HOÀN THIỆN PHÁP LUẬT VIỆT NAM ĐÁP ỨNG YÊU CẦU NỘI LUẬT HÓA CÔNG ƯỚC HÀ NỘI

NGUYỄN HUỲNH BẢO KHÁNH*

Công ước Liên Hợp quốc về chống tội phạm mạng (Công ước Hà Nội) đóng vai trò là khung pháp lý toàn cầu đầu tiên nhằm đấu tranh với tội phạm mạng trong kỷ nguyên số; đồng thời, mang ý nghĩa đặc biệt quan trọng. Việc Việt Nam gia nhập văn kiện này không chỉ đơn thuần là hoàn thành nghĩa vụ quốc tế mà còn là nền tảng cho công cuộc hiện đại hóa hệ thống pháp luật. Bài viết phân tích các yêu cầu cơ bản của Công ước Hà Nội, như: tội phạm hóa hành vi, cơ chế chứng cứ điện tử, hợp tác quốc tế và bảo đảm nhân quyền, từ đó, đối chiếu với độ tương thích của pháp luật hiện hành. Kết quả cho thấy, dù quá trình nội luật hóa đã có sự chuẩn bị tích cực, Việt Nam vẫn cần hoàn thiện hệ thống pháp luật và nâng cao năng lực áp dụng pháp luật để bảo đảm hiệu quả phòng, chống tội phạm và hội nhập quốc tế.

Từ khóa: *Nội luật hóa; tội phạm mạng; Công ước Hà Nội; hoàn thiện pháp luật.*

The United Nations Convention against Cybercrime (the Hanoi Convention) serves as the first global legal framework for combating cybercrime in the digital age and carries particular significance. Vietnam's accession to this Convention is not merely the fulfillment of an international obligation, but also provides a foundation for modernizing the national legal system. This article analyses the Convention's core requirements, including the criminalization of conduct, electronic evidence mechanisms, international cooperation, and human rights safeguards, and assesses their compatibility with Vietnam's current legal framework. The findings indicate that, despite positive preparatory efforts for domestic implementation, Vietnam still needs to further improve its legal framework and strengthen law enforcement capacity to ensure effective cybercrime prevention and control, as well as deeper international integration.

Keywords: *Domestic implementation; cybercrime; Hanoi Convention; legal improvement.*

NGÀY NHẬN: 16/12/2025 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 19/4/2026 NGÀY DUYỆT: 18/5/2026

DOI: https://doi.org/10.59394/qlnn.364.2026.1515

1. Đặt vấn đề

Sự phát triển nhanh chóng của công nghệ số và không gian mạng đã tạo ra những biến đổi sâu sắc trong đời sống kinh tế - xã hội. Bên cạnh những tác động tích cực, môi trường số cũng đặt ra nhiều thách thức với an ninh quốc gia và trật tự an toàn xã hội, điển hình là sự gia tăng của tội phạm sử dụng công nghệ cao với tính chất xuyên biên giới và phương thức thủ đoạn ngày càng tinh vi. Thực tiễn cho thấy, các quy định pháp lý riêng lẻ của từng quốc gia đang gặp những giới hạn nhất định trong

* *TS, Trường Đại học Luật TP. Hồ Chí Minh*

việc kiểm soát và xử lý tội phạm mạng. Trong bối cảnh đó, việc Đại hội đồng Liên Hợp quốc thông qua Công ước về chống tội phạm mạng (Công ước Hà Nội) đã thiết lập một cơ chế hợp tác đa phương thống nhất, tạo cơ sở pháp lý quốc tế quan trọng cho hoạt động phòng ngừa và đấu tranh với loại hình tội phạm này. Đối với Việt Nam, đây là bước đi cụ thể hóa đường lối đối ngoại và hội nhập quốc tế của Đảng và Nhà nước và đặt ra yêu cầu khách quan về việc rà soát, hoàn thiện hệ thống pháp luật trong nước.

