

BỘ NGOẠI GIAO

Số: **3018**/BNG-LPQT

V/v xin ý kiến thẩm định hồ sơ đề xuất ký
Công ước Liên hợp quốc về chống tội
phạm mạng

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày **20** tháng 5 năm 2025

Kính gửi: Bộ Tư pháp

Thực hiện ý kiến của Phó Thủ tướng Chính phủ Bùi Thanh Sơn tại Công văn số 3416/VPCP-QHQT ngày 21/4/2025 về việc Bộ Ngoại giao chủ trì, phối hợp với Bộ Công an và các cơ quan liên quan khẩn trương hoàn tất thủ tục nội bộ về việc ký Công ước Liên hợp quốc về chống tội phạm mạng (Công ước) theo quy định của Luật Điều ước quốc tế năm 2016, Bộ Ngoại giao đã hoàn thiện hồ sơ đề xuất ký Công ước trên cơ sở ý kiến góp ý của các bộ, ngành, cơ quan liên quan.

Thực hiện các thủ tục ký kết điều ước quốc tế theo quy định tại Chương II Luật Điều ước quốc tế năm 2016, Bộ Ngoại giao kính gửi quý Bộ hồ sơ đề xuất ký Công ước để thẩm định theo quy định tại khoản 2 Điều 13 Luật Điều ước quốc tế năm 2016.

Hồ sơ xin thẩm định gồm có: (1) Dự thảo Tờ trình Chính phủ về việc đề xuất ký Công ước; (2) Công ước (tiếng Việt và tiếng Anh); (3) Báo cáo đánh giá tác động chính trị, quốc phòng, an ninh, kinh tế - xã hội và các tác động khác; (4) Báo cáo đánh giá sự phù hợp giữa quy định của Công ước với quy định của pháp luật Việt Nam; (5) Báo cáo đánh giá sự tương thích của Công ước với các điều ước quốc tế trong cùng lĩnh vực mà Việt Nam là thành viên; (6) Dự kiến Kế hoạch thực hiện Công ước; (7) Văn bản ý kiến của các bộ, ngành liên quan; (8) Bảng tổng hợp, tiếp thu, giải trình ý kiến của các bộ, ngành liên quan.

Bộ Ngoại giao trân trọng cảm ơn sự hợp tác của quý Bộ.

Nơi nhận:

- Như trên;
- Lưu: HC, LPQT.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**



Ký bởi: Lê Anh
Tuấn
Cơ quan: VĂN
PHÒNG, BỘ
NGOẠI GIAO

Lê Anh Tuấn

Số: /TT-BNG-LPQT

Hà Nội, ngày tháng năm 2025

TỜ TRÌNH

**Về việc đề xuất ký Công ước của Liên hợp quốc
về chống tội phạm mạng**

Kính gửi: Chính phủ.

Căn cứ Hiến pháp 2013, Luật Điều ước quốc tế năm 2016 về đề xuất ký điều ước quốc tế, sau khi phối hợp với các Bộ: Tư pháp, Quốc phòng, Công an, Khoa học và Công nghệ (Thông tin và Truyền thông), Toà án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Bộ Ngoại giao kính báo Chính phủ về việc ký Công ước của Liên hợp quốc về chống tội phạm mạng như sau:

I. SỰ CẦN THIẾT, YÊU CẦU, MỤC ĐÍCH ĐỀ XUẤT KÝ

1. Cơ sở chính trị

- Nghị quyết số 22-NQ/TW ngày 10/4/2013 của Bộ Chính trị về hội nhập quốc tế nêu rõ nhiệm vụ “chủ động và tích cực tham gia các cơ chế đa phương, góp phần xây dựng trật tự chính trị và kinh tế công bằng, dân chủ, ngăn ngừa chiến tranh, xung đột, củng cố hoà bình, đẩy mạnh hợp tác cùng có lợi”;

- Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về “Chiến lược An ninh mạng quốc gia”, trong đó đưa ra cơ sở, khuôn khổ pháp lý để thực hiện các nhiệm vụ bảo vệ an ninh quốc gia trên không gian mạng, đấu tranh phòng, chống tấn công mạng, tội phạm mạng và ứng phó kịp thời, hiệu quả đối với những nguy cơ mới đến từ không gian mạng;

- Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia, trong đó có nhiệm vụ bảo đảm an toàn, an ninh mạng và chủ quyền quốc gia trên nền tảng số và không gian mạng; an ninh, an toàn dữ liệu hợp pháp của tổ chức, cá nhân, doanh nghiệp và chủ quyền an ninh dữ liệu quốc gia; ngăn chặn hiệu quả tội phạm lĩnh vực chuyển đổi số, chống lừa đảo trực tuyến.

- Nghị quyết số 59-NQ/TW ngày 24/01/2025 của Bộ Chính trị về hội nhập quốc tế trong tình hình mới; trong đó có nhiệm vụ chủ động, tích cực đóng góp có trách nhiệm vào các nỗ lực chung của cộng đồng quốc tế trong giữ gìn hòa bình, bảo đảm an ninh con người; chủ động tham gia các khuôn khổ hợp tác quốc tế về thông tin truyền thông, đẩy mạnh kết nối, chia sẻ và khai thác dữ liệu, bảo đảm an toàn, an ninh mạng; thúc đẩy hợp tác phát triển an ninh mạng [...] tội phạm xuyên quốc gia, tội phạm sử dụng công nghệ cao, [...] và giải quyết các thách thức an ninh phi truyền thống khác.

2. Cơ sở thực tiễn

a. Vấn đề an ninh không gian mạng ngày nay thu hút sự quan tâm của cộng đồng quốc tế do sự bùng nổ mạnh mẽ của công nghệ thông tin và truyền thông, đặc biệt trong thời đại chuyển đổi số hiện nay. Song song với sự phát triển và những lợi ích to lớn mà không gian mạng đem lại, các hoạt động gây ảnh hưởng tới an ninh mạng và tội phạm mạng cũng gia tăng một cách đáng lo ngại. Các cuộc tấn công trên không gian mạng phát triển nhanh chóng về cả hình thức và quy mô, có tính chất xuyên biên giới, gây ảnh hưởng nghiêm trọng tới sự ổn định kinh tế, chính trị, xã hội của các nước, đe dọa chủ quyền và làm xói mòn lòng tin giữa các quốc gia

Trên thế giới, các công nghệ mới cũng ngày càng được ứng dụng và phát triển nhanh chóng, không chỉ tạo ra lỗ hổng an ninh mà còn làm tăng nguy cơ tấn công với hiệu quả cao, gây khó khăn cho các cơ quan thực thi pháp luật trong việc phát hiện và ngăn chặn. Ransomware có xu hướng phát triển thành một dịch vụ thương mại hóa, cho phép các tổ chức hoặc cá nhân thuê và triển khai với mức chi phí ngày càng rẻ. Trí tuệ nhân tạo (AI), Internet vạn vật (IoT), Deepfake, tấn công giả mạo (phishing) thông minh... đang bị lợi dụng để tạo ra các cuộc tấn công với tốc độ và hiệu quả cao hơn. Tiền điện tử cũng đang được sử dụng để tài trợ cho các hoạt động tội phạm và khủng bố, rửa tiền, chuyển tiền trái phép qua biên giới. Với sự phát triển nhanh chóng của công nghệ, các lỗ hổng trong phần mềm và hệ thống ngày càng bị khai thác, đặc biệt đáng lo ngại khi phần lớn các thiết bị IoT không được thiết kế với tiêu chuẩn bảo mật cao.

b. Trong những năm qua, các nước trên thế giới, kể cả các nước vừa và nhỏ, đã tham gia tích cực vào quá trình xây dựng khuôn khổ pháp lý quốc tế trên không gian mạng nhằm xây dựng, củng cố cơ chế hợp tác quốc tế và khu vực nhằm tăng cường hiệu quả nỗ lực phòng chống tội phạm mạng. Tuy nhiên, do bản chất mới và yếu tố kỹ thuật công nghệ cao phức tạp, tính chất không biên giới, đến nay các văn kiện đang tồn tại như Công ước năm 2001 về Tội phạm mạng của Hội đồng châu Âu (còn gọi là Công ước Budapest), Công ước năm 2010 chống Tội phạm công nghệ thông tin của các nước Ả-rập và Công ước về An ninh mạng và Bảo vệ dữ liệu cá nhân của Liên minh Châu Phi đều không phản ánh được những lợi ích, quan ngại của đại đa số các nước trên thế giới, nhất là các nước đang phát triển, những nước có điều kiện chính trị, xã hội, hệ thống pháp lý và năng lực khoa học công nghệ khác nhau. Do đó, ngày 27/12/2019, Đại hội đồng Liên hợp quốc đã thông qua Nghị quyết 74/247 thành lập Ủy ban chuyên trách (Adhoc Committee – AHC) nghiên cứu khả năng xây dựng một Công ước quốc tế về chống sử dụng công nghệ thông tin và truyền thông vì mục đích tội phạm. Sau hơn 5 năm đàm phán, ngày 24/12/2024, Đại hội đồng Liên hợp quốc đã thông qua dự thảo Công ước của Liên hợp quốc về chống tội phạm mạng. Công ước đầu tiên của Liên hợp quốc và cũng là khuôn khổ pháp lý chung đầu tiên quy định về các nước hợp tác trên các lĩnh vực chia sẻ thông tin, phối hợp điều tra, thu thập chứng cứ... liên quan đến tội phạm mạng.

c. Trên cơ sở chủ trương nâng tầm đối ngoại đa phương và tích cực tham gia xây dựng khuôn khổ luật pháp quốc tế tại Liên hợp quốc, thực hiện ý kiến chỉ đạo của

Thủ tướng Chính phủ, trong năm 2022 và 2023, đoàn liên ngành¹ đã tham gia 06 phiên họp của AHC và các phiên tham vấn không chính thức với các chủ trương chung về khẳng định chủ quyền quốc gia trên không gian mạng, thúc đẩy hợp tác quốc tế về tội phạm mạng trong phạm vi tối đa, tăng cường hỗ trợ kỹ thuật và nâng cao năng lực; kết hợp với các biện pháp phòng ngừa hiệu quả. Trong quá trình tham gia, đoàn Việt Nam đã có những đóng góp thực chất, tích cực, góp phần hỗ trợ Chủ tịch và Ban Thư ký AHC xây dựng dự thảo Công ước; đóng vai trò điều phối thành công nhóm quy định thuộc chuyên đề “Các biện pháp thực thi pháp luật” tại Phiên 5. Trên cơ sở Quyết định số 44/QĐ-CTN ngày 23/01/2024 của Chủ tịch nước về việc chỉ định Đại sứ Trưởng phái đoàn Việt Nam tại Liên hợp quốc làm Trưởng đoàn đàm phán, Bộ Ngoại giao đã chủ trì, phối hợp với các bộ, ngành, cơ quan liên quan² tham gia phiên đàm phán Công ước tổ chức từ ngày 29/01-09/02/2024 và từ ngày 29/7-09/8/2024 tại Trụ sở Liên hợp quốc ở New York, Mỹ. Sau khi dự thảo Công ước được thông qua, Đoàn Việt Nam đã có phát biểu tuyên bố lập trường với một số điều khoản của văn kiện³.

Bên cạnh đó, ta đã vận động thành công để Đại hội đồng Liên hợp quốc lựa chọn Hà Nội làm địa điểm Lễ mở ký Công ước, là dấu ấn quan trọng trong đối ngoại đa phương và 47 năm quan hệ Việt Nam – Liên hợp quốc. Đây là Công ước đầu tiên của Liên hợp quốc về tội phạm mạng và là lần đầu tiên một văn kiện quốc tế được mở ký tại Việt Nam, ghi nhận Thủ đô Hà Nội trong lời văn và tên Công ước, phản ánh sự ghi nhận cao của cộng đồng quốc tế đối với những nỗ lực và cam kết của ta trong thúc đẩy hợp tác đa phương. Do đó, việc ta sớm ký và tiến tới phê chuẩn Công ước sẽ mang ý nghĩa chính trị to lớn, tiếp tục thể hiện nỗ lực và cam kết của ta trong thúc đẩy hợp tác đa phương, đề cao vai trò và giá trị của Hiến chương Liên hợp quốc và luật pháp quốc tế, tích cực đóng góp vào công việc chung của Liên hợp quốc, tham gia giải quyết các vấn đề toàn cầu, trong đó có tội phạm mạng.

d. Việt Nam là một trong những quốc gia có mức độ phổ cập Internet hàng đầu thế giới, với 79,8 triệu người sử dụng Internet tính đến đầu năm 2025, tương đương khoảng 80% dân số. Việt Nam đã và đang tích cực tham gia hợp tác quốc tế trong lĩnh vực phòng, chống tội phạm xuyên quốc gia, trong đó có tội phạm mạng. Ta đã trở thành thành viên của Công ước của Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia (UNTOC) và Công ước của Liên hợp quốc về chống tham nhũng (UNCAC); ký kết nhiều văn kiện song phương với các quốc gia để tăng cường phối hợp trong điều tra, truy tố, dẫn độ và trao đổi thông tin... liên quan đến tội phạm mạng. Tuy nhiên, với tình hình tội phạm mạng ngày càng diễn biến phức tạp cả về hình thức và quy mô, tính chất xuyên biên giới và không bị giới hạn về không gian và thời gian như nêu trên, cùng với sự ra đời của Công ước của Liên hợp quốc về chống tội phạm mạng, việc ký

¹ Do Bộ Ngoại giao chủ trì, phối hợp với Bộ Công an, Bộ Quốc phòng, Bộ Tư pháp, Bộ Thông tin và Truyền thông, Viện kiểm sát nhân dân tối cao, Tòa án nhân dân tối cao.

² Đoàn đàm phán do Bộ Ngoại giao chủ trì có sự tham gia của các Bộ: Công an, Quốc phòng, Tư pháp, Thông tin và Truyền thông; Viện kiểm sát nhân dân tối cao, Tòa án nhân dân tối cao. Tại đàm phán, Việt Nam đã đưa ra một số đề xuất về nội dung, đã được ghi nhận và phản ánh tại dự thảo Công ước, ví dụ hoạt động của các chuyên gia an ninh mạng, thủ tục hiệu lực của Công ước.

³ Bao gồm Điều 2 về quản lý tài sản ảo, Điều 6.2 về bảo vệ quyền con người và Điều 16 về hành vi phát tán ảnh nhạy cảm.

Công ước có ý nghĩa quan trọng và mở ra nhiều cơ hội và kênh hợp tác quốc tế với công tác phòng, chống tội phạm mạng tại Việt Nam, theo đó tăng cường hiệu quả hợp tác giữa cơ quan chức năng trong nước với cơ quan thực thi pháp luật nước ngoài trong phòng ngừa, điều tra, truy tố tội phạm mạng, tiếp tục thể hiện cam kết mạnh mẽ của Việt Nam trong việc góp phần bảo vệ an ninh, trật tự khu vực và toàn cầu, khẳng định vai trò là một đối tác tin cậy trong cộng đồng quốc tế.

Tại Việt Nam, sau gần 30 năm hình thành và phát triển, các ngành công nghệ thông tin và truyền thông đã phát triển gấp 300 lần. Sáu tháng đầu năm 2024 ghi nhận doanh thu của toàn ngành công nghệ thông tin và truyền thông tăng mạnh so với cùng kỳ, đạt hơn 2 triệu tỷ đồng, trong đó, lĩnh vực công nghiệp công nghệ thông tin và truyền thông có đóng góp lớn với doanh thu ước đạt 1.858.371 tỷ đồng, tăng 27% so với 6 tháng đầu năm 2023, góp phần đáng kể vào phát triển đất nước. Tuy vậy, không gian mạng cũng ẩn chứa nhiều nguy cơ, thách thức đối với sự bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng.

Từ đầu năm 2020 đến nay, hệ thống thông tin mạng của các cơ quan, tổ chức, doanh nghiệp tiếp tục là mục tiêu của hoạt động tấn công mạng, gián điệp mạng, chiếm đoạt thông tin, tài liệu, bí mật; hoạt động của tội phạm sử dụng công nghệ cao, bao gồm lừa đảo chiếm đoạt tài sản, ngày càng diễn biến phức tạp với nhiều phương thức, thủ đoạn gây thiệt hại rất lớn cho các tổ chức, doanh nghiệp và người dân. Số lượng các cuộc tấn công mạng tại Việt Nam trong năm 2024 đã tăng hơn 60% so với năm 2023, đặc biệt là tấn công mã hóa dữ liệu với mục đích tống tiền các doanh nghiệp (ransomware attack); số lượng mã độc mới được phát triển tăng hơn 52%, các nhóm tin tặc với mục đích tài chính có nhiều kỹ thuật và thủ đoạn mới, các chiến dịch cũng có sự đầu tư hơn. Các lỗ hổng mới năm 2024 gia tăng 64,33% so với cùng kỳ năm 2023, đặc biệt là số lượng các lỗ hổng có mức độ nghiêm trọng cao cũng tăng cao. Các ngành như y tế, tài chính, ngân hàng, năng lượng và hàng không đã trở thành mục tiêu chính. Các chiến dịch lừa đảo trực tuyến cũng ngày càng phức tạp, được vận hành bởi các tổ chức lừa đảo có tổ chức xuyên quốc gia; tuy nhiên, chỉ có khoảng 20% nạn nhân của các vụ lừa đảo trình báo sự việc với cơ quan chức năng. Không ít hành vi tấn công mạng, lừa đảo chiếm đoạt tài sản thông qua không gian mạng được tiến hành từ các đối tượng ở nước ngoài, lợi dụng cơ sở hạ tầng tại nước ngoài.

II. NỘI DUNG CHÍNH CỦA CÔNG ƯỚC

1. Tại Nghị quyết ngày 24/12/2024 của Đại hội đồng Liên hợp quốc, cũng như theo báo cáo của Ủy ban 3 Đại hội đồng Liên hợp quốc, việc ký kết và gia nhập Công ước là thể hiện sự đồng thuận cả gói đối với (i) Công ước và (ii) Tài liệu giải thích nhằm làm rõ phạm vi thẩm quyền của các nước liên quan đến lĩnh vực áp dụng một số quy định.

2. Công ước gồm 9 Chương, 68 điều khoản, cụ thể như sau:

- Chương I - Các điều khoản chung (Điều 01 – Điều 05) quy định về mục tiêu và phạm vi áp dụng của Công ước; các thuật ngữ cơ bản sử dụng trong Công ước; các nguyên tắc về bảo vệ chủ quyền và tôn trọng quyền con người.

- Chương II - Hình sự hóa hành vi phạm tội (Điều 06 - Điều 21) quy định về các hành vi phạm tội mà Công ước điều chỉnh (bao gồm các hành vi tội phạm truyền thống được thực hiện thông qua hệ thống công nghệ thông tin truyền thông và hành vi phạm tội trên không gian mạng); thời hiệu; nghĩa vụ về truy tố, xét xử và xử phạt.

- Chương III - Thẩm quyền (Điều 22) quy định về nghĩa vụ trong thiết lập thẩm quyền xử lý, điều tra và xét xử hành vi phạm tội mạng.

- Chương IV - Các biện pháp tố tụng và thực thi pháp luật (Điều 23 - Điều 34) quy định về phạm vi và các biện pháp tố tụng hình sự, thực thi pháp luật mà nhà chức trách các nước cần thực hiện hoặc yêu cầu các cá nhân, tổ chức liên quan thực hiện, bao gồm lưu trữ và công bố dữ liệu; thu thập dữ liệu kết nối; chặn thu dữ liệu nội dung; đóng băng, thu giữ và tịch thu tài sản do phạm tội mà có; lập án tích; bảo vệ nhân chứng; hỗ trợ và bảo vệ nạn nhân; ngoài ra quy định về các điều kiện và biện pháp bảo vệ quyền con người khi thực thi công vụ.

- Chương V - Hợp tác quốc tế (Điều 35 - Điều 52) quy định về các nguyên tắc, hình thức, biện pháp hợp tác quốc tế phòng chống tội phạm, bao gồm các hoạt động về: bảo vệ dữ liệu cá nhân; dẫn độ; chuyển giao người bị kết án tù; chuyển giao thủ tục tố tụng; hợp tác thông qua mạng lưới cơ quan thực thi pháp luật 24/7; hợp tác trong lưu trữ dữ liệu; tương trợ tư pháp trong tiếp cận, thu thập, chặn thu dữ liệu; điều tra chung; cơ chế thu hồi tài sản; hợp tác trong tịch thu tài sản; hợp tác trong trả lại tài sản do phạm tội mà có.

- Chương VI - Các biện pháp phòng ngừa (Điều 53) quy định về các biện pháp phòng ngừa tội phạm, thông qua các hình thức như hợp tác giữa cơ quan thực thi pháp luật, tăng cường nhận thức người dân, tăng cường năng lực của hệ thống tư pháp hình sự, tăng cường phối hợp giữa các khu vực công và tư...

- Chương VII - Hỗ trợ kỹ thuật và trao đổi thông tin (Điều 54 - Điều 56) quy định về nguyên tắc và các hình thức hỗ trợ kỹ thuật, chia sẻ thông tin, nhằm nâng cao năng lực của cơ quan thực thi pháp luật, cải thiện hiệu quả hoạt động phòng chống tội phạm. Các hình thức hỗ trợ kỹ thuật bao gồm: đào tạo phương pháp và kỹ thuật điều tra, truy tố, xét xử, hoạch định chính sách phòng chống tội phạm; xây dựng năng lực thu thập, lưu trữ, chia sẻ dữ liệu; hỗ trợ trang thiết bị thực thi pháp luật; đào tạo về tương trợ tư pháp; đào tạo và hỗ trợ trang thiết bị trong ngăn chặn, phát hiện, giám sát sự dịch chuyển của tài sản do phạm tội mà có; đào tạo phương pháp bảo vệ nạn nhân và nhân chứng; đào tạo ngôn ngữ; các hình thức hỗ trợ tài chính, hỗ trợ kỹ thuật, đào tạo khác; các hoạt động về chia sẻ thông tin, kinh nghiệm, thực tiễn tốt trong phòng, chống tội phạm mạng.

- Chương VIII - Cơ chế thực thi Công ước (Điều 57 - Điều 58) quy định về chức năng, nhiệm vụ, quyền hạn của Hội nghị quốc gia thành viên Công ước, bao gồm tổ chức đánh giá định kỳ việc thực thi Công ước của các quốc gia thành viên; vai trò của Ban thư ký.

- Chương IX - Các điều khoản cuối cùng (Điều 59 - Điều 68) quy định về trình tự, thủ tục, điều kiện hiệu lực, việc sửa đổi bổ sung, gia nhập và rút khỏi Công ước.

Ngoài ra, Tài liệu giải thích (Interpretative Note) cũng làm rõ phạm vi thẩm quyền của các nước liên quan đến lĩnh vực áp dụng một số quy định của Công ước. Theo đó, việc giải thích các định nghĩa trong Điều 2 của Công ước phụ thuộc vào các quy định của luật pháp quốc gia các nước thành viên, miễn là các quy định pháp luật này đủ để bao quát các định nghĩa một cách phù hợp với nguyên tắc và mục tiêu của Công ước.

3. Về cơ bản, với các chương và điều khoản như trên, nội dung chính của Công ước gồm một số điểm như sau:

Thứ nhất, khẳng định chủ quyền quốc gia trên không gian mạng và trách nhiệm thực hiện hợp tác quốc tế trong phòng, chống tội phạm mạng (như tương trợ tư pháp, điều tra chung, thu hồi tài sản...) gắn với yêu cầu bảo đảm không cản trở các quyền con người cơ bản trên không gian mạng, phù hợp với các cam kết quốc tế của quốc gia về quyền con người.

Thứ hai, quy định thống nhất các thuật ngữ chuyên ngành cơ bản của tội phạm mạng với cập nhật về tiền ảo; chuẩn hóa 06 tội danh về tội phạm công nghệ cao và 03 tội danh về lạm dụng trẻ em và ảnh cá nhân; chuẩn hóa 05 biện pháp nghiệp vụ điều tra liên quan đến tiếp cận dữ liệu (bao gồm cả dữ liệu được lưu trữ và dữ liệu trực tuyến). Các thuật ngữ, tội danh và biện pháp này được xây dựng trên cơ sở tham khảo Công ước Budapest và các công ước khu vực khác về tội phạm công nghệ cao nhằm bảo đảm liên thông giữa các văn kiện pháp lý quốc tế này.

Thứ ba, xây dựng mạng lưới liên hệ 24/7 của tất cả các Quốc gia thành viên với các chức năng phù hợp với đấu tranh tội phạm mạng như "phong tỏa" các dữ liệu điện tử trong nước theo yêu cầu, hỗ trợ xử lý các trường hợp khẩn cấp, thu thập các chứng cứ điện tử...

Thứ tư, thúc đẩy các biện pháp phòng ngừa tội phạm mạng thông qua yêu cầu các doanh nghiệp đảm bảo an ninh, an toàn của sản phẩm để bảo vệ người dùng; bảo vệ trẻ em trên không gian mạng; nâng cao nhận thức của cộng đồng về nguy cơ tội phạm mạng...

Thứ năm, thống nhất về hỗ trợ kỹ thuật và nâng cao năng lực thông qua Cơ quan Phòng chống Ma túy và Tội phạm của Liên hợp quốc (UNODC) với các hoạt động như hoàn thiện khuôn khổ pháp lý về không gian mạng; năng lực về lưu trữ và quản lý chứng cứ số; cung cấp và đào tạo các trang thiết bị hiện đại...

Thứ sáu, Công ước chỉ có hiệu lực sau khi có 40 nước tham gia và việc thông qua Nghị định thư bổ sung chỉ được thực hiện sau khi có hơn 60 nước đã tham gia Công ước.

III. TÊN GỌI, HÌNH THỨC, DANH NGHĨA KÝ, NGƯỜI ĐẠI DIỆN KÝ, NGÔN NGỮ, HIỆU LỰC, HÌNH THỨC HIỆU LỰC VÀ ÁP DỤNG TẠM THỜI CÔNG ƯỚC

1. Tên gọi: Công ước của Liên hợp quốc về chống tội phạm mạng.
2. Hình thức: Điều ước quốc tế nhiều bên.
3. Danh nghĩa ký: Điều ước quốc tế nhân danh Nhà nước.
4. Người đại diện ký: Đại diện Lãnh đạo Bộ Công an.

5. Ngôn ngữ: Sáu thứ tiếng chính thức của Liên hợp quốc (Ả-rập, Anh, Pháp, Nga, Tây Ban Nha và Trung).

6. Hiệu lực, hình thức hiệu lực: Công ước sẽ có hiệu lực sau 90 ngày kể từ ngày văn kiện phê chuẩn, phê duyệt, chấp thuận hoặc gia nhập thứ 40 được nộp lưu chiểu.

7. Áp dụng tạm thời Công ước: Không kiến nghị áp dụng tạm thời.

8. Thời điểm ký Công ước: Kiến nghị ký Công ước vào ngày mở ký tại Hà Nội, Việt Nam.

IV. QUYỀN VÀ NGHĨA VỤ PHÁT SINH TỪ CÔNG ƯỚC ĐỐI VỚI NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

1. Quyền phát sinh từ Công ước đối với Việt Nam

Về cơ bản, sau khi Công ước có hiệu lực đối với Việt Nam, ta có các quyền sau:

- Yêu cầu các quốc gia thành viên Công ước cung cấp thông tin, chứng cứ bao gồm chứng cứ điện tử, thực hiện hợp tác quốc tế, tương trợ tư pháp trong các vụ việc liên quan tới các hành vi phạm tội được điều chỉnh theo Công ước.

- Quyền tham gia vào các hoạt động hỗ trợ kỹ thuật, xây dựng năng lực, chuyển giao công nghệ triển khai trong khuôn khổ Công ước, được hỗ trợ nguồn lực để phát triển năng lực khoa học, công nghệ thông tin và truyền thông.

- Ngoài ra, nếu trở thành một trong những thành viên đầu tiên của Công ước, tham gia các phiên họp đầu tiên của Hội nghị quốc gia thành viên, Việt Nam sẽ có quyền đàm phán, biểu quyết về các nội dung quan trọng, định hình cơ chế hoạt động thực chất của Công ước như: các mức đóng góp tài chính cụ thể của các quốc gia thành viên, cơ chế hoạt động của các cơ quan do Hiệp định lập ra, cơ chế đánh giá việc thực thi Công ước, đàm phán và thông qua Nghị định thư bổ sung cho Công ước. Ta không thể tác động vào quá trình xây dựng các cơ chế, quy định cụ thể đó nếu chưa phải là thành viên Hiệp định.

2. Nghĩa vụ phát sinh từ Công ước đối với Việt Nam

Về cơ bản, sau khi Công ước có hiệu lực đối với Việt Nam, ta có các nghĩa vụ sau đây:

- Đảm bảo các hành vi phạm tội được quy định trong Công ước cũng là hành vi phạm tội theo pháp luật có liên quan của Việt Nam; đảm bảo các cơ quan thực thi pháp luật, cơ quan tổ tụng trong nước có thẩm quyền thực thi các biện pháp nghiệp vụ được quy định trong Công ước phục vụ hoạt động phòng ngừa, điều tra, truy tố, xét xử tội phạm.

- Thực hiện chia sẻ thông tin, bằng chứng điện tử, hợp tác quốc tế, tương trợ tư pháp khi có yêu cầu trong các vụ việc liên quan tới các hành vi phạm tội được điều chỉnh theo Công ước; chi định đầu mối, cung cấp nguồn lực, cơ sở vật chất, nhân sự để tham gia vận hành Mạng lưới 24/7 theo quy định tại Điều 41 của Công ước.

- Nộp niên liễm trên cơ sở thang đóng góp tài chính tương tự mô hình Liên hợp quốc nhằm đảm bảo hoạt động của Ban Thư ký và các cơ chế được thành lập theo Công ước.

V. TUÂN THỦ NGUYÊN TẮC KÝ KẾT ĐIỀU ƯỚC QUỐC TẾ

Việc ký Công ước này tuân thủ các nguyên tắc nêu tại Điều 3 Luật Điều ước quốc tế năm 2016, cụ thể là: (i) không trái với Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam; (ii) tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ quốc gia, không sử dụng hoặc đe dọa sử dụng vũ lực; không can thiệp vào công việc nội bộ, bình đẳng, cùng có lợi và những nguyên tắc cơ bản khác của luật pháp quốc tế; (iii) bảo đảm lợi ích quốc gia, dân tộc, phù hợp với đường lối đối ngoại của Việt Nam; (iv) tuân thủ điều ước quốc tế mà Việt Nam là thành viên.

VI. KIẾN NGHỊ BẢO LƯU, CHẤP NHẬN HOẶC PHẢN ĐỐI BẢO LƯU

Công ước không có quy định về việc cấm bảo lưu, do đó các quốc gia thành viên được phép đưa ra tuyên bố bảo lưu. Tuy nhiên, để thể hiện vai trò là nước chủ nhà đăng cai Lễ ký Công ước, Bộ Ngoại giao kiến nghị Việt Nam không đưa ra tuyên bố bảo lưu ở giai đoạn đề xuất ký mà sẽ cân nhắc đưa ra tuyên bố bảo lưu, nếu cần thiết, ở giai đoạn phê chuẩn.

VII. ÁP DỤNG TRỰC TIẾP HOẶC SỬA ĐỔI, BỔ SUNG, BÃI BỎ, BAN HÀNH VĂN BẢN QUY PHẠM PHÁP LUẬT ĐỂ THỰC HIỆN CÔNG ƯỚC

Bộ Ngoại giao kiến nghị không áp dụng trực tiếp toàn bộ quy định của Công ước; việc thực hiện các quy định của Công ước sẽ theo nguyên tắc Hiến pháp và pháp luật có liên quan của Việt Nam, trên cơ sở các thoả thuận hợp tác song phương hoặc đa phương với các quốc gia khác và nguyên tắc có đi có lại.

VIII. Ý KIẾN CỦA CÁC BỘ, NGÀNH LIÊN QUAN

1. Các cơ quan được lấy ý kiến gồm các Bộ: Tư pháp, Quốc phòng, Công an, Thông tin và Truyền thông; Toà án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao.

Theo đó, các bộ, ngành liên quan cơ bản ủng hộ chủ trương ký Công ước và có các ý kiến đóng góp để hoàn thiện hồ sơ đề xuất ký. Bộ Ngoại giao xin giải trình một số ý kiến như sau:

(i) Về vấn đề “tài sản số” tại khoản 1 Điều 2 Công ước quy định: “Tài sản là mọi loại của cải, vật chất hay phi vật chất, động sản hay bất động sản, hữu hình hay vô hình, bao gồm tài sản số, và các văn bản pháp lý hay giấy tờ chứng minh quyền sở hữu hoặc lợi ích đối với tài sản đó”. Theo đó, có ý kiến cho rằng chưa có văn bản quy phạm pháp luật nào của Việt Nam có quy định định nghĩa cụ thể về “tài sản số”; phạm vi định nghĩa “tài sản” theo Công ước đang rộng hơn so với quy định của Bộ Luật Dân sự năm 2015.

Về vấn đề này, Bộ Ngoại giao xin giải trình như sau: Trên cơ sở tham khảo ý kiến của đơn vị chuyên môn về BLDS của Bộ Tư pháp, Bộ Ngoại giao nhận thấy: căn cứ vào đặc trưng của tài sản số, tài sản ảo (digital asset, virtual asset)⁴, có thể thấy, tuy trường hợp, đây có thể là vật⁵ (vô hình) hoặc giấy tờ có giá (như chứng khoán) hoặc quyền tài sản, trị giá được bằng tiền và có thể chuyển giao được trong giao dịch dân sự

⁴ Một số thuật ngữ khác hiện nay đang được dùng không chính thức là tiền ảo, tiền kỹ thuật số.

⁵ BLDS năm 2015 không yêu cầu “vật” phải là “vật có thực” để ghi nhận về tài sản vô hình, tài sản hình thành trong tương lai (BLDS năm 1995 trước đây yêu cầu vật phải là “vật có thực”).

theo quy định “*tài sản*” của BIDS năm 2015 (phụ thuộc vào bản chất của token được phát hành theo Sách Trắng/White paper của nhà phát hành).

Bên cạnh đó, theo Chương trình Kỳ họp thứ 9, Quốc hội khoá XV, dự án Luật Công nghiệp công nghệ số sẽ được Quốc hội thảo luận và xem xét thông qua, trong đó có quy định về khái niệm tài sản số, tài sản ảo trong môi trường điện tử và tài sản mã hoá.

(ii) Về trách nhiệm pháp lý của pháp nhân, khoản 1 Điều 18 của Công ước: Có ý kiến cho rằng trong số các hành vi quy định từ Điều 7 đến Điều 17 của Công ước, hiện Bộ Luật Hình sự năm 2015, sửa đổi bổ sung năm 2017 chỉ mới quy định trách nhiệm hình sự của pháp nhân thương mại đối với hành vi rửa tiền do phạm tội mà có được quy định tại Điều 17 của Công ước và chưa có quy định đối với các hành vi khác được nêu tại Công ước; đề nghị cần nhắc thêm về Điều 18 của Công ước về trách nhiệm pháp lý của pháp nhân do Điều này tương ứng với Điều 26 trong UNCAC.

Về vấn đề này, Bộ Ngoại giao xin giải trình như sau:

- Theo khoản 2 Điều 18 của Công ước, “trách nhiệm pháp lý của pháp nhân” được quy định tùy theo nguyên tắc pháp luật của mỗi nước, trong đó có thể bao gồm trách nhiệm hình sự, dân sự hoặc hành chính. Vì vậy, ngoài Bộ Luật Hình sự, trách nhiệm pháp lý của pháp nhân có thể được thực hiện theo các quy định của Bộ Luật Dân sự, các quy định xử phạt hành chính, xử lý kỷ luật... theo các luật có liên quan như Luật An toàn thông tin mạng năm 2015, Luật Công nghệ thông tin năm 2006...

- Liên quan đến việc Điều 18 của Công ước về trách nhiệm pháp lý của pháp nhân tương ứng với Điều 26 trong UNCAC mà Việt Nam đã báo lưu việc áp dụng: Bộ Ngoại giao cũng cho rằng, theo pháp luật và tập quán quốc tế, các quy định mang tính tùy nghi như điều khoản này không cần thiết phải báo lưu do các quốc gia có thể lựa chọn quy định trách nhiệm hình sự, dân sự hoặc hành chính, tùy theo nguyên tắc pháp luật của mình.

