

Công ước của Liên Hợp Quốc về chống tội phạm mạng tương thích pháp luật quốc tế và yêu cầu hoàn thiện hệ thống pháp luật Việt Nam trong bối cảnh hiện thực hóa Nghị quyết số 66 - NQ/TW

PGS, TS. NGUYỄN THỊ NGỌC HOA

Học viện Báo chí và Tuyên truyền; Email: ngochoaajc10052gmail.com

Nhận ngày 19 tháng 1 năm 2026; chấp nhận đăng tháng 3 năm 2026.

Tóm tắt: Nghiên cứu này phân tích mối quan hệ biện chứng giữa các cam kết quốc tế trong Công ước của Liên Hợp Quốc về chống tội phạm mạng (Công ước Hà Nội) và các định hướng chiến lược trong Nghị quyết số 66 - NQ/TW của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật. Công ước của Liên hợp quốc về chống tội phạm mạng không chỉ là điều ước quốc tế đơn thuần, mà đóng vai trò là “chất xúc tác pháp lý”, thúc đẩy Việt Nam giải quyết các “điểm nghẽn” trong Bộ luật Hình sự (BLHS) và Bộ luật Tố tụng hình sự (BLTTHS), đặc biệt là các vấn đề về tài sản ảo, chứng cứ điện tử và tương trợ tư pháp hình sự. Bài viết đề xuất các giải pháp lập pháp nhằm cân bằng giữa yêu cầu bảo đảm an ninh quốc gia, phát triển kinh tế số và bảo vệ quyền con người theo chuẩn mực quốc tế.

Từ khóa: Công ước của Liên Hợp Quốc về chống tội phạm mạng; tội phạm mạng; Nghị quyết số 66 - NQ/TW; chứng cứ điện tử; tương trợ tư pháp.

Abstract: This study analyzes the dialectical relationship between international commitments under the United Nations Convention against Cybercrime (the Hanoi Convention) and the strategic orientations set out in Politburo Resolution No. 66-NQ/TW on reforming law-making and law enforcement. The Convention is not merely an international treaty but serves as a “legal catalyst,” encouraging Vietnam to address bottlenecks in the Criminal Code and the Criminal Procedure Code, particularly in areas such as virtual assets, electronic evidence, and mutual legal assistance in criminal matters. The article proposes legislative solutions aimed at balancing the requirements of safeguarding national security, promoting the digital economy, and protecting human rights in accordance with international standards.

Keywords: United Nations Convention against Cybercrime; cybercrime; Resolution 66-NQ/TW; electronic evidence; mutual legal assistance.

1. Đặt vấn đề

Sự ra đời của Công ước của Liên Hợp Quốc về chống tội phạm mạng (sau đây gọi là Công ước của Liên hợp quốc về chống tội phạm mạng) và việc Bộ Chính trị ban hành Nghị quyết số 66 - NQ/TW ngày 30/4/2025 (sau đây gọi là Nghị quyết 66) là hai sự kiện pháp lý trọng yếu, tạo nên bối cảnh “kép” cho tiến trình cải cách tư pháp tại Việt Nam.

Nếu như Nghị quyết 66 đặt ra yêu cầu nội tại về việc chuyển đổi tư duy lập pháp từ “quản lý” sang “kiến tạo phát triển” và xây dựng hệ thống pháp luật “tiệm cận chuẩn mực quốc tế”, thì Công ước của Liên hợp quốc về

chống tội phạm mạng cung cấp chính những chuẩn mực đó trong lĩnh vực an ninh phi truyền thống. Bài viết này tập trung phân tích tác động của Công ước của Liên Hợp Quốc về chống tội phạm mạng đối với hệ thống pháp luật Việt Nam, coi đây là cơ hội để hiện đại hóa các đạo luật trụ cột, đáp ứng yêu cầu của kỷ nguyên số.

2. Nội dung

2.1. Khái quát Công ước của Liên Hợp Quốc về chống tội phạm mạng và Nghị quyết số 66 - NQ/TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật

2.1.1. Khái quát Công ước của Liên Hợp Quốc về

chống tội phạm mạng

Ngày 24/12/2024, Đại hội đồng Liên Hợp Quốc đã thông qua Công ước của Liên Hợp Quốc về chống tội phạm mạng, còn gọi là UN Cybercrime Convention (Liên Hợp Quốc, 2024) - văn kiện toàn cầu đầu tiên do Liên Hợp Quốc bảo trợ nhằm thiết lập khuôn khổ pháp lý quốc tế thống nhất về phòng ngừa, điều tra và xử lý tội phạm mạng. Công ước được xây dựng trong bối cảnh tội phạm mạng gia tăng nhanh, xuyên biên giới, tinh vi; sự phân tán, khác biệt giữa các hệ thống pháp luật quốc gia; nhu cầu tăng cường hợp tác quốc tế về tương trợ tư pháp và dẫn độ.

Công ước hướng tới 4 mục tiêu lớn: (1) Hình sự hóa thống nhất các hành vi nguy hiểm trên không gian mạng; (2) Tăng cường hợp tác quốc tế trong điều tra, truy tố và dẫn độ; (3) Thiết lập cơ chế thu thập, bảo quản và chia sẻ chứng cứ điện tử; (4) Bảo đảm tôn trọng quyền con người và chủ quyền quốc gia trong quá trình thực thi.