Mặc dù, Quốc hội đã ban hành nhiều văn bản quy phạm pháp luật quan trọng, như: *Bộ luật Hình sự* năm 2015, *Bộ luật Tố tụng hình sự* năm 2015, *Luật An ninh mạng* năm 2018..., tạo lập hành lang pháp lý cơ bản cho công tác phòng, chống tội phạm mạng. Tuy nhiên, đối chiếu với các chuẩn mực mới của Công ước Hà Nội và thực tiễn áp dụng pháp luật, hệ thống quy định hiện hành vẫn còn những khoảng trống và điểm chưa thống nhất, đặc biệt trong các quy định về thu thập chứng cứ điện tử và tương trợ tư pháp hình sự. Do đó, việc nghiên cứu các yêu cầu của Công ước để đề xuất giải pháp hoàn thiện pháp luật Việt Nam là nhiệm vụ cần thiết nhằm bảo đảm hiệu lực, hiệu quả quản lý nhà nước và thực hiện nghĩa vụ thành viên của các điều ước quốc tế mà Việt Nam gia nhập.

2. Nội dung cơ bản của Công ước Hà Nội

Công ước Hà Nội được xây dựng với mục tiêu nâng cao hiệu quả đấu tranh phòng, chống tội phạm mạng trên phạm vi toàn cầu, bao gồm 9 chương với 71 điều khoản, thiết lập một hệ thống các quy định toàn diện từ những vấn đề chung, tội phạm hóa hành vi, thẩm quyền tài phán, thủ tục tố tụng, cho đến hợp tác quốc tế, biện pháp phòng ngừa, hỗ trợ kỹ thuật và cơ chế tổ chức thực hiện[1]. Định hướng chính của Công ước là tăng cường phối hợp quốc tế và nâng cao năng lực quốc gia, trong đó ưu tiên hỗ trợ các nước đang phát triển nhằm ứng phó với tính chất ngày càng phức tạp của các mối đe dọa an ninh mạng.

Xét về kỹ thuật lập pháp, nhiều quy phạm của Công ước Hà Nội được kế thừa và phát triển từ các điều ước quốc tế hiện hành về phòng, chống tội phạm, điển hình là Công ước Palermo năm 2000 (UNTOC) và Công ước Merida năm 2003 (UNCAC)[2]. Bên cạnh đó, các quy định về định danh tội phạm và biện pháp điều tra điện tử cũng có sự tham chiếu các chuẩn mực từ Công ước Budapest (2001) và Công ước Malabo (2014)[3]. Tuy nhiên, điểm tiến bộ của Công ước Hà Nội là việc bổ sung nhiều nội dung mới lần đầu tiên được áp dụng ở quy mô toàn cầu, qua đó, khắc phục những bất cập của các khuôn khổ pháp lý trước đây.

Thứ nhất, về yêu cầu tội phạm hóa toàn diện đối với tội phạm mạng. Công ước Hà Nội đã chuẩn hóa 9 nhóm tội danh cơ bản, bao quát cả hai loại: tội phạm có tính chất kỹ thuật công nghệ và tội phạm sử dụng công nghệ như một phương tiện. Theo đó, lần đầu tiên ở quy mô toàn cầu, các hành vi xâm phạm, như: truy cập hệ thống trái phép, chặn thu dữ liệu, can thiệp vào tính toàn vẹn của dữ liệu và hệ thống, hay việc sử dụng thiết bị sai mục đích để phạm tội đều được định danh cụ thể. Các hành vi lừa đảo, giả mạo trực tuyến và lạm dụng tình dục trẻ em qua mạng cũng được quy định rõ ràng. Công ước đã xác định hành vi phát tán hình ảnh nhạy cảm mà không có sự đồng thuận của chủ thể là một tội phạm hình sự nghiêm trọng, đánh dấu bước tiến mới trong việc bảo vệ quyền nhân thân trên trường quốc tế. Đây được xem là thắng lợi quan trọng trong nỗ lực bảo vệ nhân phẩm và quyền riêng tư của cá nhân trong thời đại số[4].

Thứ hai, đối với các yếu tố an ninh "phi truyền thống", Công ước đã có bước tiến đáng kể khi đề cập đến tài sản ảo và tiền kỹ thuật số. Cụ thể, khái niệm "tài sản" trong Công ước được mở rộng để bao quát cả tài sản ảo; đồng thời, ghi nhận thực tế việc sử dụng tiền mã hóa như một công cụ phổ biến trong các hoạt động tội phạm mạng, nhất là tội rửa tiền. Đây là quy định mang tính đột

phá nhằm lấp những "khoảng trống" pháp lý tại nhiều quốc gia, trong đó có Việt Nam, nơi mà hành lang pháp lý xác định tư cách tài sản hoặc phương tiện thanh toán hợp pháp của tiền ảo vẫn đang trong quá trình hoàn thiện. Công ước yêu cầu các quốc gia phải cập nhật định nghĩa tài sản trong pháp luật để xử lý được các hành vi chiếm đoạt, rửa tiền liên quan đến tài sản ảo[5].