(iii) Về cơ chế tịch thu tài sản thông qua hợp tác quốc tế tịch thu tài sản, điểm c khoản 1 Điều 49 Công ước yêu cầu các quốc gia thành viên xem xét áp dụng biện pháp cần thiết để cho phép tịch thu tài sản không cần kết án hình sự trong cả 03 trường hợp không thể truy tố người phạm tội, đó là: (1) người phạm tội tử vong; (2) người phạm tội bỏ trốn; (3) người phạm tội vắng mặt. Có ý kiến cho rằng hiện nay pháp luật Việt Nam chưa quy định về cơ chế tịch thu tài sản không qua kết án. Riêng đối với trường hợp không thể truy tố người phạm tội vì lý do bỏ trốn hoặc vắng mặt thì pháp luật Việt Nam chưa quy định tịch thu tài sản trong trường hợp này.

Về vấn đề này, Bộ Ngoại giao xin giải trình như sau: Toàn bộ Điều 49 của Công ước tương tự với Điều 54 của UNCAC mà Việt Nam đã là thành viên (ta không báo lưu, đưa ra tuyên bố với điều khoản này của UNCAC). Đồng thời, đối với trường hợp tịch thu tài sản mà chưa có bản án hình sự nếu người phạm tội đã chết, bỏ trốn hoặc vắng mặt, điều này là phù hợp với xu hướng phát triển của hợp tác quốc tế về pháp luật; đồng thời, đây cũng là quy định mang tính tùy nghi, theo đó các quốc gia thành viên không bắt buộc phải thực hiện theo Công ước này mà có thể “xem xét” việc áp dụng.

2. Bộ Ngoại giao xin giải trình, tiếp thu ý kiến cụ thể khác của các bộ, ngành liên quan tại Bảng tiếp thu, giải trình ý kiến gửi kèm theo Tờ trình này.

IX. KIẾN NGHỊ

Trên cơ sở quyết định về việc đàm phán Công ước, Bộ Ngoại giao nhận thấy việc quyết định ký Công ước Liên hợp quốc về chống tội phạm mạng thuộc thẩm quyền của Chủ tịch nước. Bộ Ngoại giao kính đề xuất Chính phủ trình Chủ tịch nước:

- Cho phép ký Công ước của Liên hợp quốc về chống tội phạm mạng; ủy quyền cho Chính phủ tổ chức ký Công ước;

- Ủy quyền cho Bộ trưởng Bộ Công an ký Công ước nêu trên;

- Giao Bộ Ngoại giao làm các thủ tục đối ngoại theo quy định;

- Giao Bộ Công an thực hiện các thủ tục trình Chủ tịch nước phê chuẩn Công ước.

Bộ Ngoại giao kính trình Chính phủ xem xét, quyết định./

Nơi nhận:

- Chính phủ;
- Thủ tướng Chính phủ Phạm Minh Chính (để b/c);
- Phó Thủ tướng Bùi Thanh Sơn;
- Văn phòng Chính phủ;
- Các Bộ: TP; QP; CA; KHCN;
- TANDTC, VKSNDTC;
- Bộ trưởng Ngoại giao (để b/c);
- Các đ/c Thứ trưởng;
- Lưu: HC, LPQT.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**



General Assembly

Disstr.: General
31 December 2024

Seventy-ninth session

Agenda item 108

Countering the use of information and communications
technologies for criminal purposes**Resolution adopted by the General Assembly
on 24 December 2024***[on the report of the Third Committee (A/79/460, para. 15)]***79/243. United Nations Convention against Cybercrime;****Strengthening International Cooperation for Combating Certain
Crimes Committed by Means of Information and Communications
Technology Systems and for the Sharing of Evidence in Electronic
Form of Serious Crimes***The General Assembly,*

Recalling its resolution 74/247 of 27 December 2019, in which it established an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime,

Recalling also its resolution 75/282 of 26 May 2021, in which it decided that the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes would carry out its work in New York and Vienna, commencing in January 2022, in order to provide a draft convention to the General Assembly at its seventy-eighth session,

Strongly convinced of the urgent need to strengthen international cooperation to prevent and combat cybercrime, in view of its negative economic and social implications and its ability to undermine sustainable development and the rule of law,

Strongly convinced also that the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes



Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes will constitute an effective tool and the necessary legal framework for international cooperation in preventing and combating cybercrime and in ensuring the timely and lawful collection and sharing of evidence in electronic form of a broad range of crimes that may be committed through the use of information and communications technology systems, including money-laundering, corruption, acts of terrorism, trafficking in persons, the smuggling of migrants, the illicit manufacturing of and trafficking in firearms, their parts, components and ammunition, illicit drug trafficking and illicit trafficking in cultural property,

Expressing its appreciation to the Government of Viet Nam for the offer to host a signing ceremony for the Convention,

1. *Takes note of the report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its reconvened concluding session, in which the Ad Hoc Committee submitted the final text of the draft United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes to the General Assembly for its consideration and action, and commends the Ad Hoc Committee for its work;*

2. *Adopts the United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes annexed to the present resolution, and opens it for signature in Hanoi in 2025 and thereafter at United Nations Headquarters in New York until 31 December 2026;*

3. *Urges all States and competent regional economic integration organizations to sign and ratify the Convention as soon as possible in order to ensure its rapid entry into force;*

4. *Decides that, until the Conference of the States Parties to be established pursuant to the Convention decides otherwise, the account referred to in article 56 of the Convention will be operated by the United Nations Office on Drugs and Crime, and encourages Member States to begin making adequate voluntary contributions to the above-mentioned account for the provision to developing countries and countries with economies in transition of the technical assistance that they might require to prepare for ratification and implementation of the Convention;*

5. *Also decides that the Ad Hoc Committee shall continue its work, mutatis mutandis, in accordance with General Assembly resolutions 74/247 and 75/282, with a view to negotiating a draft protocol supplementary to the Convention, addressing, inter alia, additional criminal offences as appropriate, and that, for that purpose, two sessions of a duration of 10 days each, with the first session taking place two years after the adoption of the Convention by the General Assembly and the second session in the following calendar year, in Vienna and New York, respectively, shall be convened for the purpose of submitting the outcomes to the Conference of the States Parties to the Convention, for its consideration and further action, in accordance with articles 57, paragraph 5 (g), 61 and 62 of the Convention;*

6. *Further decides that the Ad Hoc Committee will complete its tasks arising from the negotiation of the Convention by holding a session, mutatis mutandis, in accordance with General Assembly resolutions 74/247 and 75/282, of a duration of up to five days in Vienna, one year after the adoption of the Convention, in order to prepare the draft text of the rules of procedure of the Conference of the States Parties*

to the Convention and of other rules described in article 57 of the Convention, which will be submitted to the Conference for consideration at its first session;

7. *Urges Member States to provide voluntary contributions to the United Nations Office on Drugs and Crime to ensure funding to enable the participation of representatives of developing countries, especially those that do not have resident representation in Vienna, in the work of the Ad Hoc Committee, including by covering their travel costs and accommodation expenses;*

8. *Requests the Conference of the States Parties to the Convention to keep abreast of technological developments in the area of cybercrime, to make recommendations regarding appropriate action in that regard, to promote regional and international meetings of national cybercrime focal points for the exchange of experiences, challenges and good practices, and to ensure synergies with relevant work carried out by other competent intergovernmental bodies;*

9. *Requests the Secretary-General to designate the United Nations Office on Drugs and Crime to serve as the secretariat for and under the direction of the Conference of the States Parties to the Convention, in accordance with article 58 of the Convention;*

10. *Also requests the Secretary-General to provide the United Nations Office on Drugs and Crime with the resources necessary to enable it to promote in an effective manner the rapid entry into force of the Convention and to discharge the functions of secretariat of the Conference of the States Parties to the Convention, and to support the Ad Hoc Committee in its work pursuant to paragraphs 5 and 6 above;*

11. *Further requests the Secretary-General to prepare a report on the activities undertaken to promote the rapid entry into force of the Convention for submission to the General Assembly at its eightieth session;*

12. *Decides that, in order to raise awareness of cybercrime and of the role of the Convention in combating and preventing it, 24 December should be designated International Anti-Cybercrime Day.*

*55th (resumed) plenary meeting
24 December 2024*

Annex

United Nations Convention against Cybercrime:

Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

Preamble

The States Parties to the present Convention,

Bearing in mind the purposes and principles of the Charter of the United Nations,

Noting that information and communications technologies, while having enormous potential for the development of societies, create new opportunities for perpetrators, may contribute to the increase in the rate and diversity of criminal activities, and may have an adverse impact on States, enterprises and the well-being of individuals and society as a whole,

Concerned that the use of information and communications technology systems can have a considerable impact on the scale, speed and scope of criminal offences, including offences related to terrorism and transnational organized crime, such as

trafficking in persons, the smuggling of migrants, the illicit manufacturing of and trafficking in firearms, their parts, components and ammunition, drug trafficking and trafficking in cultural property,

Convinced of the need to pursue, as a matter of priority, a global criminal justice policy aimed at the protection of society against cybercrime by, inter alia, adopting appropriate legislation, establishing common offences and procedural powers and fostering international cooperation to prevent and combat such activities more effectively at the national, regional and international levels,

Determined to deny safe havens to those who engage in cybercrime by prosecuting these crimes wherever they occur,

Stressing the need to enhance coordination and cooperation among States by, inter alia, providing technical assistance and capacity-building, including the transfer of technology on mutually agreed terms, to countries, in particular developing countries, upon their request, to improve national legislation and frameworks and enhance the capacity of national authorities to deal with cybercrime in all its forms, including its prevention, detection, investigation and prosecution, and emphasizing in this context the role that the United Nations plays,

Recognizing the increasing number of victims of cybercrime, the importance of obtaining justice for those victims and the necessity to address the needs of persons in vulnerable situations in measures taken to prevent and combat the offences covered by this Convention,

Determined to prevent, detect and suppress more effectively international transfers of property obtained as a result of cybercrime and to strengthen international cooperation in the recovery and return of proceeds of the crimes established in accordance with this Convention,

Bearing in mind that preventing and combating cybercrime is a responsibility of all States and that they must cooperate with one another, with the support and involvement of relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and private sector entities, if their efforts in this area are to be effective,

Recognizing the importance of mainstreaming a gender perspective in all relevant efforts to prevent and combat the offences covered by this Convention, in accordance with domestic law,

Mindful of the need to achieve law enforcement objectives and to ensure respect for human rights and fundamental freedoms as enshrined in applicable international and regional instruments,

Acknowledging the right to protection against arbitrary or unlawful interference with one's privacy, and the importance of protecting personal data,

Commending the work of the United Nations Office on Drugs and Crime and other international and regional organizations in preventing and combating cybercrime,

Recalling General Assembly resolutions 74/247 of 27 December 2019 and 75/282 of 26 May 2021,

Taking into account the existing international and regional conventions and treaties on cooperation in criminal matters, as well as similar treaties that exist between Member States of the United Nations,

Have agreed as follows:

Chapter I

General provisions

Article 1

Statement of purpose

The purposes of this Convention are to:

- (a) Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively;
- (b) Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and
- (c) Promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries

Article 2

Use of terms

For the purposes of this Convention:

- (a) "Information and communications technology system" shall mean any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data;
- (b) "Electronic data" shall mean any representation of facts, information or concepts in a form suitable for processing in an information and communications technology system, including a program suitable to cause an information and communications technology system to perform a function;
- (c) "Traffic data" shall mean any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service;
- (d) "Content data" shall mean any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings;
- (e) "Service provider" shall mean any public or private entity that:
 - (i) Provides to users of its service the ability to communicate by means of an information and communications technology system; or
 - (ii) Processes or stores electronic data on behalf of such a communications service or users of such a service;
- (f) "Subscriber information" shall mean any information that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
 - (i) The type of communications service used, the technical provisions related thereto and the period of service;
 - (ii) The subscriber's identity, postal or geographical address, telephone or other access number, billing or payment information, available on the basis of the service agreement or arrangement;

- (ii) Any other information on the site of the installation of communications equipment, available on the basis of the service agreement or arrangement;
- (g) "Personal data" shall mean any information relating to an identified or identifiable natural person;
- (h) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;
- (i) "Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including virtual assets, and legal documents or instruments evidencing title to, or interest in, such assets;
- (j) "Proceeds of crime" shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;
- (k) "Freezing" or "seizure" shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;
- (l) "Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;
- (m) "Predicate offence" shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 17 of this Convention;
- (n) "Regional economic integration organization" shall mean an organization constituted by sovereign States of a given region to which its member States have transferred competence in respect of matters governed by this Convention and which has been duly authorized, in accordance with its internal procedures, to sign, ratify, accept, approve or accede to it, references to "States Parties" under this Convention shall apply to such organizations within the limits of their competence;
- (o) "Emergency" shall mean a situation in which there is a significant and imminent risk to the life or safety of any natural person.

Article 3

Scope of application

This Convention shall apply, except as otherwise stated herein, to:

- (a) The prevention, investigation and prosecution of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;
- (b) The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, as provided for in articles 23 and 35 of this Convention.

Article 4

Offences established in accordance with other United Nations conventions and protocols

1. In giving effect to other applicable United Nations conventions and protocols to which they are Parties, States Parties shall ensure that criminal offences established in accordance with such conventions and protocols are also considered criminal offences under domestic law when committed through the use of information and communications technology systems.

2. Nothing in this article shall be interpreted as establishing criminal offences in accordance with this Convention.

Article 5

Protection of sovereignty

1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.
2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

Article 6

Respect for human rights

1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.
2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.

Chapter II

Criminalization

Article 7

Illegal access

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally, the access to the whole or any part of an information and communications technology system without right.
2. A State Party may require that the offence be committed by infringing security measures, with the intent of obtaining electronic data or other dishonest or criminal intent or in relation to an information and communications technology system that is connected to another information and communications technology system.

Article 8

Illegal interception

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the interception, made by technical means, of non-public transmissions of electronic data to, from or within an information and communications technology system, including electromagnetic emissions from an information and communications technology system carrying such electronic data.
2. A State Party may require that the offence be committed with dishonest or criminal intent, or in relation to an information and communications technology system that is connected to another information and communications technology system.

Article 9

Interference with electronic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the damaging, deletion, deterioration, alteration or suppression of electronic data.
2. A State Party may require that the conduct described in paragraph 1 of this article result in serious harm.

Article 10

Interference with an information and communications technology system

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the serious hindering of the functioning of an information and communications technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data.

Article 11

Abuse of devices

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(a) The obtaining, production, sale, procurement for use, import, distribution or otherwise making available of:

- (i) A device, including a program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; or
- (ii) A password, access credentials, electronic signature or similar data by which the whole or any part of an information and communications technology system is capable of being accessed;

with the intent that the device, including a program, or the password, access credentials, electronic signature or similar data be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; and

(b) The possession of an item referred to in paragraph 1 (a) (i) or (ii) of this article, with intent that it be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention.

2. This article shall not be interpreted as imposing criminal liability where the obtaining, production, sale, procurement for use, import, distribution or otherwise making available, or the possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles 7 to 10 of this Convention, such as for the authorized testing or protection of an information and communications technology system.

3. Each State Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (i) of this article.

Article 12

Information and communications technology system-related forgery

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of electronic data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible.

2. A State Party may require an intent to defraud, or a similar dishonest or criminal intent, before criminal liability attaches.

Article 13

Information and communications technology system-related theft or fraud

Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by means of:

(a) Any input, alteration, deletion or suppression of electronic data;

(b) Any interference with the functioning of an information and communications technology system;

(c) Any deception as to factual circumstances made through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do;

with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property.

Article 14

Offences related to online child sexual abuse or child sexual exploitation material

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(a) Producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material through an information and communications technology system;

(b) Soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through an information and communications technology system;

(c) Possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium;

(d) Financing the offences established in accordance with subparagraphs (a) to (c) of this paragraph, which States Parties may establish as a separate offence.

2. For the purposes of this article, the term "child sexual abuse or child sexual exploitation material" shall include visual material, and may include written or audio content, that depicts, describes or represents any person under 18 years of age:

(a) Engaging in real or simulated sexual activity;

(b) In the presence of a person engaging in any sexual activity;

- (c) Whose sexual parts are displayed for primarily sexual purposes; or
- (d) Subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature.

3. A State Party may require that the material identified in paragraph 2 of this article be limited to material that:

- (a) Depicts, describes or represents an existing person; or
 - (b) Visually depicts child sexual abuse or child sexual exploitation.
4. In accordance with their domestic law and consistent with applicable international obligations, States Parties may take steps to exclude the criminalization of:
- (a) Conduct by children for self-generated material depicting them; or
 - (b) The consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved.
5. Nothing in this Convention shall affect any international obligations which are more conducive to the realization of the rights of the child.

Article 15

Solicitation or grooming for the purpose of committing a sexual offence against a child

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the act of intentionally communicating, soliciting, grooming, or making any arrangement through an information and communications technology system for the purpose of committing a sexual offence against a child, as defined in domestic law, including for the commission of any of the offences established in accordance with article 14 of this Convention.
2. A State Party may require an act in furtherance of the conduct described in paragraph 1 of this article.
3. A State Party may consider extending criminalization in accordance with paragraph 1 of this article in relation to a person believed to be a child.
4. States Parties may take steps to exclude the criminalization of conduct as described in paragraph 1 of this article when committed by children.

Article 16

Non-consensual dissemination of intimate images

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image.
2. For the purpose of paragraph 1 of this article, "intimate image" shall mean a visual recording of a person over the age of 18 years made by any means, including a photograph or video recording, that is sexual in nature, in which the person's sexual parts are exposed or the person is engaged in sexual activity, which was private at the time of the recording, and in respect of which the person or persons depicted maintained a reasonable expectation of privacy at the time of the offence.

3. A State Party may extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 years if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.
4. For the purposes of this article, a person who is under the age of 18 years and depicted in an intimate image cannot consent to the dissemination of an intimate image that constitutes child sexual abuse or child sexual exploitation material under article 14 of this Convention.
5. A State Party may require the intent to cause harm before criminal liability attaches.
6. States Parties may take other measures concerning matters related to this article, in accordance with their domestic law and consistent with applicable international obligations.

Article 17

Laundrying of proceeds of crime

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:
 - (a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of that person's actions;
 - (ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;
- (b) Subject to the basic concepts of its legal system:
 - (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;
 - (ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.
2. For purposes of implementing or applying paragraph 1 of this article:
 - (a) Each State Party shall establish as predicate offences relevant offences established in accordance with articles 7 to 16 of this Convention;
 - (b) In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in that list a comprehensive range of offences established in accordance with articles 7 to 16 of this Convention;
 - (c) For the purposes of subparagraph (b) of this paragraph, predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article, had it been committed there;

(d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;

(e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence;

(f) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.

Article 18

Liability of legal persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention.

2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.

3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Article 19

Participation and attempt

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the participation in any capacity, such as that of an accomplice, assistant or instigator, in an offence established in accordance with this Convention.

2. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, any attempt to commit an offence established in accordance with this Convention.

3. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the preparation for an offence established in accordance with this Convention.

Article 20

Statute of limitations

Each State Party shall, where appropriate, considering the gravity of the crime, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence established in accordance with this Convention and establish a longer statute of limitations period or provide for the suspension of the statute of limitations where the alleged offender has evaded the administration of justice.

Article 21

Prosecution, adjudication and sanctions

1. Each State Party shall make the commission of an offence established in accordance with this Convention liable to effective, proportionate and dissuasive sanctions that take into account the gravity of the offence.
2. Each State Party may adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to establish aggravating circumstances in relation to the offences established in accordance with this Convention, including circumstances that affect critical information infrastructures.
3. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences established in accordance with this Convention are exercised in order to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.
4. Each State Party shall ensure that any person prosecuted for offences established in accordance with this Convention enjoys all rights and guarantees in conformity with domestic law and consistent with the applicable international obligations of the State Party, including the right to a fair trial and the rights of the defence.
5. In the case of offences established in accordance with this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.
6. Each State Party shall take into account the gravity of the offences concerned when considering the eventuality of early release or parole of persons convicted of such offences.
7. States Parties shall ensure that appropriate measures are in place under domestic law to protect children who are accused of offences established in accordance with this Convention, consistent with the obligations under the Convention on the Rights of the Child and the applicable Protocols thereto, as well as other applicable international or regional instruments.
8. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.

Chapter III

Jurisdiction

Article 22

Jurisdiction

- a. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when:
 - (a) The offence is committed in the territory of that State Party; or
 - (b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time when the offence is committed.

2. Subject to article 5 of this Convention, a State Party may also establish its jurisdiction over any such offence when:

- (a) The offence is committed against a national of that State Party; or
- (b) The offence is committed by a national of that State Party or a stateless person with habitual residence in its territory; or
- (c) The offence is one of those established in accordance with article 17, paragraph 1 (b) (ii), of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with article 17, paragraph 1 (a) (i) or (ii) or (b) (i), of this Convention within its territory; or
- (d) The offence is committed against the State Party.

3. For the purposes of article 37, paragraph 11, of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that the person is one of its nationals.

4. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite the person.

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Chapter IV

Procedural measures and law enforcement

Article 23

Scope of procedural measures

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings.

2. Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

- (a) The criminal offences established in accordance with this Convention;
- (b) Other criminal offences committed by means of an information and communications technology system; and
- (c) The collection of evidence in electronic form of any criminal offence.

3. (a) Each State Party may reserve the right to apply the measures referred to in article 29 of this Convention only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in article 30 of this Convention. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in article 29;

(b) Where a State Party, owing to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 29 and 30 of this Convention to communications being transmitted within an information and communications technology system of a service provider which:

- (i) Is being operated for the benefit of a closed group of users; and
- (ii) Does not employ public communications networks and is not connected with another information and communications technology system, whether public or private;

that State Party may reserve the right not to apply these measures to such communications. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in articles 29 and 30 of this Convention.

Article 24

Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of proportionality.
2. In accordance with and pursuant to the domestic law of each State Party, such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, include, inter alia, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the proper administration of justice, each State Party shall consider the impact of the powers and procedures in this chapter upon the rights, responsibilities and legitimate interests of third parties.
4. The conditions and safeguards established in accordance with this article shall apply at the domestic level to the powers and procedures set forth in this chapter, both for the purpose of domestic criminal investigations and proceedings and for the purpose of rendering international cooperation by the requested State Party.
5. References to judicial or other independent review in paragraph 2 of this article are references to such review at the domestic level.

Article 25

Expedited preservation of stored electronic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified electronic data, including traffic data, content data and subscriber information, that have been stored by means of an information and communications technology system, in particular where there are grounds to believe that the electronic data are particularly vulnerable to loss or modification.
2. Where a State Party gives effect to paragraph 1 of this article by means of an order to a person to preserve specified stored electronic data in the person's possession or control, the State Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of those electronic data for a period of time as long as necessary, up to a maximum of

60 days, to enable the competent authorities to seek their disclosure. A State Party may provide for such an order to be subsequently renewed.

3. Each State Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the electronic data to keep confidential the undertaking of such procedures for the period of time provided for in its domestic legislation.

Article 26

Expedited preservation and partial disclosure of traffic data

Each State Party shall adopt, in respect of traffic data that are to be preserved under the provisions of article 25 of this Convention, such legislative and other measures as may be necessary to:

(a) Ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of a communication; and

(b) Ensure the expeditious disclosure to the State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication or indicated information was transmitted.

Article 27

Production order

Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

(a) A person in its territory to submit specified electronic data in that person's possession or control that are stored in an information and communications technology system or an electronic data storage medium; and

(b) A service provider offering its services in the territory of the State Party to submit subscriber information relating to such services in that service provider's possession or control.

Article 28

Search and seizure of stored electronic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

(a) An information and communications technology system, part of it, and electronic data stored therein; and

(b) An electronic data storage medium in which the electronic data sought may be stored,

in the territory of that State Party.

2. Each State Party shall adopt such legislative and other measures as may be necessary to ensure that, where its authorities search or similarly access a specific information and communications technology system or part of it, pursuant to paragraph 1 (a) of this article, and have grounds to believe that the electronic data sought are stored in another information and communications technology system or part of it in its territory, and such data are lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously conduct the search to obtain access to that other information and communications technology system.

3. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure electronic data in its territory accessed in accordance with paragraph 1 or 2 of this article. These measures shall include the power to:

- (a) Seize or similarly secure an information and communications technology system or part of it, or an electronic data storage medium;
- (b) Make and retain copies of those electronic data in electronic form;
- (c) Maintain the integrity of the relevant stored electronic data;
- (d) Render inaccessible or remove those electronic data in the accessed information and communications technology system.

4. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the information and communications technology system in question, the information and telecommunications network, or their component parts, or measures applied to protect the electronic data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 to 3 of this article.

Article 29

Real-time collection of traffic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

- (a) Collect or record, through the application of technical means in the territory of that State Party; and
- (b) Compel a service provider, within its existing technical capability:
 - (i) To collect or record, through the application of technical means in the territory of that State Party; or
 - (ii) To cooperate and assist the competent authorities in the collection or recording of,

traffic data, in real time, associated with specified communications in its territory transmitted by means of an information and communications technology system.

2. Where a State Party, owing to the principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

Article 30

Interception of content data

1. Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious criminal offences to be determined by domestic law, to empower its competent authorities to:

- (a) Collect or record, through the application of technical means in the territory of that State Party; and

- (b) Compel a service provider, within its existing technical capability;
- (i) To collect or record, through the application of technical means in the territory of that State Party; or
- (ii) To cooperate and assist the competent authorities in the collection or recording of;

content data, in real time, of specified communications in its territory transmitted by means of an information and communications technology system.

2. Where a State Party, owing to the principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory, through the application of technical means in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

Article 31

Freezing, seizure and confiscation of the proceeds of crime

1. Each State Party shall adopt, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable the confiscation of:

- (a) Proceeds of crime derived from offences established in accordance with this Convention or property the value of which corresponds to that of such proceeds;
- (b) Property, equipment or other instrumentalities used in or destined for use in offences established in accordance with this Convention.

2. Each State Party shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

3. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.

4. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

5. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

6. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled, shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

7. For the purposes of this article and article 50 of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

8. Each State Party may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings.

9. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

10. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with the provisions of the domestic law of a State Party.

Article 32

Establishment of criminal record

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as, and for the purpose that, it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence established in accordance with this Convention.

Article 33

Protection of witnesses

1. Each State Party shall take appropriate measures, in accordance with its domestic law and within its means, to provide effective protection from potential retaliation or intimidation for witnesses who give testimony or, in good faith and on reasonable grounds, provide information concerning offences established in accordance with this Convention or otherwise cooperate with investigative or judicial authorities and, as appropriate, for their relatives and other persons close to them.

2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:

(a) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where appropriate, non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of such persons;

(b) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means.

3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.

4. The provisions of this article shall also apply to victims insofar as they are witnesses.

Article 34

Assistance to and protection of victims

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences established in accordance with this Convention, in particular in cases of threat of retaliation or intimidation.

2. Each State Party shall, subject to its domestic law, establish appropriate procedures to provide access to compensation and restitution for victims of offences established in accordance with this Convention.

3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

4. With respect to the offences established in accordance with articles 14 to 16 of this Convention, each State Party shall, subject to its domestic law, take measures to provide assistance to victims of such offences, including for their physical and psychological recovery, in cooperation with relevant international organizations, non-governmental organizations, and other elements of civil society.

5. In applying the provisions of paragraphs 2 to 4 of this article, each State Party shall take into account the age, gender and the particular circumstances and needs of victims, including the particular circumstances and needs of children.

6. Each State Party shall, to the extent consistent with its domestic legal framework, take effective steps to ensure compliance with requests to remove or render inaccessible the content described in articles 14 and 16 of this Convention.

Chapter V

International cooperation

Article 35

General principles of international cooperation

1. States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of:

(a) The investigation and prosecution of, and judicial proceedings in relation to, the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;

(b) The collecting, obtaining, preserving and sharing of evidence in electronic form of criminal offences established in accordance with this Convention,

(c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention.

2. For the purpose of the collecting, obtaining, preserving and sharing of evidence in electronic form of offences as provided for in paragraph 1 (b) and (c) of this article, the relevant paragraphs of article 40, and articles 41 to 46 of this Convention shall apply.

3. In matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requesting State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties.

Article 36

Protection of personal data

1. (a) A State Party transferring personal data pursuant to this Convention shall do so in accordance with its domestic law and any obligations the transferring Party may have under applicable international law. States Parties shall not be required to transfer personal data in accordance with this Convention if the data cannot be

provided in compliance with their applicable laws concerning the protection of personal data;

(b) Where the transfer of personal data would not be compliant with paragraph 1 (a) of this article, States Parties may seek to impose appropriate conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data;

(c) States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data.

2. For personal data transferred in accordance with this Convention, States Parties shall ensure that the personal data received are subject to effective and appropriate safeguards in the respective legal frameworks of the States Parties.

3. In order to transfer personal data obtained in accordance with this Convention to a third country or an international organization, a State Party shall notify the original transferring State Party of its intention and request its authorization. The State Party shall transfer such personal data only with the authorization of the original transferring State Party, which may require that the authorization be provided in written form.

Article 37

Extradition

1. This article shall apply to the criminal offences established in accordance with this Convention where the person who is the subject of the request for extradition is present in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party. When the extradition is sought for the purpose of serving a final sentence of imprisonment or another form of detention imposed in respect of an extraditable offence, the requested State Party may grant the extradition in accordance with domestic law.

2. Notwithstanding paragraph 1 of this article, a State Party whose law so permits may grant the extradition of a person for any of the criminal offences established in accordance with this Convention that are not punishable under its own domestic law.

3. If the request for extradition includes several separate criminal offences, at least one of which is extraditable under this article and some of which are not extraditable by reason of their period of imprisonment but are related to offences established in accordance with this Convention, the requested State Party may apply this article also in respect of those offences.

4. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them.

5. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies.

6. States Parties that make extradition conditional on the existence of a treaty shall:

(a) At the time of deposit of their instruments of ratification, acceptance or approval or accession to this Convention, inform the Secretary-General of the United Nations whether they will take this Convention as the legal basis for cooperation in extradition with other States Parties to this Convention; and

(b) If they do not take this Convention as the legal basis for cooperation in extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article.

7. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.

8. Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, *inter alia*, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.

9. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.

10. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent, and at the request of the requesting State Party, including when the request is transmitted through existing channels of the International Criminal Police Organization, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure the person's presence at extradition proceedings.

11. A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that the person is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decisions and conduct their proceedings in the same manner as in the case of any other offence of a comparable nature under the domestic law of that State Party. The States Parties concerned shall cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution.

12. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State Party to serve the sentence imposed as a result of the trial or proceedings for which the extradition or surrender of the person was sought and that State Party and the State Party seeking the extradition of the person agree with this option and other terms that they may deem appropriate, such conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 11 of this article.

13. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested State Party shall, if its domestic law so permits and in conformity with the requirements of such law, upon application of the requesting State Party, consider the enforcement of the sentence imposed under the domestic law of the requesting State Party or the remainder thereof.

14. Any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present.

15. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the

request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

16. States Parties may not refuse a request for extradition on the sole ground that the offence is also considered to involve fiscal matters.

17. Before refusing extradition, the requested State Party shall, where appropriate, consult with the requesting State Party to provide it with ample opportunity to present its opinions and to provide information relevant to its allegation.

18. The requested State Party shall inform the requesting State Party of its decision with regard to the extradition. The requested State Party shall inform the requesting State Party of any reason for refusal of extradition unless the requested State Party is prevented from doing so by its domestic law or its international legal obligations.

19. Each State Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary-General of the United Nations the name and address of an authority responsible for making or receiving requests for extradition or provisional arrest. The Secretary-General shall set up and keep updated a register of authorities so designated by the States Parties. Each State Party shall ensure that the details held in the register are correct at all times.

20. States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition.

Article 38

Transfer of sentenced persons

States Parties may, taking into consideration the rights of sentenced persons, consider entering into bilateral or multilateral agreements or arrangements on the transfer to their territory of persons sentenced to imprisonment or other forms of deprivation of liberty for offences established in accordance with this Convention, in order that they may complete their sentences there. States Parties may also take into account issues relating to consent, rehabilitation and reintegration.

Article 39

Transfer of criminal proceedings

1. States Parties shall consider the possibility of transferring to one another proceedings for the criminal prosecution of an offence established in accordance with this Convention where such a transfer is deemed to be in the interests of the proper administration of justice, particularly in cases where several jurisdictions are involved, with a view to concentrating the prosecution.

2. If a State Party that makes the transfer of criminal proceedings conditional on the existence of a treaty receives a request for transfer from another State Party with which it has no treaty in this matter, it may consider this Convention as the legal basis for the transfer of criminal proceedings in respect of any offence to which this article applies.

Article 40

General principles and procedures relating to mutual legal assistance

1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences established in accordance with this Convention, and for the purposes of the

collection of evidence in electronic form, of offences established in accordance with this Convention, as well as of serious crime.

2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 18 of this Convention in the requesting State Party.

3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:

- (a) Taking evidence or statements from persons;
- (b) Effecting service of judicial documents;
- (c) Executing searches and seizures, and freezing;
- (d) Searching or similarly accessing, seizing or similarly securing, and disclosing electronic data stored by means of an information and communications technology system pursuant to article 44 of this Convention;
- (e) Collecting traffic data in real time pursuant to article 45 of this Convention;
- (f) Intercepting content data pursuant to article 46 of this Convention;
- (g) Examining objects and sites;
- (h) Providing information, evidence and expert evaluations;
- (i) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;
- (j) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;
- (k) Facilitating the voluntary appearance of persons in the requesting State Party;
- (l) Recovering proceeds of crime;
- (m) Any other type of assistance that is not contrary to the domestic law of the requested State Party.

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

6. The provisions of this article shall not affect obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance.

7. Paragraphs 8 to 31 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty on mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 8 to 31 of this article in lieu thereof. States Parties are strongly encouraged to apply the provisions of those paragraphs if they facilitate cooperation.

8. States Parties may decline to render assistance pursuant to this article on the ground of absence of dual criminality. However, the requested State Party may, when it deems appropriate, provide assistance, to the extent it decides at its discretion, irrespective of whether the conduct would constitute an offence under the domestic law of the requested State Party. Assistance may be refused when requests involve matters of a *de minimis* nature or matters for which the cooperation or assistance sought is available under other provisions of this Convention.

9. A person who is being detained or is serving a sentence in the territory of one State Party and whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for investigations, prosecutions or judicial proceedings in relation to offences established in accordance with this Convention may be transferred if the following conditions are met:

(a) The person freely gives informed consent;

(b) The competent authorities of both States Parties agree, subject to such conditions as those States Parties may deem appropriate.

10. For the purposes of paragraph 9 of this article:

(a) The State Party to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State Party from which the person was transferred;

(b) The State Party to which the person is transferred shall, without delay, implement its obligation to return the person to the custody of the State Party from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States Parties;

(c) The State Party to which the person is transferred shall not require the State Party from which the person was transferred to initiate extradition proceedings for the return of the person;

(d) The person transferred shall receive credit for service of the sentence being served in the State from which the person was transferred for time spent in the custody of the State Party to which the person was transferred.

11. Unless the State Party from which a person is to be transferred in accordance with paragraphs 9 and 10 of this article so agrees, that person, regardless of the person's nationality, shall not be prosecuted, detained, punished or subjected to any other restriction of liberty in the territory of the State to which that person is transferred in respect of acts, omissions or convictions prior to the person's departure from the territory of the State from which the person was transferred.

12. (a) Each State Party shall designate a central authority or authorities that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. Where a State Party has a special region or territory with a separate system of mutual

legal assistance, it may designate a distinct central authority that shall have the same function for that region or territory;

(b) Central authorities shall ensure the speedy and proper execution or transmission of the requests received. Where the central authority transmits the request to a competent authority for execution, it shall encourage the speedy and proper execution of the request by the competent authority;

(c) The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention, and shall set up and keep updated a register of central authorities designated by the States Parties. Each State Party shall ensure that the details held in the register are correct at all times;

(d) Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.

13. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party, under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and where agreed by the States Parties, requests may be made orally, but shall be confirmed in writing forthwith.

14. Where not prohibited by their respective laws, central authorities of States Parties are encouraged to transmit and receive requests for mutual legal assistance, and communications related thereto, as well as evidence, in electronic form under conditions allowing the requested State Party to establish authenticity and ensuring the security of communications.

