên trong ngăn ngừa, phòng chống tội phạm công nghệ cao

Ở phạm vi song phương, phổ biến nhất vẫn là các điều ước quốc tế về tương trợ tư pháp hình sự, dẫn độ, chuyển giao người bị kết án được ký kết giữa các quốc gia.

Bên cạnh đó, tập quán quốc tế cũng có vai trò nhất định trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao.

Cùng với các loại nguồn có giá trị pháp lý ràng buộc như trên, một số các loại nguồn không có giá trị pháp lý ràng buộc, đặc biệt là Nghị quyết mang tính khuyến nghị của các tổ chức quốc tế liên chính phủ và phán quyết của các cơ quan tài phán quốc tế cũng có vai trò quan trọng trong điều chỉnh hoạt động phòng chống tội phạm công nghệ cao.

2.2.3. Nguyên tắc của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

2.2.3.1. Các nguyên tắc chung của pháp luật quốc tế

Hợp tác quốc tế đấu tranh phòng chống tội phạm nói chung và phòng chống tội phạm công nghệ cao là một trong những hoạt động thuộc đối tượng điều chỉnh của luật quốc tế. Do đó, các nguyên tắc của pháp luật quốc tế trong

đấu tranh phòng chống tội phạm công nghệ cao trước tiên cũng bao gồm các nguyên tắc cơ bản của pháp luật quốc tế nói chung, đặc biệt là nguyên tắc bình đẳng tôn trọng về độc lập chủ quyền, không can thiệp vào công việc nội bộ của nhau; nguyên tắc các quốc gia có nghĩa vụ hợp tác và đặc biệt là nguyên tắc Pacta sunt Servanda...

2.2.3.2. Các nguyên tắc đặc thù

Bên cạnh những nguyên tắc chung của luật quốc tế, pháp luật quốc tế trong phòng chống tội phạm công nghệ cao còn được điều chỉnh bởi một số nguyên tắc riêng biệt sau:

***Thứ nhất*,** nguyên tắc có đi có lại

Nguyên tắc có đi có lại thực chất xuất phát từ nguyên tắc bình đẳng về chủ quyền giữa các quốc gia. Theo đó, trên cơ sở bình đẳng về chủ quyền, quốc gia có quyền "ứng xử" với quốc gia khác tương tự như cách thức mà quốc gia đó đã, đang hoặc sẽ "ứng xử" với mình.

Trong luật hình sự quốc tế, các hoạt động hợp tác đấu tranh phòng chống tội phạm được thực hiện trên những cơ sở, *một là* điều ước quốc tế, *hai là* tập quán quốc tế và *ba là* pháp luật quốc gia. Trong trường hợp có điều ước quốc tế, những vấn đề pháp lý liên quan đến các hoạt động hợp tác cụ thể sẽ được điều chỉnh bằng chính những quy định của điều ước quốc tế đó, ví dụ những vấn đề pháp lý về dẫn độ như các trường hợp dẫn độ, các trường hợp bắt buộc từ chối dẫn độ, các trường hợp cân nhắc để từ chối dẫn độ hay tài liệu cần thiết, chi phí, giải quyết yêu cầu dẫn độ khi có nhiều quốc gia cùng đưa ra yêu cầu…sẽ được ghi nhận cụ thể trong các điều ước về dẫn độ như hiệp định dẫn độ song phương, đa phương, hiệp định tương trợ tư pháp hình sự có phạm vi điều chỉnh cả vấn đề dẫn độ. Khi không có điều ước quốc tế, các hoạt động hợp tác sẽ được thực hiện trên cơ sở tập quán quốc tế hoặc pháp luật quốc gia. Trong trường hợp này, nguyên tắc có đi có lại sẽ trở thành cơ sở vô cùng quan trọng để các quốc gia cân nhắc việc có hay không tiến hành các hoạt động hợp tác theo yêu cầu của quốc gia hữu quan, đặc biệt đối với các yêu cầu về dẫn độ tội phạm và tương trợ tư pháp hình sự.

Thứ hai, nguyên tắc hợp tác với phạm vi rộng nhất có thể

Nguyên tắc hợp tác với phạm vi rộng nhất có thể được ghi nhận trong Công ước Bundapest với nội dung: Các quốc gia thành viên phải hợp tác với nhau, phù hợp với các quy định trong chương này, và thông qua việc áp dụng các văn bản quốc tế về hợp tác quốc tế trong lĩnh vực hình sự, và luật của quốc gia mình, với phạm vi rộng nhất có thể để phục vụ việc điều tra, tiến hành các hoạt động tố tụng liên quan đến các tội phạm hình sự có liên quan đến hệ thống máy tính và dữ liệu máy tính, hoặc để thu thập chứng cứ dưới hình thức điện tử (Điều 23).

2.2.4. Nội dung của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Nội dung của pháp luật quốc tế trong hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao rất đa dạng bao gồm: *Một là*, pháp luật quốc tế đặt ra và xác định rõ nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luật cũng như xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao. Xây dựng cơ sở pháp lý quốc gia cho các hoạt động ứng phó với tội phạm công nghệ cao cũng là một nghĩa vụ mang tính truyền thống trên cơ sở của nguyên tắc Pacta sunt Servanda. *Hai là*, tương trợ tư pháp hình sự. Xuất phát từ chủ quyền quốc gia, cơ quan tố tụng của quốc gia nào chỉ được thực hiện hoạt động tố tụng trên lãnh thổ của quốc gia đó. Tuy nhiên, trong nhiều trường hợp, việc giải quyết các vụ việc lại vượt ngoài phạm vi biên giới quốc gia. *Ba là*, dẫn độ tội phạm. Thông qua việc chuyển giao người phạm tội đang trốn chạy trên lãnh thổ quốc gia cho quốc gia được yêu cầu, quốc gia này mới có thể tiến hành các hoạt động tố tụng để đảm bảo mọi hành vi phạm tội đều phải bị trừng phạt trước pháp luật. *Bốn là*, chuyển giao người đã bị kết án ở nước ngoài cho quốc gia mà người đó là công dân để chấp hành hình phạt tù theo bản án mà toà án đã tuyên. *Năm là*, phân định thẩm quyền tài phán hình sự trên cơ sở một số nguyên tắc là hoạt động để xác định quốc gia có thẩm quyền tài phán đối với tội phạm công nghệ cao trong trường hợp hành vi phạm tội có liên quan đến nhiều quốc gia.

2.2.5. Vai trò của pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao

Pháp luật quốc tế chính là cơ sở để các quốc gia tiến hành những hoạt động hợp tác này. Thông qua các nội dung hợp tác như hình thành các cơ quan, thiết chế quốc tế trong phòng chống tội phạm công nghệ cao; hài hoà hoá pháp luật; tương trợ tư pháp hình sự; dẫn độ; tiến hành phối hợp điều tra… pháp luật quốc tế đã hình thành nên một cơ chế pháp lý chung ở các cấp độ khác nhau, từ song phương, khu vực đến toàn cầu để kết nối hoạt động giữa các quốc gia, từ đó, ứng phó hiệu quả với tội phạm công nghệ cao, góp phần hạn chế, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế.

CHƯƠNG 3
NỘI DUNG PHÁP LUẬT QUỐC TẾ TRONG HỢP TÁC ĐẤU TRANH, PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO VÀ THỰC TIỄN THỰC HIỆN CỦA MỘT SỐ QUỐC GIA

3.1. Pháp luật quốc tế quy định nghĩa vụ cho các quốc gia trong việc hài hòa hóa pháp luật và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động đấu tranh, phòng chống tội phạm công nghệ cao

3.1.1. Hài hoà hoá pháp luật của các quốc gia trong phòng chống tội phạm công nghệ cao

Hài hoà hoá pháp luật được ghi nhận như một trong những nội dung căn bản nhằm tạo ra sự tương đồng giữa hệ thống pháp luật của các nước, từ đó, góp phần 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 tránh việc tạo ra kẽ hở để người phạm tội có thể trốn tránh khỏi việc bị pháp luật trừng trị. 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. Hài hoà hoá pháp luật có thể ngăn chặn việc người phạm tội lợi dụng sự khác biệt trong quy định pháp luật giữa các quốc gia để trốn tránh khỏi sự trừng phạt của pháp luật, đồng thời, tạo điều kiện tăng cường hoạt động hợp tác quốc tế giữa các quốc gia trong ngăn ngừa, trừng phạt tội phạm công nghệ cao, đặc biệt liên quan đến các yêu cầu về dẫn độ, tương trợ tư pháp hình sự.

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

Theo quy định tại 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: *Một là,* nhóm hành vi chống lại sự bí mật, toàn vẹn và sẵn có của dữ liệu máy tính và hệ thống máy tính 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; *Hai là,* 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; *Ba là,* những hành vi liên quan đến các tài liệu khiêu dâm trẻ em; *Bốn là*, các hành vi xâm phạm quyền tác giả và quyền liên quan và *năm là,* hành vi nỗ lực và hỗ trợ cho việc thực hiện những hành vi trên. 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 trên, dẫn đến việc thực hiện những hành 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).

Ngoài các 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 bổ trường châu Âu thông qua hay Chỉ thị của Cộng đồng kinh tế của các quốc gia Tây Phi do Nghị viện thông qua cũng ghi nhận nghĩa vụ của các QGTV phải ban hành luật trong nước để quy định những hành vi được liệt kê trong văn kiện này là tội phạm hình sự. Việc xác định những hành vi nào sẽ bị coi là tội phạm ở các văn kiện không giống nhau, vì 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.

3.1.1.2. Hài hoà hoá hình phạt

Vấn đề hài 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 với từng hành vi và pháp luật hình sự của các quốc gia phải quy định hình phạt không được thấp hơn ngưỡng hình phạt tối thiểu này.

Cấp độ hài hoà hoá hình phạt phổ biến hiện nay là ghi nhận các nguyên tắc chung trong việc xác định hình phạt, còn việc quy định cụ thể sẽ do mỗi quốc gia tự xác định. Theo đó, những nguyên tắc được quy định phổ biến để xác định hình phạt bao gồm: Tương xứng, hiệu quả, có tính răn đe. Nguyên tắc này được ghi nhận tại hầu hết các văn kiện như ở 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.

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, sự thiện chí và mong muốn làm sâu thêm mức độ hợp tác giữa các bên. Hai yếu tố này có mối liên hệ chặt chẽ với nhau. Nếu không có sự tương đồng giữa các thành viên thì 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 thiện chí và bày tỏ mong muốn nâng cao hợp tác thì điều này cũng không thể đạt được.

3.1.2. Xây dựng và hoàn thiện cơ sở pháp lý quốc gia cho các hoạt động ứng phó với tội phạm công nghệ cao

Theo quy định của luật quốc tế, quốc gia có nghĩa vụ tôn trọng và thực hiện đầy đủ các cam kết quốc tế của quốc gia. Tuy nhiên, nguyên tắc Pacta sunt Servanda chỉ đặt ra nghĩa vụ cho quốc gia phải thực hiện những cam kết quốc tế của mình một cách tận tâm và thiện chí còn việc thực hiện như thế nào và theo cách thức nào, thường do quốc gia tự quyết định trên cơ sở chủ quyền của mình phù hợp với các quy định của pháp luật quốc gia. Do vậy, quốc gia, trên cơ sở chủ quyền, sẽ quyết định về việc thực hiện cam kết quốc tế theo một trong hai cách thức, hoặc áp dụng trực tiếp các quy định của cam kết quốc tế trên phạm vi lãnh thổ quốc gia hoặc chuyển hoá (nội luật hóa) những quy định của các cam kết quốc tế vào pháp luật quốc gia thông qua việc ban hành các văn bản quy phạm pháp luật mới hay sửa đổi, bổ sung những văn bản hiện hành để đảm bảo sự tương thích với các cam kết quốc tế đó. Tuy nhiên, cũng có một vài ngoài lệ, đó là trường hợp một số điều ước quốc tế trực tiếp quy định nghĩa vụ của quốc gia phải ban hành pháp luật để thực hiện các quy định của điều ước, điển hình như trong lĩnh vực quyền con người, rất nhiều Công ước đã ghi nhận điều khoản với nội dung "*Các quốc gia thành viên phải thực hiện các biện pháp lập pháp nhằm đảm bảo các quyền được ghi nhận trong Công ước*" như Công ước về quyền dân sự chính trị (Điều 2), Công ước về quyền kinh tế, xã hội, văn hoá (Điều 2), Công ước chống tra tấn và các hình thức trừng phạt hay đối xử tàn bạo, vô nhân đạo hoặc hạ thấp nhân phẩm (Điều 2), Công ước về quyền trẻ em (Điều 4)…

3.2. Tương trợ tư pháp hình sự

3.2.1. Nội dung tương trợ tư pháp hình sự

Nguyên tắc tương trợ tư pháp được ghi nhận trong Công ước Budapest là QGTV phải đảm bảo việc cung cấp hoạt động tương trợ tư pháp rộng nhất có thể để phục vụ cho công tác điều tra hoặc tố tụng liên quan đến các tội phạm về máy tính hoặc dữ liệu máy tính hay thu thập các chứng cứ dưới hình thức điện tử về tội phạm.

Ngoài những nội dung phổ biến như trên, một số điều ước quốc tế về tội phạm công nghệ cao như Công ước Budapest, Công ước Arab về chống tội phạm công nghệ thông tin… đã ghi nhận những nội dung tương trợ tư pháp hình sự riêng biệt liên quan đến loại tội phạm này, bao gồm:

(1) Tương trợ tư pháp liên quan đến các biện pháp tạm thời: là những biện pháp mang tính tình thế mà một quốc gia yêu cầu một quốc gia khác thực hiện với mục đích ứng phó với hoàn cảnh khẩn cấp của vụ việc đang giải quyết nhằm kịp thời thu thập chứng cứ, bảo vệ bằng chứng cho quá trình tiến hành các hoạt động tố tụng sau này.

(2) *Tương trợ tư pháp trong hoạt động điều tra:* trong quá trình tiến hành hoạt động điều tra, các quốc gia có thể yêu cầu quốc gia khác thực hiện một số hoạt động tương trợ tư pháp liên quan đến truy cập, thu thập dữ liệu hoặc chặn dữ liệu nội dung.

(3) *Thiết lập Mạng lưới 24/7:* mạng lưới 24/7 là một điểm liên lạc hoạt động 24 giờ một ngày và 7 ngày trong tuần để cung cấp sự hỗ trợ kịp thời trongviệc điều tra hoặc tiến hành các hoạt động tố tụng đối với tội phạm liên quan đến hệ thống máy tính hoặc dữ liệu máy tính, thu thập chứng cứ dưới hình thức điện tử.

(4) Truy cập xuyên biên giới dữ liệu máy tính được lưu trữ: QGTV có thể truy cập xuyên biên giới dữ liệu máy tính được lưu trữ với sự nhất trí của QGTV khác (Điều 32 Công ước Budapest).

Tuy nhiên, trong một số trường hợp đặc biệt, QGTV có thể thực hiện hoạt động này mà không cần sự cho phép của quốc gia liên quan. Ngoại lệ này được ghi nhận trong Công ước Budapest, bao gồm:

Một là, truy cập dữ liệu máy tính được lưu trữ sẵn có (nguồn mở) bất kể dữ liệu này đặt tại khu vực nào;

Hai là, truy cập hoặc tiếp nhận, thông qua hệ thống máy tính trên lãnh thổ nước mình, dữ liệu máy tính được lưu trữ đang đặt trên lãnh thổ QGTV khác nếu quốc gia nhận được sự nhất trí một cách hợp pháp và tự nguyện từ người có quyền hợp pháp được tiết lộ dữ liệu cho quốc gia liên quan thông qua hệ thống máy tính đó.

3.2.2. Thủ tục, thể thức tương trợ tư pháp

Thủ tục tương trợ tư pháp đối với tội phạm công nghệ cao vừa được quy định trực tiếp tại các điều ước về tội phạm công nghệ cao cũng như được ghi nhận trong cả các điều ước riêng biệt về tương trợ tư pháp, các điều kiện và trình tự thủ tục tương trợ được tiến hành theo những thể thức sau đây:

- Quốc gia yêu cầu sẽ gửi yêu cầu tương trợ tư pháp bằng văn bản đến cơ quan được chỉ định làm cơ quan đầu mối tiếp nhận yêu cầu tương trợ tư pháp của quốc gia được yêu cầu, trong đó, ghi nhận cụ thể các nội dung cần tương trợ tư pháp.

- Sau khi đã nhận được yêu cầu tương trợ tư pháp hình sự đúng thủ tục, quốc gia được yêu cầu sẽ nghiên cứu và cho phép tiến hành các hoạt động tương trợ tư pháp theo yêu cầu trên lãnh thổ nước mình. Tuy nhiên luật tố tụng hình sự của nước yêu cầu có thể được áp dụng, nếu quốc gia được yêu cầu đồng ý chấp thuận.

Chi phí cho hoạt động tương trợ tư pháp trên lãnh thổ của quốc gia được yêu cầu thường do quốc gia yêu cầu thanh toán, trừ các trường hợp cụ thể khác do các bên thoả thuận.

Về vấn đề từ chối tương trợ tư pháp, các trường hợp không tương trợ tư pháp được quy định trong các điều ước liên

3.3. Dẫn độ

3.3.1. Điều kiện, thể thức dẫn độ

Về nguyên tắc, dẫn độ là quyền của quốc gia và xuất phát từ chủ quyền quốc gia. Trên cơ sở quyền lực tối cao trong phạm vi lãnh thổ, quốc gia có quyền quyết định có tiến hành chuyển giao hay không cá nhân đang hiện diện trên lãnh thổ nước mình cho quốc gia yêu cầu để tiến hành truy cứu trách nhiệm hình sự. Nhiều quốc gia đã ban hành các đạo luật chuyên biệt về dẫn độ, trong đó ghi nhận một trong những nguyên tắc quan trọng cho phép dẫn độ, đó là dẫn độ được tiến hành trên cơ sở của nguyên tắc có đi có lại.

Dẫn độ tội phạm là nghĩa vụ pháp lý quốc tế ràng buộc chỉ phát sinh khi giữa các quốc gia có liên quan tồn tại điều ước quốc tế tương ứng quy định các điều kiện cụ thể cho phép dẫn độ. Tuy nhiên, nghĩa vụ này không phải là tuyệt đối. Bởi lẽ, ngay cả trong trường hợp có điều ước thì dẫn độ cũng chỉ có thể được thực hiện theo đúng các thể thức, điều kiện phù hợp với quy định của điều ước quốc tế đó. Ngay tại Điều 1 Công ước châu Âu về dẫn độ mặc dù có tiêu đề là "Nghĩa vụ dẫn độ" nhưng đã thể hiện rất rõ điều này khi quy định rằng: *"Các bên ký kết tiến hành bắt giữ cho nhau, theo những điều khoản và điều kiện đặt ra trong Công ước này, tất cả những người mà cơ quan có thẩm quyền của quốc gia yêu cầu đang điều tra về hành vi phạm tội hoặc đang bị truy nã bởi cơ quan có thẩm quyền để chấp hành bản án hoặc các quyết định giam giữ"*.