Thứ ba, về việc định rõ trách nhiệm của pháp nhân thương mại và khu vực tư nhân. Một nội dung quan trọng của Công ước là việc xác lập cơ chế trách nhiệm pháp lý, bao gồm hình sự, dân sự hoặc hành chính đối với các pháp nhân khi để xảy ra tình trạng tội phạm mạng lợi dụng hạ tầng kỹ thuật của mình để hoạt động. Theo đó, các chủ thể như doanh nghiệp cung cấp dịch vụ trực tuyến, tổ chức tài chính hay các tập đoàn công nghệ buộc phải nâng cao vai trò chủ động trong quản trị rủi ro, bảo đảm an ninh hệ thống và an toàn dữ liệu khách hàng. Trường hợp thiếu trách nhiệm, để hệ thống bị khai thác vào mục đích phạm tội, các đơn vị này sẽ phải chịu các chế tài xử lý tương ứng theo quy định[6]. Điều này là bước tiến quan trọng nhằm thúc đẩy sự tham gia của kinh tế tư nhân vào công tác đấu tranh phòng, chống tội phạm, qua đó, góp phần củng cố tiềm lực an ninh mạng quốc gia. Việc xác lập trách nhiệm của pháp nhân không chỉ bảo đảm sự tương thích với xu thế lập pháp quốc tế hiện hành mà còn đặt ra yêu cầu đối với Việt Nam trong việc nghiên cứu, bổ sung các chế tài xử lý phù hợp đối với chủ thể này trong lĩnh vực an ninh mạng[7].

Thứ tư, về sự hài hòa giữa bảo vệ chủ quyền quốc gia và bảo đảm quyền con người. Cụ thể, tại Điều 5 và Điều 6 Công ước Hà Nội đặt ra nghĩa vụ cho các quốc gia thành viên phải thiết lập sự cân bằng hợp lý giữa yêu cầu bảo vệ an ninh mạng và việc tôn trọng các quyền tự do ngôn luận, quyền riêng tư, tự do tín ngưỡng... trên cơ sở tương thích với các điều ước quốc tế về nhân quyền mà quốc gia đó là thành viên[8]. Đây là thông điệp nhấn mạnh tính pháp quyền và nhân văn trong thực thi Công ước, khuyến khích các nước nội luật hóa các biện pháp bảo vệ quyền con người trong pháp luật quốc gia tương ứng.

Thứ năm, về cơ chế phối hợp thường trực và tương trợ tư pháp khẩn cấp. Công ước quy định việc thiết lập mạng lưới liên lạc 24/7 nhằm bảo đảm tính kịp thời trong hoạt động hợp tác quốc tế. Theo đó, các quốc gia thành viên có nghĩa vụ chỉ định đầu mối chuyên trách hoạt động liên tục để tiếp nhận và xử lý các yêu cầu hỗ trợ điều tra, thu thập, bảo quản chứng cứ điện tử cũng như thực hiện các biện pháp dẫn độ hoặc ngăn chặn đối tượng phạm tội, qua đó, khắc phục các hạn chế về chênh lệch múi giờ giữa các quốc gia. Ngoài ra, còn quy định cơ chế gửi và tiếp nhận yêu cầu tương trợ tư pháp cũng như hỗ trợ các thủ tục dẫn độ thông qua các kênh liên lạc điện tử; đồng thời, cho phép chia sẻ thông tin nhanh nhằm giải quyết kịp thời các tình huống cấp bách phát sinh trên không gian mạng. Các quy định nêu trên đánh dấu sự thay đổi quan trọng trong tư duy pháp lý quốc tế: chuyển từ việc tập trung giải quyết xung đột về thẩm quyền tài phán sang ưu tiên bảo đảm hiệu quả của việc tiếp cận và bảo quản nguyên trạng dữ liệu. Đây là yếu tố tiên quyết nhằm ngăn chặn nguy cơ tẩu tán chứng cứ điện tử - đặc tính điển hình của tội phạm công nghệ cao.