15. A request for mutual legal assistance shall contain:

- (a) The identity of the authority making the request;
- (b) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;
- (c) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;
- (d) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;
- (e) Where possible and appropriate, the identity, location and nationality of any person concerned, as well as the country of origin, description and location of any item or accounts concerned;
- (f) Where applicable, the time period for which the evidence, information or other assistance is sought; and
- (g) The purpose for which the evidence, information or other assistance is sought.

16. The requested State Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.

17. A request shall be executed in accordance with the domestic law of the requested State Party and, to the extent not contrary to the domestic law of the requested State Party and where possible, in accordance with the procedures specified in the request.

18. Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a witness, victim or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by videoconference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party. If the requested State Party does not have access to the technical means necessary for holding a videoconference, such means may be provided by the requesting State Party, upon mutual agreement.

19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evidence that is exculpatory to an accused person. In the latter case, the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.

20. The requesting State Party may require that the requested State Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party.

21. Mutual legal assistance may be refused:

- (a) If the request is not made in conformity with the provisions of this article;
- (b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests;
- (c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;
- (d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.

22. Nothing in this Convention shall be interpreted as imposing an obligation to afford mutual legal assistance if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

23. States Parties may not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

24. States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy.

25. Reasons shall be given for any refusal of mutual legal assistance.

26. The requested State Party shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting State Party and for which reasons are given, preferably in the request. The requested State Party shall respond to reasonable requests by the requesting State Party on the status, and progress in its handling, of the request. The requesting State Party shall promptly inform the requested State Party when the assistance sought is no longer required.

27. Mutual legal assistance may be postponed by the requested State Party on the ground that it interferes with an ongoing investigation, prosecution or judicial proceeding.

28. Before refusing a request pursuant to paragraph 21 of this article or postponing its execution pursuant to paragraph 27 of this article, the requested State Party shall consult with the requesting State Party to consider whether assistance may be granted subject to such terms and conditions as it deems necessary. If the requesting State Party accepts assistance subject to those conditions, it shall comply with the conditions.

29. Without prejudice to the application of paragraph 11 of this article, a witness, expert or other person who, at the request of the requesting State Party, consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting State Party shall not be prosecuted, detained, punished or subjected to any other restriction of the person's liberty in that territory in respect of acts, omissions or convictions prior to the person's departure from the territory of the requested State Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of 15 consecutive days or for any period agreed upon by the States Parties from the date on which the person has been officially informed that the presence of the person is no longer required by the judicial authorities, an opportunity of leaving, has nevertheless remained voluntarily in the territory of the requesting State Party or, having left it, has returned of the person's own free will.

30. The ordinary costs of executing a request shall be borne by the requested State Party, unless otherwise agreed by the States Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfill the request, the States Parties shall consult to determine the terms and conditions under which the request will be executed, as well as the manner in which the costs shall be borne.

31. The requested State Party:

(a) Shall provide to the requesting State Party copies of government records, documents or information in its possession that under its domestic law are available to the general public;

(b) May, at its discretion, provide to the requesting State Party, in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public.

32. States Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to or enhance the provisions of this article.

Article 41

24/7 network

1. Each State Party shall designate a point of contact available 24 hours a day, 7 days a week, in order to ensure the provision of immediate assistance for the purpose of specific criminal investigations, prosecutions or judicial proceedings concerning offences established in accordance with this Convention, or for the collection, obtaining and preservation of evidence in electronic form for the purposes of paragraph 3 of this article and in relation to the offences established in accordance with this Convention, as well as to serious crime.

2. The Secretary-General of the United Nations shall be notified of such point of contact and keep an updated register of points of contact designated for the purposes of this article and shall annually circulate to the States Parties the updated list of contact points.

3. Such assistance shall include facilitating or, if permitted by the domestic law and practice of the requested State Party, directly carrying out the following measures:

- (a) The provision of technical advice;
- (b) The preservation of stored electronic data pursuant to articles 42 and 43 of this Convention, including, as appropriate, information about the location of the service provider, if known to the requested State Party, to assist the requesting State Party in making a request;
- (c) The collection of evidence and the provision of legal information;
- (d) The locating of suspects; or
- (e) The provision of electronic data to avert an emergency.

4. A State Party's point of contact shall have the capacity to carry out communications with the point of contact of another State Party on an expedited basis. If the point of contact designated by a State Party is not part of that State Party's authority or authority responsible for mutual legal assistance or extradition, the point of contact shall ensure that it is able to coordinate with that authority or those authorities on an expedited basis.

5. Each State Party shall ensure that trained and equipped personnel are available to ensure the operation of the 24/7 network.

6. States Parties may also use and strengthen existing authorized networks of points of contact, where applicable, and within the limits of their domestic laws, including the 24/7 networks for computer-related crime of the International Criminal Police Organization for prompt police-to-police cooperation and other methods of information exchange cooperation.

Article 42

International cooperation for the purpose of expedited preservation of stored electronic data

1. A State Party may request another State Party to order or otherwise obtain, in accordance with article 25 of this Convention, the expeditious preservation of electronic data stored by means of an information and communications technology system located within the territory of that other State Party, and in respect of which the requesting State Party intends to submit a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of the electronic data.

2. The requesting State Party may use the 24/7 network provided for in article 41 of this Convention to seek information concerning the location of the electronic data stored by means of an information and communications technology system and, as appropriate, information about the location of the service provider.

3. A request for preservation made under paragraph 1 of this article shall specify:

- (a) The authority seeking the preservation;
- (b) The offence that is the subject of a criminal investigation, prosecution or judicial proceeding and a brief summary of the related facts;
- (c) The stored electronic data to be preserved and their relationship to the offence;
- (d) Any available information identifying the custodian of the stored electronic data or the location of the information and communications technology system;
- (e) The necessity of the preservation;
- (f) That the requesting State Party intends to submit a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of the stored electronic data;
- (g) As appropriate, the need to keep the request for preservation confidential and not to notify the user.

4. Upon receiving the request from another State Party, the requested State Party shall take all appropriate measures to preserve expeditiously the specified electronic data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition for providing such preservation.

5. A State Party that requires dual criminality as a condition for responding to a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of stored electronic data may, in respect of offences other than those established in accordance with this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that, at the time of disclosure, the condition of dual criminality could not be fulfilled.

6. In addition, a request for preservation may be refused only on the basis of the grounds contained in article 40, paragraph 21 (b) and (c) and paragraph 22, of this Convention.

7. Where the requested State Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting State Party's investigation, it shall promptly so inform the requesting State Party, which shall then determine whether the request should nevertheless be executed.

8. Any preservation effected in response to a request made pursuant to paragraph 1 of this article shall be for a period of not less than 60 days, in order to enable the requesting State Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

9. Before the expiry of the preservation period in paragraph 8 of this article, the requesting State Party may request an extension of the period of preservation.

Article 43

International cooperation for the purpose of expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made pursuant to article 42 of this Convention to preserve traffic data concerning a specific communication, the requested State Party discovers that a service provider in another State Party was involved in the transmission of the communication, the requested State Party shall expeditiously disclose to the requesting State Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 of this article may be refused only on the basis of the grounds contained in article 40, paragraph 21 (b) and (c) and paragraph 22, of this Convention.

Article 44

Mutual legal assistance in accessing stored electronic data

1. A State Party may request another State Party to search or similarly access, seize or similarly secure, and disclose electronic data stored by means of an information and communications technology system located within the territory of the requested State Party, including electronic data that have been preserved pursuant to article 42 of this Convention.
2. The requested State Party shall respond to the request through the application of relevant international instruments and laws referred to in article 35 of this Convention, and in accordance with other relevant provisions of this chapter.
3. The request shall be responded to on an expedited basis where:
 - (a) There are grounds to believe that the relevant data are particularly vulnerable to loss or modification; or
 - (b) The instruments and laws referred to in paragraph 2 of this article otherwise provide for expedited cooperation.

Article 45

Mutual legal assistance in the real-time collection of traffic data

1. States Parties shall endeavour to provide mutual legal assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of an information and communications technology system. Subject to the provisions of paragraph 2 of this article, such assistance shall be governed by the conditions and procedures provided for under domestic law.
2. Each State Party shall endeavour to provide such assistance at least with respect to criminal offences for which the real-time collection of traffic data would be available in a similar domestic case.
3. A request made in accordance with paragraph 1 of this article shall specify:
 - (a) The name of the requesting authority;
 - (b) A summary of the main facts and the nature of the investigation, prosecution or judicial proceeding to which the request relates;
 - (c) The electronic data in relation to which the collection of the traffic data is required and their relationship to the offence;

- (d) Any available data that identify the owner or user of the data or the location of the information and communications technology system;
- (e) Justification for the need to collect the traffic data;
- (f) The period for which traffic data are to be collected and a corresponding justification of its duration.

Article 46

Mutual legal assistance in the interception of content data

States Parties shall endeavour to provide mutual legal assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of an information and communications technology system, to the extent permitted under treaties applicable to them or under their domestic laws.

Article 47

Law enforcement cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences established in accordance with this Convention. States Parties shall, in particular, take effective measures:

- (a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services, taking into account existing channels, including those of the International Criminal Police Organization, in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences established in accordance with this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

- (b) To cooperate with other States Parties in conducting inquiries with respect to offences established in accordance with this Convention concerning:

- (i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

- (ii) The movement of proceeds of crime or property derived from the commission of such offences;

- (iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

- (c) To provide, where appropriate, necessary items or data for analytical or investigative purposes;

- (d) To exchange, where appropriate, information with other States Parties concerning specific means and methods used to commit the offences established in accordance with this Convention, including the use of false identities, forged, altered or false documents and other means of concealing activities, as well as cybercrime tactics, techniques and procedures;

- (e) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers;

- (f) To exchange information and coordinate administrative and other measures taken, as appropriate, for the purpose of early identification of the offences established in accordance with this Convention.

2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the States Parties may consider this Convention to be the basis for mutual law enforcement cooperation in respect of the offences established in accordance with this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

Article 48

Joint investigations

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to offences established in accordance with this Convention that are the subject of criminal investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigations are to take place is fully respected.

Article 49

*Mechanisms for the recovery of property through international cooperation
in confiscation*

1. Each State Party, in order to provide mutual legal assistance pursuant to article 50 of this Convention with respect to property acquired through or involved in the commission of an offence established in accordance with this Convention, shall, in accordance with its domestic law:

(a) Take such measures as may be necessary to permit its competent authorities to give effect to an order of confiscation issued by a court of another State Party;

(b) Take such measures as may be necessary to permit its competent authorities, where they have jurisdiction, to order the confiscation of such property of foreign origin by adjudication of an offence of money-laundering or such other offence as may be within its jurisdiction or by other procedures authorized under its domestic law; and

(c) Consider taking such measures as may be necessary to allow confiscation of such property without a criminal conviction in cases in which the offender cannot be prosecuted by reason of death, flight or absence or in other appropriate cases.

2. Each State Party, in order to provide mutual legal assistance upon a request made pursuant to article 50, paragraph 2, of this Convention, shall, in accordance with its domestic law:

(a) Take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a freezing or seizure order issued by a court or competent authority of a requesting State Party that provides a reasonable basis for the requested State Party to believe that there are sufficient grounds for taking such actions and that the property would eventually be subject to an order of confiscation for the purposes of paragraph 1 (a) of this article;

(b) Take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a request that provides a reasonable basis

for the requested State Party to believe that there are sufficient grounds for taking such actions and that the property would eventually be subject to an order of confiscation for the purposes of paragraph 1 (a) of this article; and

(c) Consider taking additional measures to permit its competent authorities to preserve property for confiscation, such as on the basis of a foreign arrest or criminal charge related to the acquisition of such property.

Article 56

International cooperation for the purposes of confiscation

1. A State Party that has received a request from another State Party having jurisdiction over an offence established in accordance with this Convention for the confiscation of proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention situated in its territory shall, to the greatest extent possible within its domestic legal system:

(a) Submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such an order is granted, give effect to it; or

(b) Submit to its competent authorities, with a view to giving effect to it to the extent requested, an order of confiscation issued by a court in the territory of the requesting State Party in accordance with article 31, paragraph 1, of this Convention insofar as it relates to proceeds of crime, property, equipment or other instrumentalities situated in the territory of the requested State Party.

2. Following a request made by another State Party having jurisdiction over an offence established in accordance with this Convention, the requested State Party shall take measures to identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention for the purpose of eventual confiscation to be ordered either by the requesting State Party or, pursuant to a request under paragraph 1 of this article, by the requested State Party.

3. The provisions of article 40 of this Convention are applicable, *mutatis mutandis*, to this article. In addition to the information specified in article 40, paragraph 15, of this Convention, requests made pursuant to this article shall contain:

(a) In the case of a request pertaining to paragraph 1 (a) of this article, a description of the property to be confiscated, including, to the extent possible, the location, and where relevant, the estimated value of the property and a statement of the facts relied upon by the requesting State Party sufficient to enable the requested State Party to seek the order under its domestic law;

(b) In the case of a request pertaining to paragraph 1 (b) of this article, a legally admissible copy of an order of confiscation upon which the request is based issued by the requesting State Party, a statement of the facts and information as to the extent to which execution of the order is requested, a statement specifying the measures taken by the requesting State Party to provide adequate notification to bona fide third parties and to ensure due process, and a statement that the confiscation order is final;

(c) In the case of a request pertaining to paragraph 2 of this article, a statement of the facts relied upon by the requesting State Party and a description of the actions requested and, where available, a legally admissible copy of an order on which the request is based.

4. The decisions or actions provided for in paragraphs 1 and 2 of this article shall be taken by the requested State Party in accordance with and subject to the provisions of its domestic law and its procedural rules or any bilateral or multilateral treaty,

agreement or arrangement to which it may be bound in relation to the requesting State Party.

5. Each State Party shall furnish copies of its laws and regulations that give effect to this article and of any subsequent changes to such laws and regulations or a description thereof to the Secretary-General of the United Nations.

6. If a State Party elects to make the taking of the measures referred to in paragraphs 1 and 2 of this article conditional on the existence of a relevant treaty, that State Party shall consider this Convention the necessary and sufficient treaty basis.

7. Cooperation under this article may also be refused or provisional measures may be lifted if the requested State Party does not receive sufficient and timely evidence or if the property is of a *de minimis* value.

8. Before lifting any provisional measure taken pursuant to this article, the requested State Party shall, wherever possible, give the requesting State Party an opportunity to present its reasons in favour of continuing the measure.

9. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

10. States Parties shall consider concluding bilateral or multilateral treaties, agreements or arrangements to enhance the effectiveness of international cooperation undertaken pursuant to this article.

Article 31

Special cooperation

Without prejudice to its domestic law, each State Party shall endeavour to take measures to permit it to forward, without prejudice to its own criminal investigations, prosecutions or judicial proceedings, information or proceeds of offences established in accordance with this Convention to another State Party without prior request, when it considers that the disclosure of such information might assist the receiving State Party in initiating or carrying out criminal investigations, prosecutions or judicial proceedings or might lead to a request by that State Party under article 50 of this Convention.

Article 32

Return and disposal of confiscated proceeds of crime or property

1. Proceeds of crime or property confiscated by a State Party pursuant to article 31 or 50 of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures.

2. When acting on a request made by another State Party in accordance with article 50 of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their prior legitimate owners.

3. When acting on a request made by another State Party in accordance with articles 31 and 50 of this Convention, a State Party may, after due consideration has been given to compensation of victims, give special consideration to concluding agreements or arrangements on:

(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the

account designated in accordance with article 56, paragraph 2 (c), of this Convention, and to intergovernmental bodies specializing in the fight against cybercrime;

(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

4. Where appropriate, unless States Parties decide otherwise, the requested State Party may deduct reasonable expenses incurred in investigations, prosecutions or judicial proceedings leading to the return or disposition of confiscated property pursuant to this article.

Chapter VI

Preventive measures

Article 53

Preventive measures

1. Each State Party shall endeavour, in accordance with fundamental principles of its legal system, to develop and implement or maintain effective and coordinated policies and best practices to reduce existing or future opportunities for cybercrime through appropriate legislative, administrative or other measures.

2. Each State Party shall take appropriate measures, within its means and in accordance with fundamental principles of its domestic law, to promote the active participation of relevant individuals and entities outside the public sector, such as non-governmental organizations, civil society organizations, academic institutions and private sector entities, as well as the general public, in the relevant aspects of prevention of the offences established in accordance with this Convention.

3. Preventive measures may include:

(a) Strengthening cooperation between law enforcement agencies or prosecutors and relevant individuals and entities outside the public sector, such as non-governmental organizations, civil society organizations, academic institutions and private sector entities for the purpose of addressing relevant aspects of preventing and combating the offences established in accordance with this Convention;

(b) Promoting public awareness regarding the existence, causes and gravity of the threat posed by the offences established in accordance with this Convention through public information activities, public education, media and information literacy programmes and curricula that promote public participation in preventing and combating such offences;

(c) Building and making efforts to increase the capacity of domestic criminal justice systems, including training and developing expertise among criminal justice practitioners, as part of national prevention strategies against the offences established in accordance with this Convention;

(d) Encouraging service providers to take effective measures, where feasible in the light of national circumstances and to the extent permitted by domestic law, to strengthen the security of the service providers' products, services and customers;

(e) Recognizing the contributions of the legitimate activities of security researchers when intended solely, and to the extent permitted and subject to the conditions prescribed by domestic law, to strengthen and improve the security of service providers' products, services and customers located within the territory of the State Party;

(f) Developing, facilitating and promoting programmes and activities in order to discourage those at risk of engaging in cybercrime from becoming offenders and to develop their skills in a lawful manner;

(g) Endeavouring to promote the reintegration into society of persons convicted of offences established in accordance with this Convention;

(h) Developing strategies and policies, in accordance with domestic law, to prevent and eradicate gender-based violence that occurs through the use of an information and communications technology system, as well as taking into consideration the special circumstances and needs of persons in vulnerable situations in developing preventive measures;

(i) Undertaking specific and tailored efforts to keep children safe online, including through education and training on and raising public awareness of child sexual abuse or child sexual exploitation online and through revising domestic legal frameworks and enhancing international cooperation aimed at its prevention, as well as making efforts to ensure the swift removal of child sexual abuse and child sexual exploitation material;

(j) Enhancing the transparency of and promoting the contribution of the public to decision-making processes and ensuring that the public has adequate access to information;

(k) Respecting, promoting and protecting the freedom to seek, receive and impart public information concerning cybercrime;

(l) Developing or strengthening support programmes for victims of the offences established in accordance with this Convention;

(m) Preventing and detecting transfers of proceeds of crime and property related to the offences established in accordance with this Convention

4. Each State Party shall take appropriate measures to ensure that the relevant competent authority or authorities responsible for preventing and combating cybercrime are known and accessible to the public, where appropriate, for the reporting, including anonymously, of any incident that may be considered a criminal offence established in accordance with this Convention

5. States Parties shall endeavour to periodically evaluate existing relevant national legal frameworks and administrative practices with a view to identifying gaps and vulnerabilities and ensuring their relevance in the face of changing threats posed by the offences established in accordance with this Convention.

6. States Parties may collaborate with each other and with relevant international and regional organizations in promoting and developing the measures referred to in this article. This includes participation in international projects aimed at the prevention of cybercrime.

7. Each State Party shall inform the Secretary-General of the United Nations of the name and address of the authority or authorities that may assist other States Parties in developing and implementing specific measures to prevent cybercrime.

Chapter VII

Technical assistance and information exchange

Article 34

Technical assistance and capacity-building

1. States Parties shall, according to their capacity, consider affording one another the widest measure of technical assistance and capacity-building, including training

and other forms of assistance, the mutual exchange of relevant experience and specialized knowledge and the transfer of technology on mutually agreed terms, taking into particular consideration the interests and needs of developing States Parties, with a view to facilitating the prevention, detection, investigation and prosecution of the offences covered by this Convention.

2. States Parties shall, to the extent necessary, initiate, develop, implement or improve specific training programmes for their personnel responsible for the prevention, detection, investigation and prosecution of the offences covered by this Convention.

3. Activities referred to in paragraphs 1 and 2 of this article may deal, to the extent permitted by domestic law, with the following:

(a) Methods and techniques used in the prevention, detection, investigation and prosecution of the offences covered by this Convention;

(b) Building capacity in the development and planning of strategic policies and legislation to prevent and combat cybercrime;

(c) Building capacity in the collection, preservation and sharing of evidence, in particular in electronic form, including the maintenance of the chain of custody and forensic analysis;

(d) Modern law enforcement equipment and the use thereof;

(e) Training of competent authorities in the preparation of requests for mutual legal assistance and other means of cooperation that meet the requirements of this Convention, especially for the collection, preservation and sharing of evidence in electronic form;

(f) Prevention, detection and monitoring of the movements of proceeds deriving from the commission of the offences covered by this Convention, property, equipment or other instrumentalities and methods used for the transfer, concealment or disguise of such proceeds, property, equipment or other instrumentalities;

(g) Appropriate and efficient legal and administrative mechanisms and methods for facilitating the seizure, confiscation and return of proceeds of offences covered by this Convention;

(h) Methods used in the protection of victims and witnesses who cooperate with judicial authorities;

(i) Training in relevant substantive and procedural law, and law enforcement investigation powers, as well as in national and international regulations and in languages.

4. States Parties shall, subject to their domestic law, endeavour to leverage the expertise of and cooperate closely with other States Parties and relevant international and regional organizations, non-governmental organizations, civil society organizations, academic institutions and private sector entities, with a view to enhancing the effective implementation of this Convention.

5. States Parties shall assist one another in planning and implementing research and training programmes designed to share expertise in the areas referred to in paragraph 3 of this article, and to that end shall also, when appropriate, use regional and international conferences and seminars to promote cooperation and to stimulate discussion on problems of mutual concern.

6. States Parties shall consider assisting one another, upon request, in conducting evaluations, studies and research relating to the types, causes and effects of offences covered by this Convention committed in their respective territories, with a view to

developing, with the participation of the competent authorities and relevant non-governmental organizations, civil society organizations, academic institutions and private sector entities, strategies and action plans to prevent and combat cybercrime.

7. States Parties shall promote training and technical assistance that facilitates timely extradition and mutual legal assistance. Such training and technical assistance may include language training, assistance with the drafting and handling of mutual legal assistance requests, and secondments and exchanges between personnel in central authorities or agencies with relevant responsibilities.

8. States Parties shall strengthen, to the extent necessary, efforts to maximize the effectiveness of technical assistance and capacity-building in international and regional organizations and in the framework of relevant bilateral and multilateral agreements or arrangements.

9. States Parties shall consider establishing voluntary mechanisms with a view to contributing financially to the efforts of developing countries to implement this Convention through technical assistance programmes and capacity-building projects.

10. Each State Party shall endeavour to make voluntary contributions to the United Nations Office on Drugs and Crime for the purpose of fostering, through the Office, programmes and projects with a view to implementing this Convention through technical assistance and capacity-building.

Article 55

Exchange of information

1. Each State Party shall consider analysing, as appropriate, in consultation with relevant experts, including from non-governmental organizations, civil society organizations, academic institutions and private sector entities, trends in its territory with respect to offences covered by this Convention, as well as the circumstances in which such offences are committed.

2. States Parties shall consider developing and sharing with each other and through international and regional organizations statistics, analytical expertise and information concerning cybercrime, with a view to developing, insofar as possible, common definitions, standards and methodologies, as well as best practices, to prevent and combat such crime.

3. Each State Party shall consider monitoring its policies and practical measures to prevent and combat offences covered by this Convention and making assessments of their effectiveness and efficiency.

4. States Parties shall consider exchanging information on legal, policy and technological developments related to cybercrime and the collection of evidence in electronic form.

Article 56

Implementation of the Convention through economic development and technical assistance

1. States Parties shall take measures conducive to the optimal implementation of this Convention to the extent possible, through international cooperation, taking into account the negative effects of the offences covered by this Convention on society in general and, in particular, on sustainable development.

2. States Parties are strongly encouraged to make concrete efforts, to the extent possible and in coordination with each other, as well as with international and regional organizations:

(a) To enhance their cooperation at various levels with other States Parties, in particular developing countries, with a view to strengthening their capacity to prevent and combat the offences covered by this Convention;

(b) To enhance financial and material assistance to support the efforts of other States Parties, in particular developing countries, in effectively preventing and combating the offences covered by this Convention and to help them to implement this Convention;

(c) To provide technical assistance to other States Parties, in particular developing countries, in support of meeting their needs regarding the implementation of this Convention. To that end, States Parties shall endeavour to make adequate and regular voluntary contributions to an account specifically designated for that purpose in a United Nations funding mechanism;

(d) To encourage, as appropriate, non-governmental organizations, civil society organizations, academic institutions and private sector entities, as well as financial institutions, to contribute to the efforts of States Parties, including in accordance with this article, in particular by providing more training programmes and modern equipment to developing countries in order to assist them in achieving the objectives of this Convention;

(e) To exchange best practices and information with regard to activities undertaken, with a view to improving transparency, avoiding duplication of effort and making best use of any lessons learned

3. States Parties shall also consider using existing subregional, regional and international programmes, including conferences and seminars, to promote cooperation and technical assistance and to stimulate discussion on problems of mutual concern, including the special problems and needs of developing countries.

4. To the extent possible, States Parties shall ensure that resources and efforts are distributed and directed to support the harmonization of standards, skills, capacity, expertise and technical capabilities with the aim of establishing common minimum standards among States Parties to eradicate safe havens for the offences covered by this Convention and strengthen the fight against cybercrime.

5. To the extent possible, the measures taken under this article shall be without prejudice to existing foreign assistance commitments or to other financial cooperation arrangements at the bilateral, regional or international levels.

6. States Parties may conclude bilateral, regional or multilateral agreements or arrangements on material and logistical assistance, taking into consideration the financial arrangements necessary for the means of international cooperation provided for by this Convention to be effective and for the prevention, detection, investigation and prosecution of the offences covered by this Convention.

Chapter VIII

Mechanism of implementation

Article 57

Conference of the States Parties to the Convention

1. A Conference of the States Parties to the Convention is hereby established to improve the capacity of and cooperation between States Parties to achieve the objectives set forth in this Convention and to promote and review its implementation.

2. The Secretary-General of the United Nations shall convene the Conference of the States Parties not later than one year following the entry into force of this Convention.

Thereafter, regular meetings of the Conference shall be held in accordance with the rules of procedure adopted by the Conference.

3. The Conference of the States Parties shall adopt rules of procedure and rules governing the activities set forth in this article, including rules concerning the admission and participation of observers, and the payment of expenses incurred in carrying out those activities. Such rules and related activities shall take into account principles such as effectiveness, inclusivity, transparency, efficiency and national ownership.

4. In establishing its regular meetings, the Conference of the States Parties shall take into account the time and location of the meetings of other relevant international and regional organizations and mechanisms in similar matters, including their subsidiary treaty bodies, consistent with the principles identified in paragraph 3 of this article.

5. The Conference of the States Parties shall agree upon activities, procedures and methods of work to achieve the objectives set forth in paragraph 1 of this article, including:

(a) Facilitating the effective use and implementation of this Convention, the identification of any problems thereof, as well as the activities carried out by States Parties under this Convention, including encouraging the mobilization of voluntary contributions;

(b) Facilitating the exchange of information on legal, policy and technological developments pertaining to the offences established in accordance with this Convention and the collection of evidence in electronic form among States Parties and relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and private sector entities, in accordance with domestic law, as well as on patterns and trends in cybercrime and on successful practices for preventing and combating such offences;

(c) Cooperating with relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and private sector entities;

(d) Making appropriate use of relevant information produced by other international and regional organizations and mechanisms for preventing and combating the offences established in accordance with this Convention, in order to avoid unnecessary duplication of work;

(e) Reviewing periodically the implementation of this Convention by its States Parties;

(f) Making recommendations to improve this Convention and its implementation as well as considering possible supplementation or amendment of the Convention;

(g) Elaborating and adopting supplementary protocols to this Convention on the basis of articles 61 and 62 of this Convention;

(h) Taking note of the technical assistance and capacity-building requirements of States Parties regarding the implementation of this Convention and recommending any action it may deem necessary in that respect.

6. Each State Party shall provide the Conference of the States Parties with information on legislative, administrative and other measures, as well as on its programmes, plans and practices, to implement this Convention, as required by the Conference. The Conference shall examine the most effective way of receiving and acting upon information, including, *inter alia*, information received from States

Parties and from competent international and regional organizations. Inputs received from representatives of relevant non-governmental organizations, civil society organizations, academic institutions and private sector entities, duly accredited in accordance with procedures to be decided upon by the Conference, may also be considered.

7. For the purpose of paragraph 5 of this article, the Conference of the States Parties may establish and administer such review mechanisms as it considers necessary.

8. Pursuant to paragraphs 5 to 7 of this article, the Conference of the States Parties shall establish, if it deems necessary, any appropriate mechanisms or subsidiary bodies to assist in the effective implementation of the Convention.

Article 58

Secretariat

1. The Secretary-General of the United Nations shall provide the necessary secretariat services to the Conference of the States Parties to the Convention.

2. The secretariat shall:

(a) Assist the Conference of the States Parties in carrying out the activities set forth in this Convention and make arrangements and provide the necessary services for the sessions of the Conference as they pertain to this Convention;

(b) Upon request, assist States Parties in providing information to the Conference of the States Parties, as envisaged in this Convention; and

(c) Ensure the necessary coordination with the secretariats of relevant international and regional organizations.

Chapter IX

Final provisions

Article 59

Implementation of the Convention

1. Each State Party shall take the necessary measures, including legislative and administrative measures, in accordance with fundamental principles of its domestic law, to ensure the implementation of its obligations under this Convention.

2. Each State Party may adopt more strict or severe measures than those provided for by this Convention for preventing and combating the offences established in accordance with this Convention.

Article 60

Effects of the Convention

1. If two or more States Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly.

2. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a State Party under international law.

Article 61

Relation with protocols

1. This Convention may be supplemented by one or more protocols.

2. In order to become a Party to a protocol, a State or a regional economic integration organization must also be a Party to this Convention.
3. A State Party to this Convention is not bound by a protocol unless it becomes a Party to the protocol in accordance with the provisions thereof.
4. Any protocol to this Convention shall be interpreted together with this Convention, taking into account the purpose of that protocol.

Article 62

Adoption of supplementary protocols

1. At least 60 States Parties shall be required before any supplementary protocol is considered for adoption by the Conference of the States Parties. The Conference shall make every effort to achieve consensus on any supplementary protocol. If all efforts at consensus have been exhausted and no agreement has been reached, the supplementary protocol shall, as a last resort, require for its adoption at least a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference.
2. Regional economic integration organizations, in matters within their competence, shall exercise their right to vote under this article with a number of votes equal to the number of their member States that are Parties to this Convention. Such organizations shall not exercise their right to vote if their member States exercise theirs and vice versa.

Article 63

Settlement of disputes

1. States Parties shall endeavour to settle disputes concerning the interpretation or application of this Convention through negotiation or any other peaceful means of their own choice.
2. Any dispute between two or more States Parties concerning the interpretation or application of this Convention that cannot be settled through negotiation or other peaceful means within a reasonable time shall, at the request of one of those States Parties, be submitted to arbitration. If, six months after the date of the request for arbitration, those States Parties are unable to agree on the organization of the arbitration, any one of those States Parties may refer the dispute to the International Court of Justice by request in accordance with the Statute of the Court.
3. Each State Party may, at the time of signature, ratification, acceptance or approval of or accession to this Convention, declare that it does not consider itself bound by paragraph 2 of this article. The other States Parties shall not be bound by paragraph 2 of this article with respect to any State Party that has made such a reservation.
4. Any State Party that has made a reservation in accordance with paragraph 3 of this article may at any time withdraw that reservation by notification to the Secretary-General of the United Nations.

Article 64

Signature, ratification, acceptance, approval and accession

1. This Convention shall be open to all States for signature in Hanoi in 2025 and thereafter at United Nations Headquarters in New York until 31 December 2026.
2. This Convention shall also be open for signature by regional economic integration organizations, provided that at least one member State of such an

organization has signed this Convention in accordance with paragraph 1 of this article.

3. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary-General of the United Nations. A regional economic integration organization may deposit its instrument of ratification, acceptance or approval if at least one of its member States has done likewise. In that instrument of ratification, acceptance or approval, such organization shall declare the extent of its competence with respect to the matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

4. This Convention is open for accession by any State or any regional economic integration organization of which at least one member State is a Party to this Convention. Instruments of accession shall be deposited with the Secretary-General of the United Nations. At the time of its accession, a regional economic integration organization shall declare the extent of its competence with respect to matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

Article 65

Entry into force

1. This Convention shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession. For the purpose of this paragraph, any instrument deposited by a regional economic integration organization shall not be counted as additional to those deposited by member States of that organization.

2. For each State or regional economic integration organization, ratifying, accepting, approving or acceding to this Convention after the deposit of the fortieth instrument of such action, this Convention shall enter into force on the thirtieth day after the date of deposit by such State or organization of the relevant instrument or on the date on which this Convention enters into force pursuant to paragraph 1 of this article, whichever is later.

Article 66

Amendment

1. After the expiry of five years from the entry into force of this Convention, a State Party may propose an amendment and transmit it to the Secretary-General of the United Nations, who shall thereupon communicate the proposed amendment to the States Parties and to the Conference of the States Parties to the Convention for the purpose of considering and deciding on the proposal. The Conference shall make every effort to achieve consensus on each amendment. If all efforts at consensus have been exhausted and no agreement has been reached, the amendment shall, as a last resort, require for its adoption a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference.

2. Regional economic integration organizations, in matters within their competence, shall exercise their right to vote under this article with a number of votes equal to the number of their member States that are Parties to this Convention. Such organizations shall not exercise their right to vote if their member States exercise theirs and vice versa.

3. An amendment adopted in accordance with paragraph 1 of this article is subject to ratification, acceptance or approval by States Parties.

4. An amendment adopted in accordance with paragraph 1 of this article shall enter into force in respect of a State Party 90 days after the date of the deposit with the Secretary-General of the United Nations of an instrument of ratification, acceptance or approval of such amendment.

5. When an amendment enters into force, it shall be binding on those States Parties that have expressed their consent to be bound by it. Other States Parties shall still be bound by the provisions of this Convention and any earlier amendments that they have ratified, accepted or approved.

Article 67

Denunciation

1. A State Party may denounce this Convention by written notification to the Secretary-General of the United Nations. Such denunciation shall become effective one year after the date of receipt of the notification by the Secretary-General.

2. A regional economic integration organization shall cease to be a Party to this Convention when all of its member States have denounced it.

3. Denunciation of this Convention in accordance with paragraph 1 of this article shall entail the denunciation of any protocols thereto.

Article 68

Depositary and languages

1. The Secretary-General of the United Nations is designated depositary of this Convention.

2. The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Secretary-General of the United Nations.

IN WITNESS WHEREOF, the undersigned plenipotentiaries, being duly authorized therein by their respective Governments, have signed this Convention.¹

Annex

Interpretative notes on specific articles of the United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

Article 2

1. The definition of the term “service provider” in article 2 (e) includes, in subparagraph (i), those entities that store or otherwise process electronic data on behalf of the users of the services set out in subparagraph (i). For example, under this definition, a service provider includes both services that provide hosting and caching services and services that provide a connection to a network. However, persons who merely use the service of a web hosting company to host their websites are not intended to be covered by this definition.

2. States parties are not obliged to reproduce verbatim in their domestic laws the same terminology defined in article 2 of this convention, provided that those laws

¹ It is noted that interpretative notes on articles 2, 17, 23 and 33 of this Convention were annexed by the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes to the report on its renewed concluding session, held from 29 July to 3 August 2024 in New York.

cover such concepts in a manner consistent with the principles and purposes of the convention and offer an equivalent framework for its implementation.

Article 17

3. In the framework of the convention, an offence shall only be deemed an offence under article 17 when the predicate offence is an offence established in accordance with articles 7 to 16 of the convention.

Articles 23 and 35, with regard to the term "investigation"

4. The term "criminal investigations" covers situations where there are reasonable grounds to believe, on the basis of factual circumstances, that a criminal offence (including an offence set out in article 19 of the convention) has been committed or is being committed, including when such an investigation is aimed at stopping or impeding the commission of the offence in question.

Article 35

5. Outside the convention, States parties may afford one another, in accordance with their international obligations, any other forms of international cooperation allowed by the domestic law of the requested State party, applicable mutual legal assistance treaties or equivalent arrangements.