Công ước bao quát toàn diện các nhóm hành vi nguy hiểm trên không gian mạng, bao gồm: Các tội xâm phạm hệ thống và dữ liệu như truy cập trái phép vào hệ thống máy tính, can thiệp trái phép vào dữ liệu, tấn công làm gián đoạn hoạt động của hệ thống và phát tán mã độc; các hành vi sử dụng công nghệ số để thực hiện tội phạm truyền thống như lừa đảo trực tuyến, rửa tiền qua môi trường mạng, buôn bán trái phép, bóc lột trẻ em trên không gian số và phát tán nội dung bất hợp pháp; đồng thời điều chỉnh cả các loại tội phạm có tổ chức và tội phạm xuyên quốc gia sử dụng công nghệ số làm phương tiện, công cụ hoặc môi trường thực hiện hành vi phạm tội.

Công ước đặt ra các công cụ tố tụng đặc thù, gồm: thu thập nhanh và bảo toàn dữ liệu điện tử; yêu cầu cung cấp dữ liệu từ nhà cung cấp dịch vụ; khám xét và thu giữ dữ liệu số; hợp tác trực tiếp giữa cơ quan thực thi pháp luật các nước. Đây là điểm tiến bộ nhằm khắc phục khó khăn lớn nhất trong điều tra tội phạm mạng: tính dễ xóa, dễ di chuyển và xuyên biên giới của chứng cứ điện tử.

Công ước thiết lập cơ chế tương trợ tư pháp chuyên biệt về dữ liệu điện tử; nghĩa vụ chỉ định đầu mối quốc gia 24/7; cơ chế trao đổi thông tin nhanh chóng giữa các quốc gia thành viên. Điểm quan trọng là Công ước tôn trọng chủ quyền quốc gia; nguyên tắc không can thiệp; quy định nội luật của mỗi quốc gia khi thực hiện yêu cầu hợp tác.

Công ước yêu cầu các quốc gia khi thực hiện biện pháp điều tra phải bảo đảm tính cần thiết, hợp pháp và

tương xứng; tôn trọng quyền riêng tư, dữ liệu cá nhân; bảo đảm quyền được xét xử công bằng. Đây là nội dung được nhiều quốc gia tranh luận trong quá trình đàm phán.

Công ước của Liên Hợp Quốc về chống tội phạm mạng là khuôn khổ pháp lý toàn cầu đầu tiên nhằm hài hòa hóa quy định hình sự và tăng cường hợp tác quốc tế trong phòng, chống tội phạm trên không gian mạng, trên cơ sở tôn trọng chủ quyền quốc gia và bảo đảm quyền con người.

2.1.2. Khái quát Nghị quyết số 66 - NQ/TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật

Nghị quyết số 66 - NQ/TW ngày 30/4/2025 do Bộ Chính trị ban hành trong bối cảnh đất nước bước vào giai đoạn phát triển mới với yêu cầu tăng trưởng nhanh, bền vững, hội nhập sâu rộng và chuyển đổi số toàn diện (Ban Chấp hành Trung ương, 2025). Mặc dù hệ thống pháp luật đã có nhiều đổi mới, song vẫn còn tình trạng chồng chéo, thiếu đồng bộ, chất lượng một số văn bản chưa cao, khâu tổ chức thi hành còn là “điểm nghẽn”, ảnh hưởng đến môi trường đầu tư, kinh doanh và hiệu lực quản lý nhà nước.

Nghị quyết xác định rõ công tác xây dựng và thi hành pháp luật phải đặt dưới sự lãnh đạo toàn diện, trực tiếp của Đảng; coi đây là một đột phá chiến lược trong hoàn thiện thể chế phát triển. Pháp luật phải bám sát thực tiễn, lấy người dân và doanh nghiệp làm trung tâm phục vụ, đồng thời tiếp thu có chọn lọc tinh hoa pháp lý quốc tế, bảo đảm phù hợp với điều kiện Việt Nam và giữ vững định hướng xã hội chủ nghĩa.

Nghị quyết hướng tới xây dựng hệ thống pháp luật đồng bộ, thống nhất, minh bạch, khả thi, ổn định và có tính dự báo cao; nâng cao chất lượng công tác tổ chức thi hành pháp luật; khắc phục tình trạng “luật khung, luật ống”; kịp thời tháo gỡ các rào cản thể chế, tạo động lực cho đổi mới sáng tạo và phát triển kinh tế - xã hội trong kỷ nguyên số.

Nghị quyết yêu cầu đổi mới tư duy lập pháp theo hướng chuyên nghiệp, khoa học và thực chất hơn; bảo đảm thể chế hóa đầy đủ, kịp thời các chủ trương của Đảng; nâng cao chất lượng đánh giá tác động chính sách; tăng cường kỷ luật, kỷ cương trong quy trình lập pháp; khắc phục tình trạng nợ đọng văn bản quy định chi tiết. Đồng thời, phát huy vai trò phản biện xã hội, sự tham gia của chuyên gia, nhà khoa học, cộng đồng doanh nghiệp và nhân dân trong quá trình xây dựng pháp luật.

Nghị quyết nhấn mạnh yêu cầu chuyển mạnh từ “ban hành nhiều” sang “thi hành tốt”; tăng cường kiểm tra, rà soát, hệ thống hóa và xử lý văn bản trái pháp luật hoặc không còn phù hợp; nâng cao trách nhiệm của người đứng đầu trong tổ chức thi hành; đẩy mạnh ứng dụng công nghệ số trong quản lý và theo dõi thi hành pháp luật; bảo đảm pháp luật đi vào cuộc sống một cách thực chất, hiệu quả.