3. Các yêu cầu mang tính nguyên tắc trong quá trình nội luật hóa

Việc gia nhập Công ước đặt Việt Nam trước những nghĩa vụ pháp lý quốc tế mới, đòi hỏi sự tuân thủ nghiêm túc. Đây vừa là thách thức, vừa là áp lực tích cực để rà soát, hiện đại hóa hệ thống pháp luật quốc gia, tạo động lực thúc đẩy tiến trình cải cách tư pháp và xây dựng Nhà nước pháp quyền xã hội chủ nghĩa. Để quá trình chuyển hóa các cam kết quốc tế vào pháp luật trong nước đạt hiệu quả cao, cần quán triệt các nguyên tắc cơ bản và lộ trình hoàn thiện cụ thể.

Một là, bảo đảm kỹ thuật lập pháp và tính thống nhất của hệ thống pháp luật. Khi nội luật hóa các tội danh mới, cần tuân thủ triệt để nguyên tắc "nullum crimen sine lege" (không có tội nếu luật không quy định). Các hành vi khách quan phải được mô tả chính xác, rõ ràng; các khái niệm nền tảng như "hệ thống công nghệ thông tin", "dữ liệu điện tử", "tài sản ảo" cần được định nghĩa thống nhất trong các văn bản luật, tránh sự xung đột hoặc cách hiểu đa nghĩa. Đặc biệt, quy định về tội phạm mạng cần làm rõ yếu tố lỗi cố ý, tránh tội phạm hóa các hành vi vô ý hoặc quy kết trách nhiệm pháp lý quá mức đối với các đơn vị cung cấp dịch vụ trung gian nhằm không gây cản trở sự đổi mới sáng tạo của doanh nghiệp công nghệ.

Hai là, thiết lập cơ chế kiểm soát quyền lực và bảo đảm quyền con người trong tố tụng. Công ước quy định nhiều biện pháp điều tra đặc biệt (như: thu thập bí mật dữ liệu nội dung, giám sát thời gian thực). Quá trình nội luật hóa bắt buộc phải thiết kế hành lang pháp lý chặt chẽ cho các biện pháp này theo hướng: mọi hành vi can thiệp vào quyền riêng tư, bí mật thư tín, điện tín đều phải chịu sự giám sát tư pháp (sự phê chuẩn của Viện kiểm sát hoặc quyết định của Tòa án). Đây là yêu cầu then chốt để thực hiện cơ chế kiểm soát quyền lực, ngăn ngừa sự lạm quyền nhân danh phòng, chống tội phạm.

Ba là, bảo đảm tính đồng bộ trong quản lý nhà nước và phối hợp liên ngành. Không gian mạng là lĩnh vực giao thoa giữa an ninh quốc gia, trật tự an toàn xã hội và các quan hệ dân sự, kinh tế. Do đó, việc xác định cơ quan đầu mối (như Bộ Công an) cần đi đôi với cơ chế phối hợp liên ngành hiệu quả với Bộ Khoa học và Công nghệ, Bộ Quốc phòng và các doanh nghiệp viễn thông. Các quy định mới cần bảo đảm sự tương thích với các luật chuyên ngành hiện hành (*Luật An toàn thông tin mạng, Luật Giao dịch điện tử*...), tránh tình trạng chồng chéo thẩm quyền.

Bốn là, chuẩn bị nguồn lực và năng lực thực hiện. Việc bổ sung các tội danh và quy trình tố tụng mới đặt ra yêu cầu cấp thiết về đào tạo đội ngũ điều tra viên, kiểm sát viên và thẩm phán. Nhân sự áp dụng pháp luật không chỉ cần kiến thức pháp lý quốc tế mà còn phải am hiểu về kỹ thuật điều tra số, phân tích dữ liệu và ngoại ngữ. Bên cạnh đó, Tòa án nhân dân tối cao cần sớm ban hành các hướng dẫn áp dụng pháp luật thống nhất đối với các loại tội phạm mới (như: tội phạm liên quan đến AI, deepfake, tài sản ảo) để bảo đảm tính thống nhất trong xét xử.

4. Một số kiến nghị

Việc gia nhập Công ước Hà Nội đã đặt Việt Nam trước những nghĩa vụ pháp lý quốc tế mới, đòi hỏi sự tuân thủ nghiêm túc và đầy đủ. Xét dưới góc độ kỹ thuật lập pháp, quá trình nội luật hóa các quy định của Công ước đặt ra yêu cầu phải điều chỉnh đồng bộ hệ thống pháp luật hình sự Việt Nam trên cả hai phương diện: luật nội dung (quy định về tội danh, hình phạt) và luật hình thức (trình tự, thủ tục tố tụng).

Thứ nhất, bổ sung, hoàn thiện quy định về tội phạm mạng trong Bộ luật Hình sự.

