PHÂN TÍCH: LUẬT AN NINH MẠNG CỦA VIỆT NAM VÀ CÔNG ƯỚC LIÊN HIỆP QUỐC VỀ TỘI PHẠM MẠNG

Linh Nguyễn, JD

Prepared for
PERMANENT MISSIONS TO THE UNITED NATIONS

Reporting Date
3/7/2025

MỤC LỤC

1. Dẫn Nhập và Bối Cảnh

Luật An Ninh Mạng của Việt Nam (ban hành năm 2018) là một bộ khung pháp lý trong nước nhằm kiểm soát các hoạt động trên không gian mạng tại Việt Nam, với danh nghĩa bảo vệ an ninh quốc gia và trật tự xã hội. Luật này chính thức có hiệu lực kể từ ngày 1 tháng 1 năm 2019, và đã thiết lập những biện pháp kiểm soát toàn diện đối với nội dung trực tuyến và quản lý dữ liệu, cả ở cấp độ cá nhân lẫn các nhà cung cấp dịch vụ.

Trái lại, Công Ước Liên Hiệp Quốc về Tội Phạm Mạng (2024) – được gọi không chính thức là "Công Ước Hà Nội" do sẽ được khai mạc ký kết tại Hà Nội vào tháng 10 năm 2025 – là một hiệp ước toàn cầu mới được Đại Hội Đồng Liên Hiệp Quốc thông qua vào cuối năm 2024. Đây là công ước đầu tiên của Liên Hiệp Quốc về phòng chống tội phạm được ban hành trong hơn hai thập niên qua, nhằm điều hòa pháp luật và tăng cường hợp tác quốc tế trong cuộc đấu tranh chống tội phạm mạng.

Bản phúc trình này trình bày một phân tích so sánh chi tiết giữa hai bộ khung pháp lý nói trên, tập trung vào các yếu tố then chốt sau đây:

1. Phạm vi và định nghĩa pháp lý – Cách mỗi văn kiện định nghĩa phạm vi áp dụng, các loại tội danh được bao phủ, thẩm quyền tài phán và nghĩa vụ pháp lý đi kèm.
2. Cơ chế thực thi – Cơ quan cưỡng hành luật, các biện pháp thủ tục, và hệ thống giám sát trong từng khuôn khổ.
3. Tác động địa chính trị – Mức độ tương hợp hoặc xung khắc với các chuẩn mực quốc tế và bối cảnh tổng thể trong chính sách mạng của Việt Nam.
4. Phản hồi và phê bình – Những nhận xét từ các quan sát viên quốc tế, các tổ chức phi chính phủ, các tổ chức bảo vệ quyền số, và giới học giả pháp lý.

Bản phân tích này cũng cập nhật các diễn tiến mới nhất liên quan đến tiến trình xây dựng Công Ước Liên Hiệp Quốc và chính sách an ninh mạng hiện hành của Việt Nam, bảo đảm một sự đối chiếu đầy đủ và thời sự. Ngoài ra, tài liệu còn kèm theo một bảng so sánh tổng quát để tiện việc tra cứu và tham khảo nhanh.

2. Phạm Vi Pháp Lý, Định Nghĩa, Thẩm Quyền và Nghĩa Vụ

Cả Luật An Ninh Mạng của Việt Nam lẫn Công Ước Liên Hiệp Quốc về Tội Phạm Mạng đều nhằm đối phó với các mối đe dọa và hành vi phạm pháp trên không gian mạng. Tuy nhiên, hai văn kiện này khác biệt rõ rệt về phạm vi áp dụng, cách định nghĩa tội phạm, thẩm quyền tài phán, và các nghĩa vụ được đặt ra cho các đối tượng liên quan.

Luật An Ninh Mạng của Việt Nam (2018):

Luật này có phạm vi rất rộng, bao gồm mọi hoạt động trên không gian mạng có thể gây ảnh hưởng đến "an ninh quốc gia, trật tự công cộng", hay sự tồn vong của chế độ xã hội chủ nghĩa. Luật đưa ra các nhóm hành vi bị cấm với ngôn từ mơ hồ và bao quát – phần lớn liên quan đến quyền tự do ngôn luận trên mạng. Chẳng hạn, luật cấm việc sử dụng không gian mạng để "tuyên truyền chống Nhà nước," "xuyên tạc lịch sử," "gây chia rẽ," hoặc "đưa tin sai sự thật" có thể làm tổn hại đến nhà cầm quyền hoặc danh dự cá nhân. Khái niệm "gián điệp mạng" cũng được định nghĩa một cách mơ hồ là hành vi vượt tường lửa hoặc các biện pháp bảo vệ để thu thập thông tin một cách bất hợp pháp. Những định nghĩa rộng rãi này cho phép hình sự hóa một phạm vi lớn các hành vi phát biểu và phản biện ôn hòa, dưới danh nghĩa bảo vệ an ninh mạng.

Về mặt nghĩa vụ, luật này đặt gánh nặng lớn lên các công ty tư nhân: các nhà cung cấp dịch vụ (kể cả những nền tảng nước ngoài hoạt động tại Việt Nam) bị buộc phải kiểm duyệt nội dung bị coi là "vi phạm," cung cấp dữ liệu người dùng cho nhà cầm quyền khi được yêu cầu, và xác minh danh tính người dùng (qua đó vô hiệu hóa việc sử dụng ẩn danh). Các công ty phải gỡ bỏ nội dung "vi phạm" trong vòng 24 giờ theo yêu cầu của nhà cầm quyền và phải lưu trữ một số loại dữ liệu trong lãnh thổ Việt Nam.