CÔNG ƯỚC CỦA LIÊN HỢP QUỐC VỀ CHỐNG TỘI PHẠM MẠNG

Tổng cường hợp tác quốc tế nhằm đấu tranh với một số tội phạm được thực hiện thông qua hệ thống công nghệ thông tin và truyền thông và nhằm chia sẻ chứng cứ là dữ liệu điện tử của các tội phạm nghiêm trọng

LỜI NÓI ĐẦU

Các Quốc gia thành viên của Công ước này,

Ghi nhớ các mục đích và nguyên tắc của Hiến chương Liên hợp quốc,

Lưu ý rằng các công nghệ thông tin và truyền thông, mặc dù có tiềm năng to lớn cho sự phát triển của xã hội, nhưng cũng tạo ra cơ hội mới cho tội phạm, có thể góp phần làm gia tăng tỷ lệ và sự đa dạng của các hoạt động phạm tội, và có thể gây ảnh hưởng tiêu cực đến các Quốc gia, doanh nghiệp và đời sống của các cá nhân và toàn thể xã hội,

Quan ngại rằng việc sử dụng hệ thống công nghệ thông tin và truyền thông có thể có tác động đáng kể đến quy mô, tốc độ và phạm vi của các hành vi phạm tội, bao gồm cả các tội liên quan đến khủng bố và tội phạm có tổ chức xuyên quốc gia như buôn bán người, đưa người dôi cư trái phép, sản xuất trái phép và buôn lậu vũ khí, các bộ phận, thành phần và đạn dược, mua bán trái phép tra tủy và mua bán trái phép vật phẩm văn hóa,

Tin tưởng vào sự cần thiết của việc ưu tiên xây dựng chính sách tư pháp hình sự toàn cầu nhằm bảo vệ xã hội trước tội phạm mạng bằng cách, trong đó có, ban hành các quy định phù hợp, quy định hành vi cũng là tội phạm, thẩm quyền tố tụng tương tự và thúc đẩy hợp tác quốc tế nhằm ngăn ngừa và đấu tranh chống các hành vi phạm tội đó hiệu quả hơn ở cấp độ quốc gia, khu vực và quốc tế,

Kiên quyết xoá bỏ nơi ẩn náu an toàn cho các đối tượng thực hiện tội phạm mạng thông qua truy tố những tội phạm này dù chúng được thực hiện ở bất kỳ nơi nào,

Nhấn mạnh sự cần thiết phải tăng cường phối hợp và hợp tác giữa các Quốc gia bằng cách, trong đó, cung cấp hỗ trợ kỹ thuật và xây dựng năng lực, bao gồm chuyển giao công nghệ theo thỏa thuận chung, cho các nước, đặc biệt là các nước đang phát triển, khi có yêu cầu, để hoàn thiện chính sách và khuôn khổ pháp luật quốc gia và

tăng cường năng lực của các cơ quan có thẩm quyền để đối phó với mọi hình thức của tội phạm mạng, bao gồm cả việc phòng ngừa, phát hiện, điều tra và truy tố tội phạm đó, và trong bối cảnh này, nhấn mạnh vai trò của Liên hợp quốc,

Ghi nhận số lượng ngày càng tăng của nạn nhân tội phạm mạng, tầm quan trọng của việc bảo vệ công lý cho họ và sự cần thiết phải đáp ứng nhu cầu của những người ở trong tình trạng dễ bị tổn thương khi tiến hành các biện pháp phòng ngừa và đấu tranh chống các tội phạm được quy định tại Công ước này,

Kiên quyết phòng ngừa, phát hiện và ngăn chặn hiệu quả hơn sự chuyển dịch quốc tế của tài sản có được do thực hiện tội phạm mạng mà có, đồng thời tăng cường hợp tác quốc tế trong việc thu hồi và hoàn trả tài sản có phạm tội mà có phù hợp với Công ước này,

Ghi nhớ rằng phòng ngừa và đấu tranh chống tội phạm mạng là trách nhiệm của tất cả các Quốc gia và các Quốc gia phải hợp tác với nhau, với sự hỗ trợ và tham gia của các tổ chức quốc tế và khu vực liên quan, cũng như các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và các doanh nghiệp tư nhân nếu sự tham gia của họ trong lĩnh vực này mang lại hiệu quả,

Ghi nhận tầm quan trọng của việc lồng ghép vấn đề giới trong tất cả các nỗ lực liên quan đến phòng ngừa và đấu tranh chống các tội phạm được quy định tại Công ước này, phù hợp với luật pháp quốc gia,

Hiểu rằng cần phải đạt được hiệu quả trong thực thi pháp luật và đảm bảo tôn trọng quyền con người và các quyền tự do cơ bản như được ghi nhận trong các văn kiện quốc tế và khu vực có liên quan,

Nhận thức về quyền được bảo vệ đời sống riêng tư của mỗi người khỏi sự can thiệp tùy tiện hoặc bất hợp pháp, và tầm quan trọng của việc bảo vệ dữ liệu cá nhân,

Hoan nghênh công tác của Văn phòng Liên hợp quốc về Ma túy và Tội phạm, các tổ chức quốc tế và khu vực khác trong phòng ngừa và đấu tranh chống tội phạm mạng,

Nhắc lại Nghị quyết 74/247 ngày 27/12/2019 và Nghị quyết 75/282 ngày 26/5/2021 của Đại hội đồng,

Tính đến các điều ước quốc tế và khu vực hiện có về hợp tác trong lĩnh vực hình sự, cũng như các điều ước quốc tế tương tự đang có giữa các Quốc gia thành viên Liên hợp quốc,

Đã thống nhất như sau:

Chương I. Những quy định chung

Điều 1. Mục đích

Mục đích của Công ước này nhằm:

(a) Thúc đẩy và củng cố các biện pháp phòng ngừa và đấu tranh chống tội phạm mạng hiệu quả và hiệu lực hơn;

(b) Thúc đẩy, tạo thuận lợi và tăng cường hợp tác quốc tế trong phòng ngừa và đấu tranh chống tội phạm mạng; và

(c) Thúc đẩy, tạo thuận lợi hỗ trợ kỹ thuật và xây dựng năng lực phòng ngừa và đấu tranh chống tội phạm mạng, đặc biệt là vì lợi ích của các quốc gia đang phát triển.

Điều 2. Giải thích từ ngữ

Trong phạm vi Công ước này:

(a) “Hệ thống công nghệ thông tin và truyền thông” là bất cứ thiết bị hoặc nhóm thiết bị nào được kết nối với nhau hoặc có liên quan với nhau, mà các thiết bị đó, thu thập, lưu trữ và xử lý tự động dữ liệu điện tử bằng chương trình phần mềm;

(b) “Dữ liệu điện tử” là mọi hình thức biểu thị các dữ kiện, thông tin hoặc cấu trúc ở dạng phù hợp cho việc xử lý trong một hệ thống công nghệ thông tin và truyền thông, trong đó bao gồm cả chương trình phần mềm phù hợp để điều khiển một hệ thống công nghệ thông tin và truyền thông thực hiện một tác vụ;

(c) “Dữ liệu về lưu lượng” là mọi dữ liệu điện tử liên quan tới giao tiếp bằng một hệ thống công nghệ thông tin và truyền thông, được tạo ra bởi một hệ thống công nghệ thông tin và truyền thông đóng vai trò là một phần trong chuỗi giao tiếp, thể hiện nguồn gốc, đích đến, lộ trình, thời gian, ngày tháng, khối lượng, thời lượng hoặc loại hình của phương thức giao tiếp đó;

(d) “Dữ liệu về nội dung” là mọi dữ liệu điện tử không phải là thông tin thuê bao hoặc dữ liệu về lưu lượng, liên quan tới nội dung của dữ liệu được truyền tải bằng một hệ thống công nghệ thông tin và truyền thông, bao gồm nhưng không giới hạn ở hình ảnh, chữ viết, giọng nói, bản ghi âm và bản ghi hình;

(e) “Nhà cung cấp dịch vụ” là mọi thực thể công và tư mả:

(i) Cung cấp cho người sử dụng dịch vụ của mình tính năng giao tiếp thông qua một hệ thống công nghệ thông tin và truyền thông, hoặc

(ii) Xử lý hoặc lưu trữ dữ liệu điện tử nhân danh một dịch vụ viễn thông hoặc người sử dụng dịch vụ đó;

(f) “Thông tin thuê bao” là mọi thông tin mà nhà cung cấp dịch vụ nắm được, liên quan tới thuê bao của mình ngoài dữ liệu về nội dung hoặc dữ liệu lưu lượng, mà thông qua đó có thể xác định:

(i) Loại hình dịch vụ viễn thông được sử dụng, các điều kiện kỹ thuật có liên quan và thời gian sử dụng dịch vụ;

(ii) Định danh của thuê bao, địa chỉ bưu điện hoặc địa chỉ địa lý, số điện thoại hoặc số liên hệ khác, thông tin thanh toán, có sẵn trên cơ sở hợp đồng sử dụng dịch vụ;

(iii) Mọi thông tin khác về địa điểm lắp đặt thiết bị viễn thông, có sẵn trên cơ sở hợp đồng sử dụng dịch vụ;

(g) “Dữ liệu cá nhân” là mọi thông tin liên quan tới một con người cụ thể hoặc giúp xác định một con người cụ thể;

(h) “Tội phạm nghiêm trọng” là hành vi vi phạm có thể bị trừng phạt theo khung hình phạt từ ít nhất là 4 năm hoặc một hình phạt nặng hơn;

(i) “Tài sản” là mọi loại của cải, vật chất hay phi vật chất, động sản hay bất động sản, hữu hình hay vô hình, bao gồm tài sản số, và các văn bản pháp lý hay giấy tờ chứng minh quyền sở hữu hoặc lợi ích đối với tài sản đó,

(j) “Tài sản do phạm tội mà có” là bất kỳ tài sản bất nguồn hay có được một cách trực tiếp hay gián tiếp thông qua việc thực hiện một tội phạm;

(k) “Phong toá” hoặc “Thu giữ” là việc tạm thời cấm chuyển giao, chuyển đổi, định đoạt hay chuyển dịch tài sản hoặc việc tạm thời lưu giữ hay kiểm soát tài sản theo lệnh của toà án hay cơ quan có thẩm quyền khác;

(l) “Tịch thu”, kể cả việc tạm giữ khi thích hợp, nghĩa là việc vĩnh viễn tước đi tài sản theo lệnh của toà án hoặc cơ quan có thẩm quyền khác;

(m) “Tội phạm nguồn” là bất kỳ tội phạm nào mà tài sản có được từ tội phạm đó có thể trở thành đối tượng của tội phạm được quy định tại Điều 17 của Công ước này;

(n) “Tổ chức hội nhập kinh tế khu vực” là một tổ chức do các Quốc gia có chủ quyền trong một khu vực thành lập nên được các Quốc gia đó trao cho thẩm quyền đối với những vấn đề thuộc phạm vi điều chỉnh của Công ước này, được uỷ quyền hợp lệ, theo đúng những thủ tục nội bộ của tổ chức, để ký, phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập Công ước; “các Quốc gia thành viên” được đề cập đến trong Công ước này cũng sẽ được hiểu là bao gồm cả những tổ chức đó trong phạm vi thẩm quyền của họ;

(o) “Tình huống khẩn cấp” có nghĩa là một tình huống gây ra nguy hiểm nghiêm trọng và có thể xảy ra lập tức đối với tính mạng hoặc an toàn của một thể nhân.

Điều 3. Phạm vi áp dụng

Trừ trường hợp có quy định khác, Công ước này được áp dụng đối với:

(a) Việc phòng ngừa, điều tra và truy tố các hành vi phạm tội được quy định tại Công ước này, bao gồm việc phong toá, thu giữ, tịch thu và trả lại tài sản thu được từ các tội phạm đó;

(b) Việc thu thập, tiếp nhận, bảo quản và chuyển giao chứng cứ là dữ liệu điện tử nhằm mục đích điều tra hình sự hoặc truy tố, theo quy định tại các Điều 23 và 35 của Công ước này.

Điều 4. Các tội phạm quy định tại các công ước và nghị định thư khác của Liên hợp quốc

1. Để tạo điều kiện thực hiện các công ước Liên hợp quốc và nghị định thư liên quan mà các Quốc gia là Thành viên, các Quốc gia thành viên phải đảm bảo rằng các hành vi phạm tội được quy định theo các công ước và nghị định thư đó cũng được coi

là hành vi phạm tội theo pháp luật quốc gia nếu được thực hiện thông qua việc sử dụng các hệ thống công nghệ thông tin và truyền thông.

2. Điều này không được hiểu là tạo thành quy định về hành vi phạm tội lại Công ước này.

Điều 5. Bảo vệ chủ quyền

1. Các Quốc gia thành viên thực hiện nghĩa vụ trong Công ước này của mình theo cách thức phù hợp với các nguyên tắc về bình đẳng chủ quyền quốc gia và toàn vẹn lãnh thổ của các Quốc gia cũng như nguyên tắc không can thiệp vào công việc nội bộ của Quốc gia khác.

2. Không quy định nào trong Công ước này cho phép một Quốc gia thành viên được tiến hành trên lãnh thổ của quốc gia khác các hoạt động thực thi quyền tài phán và thi hành các chức năng chỉ dành riêng cho những cơ quan có thẩm quyền của quốc gia đó theo pháp luật quốc gia của họ.

Điều 6. Tôn trọng các quyền con người

1. Các Quốc gia thành viên bảo đảm việc thực hiện các nghĩa vụ của mình trong Công ước này phù hợp với các nghĩa vụ của quốc gia đó theo luật pháp quốc tế về quyền con người.

2. Không quy định nào trong Công ước này được giải thích là hạn chế các quyền con người và các quyền tự do cơ bản, bao gồm các quyền liên quan đến tự do ngôn luận, tôn giáo, tín ngưỡng, hội họp hòa bình và lập hội, theo quy định và phù hợp với luật pháp quốc tế về quyền con người có liên quan.

Chương II. Hình sự hóa

Điều 7. Truy cập trái phép

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định hành vi, khi được thực hiện cố ý và không được phép, truy cập vào toàn bộ hoặc một phần của hệ thống công nghệ thông tin và truyền thông là tội phạm theo pháp luật quốc gia của mình.

2. Một Quốc gia thành viên có thể yêu cầu tội phạm nêu trên phải được cấu thành bởi yếu tố là hành vi vi phạm các biện pháp bảo mật, với ý định thu thập dữ liệu điện tử hoặc gian lận cũng như ý định phạm tội khác hoặc có liên quan đến một hệ thống công nghệ thông tin và truyền thông được kết nối với một hệ thống công nghệ thông tin và truyền thông khác.

Điều 8. Chặn thu trái phép

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định hành vi, khi được thực hiện cố ý và không được phép, chặn thu bằng phương tiện kỹ thuật việc truyền dẫn dữ liệu điện tử không công khai đến, đi hoặc trong hệ thống công nghệ thông tin và truyền thông, bao gồm cả việc phát sóng điện từ từ hệ thống công nghệ thông tin và truyền thông mang dữ liệu điện tử đó, là tội phạm theo pháp luật quốc gia của mình.

2. Một Quốc gia thành viên có thể yêu cầu tội phạm nêu trên phải được cấu thành bởi yếu tố là khi được thực hiện với ý định phạm tội, hoặc có liên quan đến một hệ thống công nghệ thông tin và truyền thông được kết nối tới một hệ thống công nghệ thông tin và truyền thông khác.

Điều 9. Can thiệp vào dữ liệu điện tử

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác, để quy định hành vi, khi thực hiện một cách cố ý và không được phép, phá hoại, xóa, làm sai lệch, thay đổi, và nén dữ liệu điện tử, là tội phạm theo pháp luật quốc gia của mình.

2. Mỗi Quốc gia thành viên có thể yêu cầu hành vi phạm tội ở khoản 1 của Điều này gây ra hậu quả nghiêm trọng.

Điều 10 Can thiệp vào hệ thống công nghệ thông tin và truyền thông

Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định hành vi, khi thực hiện một cách cố ý và không được phép, cản trở nghiêm trọng đến việc vận hành của hệ thống công nghệ thông tin và truyền thông bằng cách nhập, truyền, phá hoại, xóa, làm sai lệch, thay đổi hoặc nén dữ liệu điện tử, là tội phạm theo pháp luật quốc gia của mình.

Điều 11. Lạm dụng các thiết bị

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác, để quy định là tội phạm theo luật pháp quốc gia của mình đối với các hành vi dưới đây, khi thực hiện cố ý và không được phép:

(a) Thu thập, sản xuất, bán, mua để sử dụng, nhập khẩu, phân phối hoặc bất kỳ cách nào để có được:

(i) Thiết bị, bao gồm một chương trình phần mềm, được thiết kế hoặc điều chỉnh chủ yếu nhằm mục đích thực hiện bất kỳ hành vi phạm tội nào được quy định từ Điều 7 đến Điều 10 của Công ước này; hoặc

(ii) Mật khẩu, thông tin truy cập, chữ ký điện tử hoặc dữ liệu tương tự mà qua đó toàn bộ hoặc một phần của hệ thống công nghệ thông tin và truyền thông có thể bị truy cập; nhằm mục đích sử dụng thiết bị, bao gồm chương trình phần mềm, hoặc mật khẩu, thông tin truy cập, chữ ký điện tử hoặc dữ liệu tương tự được sử dụng để thực hiện bất kỳ hành vi phạm tội nào được quy định từ Điều 7 đến Điều 10 của Công ước này; và

(b) Việc sở hữu thiết bị quy định tại khoản 1 (a) (i) hoặc (ii) của Điều này, với mục đích sử dụng thiết bị đó để thực hiện bất kỳ hành vi phạm tội nào được quy định từ Điều 7 đến Điều 10 của Công ước này

2. Điều này không quy định trách nhiệm hình sự đối với hành vi thu thập, sản xuất, mua, bán để sử dụng, nhập khẩu, phân phối hoặc bằng bất kỳ cách nào để có được, hoặc sở hữu theo khoản 1 của Điều này, mà không nhằm mục đích thực hiện tội phạm theo quy định từ Điều 7 đến Điều 10 của Công ước này, như để phục vụ cuộc thử nghiệm đã được cho phép hoặc sự bảo vệ theo uỷ quyền đối với hệ thống công nghệ thông tin và truyền thông.

3. Mỗi Quốc gia thành viên có thể bảo lưu quyền không áp dụng khoản 1 của Điều này, với điều kiện việc bảo lưu này không liên quan đến việc bán, phân phối hoặc bằng bất kỳ cách nào để có được các dữ liệu quy định trong khoản 1 (a) (ii) của Điều này.

Điều 12. Giả mạo liên quan đến hệ thống công nghệ thông tin và truyền thông

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác quy định là tội phạm theo pháp luật quốc gia của mình đối với hành vi nhập, thay đổi, xóa hoặc nén dữ liệu điện tử, khi được thực hiện một cách cố ý và không được phép, nhằm tạo ra dữ liệu không xác thực với mục đích dữ liệu này sẽ được ghi nhận hoặc xử lý như là dữ liệu xác thực trong các thủ tục pháp lý, bất kể dữ liệu này có thể đọc được và hiểu được trực tiếp hay không.

2. Một Quốc gia thành viên có thể yêu cầu hành vi phạm tội nêu trên phải nhằm mục đích lừa đảo hoặc gian lận hoặc mục đích phạm tội tương tự trước khi truy cứu trách nhiệm hình sự.

Điều 13. Trộm cắp hoặc lừa đảo liên quan đến hệ thống công nghệ thông tin và truyền thông

Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định là tội phạm theo pháp luật quốc gia của mình đối với hành vi gây thiệt hại về tài sản cho người khác, khi thực hiện một cách cố ý và không được phép, bằng cách:

(a) Nhập, thay đổi, xóa hoặc nén dữ liệu điện tử;

(b) Can thiệp vào hoạt động của hệ thống công nghệ thông tin và truyền thông;

(c) Lừa đảo về hoàn cảnh được tổ chức qua hệ thống công nghệ thông tin và truyền thông dẫn đến việc một người thực hiện hoặc không thực hiện một việc mà lẽ ra người đó không thực hiện như vậy;

với mục đích lừa đảo hoặc gian lận để thu lợi trái phép cho bản thân hoặc cho người khác bằng tiền hoặc tài sản khác.

Điều 14. Tội phạm liên quan đến tài liệu có nội dung xâm hại hoặc bóc lột tình dục trẻ em trực tuyến

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định là tội phạm theo pháp luật quốc gia của mình đối với hành vi sau, khi thực hiện một cách cố ý và không được phép:

(a) Sản xuất, phát tán, bán, phân phối, truyền tải, phát sóng, hiển thị, xuất bản hoặc bằng bất kỳ cách nào khác cung cấp tài liệu có nội dung xâm hại hoặc bóc lột tình dục trẻ em thông qua hệ thống công nghệ thông tin và truyền thông;

(b) Chào mời, thu mua hoặc truy cập tài liệu có nội dung xâm hại hoặc bóc lột tình dục trẻ em qua hệ thống công nghệ thông tin và truyền thông;

(c) Tàng trữ hoặc quản lý việc lưu trữ tài liệu có nội dung xâm hại hoặc bóc lột tình dục trẻ em được lưu trữ trong hệ thống công nghệ thông tin và truyền thông hoặc thiết bị lưu trữ khác;

(d) Tài trợ cho các tội phạm được quy định theo các điểm (a) đến (c) của khoản này, tuy nhiên các Quốc gia thành viên có thể quy định đây là một tội phạm riêng biệt.

1. Vì mục đích của điều này, thuật ngữ “tài liệu có nội dung xâm hại hoặc bóc lột tình dục trẻ em” bao gồm tài liệu hình ảnh, và có thể bao gồm nội dung bằng văn bản hoặc âm thanh, trong đó mô tả, miêu tả hoặc thể hiện bất kỳ người nào dưới 18 tuổi:

(a) Thực hiện hành vi tình dục thật hoặc mô phỏng;

(b) Chứng kiến bất kỳ người nào đang có quan hệ tình dục;

(c) Các bộ phận sinh dục của người đó bị phô bày với mục đích chủ yếu là tình dục; hoặc

(d) Bị tra tấn hoặc trừng phạt hoặc đối xử tàn ác, vô nhân đạo hoặc hạ nhục và tài liệu đó có tính chất tình dục.

2. Một Quốc gia thành viên có thể yêu cầu tài liệu được quy định trong khoản 2 của Điều này chỉ bao gồm các tài liệu mà:

(a) Mô tả, miêu tả hoặc thể hiện một người có thật; hoặc

(b) Mô tả bằng hình ảnh việc xâm hại hoặc bóc lột tình dục trẻ em.

3. Theo pháp luật quốc gia của mình và phù hợp với các nghĩa vụ quốc tế hiện hành có liên quan, các Quốc gia thành viên có thể thực hiện các bước để loại trừ việc hình sự hóa:

(a) Hành vi do trẻ em tự tạo ra tài liệu mô tả chính mình; hoặc

(b) Việc sản xuất, truyền tải hoặc sở hữu tài liệu có đồng thuận được quy định tại khoản 2 (a) đến (c) của điều này, khi các hành vi này là hợp pháp theo pháp luật quốc gia, và tài liệu đó được giữ hoàn toàn cho mục đích cá nhân và theo đồng thuận của các cá nhân liên quan.

4. Không quy định nào trong Công ước này ảnh hưởng đến bất kỳ nghĩa vụ quốc tế nào có lợi hơn cho việc thực hiện các quyền của trẻ em.

Điều 15. Hành vi dụ dỗ hoặc lôi kéo nhằm thực hiện tội phạm tình dục đối với trẻ em

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác, để quy định là tội phạm theo pháp luật quốc gia của mình, đối với hành vi cố ý liên lạc, dụ dỗ, lôi kéo hoặc thực hiện bất kỳ thỏa thuận nào qua hệ thống công nghệ thông tin và truyền thông nhằm mục đích thực hiện hành vi phạm tội tình dục đối với trẻ em, theo quy định trong pháp luật quốc gia, bao gồm cả việc thực hiện bất kỳ tội phạm nào được quy định theo Điều 14 của Công ước này.

2. Một Quốc gia thành viên có thể yêu cầu tội phạm nêu trên phải có hành động đến cùng đối với các hành vi phạm tội nêu tại khoản 1 của Điều này.

3. Một Quốc gia thành viên có thể xem xét việc mở rộng hình sự hóa theo khoản 1 của Điều này đối với các hành vi dụ dỗ và lôi kéo một người được cho là trẻ em.

4. Các Quốc gia thành viên có thể thực hiện các bước để loại trừ việc hình sự hóa hành vi như được mô tả trong khoản 1 của điều này khi hành vi đó được thực hiện bởi trẻ em.

Điều 16. Phát tán hình ảnh riêng tư mà không có sự đồng ý

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định là tội phạm theo pháp luật quốc gia của mình, đối với hành vi, khi thực hiện: một cách cố ý và không được phép, bán, phân phối, truyền tải, xuất bản hoặc bằng bất kỳ cách nào khác cung cấp hình ảnh riêng tư của một người qua hệ thống công nghệ thông tin và truyền thông mà không có sự đồng ý của người được mô tả trong hình ảnh đó.

2. Vì mục đích khoản 1 của Điều này, “hình ảnh riêng tư” là một bản ghi hình của một người trên 18 tuổi được thực hiện bằng bất kỳ phương tiện nào, bao gồm ảnh chụp hoặc ghi hình, có tính chất tình dục, trong đó các bộ phận sinh dục của người bị phơi bày hoặc người đó đang quan hệ tình dục, mà vào thời điểm ghi hình, hoạt động đó là riêng tư và người hoặc những người được mô tả luôn có kỳ vọng hợp lý về quyền riêng tư vào thời điểm hành vi phạm tội diễn ra.

3. Một Quốc gia thành viên có thể mở rộng định nghĩa về hình ảnh riêng tư, nếu phù hợp, để bao gồm hình ảnh của người dưới 18 tuổi nếu họ đủ tuổi theo pháp luật quốc gia để tham gia vào quan hệ tình dục và hình ảnh đó không mô tả việc xâm hại hoặc bóc lột trẻ em.

4. Vì mục đích của Điều này, một người dưới 18 tuổi và được mô tả trong một hình ảnh riêng tư không thể đồng ý cho việc phát tán một hình ảnh riêng tư mà hình ảnh đó cấu thành tội liệu xâm hại hoặc bóc lột tình dục trẻ em theo Điều 14 của Công ước này.

5. Một Quốc gia thành viên có thể yêu cầu hành vi vi phạm nêu trên phải có mục đích gây tổn hại trước khi truy cứu trách nhiệm hình sự.

6. Các Quốc gia thành viên có thể áp dụng các biện pháp khác đối với các vấn đề liên quan đến Điều này, theo pháp luật quốc gia của mình và phù hợp với các nghĩa vụ quốc tế hiện hành có liên quan.

Điều 17. Rửa tiền đối với tài sản do phạm tội mà có

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác, theo các nguyên tắc của pháp luật quốc gia của mình, để quy định là tội phạm đối với hành vi sau đây, khi thực hiện một cách cố ý:

(a) (i) Chuyển đổi hay chuyển nhượng tài sản, dù đã biết đó là tài sản do phạm tội mà có, nhằm che giấu hoặc ngụy trang nguồn gốc bất hợp pháp của tài sản đó hoặc nhằm giúp đỡ bất kỳ ai có liên quan đến việc thực hiện tội phạm nguồn để lẩn tránh trách nhiệm pháp lý đối với hành vi của người này;

(ii) Che giấu hoặc ngụy trang bản chất thực sự, nguồn gốc, địa điểm, sự chuyển nhượng, sự vận chuyển hoặc sở hữu hoặc các quyền liên quan đến tài sản, dù đã biết tài sản đó do phạm tội mà có;

(b) Theo các khái niệm cơ bản của hệ thống pháp luật quốc gia mình:

(i) Chiếm hữu, tàng trữ hoặc sử dụng tài sản mà tại thời điểm nhận đã biết rằng tài sản đó do phạm tội mà có;

(ii) Tham gia, phối hợp với hoặc lập kế hoạch thực hiện hành vi, cố gắng thực hiện hành vi hay hỗ trợ, xúi giục, tạo điều kiện và giúp sức thực hiện bất kỳ tội phạm nào quy định tại Điều này.

2. Vì mục đích thực hiện hoặc áp dụng khoản 1 của Điều này:

(a) Mỗi Quốc gia thành viên xác định tội phạm nguồn liên quan đến các tội phạm được quy định theo các Điều 7 đến 16 của Công ước này;

(b) Trong trường hợp các Quốc gia thành viên có pháp luật quy định danh sách các tội phạm nguồn cụ thể, quốc gia đó có trách nhiệm tối thiểu phải bổ sung đầy đủ các tội phạm được quy định theo các Điều 7 đến 16 của Công ước này vào danh sách các tội phạm nguồn;

(c) Vì mục đích của điểm (b) của khoản này, các tội phạm nguồn bao gồm các tội phạm thực hiện trong và ngoài phạm vi tài phán của Quốc gia thành viên có liên quan. Tuy nhiên, các tội phạm thực hiện ngoài phạm vi tài phán của một Quốc gia thành viên chỉ cấu thành các tội phạm nguồn khi hành vi tương ứng là hành vi phạm tội theo pháp luật quốc gia của nơi hành vi đó được thực hiện và cũng là hành vi phạm tội theo pháp luật của Quốc gia thành viên đang thực hiện hoặc áp dụng điều này nếu tội phạm đó được thực hiện ở đó;

(d) Mỗi Quốc gia thành viên sẽ cung cấp bản sao các văn bản pháp luật cho phép thực hiện Điều này cùng các thay đổi sau đó của các văn bản pháp luật này hoặc một bản mô tả các văn bản đó cho Tổng thư ký Liên hợp quốc;

(e) Nếu các nguyên tắc cơ bản của pháp luật quốc gia của Quốc gia thành viên yêu cầu, các tội phạm được quy định trong khoản 1 của Điều này không áp dụng cho những người thực hiện tội phạm nguồn;

(f) Sự nhận thức rõ ràng, ý định hoặc mục đích khi được quy định là dấu hiệu pháp lý cần thiết của một tội phạm được quy định trong khoản 1 của Điều này có thể được suy ra từ các tình tiết thực tế khách quan.

Điều 18. Trách nhiệm pháp lý của pháp nhân

1. Mỗi Quốc gia Thành viên áp dụng các biện pháp cần thiết để quy định trách nhiệm pháp lý của pháp nhân, phù hợp với các nguyên tắc pháp luật của mình, về việc tham gia thực hiện các tội phạm được quy định theo Công ước này.
2. Phù thuộc vào các nguyên tắc pháp luật của Quốc gia thành viên, trách nhiệm pháp lý của pháp nhân có thể là trách nhiệm hình sự, dân sự hoặc hành chính.
3. Trách nhiệm pháp lý của pháp nhân không ảnh hưởng đến trách nhiệm hình sự của các cá nhân đã thực hiện tội phạm.
4. Cụ thể, mỗi Quốc gia thành viên bảo đảm các pháp nhân chịu trách nhiệm theo quy định của Điều này phải chịu chế tài hình sự hoặc phi hình sự hiệu quả, tương xứng và có tác dụng ngăn ngừa, bao gồm phạt tiền.

Điều 19. Đồng phạm và phạm tội chưa đạt

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác, để quy định là tội phạm theo pháp luật quốc gia của mình đối với hành vi, khi thực hiện một cách cố ý, tham gia thực hiện một tội phạm được quy định tại Công ước này với bất kỳ vai trò nào, như đồng phạm, giúp sức hoặc xúi giục.
2. Mỗi Quốc gia thành viên có thể áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định là tội phạm theo pháp luật quốc gia của mình đối với hành vi cố ý thực hiện tội phạm được quy định tại Công ước này nhưng chưa đạt.
3. Mỗi Quốc gia thành viên có thể áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định là tội phạm theo pháp luật quốc gia của mình đối với hành vi cố ý chuẩn bị thực hiện tội phạm theo quy định của Công ước này.

Điều 20. Thời hiệu

Phù hợp với pháp luật quốc gia của mình, khi thích hợp, trên cơ sở mức độ nghiêm trọng của tội phạm, mỗi Quốc gia thành viên quy định về thời hiệu đủ dài để bắt đầu quá trình tố tụng đối với bất kỳ tội phạm nào được quy định tại Công ước này, và quy định về thời hiệu dài hơn hoặc quy định không áp dụng thời hiệu khi người bị buộc tội lần tránh quá trình tố tụng.

Điều 21 Truy tố, xét xử và hình phạt

1. Mỗi Quốc gia thành viên bảo đảm các tội phạm được quy định tại Công ước này phải chịu các hình phạt hiệu quả, tương xứng và có tác dụng ngăn ngừa, có tính đến mức độ nghiêm trọng của tội phạm đó.
2. Mỗi Quốc gia thành viên có thể áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định các tình tiết tăng nặng theo pháp luật quốc gia của mình, liên quan đến các tội phạm được quy định tại Công ước này, bao gồm các tình tiết có ảnh hưởng đến cơ sở hạ tầng thông tin trong yếu.
3. Mỗi Quốc gia thành viên nỗ lực bảo đảm các quyền thực thi pháp luật độc lập theo quy định của pháp luật quốc gia liên quan đến việc truy tố những người thực hiện tội phạm được quy định tại Công ước này đều được thực hiện để tối đa hoá hiệu quả của các biện pháp thực thi pháp luật xử lý các tội phạm trên và tôn trọng đúng mức sự cần thiết phải ngăn chặn các tội phạm đó.
4. Mỗi Quốc gia thành viên bảo đảm rằng bất kỳ người nào bị truy tố vì các tội phạm được quy định tại Công ước này đều được hưởng tất cả các quyền và biện pháp bảo đảm phù hợp với luật pháp quốc gia của mình và phù hợp với các nghĩa vụ quốc tế của Quốc gia thành viên, bao gồm quyền được xét xử công bằng và quyền bào chữa.
5. Đối với các tội phạm được quy định tại Công ước này, căn cứ vào pháp luật quốc gia và tôn trọng đúng mức quyền bào chữa, mỗi Quốc gia thành viên có các biện pháp thích hợp để bảo đảm các điều kiện được đặt ra đối với những quyết định miễn việc tạm giam trong thời gian chờ xét xử hoặc kháng cáo phải tính đến yêu cầu bảo đảm sự có mặt của bị cáo trong quá trình tố tụng hình sự sau đó.
6. Mỗi Quốc gia thành viên tính đến mức độ nghiêm trọng của các tội phạm có liên quan khi cần nhắc thực hiện tha tù trước thời hạn hoặc đặc xá cho người bị kết án về tội phạm này.
7. Các Quốc gia thành viên bảo đảm rằng các biện pháp thích hợp được áp dụng theo pháp luật quốc gia của mình để bảo vệ trẻ em bị cáo buộc thực hiện các tội phạm được quy định tại Công ước này, phù hợp với các nghĩa vụ theo Công

ước về Quyền Trẻ em và các Nghị định thư có liên quan, cũng như các điều ước quốc tế hoặc khu vực khác có thể áp dụng.

8. Không quy định nào trong Công ước này ảnh hưởng đến nguyên tắc là việc quy định tội phạm được quy định tại Công ước này và các quy định về bảo chữa hay các nguyên tắc pháp lý khác về tính hợp pháp của hành vi phải được đánh cho pháp luật quốc gia của Quốc gia thành viên và các tội phạm này phải bị truy tố và xử phạt theo quy định của pháp luật quốc gia đó.

Chương III. Quyền tài phán

Điều 22. Quyền tài phán

1. Mỗi Quốc gia thành viên áp dụng các biện pháp cần thiết để thiết lập quyền tài phán của mình đối với các tội phạm được quy định tại Công ước này khi:

(a) Hành vi phạm tội đó được thực hiện trên lãnh thổ của Quốc gia thành viên đó; hoặc

(b) Hành vi phạm tội đó được thực hiện trên tàu mang cờ của Quốc gia thành viên đó hoặc trên máy bay đăng ký theo luật của Quốc gia thành viên đó vào thời điểm xảy ra hành vi phạm tội.