Để có thể viện dẫn các điều ước về phòng chống tội phạm xuyên quốc gia làm căn cứ để dẫn độ, tội phạm công nghệ cao phải thoả mãn đầy đủ các điều kiện của tội phạm xuyên quốc gia. Theo quy định của Công ước Palermo, tội phạm xuyên quốc gia là tội phạm mà *hành vi phạm tội được thực hiện ở nhiều quốc gia hoặc được thực hiện ở một quốc gia, nhưng phần chủ yếu của việc chuẩn bị, lên kế hoạch, chỉ đạo hay điều khiển việc thực hiện tội phạm lại diễn ra ở một quốc gia khác, hoặc đây là hành vi tội phạm được thực hiện ở một quốc gia nhưng có liên quan đến một nhóm tội phạm có tổ chức tham gia thực hiện các hoạt động tội phạm ở nhiều quốc gia, hoặc tội phạm được thực hiện ở một quốc gia nhưng có ảnh hưởng nghiêm trọng đến một quốc gia khác (Điều 3)*.

3.3.2. Điều kiện dẫn độ, các trường hợp không dẫn độ

Điều kiện dẫn độ phổ biến được quy định là nguyên tắc "định danh kép" kèm theo yêu cầu về thời hạn tù giam. Chẳng hạn, theo quy định tại Công ước Budapest, việc dẫn độ giữa các quốc gia thành viên Công ước được thực hiện với điều kiện là tội phạm đó bị trừng phạt về hình sự theo pháp luật của cả hai quốc gia liên quan với hình phạt tước đoạt tự do tối thiểu 1 năm trở lên hoặc hình phạt nặng hơn (Điều 24).

Liên quan đến các trường hợp không dẫn độ, các căn cứ từ chối dẫn độ tội phạm công nghệ cao nói riêng cũng như tội phạm nói chung thường được quy định phổ biến như:

- Không dẫn độ tội phạm chính trị hoặc không dẫn độ công dân nước mình.
- Hành vi làm căn cứ yêu cầu dẫn độ đã được xét xử tại quốc gia được yêu cầu *(Nguyên tắc Non bis in idem – Không ai bị xét xử về cùng một hành vi phạm tội)*
- Việc dẫn độ không phù hợp với pháp luật của quốc gia được yêu cầu, xâm phạm chủ quyền quốc gia hoặc trật tự an ninh xã hội;

3.4. Chuyển giao người bị kết án

Điều kiện phổ biến để chuyển giao người bị kết án được quy định trong các điều ước bao gồm: (1) Người bị kết án là công dân của nước thi hành án; (2) Bản án đã tuyên là bản án cuối cùng, chưa còn thủ tục nào chưa giải quyết liên quan đến người bị kết án; (3) Có sự đồng ý của người bị kết án; (4) Vào thời điểm nhận được yêu cầu chuyển giao, thời gian chấp hành hình phạt còn lại theo bản án đã tuyên phải không ít hơn thời gian được quy định trong điều ước quốc tế hoặc pháp luật quốc gia; (5) Đáp ứng điều kiện "định danh kép" theo luật hình sự của các nước tuyên án và nước thi hành án; (6) Nước tuyên án và nước thi hành án đồng ý chuyển giao.

3.5. Xác định thẩm quyền tài phán

Có thể nhận thấy một số nguyên tắc của Luật hình sự quốc tế trong xác định thẩm quyền tài phán hoàn toàn áp dụng đối với tội phạm công nghệ cao, bao gồm:

- ***Nguyên tắc lãnh thổ***

Nguyên tắc lãnh thổ được ghi nhận trong Công ước Budapest với nội dung, QGTV ban hành luật và các biện pháp cần thiết khác để thực hiện thẩm quyền tài phán đối với *các hành vi tội phạm được thực hiện trên lãnh thổ nước mình*.

Trên thực tế, nguyên tắc lãnh thổ được các quốc gia quy định thành những căn cứ khác nhau để xác định thẩm quyền tài phán, bao gồm:

Một là, nơi thực hiện hành vi.

Hai là, nơi đặt máy tính.

Ba là, nơi bị tác động của hành vi phạm tội.

- ***Nguyên tắc quốc tịch***

Theo quy định của Công ước Budapest, quốc gia có thẩm quyền tài phán đối với người phạm tội mang quốc tịch của quốc gia nếu hành vi đó bị trừng phạt theo luật hình sự của quốc gia nơi hành vi đó được thực hiện hoặc hành vi được thực hiện ngoài lãnh thổ của bất kì quốc gia nào (Điểm (d) Khoản 1 Điều 22). Luật hình sự của nhiều quốc gia đã ghi nhận nguyên tắc này để xác định thẩm quyền tài phán quốc gia.

Ngoài quốc tịch của người phạm tội như quy định của Công ước Budapest, một số quốc gia cũng quy định quốc tịch của nạn nhân như một căn cứ để xác định thẩm quyền tài phán.

- ***Nguyên tắc quốc tịch của tàu thuyền, phương tiện bay***

Theo quy định của Công ước Budapest, quốc gia sẽ có thẩm quyền tài phán đối với tội phạm công nghệ cao nếu hành vi được thực hiện trên tàu thuyền treo cờ của quốc gia hoặc phương tiện bay đăng ký tại quốc gia (Điểm b, c Khoản 1 Điều 22).

Không có thứ bậc ưu tiên giữa các nguyên tắc xác định thẩm quyền tài phán. Việc xác định thẩm quyền tài phán thuộc về quốc gia nào, phụ thuộc phần lớn vào cơ quan giải quyết tranh chấp.

3.6. Thực tiễn thực hiện pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao của một số quốc gia

3.6.1. Cộng hòa Liên bang Đức

Cộng hòa Liên bang Đức đã phê chuẩn Công ước Budapest vào năm 2009 và cũng đã tiến hành sửa đổi Bộ luật Hình sự ngay sau khi phê chuẩn Công ước. Bộ luật Hình sự của Đức bao gồm tất cả các điều khoản tương đối toàn diện và tương thích với quy định cơ bản của Công ước về tội phạm máy tính và tội phạm mạng. Tương tự như vậy, Bộ luật Tố tụng hình sự của nước này cũng đề cập đến hầu hết các quyền tố tụng có liên quan đã được nêu trong Công ước, tuy nhiên có loại trừ một số điều khoản (sẽ được đề cập ở các phần tiếp theo).

Tính đến nay Cộng hòa Đức đã ban hành một số lượng khá lớn văn bản luật pháp liên quan trong lĩnh vực an ninh thông tin, bao gồm văn bản được ban hành ở cấp độ Luật, Đạo luật. Đạo luật chính liên quan đến an ninh mạng ở Đức là Đạo luật An ninh mạng, Đạo luật Viễn thông, Quy định bảo vệ dữ liệu chung của EU, Đạo luật Bảo vệ dữ liệu liên Bang và Đạo luật Văn phòng liên Bang về bảo mật thông tin

Các đạo luật về an ninh mạng của Đức đã có những quy định cụ thể các điều kiện về bảo đảm các tiêu chuẩn an ninh mạng đối với các sản phẩm, dịch vụ mạng thiết yếu; quy định về trách nhiệm bảo vệ và các hoạt động bảo mật, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; quy định về quyền và trách nhiệm pháp lý cho các doanh nghiệp lưu trữ web và nhà cung cấp truy cập cho các vi phạm bản quyền xảy ra trên hệ thống của họ... Nhìn chung, luật pháp về vấn đề hợp tác đấu tranh phòng chống tội phạm trong lĩnh vực công nghệ thông tin ở Đức phù hợp với những tiêu chuẩn quốc tế trong lĩnh vực này, đặc biệt là Công ước Budapest năm 2001.

3.6.2. Hoa Kỳ

Pháp luật Hoa Kỳ từ lâu đã được biết đến là một trong những hệ thống pháp luật toàn diện, lâu đời và hiệu quả nhất trên thế giới về bảo toàn an ninh mạng cũng như hợp tác phòng ngừa tội phạm công nghệ cao. Trên cả bình diện pháp lý và thực tiễn, Hoa Kỳ luôn xác định mối đe dọa về an ninh mạng là mối đe doạ hàng đầu đối với an ninh quốc gia. Chính vì vậy, trong Luật An ninh nội địa Hoa Kỳ (2002) quy định: *Nguy cơ an ninh mạng là các mối đe dọa và lỗ hổng của thông tin hoặc các hệ thống thông tin và bất kỳ hậu quả liên quan nào bị gây ra bởi hoặc là kết quả của việc truy cập trái phép, sử dụng, tiết lộ, làm suy giảm, gián đoạn, chỉnh sửa hoặc phá hoại các thông tin hoặc các hệ thống thông tin này, bao gồm hậu quả liên quan bởi các hành vi tấnc công và/hoặc khủng bố mạng; không bao gồm bất kỳ hành động nào chỉ liên quan đến việc vi phạm điều khoản hoặc thỏa thuận hợp đồng với khách hàng.* Đạo luật cũng đã thành lập thiết chế có tên gọi "Bộ An ninh nội địa Hoa Kỳ" (DHS), với thẩm quyền hoạt động như một bộ phận điều hành tối cáo vấn đề an ninh mạng của Hoa Kỳ. Nhiệm vụ chính của cơ quan này là ngăn chặn các cuộc tấn công khủng bố, giảm thiểu nguy cơ vũ trang và phi vũ trang đối với quốc gia, giảm thiểu thiệt hại từ các cuộc tấn công và tăng khả năng phục hồi quốc gia.

Bên cạnh đó, một số văn bản pháp luật khác có liên quan như Luật bảo vệ thông tin liên lạc điện tử, Luật Lưu trữ Truyền thông hay Luật nghe lén… 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 cao trên cơ sở phù hợp với tình hình của mỗi bang. Đây hầu hết là những văn bản luật có quy định chi tiết và cụ thể hơn so với luật chung của Liên 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 04 năm tù hoặc các hình phạt khác lên đến 15 năm tù tùy theo mức độ vi phạm.

3.6.3. Nhật Bản

Vào tháng 11 năm 2001, chính phủ Nhật Bản đã ký tham gia Công ước Budapest về tội phạm mạng của Ủy hội châu Âu. Theo đó, Nhật Bản đã tiến hành sửa đổi Bộ luật Hình sự và Bộ luật Tố tụng hình sự để tăng tính tương thích trong việc điều chỉnh phù hợp với các quy định của Công ước Budapest. Cùng với đó, Nhật Bản đã ban hành Luật bảo vệ thông tin cá nhân năm 2003 để bảo vệ dữ liệu, thông tin cá nhân và các dạng thức danh tính khác. Đặc biệt, Luật cơ bản về An ninh mạng của Nhật Bản (2014) còn mở rộng việc quy định xây dựng các tiêu chuẩn chung về các biện pháp đảm bảo an toàn an ninh mạng cho các cơ quan hành chính quốc gia và các tổ chức liên quan. Hiện tại, Nhật Bản cũng có các đạo luật khác cũng có quy định liên quan đến tội phạm công nghệ cao như Bộ luật Hình sự Nhật Bản Luật chống cạnh tranh không công bằng, Luật cấm truy cập máy tính trái phép, Luật bán trả góp, Luật bảo vệ bí mật được chỉ định đặc biệt và Luật an ninh xã hội và mã số thuế. Trên cơ sở các văn bản pháp luật của Nhật Bản quy định, có thể xác định một số hành vi phạm tội công nghệ cao cơ bản như:

- Lấy cắp dữ liệu hay truy cập trái phép (Hacking).
- Hành vi lừa đảo (Phishing)
- Hành vi lây nhiễm hệ thống CNTT với phần mềm độc hại
- Bên cạnh các hành vi nêu trên, còn một số hành vi khác như: sở hữu hoặc sử dụng phần cứng, phần mềm hoặc các công cụ khác được sử dụng để thực hiện tội phạm mạng; đánh cắp danh tính hoặc gian lận danh tính; ăn cắp điện tử; hay bất kỳ hoạt động nào khác ảnh hưởng xấu hoặc đe dọa đến an ninh, bảo mật, tính toàn vẹn hoặc tính khả dụng của bất kỳ hệ thống CNTT, cơ sở hạ tầng, mạng truyền thông, thiết bị hoặc dữ liệu nào…

Năm 2018, Quốc hội Nhật Bản tiếp tục thông qua dự luật sửa đổi Luật cơ bản về An ninh mạng năm 2014 (Basic Act on Cybersecurity). Theo đó, an ninh mạng đề cập trong Luật sửa đổi được gắn liền với các biện pháp để quản lý dữ liệu một cách an toàn, và cũng đã làm rõ trách nhiệm của Chính phủ quốc gia Nhật Bản, chính quyền địa phương và các tổ chức liên quan khác.

3.6.4. Một số bài học kinh nghiệm đối với Việt Nam

Qua một số khía cạnh pháp lý và thực tiễn thực hiện pháp luật quốc tế trong hợp tác đấu tranh, phòng chống tội phạm công nghệ cao của ở các quốc gia này, có thể đưa ra một số nhận định:

Thứ nhất, các quốc gia trên đều nhận thức rõ được tính chất, mức độ nguy hiểm của tội phạm công nghệ cao nên đã ban hành nhiều đạo luật, các văn bản có liên quan điều chỉnh về tội phạm công nghệ cao căn cứ trên những cơ sở pháp lý là các công ước quốc tế mà những quốc gia này đã tham gia là thành viên như Công ước Budapest, Công ước Palermo và một số công ước khác có liên quan đến tội phạm công nghệ cao

Thứ hai, cả ba quốc gia đều xác định rõ trọng tâm và dành những sự quan tâm đặc biệt đến các nội dung hợp tác quốc tế trong đấu tranh, phòng chống tội phạm công nghệ cao như việc đáp ứng nghĩa vụ thành viên trong hài hòa hóa và hoàn thiện pháp luật,vấn đề tương trợ tư pháp hình sự, dẫn độ tội phạm và chuyển giao người bị kết án.

Thứ ba, nguyên tắc "lãnh thổ" hay "nơi thực hiện hành vi phạm tội" là những nguyên tắc xác định thẩm quyền tài phán phổ biến của các quốc gia đối với tội phạm công nghệ cao.

Từ những nhận định, pháp luật của Việt Nam hoàn toàn có thể đúc rút ra một số kinh nghiệm giá trị mang cả tính tham khảo cũng như tính ứng dụng trong quá trình hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao như sau:

Thứ nhất, việc xây dựng, ban hành các quy định của pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao và vấn đề an ninh mạng của nước ta trong giai đoạn hiện nay là điều vô cùng cấp bách và khẩn thiết.

Thứ hai, Việt Nam cần sớm hoàn chỉnh khung pháp lý cần thiết liên quan đến các hoạt động trên không gian mạng, trong đó đặc biệt lưu tâm tới vấn đề ban hành các văn bản hướng dẫn liên quan trong vấn đề này.

Thứ ba, cần tăng tính phản hồi nhanh chóng của các văn bản pháp luật riêng biệt để điều chỉnh kịp thời và có hiệu quả khi tiến hành các hoạt động

hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao ở Việt Nam hiện nay.

Thứ tư, chủ động thực hiện phòng, chống tội phạm công nghệ cao ngay từ trong an ninh nội địa và tăng cường chất lượng của các hoạt động hợp tác quốc tế phòng, chống tội phạm công nghệ cao.

CHƯƠNG 4
PHÁP LUẬT VÀ THỰC TIỄN HỢP TÁC QUỐC TẾ ĐẤU TRANH PHÒNG CHỐNG TỘI PHẠM CÔNG NGHỆ CAO CỦA VIỆT NAM

4.1. Thực trạng pháp luật trong hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao ở Việt Nam

4.1.1. Khái quát về tội phạm công nghệ cao ở Việt Nam

4.1.1.1. Tình hình tội phạm công nghệ cao ở Việt Nam

Các hành vi do tội phạm công nghệ cao thực hiện trên thế giới hiện nay diễn biến rất phức tạp. Vì đặc thù của loại tội phạm này là tính quốc tế và hội nhập nhanh, do đó, điều này đã tác động mạnh đến tình hình tội phạm công nghệ cao thực hiện tại Việt Nam. Tội phạm công nghệ cao ở các nước xâm nhập vào Việt Nam rất nhanh, thậm chí nhiều đối tượng người nước ngoài nhập cảnh vào Việt Nam để tổ chức hoạt động tội phạm. Việt Nam đã được dự báo có thể là một trong những khu vực nóng về tội phạm công nghệ cao. Số liệu của hãng bảo mật Symantec cho thấy, Việt Nam hiện đang đứng thứ 11 trên toàn cầu về các hoạt động đe dọa tấn công mạng (năm 2018). Những hoạt động đe dọa nhắm vào cơ quan, doanh nghiệp, tổ chức tại Việt Nam bao gồm, tấn công có chủ đích, các mối đe dọa trên thiết bị di động, phát tán mã độc, virus và đánh cắp dữ liệu. Các tội phạm công nghệ cao thường tập trung tại một số tỉnh, thành phố lớn, nơi có sự giao lưu hội tụ của nhiều lĩnh vực khoa học công nghệ, tài chính ngân hàng hoặc nơi có nhiều người nước ngoài sinh sống...

4.1.1.2. Dự báo về tình hình tội phạm công nghệ cao tại Việt Nam và xu hướng hợp tác quốc tế trong đấu tranh, phòng chống tội phạm công nghệ cao tại Việt Nam

Tội phạm sử dụng công nghệ cao ở Việt Nam trong những năm tới được dự báo sẽ diễn ra phức tạp với nhiều phương thức, thủ đoạn phạm tội mới, hoạt động có tính chất xuyên quốc gia và xảy ra trên nhiều lĩnh vực.

Nếu vấn đề an ninh mạng không được giải quyết kịp thời, lĩnh vực thương mại điện tử của Việt Nam sẽ rơi vào tình trạng trì trệ, trở thành một rào cản đối với phát triển kinh tế, xã hội. Hiện nay đã xuất hiện một số mạng máy tính ma (botnet) do các hacker Việt Nam phát triển và mở rộng đã gây tác hại lớn đối với an ninh mạng nói chung và thương mại điện tử nói riêng. Ngoài ra, xu hướng gửi thư rác quy mô lớn, lừa đảo qua phishing, cài keylogger, lấy cắp thông tin, rửa tiền bằng tiền ảo… đang ngày càng phát triển.

Trong thời gian tới, hoạt động đấu tranh với loại tội phạm công nghệ cao sẽ là nội dung hợp tác trọng tâm được đưa vào chương trình hợp tác giữa các quốc gia và nhiều tổ chức đa phương và song phương. Đáp ứng nhu cầu này, thời gian tới sẽ có thêm nhiều Hiệp định TTTP và dẫn độ được ký kết giữa Việt Nam và nhiều quốc gia trong đó có các nội dung tượng trợ tư pháp hình sự và dẫn độ trong đấu tranh phòng, chống tội phạm công nghệ cao.

4.1.2. Nội dung pháp lý cho hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao của Việt Nam

Cơ sở pháp lý cho hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao gồm các quy định do Việt Nam ban hành, từ Hiến pháp cho đến các văn bản pháp luật chuyên ngành như: Luật Công nghệ thông tin 2006; Luật an toàn thông tin mạng 2015; Luật an ninh mạng 2018; Bộ luật hình sự 2015; Bộ luật Tố tụng hình sự 2015; Nghị định số 25/2014/NĐ-CP quy định về phòng, chống tội phạm và VPPL khác có sử dụng công nghệ cao; 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, VKSNDTC, TANDTC, hướng dẫn áp dụng một số quy định của BLHS về một số tội phạm trong lĩnh vực CNTT, viễn thông.