Nghị quyết yêu cầu xây dựng cơ chế phát hiện sớm và xử lý kịp thời những bất cập của pháp luật; thiết lập hệ thống theo dõi, đánh giá thi hành pháp luật dựa trên dữ liệu; tăng cường giám sát của Quốc hội, Mặt trận Tổ quốc và nhân dân; đồng thời bảo đảm sự phối hợp chặt chẽ giữa các cơ quan trong việc rà soát, sửa đổi, bổ sung quy định chưa phù hợp với thực tiễn.

Nghị quyết đặt ra yêu cầu xây dựng đội ngũ cán bộ làm công tác pháp luật có bản lĩnh chính trị vững vàng, trình độ chuyên môn cao, tư duy hiện đại và năng lực hội nhập quốc tế; coi trọng đào tạo, bồi dưỡng kỹ năng lập pháp, đánh giá chính sách, kỹ năng số; đồng thời nâng cao vai trò của cơ quan pháp chế trong các bộ, ngành, địa phương.

Nghị quyết số 66 - NQ/TW được xem là bước chuyển quan trọng trong tư duy về pháp luật, từ công cụ quản lý thuần túy sang động lực phát triển quốc gia. Việc đổi mới đồng bộ cả xây dựng và thi hành pháp luật góp phần hoàn thiện Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam, nâng cao năng lực cạnh tranh quốc gia, củng cố niềm tin của nhân dân và cộng đồng doanh nghiệp, tạo nền tảng thể chế vững chắc cho mục tiêu phát triển nhanh và bền vững của đất nước trong giai đoạn mới.

2.2. Tác động của Công ước của Liên Hợp Quốc về chống tội phạm mạng đối với pháp luật hình sự khắc phục khoảng trống về tài sản ảo và tội phạm mới, để xuất hoàn thiện hệ thống pháp luật Việt Nam

Đối với Việt Nam, Công ước có ý nghĩa tạo cơ sở pháp lý tăng cường hợp tác quốc tế trong xử lý tội phạm mạng; hỗ trợ nâng cao năng lực điều tra chứng cứ điện tử; thúc đẩy hoàn thiện pháp luật hình sự, tổ tụng hình sự và pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân; góp phần bảo đảm an ninh quốc gia, trật tự an toàn xã hội trong chuyển đổi số.

Việc nội luật hóa Công ước của Liên Hợp Quốc về chống tội phạm mạng đặt ra yêu cầu cấp thiết phải rà soát lại BLHS hiện hành (sửa đổi, bổ sung năm 2017), vốn được xây dựng trên tư duy quản lý tài sản truyền thống và đang bộc lộ những độ trễ nhất định so với tốc độ phát

triển của công nghệ (Quốc hội, 2025).

2.2.1. Vấn đề hình sự hóa và định danh “Tài sản ảo” (Virtual assets)

Một trong những điểm tiến bộ nhưng cũng là thách thức lớn nhất của Công ước của Liên Hợp Quốc về chống tội phạm mạng là cách tiếp cận đối với tài sản ảo và tiền điện tử, đặc biệt trong các quy định về rửa tiền (money laundering) và tịch thu tài sản do phạm tội mà có.

Thực trạng pháp lý: Hiện nay, Bộ luật Dân sự 2015 (Điều 105: “Tài sản là vật, tiền, giấy tờ có giá và quyền tài sản” (Quốc hội, 2025)) chưa liệt kê tài sản ảo, tiền ảo vào danh mục “tài sản”. Hiện tại, Bit coin và các loại tiền mã hóa chưa được quy định thuộc bất kỳ loại nào trong 04 loại trên. Hệ quả là trong pháp luật hình sự, các đối tượng này rơi vào “vùng xám” pháp lý. Dù thực tiễn xét xử (như vụ án Rikvip hay các vụ lừa đảo qua sàn tiền ảo) đã ghi nhận giá trị kinh tế của chúng, nhưng các cơ quan tiến hành tố tụng vẫn gặp lúng túng trong việc định lượng giá trị thiệt hại (để định khung hình phạt) và quy trình thu giữ, bảo quản, tịch thu sung công quỹ. Rất nhiều vụ án, cơ quan điều tra không thể tịch thu được “khóa riêng” (private key) hoặc không có cơ chế bán đấu giá tài sản ảo để thu hồi tiền cho ngân sách nhà nước. Điển hình như vụ án đánh bạc trực tuyến nghìn tỷ (Vụ án Phan Sào Nam và Nguyễn Văn Dương), việc thu hồi tài sản từ các nguồn tiền ảo chuyển đổi qua nhiều công trung gian thanh toán gặp rất nhiều khó khăn về cơ chế pháp lý.