2. Theo quy định tại Điều 5 của Công ước này, một Quốc gia thành viên cũng có thể thiết lập quyền tài phán của mình đối với bất kỳ hành vi phạm tội nào khi:

(a) Hành vi phạm tội được thực hiện nhằm chống lại một công dân của Quốc gia thành viên đó; hoặc

(b) Hành vi phạm tội được thực hiện bởi một công dân của Quốc gia thành viên đó hoặc bởi một người không quốc tịch thường trú trên lãnh thổ của Quốc gia thành viên đó; hoặc

(c) Hành vi phạm tội là một trong các hành vi được quy định tại Điều 17, khoản 1 (b) (ii) của Công ước này và được thực hiện bên ngoài lãnh thổ của Quốc gia thành viên đó nhằm mục đích thực hiện một hành vi phạm tội theo quy định tại Điều 17, khoản 1 (a) (i) hoặc (ii) hoặc (b) (i) của Công ước này trong phạm vi lãnh thổ của Quốc gia thành viên đó; hoặc

(d) Hành vi phạm tội được thực hiện nhằm chống lại Quốc gia thành viên đó.

3. Vì mục đích của Điều 37, khoản 11 của Công ước này, mỗi Quốc gia thành viên áp dụng các biện pháp cần thiết để thiết lập quyền tài phán của mình đối với các hành vi phạm tội được quy định tại Công ước này khi người bị tình nghi phạm tội có mặt trên lãnh thổ nước mình và không dẫn độ người đó chỉ với lý do người đó là công dân của quốc gia mình.

4. Mỗi Quốc gia thành viên cũng có thể áp dụng các biện pháp cần thiết để thiết lập quyền tài phán của mình đối với các hành vi phạm tội được quy định tại Công ước này khi người bị tình nghi phạm tội đang có mặt trên lãnh thổ quốc gia mình và quốc gia đó không dẫn độ người này.

5. Nếu một Quốc gia thành viên thực hiện quyền tài phán của mình theo khoản 1 hoặc 2 của Điều này đã được thông báo, hoặc đã biết theo cách khác, rằng một Quốc gia thành viên khác đang tiến hành điều tra, truy tố hoặc xét xử đối với cùng một hành vi, khi phù hợp, các cơ quan có thẩm quyền của các Quốc gia thành viên này tham khảo với nhau nhằm phối hợp hành động.

6. Không ảnh hưởng tới các nguyên tắc của pháp luật quốc tế nói chung, Công ước này không loại trừ việc thực hiện quyền tài phán hình sự do một Quốc gia thành viên quy định phù hợp với pháp luật của quốc gia đó.

Chương IV. Các biện pháp tố tụng và thực thi pháp luật

Điều 23. Phạm vi của các biện pháp tố tụng

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định quyền hạn và thủ tục được quy định trong Chương này nhằm mục đích tiến hành các hoạt động điều tra hoặc tố tụng hình sự cụ thể.

2. Trừ khi có quy định khác trong Công ước này, mỗi Quốc gia thành viên áp dụng quyền hạn và thủ tục được nêu ở khoản 1 Điều này đối với:

(a) Các tội phạm được quy định tại Công ước này;

(b) Các tội phạm hình sự khác được thực hiện thông qua hệ thống công nghệ thông tin và truyền thông; và

(c) Việc thu thập chứng cứ lá dữ liệu điện tử của bất kỳ tội phạm nào

3. (a) Mỗi Quốc gia thành viên có thể bảo lưu quyền chỉ áp dụng các biện pháp được quy định tại Điều 29 của Công ước này đối với các tội phạm hoặc danh mục các loại tội phạm được nêu cụ thể trong tuyên bố bảo lưu, với điều kiện phạm vi các tội phạm hoặc các loại tội phạm đó không hạn chế hơn phạm vi của các tội phạm mà quốc gia đó áp dụng các biện pháp được quy định tại Điều 30 của Công ước này. Mỗi Quốc gia Thành viên cần nhắc việc hạn chế bảo lưu này để có thể áp dụng tối đa các biện pháp được quy định tại Điều 29;

(b) Trong trường hợp một Quốc gia thành viên, do hạn chế trong các quy định pháp luật quốc gia đang có hiệu lực tại thời điểm thông qua Công ước này, không thể áp dụng các biện pháp được quy định tại các Điều 29 và 30 của Công ước đối với thông tin liên lạc đang được truyền tải trong hệ thống công nghệ thông tin và truyền thông của một nhà cung cấp dịch vụ mà:

(i) Đang được hoạt động vì lợi ích của một nhóm người dùng nhất định; và

(ii) Không sử dụng các mạng máy tính, mạng viễn thông công cộng và không được kết nối với một hệ thống công nghệ thông tin và truyền thông khác, dù thuộc công cộng hay tư nhân;

Quốc gia thành viên đó có thể bảo lưu quyền không áp dụng các biện pháp này đối với thông tin liên lạc đó. Mỗi Quốc gia thành viên cần nhắc việc hạn chế bảo lưu này để có thể áp dụng tối đa các biện pháp được quy định tại các Điều 29 và 30 của Công ước này.

Điều 24 Các tiêu chuẩn và biện pháp bảo đảm

1. Mỗi Quốc gia Thành viên bảo đảm rằng việc quy định, thực hiện và áp dụng quyền hạn và thủ tục được quy định tại Chương này tuân thủ các tiêu chuẩn và biện pháp bảo đảm được quy định trong pháp luật quốc gia của mình, trong đó có quy định về bảo vệ quyền con người, phù hợp với các nghĩa vụ theo pháp luật quốc tế về quyền con người, và bao gồm nguyên tắc tương xứng.

2. Theo quy định và phù hợp với pháp luật của mỗi Quốc gia thành viên, các tiêu chuẩn và biện pháp bảo đảm này bao gồm, trong số những điều khác, tùy theo tính chất của thủ tục

hoặc quyền hạn có liên quan, cơ chế giám sát tư pháp hoặc cơ chế giám sát độc lập khác, quyền được hưởng một biện pháp khắc phục hiệu quả, các căn cứ để áp dụng, giới hạn phạm vi và thời hiệu của quyền hạn hoặc thủ tục đó.

3. Trong phạm vi phù hợp với lợi ích công cộng, đặc biệt là việc thực thi pháp luật đúng đắn, mỗi Quốc gia thành viên xem xét tác động của quyền hạn và thủ tục nêu tại Chương này đối với quyền, trách nhiệm và lợi ích hợp pháp của các bên thứ ba.

4. Các tiêu chuẩn và biện pháp bảo đảm quy định tại Điều này được áp dụng đối với quyền hạn và thủ tục được quy định trong Chương này ở cấp độ quốc gia, cho cả mục đích điều tra và xét xử hình sự trong nước và mục đích hợp tác quốc tế mà Quốc gia thành viên được yêu cầu phải thực hiện.

5. Các dẫn chiếu đến cơ chế giám sát tư pháp hoặc các cơ chế giám sát độc lập khác trong khoản 2 của Điều này là các cơ chế giám sát của quốc gia.

Điều 25. Bảo quản khẩn cấp dữ liệu điện tử đã lưu trữ

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để cho phép các cơ quan có thẩm quyền của mình yêu cầu hoặc bằng cách tương tự, có được việc bảo quản khẩn cấp dữ liệu điện tử cụ thể, bao gồm dữ liệu về lưu lượng, dữ liệu về nội dung và thông tin thuê bao, đã được lưu trữ bằng hệ thống công nghệ thông tin và truyền thông, đặc biệt là khi có căn cứ để tin rằng dữ liệu điện tử đó đặc biệt dễ bị mất hoặc bị sửa đổi.

2. Khi một Quốc gia thành viên thực hiện khoản 1 của Điều này bằng cách yêu cầu một người bảo quản dữ liệu điện tử cụ thể đã lưu trữ thuộc sự chiếm hữu hoặc quản lý của người đó, Quốc gia thành viên đó áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để quy định người đó có trách nhiệm bảo quản và duy trì tính toàn vẹn của dữ liệu điện tử đó trong một khoảng thời gian cần thiết, tối đa là 90 ngày, để cho phép các cơ quan có thẩm quyền có được các thông tin từ dữ liệu. Một Quốc gia thành viên có thể quy định về việc gia hạn yêu cầu nói trên.

3. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để buộc người quản lý hoặc người khác có trách nhiệm bảo quản dữ liệu

điện tử phải giữ bí mật việc thực hiện các thủ tục đó trong khoảng thời gian được quy định trong pháp luật quốc gia của mình.

Điều 26. Bảo quản khẩn cấp và tiết lộ một phần dữ liệu về lưu lượng

Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác đối với dữ liệu về lưu lượng được bảo quản theo quy định tại Điều 25 của Công ước này để:

(a) Bảo đảm rằng việc bảo quản khẩn cấp dữ liệu về lưu lượng có thể thực hiện được bất kể có một hoặc nhiều nhà cung cấp dịch vụ tham gia vào quá trình truyền tải thông tin liên lạc;

(b) Bảo đảm việc tiết lộ một phần cho cơ quan có thẩm quyền của Quốc gia thành viên, hoặc người được cơ quan đó chỉ định, một lượng dữ liệu về lưu lượng đủ để Quốc gia thành viên xác định các nhà cung cấp dịch vụ và con đường truyền tải thông tin liên lạc.

Điều 27. Yêu cầu cung cấp dữ liệu

Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để cho phép các cơ quan có thẩm quyền của mình yêu cầu:

(a) Một người trên lãnh thổ của mình cung cấp dữ liệu điện tử cụ thể thuộc chiếm hữu và quản lý của người đó, được lưu trữ trong hệ thống công nghệ thông tin và truyền thông hoặc phương tiện lưu trữ dữ liệu điện tử; và

(b) Một nhà cung cấp dịch vụ trên lãnh thổ của Quốc gia thành viên cung cấp thông tin về thuê bao sử dụng dịch vụ thuộc chiếm hữu hoặc quản lý của nhà cung cấp dịch vụ đó.

Điều 28. Khám xét và thu giữ dữ liệu điện tử đã lưu trữ

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để cho phép các cơ quan có thẩm quyền của mình thực hiện khám xét hoặc truy cập vào:

(a) Một hệ thống công nghệ thông tin và truyền thông, một phần của hệ thống đó, và dữ liệu điện tử được lưu trữ trong đó; và

(b) Một phương tiện lưu trữ dữ liệu điện tử đang lưu trữ dữ liệu điện tử cần tìm;

trên lãnh thổ của Quốc gia thành viên đó.

2. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để bảo đảm rằng, khi các cơ quan có thẩm quyền của mình khám xét hoặc truy cập vào một hệ thống công nghệ thông tin và truyền thông cụ thể hoặc một phần của hệ thống đó, theo quy định tại Khoản 1 (a) của Điều này, và có căn cứ để tin rằng dữ liệu điện tử cần tìm được lưu trữ trong một hệ thống công nghệ thông tin và truyền thông khác hoặc một phần của hệ thống đó trên lãnh thổ của mình, và dữ liệu đó có thể được truy cập hợp pháp từ hệ thống ban đầu, các cơ quan đó có thể nhanh chóng tìm kiếm quyền truy cập vào hệ thống công nghệ thông tin và truyền thông khác đó.

3. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để cho phép các cơ quan có thẩm quyền của mình thu giữ hoặc niêm phong dữ liệu điện tử trên lãnh thổ của mình được truy cập theo quy định tại khoản 1 hoặc 2 của Điều này. Các biện pháp này bao gồm:

(a) Thu giữ hoặc áp dụng biện pháp tương tự với một hệ thống công nghệ thông tin và truyền thông hoặc một phần của nó, hoặc một phương tiện lưu trữ dữ liệu điện tử;

(b) Sao lưu dữ liệu điện tử đó dưới dạng điện tử;

(c) Bảo đảm và duy trì tính toàn vẹn của dữ liệu điện tử đã lưu trữ có liên quan;

(d) Không cho phép truy cập hoặc loại bỏ dữ liệu điện tử trong hệ thống công nghệ thông tin và truyền thông đó.

4. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để cho phép các cơ quan có thẩm quyền của mình yêu cầu bất kỳ cá nhân nào biết về cách thức hoạt động của hệ thống công nghệ thông tin và truyền thông đang được xem xét, mạng thông tin và viễn thông, các bộ phận cấu thành của chúng, hoặc các biện pháp bảo vệ dữ liệu điện tử, cung cấp thông tin cần thiết, trong phạm vi hợp lý, để thực hiện các biện pháp được đề cập tại các khoản 1 đến 3 của Điều này.

Điều 29. Thu thập dữ liệu về lưu lượng theo thời gian thực

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để cho phép các cơ quan có thẩm quyền của mình:

(a) Thu thập hoặc ghi lại, thông qua việc sử dụng các phương tiện kỹ thuật trên lãnh thổ của Quốc gia thành viên đó; và

(b) Yêu cầu một nhà cung cấp dịch vụ, trong khả năng kỹ thuật của mình:

(i) Thu thập hoặc ghi lại, thông qua việc sử dụng các phương tiện kỹ thuật trên lãnh thổ của Quốc gia thành viên đó; hoặc

(ii) Hợp tác và hỗ trợ các cơ quan có thẩm quyền trong việc thu thập hoặc ghi lại;

dữ liệu về lưu lượng, theo thời gian thực, liên quan đến các thông tin liên lạc cụ thể trên lãnh thổ của mình được truyền tải bằng hệ thống công nghệ thông tin và truyền thông.

2. Trong trường hợp một Quốc gia thành viên không thể thực hiện các biện pháp được nêu tại khoản 1 (a) của Điều này do các quy định của pháp luật quốc gia của mình, Quốc gia đó có thể áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để bảo đảm việc thu thập hoặc ghi lại theo thời gian thực dữ liệu về lưu lượng liên quan đến các thông tin liên lạc cụ thể được truyền tải trên lãnh thổ của mình, thông qua việc sử dụng các phương tiện kỹ thuật trên lãnh thổ của Quốc gia thành viên đó.

3. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để yêu cầu một nhà cung cấp dịch vụ giữ bí mật về việc thực hiện bất kỳ thẩm quyền nào được quy định trong Điều này và bất kỳ thông tin nào có liên quan.

Điều 30. Chặn thu dữ liệu về nội dung

1. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác, liên quan đến các tội phạm nghiêm trọng được quy định tại pháp luật quốc gia của mình, để cho phép các cơ quan có thẩm quyền của mình:

(a) Thu thập hoặc ghi lại, thông qua việc sử dụng các phương tiện kỹ thuật trên lãnh thổ của Quốc gia thành viên đó; và

(b) Yêu cầu một nhà cung cấp dịch vụ, trong khả năng kỹ thuật của mình:

(i) Thu thập hoặc ghi lại, thông qua việc sử dụng các phương tiện kỹ thuật trên lãnh thổ của Quốc gia thành viên đó; hoặc

(ii) Hợp tác và hỗ trợ các cơ quan có thẩm quyền trong việc thu thập hoặc ghi lại; dữ liệu về nội dung, theo thời gian thực, của các thông tin liên lạc cụ thể trên lãnh thổ của mình được truyền tải bằng hệ thống công nghệ thông tin và truyền thông.

2. Trong trường hợp một Quốc gia thành viên không thể thực hiện các biện pháp được nêu tại khoản 1 (a) của điều này do các quy định pháp luật quốc gia của mình, Quốc gia đó có thể áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để đảm bảo việc thu thập hoặc ghi lại theo thời gian thực dữ liệu về nội dung liên quan đến các thông tin liên lạc cụ thể được truyền tải trên lãnh thổ của mình, thông qua việc sử dụng các phương tiện kỹ thuật trên lãnh thổ của Quốc gia thành viên đó.

3. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và các biện pháp cần thiết khác để yêu cầu một nhà cung cấp dịch vụ giữ bí mật về việc thực hiện bất kỳ thẩm quyền nào được quy định trong Điều này và bất kỳ thông tin nào có liên quan.

Điều 31. Phong toà, thu giữ và tịch thu tài sản do phạm tội mà có

1. Trong phạm vi rộng nhất được pháp luật quốc gia cho phép, mỗi Quốc gia thành viên áp dụng các biện pháp cần thiết cho phép tịch thu:

(a) Tài sản do phạm tội mà có có nguồn gốc từ các tội phạm được quy định tại Công ước này hoặc tài sản có giá trị tương đương với giá trị của tài sản do phạm tội mà có nêu trên;

(b) Tài sản, trang thiết bị hoặc công cụ khác được sử dụng hoặc sẽ được sử dụng để thực hiện hành vi phạm tội quy định tại Công ước này.

2. Mỗi Quốc gia thành viên áp dụng các biện pháp cần thiết cho phép xác định, truy tìm, phong toà hoặc thu giữ bất kỳ tài sản nào quy định tại khoản 1 của Điều này để thực hiện mục đích cuối cùng là tịch thu.

3. Mỗi Quốc gia thành viên áp dụng các biện pháp lập pháp và biện pháp cần thiết khác, phù hợp pháp luật quốc gia mình, để điều chỉnh việc các cơ quan có thẩm quyền quản lý tài sản bị phong toà, thu giữ hoặc tịch thu được quy định tại các khoản 1 và 2 của Điều này.

4. Nếu tài sản do phạm tội mà có đã bị chuyển đổi toàn bộ hoặc một phần thành tài sản khác, tài sản khác này là đối tượng áp dụng các biện pháp quy định tại Điều này thay cho tài sản do phạm tội mà có.

5. Nếu tài sản do phạm tội mà có trộn lẫn với tài sản có nguồn gốc hợp pháp, trên cơ sở không phương hại đến các quyền liên quan đến việc phong tỏa hoặc thu giữ tài sản, tài sản bị trộn lẫn đó sẽ bị tịch thu phần giá trị được xác định là có được do hành vi phạm tội.

6. Thu nhập hoặc các lợi ích khác có được từ tài sản do phạm tội mà có, từ tài sản được biến đổi hoặc chuyển đổi từ tài sản do phạm tội mà có hoặc từ tài sản mà trong đó bị trộn lẫn một phần là tài sản do phạm tội mà có là đối tượng của các biện pháp quy định tại Điều này, được xử lý theo cách thức và mức độ như đối với tài sản do phạm tội mà có.

7. Vì mục đích của Điều này và Điều 50 của Công ước này, mỗi Quốc gia thành viên, trao cho tòa án hoặc các cơ quan có thẩm quyền khác quyền yêu cầu cung cấp hoặc thu giữ hồ sơ ngân hàng, tài chính và thương mại. Một Quốc gia thành viên không được từ chối thực hiện các quy định của khoản này với lý do bảo mật ngân hàng.

8. Mỗi Quốc gia thành viên có thể xem xét khả năng yêu cầu người có hành vi phạm tội phải chứng minh nguồn gốc hợp pháp của tài sản bị cho là do phạm tội mà có hoặc tài sản khác có thể bị tịch thu, trong chừng mực mà yêu cầu này phải tuân theo các nguyên tắc của pháp luật quốc gia và với tính chất của hoạt động xét xử và các hoạt động tố tụng khác.

9. Các quy định của Điều này không được hiểu là gây phương hại đến quyền lợi của các bên thứ ba ngay tình.

10. Không quy định nào của Điều này ảnh hưởng đến nguyên tắc là các quy định của Điều này phải được xác định và thực hiện theo quy định của pháp luật quốc gia của một Quốc gia thành viên.

Điều 32. Quy định về án tịch

Mỗi Quốc gia thành viên có thể áp dụng các biện pháp lập pháp hoặc các biện pháp cần thiết khác, theo các quy định và nhằm các mục đích mà quốc gia đó cho là phù hợp, nhằm xem xét đến bất kỳ bản án có từ trước nào đối với một người bị buộc

tội tại một quốc gia khác nhằm mục đích sử dụng các thông tin đó vào quá trình tố tụng hình sự liên quan đến một tội phạm theo Công ước này.

Điều 33. Bảo vệ người làm chứng

1. Mỗi Quốc gia thành viên thực hiện các biện pháp thích hợp, theo quy định của pháp luật quốc gia và trong khả năng của mình, để bảo vệ người làm chứng đã cung cấp lời khai, cung cấp thông tin, một cách thiện chí và hợp lý, liên quan đến các tội phạm theo Công ước này hoặc hợp tác với các cơ quan điều tra hoặc tư pháp, cũng như người thân thích của họ nếu phù hợp, khỏi mọi sự trả thù hoặc hành vi xâm hại.

2. Không phương hại đến các quyền của bị cáo, kể cả quyền được xét xử một cách đúng luật, các biện pháp quy định tại khoản 1 của Điều này có thể bao gồm:

(a) Thiết lập các thủ tục bảo vệ tính mạng và sức khỏe của người làm chứng, chẳng hạn, trong phạm vi cần thiết và khả thi, di chuyển và cho phép, nếu phù hợp, việc không tiết lộ hoặc hạn chế tiết lộ thông tin liên quan đến danh tính và nơi ở của họ;

(b) Ban hành các quy định về chứng cứ để cho phép cung cấp lời khai theo cách đảm bảo an toàn cho người làm chứng, chẳng hạn cho phép cung cấp lời khai thông qua việc sử dụng công nghệ truyền thông như đường dẫn video hoặc các phương tiện phù hợp khác.

3. Các Quốc gia thành viên phải xem xét việc ký kết các thỏa thuận hoặc đàm xếp với các Quốc gia khác về việc di chuyển những người được đề cập tại khoản 1 của Điều này.

4. Các quy định của Điều này cũng áp dụng đối với các nạn nhân trong trường hợp họ cũng là người làm chứng.

Điều 34. Hỗ trợ và bảo vệ người bị hại

1. Mỗi Quốc gia thành viên thực hiện các biện pháp phù hợp trong khả năng của mình để hỗ trợ và bảo vệ người bị hại của các tội phạm theo Công ước này, đặc biệt là trong các trường hợp có sự đe dọa trả thù hoặc hành vi xâm hại.

2. Mỗi Quốc gia thành viên, tùy theo quy định pháp luật quốc gia của mình, xây dựng quy trình thích hợp để giải quyết yêu cầu bồi thường hoặc đền bù cho người bị hại của các tội phạm theo Công ước này.

3. Mỗi Quốc gia thành viên, tùy theo quy định pháp luật quốc gia của mình, tạo điều kiện để ý kiến và quan ngại của người bị hại được trình bày và cân nhắc ở các giai đoạn phù hợp của quá trình tố tụng hình sự tội phạm, mà không làm phương hại đến quyền của bị cáo.

4. Đối với các tội phạm quy định tại Điều 14 đến 16 của Công ước này, mỗi Quốc gia thành viên, tùy theo quy định pháp luật quốc gia của mình, thực hiện các biện pháp để hỗ trợ cho bị hại của các tội phạm đó, bao gồm cả việc phục hồi về thể chất và tinh thần, trên cơ sở hợp tác với các tổ chức quốc tế, các tổ chức phi chính phủ và các tổ chức xã hội có liên quan.

5. Khi áp dụng quy định tại khoản 2 đến 4 của Điều này, mỗi Quốc gia thành viên, cân nhắc đến độ tuổi, giới tính và các hoàn cảnh cũng như nhu cầu đặc biệt của bị hại, bao gồm các hoàn cảnh và nhu cầu đặc biệt của trẻ em.

6. Mỗi Quốc gia thành viên, trong phạm vi pháp luật quốc gia của mình, thực hiện các bước hiệu quả để đảm bảo tuân thủ các yêu cầu xóa bỏ hoặc không cho phép truy cập các nội dung được mô tả tại Điều 14 và 16 của Công ước này.

Chương V. Hợp tác quốc tế

Điều 35. Nguyên tắc chung về hợp tác quốc tế

1. Các Quốc gia thành viên hợp tác với nhau theo các quy định của Công ước này, cũng như các văn kiện quốc tế khác được áp dụng về hợp tác quốc tế trong các vấn đề hình sự, và pháp luật quốc gia, nhằm mục đích:

(a) Điều tra, truy tố, và xét xử các tội phạm được quy định tại Công ước này, bao gồm việc phong tỏa, thu giữ, tịch thu và hoàn trả tài sản thu được từ các tội phạm đó;

(b) Thu thập, tiếp nhận, bảo quản và chia sẻ chứng cứ là dữ liệu điện tử có liên quan đến các tội phạm được quy định tại Công ước này;

(c) Thu thập, tiếp nhận, bảo quản và chia sẻ chứng cứ là dữ liệu điện tử có liên quan đến bất kỳ tội phạm nghiêm trọng nào, bao gồm các tội phạm nghiêm trọng được quy định theo các công ước của Liên hợp quốc và nghị định thư liên quan có hiệu lực tại thời điểm Công ước này được thông qua.

2. Đối với mục đích thu thập, tiếp nhận, bảo quản và chia sẻ chứng cứ là dữ liệu điện tử về các tội phạm như quy định tại khoản 1 (b) và (c) của Điều này, các khoản liên quan của Điều 40 và các Điều từ 41 đến 46 của Công ước này được áp dụng.

3. Trong các vấn đề hợp tác quốc tế, khi có yêu cầu về nguyên tắc cùng bình sự hoá thì yêu cầu này được coi là đáp ứng nếu hành vi cấu thành tội phạm được yêu cầu trợ giúp là một tội phạm theo pháp luật của cả hai Quốc gia thành viên, bất kể pháp luật của Quốc gia Thành viên được yêu cầu có quy định tội phạm liên quan có cùng loại với tội phạm hoặc định danh tội phạm theo cùng một thuật ngữ giống như Quốc gia thành viên yêu cầu hay không.

Điều 36. Bảo vệ dữ liệu cá nhân

1. (a) Một Quốc gia thành viên chuyển giao dữ liệu cá nhân theo Công ước này thực hiện theo pháp luật quốc gia của mình và bất kỳ nghĩa vụ nào mà Quốc gia chuyển giao thực hiện theo pháp luật quốc tế có liên quan. Các Quốc gia thành viên không bị yêu cầu chuyển giao dữ liệu cá nhân theo Công ước này nếu dữ liệu không thể được cung cấp theo các luật liên quan đến bảo vệ dữ liệu cá nhân của quốc gia đó;

(b) Khi việc chuyển giao dữ liệu cá nhân không tuân thủ khoản 1 (a) của Điều này, các Quốc gia thành viên có thể tìm cách quy định các điều kiện phù hợp, theo các luật áp dụng, để đạt được sự tuân thủ nhằm phản hồi yêu cầu về chuyển giao dữ liệu cá nhân;

(c) Các Quốc gia thành viên được khuyến khích thiết lập các thỏa thuận song phương hoặc đa phương để tạo điều kiện cho việc chuyển giao dữ liệu cá nhân.

2. Đối với dữ liệu cá nhân được chuyển giao theo Công ước này, các Quốc gia thành viên phải đảm bảo rằng dữ liệu cá nhân nhận được phải được bảo vệ bằng các biện pháp hiệu quả và phù hợp trong khuôn khổ pháp lý tương ứng của các Quốc gia thành viên.

3. Để chuyển giao dữ liệu cá nhân thu được theo Công ước này đến một quốc gia thứ ba hoặc một tổ chức quốc tế, Quốc gia thành viên phải thông báo cho Quốc gia chuyển giao ban đầu về ý định của mình và yêu cầu sự cho phép của Quốc gia chuyển giao ban đầu. Quốc gia thành viên chỉ được chuyển giao dữ liệu cá nhân đó khi có sự cho phép của Quốc gia chuyển giao ban đầu, và Quốc gia chuyển giao ban đầu có thể yêu cầu sự cho phép này được cung cấp bằng văn bản.

Điều 37. Dẫn độ

1. Điều này được áp dụng đối với các tội phạm được quy định tại Công ước này khi một người bị của yêu cầu dẫn độ có mặt trên lãnh thổ của Quốc gia được yêu cầu, với điều kiện tội phạm làm nảy sinh yêu cầu dẫn độ là tội phạm mà cả Quốc gia thành viên yêu cầu và Quốc gia thành viên được yêu cầu đều quy định sẽ bị truy cứu trách nhiệm hình sự theo quy định của pháp luật quốc gia. Khi yêu cầu dẫn độ được đưa ra nhằm thi hành một bản án đã có hiệu lực pháp luật bằng hình phạt tù hoặc hình phạt giam giữ khác đối với một số tội bị dẫn độ, Quốc gia thành viên được yêu cầu có thể đồng ý dẫn độ theo pháp luật quốc gia của mình.

2. Dù có các quy định tại khoản 1 của Điều này, nếu pháp luật quốc gia cho phép, một Quốc gia thành viên có thể cho tiến hành dẫn độ của một người về bất kỳ tội phạm nào được quy định tại Công ước này mà tội phạm đó không bị trừng phạt theo luật pháp quốc gia của mình.

3. Nếu yêu cầu dẫn độ bao gồm một số tội phạm riêng biệt mà ít nhất một trong số đó có thể bị dẫn độ theo Điều này và một số không bị dẫn độ theo Điều này vì lý do thời hạn bị phạt tù nhưng có liên quan đến các tội phạm quy định tại Công ước này thì Quốc gia thành viên được yêu cầu cũng có thể áp dụng Điều này đối với các tội phạm đó.

4. Mỗi tội phạm trong số các tội phạm mà Điều này áp dụng được coi là một tội phạm có thể bị dẫn độ trong các điều ước quốc tế về dẫn độ hiện có giữa các Quốc gia thành viên. Các Quốc gia thành viên cam kết quy định các tội phạm đó là các tội phạm có thể bị dẫn độ trong các điều ước quốc tế về dẫn độ mà mình sẽ ký kết.

5. Nếu một Quốc gia thành viên quy định việc dẫn độ chỉ được thực hiện trên cơ sở có một điều ước quốc tế, nhận được yêu cầu dẫn độ từ một Quốc gia thành viên khác mà giữa hai quốc gia này không có điều ước quốc tế về dẫn độ, quốc gia được yêu cầu có thể lấy Công ước này làm cơ sở pháp lý cho việc dẫn độ đối với bất kỳ tội phạm nào mà Điều này áp dụng.

(a) Các Quốc gia thành viên quy định việc dẫn độ chỉ được thực hiện trên cơ sở một điều ước quốc tế về dẫn độ;

(b) Vào thời điểm nộp văn kiện phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập Công ước này, thông báo cho Tổng Thư ký Liên hợp quốc biết về việc có lấy Công ước này làm cơ sở pháp lý cho hợp tác dẫn độ với các Quốc gia thành viên khác của Công ước này hay không; và

6. Nếu không chấp nhận Công ước này là cơ sở pháp lý cho việc hợp tác dẫn độ, thì khi phù hợp, sẽ ký kết các điều ước quốc tế về dẫn độ với các Quốc gia thành viên khác của Công ước này để thực hiện Điều này.

7. Các Quốc gia thành viên không quy định việc dẫn độ phụ thuộc vào một điều ước quốc tế về dẫn độ sẽ công nhận các tội phạm mà Điều này áp dụng là các tội phạm có thể bị dẫn độ giữa họ.

8. Việc dẫn độ tuân theo các điều kiện quy định trong pháp luật của quốc gia được yêu cầu dẫn độ hoặc các điều ước quốc tế về dẫn độ liên quan, trong đó có điều kiện về yêu cầu hình phạt tối thiểu và về các căn cứ mà dựa vào đó Quốc gia Thành viên được yêu cầu có thể từ chối dẫn độ.

9. Các Quốc gia Thành viên, tùy theo pháp luật quốc gia của mình, nỗ lực đẩy nhanh quy trình dẫn độ và đơn giản hóa các yêu cầu về chứng cứ liên quan đến việc dẫn độ đối với bất kỳ tội phạm nào mà Điều này áp dụng.

10. Trên cơ sở tuân thủ quy định của pháp luật quốc gia và các điều ước quốc tế về dẫn độ của mình, Quốc gia thành viên được yêu cầu dẫn độ khi thấy hoàn cảnh cho phép và cấp thiết, đồng thời nếu được đề nghị bởi Quốc gia yêu cầu dẫn độ, bao gồm khi yêu cầu được chuyển qua các kênh hiện có của Tổ chức Cảnh sát Hình sự Quốc tế, thì có thể tạm giam

người là đối tượng dẫn độ đang có mặt trên lãnh thổ nước mình hoặc áp dụng các biện pháp phù hợp khác để bảo đảm rằng người đó sẽ có mặt khi tiến hành thủ tục dẫn độ.

11. Đối với Quốc gia Thành viên mà người bị tình nghi phạm tội có mặt trên lãnh thổ của mình, đồng thời không dẫn độ người này chỉ vì đó là công dân quốc gia mình, thì theo đề nghị của Quốc gia thành viên yêu cầu dẫn độ, Quốc gia đó nhanh chóng đưa vụ việc ra cho các cơ quan có thẩm quyền của mình để truy cứu trách nhiệm hình sự. Các cơ quan có thẩm quyền này đưa ra quyết định và thực hiện quá trình tố tụng theo cách tương tự như đối với bất kỳ tội phạm nào khác có tính chất tương tự theo pháp luật quốc gia của Quốc gia thành viên đó. Các Quốc gia thành viên có liên quan hợp tác với nhau, đặc biệt về mặt thủ tục và chứng cứ, để bảo đảm hiệu quả của việc truy tố.

12. Bất cứ khi nào một Quốc gia Thành viên, theo luật pháp quốc gia của mình, được phép dẫn độ hoặc giao nộp một công dân của quốc gia mình chỉ với điều kiện là người này sẽ được đưa trở lại quốc gia của mình để chấp hành hình phạt là kết quả của một phiên tòa hoặc thủ tục tố tụng được thực hiện sau khi người này bị dẫn độ hay giao nộp và Quốc gia thành viên đó và Quốc gia thành viên yêu cầu dẫn độ cùng nhất trí với lựa chọn này, cũng như với các điều kiện khác mà hai bên thấy phù hợp, việc dẫn độ hoặc giao nộp có điều kiện đó sẽ được coi là đủ để đáp ứng các nghĩa vụ quy định tại khoản 11 của Điều này.

13. Nếu yêu cầu dẫn độ để thi hành một bản án bị từ chối do đối tượng yêu cầu dẫn độ là công dân của Quốc gia được yêu cầu thì Quốc gia thành viên được yêu cầu, nếu pháp luật quốc gia của mình cho phép và phù hợp với các yêu cầu của pháp luật quốc gia của mình, xem xét việc thi hành bản án đã có hiệu lực theo pháp luật quốc gia của Quốc gia thành viên yêu cầu hoặc phần còn lại của bản án đó, trên cơ sở đề nghị của Quốc gia Thành viên yêu cầu.

14. Bất cứ người nào đang trong quá trình tố tụng vì có liên quan đến các tội phạm mà Điều này áp dụng đều được bảo đảm đối xử công bằng trong tất cả các giai đoạn tố tụng, bao gồm việc hưởng tất cả các quyền và biện pháp bảo vệ mà pháp luật của quốc gia nơi người đó đang có mặt quy định.

15. Không quy định nào trong Công ước này được hiểu là bắt buộc dẫn độ nếu Quốc gia thành viên được yêu cầu dẫn độ có cơ sở đầy đủ để tin rằng yêu cầu dẫn

độ đó nhằm mục đích truy tố hay truy cứu trách nhiệm hình sự một người vì lý do giới tính, chủng tộc, ngôn ngữ, tôn giáo, quốc tịch, nguồn gốc sắc tộc hoặc quan điểm chính trị của người đó, hoặc việc đáp ứng yêu cầu dẫn độ có thể gây tổn hại đến tinh thể của người đó vì bất kỳ lý do nào nêu trên.

16. Các Quốc gia thành viên không được từ chối yêu cầu dẫn độ chỉ dựa trên lý do duy nhất là tội phạm đó cũng được coi là có liên quan đến các vấn đề tài chính.

17. Trước khi từ chối dẫn độ, Quốc gia thành viên được yêu cầu, khi phù hợp, tham vấn với Quốc gia thành viên yêu cầu để tạo điều kiện cho quốc gia yêu cầu trình bày quan điểm của mình và cung cấp thông tin về việc nghi vấn của họ.

18. Quốc gia thành viên được yêu cầu thông báo cho Quốc gia thành viên yêu cầu về quyết định của mình liên quan đến việc dẫn độ. Quốc gia thành viên được yêu cầu thông báo cho Quốc gia Thành viên yêu cầu về bất kỳ lý do từ chối dẫn độ nào trừ khi Quốc gia thành viên được yêu cầu bị cấm làm như vậy theo pháp luật quốc gia hoặc nghĩa vụ pháp lý quốc tế của mình.

19. Mỗi Quốc gia thành viên, vào thời điểm ký hoặc khi nộp văn kiện phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập, thông báo cho Tổng Thư ký Liên hợp quốc tên và địa chỉ của cơ quan chịu trách nhiệm thực hiện hoặc tiếp nhận các yêu cầu dẫn độ hoặc bắt tạm giam. Tổng Thư ký sẽ thiết lập và cập nhật sổ đăng ký các cơ quan do các Quốc gia thành viên chỉ định. Mỗi Quốc gia thành viên bảo đảm rằng các thông tin trong sổ đăng ký luôn chính xác.