Đặc biệt, gần đây nhất, trong Văn kiện Đại hội XIII, Đảng ta nêu rõ: "Tích cực, chủ động…giữ vững chủ quyền số quốc gia trên không gian mạng trong mọi tình huống". Đây là một nội dung lần đầu tiên được ghi trong một

Văn kiện Đại hội, phản ánh sự nhận thức sâu sắc của Đảng ta về tính chất của thời đại dưới góc độ khoa học – công nghệ, bởi cuộc Cách mạng Công nghiệp lần thứ tư sẽ chuyển dịch toàn bộ thế giới từ thế giới thực sang thế giới số.

Bên cạnh các quy định do Việt Nam ban hành, thực hiện chính sách đa phương hóa, đa dạng hóa và tích cực, chủ động hội nhập quốc tế, là thành viên có trách nhiệm trong cộng đồng quốc tế, tính đến tháng 9/2017, Việt nam là thành viên của 22 điều ước quốc tế đa phương về TTTP về hình sự, dẫn độ, chuyển giao người bị kết án phạt tù và 27 Hiệp định TTTP về dân dự và hình sự với các quốc gia. Trong các Hiệp định này đều có các quy định về TPCNC hoặc các tội phạm xuyên quốc gia có yếu tố công nghệ cao. Trong số 22 điều ước quốc tế đa phương, Việt Nam tuyên bố không coi 10/22 điều ước quốc tế đa phương là cơ sở pháp lý trực tiếp về dẫn độ như Công ước về trừng trị việc chiếm giữ bất hợp pháp tàu bay năm 1970, Công ước thống nhất về các chất ma túy năm 1961, Công ước của Liên hợp quốc về chống tham nhũng năm 2003, Công ước của Liên hợp quốc về chống tra tấn và các hình thức đối xử hoặc trừng phạt tàn bạo vô nhân đạo hoặc hạ nhục con người…

Trên cơ sở đó, nội dung cơ bản của pháp luật về tội phạm công nghệ cao cũng như công tác hợp tác quốc tế đấu tranh phòng chống loại hình tội phạm này bao gồm những vẫn đề chủ đạo sau đây:

4.1.2.1. Các quy định về phòng ngừa tội phạm công nghệ cao

Việc phòng ngừa tội phạm công nghệ cao hiện nay bên cạnh thuộc trách nhiệm của cơ quan chuyên trách phòng, chống TPCNC (là các đơn vị nghiệp vụ trong Công an nhân dân – Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Quân đội nhân dân được giao nhiệm vụ chuyên trách tham mưu, tổ chức, trực tiếp thực hiện nhiệm vụ đấu tranh phòng, chống TPCNC) còn có sự tham gia của các cá nhân, tổ chức, doanh nghiệp và cơ quan thông tin đại chúng.

4.1.2.2. Các quy định về đấu tranh, triệt phá tội phạm công nghệ cao

Thứ nhất, quy định về phát hiện, xử lý tội phạm công nghệ cao

Thứ hai, về các biện pháp tổ chức, đấu tranh chống TPCNC của Cơ quan chuyên trách

Thứ ba, quy định về hình sự hóa đối với các hành vi sử dụng công nghệ cao để gây tổn hại đến quyền lợi chính đáng của cá nhân, tổ chức và nhà nước

Thứ tư, quy định về hình phạt đối với TPCNC

4.1.2.3. Các quy định về chủ thể trong hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao

Chủ thể trực tiếp thực hiện các hoạt động hợp tác quốc tế trong phòng, chống TPCNC là Bộ Công an. Bên cạnh đó, theo quy định tại Điều 65 của Luật TTTP năm 2007, Bộ Công an là cơ quan có trách nhiệm tiếp nhận, chuyển giao, xem xét, giải quyết các yêu cầu của nước ngoài về dẫn độ, chuyển giao người đang chấp hành hình phạt tù; xem xét và chuyển hồ sơ cho VKSND, TAND và thực hiện hoạt động TTTP theo thẩm quyền. Bộ Công an đề xuất việc ký kết, gia nhập và thực hiện điều ước quốc tế về dẫn độ và chuyển giao người đang chấp hành hình phạt tù; kiến nghị sửa đổi, bổ sung và hoàn thiện pháp luật Việt Nam về TTTP. Định kỳ sáu tháng và hàng năm Bộ công an phải thông báo với Bộ Tư pháp tình hình thực hiện yêu cầu dẫn độ và chuyển giao người đang chấp hành hình phạt tù.

Trong hoạt động phòng chống TPCNC của Bộ Công an, lực lượng đóng vai trò nòng cốt là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao A05.

Các chủ thể phối hợp tham gia thực hiện hợp tác quốc tế trong phòng, chống tội phạm gồm có:

- Bộ Tư pháp: Với tư cách là cơ quan quản lý nhà nước về TTTP, Bộ Tư pháp có trách nhiệm phối hợp với Bộ Công an, VKSNDTC, TANDTC, Bộ Ngoại giao soạn thảo các văn bản quy phạm pháp luật hướng dẫn thực thi Luật TTTP; tham gia đàm phán, góp ý, thẩm định các hiệp định TTTP về hình sự, dẫn độ và chuyển giao người chấp hành án phạt tù. Bên cạnh đó, Bộ Tư pháp cũng phối hợp với Bộ Công an và VKSNDTC xử lý những yêu cầu ủy thác phức tạp và nhạy cảm.

- Bộ Ngoại giao: Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Tư pháp, TANDTC, Bộ Công an, VKSNDTC trong công tác xây dựng pháp luật về TTTP, phối hợp thực hiện các hoạt động trong hợp tác quốc tế trong đấu tranh phòng chống tội phạm trên nguyên tắc có đi có lại.

4.1.2.4. Các quy định về dẫn độ tội phạm công nghệ cao

Thứ nhất, Quy định về thẩm quyền thực hiện dẫn độ.

Các cơ quan có thẩm quyền về dẫn độ TPCNC gồm có Bộ Công an, Tòa án, Viện Kiểm sát, Bộ Ngoại giao.

Thứ hai, Quy định về các trường hợp bị dẫn độ, từ chối dẫn độ và dẫn độ kèm theo một số điều kiện

4.1.2.5. Tương trợ tư pháp về hình sự

Căn cứ vào quy định của Luật TTTP 2007, Bộ luật TTHS năm 2015 và thực tiễn áp dụng hoạt động TTTP về hình sự giữa Việt Nam với các quốc gia, phạm vi TTTP về hình sự bao gồm: tống đạt giấy tờ, hồ sơ, tài liệu liên quan đến TTTP về hình sự; triệu tập người làm chứng, người giám định; thu thập, cung cấp chứng cứ; truy cứu trách nhiệm hình sự; trao đổi thông tin; các yêu cầu tương trợ tư pháp khác về hình sự. Ngoài ra, Bộ luật TTHS quy định TTTP về hình sự là một trong các hoạt động hợp tác quốc tế trong tố tụng hình sự (Điều 491), theo đó, các hoạt động TTTP về hình sự cụ thể như: Xác định giá trị pháp lý của tài liệu, đồ vật thu thập được (Điều 494); Quy định về việc tiến hành tố tụng của người có thẩm quyền của Việt Nam ở nước ngoài và người có thẩm quyền của nước ngoài ở Việt Nam được thực hiện theo điều ước quốc tế mà Việt Nam là thành viên hoặc theo nguyên tắc có đi có lại (Điều 495); cho người làm chứng, người giám định, người đang chấp hành án phạt tù tại nước được đề nghị có mặt ở Việt Nam để phục vụ việc giải quyết vụ án hình sự hoặc có thể cho phép người làm chứng, người giám định, người đang chấp hành án phạt tù tại Việt Nam có mặt ở nước ngoài để phục vụ việc giải quyết vụ án hình sự (Điều 469); truy tìm, tạm giữ, kê biên, phong tỏa, tịch thu, xử lý tài sản do phạm tội mà có để phục vụ yêu cầu điều tra, truy tố, xét xử và thi hành án hình sự (Điều 507); phong tỏa tài khoản có thể được áp dụng nếu có căn cứ cho rằng số tiền trong tài khoản đó liên quan đến hành vi phạm tội của người bị buộc tội (Điều 129); phối hợp điều tra hoặc áp dụng các biện pháp điều tra tố tụng đặc biệt (Điều 508);

4.1.2.6. Các quy định về chuyển giao người đang chấp hành hình phạt tù

Thứ nhất, căn cứ tiếp nhận, chuyển giao người đang chấp hành án phạt tù: được thực hiện theo quy định tại khoản 2 Điều 49, Điều 50 Luật TTTP năm 2007 và Điều 6 Thông tư liên tịch số 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC.

Thứ hai, các trường hợp từ chối chuyển giao người đang chấp hành án phạt tù.

Việc từ chối chuyển giao người đang chấp hành hình phạt tù tại Việt Nam cho nước ngoài khi: có căn cứ cho rằng người được chuyển giao có thể bị tra tấn, trả thù hoặc truy bức tại nước tiếp nhận chuyển giao; việc chuyển giao có thể phương hại đến chủ quyền, an ninh quốc gia của Việt Nam.

Thứ ba, lưu ý về việc tiếp nhận, chuyển giao người đang chấp hành hình phạt tù

Trình tự, thủ tục nhận yêu cầu chuyển giao và xem xét, quyết định việc tiếp nhận được quy định tại Điều 9 Thông tư liên tịch số 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC.

Thông báo quyền được yêu cầu chuyển giao cho người đang chấp hành án phạt tù.Theo quy định của pháp luật TTTP 2007 và Điều 12 Thông tư liên tịch số 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC.

Bộ Công an có trách nhiệm lập hồ sơ đề nghị tiếp nhận và chuyển giao cho Bộ Ngoại giao xem xét, quyết định áp dụng nguyên tắc có đi có lại. Tại các quốc gia có điều ước quốc tế mà Việt Nam là thành viên thì khi có đơn xin chuyển giao, bản tuyên bố của người này về việc họ hiểu biết đầy đủ về hệ quả của việc chuyển giao và các quyền, nghĩa vụ của việc chuyển giao. Khi đó Bộ trưởng Bộ Công an quyết định cho phép nước tiếp nhận cử đại diện sang Việt Nam để xác minh sự đồng ý chuyển giao của người đang chấp hành án phạt tù.

4.1.2.7. Một số nội dung khác trong hợp tác quốc tế về phòng chống tội phạm công nghệ cao

Thứ nhất, hoạt động thu thập, trao đổi thông tin và truy nã tội phạm thông qua vai trò của Cơ quan INTERPOL Việt Nam.

Thứ hai, hoạt động đẩy trả, trục xuất

Trục xuất là hành vi đưa người nước ngoài ra khỏi lãnh thổ nước mình bằng hành động đơn phương của cơ quan chức năng của nước mà người đó

đang cư trú.

Đẩy trả là biện pháp thường được áp dụng đối với những đối tượng phạm tội ở nước ngoài, sau đó lẩn trốn ở lại nước đó.

Thứ ba, hoạt động phối hợp công an các tỉnh biên giới tại các quốc gia trong đấu tranh, phòng chống TPCNC

Công an các tỉnh biên giới (Công an cấp tỉnh của Việt Nam: với Cơ quan tương ứng cấp tỉnh của nước láng giềng) hợp tác quốc tế trong phòng, chống tội phạm gồm các hoạt động:

+ Hợp tác quốc tế trong điều tra khám phá các vụ án hình sự mà hai bên có trách nhiệm cùng nhau giải quyết.

+ Hợp tác quốc tế trong truy bắt, dẫn giải và chuyển giao đối tượng phạm tội hình sự.

+ Hợp tác quốc tế trong tiếp nhận, giải cứu nạn nhân của tội phạm hình sự.

Thứ tư, hợp tác quốc tế trong việc trao đổi, cung cấp thông tin về tội phạm với các tổ chức cảnh sát trong khu vực và toàn cầu

Thứ năm, trao đổi kinh nghiệm đào tạo và chuyển giao công nghệ

Trong khuôn khổ, phạm vi đã ký kết tại điều ước quốc tế song phương hoặc đa phương, Bộ Công an, VKSNDTC, TANDTC có thể tổ chức các hội nghị, quốc tế để trao đổi kinh nghiệm, tổng kết công tác hợp tác đấu tranh phòng, chống tội phạm giữa các bên.

Thứ sáu, hợp tác quốc tế đấu tranh phòng, chống tội phạm giữa lực lượng Cảnh sát nhân dân Việt Nam với lực lượng Cảnh sát các nước

Cơ chế hợp tác quốc tế trong phòng, chống tội phạm liên quan đến Việt Nam, lực lượng cảnh sát nhân dân Việt Nam thường chủ yếu thực hiện theo những khuôn khổ hợp tác đó là: Thông qua khuôn khổ hợp tác INTERPOL; thông qua khuôn khổ hợp tác ASEAN/ASEANAPOL; qua kênh hợp tác với Văn phòng Sỹ quan liên lạc Cảnh sát các nước tại Việt Nam và trong khu vực Đông Nam Á; qua kênh hợp tác trực tiếp với một số cơ quan thi hành pháp luật khác như Cục điều tra Liên hang Hoa Kỳ; Cơ quan Bài trừ ma tuý Liên bang Hoa Kỳ; các Trung tâm chống tội phạm xuyên quốc gia trong mạng lưới Trung tâm chống tội phạm xuyên quốc gia Châu Á - Thái Bình Dương,...

Hoặc cơ chế hợp tác song phương phòng, chống tội phạm nói chung và với một số loại tội phạm nói riêng giữa Công an các tỉnh biên giới của Việt Nam với các đối tác tương ứng của nước ngoài dưới hình thức hợp tác giữa các tỉnh biên giới, hoặc bằng hình thức kết nghĩa đối với những tỉnh chưa ký kết thỏa thuận quốc tế phòng, chống tội phạm cấp tỉnh.

4.2. Thực tiễn thực thi pháp luật trong hợp tác quốc tế đấu tranh phòng chống tội phạm công nghệ cao của Việt Nam

4.2.1. Kết quả hợp tác quốc tế trong đấu tranh phòng chống tội phạm công nghệ cao trong thời gian vừa qua

4.2.1.1. Về đàm phán, ký kết, gia nhập điều ước quốc tế trong phòng chống tội phạm công nghệ cao:

- Các điều ước quốc tế đa phương về phòng, chống tội phạm:

Theo thống kê của Bộ Công an, tính đến tháng 9/2019, Việt Nam là thành viên của 22 điều ước quốc tế đa phương quy định về TTTP về hình sự, dẫn độ và chuyển giao người bị kết án phạt tù. Trong số này có 01 Hiệp định chuyên biệt TTTP 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 ngày 20/9/2005). Có 03 điều ước quốc tế đa phương có quy định về chuyển giao người bị kết án phạt tù và các điều ước quốc tế đa phương còn lại đều quy định về dẫn độ

Trong số các điều ước quốc tế đa phương mà Việt Nam là thành viên quy định về HTQT trong đấu tranh, phòng chống tội phạm thì có điều ước quốc tế điều chỉnh HTQT trong lĩnh vực phòng chống TPCNC như.

+ Công ước của Liên Hợp quốc về chống tội phạm có tổ chức xuyên quốc gia;

+ Hiệp định TTTP về hình sự giữa các nước ASEAN.

- *Các điều ước quốc tế song phương (Hiệp định) về hợp tác quốc tế trong đấu tranh, phòng chống tội phạm nói chung và TPCNC nói riêng*

Trong lĩnh vực hợp tác quốc tế phòng, chống tội phạm nói chung và TPCNC nói riêng, Việt Nam đã ký 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 vào nhu cầu về phạm vi, 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. Ngoài ra, trong lĩnh vực hợp tác quốc tế phòng, chống TPCNC còn có những Hiệp định song phương giữa Chính phủ Việt Nam và Chính phủ các quốc gia hữu quan điều chỉnh trực tiếp đấu tranh phòng, chống các loại tội phạm mà Việt Nam cũng đã ký kết, gia nhập.

4.2.1.2. Về phối hợp phát hiện, ngăn chặn và điều tra, xử lý tội phạm sử dụng công nghệ cao theo quy định của pháp luật và các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

Phối hợp trong việc thu thập, xác minh thông tin tài liệu phục vụ công tác phát hiện, điều tra TPSDCNC là một trong những yêu cầu hợp tác thông thường giữa lực lượng Công an nhân dân Việt Nam với Công an các nước. Đó có thể là xác minh các địa chỉ IP mà đối tượng phạm tội sử dụng vào hoạt động phạm.

Phối hợp trong việc phát hiện và điều tra các vụ án lừa đảo nhằm chiếm đoạt tài sản, đánh bạc bằng công nghệ cao trên lãnh thổ Việt Nam: Từ năm 2010 đến năm 2017, lực lượng Công an Việt Nam đã phát hiện và điều tra làm rõ gần 200 vụ án lừa đảo nhằm chiếm đoạt tài sản bằng cách sử dụng công nghệ cao, các đối tượng chủ yếu là người Trung Quốc thực hiện trên lãnh thổ Việt Nam.

4.2.1.3. Kết quả công tác dẫn độ, tương trợ tư pháp về hình sự về tội phạm sử dụng công nghệ cao trong tương quan với các loại hình tội phạm khác

- Kết quả công tác dẫn độ trong việc điều tra, truy tố, xét xử và thi hành án:

Trong Báo cáo tổng kết công tác thi hành pháp luật về dẫn độ đối với tội phạm nói chung của Bộ Công an năm 2019, số đối tượng có lệnh truy nã đỏ của Interpol có thông tin lẩn trốn vào Việt Nam là 317 đối tượng, nhưng rất ít trường hợp nước ngoài yêu cầu dẫn độ về TPCNC. Đến năm 2017, Bộ Công an đã tiếp nhận và xử lý 23 yêu cầu dẫn độ của nước ngoài (12 yêu cầu dẫn độ theo các hiệp định song phương về dẫn độ, 11 yêu cầu dẫn độ theo nguyên tắc có đi có lại) và từ chối 03 yêu cầu dẫn độ không hợp lệ. Có khoảng 1.200 đối tượng phạm tội tại Việt Nam bỏ trốn ra nước ngoài, trong đó có 235 đối tượng đã bị INTERPOL ra lệnh truy nã đỏ, nhiều đối tượng phạm tội đặc biệt nghiêm trọng, trong đó có TPCNC. Bộ Công an đã lập và chuyển 35 hồ sơ yêu cầu dẫn độ đến cơ quan có thẩm quyền của nước ngoài (đến năm 2017), gồm 21 yêu cầu dẫn độ theo các hiệp định song phương và 14 yêu cầu dẫn độ theo nguyên tắc có đi có lại.

- Kết quả tương trợ tư pháp về hình sự trong việc điều tra, truy tố, xét xử:

Trong giai đoạn từ 1/7/2008 đến hết 31/5/2017 thì VKSNDTC đã tiếp nhận 627 yêu cầu TTTPHS của nước ngoài, trong đó Văn phòng Cơ quan CSĐT Bộ Công an thực hiện 512 yêu cầu (chiếm 81,7%), chuyển các cơ quan khác (Bộ ngoại giao, Tòa án, Cục lãnh sự BNG, VKSND…) thực hiện 115 yêu cầu (chiếm 18,3%). Các nội dung yêu cầu TTTP về hình sự mà nước ngoài đề nghị Việt Nam thực hiện chủ yếu là tống đạt giấy tờ, hồ sơ, tài liệu có liên quan.