(1) Tội phạm hóa hành vi phạm tội mới. Chương II của Công ước đã liệt kê nhiều hành vi phạm tội lần đầu được quy định rõ ràng ở cấp độ quốc tế, như các dạng tấn công mạng hay xâm hại trẻ em trực tuyến. *Bộ luật Hình sự* năm 2015 (sửa đổi, bổ sung năm 2017, 2024, 2025) (gọi tắt là *Bộ luật Hình sự* năm 2025) mặc dù đã có một số điều khoản về tội phạm công nghệ cao (ví dụ: Điều 289 về "Tội xâm nhập trái phép mạng máy tính, viễn thông...", Điều 290 về "Tội sử dụng mạng máy tính, mạng viễn thông để chiếm đoạt tài sản",...) nhưng vẫn thiếu những tội danh cụ thể tương ứng với các hành vi mà Công ước đòi hỏi[9]. Chẳng hạn, *Bộ luật Hình sự* năm 2025 chưa có tội danh riêng về "chặn thu trái phép dữ liệu", chưa quy định rõ về hành vi phổ biến ảnh nhạy cảm mà không có sự đồng ý hay dụ dỗ trẻ em qua mạng, đây là những hành vi Công ước nêu rõ cần tội phạm hóa. Do đó, cần phải sửa đổi, bổ sung *Bộ luật Hình sự* năm 2025 để

định danh đầy đủ các tội phạm mạng mới theo Công ước, tránh bỏ lọt hành vi phạm tội. Việc bổ sung cần tuân thủ nguyên tắc không có tội nếu luật không quy định, tức là diễn đạt tội danh một cách cụ thể, rõ ràng nhằm ngăn ngừa sự tùy tiện hoặc lạm dụng khi áp dụng.

(2) Hoàn thiện tội phạm truyền thống liên quan đến công nghệ theo yêu cầu của Công ước. Một số hành vi, như: lừa đảo qua mạng, xâm hại tình dục trẻ em trên môi trường mạng tuy đã có thể xử lý dưới các tội danh truyền thống; tội lừa đảo chiếm đoạt tài sản (Điều 174); tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290); tội truyền bá văn hóa phẩm đồi trụy (Điều 326) hoặc tội dâm ô đối với người dưới 16 tuổi (Điều 146) trong *Bộ luật Hình sự* hiện hành nhưng đặc điểm hành vi trên môi trường số có nhiều khác biệt. Công ước Hà Nội quy định các yếu tố cấu thành chi tiết hơn cho những tội phạm này trong bối cảnh số hóa. Ví dụ, hành vi grooming (dụ dỗ trẻ em qua mạng) hoặc phát tán tài liệu xâm hại tình dục trẻ em cần được quy định rõ ràng, phù hợp với thủ đoạn tinh vi mà chủ thể phạm tội sử dụng internet để thực hiện[10]. Khi nội luật hóa, *Bộ luật Hình sự* cần sửa đổi, bổ sung theo các yêu cầu của Công ước tại các điều luật tương ứng để bảo đảm nghĩa vụ của các quốc gia thành viên và không bỏ lọt tội phạm.

(3) Đưa "tài sản ảo" vào đối tượng bảo vệ của pháp luật hình sự. Công ước yêu cầu các quốc gia mở rộng khái niệm tài sản. *Bộ luật Hình sự* hiện nay chưa công nhận tiền mã hóa (ví dụ Bitcoin) là tài sản, dẫn đến khó xử lý hình sự các vụ trộm cắp, lừa đảo tiền ảo hoặc rửa tiền qua tiền ảo. Nội luật hóa Công ước đòi hỏi phải sửa *Bộ luật Hình sự* và *Luật Phòng, chống rửa tiền* để coi tiền kỹ thuật số, tài sản ảo là tài sản trong cấu thành tội phạm, qua đó, truy cứu được hành vi chiếm đoạt hoặc rửa tiền liên quan.

(4) Trách nhiệm hình sự của pháp nhân. *Bộ luật Hình sự* lần đầu quy định trách nhiệm hình sự đối với pháp nhân nhưng mới giới hạn ở một số ít tội phạm về kinh tế, môi trường, an toàn công cộng. Theo Công ước Hà Nội, Việt Nam nên cân nhắc mở rộng danh mục tội phạm mà pháp nhân phải chịu trách nhiệm, bao gồm các vi phạm về an ninh mạng (ví dụ nếu pháp nhân thiếu quản lý để xảy ra lộ lọt dữ liệu quy mô lớn hoặc không tuân thủ biện pháp bảo mật khiến tội phạm lợi dụng hệ thống). Điều này không chỉ đáp ứng yêu cầu Công ước về truy cứu pháp nhân[11] mà còn phù hợp với xu hướng pháp luật nhiều nước, đặt trách nhiệm cho các công ty công nghệ và tổ chức quản trị dữ liệu trong phòng, chống tội phạm mạng.