Gần đây, ngày 14 tháng 6 năm 2025, Quốc hội ban hành Luật Công nghiệp công nghệ số. Luật này có hiệu lực thi hành từ ngày 1 tháng 1 năm 2026, trong đó Điều 46 quy định: “Tài sản số là tài sản theo quy định của Bộ luật Dân sự, được thể hiện dưới dạng dữ liệu số, được tạo lập, phát hành, lưu trữ, chuyển giao và xác thực bởi công nghệ số trên môi trường điện tử”. Khoản 2 Điều 47 quy định: “2. Tài sản số bao gồm: a) Tài sản ảo trên môi trường điện tử là một loại tài sản số có thể được dùng cho mục đích trao đổi hoặc đầu tư. Tài sản ảo không bao gồm chứng khoán, các dạng số của tiền pháp định và tài sản tài chính khác theo quy định của pháp luật về dân sự; tài chính” (Quốc hội, 2025). Tuy nhiên, các quy định này chưa được hình sự hóa và định danh “Tài sản ảo” cụ thể trong Bộ luật Hình sự. Yêu cầu từ Công ước của Liên Hợp Quốc về chống tội phạm mạng: Công ước yêu cầu các Quốc gia thành viên phải có khung pháp lý để hình sự hóa hành vi rửa tiền liên quan đến mọi loại tài sản, bao gồm cả tài sản số. Đặc biệt, Công ước nhấn mạnh cơ chế

“tịch thu giá trị tương đương” nếu tài sản gốc không thể thu hồi hoặc đã bị chuyển đổi (Liên Hợp Quốc, 2024). Chương IV (tịch thu và tước bỏ tài sản), Công ước khuyến nghị các quốc gia thành viên cho phép tịch thu các tài sản có giá trị tương đương với khoản thu lợi bất chính nếu khoản thu lợi đó đã bị tẩu tán. Điều này đòi hỏi pháp luật quốc gia phải công nhận tư cách tài sản (ít nhất là trong lĩnh vực hình sự) của tiền mã hóa.

Kiến nghị lập pháp theo tinh thần Nghị quyết 66: Để thực hiện mục tiêu mà Nghị quyết 66 đặt ra, Việt Nam cần thực hiện một trong hai hướng tiếp cận lập pháp:

Phương án 1 (Sửa đổi gốc): Sửa đổi khái niệm tài sản trong Bộ luật Dân sự thống nhất, rõ ràng như Luật Công nghiệp công nghệ số để bao hàm tài sản ảo, tạo nền tảng thống nhất cho cả hình sự, dân sự và hành chính.

Phương án 2 (Quy định chuyên biệt): Bổ sung quy định giải thích từ ngữ trong BLHS hoặc ban hành Nghị quyết của Hội đồng Thẩm phán, xác định tài sản ảo là “phương tiện phạm tội” hoặc “tài sản do phạm tội mà có” có giá trị quy đổi, từ đó tạo cơ sở pháp lý cho việc kê biên, phong tỏa và tịch thu loại tài sản này. Đây là bước đi cần thiết để ngăn chặn Việt Nam trở thành “vùng trũng” rửa tiền công nghệ cao.

2.2.2. Chuẩn hóa các tội danh xâm phạm an toàn mạng máy tính

Công ước của Liên Hợp Quốc về chống tội phạm mạng đặt ra các chuẩn mực kỹ thuật pháp lý rất cao đối với các tội danh thuộc nhóm xâm phạm an toàn mạng máy tính (tương ứng với các Điều 285 - 294 BLHS Việt Nam), đòi hỏi sự tinh chỉnh về cấu thành tội phạm.

Về hành vi “Truy cập bất hợp pháp” và yếu tố “Lỗi”: Quy định hiện hành của BLHS về tội xâm nhập trái phép mạng máy tính thường dựa trên hành vi khách quan (truy cập mà không được phép) (Điều 289). Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Quốc hội, 2025). Tuy nhiên, trong kỷ nguyên an ninh mạng, ranh giới giữa tội phạm và chuyên gia bảo mật (white - hat hackers) - những người xâm nhập để tìm lỗ hổng và cảnh báo - là rất mong manh. Vì vậy, nội luật hóa Công ước của Liên Hợp Quốc về chống tội phạm mạng đòi hỏi BLHS phải quy định rõ ràng về mặt chủ quan của tội phạm. Cụ thể, cần bổ sung yếu tố “với ý định không trung thực” (dishonest intent) hoặc “nhằm mục đích chiếm đoạt, phá hoại” vào cấu thành tội phạm cơ bản (Điều 6, truy cập bất hợp pháp) thường yêu cầu yếu tố lỗi cố ý và mục đích bất chính để

cấu thành tội phạm, phân biệt với việc truy cập nhằm mục đích kiểm thử an ninh (pentest) được ủy quyền (Liên Hợp Quốc, 2024). Điều này giúp bảo vệ các hoạt động nghiên cứu an ninh mạng hợp pháp, khuyến khích sự phát triển của công nghệ bảo mật quốc gia.

Về tội phạm sử dụng công nghệ cao (Deepfake/AI) để lừa đảo: Sự bùng nổ của trí tuệ nhân tạo tạo sinh (GenAI) đã sinh ra các hành vi lừa đảo bằng Deepfake (giả mạo giọng nói, hình ảnh) cực kỳ tinh vi. Điều 290 BLHS hiện hành (tội sử dụng mạng máy tính... để thực hiện hành vi chiếm đoạt tài sản) đã quy định hành vi “lừa đảo trong thương mại điện tử, kinh doanh tiền tệ...” nhưng chưa có quy định cụ thể về việc sử dụng công nghệ giả mạo (Deepfake) như một tình tiết định khung tăng nặng và chưa bao quát hết các thủ đoạn sử dụng AI để thao túng tâm lý nạn nhân hoặc giả mạo dữ liệu sinh trắc học. Vì vậy, cần bổ sung các tình tiết định khung tăng nặng đối với hành vi sử dụng công nghệ trí tuệ nhân tạo, giả mạo dữ liệu sinh trắc học để lừa đảo hoặc xâm phạm nhân phẩm (đặc biệt là đối với trẻ em, phù hợp với các điều khoản nghiêm ngặt của Công ước về chống lạm dụng tình dục trẻ em trực tuyến). Việc này thể hiện sự phản ứng linh hoạt, “bám sát thực tiễn” của hệ thống pháp luật theo đúng tinh thần chỉ đạo của Nghị quyết 66.