Cũng trong thời gian trên, các cơ quan có thẩm quyền của Việt Nam (Cơ quan điều tra trong CAND, TAND, VKSND…) đã yêu cầu phía nước ngoài thực hiện tổng số 660 yêu cầu TTTPHS, trong đó phía Cơ quan điều tra trong CAND có 554 yêu cầu (chiếm 83,9%) và các cơ quan khác có thẩm quyền đề nghị 116 yêu cầu (chiếm 16,1%). Trong đó có khoảng 78% yêu cầu liên quan đến các nước đã ký Hiệp định với Việt Nam. Trong đó, nội dung yêu cầu do cơ quan điều tra trong Công an nhân dân đề nghị nước ngoài thực hiện thì thu thập chứng cứ chiếm 68% và xác minh lý lịch tư pháp chiếm 32%, việc lấy lời khai chiếm 17% trong tổng số nội dung thu thập chứng cứ.

4.2.1.4. Công tác tổ chức hội nghị, hội thảo trao đổi thông tin, kinh nghiệm và phối hợp đào tạo, bồi dưỡng, huấn luyện nghiệp vụ:

Bộ Công an Việt Nam với vai trò nòng cốt trong phòng chống tội phạm sử dụng công nghệ cao đã phối hợp với các tổ chức quốc tế, cảnh sát các quốc gia thường xuyên tiến hành các hội nghị, hội thảo về an ninh, an toàn thông tin cũng như phòng chống tội phạm sử dụng công nghệ cao.

Đồng thời, Bộ Công an cũng thường xuyên cử lực lượng tham gia các hội nghị, hội thảo do lực lượng INTERPOL quốc tế và các ủy ban của Liên

Hợp Quốc tổ chức trong phòng chống tội phạm nói chung và phòng chống tội phạm sử dụng công nghệ cao nói riêng.

Ngoài ra, với đầu mối trao đổi thông tin về tội phạm quốc tế, Văn phòng INTERPOL Việt Nam đóng vai trò cung cấp cảnh báo của các tổ chức cảnh sát, an ninh quốc gia cũng như quốc tế trong phòng chống TPCNC.

4.2.2. Hạn chế trong hoạt động hợp tác quốc tế đấu tranh, phòng chống tội phạm công nghệ cao

4.2.2.1. Vướng mắc, hạn chế từ quy định của Luật Tương trợ tư pháp lien quan đến hợp tác quốc tế phòng chống tội phạm sử dụng công nghệ cao

Sau gần 15 năm áp dụng Luật TTTP, một số quy định trong Luật TTTP chưa tương thích hoặc chưa có quy định, trong đó có nhiều nội dung phức tạp, nhạy cảm, dẫn đến khó khăn trong việc triển khai tổ chức thực hiện các hoạt động HTQT phòng chống tội phạm nói chung và TPCNC nói riêng, cụ thể:

Quy định liên quan đến dẫn độ

Theo 11 Hiệp định TTTP có quy định về dẫn độ mà Việt Nam ký với các quốc gia trước đây, VKSNDTC là cơ quan đầu mối về dẫn độ của Việt Nam. Nhưng Luật TTTP lại quy định Bộ Công an là cơ quan đầu mối về dẫn độ, chuyển giao người đang chấp hành hình phạt tù. Sự không thống nhất này đã gây khó khăn cho quá trình thực hiện chức năng của Bộ Công an trong dẫn độ.

Về vấn đề cam kết không áp dụng án tử hình. Một số Hiệp định về dẫn độ giữa Việt Nam và các nước có quy định về cam kết không áp dụng án tử hình (như Hiệp định với Cộng hòa Bê-la-rút (Điều 70), với Nga và Austraylia. Pháp Luật Việt Nam vẫn còn quy định nhiều loại tội phạm có quy định hình phạt tử hình và không hạn chế việc dẫn độ đối với người có thể bị kết án tử hình. Điều này gây khó khăn cho Việt Nam khi đàm phán các Hiệp định về dẫn độ với các quốc gia châu Âu (nơi mà pháp luật tại nhiều quốc gia không có án tử hình).

Quy định của Luật TTTP đã bỏ lọt trường hợp từ chối dẫn độ phạm nhân (hoặc người đã bị kết án bằng bản án hình sự có hiệu lực pháp luật) bỏ trốn để tiếp tục thi hành án hình sự.

Quy định liên quan đến thực hiện công tác chuyển giao người đã bị kết án phạt tù

Về thời hạn còn lại phải chấp hành án của người được chuyển giao. Luật TTTP quy định người bị kết án phạt tù còn phải chấp hành ít nhất 01 năm, trong trường hợp đặc biệt còn ít nhất 06 tháng. Tuy nhiên, trong hầu hết các Hiệp định song phương về chuyển giao người bị kết án phạt tù mà Việt Nam đã ký kết đều quy định người bị kết án phạt tù còn phải chấp hành ít nhất 01 năm hoặc do các bên thống nhất.

Cần có sự đồng ý của người bị kết án phạt tù còn nhiều vướng mắc. Hiện nay Luật TTTP quy định người đang chấp hành hình phạt tù ở nước ngoài có thể được tiếp nhận về Việt Nam để thi hành hình phạt tù thì cần phải có sự đồng ý của người được chuyển giao. Như vậy, trong trường hợp nhiều người Việt Nam phạm tội ở nước ngoài (đặc biệt là phạm tội liên quan đến ma túy) sẽ không muốn về Việt Nam để thi hành hình phạt tù. Bên cạnh đó, trong một số trường hợp phía nước ngoài đề nghị Việt Nam cam kết không tuyên hình phạt tử hình hoặc có tuyên nhưng không thi hành hình phạt tử hình đối với người đang chấp hành án phạt tù đồng thời là đối tượng truy nã của Việt Nam sau khi được chuyển giao về Việt Nam. Tuy nhiên, pháp luật Việt Nam chưa có quy định này.

Về chi phí, Luật TTTP quy định chi phí về chuyển giao người đang chấp hành hình phạt tù do Bên yêu cầu chi trả. Nhưng các Hiệp định TTTP Việt Nam đã kí lại quy định là chi phí do Bên nhận chi trả trừ chi phí phát sinh hoàn toàn trong lãnh thổ Bên chuyển giao.

Quy định thực hiện công tác TTTP về hình sự

Để thực hiện yêu cầu TTTP, các nước yêu cầu không áp dụng án tử hình. Tuy nhiên, Luật TTTP chưa có quy định về trình tự, thủ tục cam kết không áp dụng hình phạt tử hình trong hoạt động TTTP về hình sự.

Phạm vi TTTP về hình sự quy định tại Điều 17 Luật TTTP còn hạn chế, chưa phù hợp với các cam kết quốc tế của Việt Nam.

Chưa có quy định cụ thể về trình tự, thủ tục thực hiện một số yêu cầu tương trự như triệu tập người làm chứng, người giám định, dẫn giải người chấp hành hình phạt tù ra nước ngoài để hỗ trợ điều tra hoặc cung cấp chứng

cứ; chuyển giao truy cứu trách nhiệm hình sự công dân Việt Nam tại Việt Nam….

4.2.2.2. Khó khăn từ thực tiễn áp dụng pháp luật trong đấu tranh, phòng chống tội phạm sử dụng công nghệ cao

Một là, việc hợp tác quốc tế trong trao đổi thông tin về TPCNC còn chưa đầy đủ.

Hai là, việc hợp tác với các cơ quan thực thi pháp luật nước ngoài thường bị kéo dài.

Ba là, các quy định của luật chưa dự báo điều chỉnh hết các trường hợp sẽ phát sinh và chưa phù hợp với điều kiện tại Việt Nam.

Bốn là, vẫn còn hiện tượng né tránh, đùn đẩy trách nhiệm của các lực lượng thực thi pháp luật tại Việt Nam.

Năm là, các chế tài và hình phạt xử lý tội phạm sử dụng công nghệ cao còn nhẹ, chưa đủ sức răn đe phục vụ công tác đấu tranh, phòng ngừa tội phạm.

Sáu là, công tác tuyên truyền, phổ biến giáo dục, pháp luật chưa được quan tâm đúng mức.

4.3. Giải pháp hoàn thiện pháp luật và nâng cao hiệu quả hợp tác quốc tế trong đấu tranh phòng, chống tội phạm công nghệ cao của Việt Nam

4.3.1. Giải pháp hoàn thiện pháp luật Việt Nam về đấu tranh phòng chống tội phạm công nghệ cao

Thứ nhất, về mặt văn bản pháp luật cần thiết phải có những quy định rõ ràng, cụ thể về việc thu thập, kiểm tra, đánh giá chứng điện tử cũng như ban hành văn bản hướng dẫn về đường lối xử lý đối với các TPCNC trong Bộ luật hình sự năm 2015, sửa đổi, bổ sung năm 2017. Ngoài ra, cần có quy định chặt chẽ về trách nhiệm thậm chí là chế tài xử lý đối với cá nhân, tổ chức (cơ quan thứ 3) trong việc chậm trễ cung cấp dữ liệu điện tử, giám định dữ liệu điện tử làm ảnh hưởng tới tiến trình giải quyết vụ án.

Làm rõ các khái niệm như "thu thập phương tiện điện tử" và "thu giữ phương tiện điện tử".

Bổ sung thêm tội danh về lạm dụng trẻ em trong nhóm các TPCNC của Bộ luật hình sự.

Thứ hai, những người tiến hành tố tụng cần nâng cao kiến thức cơ bản về dữ liệu điện tử, về CNTT (am hiểu nhất định về đối tượng đang được khai thác)...

Thứ ba, cần thiết phải có những tổng kết khoa học và thực tiễn về thu thập, đánh giá, sử dụng chứng cứ điện tử trong các vụ án hình sự. Mặt khác, dữ liệu điện tử là nguồn chứng cứ phi truyền thống, tồn tại trên không gian mạng, sự tồn tại đó có thể vượt ra khỏi phạm vi của một quốc gia và loại tội phạm để lại dấu vết này cũng thường mang tính chất xuyên quốc gia. Do vậy, cơ quan có thẩm quyền cần tăng cường hợp tác quốc tế trong đấu tranh với loại tội phạm này.

4.3.2. Hoàn thiện pháp luật Việt Nam trong hợp tác quốc tế trong đấu tranh phòng, chống tội phạm công nghệ cao

Xây dựng các đạo luật mang tính chuyên biệt như Luật TTTP về hình sự, Luật dẫn độ.

- *Về công tác dẫn độ:* Quốc hội sớm ban hành đạo luật chuyên biệt về dẫn độ trên cơ sở tách quy định về dẫn độ trong Luật TTTP năm 2007. Đồng thời, Nhà nước cần tiếp tục đàm phán, ký kết và triển khai thực hiện có hiệu quả các hiệp định hợp tác song phương về dẫn độ. Ngoài ra, các cơ quan có thẩm quyền cần tăng cường áp dụng nguyên tắc có đi có lại trong giải quyết vụ việc dẫn độ khi Việt Nam chưa ký kết hiệp định hợp tác song phương về dẫn độ với nước ngoài, tránh việc người phạm tội lợi dụng "kẽ hở" của pháp luật và trong hợp tác quốc tế để trốn tránh sự trừng phạt của pháp luật dẫn đến bỏ lọt tội phạm...

- *Về tương trợ tư pháp về hình sự:* bổ sung các nội dung như: xác minh, giải quyết tin báo, tố giác tội phạm; liên kết điều tra, phối hợp điều tra; quy định cho phép sử dụng các phương tiện kỹ thuật áp dụng công nghệ cao (thư điện tử, fax...) trong việc gửi, tiếp nhận hồ sơ ủy thác tư pháp và thực hiện một số hoạt động TTTP. Ngoài ra, cần xem xét sửa đổi, bổ sung căn cứ từ chối TTTP theo hướng phân biệt giữa những trường hợp "bắt buộc" phải từ chối và "có thể" từ chối.

Xây dựng Luật Tương trợ tư pháp về hình sự tách khỏi Luật TTTP 2007 vừa là xu thế vừa là nhu cầu thực tiễn.

- *Về hoạt động chuyển giao người đang chấp hành án phạt tù,* trong thời gian tới, các cơ quan có thẩm quyền cần cần sớm ban hành 01 đạo luật riêng biệt về chuyển giao người đang chấp hành án phạt tù trên cơ sở tách từ Luật TTTP năm 2007 để phân biệt rõ giữa các hoạt động mang bản chất nhân đạo với các hoạt động mang tính cưỡng chế cao như dẫn độ, TTTP về hình sự của Luật TTTP hiện hành. Đồng thời, cần tăng cường đàm phán, ký kết ĐƯQT về chuyển giao người đang chấp hành án phạt tù với các quốc gia và vùng lãnh thổ nơi có nhiều công dân Việt Nam đang làm việc, sinh sống, lao động, học tập

4.3.3. Nhóm giải pháp nâng cao hiệu quả hợp tác quốc tế phòng chống tội phạm sử dụng công nghệ cao

4.3.3.1. Giải pháp chung

Các cơ quan có thẩm quyền của Việt Nam cần tiếp tục mở rộng quan hệ đối ngoại và tăng cường hợp tác quốc tế về phòng, chống tội phạm sử dụng công nghệ cao trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với pháp luật Việt Nam và điều ước quốc tế mà Việt Nam tham gia ký kết;

Nhà nước cần huy động sức mạnh của cả hệ thống chính trị, tăng cường sự lãnh đạo của cấp ủy đảng, hiệu quả quản lý, điều hành của chính quyền, phát huy vai trò của Mặt trận Tổ quốc, các đoàn thể quần chúng các cấp trong công tác phòng, chống TPCNC.

Nhà nước từng bước nâng cao năng lực phòng, chống tội phạm sử dụng công nghệ cao của các cơ quan bảo vệ pháp luật và các lực lượng chuyên trách. Ưu tiên đầu tư ngân sách, mua sắm, cung ứng vật tư, phương tiện một cách hợp lý cho hoạt động của các cơ quan tư pháp và lực lượng chuyên trách trong đấu tranh với loại tội phạm này;

Tập trung lãnh đạo, chỉ đạo công tác rà soát, xây dựng, hoàn thiện hệ thống pháp luật về phòng, chống TPCNC, trong đó chú trọng cần nghiên cứu sửa đổi, bổ sung Bộ luật hình sự, Bộ luật Tố tụng hình sự, pháp luật về các biện pháp phòng, chống tội phạm sử dụng công nghệ cao và một số đạo luật có liên quan khác.

Việt Nam cần mở rộng không gian phòng thủ của quốc gia, tranh thủ nguồn lực, tài trợ và tận dụng kinh nghiệm của các nước tiên tiến nhằm nâng cao hiệu quả đấu tranh phòng, chống tội phạm sử dụng công nghệ cao.

4.3.3.2. Giải pháp cụ thể

Thứ nhất, đẩy mạnh hợp tác quốc tế nhằm phòng ngừa từ xa đối với tội phạm sử dụng công nghệ cao.

Thứ hai, tranh thủ nguồn nhân lực và học hỏi kinh nghiệm các quốc gia

Thứ ba, nâng cao năng lực cho lực lượng chuyên trách đấu tranh, phòng ngừa TPCNC

Thứ tư, xây dựng trang thiết bị, công nghệ tiên tiến trong công tác đấu tranh, phòng ngừa TPCNC.

Thứ năm, thiết lập và duy trì các kênh thông tin trao đổi

Thứ sáu, hợp tác quốc tế đấu tranh phòng chống tội phạm sử dụng công nghệ cao cần có trọng tâm, trọng điểm.

Thứ bảy, đề cao vai trò của ASEANPOL và INTERPOL trong hợp tác quốc tế đấu tranh phòng chống TPCNC.

KẾT LUẬN CHUNG

* * *

Cuộc cách mạng công nghiệp lần thứ 4.0 không chỉ đơn thuần là một xu thế tất yếu mà nó đã trở thành thực tiễn sôi động diễn ra tại hầu khắp các quốc gia trên thế giới cũng như trên phạm vi toàn cầu. Bên cạnh những lợi ích to lớn đưa lại, chính nó cũng đem đến những thách thức an ninh phi truyền thống không hề nhỏ đối với mỗi quốc gia, khu vực. Không giống với các cuộc cách mạng trước đó, cuộc cách mạng công nghiệp lần thứ 4.0 bắt buộc mỗi cá nhân, mỗi quốc gia hay mỗi thể chế phải thay đổi nếu như không muốn bị tụt lại phía sau.

Tội phạm công nghệ cao, hay còn có thể được tiếp cận dưới nhiều tên gọi khác nhau như tội phạm mạng, tội phạm máy tính, tội phạm internet... là những thuật ngữ có thể sử dụng hoán đổi cho nhau nhằm để chỉ một loại hình tội phạm mới hình thành trong quá trình phát triển của cuộc cách mạng công nghệ thông tin 4.0 vào cuối thế kỷ 20 và được dự báo là sẽ phát triển rất nhanh trong thời gian sắp tới. Có thể nhận định, tội phạm công nghệ cao chính là

"sản phẩm" của thời đại mà các cá nhân, tổ chức, các quốc gia và cộng đồng quốc tế phải chấp nhận để đổi lấy sự thịnh vượng và phát triển. Ở phạm vi toàn cầu, đến nay mới chỉ có một điều ước quốc tế điều chỉnh loại tội phạm này là Công ước về tội phạm mạng của Uỷ hội châu Âu năm 2001 (Công ước Budapest).

Đứng trước sự tinh vi phức tạp và những hậu quả nghiêm trọng của tội phạm công nghệ cao, việc hợp tác để đấu tranh, phòng chống tội phạm công nghệ cao giữa các quốc gia ngày càng trở nên cấp thiết hơn bao giờ hết. Pháp luật quốc tế chính là cơ sở để các quốc gia tiến hành những hoạt động hợp tác này. Thông qua các nội dung hợp tác như hình thành các cơ quan, thiết chế quốc tế trong phòng chống tội phạm công nghệ cao; hài hoà hoá pháp luật; tương trợ tư pháp hình sự; dẫn độ; tiến hành phối hợp điều tra… pháp luật quốc tế đã hình thành nên một cơ chế pháp lý chung ở các cấp độ khác nhau, từ song phương, khu vực đến toàn cầu để kết nối hoạt động giữa các quốc gia, từ đó, ứng phó hiệu quả với tội phạm công nghệ cao, góp phần hạn chế, loại bỏ tội phạm công nghệ cao ra khỏi đời sống quốc tế./.

DANH MỤC CÔNG TRÌNH NGHIÊN CỨU KHOA HỌC ĐÃ CÔNG BỐ CỦA NGHIÊN CỨU SINH CÓ LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN TIẾN SĨ

* * *

*** Các công trình khoa học đã được công bố trên các Tạp chí chuyên ngành trong thời gian Nghiên cứu sinh thực hiện Luận án tiến sĩ:**

1. "*Hài hòa hóa pháp luật trong phòng chống tội phạm công nghệ cao*", Tạp chí Luật học, số 8 năm 2020.
2. "*Khung pháp lý về cơ chế hợp tác phòng chống tội phạm mạng trong khu vực ASEAN*", Tạp chí Luật học, số 12 năm 2020.
3. "*Nhận diện tội phạm công nghệ cao trong pháp luật quốc tế và một số kinh nghiệm đối với Việt Nam trong tình hình mới*", Tạp chí Giáo dục và xã hội, số đặc biệt năm 2020.