Thứ hai, về yêu cầu nội luật hóa các quy định liên quan đến chứng cứ điện tử trong *Bộ luật Tố tụng hình sự* năm 2015. Tại Chương IV, Công ước đã xây dựng hệ thống quy định chi tiết về các biện pháp (công cụ) tố tụng nhằm tạo điều kiện cho cơ quan chức năng có khả năng xử lý nhanh các hành vi phạm tội trên mạng. Theo đó, các quốc gia thành viên cần cụ thể hóa các quy định về thu thập và bảo quản chứng cứ điện tử, bao gồm: cơ chế lưu trữ nhanh dữ liệu máy tính; khám xét và thu giữ dữ liệu đã lưu trữ; lệnh yêu cầu cung cấp thông tin thuê bao; thu thập trực tiếp dữ liệu ngay tại thời điểm truyền đưa (thời gian thực); cũng như các biện pháp phong tỏa, kê biên tài sản kỹ thuật số liên quan đến vụ án.

Bộ luật Tố tụng hình sự năm 2015 tuy có đề cập "dữ liệu điện tử" là một dạng nguồn chứng cứ nhưng chưa có quy trình chặt chẽ và đầy đủ cho việc thu thập, bảo quản loại chứng cứ đặc thù này (Điều 87, Điều 99, Điều 107). Do vậy, nội luật hóa Công ước đòi hỏi phải sửa đổi *Bộ luật* này theo hướng:

(1) Bảo quản khẩn cấp dữ liệu điện tử: cho phép cơ quan điều tra ra lệnh yêu cầu công ty viễn thông, nhà cung cấp dịch vụ internet lưu giữ ngay lập tức dữ liệu trong một thời gian ngắn để chờ lệnh khám xét chính thức[12]. Công ước yêu cầu cơ chế này

nhằm tránh dữ liệu bị xóa trước khi có tương trợ tư pháp hoặc quyết định khám xét.

(2) Khám xét, thu giữ dữ liệu từ xa: cho phép thu thập dữ liệu từ hệ thống máy tính, thiết bị lưu trữ dù ở ngoài lãnh thổ, miễn là có sự phối hợp hợp pháp với quốc gia liên quan. Điều này gắn liền với hợp tác quốc tế, đòi hỏi *Bộ luật Tố tụng hình sự* năm 2015 và *Luật Tương trợ tư pháp hình sự* năm 2025 phải đồng bộ.

(3) Thu thập dữ liệu lưu lượng, nội dung thời gian thực: đây là các biện pháp can thiệp sâu vào quyền riêng tư (ví dụ nghe lén, đọc trộm email). Công ước không những đòi hỏi quốc gia có khả năng thực hiện mà còn nhấn mạnh các biện pháp này phải chịu sự giám sát tư pháp độc lập. Vì vậy, *Bộ luật Tố tụng hình sự* năm 2015 cần quy định chặt chẽ theo hướng chỉ được chặn thu dữ liệu khi có phê chuẩn của Viện Kiểm sát hoặc lệnh Tòa án, tránh tình trạng quyết định hành chính đơn phương.

(4) Công nhận và xử lý chứng cứ điện tử do quốc tế cung cấp: trong bối cảnh điều tra chung và tương trợ tư pháp điện tử, *Bộ luật Tố tụng hình sự* năm 2015 cần có điều khoản công nhận giá trị pháp lý của chứng cứ do nước ngoài gửi qua kênh hợp tác 24/7 hoặc MLA (mutual legal assistance), miễn là đáp ứng các tiêu chuẩn xác thực. Hiện nay chưa có quy định rõ về việc này, gây khó cho Tòa án và Viện Kiểm sát khi sử dụng chứng cứ số từ nước ngoài.