2.3. Tác động đối với pháp luật tố tụng hình sự từ cuộc cách mạng về chứng cứ điện tử

Nếu BLHS là phần nội dung, định danh tội phạm, thì BLTTHS là công cụ hiện thực hóa Công ước. Chương IV của Công ước của Liên Hợp Quốc về chống tội phạm mạng (từ Điều 23 đến Điều 35) về các biện pháp tố tụng trong nước đặt ra những yêu cầu mang tính kỹ thuật cao mà BLTTHS 2015 của Việt Nam, dù đã có những tiến bộ nhất định, đã bổ sung “Dữ liệu điện tử” là một nguồn chứng cứ (Điều 87) và quy định về thu thập phương tiện điện tử (Điều 107) (Quốc hội, 2025) nhưng chưa có các quy định về quy trình tố tụng đặc thù cho việc “bảo toàn” hay “thu thập thời gian thực” nên chưa bao quát hết được sự phức tạp của môi trường số.

2.3.1. Chuyển dịch từ tư duy “Thu giữ vật mang tin” sang “Bảo toàn dữ liệu nguồn”

Công ước của Liên Hợp Quốc về chống tội phạm mạng yêu cầu các quốc gia thành viên phải thiết lập cơ chế pháp lý cho phép thực hiện ba biện pháp tố tụng cốt lõi: (i) Bảo toàn nhanh dữ liệu máy tính đã lưu trữ (expedited preservation); (ii) Tiết lộ nhanh dữ liệu lưu lượng (traffic data); và (iii) Thu thập thời gian thực (real - time

collection) đối với dữ liệu nội dung. (Điều 29, Bảo toàn nhanh dữ liệu máy tính đã lưu trữ, Điều 30, Tiết lộ nhanh dữ liệu lưu lượng và Điều 34, Thu thập thời gian thực dữ liệu nội dung) (Liên Hợp Quốc, 2025).

Quy trình tố tụng hiện nay theo BLTTHS 2015 và Nghị định số 08/2020/NĐ - CP về cơ bản vẫn chịu ảnh hưởng của tư duy điều tra truyền thống: coi dữ liệu điện tử gắn liền với vật mang tin vật lý (ổ cứng, máy tính, điện thoại). Cơ quan điều tra thường áp dụng biện pháp thu giữ, niêm phong thiết bị. Theo quy định tại Điều 196 BLTTHS việc khám xét, thu giữ phương tiện điện tử thường đi kèm với việc niêm phong thiết bị cứng (Quốc hội, 2025). Điều này gây khó khăn cho hoạt động của doanh nghiệp nếu máy chủ bị thu giữ, và không hiệu quả đối với dữ liệu đám mây. Tuy nhiên, trong kỷ nguyên điện toán đám mây (cloud computing), dữ liệu không nằm trong thiết bị của nghi phạm mà nằm tại các máy chủ ảo, phân tán ở nhiều quốc gia. Việc niêm phong máy tính cá nhân trở nên vô nghĩa khi dữ liệu có thể bị xóa từ xa (remote wipe) chỉ trong vài giây.

Đề nghị luật hóa Công ước và thực hiện yêu cầu “nâng cao hiệu quả thi hành pháp luật” của Nghị quyết 66, Việt Nam cần bổ sung quy định về “Lệnh bảo toàn dữ liệu khẩn cấp”. Lệnh này cho phép Cơ quan điều tra yêu cầu nhà cung cấp dịch vụ hoặc người quản lý hệ thống “đóng băng” dữ liệu ngay lập tức trong thời gian chờ (ví dụ: 90 ngày) để hoàn tất thủ tục xin lệnh thu thập chính thức từ Viện kiểm sát hoặc tòa án. Đây là biện pháp ngăn chặn tình trạng tẩu tán chứng cứ điện tử - vốn có đặc tính “dễ bay hơi” (volatility).

2.3.2. Thẩm quyền và quy trình đối với dữ liệu xuyên biên giới

Điều 25 của Công ước của Liên Hợp Quốc về chống tội phạm mạng đặt ra vấn đề nhạy cảm về việc tiếp cận dữ liệu được lưu trữ tại lãnh thổ của một bên khác. Hiện nay, BLTTHS 2015 chưa có quy định rõ ràng về thẩm quyền của Cơ quan điều tra Việt Nam trong việc yêu cầu các tập đoàn công nghệ xuyên biên giới (Big Tech) cung cấp dữ liệu người dùng Việt Nam phục vụ tố tụng hình sự. Quy trình hiện tại chủ yếu dựa vào kênh tương trợ tư pháp (MLAT) truyền thống, thường mất từ 6 đến 12 tháng - khoảng thời gian quá dài để điều tra tội phạm mạng.

Vì vậy, cần xây dựng cơ chế pháp lý cho phép cơ quan tiến hành tố tụng Việt Nam gửi yêu cầu trực tiếp đến các nhà cung cấp dịch vụ hoạt động tại Việt Nam để thu thập “dữ liệu thuê bao” (subscriber information) và

“dữ liệu truy cập” (access data) mà không cần qua kênh ngoại giao phức tạp, miễn là tuân thủ các nguyên tắc bảo vệ dữ liệu cá nhân.