MINISTRY OF EDUCATION AND TRAINING MINISTRY OF JUSTICE

HANOI LAW UNIVERSITY

DO QUI HOANG

INTERNATIONAL LAW IN COOPERATION TO FIGHT HIGH-TECH CRIME – ISSUES FOR VIETNAM

Specialization: International Law

Code: 9 38 01 08

SUMMARY OF DOCTORAL THESIS OF LAW

Hà Nội - 2021

The work was completed at:

Hanoi Law University

Science instructor:

1. Prof. Dr. Lieutenant General. Nguyen Ngoc Anh

2. Assoc.Prof.Dr. Nguyen Thi Kim Ngan

Reviewer 1:

Reviewer 2:

Reviewer 3:

The thesis will be defended in front of the School-level Thesis Judging Committee at Hanoi Law University at…

Thesis can be found at:

1. National Library
2. Library of Hanoi Law University

PREAMBLE

1. The urgency of the topic

In the 21st century, with the development of science and technology, the explosion of high technology and new technology-applied products have made our life a lot more convenient, and at the same time quickly narrowed the gap between countries. However, the surge of science and technology, although boosts up the process of international exchange and cooperation, but also creates means for the development of crimes. The development of crimes expands not only in scope and level of damage, but also becomes more sophisticated when criminals apply new technologies in their crimes. This causes concerns for, and greatly effects, not only one single country but also the whole international community.

In addition to the known carefully organized nature of criminals, now, with the surge of science and technology, their methods and tricks are even more variable, sophisticated, and discret. Not stopping there, high-tech crimes exist in almost every field of cooperation, causing enormous damage, seriously effecting the security of each country as well as the entire network security.

In practice, international law does not have a comprehensive and uniform legal basis in preventing and fighting against high-tech crimes. However, the international community has also realized the need for an international legal document to create a common and effective framework for cooperation in preventing and fighting against this form of dangerous crime.

In Vietnam, high-tech crime is a new type of crime that just occured in the recent years, but has escalated rapidly in both quantity, how threatening it is, and level of damage. In national security, international hostility and reactionary forces constantly take advantage of communication channels through social networks and the Internet to: distort, falsify, bombard the policies and laws of the Party and State; call for gathering forces to create chao, especially before and during important political events of the country. In addition, criminals use high technology through computer networks, telecommunications networks, the Internet or digital devices to illegally seize properties; buy and sell all kinds of equipment and software to eavesdrop voice calls, steal personal information in mobile phones; gamble online and put down bets for football on the Internet, etc. The situation is complicated and unpredictable.

From the actual facts and consequences caused by high-tech criminals, it is clear that high-tech crimes have some particular specification, make them different from other types of international crimes, such as: acts of crime on the use of electronic devices with network connections (mainly computers, digital devices...); The subjects to carry out crime are those who have knowledge, ability to update, access quickly and have proficient skills in information technology and especially, high-tech crimes often cause serious consequences economically, and is hard to estimate the aftermath. Therefore, cooperation in the security system requires to be implemented at a high level; Along with that, requirements in information connection and sharing to identify criminals also need to be set out. It is impossible to punish this type of crime without cooperation at a comprehensive level. In fact, most cases of national security data breaches are carried out by individuals who have previously served in government agencies (the Edward Snowden case or the Wikileaks case). Along with that, in cooperation mechanism, the professional qualifications in information technology of this crime prevention team also need to be upgraded and updated regularly; ensure the capacity to prevent and fight high-tech crimes in the future.

For the above mentioned reasons, the study and clarification of international law provisions related to high-tech crimes as well as cooperation activities to fight against this type of crime are necessary, especially in context of the current industrial revolution 4.0. From there, to draw reference values for Vietnam in the process of cooperation in the fight against high-tech crime.

2. Object and scope of the thesis's research

The object and scope of research of the thesis focus on international legal issues on high-tech crime as well as cooperation activities to fight against this type of crime. Whereby:

Research subjects of the thesis topic include:

- Theoretical issues on high-tech crime and cooperation activities in the fight and prevention against hi-tech crimes; distinguish and identify high-tech criminals with other related crimes.

- The provisions of international law and the laws of some particular countries on high-tech crimes as well as activities in the fight against and prevention of hi-tech crimes in current context.

- Current situation of high-tech crime in the world as well as cooperation activities in the fight against high-tech crime. Thereby, the thesis topic will also draw some experiences and reference values for Vietnam.

- Legal basis and actual facts of cooperation in fighting against high-tech crimes in Vietnam. Some projections, solutions and directions in preventing this type of crime in the new condition.

On the basis of analyzing content of the above research objects, the scope of research of the thesis includes:

- Identify and distinguish several terms related to high-tech crime, present and analyze approaches to high-tech crime, thereby building a common definition of high-tech crime, its characteristics and classification.

- Contents of regulations of international law and laws of some countries on high-tech crime; regulations governing cooperation activities in the fight against high-tech crime.

- The current situation and Vietnamese law on high-tech crime and cooperation in the fight against high-tech crime in the current context. On that basis, give directions and solutions for Vietnam in the upcoming period.

3. Purpose and research tasks of the thesis

The purpose of this thesis is to clarify the theoretical-legal issues of high-tech crime as well as the provisions of international law in cooperation to fight against this type of crime; At the same time, clarify Vietnam's regulations and enforcement practice, on that basis, present projections and propose solutions to improve the law and enhance the efficiency of law enforcement activities in Vietnam regarding high-tech crime.

To achieve the above objectives, the thesis will focus on solving the following tasks:

- Analyze and research theoretical issues on high-tech crime and the contents, principles, roles and sources of international law in cooperation to fight against high-tech crime;

- Analyze and evaluate the provisions of international law, the implementation of international law on high-tech crime in some countries. Thereby, draw some experiences and reference values for Vietnam;

- Comment and evaluate the regulations and practice of Vietnam's law enforcement process regarding high-tech crime, thereby, proposing solutions and directions to improve the law in order to enhance the effectiveness of law enforcement activities in field of cooperating to fight and prevent high-tech crime.

4. Methodology and research methods

The thesis topic is made on the basis of the scientific methodology of Marxism - Leninism, applying a combination of the views of dialectical materialism and historical materialism. In addition, specific research methods are also used in the thesis, for example: deductive-inductive (chapters 2 and 3), analysis (chapters 2, 3 and 4), synthesis. (chapters 3 and 4), comparison (chapter 2, chapter 3 and chapter 4), systematization-generalization (chapter 2, chapter 3 and chapter 4), etc.

In addition, the thesis is also conducted on the basis of deeply grasping the viewpoints on the leadership of the Communist Party and the State of the Socialist Republic of Vietnam, especially the views and orientations of the Communist Party of Vietnam. The Party on crime prevention and control in the new situation and the National Strategy for Crime Prevention and Control up to 2020.

5. Scientific significance and novelty of the thesis

The thesis is a scientific work that comprehensively studies theoretical and legal issues about the formation and development of high-tech crimes as well as the provisions of international law in combating cooperation. prevent this type of crime; At the same time, clarify Vietnam's regulations and enforcement practices, on that basis, propose solutions to improve the law and

improve the efficiency of law enforcement activities in Vietnam regarding high-tech crime. The thesis has some new scientific contributions as follows:

- First, the thesis analyzes and synthesizes theoretical issues on high-tech crime and the provisions of international law in cooperating to fight against high-tech crime. Thereby, the concept of high-tech crime was developed as well as clarified the characteristics of this type of crime on the basis of comparison with other relating terminologies.

- Second, the thesis evaluates the provisions of international law, the practice of implementing international law on high-tech crimes of some specific countries. Thereby, draws out some experiences and reference values for Vietnam.

- Third, the thesis gives comments and evaluates the regulations and practice of law enforcement in international cooperating to fight against and prevent high-tech crimes in Vietnam, thereby, proposes solutions, methods and directions to improve the law in order to enhance the effectiveness of law enforcement activities in field of international cooperation to fight against high-tech crime.

6. Research question and research hypothesis

Before conducting research on the doctoral thesis, the PhD student asked himself a number of research questions, including:

- Descriptive question: What is high-tech crime? The crime is regulated at what level and to what extend? Regarding high-tech crime, what are the approaches and how to use the terminology? What is the actual situation of these crimes in reality? What is the correlation rate between the types of crimes? The frequency of the most common crime in reality? What are the activities to fight and cooperate to prevent this type of crime? How effective are they actually? Etc.

- Comparative and cause-and-effect questions: compare to show the similarities and differences between high-tech crime and other types of crime; After comparison, how is high-tech crime related to other types of crime? Is this a new type of crime or just a variation of traditional crime types? Compare the experience and legal practice of some developed countries in the area of high-tech crime prevention? Draw some lessons from experience and relate to Vietnam? Etc.

Starting from the research questions, the PhD student made an initial preliminary statement of research hypothesis, which is:

High-tech crime is a type of crime arising in the information technology era, with many characteristics similar to crimes of international nature or transnational organized crime, much more dangerous and cause more unpredictable consequences than traditional crimes. Therefore, it is necessary to study, adjust and jointly solve through international cooperation (hypothesis 1).

- High-tech crime is just a variation of traditional crimes, so it is only necessary to improve the provisions of national laws to prevent this type of crime (Hypothesis 2)

- The method of international cooperation plays a decisive role in the process of fighting against high-tech crime (hypothesis 3)

Through the research process, the PhD student rejects Hypothesis 2 and focuses on developing and proving Hypothesis 1 and 3. At the same time, the PhD student presents the Main Thesis for his research work as follows: "In the current context, high technology crime is both a challenge and a new product of the era along with the negative impact to individuals, legal persons, national or even the will of the whole community; Therefore, the legal basis, content and methods of international cooperation in the fight against this type of crime also have many specific features and need the dedication and goodwill of the actual factors".

Around the main thesis, the PhD student has designed an argument system to prove his main thesis. The system of accompanying arguments includes all three dimensions: supporting arguments, opposing arguments and opposing arguments. In addition to the three-dimensional arguments above, the PhD student also uses another type of argument, which we will call "data argument" here; these are figures, tables, factual evidence or factual references and are cited by authentic, reliable sources. Combine all of these

arguments to support the main thesis. of his doctoral thesis (see details in the following sections of the thesis).

7. Structure of the thesis

In addition to the introduction and conclusion, the structure of the thesis includes 4 chapters:

- Chapter 1: Overview of research on issues related to the thesis topic;

- Chapter 2: Some theoretical issues on high-tech crime and international law in cooperation in the fight against high-tech crime.

- Chapter 3: Contents of international law in cooperation in the fight against high-tech crime and the practice of some countries.

- Chapter 4: Law and practice of international cooperation in the fight against high-tech crime in Vietnam..

CHAPTER 1
OVERVIEW OF RESEARCH ISSUES RELATED TO THESIS THEME

The 4th industrial revolution is not merely an inevitable trend, but it has become an active practice taking place in most countries around the world as well as on a global scale. Besides the great benefits, it also brings non-trivial, non-traditional security challenges for each country and region. Since the late 90s, early 2000s until now, the term " high-tech crime " has been mentioned with increasing frequency in both legal and practical aspects, on many levels from from international, regional to national and has become the object of research in many scientific research works of different authors in foreign countries as well as in Vietnam and mentioned through a number of format, as cybercriminals; computer crime; computer-related crimes; technology criminal offenses; virtual crime; electronic crime. Regarding the form of expression, the category of "high-tech crime" is studied through categories such as monographs, thesises, articles published in specialized journals, scientific research topics. Studies or articles in scientific conferences... The research works related to the thesis topic initially provide an overview from which readers can have an overall idea about what high-tech crime is; the characteristics and common patterns of high-tech crimes compared to other types of crimes; the impacts of high-tech crime on the rights and interests of each individual, legal entity as well as each country and region in many fields; from there, the works evaluate and point out the "gaps" of the law (including international law and national law) in regulating the current high-tech crime. However, the research works mainly focus on the type of cybercrime or have not approached and researched systematically, comprehensively and fully on high-tech crime in all theoretical, legal and practical aspects. Or the works approaching from an international legal perspective that have not received much attention; The works are mainly approached through the perspective of national criminal law and presented in form of short articles published in specialized journals, so they only mention a few aspects of high-tech crime. On the basis of comparison with the purpose, research tasks of the thesis, and limitations of the previously finished works, the thesis will clarify the following issues, to shed light on the cooperation to fight against high-tech crime in the international as well as Vietnamese law fom theoretical, legal and practical perspective, including:

* In theory: the thesis will delineate and clarify the connotations of terms being used inconsistently but directly relate to high-tech crimes, from there construct a comprehensive definition of high-tech crime, especially in the current context and practical situation and theoretical issues in international cooperation in crime prevention and control in general and especially in crime prevention and control. high-tech crime in particular (law sources, content, roles and cooperation methods).

* Legal: the thesis will focus on researching, in a comprehensive and systematic way, legal issues relate to high-tech crime and international cooperation to prevent this type of crime, especially the provisions in a number of current documents, typically the Budapest Convention on Cybercrime of the Commission of Europe and other relevant international treaties and documents. The thesis will also expand the scope of research to the implementation of international law in cooperation in the fight against high-tech crime of some typical countries; Thereby, drawing some values of experience and reference lessons for Vietnam related to this issue.

* In practice: the thesis will assess current situation and updated developments on high-tech crimes both internationally and in Vietnam; Thereby, making projections and solutions that are applicable in the process of cooperation to fight and prevent high-tech crimes today. In addition, the thesis will focus on evaluating the construction and enforcement of international and Vietnamese laws in the field of cooperation in the fight against high-tech crime according to the criteria of the Pacta sunt servanda principle. On that basis, the thesis will continue to comment on issues of the current legal regulations in order to offer comprehensive directions and solutions from many angles to improve the law and enhance the efficiency in law enforcement in cooperation to fight against high-tech crime, especially in Vietnam, especially in the context of the current 4.0 industrial revolution.

CHAPTER 2
SOME THEORY ISSUES ABOUT HIGH-TECH CRIME AND INTERNATIONAL LAW IN COOPERATION TO FIGHT AGAINST HIGH-TECH CRIME

***

2.1. High-tech crime concept and cooperation to fight and prevent high-tech crime

Before studying international law of cooperation to fight against high-tech crime, it is necessary to clarify the connotations of some concepts such as "high-tech crime", "cooperation to fight" in order to prevent and fight high-tech crime. It is possible to unify the concept of legal relations and legal regulations governing this issue, thereby define the basis, content, principles, subjects, forms and institutions in cooperation to fight against high-tech crime.

2.1.1. High-tech crime concept

2.1.1.1. Definition of high-tech crime

As for terminology, the term "high-tech crime" in the laws of many countries around the world such as Australia, USA, UK, etc. has defined related crimes such as high-tech crime (high- tech crime); cybercrime (cybercrime); virtual crime (Virtual Crime); computer crime / computer crime (computer crime); computer-related crime (computer-related crime); crime is enabled / supported by technology (Technologically Enabled / Supported Crime)...

Through studying the above definitions and approaches, it is possible to see the similarities in the content of these concepts; All are directed towards acts related to the illegal use of computers and digital devices, illegal exploitation of computer networks and telecommunications networks to harm the interests of organizations, individuals and organizations, the whole society. Therefore, a general definition of high-tech crime can be drawn as follows: high-tech crime is a form of crime carried out through the use of knowledge, skills, tools, and achievements of high-level information technology, violate digital information and stored electronic data, processed and transmitted in computer systems and high technology devices, seriously harm the legitimate rights and interests of individuals, organizations as well as countries and the international community.

2.1.1.2. Characteristics of high-tech crime

Foremost, high-tech crimes are dangerous acts to society, the similarity in the basic components of a crime. However, the core difference between them and other crimes is "information technology, computers and the internet" plays a decisive role in the implementation, concealment and incalculable consequences for society of criminal acts.

Second, about the subject of the crime, high-tech crimes are carried out by subjects with up-to-date knowledge and deep understanding of computers. However, there are also cases where the subject is the person who does not fully understand the regulations related to the operation, exploitation and use of computer networks or electronic tools, leading to unintended damages.

Third, about the nature of the crime and the acts related to high-tech crimes are often very sophisticated.

In addition to the above-mentioned basic differences, there are also some other specific signs compared to common criminal groups such as the international and cross-border nature of this type of crime; the increasing

nature of the number and consequences, the sophistication of how to proceed with the development of the scientific and technology revolution.

2.1.1.3. Classification of high-tech crimes

A common classification in the world today is to classify crimes using high technology according to the method and purpose of committing the crime; Accordingly, high-tech crimes include two groups:

- Group 1: Criminals whose main target is computer networks and devices

- Group 2: Criminals use computer networks or devices to support criminal activities

Based on the role of computers in criminal acts, high-tech crimes include crimes involving computers and crimes with the following three roles:

- Computer is the purpose of criminals

- Computers are tools of crime

- The computer is a medium to hide and store the things that have been appropriated

Based on the nature of the criminal activity, high-tech crimes can be divided into many forms such as:

- First, Hacking: This is a type of criminal act capable of understanding online programs in a sophisticated way and using their abilities to infiltrate computer systems and data systems and access to users' personal information

- Second, Identity Theft: This type steals people's personal identity information and use that information for themselves or put it up for sale in underground forums online.

- Third, Fraud: This type of crime does not need to break into the server to get personal information, Hacker and Identity Theft can build fake programs to trick users into automatically providing personal information for them.

- Fourth, Predators: This is a type of cybercriminal who specializes in using social networks to find victims and collect information.

In Vietnam, Instruction 16/HD-BCA-C41 dated December 31, 2013 of the Ministry of Public Security guiding the implementation of a number of provisions in Circulars 18, 19, 20, 21, 22 dated April 1, 2013, The Minister of Public Security's regulation on basic professional work of the People's Police force instructs how to classify groups of criminals using high technology into two systems: the system of violating the activities of computer and telecommunication networks, and the system that takes advantages of computer and telecommunications networks to conduct illegal activities. Accordingly, crimes using high technology are classified as follows: (i) Crimes of using computers, digital devices, computer networks, and telecommunications networks to damage confidentiality, integrity and availability use of computer systems; and (ii) Criminals use computers, digital devices, computer networks, and telecommunications networks as tools and means to commit crimes.

2.1.2. The concept of cooperation to fight high-tech crime

Cooperation in the fight against high-tech crime is the practice of states as well as other subjects of international law on the basis of national laws, international treaties or international practices, as well as principles of international law. To coordinate and assist each other in building a legal basis and providing mutual legal assistance in criminal matters, extradition, receipt and transfer of convicts and other cooperative activities in service of the investigation, prosecution, trial, judgment enforcement and punishment of high-tech criminals.

2.1.2.2. Features of cooperation in the fight against high-tech crime

On the basis of the concept of cooperation in the fight against high-tech crime, some basic characteristics can be drawn as follows:

First, subject of cooperation: the subject of international law

Second, object of cooperation: The object of cooperation in the fight against high-tech crimes is real life high-tech crimes.