20. Các Quốc gia thành viên nỗ lực ký kết các hiệp định hoặc thỏa thuận song phương và đa phương để thực hiện việc dẫn độ hoặc tăng cường hiệu quả dẫn độ.

Điều 38. Chuyển giao người bị kết án

Khi xem xét quyền của người bị kết án, các Quốc gia thành viên có thể cân nhắc việc ký kết các hiệp định hoặc thỏa thuận song phương hoặc đa phương về việc chuyển giao đến lãnh thổ của mình những người bị kết án phạt tù hoặc chịu các hình phạt tước quyền tự do khác có đã thực hiện các tội được quy định tại Công ước này để họ có thể chấp hành xong bản án ở nơi chuyển đến. Các Quốc gia thành viên cũng có thể lưu ý đến các vấn đề liên quan đến đồng thuận, cải tạo và tái hòa nhập xã hội.

Điều 39. Chuyển giao hồ sơ vụ án để truy cứu trách nhiệm hình sự

1. Các Quốc gia thành viên xem xét khả năng chuyển giao cho nhau các hồ sơ vụ án để xem xét, truy cứu trách nhiệm hình sự đối với một tội phạm được quy định tại Công ước này, nếu việc chuyển giao đó được coi là có lợi cho việc thực thi pháp luật nghiêm minh, đặc biệt là trong các trường hợp liên quan đến quyền tài phán của nhiều quốc gia, với mục đích tập trung vào việc truy tố.
2. Nếu một Quốc gia thành viên yêu cầu việc chuyển giao hồ sơ vụ án để truy cứu trách nhiệm hình sự được tiến hành trên cơ sở một điều ước quốc tế mà nhận được yêu cầu chuyển giao từ một Quốc gia thành viên khác và hai nước không có điều ước quốc tế về vấn đề này, quốc gia đó có thể coi Công ước này là cơ sở pháp lý cho việc chuyển giao hồ sơ vụ án để truy cứu trách nhiệm hình sự đối với bất kỳ tội phạm nào mà Điều này áp dụng.

Điều 40. Nguyên tắc chung và thủ tục liên quan đến tương trợ tư pháp

1. Các Quốc gia thành viên dành cho nhau các biện pháp tương trợ tư pháp tối đa trong việc điều tra, truy tố và xét xử liên quan đến các tội phạm được quy định tại Công ước này, và vì mục đích thu thập chứng cứ là dữ liệu điện tử của các tội phạm được quy định tại Công ước này, cũng như các tội phạm nghiêm trọng.
2. Tương trợ tư pháp được thực hiện ở mức độ cao nhất có thể theo các luật, điều ước quốc tế, hiệp định và thỏa thuận tương ứng của các Quốc gia thành viên được yêu cầu liên quan tới việc điều tra, truy tố và xét xử đối với các tội phạm mà một pháp nhân có thể phải chịu trách nhiệm hình sự theo điều 18 của Công ước này ở Quốc gia thành viên yêu cầu.
3. Yêu cầu tương trợ tư pháp theo Điều này có thể được đưa ra thể thực hiện một trong các mục đích sau đây:
 - (a) Thu thập chứng cứ hoặc lấy lời khai của người có liên quan;
 - (b) Tổng đạt giấy tờ, tài liệu liên quan đến tư pháp;
 - (c) Tiến hành khám xét, thu giữ, và phong tỏa;
 - (d) Khám xét hoặc truy cập, thu giữ hoặc niêm phong, và tiết lộ dữ liệu điện tử được lưu trữ bằng hệ thống công nghệ thông tin và truyền thông theo Điều 44 của Công ước này;

- (e) Thu thập dữ liệu lưu lượng theo thời gian thực theo Điều 45 của Công ước này;
- (f) Chặn thu dữ liệu về nội dung theo Điều 46 của Công ước này;
- (g) Khám xét vật thể và hiện trường;
- (h) Cung cấp thông tin, chứng cứ và giám định của chuyên gia;
- (i) Cung cấp bản gốc hoặc bản sao có chứng thực của tài liệu và hồ sơ, bao gồm cả hồ sơ của chính phủ, ngân hàng, tài chính, doanh nghiệp hoặc thương mại;
- (j) Xác định hoặc truy tìm tài sản do phạm tội mà có, tài sản, công cụ hoặc đồ vật khác để làm chứng cứ;
- (k) Tạo điều kiện thuận lợi cho sự có mặt tự nguyện của cá nhân tại Quốc gia thành viên yêu cầu;
- (l) Thu hồi tài sản do phạm tội mà có;
- (m) Bất kỳ hình thức tương trợ nào khác không trái với pháp luật trong nước của Quốc gia thành viên được yêu cầu.

4. Trên cơ sở không trái với pháp luật quốc gia, dù không có yêu cầu trước đó, các cơ quan có thẩm quyền của Quốc gia thành viên có thể chuyển thông tin liên quan đến tội phạm cho cơ quan có thẩm quyền của Quốc gia thành viên khác nếu họ tin rằng thông tin đó có thể hỗ trợ cho cơ quan này tiến hành hay kết thúc thành công các cuộc điều tra và các thủ tục tố tụng hình sự hoặc rằng việc chuyển thông tin đó có thể dẫn đến việc Quốc gia thành viên kia gửi yêu cầu tương trợ tư pháp theo Công ước này.

5. Việc chuyển thông tin theo khoản 4 của Điều này không ảnh hưởng đến quá trình điều tra và thủ tục tố tụng hình sự ở Quốc gia của các cơ quan có thẩm quyền cung cấp thông tin. Các cơ quan có thẩm quyền nhận thông tin tuân thủ yêu cầu về việc giữ bí mật thông tin, dù chỉ tạm thời, hoặc yêu cầu về việc hạn chế sử dụng. Tuy nhiên, điều này không cản trở Quốc gia thành viên nhận thông tin tiết lộ thông tin này trong quá trình tố tụng để minh oan cho một người bị buộc tội. Trong trường hợp đó, Quốc gia thành viên nhận thông tin thông báo cho Quốc gia thành viên cung cấp thông tin trước khi thông tin được tiết lộ và, nếu được yêu cầu, thì sẽ tham vấn với Quốc gia thành viên cung cấp thông tin. Trong trường hợp đặc biệt, nếu không thể thông báo trước

được, Quốc gia thành viên nhận thông tin thông báo ngay cho Quốc gia thành viên cung cấp thông tin về việc đã tiết lộ thông tin.

6. Các quy định của Điều này không ảnh hưởng đến nghĩa vụ được quy định tại bất kỳ điều ước quốc tế song phương hoặc đa phương nào, điều chỉnh hoặc sẽ điều chỉnh, một phần hoặc toàn bộ, hoạt động về tương trợ tư pháp.

7. Các khoản 8 đến 31 của Điều này áp dụng đối với các yêu cầu được lập căn cứ theo Điều này nếu giữa các Quốc gia thành viên liên quan không có điều ước quốc tế về tương trợ tư pháp. Nếu giữa các Quốc gia thành viên đó có điều ước quốc tế về tương trợ tư pháp, các quy định tương ứng của điều ước quốc tế đó sẽ được áp dụng trừ khi các Quốc gia thành viên đồng ý áp dụng các khoản 8 đến 31 của Điều này để thay thế. Các Quốc gia thành viên được khuyến khích mạnh mẽ áp dụng các quy định của những khoản này nếu chúng tạo điều kiện thuận lợi cho sự hợp tác.

8. Các Quốc gia thành viên có thể từ chối tiến hành tương trợ tư pháp theo Điều này với lý do thiếu điều kiện cũng là tội phạm. Tuy nhiên, Quốc gia thành viên được yêu cầu có thể, khi thấy phù hợp, tiến hành tương trợ trong phạm vi mà họ tự quyết định, bất kể hành vi đó có cấu thành tội phạm theo pháp luật quốc gia của Quốc gia thành viên được yêu cầu hay không. Tương trợ có thể bị từ chối khi các yêu cầu liên quan đến các vấn đề không quan trọng hoặc các vấn đề mà sự hợp tác hoặc tương trợ được yêu cầu đã có sẵn theo các quy định khác của Công ước này.

9. Người đang chịu hình phạt tù hoặc đang thi hành một bản án trên lãnh thổ của một Quốc gia thành viên nhưng lại bị Quốc gia thành viên khác yêu cầu trích diện để xác định danh tính, làm chứng hoặc cung cấp trợ giúp trong việc thu thập chứng cứ cho quá trình điều tra, truy tố hoặc xét xử các tội phạm được quy định tại Công ước này có thể bị chuyển giao nếu đáp ứng các điều kiện sau:

(a) Người đó tự nguyện đồng ý sau khi đã biết rõ yêu cầu;

(b) Các cơ quan có thẩm quyền của cả hai Quốc gia thành viên đồng ý, phụ thuộc vào các điều kiện mà các Quốc gia thành viên này cho là phù hợp.

10. Vì mục đích của khoản 9 của Điều này:

(a) Quốc gia thành viên mà người đó được dẫn giải đến có quyền và nghĩa vụ phải giam giữ người được dẫn giải, trừ trường hợp Quốc gia thành viên mà người đó được dẫn giải đi có ủy quyền hoặc yêu cầu khác;

(b) Quốc gia thành viên nơi người đó được dẫn giải tới sẽ không chậm trễ thực hiện nghĩa vụ trao trả người đó lại cho Quốc gia thành viên nơi người đó được dẫn giải đi như đã thoả thuận trước, hoặc theo thoả thuận giữa các cơ quan có thẩm quyền của cả hai Quốc gia thành viên;

(c) Các Quốc gia thành viên mà người đó được dẫn giải tới không được yêu cầu Quốc gia thành viên nơi người đó được dẫn giải đi phải tiến hành thủ tục dẫn độ để trao trả lại người đó;

(d) Thời gian bị giam giữ của người đó tại Quốc gia thành viên nơi họ được dẫn giải tới sẽ được tính vào thời gian phạt tù mà họ phải chấp hành tại Quốc gia nơi họ được dẫn giải đi.

11. Trừ khi Quốc gia thành viên nơi một người được dẫn giải đi theo quy định tại Khoản 9 và 10 của Điều này đồng ý, người đó, bất kể có quốc tịch của nước nào, không bị truy tố, giam giữ, trừng phạt hoặc phải chịu bất kỳ sự hạn chế về tự do cá nhân nào tại lãnh thổ của Quốc gia nơi người đó được dẫn giải tới liên quan đến các hành vi mà người đó thực hiện trước khi rời khỏi lãnh thổ của Quốc gia nơi người đó được dẫn giải đi.

12. (a) Mỗi Quốc gia thành viên chỉ định một hoặc các cơ quan trung ương có trách nhiệm và quyền hạn tiếp nhận các yêu cầu về tương trợ tư pháp, thực hiện hoặc chuyển chúng đến các cơ quan có thẩm quyền khác để thực hiện. Trường hợp Quốc gia thành viên có một khu vực hoặc vùng lãnh thổ đặc biệt với một hệ thống tương trợ tư pháp riêng biệt, thì Quốc gia đó có thể chỉ định một cơ quan trung ương riêng biệt có chức năng tương trợ cho khu vực hoặc vùng lãnh thổ đó;

(b) Các cơ quan trung ương đảm bảo việc thực hiện hoặc chuyển nhanh chóng và đầy đủ các yêu cầu nhận được. Trường hợp cơ quan trung ương chuyển yêu cầu đến cơ quan có thẩm quyền để thực hiện, cơ quan trung ương phải khuyến khích việc thực hiện nhanh chóng và đầy đủ yêu cầu đó;

(c) Tổng Thư ký Liên hợp quốc được thông báo về cơ quan trung ương được chỉ định cho mục đích này tại thời điểm mỗi Quốc gia thành viên nộp văn kiện phê chuẩn, chấp nhận hoặc phê duyệt hoặc gia nhập Công ước này, và sẽ thiết lập và cập nhật sổ đăng ký các cơ quan trung ương được chỉ định bởi các Quốc gia thành viên. Mỗi Quốc gia Thành viên sẽ đảm bảo rằng các thông tin được giữ trong sổ đăng ký luôn chính xác;

(d) Các yêu cầu tương trợ tư pháp và mọi liên lạc có liên quan phải được chuyển đến các cơ quan trung ương mà các Quốc gia thành viên chỉ định. Yêu cầu này không ảnh hưởng đến quyền của một Quốc gia thành viên yêu cầu rằng các yêu cầu tương trợ tư pháp và liên lạc đó phải thông qua kênh ngoại giao và, trong các trường hợp khẩn cấp, nếu các Quốc gia thành viên đồng ý, thông qua Tổ chức Cảnh sát Hình sự Quốc tế, nếu có thể.

13. Yêu cầu tương trợ tư pháp được lập thành văn bản hoặc, nếu có thể, bằng các cách có khả năng tạo ra văn bản, bằng ngôn ngữ mà Quốc gia thành viên được yêu cầu chấp nhận, theo các điều kiện cho phép Quốc gia thành viên đó xác định được tính xác thực. Tổng Thư ký Liên hợp quốc được thông báo về ngôn ngữ hoặc các ngôn ngữ trong yêu cầu tương trợ tư pháp mà mỗi Quốc gia thành viên có thể chấp nhận vào thời điểm mỗi bên nộp văn kiện phê chuẩn, chấp nhận hoặc phê duyệt hoặc gia nhập Công ước này. Trong các trường hợp khẩn cấp và nếu các Quốc gia thành viên đồng ý, các yêu cầu tương trợ tư pháp bằng lời nói có thể được chấp nhận, nhưng sau đó sẽ phải được xác nhận lại bằng văn bản.

14. Nếu pháp luật quốc gia không cấm, các cơ quan trung ương của các Quốc gia thành viên được khuyến khích gửi và nhận các yêu cầu tương trợ tư pháp, cũng như các thông tin liên quan, dưới dạng điện tử, với các điều kiện cho phép Quốc gia thành viên được yêu cầu xác định tính xác thực và đảm bảo tính bảo mật của các liên lạc.

15. Một yêu cầu tương trợ tư pháp phải bao gồm các thông tin sau:

(a) Danh tính của cơ quan yêu cầu;

(b) Đối tượng và bản chất của việc điều tra, truy tố hoặc xét xử liên quan đến yêu cầu và tên gọi, chức năng của cơ quan tiến hành điều tra, truy tố hoặc xét xử;

(c) Tóm tắt các sự kiện liên quan, trừ trường hợp yêu cầu tương trợ tư pháp nhằm mục đích tổng đại giấy tờ;

(d) Miêu tả về sự tương trợ và nêu chi tiết về quy trình cụ thể mà Quốc gia thành viên yêu cầu muốn thực hiện;

(e) Nếu có thể và phù hợp, nêu đặc điểm nhận dạng, nơi ở và quốc tịch của cá nhân có liên quan, cũng như quốc gia xuất xứ, mô tả và vị trí của bất kỳ vật phẩm hoặc tài khoản nào liên quan;

(f) Nếu có thể áp dụng, thời hạn đối với bằng chứng, thông tin hoặc sự tương trợ khác;

(g) Mục đích của việc tìm kiếm bằng chứng, thông tin hoặc sự tương trợ khác.

16. Quốc gia thành viên được yêu cầu có thể đề nghị được cung cấp thêm thông tin nếu điều đó là cần thiết cho việc thực hiện yêu cầu theo quy định của pháp luật quốc gia của mình hoặc nếu thông tin bổ sung đó hỗ trợ việc thực hiện tương trợ.

17. Yêu cầu được thực hiện trên cơ sở phù hợp với pháp luật của Quốc gia thành viên được yêu cầu và, trong chừng mực không trái với pháp luật của Quốc gia thành viên được yêu cầu và khi có thể, theo trình tự thủ tục nêu cụ thể trong yêu cầu.

18. Bất cứ khi nào có thể và phù hợp với các nguyên tắc cơ bản của pháp luật quốc gia, khi một cá nhân đang trên lãnh thổ của một Quốc gia thành viên và cần phải trình bày ý kiến trước cơ quan tư pháp của một Quốc gia thành viên khác với tư cách là người làm chứng, bị hại hoặc chuyên gia, thì theo đề nghị của bên kia, Quốc gia thành viên ban đầu có thể cho phép buổi trình bày được thực hiện qua hình thức trực tuyến (trao đổi qua video) nếu người có liên quan không thể hoặc không muốn có mặt trực tiếp tại lãnh thổ của Quốc gia thành viên yêu cầu. Các Quốc gia thành viên có thể đồng ý rằng buổi trình bày sẽ được tổ chức bởi một cơ quan tư pháp của Quốc gia thành viên yêu cầu với sự tham gia của một cơ quan tư pháp của Quốc gia thành viên được yêu cầu. Nếu Quốc gia thành viên được yêu cầu không có phương tiện kỹ thuật cần thiết để tổ chức các cuộc họp trực tuyến, các phương tiện kỹ thuật này có thể được cung cấp bởi Quốc gia thành viên yêu cầu trên cơ sở thỏa thuận giữa các bên.

19. Quốc gia thành viên yêu cầu không được chuyển giao hoặc sử dụng thông tin hoặc bằng chứng được cung cấp bởi Quốc gia thành viên được yêu cầu cho việc điều tra, truy tố hoặc xét xử khác với các việc đã nêu cụ thể trong yêu cầu mà chưa có sự đồng ý trước

của Quốc gia được yêu cầu. Không quy định nào trong khoản này ngăn cản việc Quốc gia thành viên yêu cầu tiết lộ các thông tin hoặc bằng chứng minh oan cho người bị kết tội trong quá trình xét xử. Trong trường hợp vừa nêu, Quốc gia thành viên yêu cầu thông báo cho Quốc gia thành viên được yêu cầu biết trước khi tiết lộ và, nếu được yêu cầu, thì sẽ tham vấn với Quốc gia thành viên được yêu cầu về việc này. Trong trường hợp đặc biệt, nếu việc báo trước không thể thực hiện được, Quốc gia thành viên yêu cầu phải thông báo ngay cho Quốc gia thành viên được yêu cầu sau khi đã tiết lộ thông tin.

20. Quốc gia thành viên yêu cầu có thể đề nghị Quốc gia thành viên được yêu cầu giữ bí mật về tính tiết và nội dung của yêu cầu, trừ khi phải tiết lộ tới phạm vi cần thiết để thực hiện yêu cầu. Nếu Quốc gia thành viên được yêu cầu không thể tuân thủ yêu cầu về bảo mật thì thông báo nhanh chóng cho Quốc gia thành viên yêu cầu biết.

21. Việc tương trợ tư pháp có thể bị từ chối trong các trường hợp sau:

- (a) Nếu yêu cầu được lập không tuân thủ các quy định của Điều này;
- (b) Nếu Quốc gia thành viên được yêu cầu nhận thấy việc thực hiện yêu cầu có khả năng xâm phạm đến chủ quyền, an ninh, trật tự công cộng hoặc các lợi ích thiết yếu khác của mình;
- (c) Nếu các cơ quan của Quốc gia thành viên được yêu cầu bị pháp luật quốc gia cấm thực hiện việc được yêu cầu đối với bất kỳ tội phạm tương tự nào, bởi tội phạm đó đã là đối tượng của việc điều tra, truy tố hoặc xét xử trong phạm vi quyền hạn của chính các cơ quan này;
- (d) Nếu việc chấp nhận yêu cầu tương trợ tư pháp của yêu cầu này là trái pháp luật của Quốc gia thành viên được yêu cầu.

22. Không quy định nào trong Công ước này được hiểu là áp đặt nghĩa vụ tương trợ tư pháp nếu Quốc gia thành viên được yêu cầu có căn cứ chắc chắn về việc yêu cầu đã được đưa ra với mục đích truy tố hoặc truy cứu trách nhiệm hình sự một người vì lý do giới tính, chủng tộc, ngôn ngữ, tôn giáo, quốc tịch, nguồn gốc sắc tộc hoặc quan điểm chính trị của người đó, hoặc rằng việc tuân thủ yêu cầu sẽ gây bất lợi cho tình thế của người đó vì bất kỳ lý do nào nêu trên.

23. Các Quốc gia thành viên không được từ chối yêu cầu tương trợ tư pháp chỉ dựa trên lý do duy nhất là tội phạm đó cũng được coi là có liên quan đến các vấn đề tài chính.

24. Các Quốc gia thành viên không từ chối tương trợ tư pháp theo Điều này vì lý do đảm bảo bí mật ngân hàng.

25. Bất kỳ sự từ chối tương trợ tư pháp nào đều phải đưa ra lý do.

26. Các Quốc gia thành viên được yêu cầu phải thực hiện yêu cầu tương trợ tư pháp ngay khi có thể và sẽ tính toán đầy đủ đến bất kỳ thời hạn nào do Quốc gia thành viên yêu cầu đề xuất cũng như các lý do được đưa ra đối với thời hạn đó, trước hết là các thời hạn nêu trong yêu cầu. Quốc gia thành viên được yêu cầu trả lời các đề nghị hợp lý của Quốc gia thành viên yêu cầu về tình hình và tiến triển giải quyết yêu cầu của mình. Quốc gia thành viên yêu cầu phải nhanh chóng thông báo cho Quốc gia thành viên được yêu cầu khi việc tương trợ không cần thiết nữa.

27. Việc tương trợ tư pháp có thể bị hoãn bởi Quốc gia thành viên được yêu cầu, do việc đó cản trở một vụ việc đang được điều tra, truy tố hoặc xét xử.

28. Trước khi từ chối một yêu cầu theo khoản 21 của Điều này hoặc hoãn việc thực hiện yêu cầu theo khoản 27 của Điều này, Quốc gia thành viên được yêu cầu tham vấn với Quốc gia thành viên yêu cầu để xem xét liệu việc tương trợ có thể được thực hiện theo các điều khoản và điều kiện mà mình cho là cần thiết. Nếu Quốc gia thành viên yêu cầu chấp nhận việc tương trợ theo các điều kiện nêu trên thì tuân thủ các điều kiện này.

29. Không ảnh hưởng đến việc áp dụng khoản 11 của Điều này, người làm chứng, chuyên gia hoặc người nào khác, theo yêu cầu của Quốc gia thành viên yêu cầu, đồng ý đưa ra bằng chứng trong quá trình tố tụng hoặc đồng ý trợ giúp việc điều tra, truy tố hoặc xét xử trên lãnh thổ của Quốc gia thành viên yêu cầu, sẽ không bị truy tố, giam giữ, truy cứu trách nhiệm hình sự hoặc chịu bất kỳ sự hạn chế nào về tự do cá nhân trên lãnh thổ đó vì việc hành động hay không hành động hoặc vì một bản án có trước khi người đó rời khỏi lãnh thổ của Quốc gia thành viên được yêu cầu. Sự đảm bảo an toàn này chấm dứt khi người làm chứng, chuyên gia hoặc người nào khác, dù đã có cơ

hội trở về nước, trong khoản thời gian là 15 ngày liên tục hoặc bất kỳ khoản thời gian nào khác theo thoả thuận của Quốc gia thành viên kể từ khi người này được chính thức thông báo rằng sự có mặt của người này không còn cần thiết nữa đối với các cơ quan tư pháp, nhưng vẫn tự nguyện ở lại trong lãnh thổ của Quốc gia thành viên yêu cầu, hoặc đã rời đi nhưng sau đó lại quay trở lại theo ý nguyện của chính người này.

30. Các chi phí thông thường cho việc thực hiện một yêu cầu do Quốc gia thành viên được yêu cầu chịu, trừ khi các Quốc gia thành viên có liên quan thoả thuận khác. Nếu đòi hỏi phải có các chi phí lớn hoặc đặc biệt để thực hiện được yêu cầu, các Quốc gia thành viên tham vấn để quyết định các điều khoản và điều kiện mà theo đó yêu cầu được thực hiện, cũng như cách thức thanh toán chi phí.

31. Quốc gia thành viên được yêu cầu:

(a) Cung cấp cho Quốc gia thành viên yêu cầu các bản sao của hồ sơ, tài liệu hoặc thông tin của chính phủ mà theo pháp luật quốc gia mình thì các hồ sơ, tài liệu hay thông tin này được công khai cho công chúng;

(b) Tùy theo quyết định của mình, có thể cung cấp cho Quốc gia thành viên yêu cầu, toàn bộ hoặc một phần, hoặc với các điều kiện mà Quốc gia thành viên đó cho là phù hợp, bản sao của bất kỳ hồ sơ, tài liệu hoặc thông tin của chính phủ nào mà theo pháp luật quốc gia của mình thì không thuộc diện được công khai cho công chúng.

32. Khi cần thiết, các Quốc gia thành viên xem xét khả năng ký kết các hiệp định hoặc thoả thuận song phương hoặc đa phương phục vụ cho các mục đích, đảm bảo hiệu lực thực tế hoặc củng cố các quy định tại Điều này.

Điều 41. Mạng lưới 24/7

1. Mỗi Quốc gia thành viên chỉ định một đầu mối liên lạc sẵn sàng 24 giờ mỗi ngày, 7 ngày mỗi tuần, nhằm đảm bảo việc cung cấp sự hỗ trợ ngay lập tức cho các hoạt động điều tra, truy tố hoặc xét xử có liên quan đến các tội phạm được quy định tại Công ước này, hoặc cho việc thu thập và bảo quản chứng cứ là dữ liệu điện tử theo mục đích của khoản 3 của Điều này và liên quan đến các tội phạm được quy định tại Công ước này, cũng như các tội phạm nghiêm trọng.

2. Tổng Thư ký Liên hợp quốc được thông báo về đầu mối liên lạc này và duy trì một sổ đăng ký cập nhật các đầu mối liên lạc được chỉ định cho mục đích của Điều này và hàng năm phải phát hành danh sách đầu mối liên lạc cập nhật cho các Quốc gia thành viên.

3. Sự hỗ trợ theo Điều này bao gồm việc tạo điều kiện hoặc, trên cơ sở của pháp luật và thực tiễn của Quốc gia thành viên được yêu cầu, trực tiếp thực hiện các biện pháp sau:

4. (a) Cung cấp tư vấn kỹ thuật;

(b) Bảo quản dữ liệu điện tử đã được lưu trữ theo các Điều 42 và 43 của Công ước này, bao gồm, khi phù hợp, thông tin về vị trí của nhà cung cấp dịch vụ, nếu Quốc gia thành viên được yêu cầu biết, để hỗ trợ Quốc gia thành viên yêu cầu trong việc đưa ra yêu cầu;

(c) Thu thập bằng chứng và cung cấp các thông tin hợp pháp;

(d) Xác định vị trí nghi phạm; hoặc

(e) Cung cấp dữ liệu điện tử để ngăn chặn tình huống khẩn cấp.

5. Đầu mối liên lạc của một Quốc gia thành viên có khả năng thực hiện liên lạc với đầu mối liên lạc của một Quốc gia thành viên khác một cách nhanh chóng. Nếu đầu mối liên lạc do một Quốc gia thành viên chỉ định không thuộc quyền quản lý của cơ quan có thẩm quyền của Quốc gia thành viên đó hoặc các cơ quan chịu trách nhiệm về tương trợ tư pháp hoặc dẫn độ, đầu mối liên lạc phải đảm bảo rằng đơn vị này có thể phối hợp với các cơ quan đó một cách nhanh chóng.

6. Mỗi Quốc gia thành viên bảo đảm rằng các nhân viên được đào tạo và trang bị để luôn sẵn sàng đảm bảo hoạt động của mạng lưới 24/7.

7. Các Quốc gia thành viên cũng có thể sử dụng và tăng cường các mạng lưới đầu mối liên lạc được ủy quyền hiện có, nếu có, và trong phạm vi pháp luật quốc gia của mình, bao gồm các mạng lưới 24/7 cho tội phạm máy tính của Tổ chức Cảnh sát Hình sự Quốc tế để đẩy nhanh hợp tác giữa cảnh sát với cảnh sát và các phương pháp hợp tác trao đổi thông tin khác.

Điều 42. Hợp tác quốc tế nhằm bảo quản khẩn cấp dữ liệu điện tử đã lưu trữ

1. Một Quốc gia thành viên có thể yêu cầu một Quốc gia thành viên khác ra yêu cầu hoặc bằng cách khác đạt được, theo quy định tại Điều 25 của Công ước này, việc bảo quản khẩn cấp dữ liệu điện tử được lưu trữ bằng hệ thống công nghệ thông tin và truyền thông trong lãnh thổ của Quốc gia thành viên khác đó, và đối với dữ liệu mà Quốc gia thành viên yêu cầu dự định sẽ gửi yêu cầu tương trợ tư pháp để khám xét hoặc truy cập, thu giữ hoặc niêm phong, hoặc tiết lộ dữ liệu điện tử.

2. Quốc gia thành viên yêu cầu có thể sử dụng mạng lưới 24/7 quy định tại Điều 41 của Công ước này để tìm kiếm thông tin về vị trí của dữ liệu điện tử được lưu trữ bằng hệ thống công nghệ thông tin và truyền thông và, nếu phù hợp, thông tin về vị trí của nhà cung cấp dịch vụ.

3. Một yêu cầu bảo quản được đưa ra theo khoản 1 của Điều này phải nêu rõ:

- (a) Cơ quan đang yêu cầu bảo quản;
- (b) Tội phạm là đối tượng của điều tra hình sự, truy tố hoặc xét xử và một tóm tắt về các sự kiện liên quan;
- (c) Dữ liệu điện tử đã lưu trữ cần được bảo quản và mối quan hệ của các dữ liệu này với tội phạm;
- (d) Bất kỳ thông tin nào có sẵn để xác định người giữ dữ liệu điện tử đã lưu trữ hoặc vị trí của hệ thống công nghệ thông tin và truyền thông;
- (e) Sự cần thiết của việc bảo quản;
- (f) Quốc gia thành viên yêu cầu dự định sẽ gửi yêu cầu tương trợ tư pháp để khám xét hoặc truy cập, thu giữ hoặc niêm phong, hoặc tiết lộ dữ liệu điện tử đã lưu trữ;
- (g) Nếu phù hợp, sự cần thiết phải giữ bí mật về yêu cầu và không thông báo cho người sử dụng.

4. Sau khi nhận được yêu cầu từ một Quốc gia thành viên khác, Quốc gia Thành viên được yêu cầu phải thực hiện tất cả các biện pháp thích hợp để bảo quản nhanh chóng dữ

liệu điện tử theo quy định của pháp luật quốc gia của mình. Để đáp ứng yêu cầu, nguyên tắc cùng hình sự hoá không được coi là điều kiện để thực hiện việc bảo quản đó.

5. Mọi Quốc gia thành viên yêu cầu cùng hình sự hoá là điều kiện để đáp ứng yêu cầu tương trợ tư pháp trong việc khám xét hoặc truy cập, thu giữ hoặc niêm phong, hoặc tiết lộ dữ liệu điện tử đã lưu trữ có thể, đối với các tội phạm khác ngoài các tội phạm được quy định tại Công ước này, bảo lưu quyền từ chối yêu cầu bảo quản theo Điều này trong trường hợp có lý do để tin rằng, tại thời điểm tiết lộ, điều kiện cùng hình sự hoá không được đáp ứng.

6. Ngoài ra, yêu cầu bảo quản có thể chỉ bị từ chối dựa trên cơ sở các lý do được quy định tại Điều 40, khoản 21 (b) và (c) và khoản 22 của Công ước này.

7. Nếu Quốc gia thành viên được yêu cầu tin rằng việc bảo quản sẽ không đảm bảo tính khả dụng trong tương lai của dữ liệu hoặc sẽ đe dọa tính bảo mật hoặc gây tổn hại khác cho việc điều tra của Quốc gia thành viên yêu cầu, Quốc gia thành viên được yêu cầu phải thông báo ngay lập tức cho Quốc gia thành viên yêu cầu, và Quốc gia thành viên yêu cầu sau đó sẽ quyết định xem yêu cầu đó có nên được thực hiện hay không.

8. Mọi việc bảo quản được thực hiện theo yêu cầu quy định tại khoản 1 của Điều này sẽ có thời hạn không dưới 60 ngày, để cho phép Quốc gia thành viên yêu cầu gửi yêu cầu về việc khám xét hoặc truy cập, thu giữ hoặc niêm phong, hoặc tiết lộ dữ liệu. Sau khi nhận được yêu cầu như vậy, dữ liệu sẽ tiếp tục được bảo quản cho đến khi có quyết định về yêu cầu đó.

9. Trước khi hết thời gian bảo quản theo khoản 8 của Điều này, Quốc gia thành viên yêu cầu có thể yêu cầu gia hạn thời gian bảo quản.

Điều 43. Hợp tác quốc tế nhằm tiết lộ nhanh chóng dữ liệu về lưu lượng đã bảo quản

1. Trong quá trình thực hiện yêu cầu theo Điều 42 của Công ước này để bảo quản dữ liệu lưu lượng liên quan đến một liên lạc cụ thể, nếu Quốc gia thành viên được yêu cầu phát hiện rằng một nhà cung cấp dịch vụ ở Quốc gia thành viên khác đã tham gia vào việc truyền tải liên lạc đó, Quốc gia thành viên được yêu cầu tiết lộ nhanh chóng cho Quốc gia Thành viên yêu cầu một hững dữ liệu về lưu lượng đủ để xác định nhà cung cấp dịch vụ đó và con đường mà qua đó liên lạc đã được truyền tải.

2. Việc tiết lộ dữ liệu về lưu lượng theo khoản 1 của Điều này có thể bị từ chối trên cơ sở các lý do được quy định tại Điều 40, khoản 21 (b) và (c) và khoản 22 của Công ước này.

Điều 44. Tương trợ tư pháp về truy cập dữ liệu điện tử đã lưu trữ

1. Một Quốc gia thành viên có thể yêu cầu Quốc gia thành viên khác khám xét hoặc truy cập, thu giữ hoặc biện pháp tương tự, và tiết lộ dữ liệu điện tử đã lưu trữ bằng hệ thống công nghệ thông tin và truyền thông nằm trong lãnh thổ của Quốc gia thành viên được yêu cầu, bao gồm cả dữ liệu điện tử đã được bảo quản theo Điều 42 của Công ước này.

2. Quốc gia thành viên được yêu cầu đáp ứng yêu cầu bằng cách áp dụng các văn kiện pháp lý và pháp luật quốc tế liên quan được đề cập tại Điều 35 của Công ước này, và theo các quy định khác của Chương này.

3. Yêu cầu phải được phân hồ: khẩn cấp khi:

(a) Có lý do để tin rằng dữ liệu liên quan đang rất dễ bị mất mát hoặc thay đổi; hoặc

(b) Các văn kiện pháp lý và pháp luật quốc tế được đề cập trong khoản 2 của Điều này quy định về việc hợp tác khẩn cấp.

Điều 45. Tương trợ tư pháp trong thu thập dữ liệu về lưu lượng theo thời gian thực

1. Các Quốc gia thành viên nỗ lực cung cấp tương trợ tư pháp lẫn nhau trong việc thu thập dữ liệu lưu lượng theo thời gian thực liên quan đến các giao tiếp trong lãnh thổ của họ được truyền tải bằng hệ thống công nghệ thông tin và truyền thông. Tùy thuộc vào các quy định tại khoản 2 của Điều này, sự hỗ trợ như vậy sẽ được điều chỉnh bởi các điều kiện và thủ tục theo pháp luật quốc gia.

2. Mỗi Quốc gia thành viên nỗ lực cung cấp tương trợ tư pháp ít nhất đối với các tội phạm mà việc thu thập dữ liệu về lưu lượng theo thời gian thực sẽ có sẵn trong một vụ án tương tự trong quốc gia mình.

3. Một yêu cầu được thực hiện theo khoản 1 của Điều này phải nêu rõ:

(a) Tên cơ quan yêu cầu;

(b) Tóm tắt các sự kiện chính và bản chất của cuộc điều tra, truy tố hoặc xét xử mà yêu cầu liên quan đến;

(c) Dữ liệu điện tử liên quan đến việc thu thập dữ liệu về lưu lượng cần thiết và mối liên hệ của chúng với tội phạm;

(d) Bất kỳ dữ liệu nào có sẵn để xác định chủ sở hữu hoặc người sử dụng dữ liệu hoặc vị trí của hệ thống công nghệ thông tin và truyền thông;

(e) Giải thích lý do cần thu thập dữ liệu về lưu lượng;

(f) Thời gian dữ liệu về lưu lượng được thu thập và giải thích tương ứng về thời gian đó.