2.3.3. Chuẩn hóa quy trình giám định và “Chuỗi hành trình chứng cứ” (Chain of Custody)

Giá trị chứng minh của chứng cứ điện tử phụ thuộc hoàn toàn vào tính nguyên vẹn (integrity) từ lúc thu thập đến lúc xét xử. Công ước của Liên Hợp Quốc về chống tội phạm mạng nhấn mạnh việc sử dụng các công cụ kỹ thuật hình sự để đảm bảo dữ liệu không bị can thiệp. Hiện nay, nhiều luật sư tại các phiên tòa thường bác bỏ giá trị của chứng cứ điện tử do quy trình thu thập không đảm bảo tính khách quan, dễ bị chỉnh sửa. Thực tiễn xét xử cho thấy, tranh tụng về tính hợp pháp của chứng cứ điện tử (tin nhắn zalo, facebook, email...) là rất phổ biến. Việc thiếu quy trình chuẩn về digital forensics (kỹ thuật hình sự số) khiến tòa án gặp khó khăn trong việc đánh giá chứng cứ.

Vì vậy, chúng tôi đề xuất “Biện pháp điều tra đặc biệt đối với dữ liệu số” theo hướng bổ sung một Mục riêng trong BLTTHS hoặc ban hành Luật sửa đổi bổ sung một số điều của BLTTHS quy định chi tiết về: Quy trình sao chép dữ liệu (bit - stream image); sử dụng mã băm (hash value) để xác thực tính nguyên vẹn của tập tin tại mọi thời điểm chuyển giao. Thẩm quyền phê chuẩn của Viện kiểm sát đối với các biện pháp kỹ thuật nghiệp vụ xâm phạm quyền riêng tư (như nghe lén, thu thập dữ liệu nội dung thời gian thực) để đảm bảo cơ chế kiểm soát quyền lực nhà nước theo tinh thần Nghị quyết 66.

2.3.4. Tương trợ tư pháp và hợp tác quốc tế giúp giải quyết bài toán về tốc độ và xung đột pháp lý

Trong kỷ nguyên số, “chứng cứ điện tử không biết đến biên giới quốc gia”, nhưng quyền lực tư pháp lại bị giới hạn bởi lãnh thổ. Công ước của Liên Hợp Quốc về chống tội phạm mạng dành Chương V (hợp tác quốc tế) để thiết lập một khung khổ pháp lý mới nhằm giải quyết mâu thuẫn này. Việc nội luật hóa các cam kết này đòi hỏi Việt Nam phải sửa đổi căn bản pháp luật về tương trợ tư pháp, chuyển dịch từ cơ chế hành chính quan liêu sang cơ chế phản ứng nhanh, cụ thể là:

Thứ nhất, thể chế hóa “Mạng lưới 24/7” và tháo gỡ độ trễ hành chính: Điều 35 (Mạng lưới 24/7) quy định các điểm liên lạc phải sẵn sàng 24/7 để tạo điều kiện thuận lợi cho việc hỗ trợ ngay lập tức các cuộc điều tra, yêu cầu mỗi quốc gia thành viên phải chỉ định một “Điểm liên lạc 24/7” (24/7 Point of Contact). Cơ quan này phải có

khả năng hoạt động liên tục bảy ngày trong tuần để hỗ trợ khẩn cấp việc bảo toàn dữ liệu và thu thập chứng cứ (Liên Hợp Quốc, 2024).

Quy trình tương trợ tư pháp về hình sự hiện nay của Việt Nam còn nặng tính hành chính, phải đi vòng qua nhiều cấp: Cơ quan điều tra, Viện kiểm sát nhân dân tối cao, Bộ Tư pháp/Bộ Ngoại giao, Cơ quan đối tác nước ngoài. “Độ trễ” của quy trình này thường kéo dài từ 6 tháng đến 1 năm, trong khi dữ liệu điện tử có thể bị xóa hoặc thay đổi chỉ trong vài giây. Thực tiễn cho thấy, các yêu cầu tương trợ tư pháp gửi đến các tập đoàn công nghệ lớn (thường đặt trụ sở tại Mỹ hoặc châu Âu) thường bị từ chối hoặc chậm trễ do không đáp ứng đúng chuẩn mực pháp lý của nước sở tại (ví dụ: Đạo luật CLOUD Act của Mỹ) hoặc do quy trình ngoại giao quá phức tạp.

Vì vậy, cần luật hóa địa vị pháp lý của điểm liên lạc quốc gia (đặt tại Bộ Công an - Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao). Điểm liên lạc không chỉ đóng vai trò “hòm thư” trung chuyển, mà cần được trao thẩm quyền ra các Lệnh phong tỏa tạm thời (provisional measures) đối với dữ liệu ngay khi nhận được yêu cầu hợp lệ từ nước ngoài, trước khi hồ sơ chính thức được hoàn thiện. Đây là bước đột phá cần thiết để đảm bảo tính “kịp thời” theo tinh thần cải cách tư pháp của Nghị quyết số 66.