Third, cooperation objectives: cooperation in the fight against high-tech crime towards the following main objectives: (1) Cooperation in the fight against high-tech crime for the purpose of solving the case about TPCNC quickly, objectively, fairly and effectively not only within a country but also globally; (2) Cooperation in the fight against high-tech crime towards

protecting the sovereignty of countries, protecting the country from negative impacts from the infringement and attack of criminals nationally and globally; (3) Cooperation in the fight against high-tech crime, strengthening the friendship and cooperation among countries requires efforts, especially the goodwill of countries towards lawful internation activities in cooperation to prevent crimes.

Fourth, form of cooperation: in fact, international cooperation activities are carried out by way of mutual legal assistance in tracking down criminals hiding in the territory of other countries, extraditing criminals. to the relevant countries or to transfer the convicted person or to receive the necessary information and documents on the criminal case.

2.2. Theory of international law in international cooperation in the fight against high-tech crime

2.2.1. Definitions and characteristics of international law in cooperation in the fight and prevention of high-tech crimes

International law in cooperation to fight and prevent high-tech crimes includes a set of principles and legal norms that mornitor the relations between subjects of international law in conducting all the necessary activities between the parties, in order to prevent, punish and eliminate high-tech crimes from international as well as national environments.

2.2.2. Sources of international law in cooperation in the fight against high-tech crime

On a global scale, to date, there is only one international treaty to regulate this type of crime, the 2001 Commission on Cybercrime Convention (Budapest Convention). In addition to the Budapest Convention, some contents of the Palermo Convention against Interstate Organized Crime of 2000, although not directly referring specifically to types of high-tech crime, but the Palermo Convention with 41 articles, is always considered as a necessary reference in the process of international cooperation in the fight against crime.

On regional level, a number of legal frameworks have been formed as a legal basis for cooperation activities among members of a number of regions in the prevention and control of high-tech crimes, including mainly two types: regional international treaties, and documents by relevant authorities of international organizations provide, that bind the member states together in preventing and controlling high-tech crimes.

On bilateral level, the most common are still international treaties signed between countries on mutual assistance of criminal justice, extradition and transfer of convicted criminals.

In addition, international practices also play a certain role in international cooperation in the fight against high-tech crime.

Along with the types of legally binding sources above, a number of sources have no binding legal value, especially the Resolutions recommended by international intergovernmental organizations and the rulings. International jurisdictions also play an important role in regulating high-tech crime prevention activities.

2.2.3. Principles of international law in cooperation in the fight against high-tech crime

2.2.3.1. General principles of international law

International cooperation to fight against crime in general and prevent high-tech crime is one of the activities subject to international law. Therefore, the principles of international law in the fight against high-tech crime also include the basic principles of international law in general, especially the principle of equality and respect for the independence, sovereignty, and do not interfere in each other's internal affairs; principle that all the countries have the obligation to cooperate, and especially the principle of Pacta sunt Servanda.

2.2.3.2. Special principles

In addition to the general principles, international law in the prevention of high-tech crimes is also regulated by a number of separate principles as follows:

First, the principle of reciprocity

The principle of reciprocity is essentially derived from the principle of sovereign equality between states. Accordingly, on the basis of sovereign equality, a state has the right to "treat" another state the same way that that country has been, is doing or will "treat" itself.

In international criminal law, cooperation activities to fight against crime are carried out on the basis of: 1. international treaties, 2. international practices, and 3. national law. With international treaties, legal issues regarding specific cooperative activities will be regulated by the provisions of the treaties themselves, for example legal issues of extradition cases, cases of mandatory refusal of extradition, considerations to refuse extradition or required documents, costs, handling of extradition requests when there are many countries making the same request... will be specifically recognized in extradition treaties such as bilateral and multilateral extradition agreements, mutual criminal justice agreements, which also cover extradition issues. If there is no international treaty applicable, cooperative activities will be carried out on the basis of international customs or national law. In this case, the principle of reciprocity will become a very important basis for the countries to consider whether or not to conduct cooperative activities at the request of the related country, especially for criminal extradition and criminal justice assistance requirements.

Second, the principle that the scope of cooperation must be as wide as possible

The principle that the scope of cooperation to as wide as possible is enshrined in the Bundapest Convention, which states: State Parties shall cooperate with each other, in accordance with the provisions of this chapter, and through the application of these principles, international documents on international cooperation in field of criminal justice, and the laws of their respective countries, to the greatest extent possible for the purposes of the investigation and conduct of proceedings in relation to criminal offences regarding computer systems and computer data, or to collect evidence in electronic form (Article 23).

2.2.4. Contents of international law in cooperation in the fight against high-tech crime

The content of international law in international cooperation in the fight against high-tech crime is very diverse, including: First, international law sets out and clearly defines obligations for countries to comply with. harmonize the law as well as build and perfect the national legal basis for activities in the fight and prevention of high-tech crimes. Build a national legal basis for high-tech crime response activities is also a traditional obligation on the basis of the Pacta sunt Servanda principle. Second, mutual criminal justice assistance. From national sovereignty, the procedural authority of any country may only conduct procedural activities in the territory of that country. However, in many cases, the resolution of cases goes beyond national borders. Third, extradite criminals. It is through the transfer of criminals who are on the run from the national territory to the requested State that the State can initiate legal proceedings to ensure that any offenses are punished before law. Fourth, transfer the person who has been sentenced abroad to the country of which he is a citizen to serve the prison sentence according to the sentence pronounced by the court. Fifth, the delimitation of criminal jurisdiction on the basis of a number of principles is the act of determining which country has jurisdiction over high-tech crimes in cases where the offenses involve more than one nation.

2.2.5. The role of international law in cooperation in the fight against high-tech crime

International law is the basis for states to conduct these cooperative activities. Through cooperation contents such as the formation of international agencies and institutions in the prevention of high-tech crime; harmonization of laws; mutual criminal justice assistance; extradition; conducting investigation coordination… international law has formed a common legal mechanism at different levels, from bilateral, regional to global to connect activities between countries, from there, effectively respond to high-tech crimes, contributing to limiting and eliminating high-tech crimes from international life.

CHAPTER 3
CONTENT OF INTERNATIONAL LAW IN COOPERATION FIGHT, HIGH-TECH CRIME AND PRACTICE IMPLEMENTATION OF SOME COUNTRIES

3.1. International law stipulates obligations for countries to harmonize laws and perfect the national legal basis for high-tech crime prevention and combat activities.

3.1.1. Harmonizing the laws of countries in the prevention of high- tech crime

Legal harmonization is recognized as one of the basic contents in order to create similarities between the legal systems of countries, thereby, contributing to reducing barriers in the implementation of cooperative activities. specifically in the process of investigating and adjudicating crimes or avoiding creating loopholes so that offenders can avoid being punished by the law. The degree of harmonization depends on many factors such as the degree of association between members; the degree of difference between countries in terms of policies and laws and the degree of "openness" in receiving changes to the national legal system itself when implementing commitments on harmonization. Legal harmonization can prevent offenders from taking advantage of differences in legal regulations between countries to evade legal punishment, and at the same time, facilitate cooperation activities. international cooperation between countries in preventing and punishing high-tech crimes, especially related to extradition and mutual criminal justice requests.

3.1.1.1. Criminalizing violations related to high technology

Subject to the provisions of the Budapest Convention, each State Party shall enact legislation and other measures as necessary for the recognition of criminal offenses under its domestic law for acts committed intentionally, include: First, the group of acts against the confidentiality, integrity and availability of computer data and computer systems including illegal access, illegal interception, data disturbance, disturbance system, misuse of equipment; Second, computer-related acts, including computer-related forgery, computer-related fraud; Third, acts involving child pornographic materials; Fourth , acts of infringing copyright and related rights and fifth, acts of attempting and supporting the performance of the above acts. In the event that the above act is performed by an individual for the benefit of the juridical person, and if that individual is a representative or holds a leadership position at an agency of the juridical person on the basis of his authority to represent the juridical person, the the right to make decisions on behalf of the legal person or the authority to exercise internal control, or the legal person has failed to properly control and supervise the above individuals, leading to the implementation of the above actions for the benefit of the legal entity. juridical persons, States must also enact laws and other measures where necessary to recognize the liability of juridical persons, including criminal, civil or administrative liability (Article 12).

In addition to international treaties, a number of legally binding documents are adopted by international organizations such as European Union Directives passed by the European Parliament, the European Complementary Council or the European Union. The Economic Community of West African States directive passed by Parliament also recognizes the obligation of member states to enact domestic legislation to make the acts listed in this document a criminal offence. . The determination of what acts will be considered a crime in different documents, because there is no document that defines technology crime in the direction of pointing out common characteristics for identification, but only in accordance with the law. list of behaviors that are considered high-tech crimes.

3.1.1.2. Harmonization of punishment

The problem of harmonizing punishments prescribed in international documents on high-tech crimes can be divided into two levels: First , recognizing the general rules in determining penalties in countries; Second , stipulate the minimum penalty threshold for each act and the criminal law of

the country must stipulate that the penalty must not be lower than this minimum penalty threshold.

The current common level of harmonization of penalties is the recognition of general principles in penalty determination, while the specific regulation will be determined by each country. Accordingly, the principles commonly prescribed to determine punishment include: proportionality, effectiveness, and deterrence. This principle is enshrined in most documents such as Article 13 of the Budapest Convention, Article 31 of the African Union Convention on Cybersecurity and Protection of Personal Data, Article 28 of the Directive on Combating Cybercrime. by the Parliament of the Economic Community of West African States… However, the content of these principles will be determined by each country.

Compared with the first level, the provision of a minimum penalty threshold represents a higher level of cooperation. To achieve this, it is required to satisfy two factors at the same time, one is the similarity between members; the second is political determination, goodwill and the desire to deepen the level of cooperation between the parties. These two factors are closely related. If there is no similarity between members, there will be no basis for upgrading the level of cooperation. On the contrary, even though there are great similarities between the members, if there is no goodwill and expressed desire to enhance cooperation, this cannot be achieved.

3.1.2. Building and perfecting the national legal basis for high-tech crime response activities

According to the provisions of international law, the country is obliged to respect and fully implement the international commitments of the country. However, the Pacta sunt Servanda principle only imposes an obligation on a state to fulfill its international commitments conscientiously and in good faith, and how and in what manner is usually up to the state. decide for themselves on the basis of their sovereignty in accordance with the provisions of national law. Therefore, the country, on the basis of sovereignty, will decide on the implementation of its international commitments in one of two ways, or directly apply the provisions of the international commitments within its territory. or transform (introduce) the provisions of international commitments into national law through the issuance of new legal documents or amending and supplementing existing ones to ensure compliance. compatible with those international commitments. There are, however, a few exceptions, which are the case where some international treaties directly prescribe the obligation of states to enact legislation to implement the treaty's provisions, typically in the area of human rights, many Conventions have recognized a clause that says " States Parties must take legislative measures to ensure the rights enshrined in the Covenant " such as the Covenant on Main Civil Rights (Article 2), Covenant on Economic, Social and Cultural Rights (Article 2), Convention Against Torture and Other Cruel, Inhuman or Degrading Punishment or Treatment (Article 2) 2), Convention on the Rights of the Child (Article 4)…

3.2. Mutual criminal justice assistance

3.2.1. Contents of mutual criminal justice assistance

The principle of mutual legal assistance enshrined in the Budapest Convention is that the QGTV must ensure the widest possible provision of mutual legal assistance for the investigation or prosecution of computer crimes. computer or computer data or collect evidence in electronic form about the crime.

In addition to the above common contents, a number of international treaties on high-tech crimes such as the Budapest Convention, the Arab Convention on combating information technology crimes, etc. have recorded the contents of mutual criminal justice assistance. specifically related to this type of crime, including:

(1) Mutual legal assistance relating to provisional measures: are ad hoc measures that one State requests another State to take for the purpose of responding to the urgent circumstances of the case under consideration. promptly collect evidence, protect evidence for the process of conducting legal activities in the future.

(2) Mutual legal assistance in investigative activities: in the course of conducting investigations, countries may require other countries to perform

certain MLA activities related to data access and collection. or block content data.

(3) Establish a 24/7 Network: a 24/7 network is a point of contact that operates 24 hours a day and 7 days a week to provide timely assistance in the investigation or conduct of legal proceedings against crimes involving computer systems or computer data, collecting evidence in electronic form.

(4) Cross-border access to stored computer data: QGTV may cross-border access to stored computer data with the consent of another QGTV (Article 32 of the Budapest Convention).

However, in some special cases, QGTV may carry out this activity without the permission of the country concerned. This exception is documented in the Budapest Convention, which includes:

First, access to stored computer data available (open source) regardless of where the data is located;

Second, to access or receive, through a computer system in its territory, computer data stored in the territory of another State, if the State has legally and voluntarily consented to it. from a person who has the legal right to disclose the data to the country concerned through that computer system.

3.2.2. Procedures and modalities for mutual legal assistance

Mutual legal assistance procedures for high-tech crimes are both directly regulated in treaties on high-tech crimes as well as recognized in separate treaties on mutual legal assistance, conditions and the order of procedures for mutual assistance is conducted in the following ways:

- The requesting State shall send the request for mutual legal assistance in writing to the agency designated as the focal point for receiving the request for mutual legal assistance, which specifically notes the content requiring mutual legal assistance.

- After receiving the request for criminal legal assistance in accordance with the procedures, the requested State shall study and authorize the conduct of the requested mutual legal assistance activities in its territory. However, the criminal procedure laws of the requesting State may apply, if the requested State consents.

Expenses for mutual legal assistance in the territory of the requested State are usually paid by the requesting State, unless otherwise agreed upon by the parties in other specific cases.

Regarding the refusal of mutual legal assistance, the cases of non-mutual legal assistance are provided for in treaties relating to the mutual legal assistance

3.3. Extradition

3.3.1. Conditions and modalities for extradition

In principle, extradition is a state right and derives from state sovereignty. On the basis of the supreme power within the territory, the State has the right to decide whether to transfer or not the individual present in its territory to the requesting State for criminal prosecution. . Many countries have enacted specific extradition laws, which recognize one of the important principles of extradition, that is, extradition is conducted on the basis of the principle of reciprocity.

Extradition of criminals is a binding international legal obligation that arises only when there exists a corresponding international treaty between the countries concerned that stipulates specific conditions for extradition. However, this obligation is not absolute. Because, even in the case of a treaty, extradition can only be carried out in accordance with the procedures and conditions consistent with the provisions of that international treaty. Even in Article 1 of the European Convention on Extradition, although titled "Obligation to Extradition", it clearly shows this when it stipulates that: "The Contracting Parties shall make arrests for each other, in accordance with under the terms and conditions set forth in this Convention, all persons whom the competent authority of the requesting State is investigating for an offense or is wanted by the competent authority in order to comply with the law. sentence or detention decisions".

In order to be able to invoke treaties on the prevention of transnational crimes as a basis for extradition, high-tech criminals must fully satisfy the conditions of transnational crimes. As defined by the Palermo Convention, a transnational crime is a crime where the offense is committed in more than

one country or is committed in one country, but the main part of the preparation, planning, directs or directs the commission of a crime to take place in another country, or the crime is committed in one country but involves an organized criminal group engaged in the commission of crimes. criminal activity in more than one country, or a crime committed in one country that has a serious effect on another (Article 3).

3.3.2. Extradition conditions, non-extradition cases

The most common extradition condition is the principle of "double identification" with the requirement of a prison term. For example, under the provisions of the Budapest Convention, extradition between States Parties to the Convention is made provided that the offense is criminally punishable under the laws of both States concerned with the crime. penalty of deprivation of liberty for at least 1 year or more or a heavier penalty (Article 24).

Regarding non-extradition cases, the grounds for refusing to extradite high-tech criminals in particular as well as crimes in general are commonly prescribed as follows:

- Do not extradite political criminals or do not extradite their own citizens.

- The act on which the extradition request is based has been tried in the requested country (Non bis in idem principle – No one should be tried for the same offence)

- The extradition is inconsistent with the law of the requested country, infringes upon national sovereignty or social security order;

3.4. Transfer of convicts

Common conditions for the transfer of convicts set forth in treaties include: (1) The convict is a national of the country of execution; (2) The judgment that has been pronounced is the final judgment, and there are no pending proceedings related to the convict; (3) Consent of the convicted person; (4) At the time of receipt of the request for transfer, the remaining period of serving the sentence under the sentence imposed must not be less than the time specified in an international treaty or national law; (5) Satisfy the condition of “double identification” under the criminal laws of the sentencing and executing countries; (6) The sending State and the executing State agree to transfer.

3.5. Determination of jurisdiction

Some principles of International Criminal Law in determining jurisdiction are fully applicable to high-tech crimes, including:

Territorial Principle

The territorial principle is enshrined in the Budapest Convention with the content that the QGTV enacts laws and other measures necessary to exercise jurisdiction over criminal acts committed in its territory .

In fact, the territorial principle has been established by different states as a basis for determining jurisdiction, including:

One is, where the behavior is performed.

Second , where the computer is located.

Third, the place affected by the crime.

Nationality Principle

Under the provisions of the Budapest Convention, a state has jurisdiction over an offender who is a national of that country if the act is punishable under the criminal law of the country in which it was committed or the act is committed. made outside the territory of any State (Point (d) Paragraph 1 of Article 22). The criminal law of many countries has adopted this principle in determining national jurisdiction.

In addition to the nationality of the offender as provided for by the Budapest Convention, some countries also provide for the nationality of the victim as a basis for determining jurisdiction.

Principles of nationality of ships and aircraft

According to the provisions of the Budapest Convention, a country will have jurisdiction over high-tech crimes if the act is committed on board a vessel flying the flag of the country or an aircraft registered in the country (Point b, c Clause 1 Article 22).

There is no hierarchy of precedence between the principles that define jurisdiction. The determination of which jurisdiction belongs to which country depends largely on the dispute settlement body.

3.6. The practice of implementing international law in cooperation in the fight and prevention of high-tech crimes of some countries

3.6.1. Germany

The Federal Republic of Germany ratified the Budapest Convention in 2009 and also made amendments to the Penal Code immediately after ratifying the Convention. The German Penal Code includes all the provisions that are relatively comprehensive and compatible with the basic provisions of the Convention on Computer Crimes and Cyber Crimes. Likewise, the country's Criminal Procedure Code covers most of the relevant procedural rights covered by the Convention, with the exception of a few provisions (which will be covered in subsequent chapters). next part).

Up to now, the German Republic has issued a fairly large number of relevant legal documents in the field of information security, including those enacted at the level of Laws and Acts. The main legislation related to cybersecurity in Germany are the Cybersecurity Act, the Telecommunications Act, the EU General Data Protection Regulation, the Federal Data Protection Act and the Federal Office for Privacy Act. confidential information

Germany's cyber security laws have specified conditions for ensuring network security standards for essential network products and services; regulations on responsibility for protection and activities of confidentiality, protection of information systems important to national security; regulations on rights and liabilities for web hosting businesses and access providers for piracy that occurs on their systems... In general, the law on cooperation issues struggles Crime prevention in the field of information technology in Germany is in line with international standards in this area, especially the 2001 Budapest Convention.