Điều 46. Tương trợ tư pháp trong chặn thu dữ liệu về nội dung

Trong phạm vi được cho phép theo các điều ước quốc tế áp dụng với các quốc gia đó hoặc theo pháp luật quốc gia, các Quốc gia thành viên nỗ lực cung cấp tương trợ tư pháp lẫn nhau trong việc thu thập hoặc ghi lại dữ liệu về nội dung của các liên lạc theo thời gian thực được truyền tải bằng hệ thống công nghệ thông tin và truyền thông.

Điều 47. Hợp tác thực thi pháp luật

1. Các Quốc gia thành viên hợp tác chặt chẽ với nhau, trên cơ sở tuân thủ hệ thống pháp luật và hành chính quốc gia của mình, để nâng cao hiệu quả của hoạt động thực thi pháp luật nhằm đấu tranh chống các tội phạm được quy định tại Công ước này. Đặc biệt, mỗi Quốc gia thành viên áp dụng các biện pháp hiệu quả:

(a) Để tăng cường và, khi cần thiết, thành lập các kênh liên lạc giữa các cơ quan, tổ chức và ban ngành có thẩm quyền của các bên, cân nhắc các kênh hiện có, bao gồm cả các kênh của Tổ chức Cảnh sát Hình sự Quốc tế, nhằm tạo điều kiện cho việc trao đổi an toàn và nhanh chóng thông tin về tất cả các khía cạnh của tội phạm được quy định tại Công ước này, kể cả mối liên hệ với các tội phạm khác nếu các Quốc gia thành viên có liên quan cho là phù hợp;

(b) Để hợp tác với các Quốc gia thành viên khác trong hoạt động điều tra các tội phạm được quy định tại Công ước này liên quan đến:

(i) Đặc điểm nhận dạng, nơi ở và các hoạt động của người bị nghi ngờ có liên quan đến tội phạm đó, hoặc địa điểm của các cá nhân khác có liên quan;

(ii) Sự di chuyển của tiền do phạm tội mà có hoặc tài sản có được từ việc thực hiện tội phạm đó;

(c) Sự di chuyển của tài sản, thiết bị hoặc công cụ khác được sử dụng hoặc sẽ sử dụng trong việc thực hiện tội phạm đó;

(d) Cung cấp, khi phù hợp, các thiết bị hoặc dữ liệu cần thiết cho mục đích phân tích hoặc điều tra;

(e) Để trao đổi với các Quốc gia thành viên khác, khi phù hợp, thông tin về các phương tiện và thủ đoạn cụ thể được sử dụng trong quá trình thực hiện tội phạm được quy định tại Công ước này, bao gồm cả việc sử dụng giấy tờ nhân thân giả, tài liệu bị làm giả hoặc sửa chữa sai lệch và các thủ đoạn che đậy khác, cũng như các chiến thuật, kỹ thuật và quy trình về tội phạm mạng;

(f) Để tạo điều kiện thuận lợi cho việc phối hợp hiệu quả giữa các cơ quan, tổ chức, ban ngành có thẩm quyền của các bên, và để thúc đẩy trao đổi cán bộ và các chuyên gia, theo các hiệp định hoặc thỏa thuận song phương giữa các Quốc gia thành viên có liên quan, kể cả việc hỗ trợ các cán bộ liên lạc;

(g) Để trao đổi thông tin và phối hợp thực hiện các biện pháp hành chính và các biện pháp khác, khi phù hợp, nhằm mục đích sớm xác định được các tội phạm mà Công ước này quy định.

2 Để Công ước này có hiệu lực, các Quốc gia thành viên xem xét việc ký kết các hiệp định hoặc thỏa thuận song phương hoặc đa phương về hợp tác trực tiếp giữa các cơ quan thực thi pháp luật của các bên và, nếu đã có hiệp định hoặc thỏa thuận như vậy, thì sửa đổi chúng. Nếu chưa có các hiệp định hoặc thỏa thuận như vậy, các Quốc gia thành viên có thể coi Công ước này là cơ sở cho hợp tác thực thi pháp luật đối với các tội phạm được quy định tại Công ước này. Bất cứ khi nào phù hợp, các Quốc gia thành viên tận dụng các hiệp định hoặc thỏa thuận, kể cả các tổ chức quốc tế hoặc khu vực, để tăng cường hợp tác giữa các cơ quan thực thi pháp luật của các bên.

Điều 48. Phối hợp điều tra

Các Quốc gia thành viên xem xét việc ký kết các hiệp định hoặc thỏa thuận song phương hoặc đa phương để qua đó, đối với tội phạm được quy định tại Công ước này

là đối tượng của quá trình điều tra, truy tố hoặc xét xử tại một hoặc nhiều Quốc gia thành viên, các cơ quan có thẩm quyền liên quan có thể thành lập các cơ quan phối hợp điều tra. Trong trường hợp không có hiệp định hoặc thỏa thuận như vậy, hoạt động phối hợp điều tra chung có thể được thực hiện theo thỏa thuận trong từng vụ việc cụ thể. Các Quốc gia thành viên liên quan bảo đảm rằng chủ quyền của Quốc gia thành viên nơi đang tiến hành việc điều tra như vậy phải được tôn trọng đầy đủ.

Điều 49. Cơ chế thu hồi tài sản thông qua hợp tác quốc tế về tịch thu tài sản

1. Để tương trợ tư pháp theo Điều 50 của Công ước này, liên quan đến tài sản có được do phạm tội hay liên quan đến tội phạm được quy định tại Công ước này, căn cứ theo pháp luật quốc gia mình, mỗi Quốc gia thành viên:

(a) Áp dụng các biện pháp cần thiết để cho phép các cơ quan có thẩm quyền công nhận hiệu lực thi hành đối với lệnh tịch thu được đưa ra bởi Quốc gia Thành viên khác;

(b) Áp dụng các biện pháp cần thiết để cho phép các cơ quan có thẩm quyền, trong phạm vi quyền hạn, ra lệnh tịch thu tài sản có nguồn gốc nước ngoài theo phán quyết đối với tội phạm rửa tiền hoặc tội phạm khác thuộc thẩm quyền xét xử của các cơ quan này hay theo các thủ tục khác được quy định tại pháp luật quốc gia mình;

(c) Xem xét áp dụng các biện pháp cần thiết cho phép tịch thu tài sản mà chưa có bản án hình sự trong trường hợp không thể truy tố người phạm tội vì lý do người này đã chết, bỏ trốn hoặc vắng mặt, hoặc trong các trường hợp phù hợp khác.

2. Mỗi Quốc gia thành viên, để tương trợ tư pháp theo yêu cầu được đưa ra theo Điều 50, khoản 2 của Công ước này, căn cứ theo pháp luật quốc gia của mình:

(a) Áp dụng các biện pháp cần thiết để cho phép các cơ quan có thẩm quyền phong toả hoặc thu giữ tài sản dựa trên một lệnh phong toả hoặc thu giữ được ban hành bởi một tòa án hoặc cơ quan có thẩm quyền của Quốc gia thành viên yêu cầu, trong đó đưa ra căn cứ hợp lý để Quốc gia thành viên được yêu cầu tin rằng đã có đủ căn cứ để áp dụng các biện pháp này, và rằng tài sản đó sẽ chịu lệnh tịch thu theo khoản 1 (a) của Điều này,

(b) Áp dụng các biện pháp cần thiết để cho phép các cơ quan có thẩm quyền phong toả hoặc thu giữ tài sản dựa trên một đề nghị trong đó đưa ra những căn cứ hợp lý để Quốc gia thành viên được yêu cầu tin rằng đã có đủ căn cứ để áp dụng các biện

pháp này, và rằng tài sản đó sẽ phải chịu lệnh tịch thu theo khoản 1 (a) của Điều này; và

(c) Xem xét áp dụng các biện pháp bổ sung để cho phép các cơ quan có thẩm quyền bảo quản tài sản để tịch thu, chẳng hạn dựa trên cơ sở việc bắt giữ hoặc buộc tội hình sự có yếu tố ngoài liên quan đến việc tịch thu những tài sản này.

Điều 50. Hợp tác quốc tế nhằm mục đích tịch thu tài sản

1. Một Quốc gia thành viên nhận được yêu cầu từ một Quốc gia thành viên khác có thẩm quyền đối với một tội phạm được quy định tại Công ước này về việc tịch thu tài sản do phạm tội mà có, tài sản, thiết bị hoặc công cụ khác được đề cập tại Điều 31, khoản 1 của Công ước này, đang có trên lãnh thổ của mình, trong phạm vi rộng nhất có thể mà pháp luật quốc gia của mình cho phép:

(a) Trình yêu cầu đến các cơ quan có thẩm quyền của mình để xin cấp lệnh tịch thu và, nếu lệnh tịch thu đó được cấp thì hành nó; hoặc

(b) Trình các cơ quan có thẩm quyền của mình, với mục đích thực hiện trong phạm vi được yêu cầu, một lệnh tịch thu do tòa án trong lãnh thổ của Quốc gia thành viên yêu cầu ban hành theo Điều 31, khoản 1 của Công ước này ở chừng mực lệnh đó liên quan đến tài sản do phạm tội mà có, tài sản, thiết bị hoặc công cụ khác nằm trong lãnh thổ của Quốc gia thành viên được yêu cầu.

2. Theo yêu cầu của một Quốc gia thành viên khác có thẩm quyền đối với một tội phạm được quy định tại Công ước này, Quốc gia thành viên được yêu cầu áp dụng các biện pháp để xác định, truy tìm và phong toả hoặc thu giữ tài sản do phạm tội mà có, tài sản, thiết bị hoặc công cụ khác được đề cập tại Điều 31, khoản 1 của Công ước này với mục đích cuối cùng là tịch thu theo lệnh của Quốc gia thành viên yêu cầu hoặc của Quốc gia thành viên được yêu cầu, căn cứ vào yêu cầu theo khoản 1 của Điều này.

3. Các quy định của Điều 40 của Công ước này được áp dụng đối với Điều này với các sửa đổi cần thiết. Ngoài các thông tin được quy định trong khoản 15 Điều 40 của Công ước này, các yêu cầu theo Điều này phải bao gồm:

(a) Miêu tả về tài sản cần tịch thu, bao gồm, trong phạm vi có thể, địa điểm, và nếu phù hợp, giá trị ước lượng của tài sản và bản trình bày về những tính

tiếp được Quốc gia thành viên yêu cầu dựa vào dù để Quốc gia thành viên được yêu cầu đòi hỏi lệnh tịch thu theo pháp luật quốc gia của mình trong trường hợp văn bản yêu cầu theo khoản 1 (a) của Điều này;

(b) Một bản sao hợp pháp của lệnh tịch thu là cơ sở cho yêu cầu được ban hành bởi Quốc gia thành viên yêu cầu, bản trình bày về những tình tiết và thông tin ở phạm vi mà việc thi hành lệnh đó đòi hỏi, bản trình bày về các biện pháp mà Quốc gia thành viên yêu cầu đưa ra để cung cấp thông tin phù hợp cho các bên thứ ba ngay tình đồng thời để đảm bảo quy trình đúng đắn, và một tuyên bố rằng lệnh tịch thu là lệnh cuối cùng trong trường hợp văn bản yêu cầu theo khoản 1 (b) của Điều này;

(c) Bản trình bày về những tình tiết được Quốc gia thành viên yêu cầu dựa vào và miêu tả về các công việc được yêu cầu và, nếu được, một bản sao hợp pháp của lệnh làm căn cứ cho yêu cầu trong trường hợp văn bản yêu cầu theo khoản 2 của Điều này.

4. Các quyết định hay công việc được quy định trong các khoản 1 và 2 của Điều này được Quốc gia thành viên được yêu cầu thực hiện theo và phù hợp với các quy định của pháp luật quốc gia và các quy tắc về thủ tục của Quốc gia thành viên này hoặc một hiệp định hoặc thỏa thuận song phương hoặc đa phương bất kỳ mà Quốc gia thành viên này bị ràng buộc trong quan hệ với các Quốc gia Thành viên yêu cầu.

5. Mỗi Quốc gia thành viên cung cấp bản sao các luật và quy định để thực hiện Điều này và bản sao các sửa đổi sau đó của các luật và quy định nêu trên hoặc bản trình bày về các văn bản này cho Tổng Thư ký Liên hợp quốc.

6. Nếu một Quốc gia thành viên quyết định áp dụng các biện pháp nêu tại các khoản 1 và 2 của Điều này phụ thuộc vào việc có một điều ước quốc tế liên quan, Quốc gia thành viên đó coi Công ước này là cơ sở pháp lý cần và đủ.

7. Việc hợp tác theo Điều này có thể bị từ chối hoặc các biện pháp tạm thời có thể bị hủy bỏ nếu Quốc gia thành viên được yêu cầu không nhận được bằng chứng đầy đủ và kịp thời hoặc nếu giá trị của tài sản là không đáng kể.

8. Trước khi hủy bỏ các biện pháp tạm thời theo Điều này khi có thể, Quốc gia thành viên được yêu cầu phải tạo cho Quốc gia thành viên yêu cầu cơ hội trình bày lý do nên tiếp tục áp dụng các biện pháp này.

9. Các quy định của Điều này không được hiểu là gây phương hại đến quyền của các bên thứ ba ngay tính.

10. Các Quốc gia thành viên xem xét việc ký kết các điều ước quốc tế song phương hoặc đa phương nhằm nâng cao hiệu quả của việc hợp tác quốc tế được thực hiện theo Điều này.

Điều 51. Hợp tác đặc biệt

Không phương hại đến pháp luật quốc gia của mình, mỗi Quốc gia thành viên cố gắng áp dụng các biện pháp không ảnh hưởng đến việc điều tra, truy tố hoặc xét xử của chính Quốc gia đó để có thể chuyển cho Quốc gia thành viên khác thông tin về tài sản có được từ các tội phạm được quy định tại Công ước mà không cần phải có đề nghị trước, khi xét thấy thông tin tiết lộ có thể giúp Quốc gia thành viên nhận tin báo đầu hoặc tiến hành điều tra, truy tố hoặc xét xử hoặc có thể dẫn đến việc Quốc gia thành viên đó đưa ra yêu cầu theo quy định tại Điều 50 của Công ước này.

Điều 52. Hoàn trả và xử lý tài sản do phạm tội mà có bị tịch thu

1. Tài sản do phạm tội mà có hoặc tài sản bị tịch thu bởi một Quốc gia thành viên, theo Điều 31 hoặc điều 50 của Công ước này được xử lý bởi Quốc gia thành viên đó theo pháp luật và quy trình, thủ tục quốc gia của mình.

2. Trên cơ sở phù hợp với pháp luật quốc gia của mình và được yêu cầu, khi thực hiện theo yêu cầu của một Quốc gia thành viên khác theo Điều 50 của Công ước này, các Quốc gia thành viên xem xét ưu tiên việc hoàn trả tài sản do phạm tội mà có bị tịch thu cho Quốc gia thành viên yêu cầu để Quốc gia thành viên đó có thể bồi thường cho các bị hại của tội phạm hoặc trả lại tài sản do phạm tội mà có cho các chủ sở hữu hợp pháp trước đó.

3. Khi thực hiện theo yêu cầu của một Quốc gia thành viên khác theo Điều 31 và Điều 50 của Công ước này, một Quốc gia thành viên có thể, sau khi đã xem xét đầy đủ việc bồi thường cho các bị hại, xem xét đặc biệt việc ký kết hiệp định và thoả thuận về:

(a) Đóng góp giá trị của tài sản do phạm tội mà có hoặc tiền hoặc quỹ thu được từ việc bán tài sản do phạm tội mà có vào tài khoản được chỉ định theo khoản 2 (c), Điều 56 của Công ước này, và vào các cơ quan liên chính phủ chuyển về chống tội phạm mạng;

(b) Chia sẻ với các Quốc gia thành viên khác, trên cơ sở thường xuyên hoặc theo từng trường hợp, tiền hoặc quỹ hoặc tài sản do phạm tội mà có thu được từ việc bán tài sản do phạm tội mà có, theo pháp luật hoặc quy trình hành chính của quốc gia đó.

4. Khi phù hợp, trừ khi các Quốc gia thành viên quyết định khác, Quốc gia thành viên được yêu cầu có thể khiếu trừ các chi phí hợp lý phát sinh trong quá trình điều tra, truy tố hoặc xét xử dẫn đến việc trả lại hoặc xử lý tài sản bị tịch thu theo Điều này.

Chương VI. Các biện pháp phòng ngừa

Điều 53. Các biện pháp phòng ngừa

1. Mỗi Quốc gia Thành viên nỗ lực, phù hợp với các nguyên tắc cơ bản của pháp luật quốc gia mình, xây dựng và thực hiện hoặc duy trì các chính sách và thực tiễn hiệu quả và phối hợp nhằm giảm thiểu các cơ hội trong hiện tại hoặc tương lai cho tội phạm mạng thông qua các quy định pháp luật hoặc hành chính hoặc các biện pháp khác phù hợp.

2. Mỗi Quốc gia thành viên thực hiện các biện pháp phù hợp, trong khả năng của mình và theo các nguyên tắc cơ bản của pháp luật quốc gia, để khuyến khích sự tham gia tích cực của các cá nhân và các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và các thực thể tư nhân, và công chúng nói chung, trong các khía cạnh liên quan đến việc phòng ngừa các tội phạm được quy định tại Công ước này.

3. Các biện pháp phòng ngừa có thể bao gồm:

(a) Tăng cường hợp tác giữa các cơ quan thực thi pháp luật hoặc kiểm sát viên và các cá nhân, các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và các thực thể tư nhân nhằm giải quyết các khía cạnh liên quan đến việc phòng ngừa và đấu tranh chống các tội phạm được quy định tại Công ước này;

(b) Khuyến khích công chúng nhận thức về sự tồn tại, nguyên nhân và mức độ nghiêm trọng của các mối đe dọa tạo ra bởi các tội phạm được quy định tại Công ước này, thông qua việc cung cấp thông tin, giáo dục cộng đồng, chương trình giảng dạy trên truyền thông nhằm thúc đẩy sự tham gia của công chúng vào việc phòng ngừa và đấu tranh chống lại các tội phạm đó;

(c) Xây dựng và nỗ lực tăng cường năng lực của hệ thống tư pháp hình sự quốc gia, bao gồm đào tạo và phát triển chuyên môn của các chuyên gia tư pháp hình sự,

như một phần của các chiến lược của quốc gia trong phòng ngừa và đấu tranh chống lại các tội phạm được quy định tại Công ước này;

(d) Khuyến khích các nhà cung cấp dịch vụ thực hiện các biện pháp hiệu quả, nêu khả thi trong bối cảnh quốc gia và trên cơ sở pháp luật quốc gia, để tăng cường an ninh cho các sản phẩm, dịch vụ và khách hàng của các nhà cung cấp dịch vụ;

(e) Nhận nhận đóng góp của các hoạt động hợp pháp của các nhà nghiên cứu bảo mật chỉ khi, và trên cơ sở pháp luật quốc gia, nhằm tăng cường và cải thiện an ninh cho các sản phẩm, dịch vụ và khách hàng của các nhà cung cấp dịch vụ trong lãnh thổ của Quốc gia thành viên;

(f) Phát triển, tạo điều kiện và khuyến khích các chương trình và hoạt động nhằm ngăn ngừa những người có nguy cơ tham gia vào tội phạm mạng trở thành tội phạm và phát triển kỹ năng của họ một cách hợp pháp;

(g) Nỗ lực thúc đẩy việc tái hòa nhập vào xã hội của những người bị kết án về các tội phạm được quy định tại Công ước này;

(h) Xây dựng các chiến lược và chính sách, theo pháp luật quốc gia, để ngăn ngừa và xóa bỏ bạo lực về giới xảy ra thông qua việc sử dụng hệ thống công nghệ thông tin và truyền thông, đồng thời cân nhắc các tình huống và nhu cầu đặc biệt của các đối tượng dễ bị tổn thương trong việc phát triển các biện pháp phòng ngừa;

(i) Thực hiện các nỗ lực cụ thể và phù hợp để bảo vệ trẻ em trên môi trường trực tuyến, bao gồm thông qua giáo dục và đào tạo và nâng cao nhận thức công chúng về xâm hại tình dục trẻ em hoặc bóc lột tình dục trẻ em trên mạng, cũng như sửa đổi các khuôn khổ pháp lý trong nước và tăng cường hợp tác quốc tế nhằm phòng ngừa điều này; đồng thời nỗ lực đảm bảo việc gỡ bỏ nhanh chóng các tài liệu có nội dung xâm hại tình dục trẻ em hoặc bóc lột tình dục trẻ em;

(j) Tăng cường tính minh bạch và khuyến khích sự đóng góp của người dân vào quá trình xây dựng chính sách và pháp luật và đảm bảo rằng người dân có quyền tiếp cận thông tin đầy đủ;

(k) Tôn trọng, khuyến khích và bảo vệ quyền tự do tìm kiếm, nhận và truyền đạt thông tin công cộng liên quan đến tội phạm mạng;

(l) Phát triển hoặc tăng cường các chương trình hỗ trợ cho các nạn nhân của các tội phạm được quy định tại Công ước này;

(m) Ngăn ngừa và phát hiện việc chuyển giao tài sản do tội phạm mà có và tài sản liên quan đến các tội phạm được quy định tại Công ước này

4. Mỗi Quốc gia thành viên sẽ thực hiện các biện pháp phù hợp để đảm bảo rằng cơ quan có thẩm quyền liên quan đến việc phòng ngừa và đấu tranh chống tội phạm mạng được người dân biết đến và có thể tiếp cận, nếu phù hợp, để tố cáo, bao gồm cả ẩn danh, bất kỳ hành vi nào có thể được coi là tội phạm theo Công ước này.

5. Các Quốc gia thành viên sẽ nỗ lực đánh giá định kỳ khuôn khổ pháp luật và thực tiễn hành chính quốc gia hiện hành với mục đích xác định các lỗ hổng và điểm yếu và đảm bảo rằng các quy định pháp luật và hành chính phù hợp với những mối đe dọa đang thay đổi do các tội phạm được quy định tại Công ước này.

6. Các Quốc gia thành viên có thể hợp tác với nhau và với các tổ chức quốc tế và khu vực liên quan trong việc thúc đẩy và xây dựng các biện pháp được nêu trong Điều này, bao gồm việc tham gia vào các dự án mạng lưới quốc tế nhằm phòng ngừa tội phạm mạng.

7. Mỗi Quốc gia thành viên thông báo cho Tổng thư ký Liên hợp quốc về tên và địa chỉ của cơ quan hoặc có thể hỗ trợ các Quốc gia thành viên khác trong việc xây dựng các biện pháp cụ thể nhằm phòng ngừa tội phạm mạng.

Chương VII. Hỗ trợ kỹ thuật và trao đổi thông tin

Điều 54. Hỗ trợ kỹ thuật và xây dựng năng lực

1. Các Quốc gia thành viên, theo khả năng của mình, xem xét việc hỗ trợ kỹ thuật và xây dựng năng lực cho nhân viên nhất có thể, bao gồm đào tạo và các hình thức hỗ trợ khác, trao đổi kinh nghiệm và kiến thức chuyên môn liên quan và chuyển giao công nghệ theo thỏa thuận, đặc biệt là xem xét lợi ích và nhu cầu của các Quốc gia thành viên đang phát triển, qua đó tạo điều kiện thuận lợi cho việc phòng ngừa, phát hiện, điều tra và truy tố các tội phạm được Công ước này điều chỉnh.

2. Các Quốc gia thành viên, trong chừng mực cần thiết, đề xuất, xây dựng, thực hiện hoặc nâng cao các chương trình đào tạo cụ thể cho cán bộ phòng ngừa, phát hiện, điều tra và truy tố các tội phạm được Công ước này điều chỉnh.

3. Các hoạt động được đề cập trong các khoản 1 và 2 của Điều này có thể, trên cơ sở pháp luật quốc gia của mình, liên quan đến các vấn đề sau:

(a) Các phương pháp và kỹ thuật sử dụng trong việc phòng ngừa, phát hiện, điều tra và truy tố các tội phạm được Công ước này điều chỉnh;

(b) Xây dựng năng lực trong việc xây dựng và hoạch định các chính sách và quy định mang tính chiến lược để phòng ngừa và đấu tranh chống lại tội phạm mạng;

(c) Xây dựng năng lực trong việc thu thập, bảo quản và chia sẻ chứng cứ, đặc biệt chứng cứ điện tử, bao gồm việc duy trì chuỗi bảo quản và phân tích giám định;

(d) Công cụ thực thi pháp luật và việc sử dụng các công cụ đó;

(e) Đào tạo các cơ quan có thẩm quyền trong việc chuẩn bị các yêu cầu tương trợ tư pháp và các hình thức hợp tác khác đáp ứng yêu cầu của Công ước này, đặc biệt là cho việc thu thập, bảo quản và chia sẻ chứng cứ là dữ liệu điện tử;

(f) Phòng ngừa, phát hiện và theo dõi sự dịch chuyển của tài sản có được từ việc thực hiện các tội phạm được quy định tại Công ước này, tài sản, trang thiết bị hoặc các công cụ khác và các phương pháp sử dụng cho việc chuyển nhượng, che giấu hoặc cải trang của những khoản thu, tài sản, hoặc công cụ đó;

(g) Các cơ chế pháp lý và hành chính phù hợp và hiệu quả để tạo điều kiện cho việc thu giữ, tịch thu và trả lại tiền cơ được từ các tội phạm được quy định tại Công ước này;

(h) Các phương pháp sử dụng trong việc bảo vệ bị hại và nhân chứng hợp tác với các cơ quan tư pháp;

(i) Đào tạo về luật và các quy trình liên quan, thẩm quyền điều tra của cơ quan thực thi pháp luật, cũng như các quy định của quốc gia và quốc tế và bằng các ngôn ngữ khác nhau.

4. Các Quốc gia thành viên, trên cơ sở pháp luật quốc gia của mình, nỗ lực tận dụng chuyên môn và hợp tác chặt chẽ với các Quốc gia thành viên khác và các tổ chức quốc tế và khu vực liên quan, các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và các thực thể tư nhân, nhằm tăng cường hiệu quả thực hiện Công ước này.

5. Các Quốc gia thành viên hỗ trợ lẫn nhau trong việc lập kế hoạch và thực hiện các chương trình nghiên cứu và đào tạo nhằm chia sẻ chuyên môn trong các lĩnh vực được đề cập đến trong khoản 3 của Điều này, và để đạt được mục tiêu đó, các Quốc gia thành viên cũng sẽ, khi phù hợp, tổ chức các hội nghị và hội thảo quốc tế và khu vực nhằm thúc đẩy hợp tác và tăng cường thảo luận về các vấn đề quan tâm chung.

6. Các Quốc gia thành viên xem xét hỗ trợ lẫn nhau, khi có yêu cầu, trong việc thực hiện các đánh giá và nghiên cứu liên quan đến các loại tội phạm, nguyên nhân và tác động của các tội phạm được quy định tại Công ước này mà xảy ra trên lãnh thổ của Quốc gia thành viên, nhằm xây dựng, với sự tham gia của các cơ quan có thẩm quyền và các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và các thực thể tư nhân, các chiến lược và kế hoạch hành động để phòng ngừa và đấu tranh chống lại tội phạm mạng.

7. Các Quốc gia thành viên thúc đẩy đào tạo và hỗ trợ kỹ thuật nhằm tạo điều kiện thuận lợi cho việc dẫn độ và tương trợ tư pháp kịp thời. Việc đào tạo và hỗ trợ kỹ thuật như vậy có thể bao gồm đào tạo về ngôn ngữ, hỗ trợ việc soạn thảo và xử lý các yêu cầu tương trợ tư pháp, và trao đổi giữa nhân viên ở các cơ quan hoặc tổ chức có trách nhiệm liên quan.

8. Các Quốc gia thành viên tăng cường, trong chừng mực có thể, các nỗ lực để tối đa hóa hiệu quả của các hỗ trợ kỹ thuật và xây dựng năng lực trong các tổ chức quốc tế và khu vực và trong khuôn khổ các hiệp định và thoả thuận song phương và đa phương liên quan.

9. Các Quốc gia thành viên xem xét việc thiết lập các cơ chế tự nguyện nhằm đóng góp tái chính cho nỗ lực của các quốc gia đang phát triển để thực hiện Công ước này thông qua các chương trình hỗ trợ kỹ thuật và các dự án xây dựng năng lực.

10. Mỗi Quốc gia thành viên phải nỗ lực đóng góp một cách tự nguyện cho Văn phòng Liên hợp quốc về Ma túy và Tội phạm, nhằm mục đích thông qua Văn phòng này thúc đẩy các chương trình và dự án hỗ trợ kỹ thuật và xây dựng năng lực nhằm thực hiện Công ước này.

Điều 5.5. Trao đổi thông tin

1. Với sự tham vấn của các chuyên gia liên quan, bao gồm từ các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và các thực thể tư nhân, khi phù hợp, mỗi Quốc

gia thành viên xem xét việc phân tích các xu hướng tội phạm trong quốc gia mình được quy định tại Công ước này, cũng như các hoàn cảnh mà tội phạm được thực hiện.

2. Các Quốc gia thành viên cân nhắc xây dựng và chia sẻ số liệu tổng kê, phân tích chuyên môn và thông tin liên quan đến tội phạm mạng với nhau, thông qua các tổ chức quốc tế và khu vực, nhằm mục đích phát triển, trong chừng mực có thể, các định nghĩa, chuẩn mực và phương pháp luận chung, đồng thời chia sẻ thông tin về những thực tiễn tốt nhất về phòng ngừa và đấu tranh chống lại tội phạm này.

3. Mỗi Quốc gia thành viên xem xét về việc điều tiết chính sách và biện pháp thực tiễn của mình để phòng ngừa và đấu tranh chống lại các tội phạm được quy định tại Công ước này và đánh giá tính hiệu quả của các chính sách và biện pháp đó.

4. Các Quốc gia thành viên xem xét trao đổi thông tin về các thay đổi về pháp luật, chính sách và công nghệ liên quan đến tội phạm mạng và việc thu thập chứng cứ là dữ liệu điện tử.

Điều 56. Thực hiện Công ước thông qua phát triển kinh tế và hỗ trợ kỹ thuật

1. Các Quốc gia thành viên, trong chừng mực có thể, phải áp dụng các biện pháp đẩy việc thực hiện tối đa Công ước này thông qua hợp tác quốc tế, có tính đến các tác động tiêu cực của tội phạm được quy định tại Công ước này đối với xã hội nói chung và đối với phát triển bền vững nói riêng.

2. Các Quốc gia thành viên được khuyến khích có các nỗ lực cụ thể, trong chừng mực có thể và trên cơ sở phối hợp với nhau, với các tổ chức quốc tế và khu vực, trong việc:

(a) Tăng cường hợp tác ở các cấp độ khác nhau với các Quốc gia thành viên khác, đặc biệt là các quốc gia đang phát triển, nhằm tăng cường năng lực của các quốc gia này trong việc phòng ngừa và đấu tranh chống lại các tội phạm được quy định tại Công ước này;

(b) Tăng cường hỗ trợ tài chính và vật chất để hỗ trợ các Quốc gia thành viên khác, đặc biệt là các quốc gia đang phát triển, trong việc phòng ngừa và đấu tranh hiệu quả chống lại các tội phạm được quy định tại Công ước và giúp họ thực hiện Công ước này;

(c) Hỗ trợ kỹ thuật cho các Quốc gia thành viên khác, đặc biệt là các quốc gia đang phát triển, giúp họ đáp ứng được các yêu cầu về thực hiện Công ước này. Để đạt

được mục đích này, các Quốc gia thành viên phải nỗ lực đóng góp tự nguyện đều đặn và thích đáng vào một tài khoản được lập đặc biệt cho mục đích này trong một cơ chế tài trợ của Liên hợp quốc;

(d) Khuyến khích, khi phù hợp, các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và thực thể tư nhân, cũng như các tổ chức tái chính, đóng góp vào nỗ lực của các Quốc gia thành viên, bao gồm, cung cấp các chương trình đào tạo và thiết bị hiện đại hơn cho các quốc gia đang phát triển nhằm hỗ trợ các quốc gia này đạt được các mục tiêu của Công ước này;

(e) Trao đổi các thực tiễn tốt và thông tin liên quan đến các hoạt động đã thực hiện nhằm cải thiện tính minh bạch, tránh sự trùng lặp của các nỗ lực của các quốc gia và tận dụng tối đa các chương trình đã có.

3. Các Quốc gia thành viên cũng xem xét tham gia các chương trình mang tính khu vực và quốc tế hiện có, bao gồm các hội nghị và hội thảo, để thúc đẩy hợp tác và hỗ trợ kỹ thuật và tăng cường thảo luận về các vấn đề cùng quan tâm, bao gồm các vấn đề và nhu cầu đặc biệt của các quốc gia đang phát triển.

4. Trong chừng mực có thể, các Quốc gia thành viên đảm bảo rằng các nguồn lực được phân phối và định hướng để hỗ trợ việc hài hòa hoá các chuẩn mực, kỹ năng, năng lực, chuyên môn và khả năng kỹ thuật với mục đích thiết lập các chuẩn mực tối thiểu chung giữa các Quốc gia thành viên để xóa bỏ những nơi ẩn náu an toàn cho các tội phạm được quy định tại Công ước này và tăng cường đấu tranh chống tội phạm mạng.

5. Trong chừng mực có thể, các biện pháp theo Điều này không được gây ảnh hưởng đến các cam kết trợ giúp quốc tế hiện có hoặc đến các thỏa thuận hợp tác tái chính khác ở các cấp độ song phương, khu vực hoặc quốc tế.

6. Các Quốc gia thành viên có thể ký kết các hiệp định, thỏa thuận song phương, khu vực hoặc đa phương về trợ giúp vật chất và hậu cần, có tính đến các thỏa thuận tái chính cần thiết để đảm bảo cho các biện pháp hợp tác quốc tế được quy định tại Công ước này có hiệu quả và nhằm phục vụ việc phòng ngừa, phát hiện, điều tra và truy tố các tội phạm được quy định tại Công ước này.

Chương VIII. Cơ chế thực hiện

Điều 57. Hội nghị các Quốc gia thành viên của Công ước

1. Hội nghị các Quốc gia thành viên của Công ước được thành lập để tăng cường năng lực và hợp tác giữa các Quốc gia thành viên nhằm đạt được các mục tiêu đề ra trong Công ước này và nhằm thúc đẩy và kiểm tra việc thi hành Công ước.

2. Tổng Thư ký Liên hợp quốc triệu tập Hội nghị các Quốc gia thành viên không muộn hơn một năm kể từ khi Công ước này có hiệu lực. Sau đó, các cuộc họp thường kỳ của Hội nghị sẽ được tổ chức theo các quy tắc về thủ tục do Hội nghị thông qua.

3. Hội nghị các Quốc gia thành viên thông qua quy tắc về thủ tục và quy tắc về quản lý các chức năng hoạt động được đề ra tại Điều này, bao gồm các điều lệ gia nhập và chấp thuận tham gia của các quan sát viên, cũng như việc chi trả cho các chi phí phát sinh từ việc tiến hành các hoạt động này. Các quy tắc và hoạt động liên quan này phải tính đến các nguyên tắc như hiệu quả, tính bao trùm, minh bạch, hiệu suất và quyền sở hữu quốc gia.

4. Khi thiết lập các cuộc họp thường kỳ của mình, Hội nghị các Quốc gia thành viên sẽ xem xét thời gian và địa điểm của các cuộc họp của các tổ chức và cơ chế quốc tế, khu vực có liên quan khác trong các vấn đề tương tự, bao gồm các cơ quan chuyên môn, phù hợp với các nguyên tắc được quy định trong khoản 3 của Điều này.