Thứ hai, hợp tác trực tiếp với nhà cung cấp dịch vụ và vấn đề chủ quyền số: Một xu hướng mới trong Công ước của Liên Hợp Quốc về chống tội phạm mạng (và các điều ước quốc tế hiện đại) là khuyến khích cơ chế hợp tác trực tiếp giữa cơ quan thực thi pháp luật của một quốc gia với nhà cung cấp dịch vụ (ISP/OSP) ở quốc gia khác trong trường hợp khẩn cấp mà không cần qua kênh ngoại giao. Điều 25 Công ước của Liên Hợp Quốc về chống tội phạm mạng (Truy cập xuyên biên giới tới dữ liệu máy tính được lưu trữ...) cho phép các quốc gia truy cập dữ liệu công khai hoặc dữ liệu mà người dùng tự nguyện đồng ý, nhưng các quy định về truy cập cưỡng chế vẫn còn nhiều tranh luận (Liên Hợp Quốc, 2024).

Điều này tạo ra thách thức lớn đối với nguyên tắc chủ quyền dữ liệu được quy định cứng trong Luật An ninh mạng 2018 (yêu cầu lưu trữ dữ liệu tại Việt Nam và kiểm soát luồng thông tin). Điều 26 Luật này quy định về lưu trữ dữ liệu người sử dụng dịch vụ tại Việt Nam và yêu cầu doanh nghiệp cung cấp dữ liệu khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an (Quốc hội, 2018). Việc cho phép một thực thể

nước ngoài yêu cầu Facebook hay Google cung cấp dữ liệu của công dân Việt Nam (hoặc ngược lại) mà không có sự kiểm soát của cơ quan nhà nước có thể dẫn đến rủi ro lộ lọt bí mật nhà nước hoặc xâm phạm quyền riêng tư.

Vì vậy, Việt Nam cần xây dựng một Quy chế phối hợp đặc biệt. Theo đó, cho phép hợp tác trực tiếp đối với các thông tin ít nhạy cảm (như thông tin thuê bao, dữ liệu truy cập) nhưng bắt buộc phải thông qua Điểm liên lạc quốc gia đối với dữ liệu nội dung (content data). Điều này đảm bảo sự cân bằng giữa yêu cầu truy vết tội phạm nhanh chóng và yêu cầu bảo vệ an ninh quốc gia.

Thứ ba, vượt qua rào cản “Song trùng tội phạm” (Dual criminality) một cách linh hoạt: Theo truyền thống, tương trợ tư pháp chỉ được thực hiện khi hành vi bị yêu cầu điều tra là tội phạm ở cả hai quốc gia “song trùng”. Tuy nhiên, trong môi trường Internet, khái niệm này gặp nhiều va chạm do sự khác biệt về văn hóa và thể chế chính trị (ví dụ: Các tội danh về an ninh quốc gia, tự do ngôn luận, hay các hành vi lệch chuẩn trên mạng).

Đối với biện pháp cưỡng chế mạnh (như khám xét, thu giữ, dẫn độ), Việt Nam cần kiên quyết giữ nguyên tắc song trùng tội phạm để bảo vệ công dân và chủ quyền tư pháp, phù hợp với các tuyên bố bảo lưu khi ký kết Công ước.

Đối với biện pháp hỗ trợ (bảo toàn dữ liệu, xác minh thông tin), pháp luật về tương trợ tư pháp nên áp dụng nguyên tắc linh hoạt hơn. Có thể xem xét bỏ yêu cầu song trùng tội phạm đối với các yêu cầu bảo toàn dữ liệu khẩn cấp (expedited preservation). Lý do là việc “đóng băng” dữ liệu chưa xâm phạm sâu vào quyền con người như việc “thu giữ/đọc” dữ liệu, và việc này giúp ngăn chặn tội phạm tẩu tán chứng cứ trong khi chờ xem xét tính hợp pháp của yêu cầu. Cách tiếp cận này phù hợp với xu hướng quốc tế (như Công ước Budapest). Việc tách bạch yêu cầu song trùng tội phạm giữa giai đoạn “bảo toàn” và giai đoạn “cung cấp/khám xét” giúp tăng hiệu quả hợp tác mà không đánh đổi các nguyên tắc pháp lý căn bản.

2.4. Thách thức và giải pháp cân bằng giữa bảo đảm an ninh và bảo đảm, bảo vệ quyền con người

Nghị quyết số 66 - NQ/TW xác định mục tiêu xây dựng hệ thống pháp luật “dân chủ, công bằng, nhân văn”, trong đó đặc biệt nhấn mạnh yêu cầu “bảo đảm, bảo vệ hiệu quả quyền con người, quyền công dân”. Do đó, quá trình nội luật hóa các biện pháp tố tụng mạnh mẽ của Công ước của Liên Hợp Quốc về chống tội phạm mạng không được phép trở thành công cụ để mở rộng quyền

giám sát thiếu kiểm soát, mà phải tuân thủ chặt chẽ các điều kiện bảo đảm quyền con người quy định tại Điều 24 của chính Công ước này (các điều kiện và biện pháp bảo vệ). Điều này quy định rằng việc áp dụng các quyền hạn tố tụng phải chịu sự điều chỉnh của các điều kiện và biện pháp bảo vệ theo pháp luật trong nước, bao gồm cả sự giám sát tư pháp và tôn trọng các công ước quốc tế về quyền con người (Liên Hợp Quốc, 2024).

2.4.1. Thiết lập cơ chế “Kiểm soát quyền lực” qua giám sát tư pháp

Công ước của Liên Hợp Quốc về chống tội phạm mạng cho phép áp dụng các biện pháp xâm phạm sâu vào quyền riêng tư như: Nghe lén, thu thập dữ liệu nội dung, theo dõi vị trí. Tuy nhiên, nếu các biện pháp này chỉ dựa trên quyết định hành chính đơn phương của Cơ quan điều tra, nguy cơ lạm quyền là rất lớn.