3.6.2. USA

US law has long been known as one of the most comprehensive, oldest and most effective legal systems in the world in terms of cybersecurity as well as high-tech crime prevention cooperation. On both legal and practical levels, the United States has always identified the threat of cyber security as the top threat to national security. Therefore, in the US Homeland Security Act (2002) stipulates: Cybersecurity risks are threats and vulnerabilities of information or information systems and any related consequences that are caused by or as a result of unauthorized access, use, disclosure, deterioration, interruption, modification or destruction of such information or information systems, including consequences associated with hacking and/or cyber-terrorism; does not include any action solely related to a breach of a term or contractual agreement with a customer. The act also established an institution called the "DHS of the United States," with the authority to act as the ultimate regulator of U.S. cyber security. Its primary mission is to prevent terrorist attacks, reduce armed and unarmed threats to the nation, minimize damage from attacks, and increase national resilience.

In addition, a number of other relevant legal documents such as the Law on Protection of Electronic Communications, the Law on Media Archives or the Law on Eavesdropping... In addition to the general laws of the Federation, the laws of the United States also create conditions for each state to pass its own laws to prevent and combat high-tech crime on a basis appropriate to the situation of each state. These are mostly legal documents with more detailed and specific provisions than general Federal law. For example, New York prohibits the use of high-tech tools and equipment for the purpose of illegally accessing documents in a computer (computer trespass), with the above violations having penalties of up to 04 years in prison or other penalties of up to 15 years in prison, depending on the seriousness of the violation.

3.6.3. Japan

In November 2001, the Japanese government signed the Budapest Convention on Cybercrime by the Commission of Europe. Accordingly, Japan has revised the Penal Code and Criminal Procedure Code to increase compatibility in the adjustment in accordance with the provisions of the Budapest Convention. Along with that, Japan enacted the Personal Information Protection Law in 2003 to protect data, personal information and

other forms of identity. In particular, the Basic Law on Cybersecurity of Japan (2014) also expands the regulation to develop common standards on measures to ensure cybersecurity for national administrative agencies and organizations. related office. Currently, Japan also has other laws that also have provisions related to high-tech crimes such as the Japanese Penal Code, the Law against Unfair Competition, the Law on Prohibition of Unauthorized Computer Access, the Law on the Sale of Paid-Instances, contributions, the Law on Protection of Specially Designated Secrets, and the Law on Social Security and Tax Code. On the basis of Japanese legal documents, it is possible to identify some basic high-tech crimes such as:

- Data theft or unauthorized access (Hacking).
- Phishing (Phishing)
- Acts of infecting IT systems with malware
- Besides the above-mentioned acts, there are some other acts such as: possessing or using hardware, software or other tools used to commit cybercrime; identity theft or identity fraud; electronic theft; or any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communication network, equipment or data...

In 2018, the National Assembly of Japan continued to pass a bill amending the Basic Act on Cybersecurity 2014 (Basic Act on Cybersecurity). Accordingly, the cybersecurity mentioned in the Amendment Law is tied to measures to manage data securely, and also clarified the responsibilities of the Japanese National Government, local governments and other agencies. other relevant organizations.

3.6.4. Some lessons learned for Vietnam

Through some legal aspects and practical implementation of international law in high-tech crime prevention cooperation in these countries, some observations can be made:

Firstly , the above countries are well aware of the nature and danger of high-tech crimes, so they have issued many laws and related documents to regulate high-tech crimes based on the the legal basis is the international conventions to which these countries are parties such as the Budapest Convention, the Palermo Convention and a number of other conventions related to high-tech crimes

Second, all three countries have clearly defined the focus and paid special attention to the contents of international cooperation in the fight and prevention of high-tech crime such as meeting the member obligations in the international cooperation agreement. harmonize and perfect the law, the issue of mutual criminal justice assistance, the extradition of criminals and the transfer of convicts.

Third, the “territory” or “place of crime” principles are principles that define the common jurisdiction of states over high-tech crimes.

From these observations, Vietnam's law can fully draw some valuable experiences for both reference and applicability in the process of international cooperation in the fight and prevention of high-tech crime. as follows:

Firstly, it is extremely urgent to develop and promulgate legal provisions in international cooperation in the fight and prevention of high-tech crimes and cyber security issues in our country in the current period. and urgent.

Secondly, Vietnam needs to soon complete the necessary legal framework related to activities in cyberspace, with special attention to the issue of relevant guiding documents in this regard.

Third, it is necessary to increase the responsiveness of separate legal documents to make timely and effective adjustments when conducting international cooperation activities to fight and prevent high-tech crime in Vietnam. Currently.

Fourth, proactively implement the prevention and combat of high-tech crimes right from within domestic security and enhance the quality of international cooperation activities in the prevention and combat of high-tech crimes..

CHAPTER 4

VIETNAMESE LAW AND PRACTICE OF INTERNATIONAL COOPERATION FIGHT HIGH-TECH CRIME

4.1. Legal status in international cooperation to fight and prevent high-tech crime in Vietnam

4.1.1. Overview of high-tech crime in Vietnam

4.1.1.1. The situation of high-tech crime in Vietnam

The acts committed by high-tech criminals in the world today are very complicated. Because the characteristics of this type of crime are internationalization and rapid integration, this has strongly influenced the situation of high-tech crimes committed in Vietnam. High-tech criminals in other countries infiltrate into Vietnam very quickly, even many foreigners enter Vietnam to organize criminal activities. Vietnam has been forecasted to be one of the hot areas for high-tech crime. Data from security firm Symantec shows that Vietnam is currently ranked 11th globally in terms of cyber threat activities (in 2018). Threatening activities targeting agencies, businesses and organizations in Vietnam include targeted attacks, threats on mobile devices, distribution of malicious code, viruses, and data theft. High-tech crimes are often concentrated in a few large provinces and cities, where there is a convergence of many fields of science and technology, finance and banking, or where many foreigners live...

4.1.1.2. Forecast of the situation of high-tech crime in Vietnam and the trend of international cooperation in the fight and prevention of high-tech crime in Vietnam

Crime using high technology in Vietnam in the coming years is forecasted to be complicated with many new criminal methods and tricks, transnational activities and occurring in many fields.

If the issue of cybersecurity is not resolved in time, Vietnam's e-commerce sector will fall into a state of stagnation, becoming a barrier to socio-economic development. Currently, there have appeared a number of ghost computer networks (botnets) developed and expanded by Vietnamese hackers, which have caused great harm to network security in general and e-commerce in particular. In addition, the trend of large-scale spamming, phishing scams, installing keyloggers, stealing information, laundering money with virtual money... is growing.

In the coming time, the fight against high-tech crimes will be a key cooperation content included in the cooperation program between countries and many multilateral and bilateral organizations. To meet this demand, in the coming time, there will be more TTTP and extradition agreements signed between Vietnam and many countries, including the content of criminal justice assistance and extradition in the fight against crime. High-tech crime.

4.1.2. Legal content for international cooperation in the fight and prevention of high-tech crimes in Vietnam

The legal basis for international cooperation in the fight against high-tech crime includes regulations promulgated by Vietnam, from the Constitution to specialized legal documents such as: Law on Information Technology 2006; Cyberinformation Security Law 2015; Cybersecurity Law 2018; Penal Code 2015; Criminal Procedure Code 2015; Decree No. 25/2014/ND-CP stipulating the prevention and combat of crimes and other legal crimes using high technology; Joint Circular No. 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC dated September 10, 2012 of the inter-agency Ministry of Public Security, Ministry of Defense, Ministry of Justice, Ministry of Information and Communications, People's Procuracy, People's Court, guiding the application of a number of provisions of the Penal Code on a number of crimes in the field of IT and telecommunications.

Especially, most recently, in the Document of the 13th National Congress, our Party clearly stated: "Actively, proactively... uphold national digital sovereignty in cyberspace in all situations". This is a content recorded for the first time in a Congress document, reflecting the Party's profound awareness of the nature of the times from the perspective of science and technology, because of the Second Industrial Revolution. It will transform the entire world from the real world to the digital world.

In addition to the regulations issued by Vietnam, implementing the policy of multilateralization, diversification and active, proactive international integration, as a responsible member in the international community, as of

September/September/ In 2017, Vietnam is a party to 22 multilateral international treaties on criminal justice, extradition and transfer of sentenced persons and 27 civil and criminal agreements with other countries. In these Agreements, there are provisions on TNCs or transnational crimes with high technology elements. Among 22 multilateral international treaties, Vietnam declares that it does not consider 10/22 multilateral international treaties as a direct legal basis for extradition such as the Convention on the Suppression of the Illicit Possession of Aircraft. 1970, United Nations Convention on Narcotic Substances 1961, United Nations Convention Against Corruption 2003, United Nations Convention Against Torture and Other Cruel Treatment or Punishment religious or humiliating people…

On that basis, the basic contents of the law on high-tech crime as well as international cooperation to fight against this type of crime include the following key topics:

4.1.2.1. Regulations on prevention of high-tech crime

The prevention of high-tech crimes today is next to the responsibility of the specialized agency in charge of preventing and combating cyber crimes (which are professional units in the People's Public Security - Department of Cybersecurity and crime prevention using technology. The People's Army is assigned the task of advising, organizing, and directly performing the task of combating and combating anti-terrorism) with the participation of individuals, organizations, enterprises and information agencies. mass news.

4.1.2.2. Regulations on fighting and dismantling high-tech crimes

Firstly, regulations on detecting and handling high-tech crimes

Second, about the measures to organize and fight against Terrorism by the specialized agency

Third, regulations on criminalization of acts of using high technology to harm the legitimate interests of individuals, organizations and the State.

Fourth, regulations on penalties for TPCNC

4.1.2.3. Regulations on subjects in international cooperation in the fight against high-tech crime

The entity directly implementing international cooperation activities in the prevention and control of crime is the Ministry of Public Security. In addition, according to the provisions of Article 65 of the 2007 Law on Food Information, the Ministry of Public Security is the agency responsible for receiving, transferring, considering and dealing with foreign requests for extradition and transfer of persons in exile. serve prison sentences; consider and transfer the file to the People's Procuracy, People's Court and carry out food concentration activities according to its competence. The Ministry of Public Security proposes the conclusion, accession and implementation of international treaties on extradition and transfer of persons serving prison sentences; propose to amend, supplement and perfect the Vietnamese law on food market. Every six months and annually, the Ministry of Public Security must notify the Ministry of Justice of the status of the implementation of requests for extradition and transfer of persons serving prison sentences.

In the anti-TPCNC activities of the Ministry of Public Security, the force that plays a key role is the Department of Cybersecurity and high-tech crime prevention and control A05 .

Coordinating entities participating in international cooperation in crime prevention and control include:

- Ministry of Justice: As the state management agency on food information, the Ministry of Justice is responsible for coordinating with the Ministry of Public Security, the People's Procuracy, the People's Court, the Ministry of Foreign Affairs, and the Ministry of Foreign Affairs in drafting legal documents guiding the implementation. Examining the Law on Food Information; participate in the negotiation, comment and appraisal of TPT agreements on criminal matters, extradition and transfer of persons serving prison sentences. In addition, the Ministry of Justice also coordinates with the Ministry of Public Security and the People's Procuracy to handle complex and sensitive entrustment requests.

- Ministry of Foreign Affairs: The Ministry of Foreign Affairs is responsible for coordinating with the Ministry of Justice, the People's Court, the Ministry of Public Security, and the People's Procuracy of the People's

Republic of China in formulating legislation on food security, and coordinating in the implementation of activities in international cooperation in the fight. crime prevention on the principle of reciprocity.

4.1.2.4. Regulations on extradition of high-tech criminals

First, the Regulation on the competence to carry out extradition.

Competent agencies on TPCNC extradition include the Ministry of Public Security, the Court, the Procuracy, and the Ministry of Foreign Affairs.

Second, Regulations on cases of extradition, refusal of extradition and extradition with a number of conditions

- In case of extradition:

+ In case a competent procedure-conducting agency of Vietnam requests the relevant foreign agency to extradite, the person to be extradited (currently residing abroad) is the person who committed the crime. or has been convicted of a criminal offence, the judgment has taken legal effect.

+ In case a foreign procedure-conducting competent agency requests the corresponding competent Vietnamese agency to carry out the extradition, the extradited subject must be a foreigner who commits a crime or is subject to extradition. a criminal conviction that has taken legal effect and is currently residing in the Vietnamese territory.

- Cases automatically refuse and can refuse to extradite to a foreign country.

- Extradition cases subject to certain conditions

4.1.2.5. Mutual legal assistance in criminal matters

Pursuant to the provisions of Law TTTP 2007 Code TTHS 2015 and practical application of operational TTTP penal between Vietnam and other countries, the scope TTTP criminal including: serving the documents, records and documents relating to the criminal TTTP; summon witnesses and experts; collect and provide evidence; Criminal prosecution; information exchange; requirements other legal assistance on criminal matters. In addition, the Code TTHS provisions TTTP criminal is one of the activities of international cooperation in criminal proceedings (Article 491), under which the activities TTTP criminal such as: Valuation legal documents and objects collected (Article 494); Regulations on the conduct of proceedings of the competent authorities of Vietnam in foreign countries and competent persons of foreigners in Vietnam shall comply with the international treaties to which Vietnam is a member or the principle of travel reciprocity (Article 495); for witnesses, experts, who are serving prison terms in the country recommended presence in Vietnam to serve the resolution of criminal cases or may allow witnesses, experts, people are serving prison terms in Vietnam presence abroad to serve the resolution of criminal cases (Article 469); tracing, seizure, distraint, freezing, confiscation and asset disposal proceeds of crime have to serve the requirements of investigation, prosecution, adjudication and enforcement of criminal judgments (Article 507); frozen accounts can be applied if there are grounds to believe that the money in the account related to the offense of the accused (Article 129); coordinate the investigation or apply measures investigation special proceedings (Article 508);

4.1.2.6. Regulations on transfer of people serving prison sentences

First, the grounds for receiving and transferring people currently serving prison sentences: comply with the provisions of Clause 2, Article 49, Article 50 of the 2007 Law on Food Trafficking and Article 6 of Joint Circular No. 01/2013/TTLT- BCA-BTP-BNG-VKSNDTC-TANDTC.

Second, cases of refusal to transfer people who are serving prison sentences.

Refusal to transfer a person currently serving a prison sentence in Vietnam to a foreign country when: there are grounds to believe that the transferee may be subjected to torture, retaliation or persecution in the receiving country; the transfer may be detrimental to Vietnam's sovereignty and national security.

Third, note about the receipt and transfer of people who are serving prison sentences

The order and procedures for receiving transfer requests and considering and deciding on the receipt are specified in Article 9 of the Joint Circular No. 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC.

Notify the right to request transfer to the person serving a prison sentence. According to the provisions of the Law TTTP 2007 and Article 12 of the Joint Circular No. 01/2013/TTLT-BCA-BTP-BNG-VKSNDTC-TANDTC.

The Ministry of Public Security shall compile a dossier of request for receipt and transfer it to the Ministry of Foreign Affairs for consideration and decision on the application of the principle of reciprocity. In countries with international treaties to which Vietnam is a contracting party, upon application for a transfer, a statement by this person that he or she fully understands the consequences of the transfer and his or her rights and obligations. the transfer. At that time, the Minister of Public Security decided to allow the receiving country to send a representative to Vietnam to verify the consent of the person serving a prison sentence.

4.1.2.7. Some other contents in international cooperation on high-tech crime prevention

Firstly, the collection, exchange of information and the pursuit of criminals through the role of INTERPOL Vietnam.

Second, push returns, evictions

Expulsion is the act of taking a foreigner out of its territory by unilateral action by the authorities of the country in which that person resides.

Push back is a measure often applied to criminals abroad, then hiding in that country.

Third, coordinating activities of police in border provinces in other countries in the fight against and prevention of crime

Police of border provinces (Vietnam's provincial police: with respective provincial-level agencies of neighboring countries) international cooperation in crime prevention and control includes the following activities:

+ International cooperation in investigation and discovery of criminal cases that the two parties are responsible for solving together.

+ International cooperation in apprehending, escorting and transferring criminal offenders.

+ International cooperation in receiving and rescuing victims of criminal offences.

Fourth, international cooperation in exchanging and providing information on crime with regional and global police organizations

Fifth, exchange of training experience and technology transfer

Within the scope and scope signed in bilateral or multilateral international treaties, the Ministry of Public Security, the People's Procuracy, and the People's Court can organize international conferences to exchange experiences and summarize combat cooperation. fight against crime between the parties.

Sixth, international cooperation in crime prevention and control between the Vietnam People's Police force and the police forces of other countries

The international cooperation mechanism in crime prevention and control related to Vietnam, the Vietnamese people's police force usually mainly follows the cooperation frameworks that are: Through the cooperation framework INTERPOL; through the ASEAN/ASEANAPOL cooperation framework; through cooperation channels with the Office of Liaison Officers of the Police of other countries in Vietnam and in Southeast Asia; through direct cooperation with a number of other law enforcement agencies such as the United States Federal Bureau of Investigation; United States Federal Drug Enforcement Administration; Transnational Crime Prevention Centers in the Asia-Pacific Network of Transnational Crime Centers,...

Or a bilateral cooperation mechanism in crime prevention and control in general and with some types of crimes in particular between the police of Vietnam's border provinces and their respective foreign partners in the form of cooperation between provinces. border, or in the form of twinning for provinces that have not signed international agreements on crime prevention and control at provincial level.

4.2. Law enforcement practice in international cooperation in the fight against high-tech crime in Vietnam

4.2.1. Results of international cooperation in the fight against high-tech crime in recent times

4.2.1.1. Regarding negotiation, signing and accession to international treaties in the prevention of high-tech crime:

- Multilateral international treaties on crime prevention and control:

According to statistics from the Ministry of Public Security, as of September 2019, Vietnam is a member of 22 multilateral international treaties that regulate criminal justice, extradition and transfer of convicts. Among these, there is 01 Special Agreement on Criminal Justice, which is the Agreement on mutual legal assistance in criminal matters between ASEAN countries in 2004 (effective in Vietnam on September 20, 2005). There are 03 multilateral international treaties that provide for the transfer of sentenced persons and the remaining multilateral international treaties all provide for extradition.

Among the multilateral international treaties to which Vietnam is a member, providing for international cooperation in the fight and prevention of crime, there are international treaties governing international cooperation in the field of crime prevention, such as.

+ United Nations Convention against Transnational Organized Crime;

+ Agreement on TP on criminal matters between ASEAN countries.

- Bilateral international treaties (Agreements) on international cooperation in crime prevention and control in general and TPCNC in particular

In the field of international cooperation in crime prevention and control in general and TPCNC in particular, Vietnam has signed many bilateral international treaties with different countries on the basis of the level of diplomatic relations and depending on the situation. demand on the scope and content of international cooperation in crime prevention and control of each country.

Currently, Vietnam has signed 45 bilateral agreements with other countries. In addition, in the field of international cooperation in the prevention and combat of crime, there are bilateral agreements between the Government of Vietnam and the Governments of relevant countries that directly regulate the fight against crimes committed by Vietnam. also signed and joined.

4.2.1.2. Regarding coordination in detecting, preventing, investigating and handling crimes using high technology in accordance with the law and international treaties to which the Socialist Republic of Vietnam is a signatory

Cooperation in the collection and verification of information and documents in service of the detection and investigation of high-risk crimes is one of the usual cooperation requirements between the Vietnamese People's Public Security Forces and the Public Security Forces of other countries. It can be verified addresses only IP that criminals use in criminal activities.

Cooperation in detecting and investigating cases of fraud aimed at appropriating property and gambling with high technology in the territory of Vietnam: From 2010 to 2017, the Vietnamese police force detected and investigated investigating and clarifying nearly 200 cases of fraud aimed at appropriating property by using high technology, mainly Chinese people, carried out in the territory of Vietnam.