5. Hội nghị các Quốc gia thành viên thống nhất về các hoạt động, quy trình và phương pháp làm việc để đạt được các mục tiêu đã đề ra trong khoản 1 của Điều này, bao gồm:

(a) Tạo điều kiện thuận lợi cho việc sử dụng và thực hiện hiệu quả Công ước, xác định bất kỳ vấn đề nào liên quan đến Công ước, cũng như hoạt động do các Quốc gia thành viên thực hiện theo Công ước này, bao gồm tăng cường huy động các đóng góp tự nguyện;

(b) Tạo điều kiện thuận lợi cho việc trao đổi thông tin về các thay đổi về pháp luật, chính sách và công nghệ liên quan đến các tội phạm được quy định tại Công ước này và việc thu thập chứng cứ là dữ liệu điện tử giữa các Quốc gia thành viên và các tổ chức quốc tế và khu vực có liên quan, cũng như các tổ chức phi chính phủ, tổ chức xã

hội, cơ sở học thuật và thực thể tư nhân, theo pháp luật quốc gia của mình, cũng như về các mô hình và xu hướng của tội phạm mạng và thực tiễn trong việc phòng ngừa và đấu tranh chống lại các tội phạm đó;

(c) Hợp tác với các tổ chức quốc tế và khu vực có liên quan, cũng như các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và thực thể tư nhân;

(d) Sử dụng một cách phù hợp các thông tin liên quan do các tổ chức và cơ chế quốc tế và khu vực khác cung cấp để phòng ngừa và đấu tranh chống lại các tội phạm được quy định lại Công ước này, nhằm tránh sự trùng lặp không cần thiết;

(e) Định kỳ xem xét việc các Quốc gia thành viên thực hiện Công ước này;

(f) Đề xuất việc củng cố Công ước này và việc thực hiện Công ước, cũng như xem xét khả năng bổ sung hoặc sửa đổi Công ước này;

(g) Xây dựng và thông qua các Nghị định thư bổ sung cho Công ước này dựa trên các Điều 61 và 62 của Công ước này;

(h) Ghi nhận các yêu cầu trợ giúp kỹ thuật và nâng cao năng lực của các Quốc gia thành viên liên quan đến việc thực hiện Công ước và khuyến nghị hành động mà Hội nghị cho là cần thiết về vấn đề này.

6. Mỗi Quốc gia thành viên cung cấp cho Hội nghị các Quốc gia thành viên thông tin về các biện pháp lập pháp, hành chính và các biện pháp khác, cũng như thông tin về các chương trình, kế hoạch và thực tiễn để thực hiện Công ước này theo yêu cầu của Hội nghị. Hội nghị phải xem xét cách thức hiệu quả nhất để tiếp nhận và hành động dựa trên thông tin được cung cấp, bao gồm cả thông tin nhận được từ các Quốc gia thành viên và từ các tổ chức quốc tế và khu vực có thẩm quyền. Thông tin nhận được từ các đại diện của các tổ chức phi chính phủ, tổ chức xã hội, cơ sở học thuật và thực thể tư nhân có liên quan được công nhận hợp lệ theo quy trình do Hội nghị quy định cũng có thể được xem xét

7. Vì mục đích của khoản 5 Điều này, Hội nghị các Quốc gia thành viên có thể thành lập và quản lý các cơ chế đánh giá cần thiết.

8. Theo các khoản 5 đến 7 Điều này, Hội nghị các Quốc gia thành viên sẽ thành lập, nếu họ cho là cần thiết, bất kỳ cơ chế hoặc cơ quan chuyên môn nào để hỗ trợ việc thực hiện hiệu quả Công ước.

Điều 58. Ban Thư ký

1. Tổng Thư ký Liên hợp quốc bảo đảm về công tác thư ký cho Hội nghị các Quốc gia thành viên của Công ước này.

2. Ban Thư ký phải:

(a) Trợ giúp Hội nghị các Quốc gia thành viên trong việc tiến hành các hoạt động được quy định Công ước này và chuẩn bị công tác phục vụ cho các kỳ họp của Hội nghị khi liên quan đến Công ước này;

(b) Theo yêu cầu, giúp các Quốc gia thành viên trong việc cung cấp thông tin cho Hội nghị các Quốc gia thành viên, như được quy định tại Công ước này; và

(c) Đảm bảo sự phối hợp cần thiết với Ban Thư ký của các tổ chức quốc tế và khu vực có liên quan.

Chương IX. Các điều khoản cuối cùng

Điều 59. Thực hiện Công ước

1. Mỗi Quốc gia thành viên tiến hành các biện pháp cần thiết, kể cả các biện pháp lập pháp và hành chính, phù hợp với các nguyên tắc cơ bản của pháp luật quốc gia của mình, để thi hành các nghĩa vụ của mình theo Công ước này.

2. Mỗi Quốc gia thành viên có thể áp dụng các biện pháp chặt chẽ và nghiêm khắc hơn so với những biện pháp được quy định tại Công ước này nhằm phòng ngừa và đấu tranh chống lại các tội phạm được quy định tại Công ước này.

Điều 60. Hiệu lực của Công ước

1. Nếu hai hoặc nhiều Quốc gia thành viên đã ký kết thỏa thuận hoặc điều ước quốc tế về các vấn đề được đề cập trong Công ước này hoặc đã thiết lập quan hệ về các vấn đề tương tự, các Quốc gia thành viên đó cũng có quyền áp dụng các thỏa thuận hoặc điều ước quốc tế nêu trên hoặc điều chỉnh các mối quan hệ đó một cách tương ứng.

2. Không quy định nào trong Công ước này ảnh hưởng đến các quyền và nghĩa vụ khác của một Quốc gia thành viên theo pháp luật quốc tế.

Điều 61. Quan hệ với các nghị định thư

1. Công ước này có thể được bổ sung bởi một hoặc nhiều nghị định thư.
2. Để trở thành một Bên tham gia của một nghị định thư, một quốc gia hoặc một tổ chức hội nhập kinh tế khu vực cũng phải là một Bên tham gia Công ước này.
3. Một Quốc gia thành viên của Công ước này không bị ràng buộc bởi một nghị định thư trừ khi quốc gia đó trở thành một Bên tham gia nghị định thư đó theo các quy định của nghị định thư.
4. Bất kỳ nghị định thư nào của Công ước này được giải thích cùng với Công ước này, có tính đến mục đích của nghị định thư đó.

Điều 62. Thông qua các nghị định thư bổ sung

1. Ít nhất 60 Quốc gia thành viên phải tham gia trước khi bất kỳ nghị định thư bổ sung nào được xem xét để thông qua bởi Hội nghị các Quốc gia thành viên. Hội nghị sẽ nỗ lực hết sức để đạt được sự đồng thuận về bất kỳ nghị định thư bổ sung nào. Nếu tất cả các nỗ lực để đạt được sự đồng thuận đã được sử dụng hết và không có thỏa thuận nào đạt được, nghị định thư bổ sung sẽ, như một biện pháp cuối cùng, yêu cầu ít nhất hai phần ba số phiếu thuận của các Quốc gia thành viên có mặt và bỏ phiếu tại cuộc họp của Hội nghị để được thông qua.
2. Các tổ chức hội nhập kinh tế khu vực, trong các vấn đề thuộc thẩm quyền của mình, sẽ thực hiện quyền bỏ phiếu của họ theo Điều này với số phiếu bằng số lượng các quốc gia thành viên của tổ chức đó tham gia Công ước này. Các tổ chức như vậy không thực hiện quyền bỏ phiếu của mình nếu các Quốc gia thành viên của tổ chức đó thực hiện quyền bỏ phiếu của mình và ngược lại.

Điều 63. Giải quyết tranh chấp

1. Các Quốc gia thành viên cố gắng giải quyết các tranh chấp liên quan đến việc giải thích hoặc áp dụng Công ước này thông qua thương lượng hoặc bất kỳ biện pháp hòa bình nào khác do các quốc gia đó lựa chọn.
2. Tranh chấp giữa hai hoặc nhiều Quốc gia thành viên liên quan đến việc giải thích hoặc áp dụng Công ước này mà không thể giải quyết được thông qua thương

lượng hoặc các biện pháp hòa bình khác trong một thời hạn hợp lý, thì theo yêu cầu của một trong các Quốc gia Thành viên đó, được đưa ra trọng tài phân xử. Nếu sau sáu tháng kể từ ngày có yêu cầu đưa tranh chấp ra trọng tài mà các Quốc gia thành viên đó không thể thoả thuận được về tổ chức trọng tài thì bất kỳ Quốc gia thành viên nào trong số các quốc gia thành viên tranh chấp đều có thể đưa tranh chấp ra Tòa án Công lý quốc tế theo Quy chế của Tòa án này

3. Mỗi Quốc gia thành viên, tại thời điểm ký, phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập Công ước này, có thể tuyên bố là mình không bị ràng buộc bởi khoản 2 của Điều này. Các Quốc gia thành viên khác sẽ không bị ràng buộc bởi khoản 2 của Điều này đối với các quốc gia đã đưa ra báo lưu nội trên.

4. Quốc gia thành viên đã đưa ra báo lưu theo khoản 3 của Điều này có thể rút lại báo lưu đó tại bất kỳ thời điểm nào bằng việc thông báo cho Tổng Thư ký Liên hợp quốc.

Điều 64. Ký, phê chuẩn, chấp nhận, phê duyệt và gia nhập

1. Công ước này được mở cho tất cả các Quốc gia ký tại Hà Nội năm 2025 và sau đó tại Trụ sở Liên Hợp Quốc ở New York cho đến ngày 31 tháng 12 năm 2026.

2. Công ước này cũng sẽ được mở cho các tổ chức hội nhập kinh tế khu vực, với điều kiện có ít nhất một quốc gia thành viên của tổ chức đó đã ký Công ước này theo quy định tại khoản 1 của Điều này.

3. Công ước này phải được phê chuẩn, chấp thuận hoặc phê duyệt. Các văn kiện phê chuẩn, chấp thuận hoặc phê duyệt phải được gửi cho Tổng Thư ký Liên hợp quốc. Tổ chức hội nhập kinh tế khu vực có thể nộp văn kiện phê chuẩn, chấp thuận hoặc phê duyệt của mình nếu có ít nhất một quốc gia thành viên của tổ chức đó đã nộp văn kiện đó. Trong văn kiện phê chuẩn, chấp thuận hoặc phê duyệt đó, tổ chức này sẽ tuyên bố về phạm vi thẩm quyền của mình; liên quan đến các vấn đề mà Công ước điều chỉnh. Tổ chức nêu trên cũng sẽ thông báo cho cơ quan lưu trữ về bất kỳ sự thay đổi nào liên quan đến phạm vi thẩm quyền của mình.

4. Công ước này mở cho tất cả các quốc gia hoặc tổ chức hội nhập kinh tế khu vực gia nhập, có ít nhất một quốc gia thành viên của tổ chức nêu trên là thành viên của Công ước này. Văn kiện gia nhập sẽ được Tổng Thư ký Liên hợp quốc lưu trữ. Tại thời điểm gia

nhập, tổ chức hội nhập kinh tế khu vực phải tuyên bố về phạm vi thẩm quyền của mình liên quan đến các vấn đề mà Công ước điều chỉnh. Tổ chức nêu trên cũng phải thông báo cho cơ quan lưu chiểu về bất kỳ sự thay đổi nào liên quan đến phạm vi thẩm quyền của mình.

Điều 65.- Hiệu lực

1. Công ước này sẽ có hiệu lực vào ngày thứ chín mươi sau ngày thứ 40 văn kiện phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập được lưu chiểu. Vì mục đích của khoản này, văn kiện được nộp bởi tổ chức hội nhập kinh tế khu vực nộp sẽ không được tính để bổ sung cho các văn kiện do các quốc gia thành viên của tổ chức đó đã nộp.

2. Đối với mỗi quốc gia và các tổ chức hội nhập kinh tế khu vực phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập Công ước này sau khi có 40 văn kiện phê chuẩn, chấp thuận, phê duyệt hoặc gia nhập được lưu chiểu, thì Công ước này sẽ có hiệu lực vào ngày thứ ba mươi sau ngày quốc gia hay tổ chức đó nộp văn kiện liên quan hoặc vào ngày Công ước này có hiệu lực theo quy định tại khoản 1 của Điều này, tùy thuộc vào ngày nào muộn hơn.

Điều 66. Sửa đổi

1. Sau khi hết năm năm kể từ ngày Công ước này có hiệu lực, một Quốc gia thành viên có thể đề nghị sửa đổi và chuyển đề nghị này cho Tổng Thư ký Liên hợp quốc, và sau đó Tổng Thư ký sẽ thông báo đề nghị sửa đổi cho các Quốc gia thành viên và Hội nghị các Quốc gia thành viên của Công ước để xem xét và quyết định về đề nghị đó. Hội nghị các Quốc gia thành viên nỗ lực để đạt được sự đồng thuận về đề nghị sửa đổi. Nếu mọi nỗ lực để đạt được sự đồng thuận đã được thực hiện nhưng vẫn không đạt được sự đồng thuận về đề nghị sửa đổi, thì đề đề nghị sửa đổi được thông qua cần được sự đồng ý của ít nhất hai phần ba tất cả các Quốc gia thành viên có mặt và bỏ phiếu tại phiên họp của Hội nghị các Quốc gia thành viên.

2. Các tổ chức hội nhập kinh tế khu vực, liên quan đến các vấn đề thuộc phạm vi thẩm quyền của mình, thực hiện quyền bỏ phiếu theo Điều này với số lượng phiếu bằng số lượng các quốc gia thành viên của tổ chức đó là Quốc gia thành viên của Công ước này. Các tổ chức nói trên không được thực hiện quyền bỏ phiếu của mình nếu các quốc gia thành viên của họ thực hiện các quyền này và ngược lại.

3. Bất kỳ sửa đổi nào được thông qua theo quy định tại khoản 1 của Điều này cần được các Quốc gia thành viên phê chuẩn, chấp thuận hoặc phê duyệt.

4. Việc sửa đổi được thông qua theo quy định tại khoản 1 của Điều này sẽ có hiệu lực đối với Quốc gia thành viên vào ngày thứ 90 sau ngày nộp cho Tổng Thư ký Liên hợp quốc văn kiện phê chuẩn, chấp thuận hoặc phê duyệt sửa đổi.

5. Khi sửa đổi có hiệu lực, sửa đổi này sẽ ràng buộc đối với các Quốc gia thành viên đã thể hiện sự đồng ý của mình về sự ràng buộc đó. Các Quốc gia thành viên khác vẫn bị ràng buộc bởi các quy định của Công ước này và các sửa đổi trước đó mà các quốc gia này đã phê chuẩn, chấp thuận hoặc phê duyệt.

Điều 67. Từ bỏ

1. Quốc gia thành viên có thể từ bỏ Công ước này bằng một thông báo bằng văn bản gửi cho Tổng Thư ký Liên hợp quốc. Việc từ bỏ sẽ có hiệu lực một năm sau ngày Tổng Thư ký nhận được thông báo nêu trên.

2. Tổ chức hội nhập kinh tế khu vực sẽ không còn là một thành viên của Công ước này khi tất cả các quốc gia thành viên của tổ chức đó đã từ bỏ Công ước này.

3. Việc từ bỏ Công ước theo quy định tại khoản 1 của Điều này sẽ kéo theo việc từ bỏ bất kỳ nghị định thư nào liên quan đến Công ước.

Điều 68. Lưu chiều và ngôn ngữ

1. Tổng Thư ký Liên hợp quốc được chỉ định làm người lưu chiều Công ước này.

2. Các bản gốc của Công ước này, mà các bản tiếng Ả Rập, Trung Quốc, Anh, Pháp, Nga và Tây Ban Nha đều có giá trị như nhau và sẽ được lưu chiều cho Tổng Thư ký Liên hợp quốc.

ĐỂ LÀM BẰNG, các đại diện toàn quyền ký tên dưới đây, được ủy quyền chính thức một cách hợp lệ, đã ký Công ước này.

BÁO CÁO

ĐÁNH GIÁ TÁC ĐỘNG CHÍNH TRỊ, QUỐC PHÒNG, AN NINH, KINH TẾ - XÃ HỘI VÀ CÁC TÁC ĐỘNG KHÁC VỀ VIỆC KÝ CÔNG ƯỚC LIÊN HIỆP QUỐC VỀ CHỐNG TỘI PHẠM MẠNG

(Kèm theo Tờ trình số /TTr-BNG-LPQT ngày / /2025 của Bộ Ngoại giao)

1. Tội phạm mạng đang ngày càng trở thành một trong những mối đe dọa lớn nhất đối với sự ổn định kinh tế, xã hội và an ninh quốc gia trên phạm vi toàn cầu. Giai đoạn từ năm 2022 đến 2024 chứng kiến sự leo thang chưa từng có của các hoạt động phạm tội trên không gian mạng, cả về quy mô, mức độ tinh vi lẫn hậu quả để lại. Các hình thức tội phạm phổ biến như mã độc tống tiền (ransomware), lừa đảo trực tuyến, xâm phạm dữ liệu cá nhân, giả mạo thư điện tử doanh nghiệp, phần mềm gián điệp, gian lận thương mại điện tử và các cuộc tấn công từ chối dịch vụ (DDoS) không chỉ gây tổn thất hàng nghìn tỷ đô-la Mỹ mỗi năm mà còn để lại những vết thương tâm lý sâu sắc, làm gián đoạn hoạt động của doanh nghiệp và đe dọa trực tiếp đến hạ tầng trọng yếu của các quốc gia.

Theo các tổ chức an ninh mạng hàng đầu thế giới, năm 2022, tổng thiệt hại kinh tế toàn cầu do tội phạm mạng gây ra ước tính khoảng 8 nghìn tỷ USD. Sang năm 2023, con số này đã vượt ngưỡng 11 nghìn tỷ USD, và dự kiến đạt mốc 10,5 nghìn tỷ USD vào năm 2025. Đáng chú ý, Trung tâm Khiếu nại Tội phạm Internet (IC3) của Cục Điều tra Liên bang Mỹ (FBI) đã ghi nhận hơn 880.000 vụ việc được báo cáo trong năm 2023, với tổng thiệt hại lên tới 12,5 tỷ USD, tăng hơn 22% so với năm trước. Các loại tội phạm mạng gây thiệt hại nặng nề nhất bao gồm lừa đảo đầu tư với 4,57 tỷ USD thiệt hại, giả mạo thư điện tử doanh nghiệp (BEC) chiếm đoạt 2,9 tỷ USD, lừa đảo hỗ trợ kỹ thuật với mức thiệt hại gần 925 triệu USD và ransomware tuy chỉ ghi nhận chính thức khoảng 59,6 triệu USD tại Mỹ, nhưng theo phân tích blockchain, số tiền chuộc mà các nhóm tin tặc thu được từ nạn nhân trên toàn cầu trong năm 2023 thực tế đã vượt mức 1,1 tỷ USD.

Bên cạnh tổn thất về tài chính, tác động về mặt tâm lý và cảm xúc đối với nạn nhân là không thể xem nhẹ. Một nghiên cứu toàn cầu cho thấy có tới 54% nạn nhân các vụ lừa đảo mạng báo cáo rằng họ trải qua tổn thương tinh thần nghiêm trọng, bao gồm lo âu kéo dài, trầm cảm, mất ngủ và thậm chí là ý nghĩ tự tử. Hành vi lừa đảo, đánh cắp danh tính và các hình thức quấy rối qua mạng đã khiến hàng triệu người

mất lòng tin vào không gian số, từ đó hạn chế khả năng tiếp cận các dịch vụ số vốn đang ngày càng trở nên thiết yếu trong đời sống hiện đại.

Đối với các doanh nghiệp, tội phạm mạng là mối đe dọa trực tiếp tới khả năng vận hành liên tục và uy tín thương hiệu. Các cuộc tấn công bằng mã độc tổng tiền thường khiến hệ thống công nghệ thông tin bị đóng băng hoàn toàn. Trung bình, một cuộc tấn công bằng ransomware vào hệ thống y tế gây gián đoạn 17 ngày, với tổn thất kinh tế lên đến 1,9 triệu USD cho mỗi ngày ngừng hoạt động. Chi phí phục hồi sau mỗi vụ vi phạm dữ liệu lên tới 4,45 triệu USD, trong đó bao gồm chi phí khắc phục, tổn thất khách hàng, chi phí pháp lý và các khoản phạt hành chính. Nhiều doanh nghiệp, kể cả khi chấp nhận trả tiền chuộc, vẫn không thể khôi phục hoàn toàn dữ liệu, dẫn đến những hậu quả kéo dài về năng suất lao động, niềm tin khách hàng và uy tín trên thị trường.

Không chỉ dừng lại ở khía cạnh kinh tế và doanh nghiệp, tội phạm mạng còn đang đe dọa nghiêm trọng đến an ninh quốc gia. Các cuộc tấn công nhắm vào cơ sở hạ tầng thiết yếu như lưới điện, hệ thống cung ứng năng lượng, giao thông và viễn thông đang gia tăng nhanh chóng. Trong giai đoạn từ tháng 1/2023 đến tháng 1/2024, các cơ sở hạ tầng trọng yếu trên toàn cầu đã phải hứng chịu hơn 420 triệu cuộc tấn công mạng, tương đương với khoảng 13 cuộc tấn công mỗi giây. Các hệ thống của chính phủ, quốc phòng và cơ quan tình báo cũng trở thành mục tiêu của các nhóm tin tặc nước ngoài, với mục đích gián điệp, phá hoại hoặc gây rối loạn. Nhiều quốc gia đã buộc phải nâng cấp mức cảnh báo an ninh mạng lên mức cao nhất, coi đây là một phần không thể tách rời trong chiến lược an ninh quốc gia.

2. Tại Việt Nam, tình hình tội phạm mạng cũng đang diễn biến vô cùng phức tạp. Là quốc gia có tốc độ phát triển kinh tế số nhanh, với hơn 77 triệu người dùng Internet và tỷ lệ sử dụng mạng xã hội cao hàng đầu khu vực, Việt Nam đã trở thành điểm nhắm của nhiều tổ chức tội phạm mạng xuyên quốc gia. Theo báo cáo công bố năm 2023 của Tổ chức Toàn cầu Chống Lừa đảo (GASA), người dân Việt Nam đã bị lừa mất tổng cộng 391.800 tỷ đồng, tương đương 16,23 tỷ USD – chiếm 3,6% tổng GDP quốc gia. Trung bình mỗi nạn nhân tại Việt Nam bị thiệt hại 17,7 triệu đồng (tương đương 737 USD), một con số đáng báo động cho thấy mức độ nghiêm trọng của vấn nạn lừa đảo trên không gian mạng.

Các hình thức lừa đảo phổ biến nhất tại Việt Nam bao gồm lừa đảo đầu tư tài chính qua mạng, giả mạo cơ quan công an hoặc ngân hàng để yêu cầu chuyển tiền, giả danh người quen qua mạng xã hội, và lừa đảo bán hàng trực tuyến. Theo khảo sát, có tới 70% người dân cho biết họ gặp phải các hình thức lừa đảo qua mạng ít

nhất một lần mỗi tháng. Đặc biệt, 29% người được hỏi thừa nhận đã bị mất tiền vào một hình thức lừa đảo nào đó trong năm vừa qua. Ngoài ra, các nền tảng như Facebook, Gmail và Zalo là những kênh bị khai thác phổ biến nhất để thực hiện hành vi lừa đảo, do mức độ phổ biến và tính tương tác cao.

Không chỉ dừng lại ở cấp độ cá nhân, nhiều doanh nghiệp tại Việt Nam cũng là nạn nhân của các cuộc tấn công mạng có chủ đích. Một số vụ việc nghiêm trọng đã gây rúng động dư luận. Đơn cử như vụ việc xảy ra vào tháng 3/2023, công ty chứng khoán VNDirect – một trong những sàn giao dịch lớn nhất Việt Nam – đã bị mã độc tống tiền tấn công, khiến toàn bộ hệ thống bị tê liệt trong nhiều ngày, hàng trăm nghìn nhà đầu tư không thể giao dịch hoặc rút tiền. Ngay sau đó, đến tháng 4/2023, Công ty Cổ phần Xăng dầu Dầu khí Việt Nam (PVOIL) – đơn vị phân phối nhiên liệu trên toàn quốc – cũng bị mã độc tấn công, làm gián đoạn hệ thống cung ứng xăng dầu và đặt ra nguy cơ thiếu hụt nhiên liệu nếu không được khắc phục kịp thời.

Theo Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), năm 2023, hệ thống đã ghi nhận 13.900 vụ tấn công mạng tại Việt Nam – tăng 9,5% so với năm 2022. Chỉ trong quý I/2024, hơn 20 triệu cảnh báo tấn công mạng đã được ghi nhận – tăng 33% so với cùng kỳ năm trước. Đáng chú ý, 25,3% các vụ tấn công nhằm vào website doanh nghiệp, gây gián đoạn hoạt động, mất doanh thu và ảnh hưởng đến uy tín thương hiệu. Phần lớn doanh nghiệp nhỏ và vừa tại Việt Nam chưa có hệ thống phòng thủ mạng đủ mạnh, dẫn đến khả năng phục hồi sau sự cố thấp, mất nhiều ngày hoặc thậm chí hàng tuần để khôi phục hoạt động.

Về phía chính phủ, nhiều cơ quan nhà nước tại trung ương và địa phương đã trở thành mục tiêu tấn công của các nhóm tin tặc có tổ chức. Một số vụ tấn công có dấu hiệu cho thấy sự can dự của các nhóm hacker nước ngoài, với mục đích thu thập thông tin nhạy cảm, gián điệp kinh tế hoặc phá hoại hệ thống điều hành. Các cuộc tấn công mạng và tội phạm mạng có thể dẫn đến nguy cơ lộ, lọt bí mật nhà nước, tạo điều kiện để các thế lực thù địch lợi dụng khai thác, gây bất lợi nghiêm trọng cho Việt Nam. Các hoạt động này đặt ra áp lực đối với đất nước trên nhiều phương diện, đặc biệt là về vấn đề chủ quyền quốc gia, khi chúng thường đi kèm với các hành vi tuyên truyền, xuyên tạc, vu cáo và chống phá, tập trung vào các vấn đề như dân chủ, nhân quyền, cũng như thể chế và chính sách của nhà nước. Các cơ quan chức năng Việt Nam đã tăng cường phối hợp với INTERPOL, ASEAN và các tổ chức an ninh mạng quốc tế nhằm truy vết các dòng tiền phi pháp, truy bắt đối tượng và nâng cao khả năng ứng phó. Thủ tướng Chính phủ cũng đã có chỉ đạo yêu cầu tất cả các cơ

quan nhà nước, doanh nghiệp trọng yếu phải tiến hành rà soát, đánh giá và nâng cấp hệ thống an ninh mạng ở mức cao nhất.

Tội phạm mạng tại Việt Nam hiện nay có đầy đủ các loại hình phổ biến như trên thế giới, bao gồm ransomware, phishing, vi phạm dữ liệu, giả mạo thư điện tử doanh nghiệp, phần mềm gián điệp, gian lận trực tuyến và tấn công DDoS. Trong đó, phishing chiếm tỷ lệ cao nhất, khoảng 32,6% tổng số vụ việc, do người dùng Việt Nam dễ bị đánh lừa qua các đường dẫn giả mạo trên mạng xã hội, email hoặc ứng dụng nhắn tin. Các vụ rò rỉ dữ liệu cá nhân tuy chưa ở quy mô lớn như các quốc gia phát triển nhưng cũng đã xuất hiện, đặc biệt là trong lĩnh vực thương mại điện tử và tài chính. Một số dữ liệu cá nhân người Việt đã bị rao bán trên các diễn đàn chợ đen quốc tế.

3. Với thực trạng nói trên, có thể khẳng định rằng tội phạm mạng đang gây ra những thiệt hại nghiêm trọng, toàn diện và lâu dài tại Việt Nam. Không chỉ gây tổn thất về tiền bạc, làm xáo trộn cuộc sống, tội phạm mạng còn tạo ra cảm giác bất an trong xã hội, làm tổn hại niềm tin vào công nghệ và cản trở tiến trình chuyển đổi số. Hoạt động tấn công hệ thống mạng và các loại tội phạm sử dụng không gian mạng đang trở thành những vấn đề hết sức nghiêm trọng, gây ra những tác động tiêu cực sâu rộng đến nhiều lĩnh vực của đời sống xã hội. Đây không chỉ là một trong những yếu tố làm mất ổn định xã hội mà còn ảnh hưởng trực tiếp đến an ninh quốc gia.

Ngoài ra, những hoạt động tấn công mạng và tội phạm mạng còn gây ra những hệ quả mang tính toàn cầu, làm xói mòn lòng tin giữa các quốc gia, đe dọa hòa bình, an ninh và sự ổn định của khu vực cũng như thế giới. Điều này càng khiến cho việc đối phó với tội phạm mạng trở thành một ưu tiên cấp bách, không chỉ đối với từng quốc gia mà còn là trách nhiệm chung của cộng đồng quốc tế.

4. Việc Việt Nam ký kết Công ước quốc tế về phòng chống tội phạm công nghệ cao sẽ tạo ra một cơ sở pháp lý vững chắc, cho phép các cơ quan chức năng trong nước đẩy mạnh hợp tác với các quốc gia khác trong khu vực và trên thế giới. Đặc biệt, sự hợp tác này sẽ hướng đến các quốc gia lớn và những nước có nền công nghệ thông tin phát triển. Điều này không chỉ mở ra cơ hội tiếp cận các chương trình hỗ trợ kỹ thuật, hoạt động đào tạo nâng cao năng lực mà còn thúc đẩy việc chuyển giao công nghệ, giúp tăng cường năng lực của các cơ quan thực thi pháp luật. Thông qua đó, Việt Nam sẽ có thêm điều kiện để bảo vệ an ninh quốc gia, nâng cao hiệu quả trong công tác phòng chống tội phạm mạng, đồng thời làm sâu sắc hơn quan hệ song phương với các nước đối tác. Những nỗ lực này sẽ góp phần đưa các mối quan hệ

hợp tác đi vào thực chất, thúc đẩy sự phát triển toàn diện và bền vững trong bối cảnh toàn cầu hóa hiện nay.

5. Công ước sẽ được mở ký tại Hà Nội trong năm 2025. Việc ta vận động thành công đề Đại hội đồng Liên hợp quốc lựa chọn Hà Nội làm địa điểm Lễ mở ký Công ước là dấu ấn quan trọng trong đối ngoại đa phương và 47 năm quan hệ Việt Nam – Liên hợp quốc. Đây là Công ước đầu tiên của Liên hợp quốc về tội phạm mạng và là lần đầu tiên một văn kiện quốc tế được mở ký tại Việt Nam, ghi nhận Thủ đô Hà Nội trong lời văn và tên Công ước, phản ánh sự ghi nhận cao của cộng đồng quốc tế đối với những nỗ lực và cam kết của ta trong thúc đẩy hợp tác đa phương.

Do đó, việc ta sớm hoàn thành các thủ tục nội bộ để thúc đẩy việc chuẩn bị tốt cho Lễ mở ký và tiến tới phê chuẩn Công ước sẽ mang ý nghĩa chính trị to lớn, tiếp tục thể hiện nỗ lực và cam kết của ta trong thúc đẩy hợp tác đa phương, đề cao vai trò và giá trị của Hiến chương Liên hợp quốc và luật pháp quốc tế, tích cực đóng góp vào công việc chung của Liên hợp quốc, tham gia giải quyết các vấn đề toàn cầu, trong đó có tội phạm mạng./.

BÁO CÁO
ĐÁNH GIÁ SỰ PHÙ HỢP GIỮA QUY ĐỊNH CỦA CÔNG ƯỚC
LIÊN HỢP QUỐC VỀ CHỐNG TỘI PHẠM MẠNG VỚI QUY ĐỊNH
CỦA PHÁP LUẬT VIỆT NAM

(Kèm theo Tờ trình số /TTr-BNG-LPQT ngày / /2025 của Bộ Ngoại giao)

1. Về sự phù hợp với các quy định pháp luật hiện hành Việt Nam:

Qua rà soát, các quy định của Công ước Liên hợp quốc về chống tội phạm mạng không trái với Hiến pháp năm 2013, phù hợp với các quy định hiện hành của Luật Điều ước quốc tế 2016, Bộ luật Hình sự năm 2015, Bộ luật Hình sự sửa đổi năm 2017, Bộ luật Tố tụng hình sự năm 2015, Bộ luật Tố tụng hình sự sửa đổi năm 2021 (hiện đang được sửa đổi, bổ sung tại Kỳ họp thứ 9, Quốc hội khóa XV năm 2025), Bộ luật Dân sự năm 2015, Luật An ninh mạng năm 2018, Luật An toàn thông tin mạng năm 2015, Luật Lý lịch tư pháp năm 2009, Luật Trợ giúp pháp lý năm 2017, Nghị định 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân (hiện dự án Luật Bảo vệ dữ liệu cá nhân đang được hoàn thiện và thảo luận tại Kỳ họp thứ 9, Quốc hội khóa XV)...

Việc ký kết Công ước Liên hợp quốc về phòng chống tội phạm mạng phù hợp với quy định của Luật Điều ước quốc tế 2016, Bộ luật Hình sự năm 2015, Bộ luật Hình sự sửa đổi năm 2017, Bộ luật Tố tụng hình sự năm 2015, Bộ luật Tố tụng hình sự sửa đổi năm 2021, Bộ luật Dân sự năm 2015, Luật An ninh mạng năm 2018, Luật An toàn thông tin mạng năm 2015, Luật Công nghệ thông tin năm 2006, Luật Lý lịch tư pháp năm 2009, Luật Tương trợ tư pháp năm 2007, Luật Trẻ em năm 2016, sửa đổi bổ sung năm 2018, Luật Trợ giúp pháp lý năm 2017, Luật Giao dịch điện tử năm 2023, Luật Viễn thông năm 2023, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân, Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng... *(Bảng chi tiết kèm theo).*

2. Các quy định của Công ước Liên hợp quốc về chống tội phạm mạng phù hợp với Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia; chủ trương bảo vệ vững chắc chủ quyền, lợi ích quốc gia, xây dựng không gian mạng an toàn, lành mạnh, trở thành nguồn lực quan trọng để xây dựng, phát triển và bảo vệ tổ quốc tại Nghị quyết số 30-NQ/TW ngày 25/07/2018 của Bộ Chính trị, phù hợp với chủ trương về xây dựng, hoàn thiện hệ thống pháp luật về phòng, chống tội phạm mạng

của Chiến lược quốc gia phòng, chống tội phạm mạng giai đoạn 2016-2025 và định hướng đến năm 2030 ban hành kèm Quyết định số 623/QĐ-TTg ngày 14/4/2016 của Thủ tướng Chính phủ./.

BÁO CÁO

ĐÁNH GIÁ SỰ PHÙ HỢP GIỮA QUY ĐỊNH CỦA CÔNG ƯỚC LIÊN HỢP QUỐC VỀ CHỐNG TỘI PHẠM MẠNG VỚI CÁC ĐIỀU ƯỚC QUỐC TẾ TRONG CÙNG LĨNH VỰC MÀ VIỆT NAM LÀ THÀNH VIÊN

(Kèm theo Tờ trình số /TTr-BNG-LPQT ngày / /2025 của Bộ Ngoại giao)

Công ước Liên hợp quốc về chống tội phạm mạng về cơ bản tương thích với các điều ước quốc tế trong cùng lĩnh vực mà Việt Nam là thành viên, trong đó có Công ước Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia, Công ước Liên hợp quốc về chống tham nhũng, Công ước Liên hợp quốc về chống mua bán trái phép chất ma túy và các chất hướng thần (*Bảng chi tiết kèm theo*). Cụ thể:

- Khoản 1 Điều 4 Công ước này quy định các hành vi phạm tội được quy định trong các công ước và nghị định thư khác của Liên hợp quốc cũng được coi là hành vi phạm tội khi được thực hiện thông qua việc sử dụng các hệ thống công nghệ thông tin và truyền thông; khoản 1 Điều 35 Công ước này quy định các quốc gia thành viên sẽ hợp tác trong thu nhập, tiếp nhận, bảo quản và chia sẻ chứng cứ điện tử với mọi tội phạm nghiêm trọng, bao gồm tội phạm nghiêm trọng theo quy định của các công ước và nghị định thư của Liên hợp quốc đang có hiệu lực vào thời điểm Công ước này được thông qua.

- Các quy định về hình sự hoá các hành vi phạm tội trong Công ước này không mâu thuẫn với các quy định tương ứng của Công ước Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia, Công ước Liên hợp quốc về chống tham nhũng, Công ước Liên hợp quốc về chống mua bán trái phép chất ma túy và các chất hướng thần.

- Các quy định về hợp tác quốc tế, tương trợ tư pháp trong Công ước này cơ bản tương tự và không mâu thuẫn với các quy định tương ứng của Công ước Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia, Công ước Liên hợp quốc về chống tham nhũng, Công ước Liên hợp quốc về chống mua bán trái phép chất ma túy và các chất hướng thần; đồng thời, Công ước cũng cho phép các Quốc gia thành viên xem xét khả năng ký kết các hiệp định hoặc thỏa thuận song phương hoặc đa phương nhằm thực hiện các hoạt động dẫn độ, tương trợ tư pháp và hợp tác quốc tế khác./.