Cần sửa đổi BLTTHS theo hướng: Các biện pháp điều tra kỹ thuật số xâm phạm bí mật đời tư, thư tín, điện tín (được bảo vệ bởi Điều 21 Hiến pháp). “Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình... Việc bóc mở, kiểm soát, thu giữ thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác của người khác chỉ được thực hiện trong trường hợp luật định” (Quốc hội, 2025). Đây là cơ chế “kiểm soát quyền lực” tối cần thiết để đảm bảo tính khách quan.

Để các quy định giám sát đi vào thực chất, BLTTHS cần quy định cứng rắn: Mọi dữ liệu điện tử thu thập không đúng trình tự luật định, không có lệnh của cơ quan có thẩm quyền, hoặc thu thập qua các phương tiện kỹ thuật chưa được kiểm định... đều không có giá trị pháp lý và không được dùng làm chứng cứ buộc tội. Quy định này sẽ buộc các cơ quan tiến hành tố tụng phải tuân thủ nghiêm ngặt quy trình tố tụng. Điều 87 BLTTHS hiện hành quy định: “Những gì có thật nhưng không được thu thập theo trình tự, thủ tục do Bộ luật này quy định thì không có giá trị pháp lý và không được dùng làm căn cứ để giải quyết vụ án hình sự” (Quốc hội, 2025). Tuy nhiên, thực tiễn áp dụng quy định này đối với chứng cứ điện tử còn nhiều bất cập, cần được hướng dẫn chi tiết hơn.

2.4.2. Bảo vệ dữ liệu cá nhân trong hợp tác quốc tế

Một trong những lo ngại lớn nhất khi tham gia Công ước là nguy cơ dữ liệu của công dân Việt Nam bị chuyển giao ra nước ngoài và bị sử dụng sai mục đích.

Quá trình chia sẻ dữ liệu tội phạm theo Công ước phải được coi là một trường hợp “chuyển dữ liệu ra nước ngoài”. Do đó, nó phải tuân thủ các nguyên tắc của Nghị

định 13/2023/NĐ - CP. Cần thiết lập các “bộ lọc” pháp lý, cụ thể: Trước khi chuyển giao dữ liệu (đặc biệt là dữ liệu nhạy cảm, sinh trắc học), cơ quan có thẩm quyền Việt Nam phải đánh giá mức độ bảo vệ dữ liệu của quốc gia nhận yêu cầu. Dữ liệu chuyển giao chỉ được sử dụng cho mục đích điều tra vụ án hình sự cụ thể đã nêu trong yêu cầu, tuyệt đối không được chia sẻ cho bên thứ ba hoặc sử dụng vào mục đích chính trị, thương mại. Điều 25 Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân quy định về chuyển dữ liệu cá nhân ra nước ngoài, yêu cầu bên chuyển dữ liệu phải lập hồ sơ đánh giá tác động (Chính phủ, 2023). Trong bối cảnh tố tụng hình sự, cần có quy chế riêng để đảm bảo vừa tuân thủ Nghị định này, vừa không làm chậm trễ quá trình điều tra.

3. Kết luận

Công ước của Liên Hợp Quốc về chống tội phạm mạng không chỉ là một văn kiện ngoại giao, mà là một khuôn khổ tham chiếu quan trọng cho tiến trình cải cách pháp luật tại Việt Nam. Việc nội luật hóa Công ước này chính là hành động cụ thể nhất để hiện thực hóa Nghị quyết 66 - NQ/TW: xây dựng một hệ thống pháp luật vừa đảm bảo an ninh quốc gia, vừa kiến tạo môi trường số an toàn, minh bạch và hội nhập.

Để làm được điều này, Quốc hội và Chính phủ cần ưu tiên: (1) Sửa đổi đồng bộ Bộ luật Hình sự, Bộ luật Tố tụng hình sự và pháp luật liên quan đến tương trợ tư pháp; (2) Xây dựng khung pháp lý về tài sản ảo; và (3) Đào tạo nguồn nhân lực tư pháp có năng lực số và ngoại ngữ để tham gia hiệu quả vào mạng lưới hợp tác toàn cầu./.

TÀI LIỆU THAM KHẢO

- Ban Chấp hành Trung ương (2025). *Nghị quyết số 66-NQ/TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật*.
- Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân*.
- Liên Hợp Quốc (2024). *Công ước Chống tội phạm mạng*.
- Luật số 34/2024/QH15. *Luật số 59/2024/QH15, Luật số 99/2025/QH15*.
- Quốc hội (2015). *Bộ luật Dân sự*.
- Quốc hội (2025). *Bộ luật Hình sự số 100/2015/QH13 được sửa đổi, bổ sung bởi Luật số 12/2017/QH14, Luật số 59/2024/QH15, Luật số 86/2025/QH15*.
- Quốc hội (2025). *Bộ luật Tố tụng hình sự số 101/2015/QH13 được sửa đổi, bổ sung bởi Luật số 02/2021/QH15*.
- Quốc hội (2025). *Luật Công nghiệp công nghệ số*.
- Quốc hội (2025). *Hiến pháp năm 2013 được sửa đổi, bổ sung bởi Nghị quyết số 203/2025/QH15*.