Thứ ba, hoàn thiện quy định về tương trợ tư pháp và hợp tác dẫn độ. Công ước Hà Nội thiết lập các cơ chế hợp tác hiệu quả như dẫn độ, tương trợ tư pháp (MLA), điều tra chung, chuyển giao người bị kết án, thu hồi tài sản...; đồng thời, yêu cầu mỗi nước chỉ định một điểm liên lạc 24/7 để tiếp nhận yêu cầu khẩn cấp. Để nội luật hóa, Việt Nam cần:

(1) Tiếp tục hoàn thiện *Luật Tương trợ tư pháp hình sự* năm 2025 theo hướng: bổ sung quy định về ủy thác tư pháp điện tử (gửi nhận yêu cầu qua phương tiện điện tử nhanh chóng, thay vì chỉ qua đường ngoại giao truyền thống); quy định việc dẫn độ trực tuyến (ví dụ: xét xử vắng mặt hoặc trực tuyến khi dẫn độ) nếu phù hợp; đặc biệt là bổ sung cơ sở pháp lý cho điều tra chung giữa Việt Nam và nước ngoài trong vụ án[13].

(2) Ban hành các văn bản liên tịch giữa Bộ Công an - Viện Kiểm sát nhân dân tối cao - Tòa án Nhân dân tối cao hướng dẫn phối hợp liên ngành về tương trợ tư pháp hình sự trong môi trường mạng (ví dụ: hướng dẫn thủ tục tiếp nhận, thực thi yêu cầu từ điểm liên lạc 24/7, chia sẻ dữ liệu xuyên biên giới, bảo quản chứng cứ trong quá trình chờ MLA chính thức).

(3) Giao rõ thẩm quyền và trách nhiệm đầu mối: dự kiến Bộ Công an (Cục An ninh mạng và Phòng, chống tội phạm công nghệ cao - A05) sẽ là đầu mối quốc gia về hợp tác 24/7. *Luật An ninh mạng* (sửa đổi, bổ sung năm 2025) và các văn bản dưới luật cần ghi nhận vai trò của đơn vị này trong việc phối hợp quốc tế, thiết lập Trung tâm điều phối hợp tác quốc tế về tội phạm mạng để hỗ trợ thường trực các yêu cầu điều tra, dẫn độ, thu hồi tài sản số theo Công ước.

Thứ tư, tiếp tục hoàn thiện các luật liên quan an ninh mạng và bảo vệ dữ liệu cá nhân. Bên cạnh hai đạo luật nền tảng là *Bộ luật Hình sự* và *Bộ luật Tố tụng hình sự,* quá trình nội luật hóa Công ước Hà Nội còn liên quan mật thiết đến các luật chuyên ngành, như: *Luật An ninh mạng, Luật Bảo vệ dữ liệu cá nhân*... Đây là các luật điều chỉnh hoạt động quản lý nhà nước và thiết lập môi trường pháp lý về không gian mạng, do đó, cần được điều chỉnh để tương thích với các cam kết mới.

Hiện nay, đối chiếu với các chuẩn mực quốc tế mới, *Luật An ninh mạng* năm 2025 vẫn bộc lộ những "khoảng trống" về cơ chế thực hiện, điển hình là sự thiếu vắng quy định về mạng lưới hợp tác 24/7, chưa có cơ chế bắt buộc nhà cung cấp dịch vụ thực hiện "bảo quản nhanh" dữ liệu trước khi có lệnh thu giữ và chưa quy định rõ trách nhiệm của

các nền tảng xuyên biên giới trong việc xác thực danh tính người dùng liên quan đến tài sản ảo. Do đó, để bảo đảm sự tương thích đầy đủ, *Luật An ninh mạng* cần hoàn thiện theo hướng cụ thể sau: (1) Về hợp tác quốc tế: luật hóa vai trò của Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an là "đầu mối quốc gia 24/7", có thẩm quyền trực tiếp tiếp nhận và xử lý các yêu cầu tương trợ tư pháp khẩn cấp mà không cần qua thủ tục ngoại giao trung gian; (2) Về trách nhiệm doanh nghiệp: bổ sung quy định buộc các doanh nghiệp cung cấp dịch vụ viễn thông, internet phải thực hiện lệnh "bảo quản nhanh" (đóng băng dữ liệu nguyên trạng) trong vòng tối đa 24 giờ kể từ khi nhận yêu cầu của cơ quan chức năng để ngăn chặn việc xóa bỏ chứng cứ; (3) Về phạm vi điều chỉnh: mở rộng các quy định bảo vệ an ninh đối với dữ liệu cá nhân và bổ sung chế tài quản lý đối với các giao dịch liên quan đến tài sản ảo, tiền kỹ thuật số nhằm triệt tiêu điều kiện hoạt động của tội phạm rửa tiền và lừa đảo trực tuyến.