4.2.1.3. Results of extradition and mutual legal assistance in criminal matters involving high-tech crimes in relation to other types of crimes

- Results of extradition work in investigation, prosecution, trial and judgment enforcement:

In the summary report of law enforcement on extradition for crimes in general by the Ministry of Public Security in 2019, the number of people with Interpol's red wanted warrants with information about hiding into Vietnam is 317. but very few foreign cases request extradition to TPCNC. By 2017, the Ministry of Public Security had received and handled 23 foreign extradition requests (12 extradition requests under bilateral extradition agreements, 11 extradition requests on the principle of reciprocity). and refused 03 invalid extradition requests. There are about 1,200 criminals in Vietnam who have fled abroad, of which 235 people have been ordered red by INTERPOL, many of whom have committed particularly serious crimes, including TPCNC. The Ministry of Public Security has prepared and forwarded 35 extradition request

dossiers to foreign competent authorities (by 2017), including 21 extradition requests under bilateral agreements and 14 extradition requests under the principle of law. reciprocity.

- Results of criminal legal assistance in investigation, prosecution and trial:

In the period from July 1, 2008 to the end of May 31, 2017, the People's Procuracy received 627 requests for criminal prosecution from abroad, of which the Office of the Investigation Police Agency of the Ministry of Public Security made 512 requests (accounting for 81.7%.), transfer to other agencies (Ministry of Foreign Affairs, Court, Consular Department of the BNG, People's Procuracy, etc.) to carry out 115 requests (accounting for 18.3%). The contents of criminal information requests that foreign countries request Vietnam to perform are mainly the service of relevant papers, records and documents.

Also during the above period, the competent authorities of Vietnam (Investigating Agencies in the People's Police, People's Court, People's Procuracy ...) have requested the foreign side to carry out a total of 660 requests for criminal investigation, in which the investigating authority. In the CAND, there were 554 requests (accounting for 83.9%) and other competent agencies requested 116 requests (accounting for 16.1%). Of which, about 78% of requests are related to countries that have signed Agreements with Vietnam. In which, the content of the request made by the investigating agency in the People's Public Security, which requested a foreign country, the collection of evidence accounted for 68% and the verification of the criminal record accounted for 32%, the taking of testimony accounted for 17% of the request total content of evidence collection.

4.2.1.4. Organization of conferences and seminars to exchange information and experiences and coordinate training, retraining and professional training:

The Ministry of Public Security of Vietnam, with a key role in preventing high-tech crimes, has coordinated with international organizations and national police to regularly conduct conferences and seminars on security and safety information security as well as crime prevention using high technology.

At the same time, the Ministry of Public Security also regularly sends forces to participate in conferences and seminars organized by the international INTERPOL force and the United Nations' committees in the prevention of crime in general and the prevention of criminal use. high technology in particular.

In addition, as a focal point for exchanging information on international crimes, INTERPOL Vietnam Office plays the role of providing warnings to police, national and international security organizations in the prevention of TPCNC.

4.2.2. Limitations in international cooperation in the fight and prevention of high-tech crimes

4.2.2.1. Problems and limitations from the provisions of the Law on Mutual Legal Assistance related to international cooperation in the prevention of crimes using high technology

After nearly 15 years of application of the Food Information Law, a number of provisions in the Food Information Law are not compatible or do not have regulations, in which there are many complex and sensitive contents, leading to difficulties in implementing the provisions of the Law on Food Information. international cooperation activities for crime prevention in general and criminal justice in particular, specifically:

Regulations related to extradition

According to 11 Agreements on TP with provisions on extradition that Vietnam has signed with other countries in the past, the People's Procuracy is the focal point of Vietnam's extradition. However, the Law on Food Information and Communications stipulates that the Ministry of Public Security is the focal point for the extradition and transfer of people who are serving prison sentences. This inconsistency has made it difficult to carry out the function of the Ministry of Public Security in extradition.

On the issue of commitment not to apply the death penalty. Some extradition agreements between Vietnam and other countries have provisions

on commitments not to apply the death penalty (such as the Agreement with the Republic of Belarus (Article 70), with Russia and Austraylia. South Vietnam still regulates many types of crimes with the death penalty and does not limit the extradition of people who has death sentence, which makes it difficult for Vietnam to negotiate agreements on extradition with European countries (where the law in many countries does not except death penalty).

The provisions of the Law on TP have omitted the case of refusing to extradite a prisoner (or a person who has been sentenced by a legally effective criminal sentence) to flee to continue criminal execution.

Regulations related to the transfer of people who have been sentenced to prison

Regarding the remaining time limit to serve the transferee's sentence. The Law on Food and Drug Administration stipulates that people sentenced to imprisonment must still serve at least 1 year, in special cases at least 6 months. However, in most of the bilateral agreements on the transfer of persons sentenced to prison that Vietnam has signed, the person sentenced to prison must still serve at least 1 year or as agreed by the parties.

Consent of the person sentenced to prison still has many problems. Currently, the Law on Food Trafficking stipulates that if a person serving a prison sentence abroad can be admitted to Vietnam to serve a prison sentence, the consent of the person being transferred is required. Thus, in case many Vietnamese commit crimes abroad (especially drug-related crimes) they will not want to return to Vietnam to execute their prison sentences. In addition, in some cases, the foreign side asked Vietnam to commit not to declare the death penalty or declare but not execute the death penalty for a person serving a prison sentence who is also the subject of criminal prosecution. of Vietnam after being transferred to Vietnam. However, Vietnamese law does not have this provision.

Regarding costs, the Law on Food Trafficking stipulates that the costs of transferring persons serving prison sentences shall be paid by the Requesting Party. But the Food Trade Agreements that Vietnam has signed again stipulate that the costs are paid by the Receiving Party minus the costs incurred entirely in the territory of the Transferring Party.

Regulations on implementation of criminal justice work

To implement the TPTP requirement, the requesting countries do not apply the death penalty. However, the Law on Food Court does not have regulations on the order and procedures for committing not to apply the death penalty in criminal proceedings.

The scope of criminal penalties prescribed in Article 17 of the Law on Food Trafficking is still limited and inconsistent with Vietnam's international commitments.

There are no specific regulations on the order and procedures for carrying out a number of similar requests, such as summoning witnesses and experts, and escorting prisoners abroad to assist in the investigation or provide evidence; transfer criminal prosecution of Vietnamese in Vietnam.

4.2.2.2. Difficulties from practical application of the law in the fight and prevention of crimes using high technology

First, the international cooperation in information exchange on TPCNC is still incomplete . USA

Second, cooperation with foreign law enforcement agencies is often time consuming. The reason for the delay is that information about criminals who want to be exchanged with foreign competent authorities must be reported through many competent levels, which leads to slowness and no combat. Or there are TTTP requests from your country requesting Vietnam with the document names accompanying the order or decision, which is not enforceable in the territory of Vietnam, so it takes time for the agency to conduct the proceedings in Vietnam. implemented by documents and decisions in accordance with domestic laws.

Third , the provisions of the law have not forecasted to adjust all the cases that will arise and are not suitable with the conditions in Vietnam . As with the extradition provisions, when the TPCNC commits an act committed in many countries or the crime is committed by a transnational criminal organization, it will result in the Ministry of Public Security receiving

documents from two or If many countries request the extradition of a person for the same crime or different crimes, the Ministry of Public Security shall assume the prime responsibility for, and coordinate with the Ministry of Foreign Affairs, the Ministry of Justice, the Procuracy of the People's Procuracy, and the People's Court to consider and decide to satisfy the extradition request. to one of the requesting countries and transfer the extradition request file to the provincial People's Court for consideration and extradition decision. However, in practice, extradition requests from different countries are often not sent to the Ministry of Public Works at the same time. The time limit for requesting file examination is 20 days, so there will be cases where the Ministry of Public Security sends to the competent provincial-level People's Courts for handling and settlement, then the Ministry of Public Security receives an extradition request in the third country. two. In this case, the provincial-level People's Court that has accepted the first extradition request must return the file to the Ministry of Public Security for consideration and decision on the satisfaction of the request. But the Law does not provide for the return of the extradition request file after it has been accepted. So this would be time consuming and wasteful, not to mention having more than two countries requesting the extradition of the same person, there needs to be an appropriate resolution.

Fourth, there is still the phenomenon of avoiding and pushing the responsibility of law enforcement forces in Vietnam in handling cases with foreign elements in general and cases with signs of criminal offenses related to law enforcement. related to the use of high technology in particular in relation to the application of the international treaty on crime prevention to which Vietnam is a contracting party. In many cases, when the police of local units receive information that the criminal has fled abroad, the investigating agency immediately suspends the investigation and closes the file without a domestic legal basis; or transfer it to a wanted agency or an international cooperation unit to implement the application of the international treaty. When the police of some units and localities believe that the procedure related to criminal proceedings, extradition request, request The transfer of the sentenced person is too complicated to carry out these procedures, leading to the neglect of the criminal or the failure to protect the legitimate interests of the parties involved or the sentenced person.

Fifth, the sanctions and penalties for handling crimes using high technology are still light, not enough of a deterrent to serve the fight and prevention of crimes. In Vietnam, according to the High-tech Anti-TPTP Police Department (C50), now renamed the Department of Cybersecurity and High-Tech Crime Prevention and Control (A05) under the Ministry of Public Security, from 2010 to In June 2014, the high-tech anti-terrorism police force across the country discovered and verified 11,476 clues of cases with signs of criminal offenses related to high-tech elements with 3,220 subjects, of which 823 cases. and 1,990 objects detected by C50; 450 cases and 1,230 subjects were discovered by the local police; The total damage caused by this type of crime is up to tens of thousands of billions of dong. But the number of cases of these types brought to trial is very small. This is also the reason why the Legislature added laws regulating crimes using high technology in the 2015 Penal Code, amended and supplemented in 2017. Due to being newly promulgated, the number of criminal cases is limited. being tried at Court for crimes using high technology accounts for a small proportion compared to other criminal cases.

Sixth, the propaganda and dissemination of education and law have not been paid due attention, leading many people to know that foreign objects borrow or rent places for non-transparent purposes, but still accept or lease them. For countries sharing a border, patrolling, border control and protection is not regular, in the context of political, economic, and regional instability affecting some people. borderline criminals are lured, deceived, bribed... to engage in criminal activities.

4.3. Solutions to perfect the law and improve the efficiency of international cooperation in the fight against high-tech crime in Vietnam

4.3.1. Solutions to improve Vietnam's law on the fight against high-tech crime

First, in terms of legal documents, it is necessary to have clear and specific regulations on the collection, examination and evaluation of electronic certificates as well as to issue guiding documents on how to handle such cases. TPCNC in the 2015 Penal Code, revised and supplemented in 2017. In addition, there should be strict regulations on responsibility and even sanctions for individuals and organizations (third agencies) in The delay in providing electronic data and assessing electronic data affects the case settlement process.

Clarify concepts such as “electronic media collection” and “electronic media capture”.

Adding the crime of child abuse in the group of TPCNCs of the Penal Code.

Second , those conducting the proceedings need to improve their basic knowledge of electronic data, IT (certain understanding of the object being exploited)...

Third , it is necessary to have scientific and practical summaries on the collection, evaluation and use of electronic evidence in criminal cases. On the other hand, electronic data is a non-traditional source of evidence, existing in cyberspace, the existence of which can extend beyond a country, and this type of crime that leaves a trace is also often transnational substance. Therefore, competent authorities need to strengthen international cooperation in combating this type of crime.

4.3.2. Perfecting Vietnamese law in international cooperation in the fight against high-tech crime

X stood statutes specifically identifiable as TTTP criminal law, extradition law.

- On extradition: The National Assembly soon promulgates a special law on extradition on the basis of separating the provisions on extradition in the 2007 Law on Food Information. At the same time, the State needs to continue to negotiate, sign and implement. effectively implement bilateral cooperation agreements on extradition. In addition, the competent authorities should strengthen the application of the principle of reciprocity in settling extradition cases when Vietnam has not signed a bilateral cooperation agreement on extradition with foreign countries, to avoid the violation of the law on extradition. Crime of taking advantage of "loopholes" in the law and in international cooperation to evade the punishment of the law, leading to the omission of criminals...

- Regarding criminal legal assistance: supplementing contents such as verification, settlement of information and crime denunciations; joint investigation, investigation coordination; regulations permitting the use of high-tech technical means (e-mail, fax, etc.) in sending and receiving judicial entrustment documents and performing a number of food information activities. In addition, it is necessary to consider amending and supplementing the grounds for refusal of food information in the direction of distinguishing between "forced" and "possible" refusal cases.

Building the Law on Mutual Legal Assistance in criminal matters separate from the Law on TPT 2007 is both a trend and a practical need.

- Regarding the transfer of people currently serving prison sentences, in the near future, competent agencies should soon issue a separate law on the transfer of people currently serving prison sentences on the basis of separation from The Law on Food Trafficking 2007 clearly distinguishes between humanitarian activities and highly coercive activities such as extradition and criminal proceedings under the current Law on Food Trafficking. At the same time, it is necessary to strengthen negotiations and sign international agreements on transfer of people serving prison sentences with countries and territories where many Vietnamese citizens are working, living, working and studying.

4.3.3. A group of solutions to improve the efficiency of international cooperation in the prevention of high-tech crimes

4.3.3.1. General solution

The competent authorities of Vietnam need to continue to expand their foreign relations and strengthen international cooperation in the prevention and combat of high-tech crimes on the basis of respecting independence,

sovereignty, equality, for mutual benefits, in accordance with Vietnamese law and international treaties to which Vietnam is a signatory;

The State need to mobilize the strength of the whole political system, strengthen the leadership of the Party committee, and effectively manage and administer the government, and bring into play the role of the Fatherland Front and mass organizations. levels in the prevention and control of high-risk crimes.

The State has gradually improved the capacity of law enforcement agencies and specialized forces to prevent and combat crimes using high technology. Prioritize budgetary investment, procurement and supply of materials and means in a reasonable manner for the operation of judicial agencies and specialized forces in the fight against this type of crime;

Focusing on leading and directing the review, building and perfecting of the legal system on prevention and control of drug trafficking, in which the focus should be on studying and amending and supplementing the Penal Code and the Criminal Procedure Code. , the law on measures to prevent and combat crimes using high technology and a number of other relevant laws.

Vietnam need to expand the defense space of the country, take advantage of resources, finance and take advantage of the experience of advanced countries to improve the effectiveness of the fight against crime using high technology.

4.3.3.2. Specific solutions

Firstl, promote international cooperation to prevent crimes using high technology remotely.

It is necessary to strengthen the negotiation, signing and accession to international treaties on crime prevention and control in general and on criminal justice in particular, focusing on strategic partner countries, comprehensive partners, and countries with important interests traditional systems, neighboring countries, countries with a large number of Vietnamese people living, countries with economic cooperation - investment and development with Vietnam.

Second, take advantage of human resources and learn from other countries' experiences.

Law enforcement agencies in the fight against Terrorism need to take advantage of human resources and learn from the experiences of other countries in the fight against Terrorism using high technology, experience in network management and operation. Continue to study and take advantage of funding projects on equipment and vehicles; international training courses, conferences and seminars on crime prevention and control using high technology to share information and coordinate anti-TPD using high technology effectively. Especially, it is necessary to actively and actively participate in bilateral and multilateral cooperation frameworks, international law enforcement organizations and associations such as INTERPOL, ASEANAPOL, and the United Nations Office on Drugs and Crime (UNODC)...

Third, improve the capacity of specialized forces to fight and prevent TPCNCs

The Government needs to have proposals for training, retraining (both at home and abroad) in international law, in professional techniques and in languages to respond to the change of methods, criminal tricks using high technology. It is necessary to focus on better promoting the role and strengthening the activities of the core force in the prevention of high-tech crime, which is the Vietnam Office of INTERPOL and the force for cyber security and crime prevention using high technology.

The Government needs to orient the strategy to build and develop a contingent of full-time staff at the same level of duties in the new situation, with sufficient knowledge of law, profession and information technology. The State needs to have reasonable policies to encourage, attract and select cadres with high qualifications in science and technology and the ability to fight against high-level crimes to serve in specialized agencies.

Fourth, build advanced equipment and technology in the fight and prevention of high-level crimes.

The Government should continue to issue projects on investment and procurement of equipment for specialized agencies in addition to Project 5 of the National Crime Prevention Program on "Fighting and preventing crime using high technology" was adopted.

Fifth, establish and maintain communication channels

Research and select an information exchange mechanism suitable for each country through the following forms: Hotline, office of liaison officer in charge of crime prevention, or representative of the Ministry of Public Security located in the host country...

Sixth, international cooperation in the fight against crime using high technology should have a focus.

Law enforcement agencies need to determine the location and nationality of the subjects in order to set out key and key contents in international cooperation to prevent and fight against frauds. Which note with China.

Seventh, highlighting the role of ASEANPOL and INTERPOL in international cooperation to fight against terrorism.

Vietnam, with the role of ASEAN Chair in 2020, should make efforts to discuss, discuss and propose the most feasible solutions for the police forces of ASEANAPOL member countries and partners to have close and comprehensive cooperation. Moreover, in preventing and fighting crimes in general and high-tech crimes in particular, in the spirit of responsibility, solidarity and mutual trust in order to keep the area safer.

CONCLUSION

The 4th industrial revolution is not merely an inevitable trend, but it has become an active practice which is happening in most countries around the world, as well as globally. Besides great benefits, it also brings non-trivial non-traditional security challenges for each country and region. Unlike previous revolutions, the 4.0 industrial revolution forces each individual, each country or each institution to change if they do not want to be left behind.

High-tech crime, which can also be approached under many different names such as cybercrime, computer crime, internet crime, etc. are terms that can be used interchangeably to refer to A new type of crime was formed during the development of the information technology revolution 4.0 at the end of the 20th century and is foreseen to develop very quickly in the near future. To be sure, high-tech crime is a "product" of an era that individuals, organizations, countries and the international community must accept in exchange for prosperity and development. Globally, to date, there is only one international treaty governing this type of crime, the 2001 Commission on Cybercrime Convention (Budapest Convention).

Faced with the sophistication and serious consequences of high-tech crime, cooperation to fight and prevent high-tech crime between countries has become more urgent than ever. International law is the basis for states to conduct these cooperative activities. Through cooperation contents such as the formation of international agencies and institutions in the prevention of high-tech crime; harmonization of laws; mutual criminal justice assistance; extradition; conducting investigation coordination. international law has formed a common legal mechanism at different levels, from bilateral, regional to global to connect activities between countries, from there, effectively respond to high-tech crimes, contributing to limiting and eliminating high-tech crimes from international life../.

LIST OF SCIENTIFIC RESEARCH WORKS FOR PUBLICATION OF RELATED STUDENTS GO TO THE THEME OF THE DISCUSSION

* * *

*** Scientific works that have been published in specialized journals during the PhD thesis:**

1. " *Harmonizing law in high-tech crime prevention* ", Journal of Jurisprudence, No. 8 2020.
2. " *Legal framework on cooperation mechanism to prevent cybercrime in ASEAN* ", Journal of Jurisprudence, No. 12, 2020.
3. " *Identifying high-tech crimes in international law and some experiences for Vietnam in the new situation* ", Education and Society Magazine, special issue 2020.