Luật Bảo vệ dữ liệu cá nhân năm 2025 và *Luật An ninh mạng* năm 2025 đã nội luật hóa các nguyên tắc bảo vệ dữ liệu trong hợp tác quốc tế; đồng thời, quy định chặt chẽ về các biện pháp kỹ thuật phòng ngừa sự cố, bảo đảm tính toàn vẹn và bảo mật của thông tin trên môi trường mạng. Đây là nền tảng quan trọng để Việt Nam thực hiện nghĩa vụ thành viên về bảo vệ quyền riêng tư và phòng ngừa tội phạm. Tuy nhiên, trước sự phát triển của công nghệ và tính chất phức tạp của tội phạm mạng, hệ thống pháp luật này cần được bổ sung, hoàn thiện ở hai khía cạnh trọng yếu: lấp đầy "khoảng trống" về an ninh dữ liệu tổ chức và bổ sung chế tài đối với công nghệ mới (AI, deepfake).

5. Kết luận

Việc Việt Nam tham gia Công ước Liên Hợp quốc về chống tội phạm mạng không chỉ khẳng định cam kết chính trị - pháp lý của quốc gia đối với cộng đồng quốc tế mà còn tạo động lực quan trọng thúc đẩy tiến trình hoàn thiện hệ thống pháp luật trong nước. Mối quan hệ giữa các chuẩn mực của Công ước Hà Nội và pháp luật quốc gia chính là cơ sở then chốt để xây dựng một hành lang pháp lý hiện đại, minh bạch, đáp ứng yêu cầu hội nhập và phát triển bền vững trong kỷ nguyên số❐

Chú thích:

1, 8. *Tổng quan Công ước Hà Nội: Nội dung chính, cấu trúc và phạm vi áp dụng*, https://baochinhphu.vn, ngày 25/10/2025.

2. Nguyễn Viết Tăng (2025). *Nội luật hóa Công ước Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia đối với hành vi tham nhũng - thực trạng và kiến nghị*. Tòa án nhân dân số 1 (2025), tr. 35 - 36.

3. Lê Huy Hoàng (2025). *Áp dụng pháp luật trong điều tra tội phạm ma túy có yếu tố nước ngoài*. Tạp chí Quản lý nhà nước, số 355 (2025), tr. 71 - 75, https://doi.org/10.59394/qlnn.355.2025.1264.

4. Nguyễn Đăng Khoa (2023). *Sự phát triển của công nghệ và tình trạng gia tăng tội phạm mạng hiện nay*. Tạp chí Luật sư Việt Nam, số 9 (2023), tr. 21 - 23.

5. Nguyễn Đức Hà (2023). *Khung pháp lý đấu tranh với tội phạm mạng tại Singapore và kinh nghiệm cho Việt Nam*. Tạp chí Kiểm sát, số 9 (2023).

6, 11. *Công ước Hà Nội: Cơ chế hợp tác thực chiến toàn cầu về phòng, chống tội phạm mạng"*, https://xaydungchinhsach.chinhphu.vn, ngày 22/11/2025.

7. Nguyễn Trọng Tuấn, Đào Ngân (2021). *Trách nhiệm hình sự đối với pháp nhân thương mại*. Tạp chí Dân chủ và pháp luật, số 3 (2021), tr. 22 - 26.

9. *Nội luật hóa Công ước Hà Nội, đưa Việt Nam thành trung tâm khu vực quản trị không gian mạng an toàn, nhân văn*. https://daibieunhandan.vn, ngày 07/11/2025.

10. Nguyễn Đức Hạnh (2021). *Tội phạm mạng và việc khai thác dữ liệu điện tử phục vụ buộc tội, tranh tụng tại phiên tòa hình sự*. Tạp chí Khoa học Kiểm sát, số 01 (2021), tr. 8 - 10.

12. *Nội luật hóa Công ước Hà Nội về bảo vệ trẻ em và các nhóm yếu thế trong Luật An ninh mạng Việt Nam*. https://cand.com.vn/, ngày 01/12/2025.

13. Plokhov Sergey Ladimirovich (2022). *Đấu tranh phòng, chống tội phạm mạng: Thực tiễn ở Nga và triển vọng của sự hợp tác* quốc tế. Tạp chí Khoa học Kiểm sát, số 6 (2022), tr. 18 - 20.