Về thẩm quyền tài phán, luật tuyên bố quyền kiểm soát đối với mọi dịch vụ trong không gian mạng Việt Nam – bao gồm cả việc yêu cầu các nền tảng nước ngoài phải đặt văn phòng đại diện và máy chủ tại Việt Nam nếu thu thập hoặc truyền bá dữ liệu người dùng Việt. Trên hết, luật này đặt ưu tiên tối hậu cho cái gọi là "lợi ích an ninh" do Đảng Cộng Sản xác định, và công khai xếp các quyền tự do cá nhân – như quyền tự do ngôn luận – dưới các "lợi ích chính trị của nước Cộng Hòa Xã Hội Chủ Nghĩa Việt Nam."

Công Ước Liên Hiệp Quốc về Tội Phạm Mạng (2024):

Về hình thức, Công Ước này có phạm vi hẹp hơn khi tập trung vào tội phạm mạng – tức các hành vi phạm pháp liên quan đến hệ thống máy tính và mạng thông tin. Tuy nhiên, trên thực tế, Công Ước lại bao trùm phạm vi rộng lớn. Nó xác định một loạt tội danh cốt lõi như xâm nhập trái phép hệ thống máy tính, gian lận mạng, và phát tán tài liệu lạm dụng tình dục trẻ em (CSAM), phản ánh các tiêu chuẩn hình sự truyền thống trong lĩnh vực tội phạm mạng.

Tuy nhiên, Công Ước cũng quy định rằng các quốc gia thành viên phải hợp tác trong việc điều tra bất kỳ "tội phạm nghiêm trọng" nào có liên quan đến bằng chứng điện tử. Điều đáng chú ý là khái niệm "tội phạm nghiêm trọng" được định nghĩa rất rộng – bất kỳ hành vi nào bị luật quốc gia quy định mức án tối thiểu là bốn năm tù. Quan trọng hơn, định nghĩa này không đòi hỏi tội phạm phải có bản chất "mạng" hoặc kỹ thuật số. Nói cách khác, nếu một quốc gia xem một hình thức phát biểu hay hoạt động nào đó là "tội phạm nghiêm trọng" (thí dụ: "tuyên truyền phản động" hay phát biểu chống nhà cầm quyền bị xử phạt nặng theo luật quốc nội), thì các cơ chế hợp tác theo Công Ước vẫn có thể được kích hoạt – kể cả khi hành vi đó không mang yếu tố mạng rõ rệt.

Công Ước đặt ra nghĩa vụ cho các quốc gia, chứ không trực tiếp cho các công ty tư nhân: các quốc gia phải hình sự hóa một số tội phạm mạng trong hệ thống luật nội địa của mình, thiết lập các biện pháp thủ tục (như lưu trữ và thu giữ dữ liệu) để phục vụ điều tra tội phạm mạng, và tạo điều kiện cho hợp tác quốc tế thông qua các hình thức như tương trợ tư pháp và dẫn độ. Ngoài ra, mỗi quốc gia phải chỉ định một cơ quan đầu mối (chẳng hạn, điểm liên lạc 24/7 về tội phạm mạng) để xử lý các yêu cầu xuyên quốc gia.

Về thẩm quyền tài phán, Công Ước có phạm vi rất rộng – nó công khai xác lập nguyên tắc tài phán ngoài lãnh thổ. Đặc biệt, Điều 22 cho phép một quốc gia khởi tố các hành vi phạm pháp do "bất kỳ ai, ở bất kỳ nơi đâu" thực hiện, miễn là hành vi đó gây tổn hại cho công dân của họ – nguyên tắc này được gọi là "tài phán thụ động theo quốc tịch nạn nhân." Điều đó có nghĩa là, chẳng hạn, một quốc gia có thể yêu cầu dẫn độ một công dân nước ngoài vì hành vi trực tuyến ở nước khác, nếu hành vi đó bị cho là đã gây hại đến công dân của nước yêu cầu – qua đó mở rộng đáng kể phạm vi tài phán truyền thống trong các vụ án mạng.

Mặc dù Công Ước có bao gồm một điều khoản chung nêu rõ rằng "không điều khoản nào trong Công Ước này được hiểu là cho phép vi phạm nhân quyền" (Điều 6.2), nhưng phần lớn các biện pháp bảo vệ được giao về thẩm quyền của luật quốc gia, và Công Ước không thiết lập một cơ chế giám sát độc lập để đảm bảo sự tuân thủ các tiêu chuẩn nhân quyền.

Yếu Tố	Luật An Ninh Mạng của Việt Nam (2018)	Công Ước Liên Hiệp Quốc về Tội Phạm Mạng (2024)
Phạm Vi & Mục Tiêu	Luật trong nước nhằm bảo vệ "an ninh quốc gia và trật tự xã hội" trên không gian mạng. Bao quát cả an ninh mạng và kiểm soát thông tin trong nước.	Hiệp ước quốc tế nhằm chống tội phạm mạng và tăng cường hợp tác toàn cầu. Tập trung vào các tội phạm sử dụng công nghệ thông tin và truyền thông (CNTT-TT), nhưng cho phép hợp tác rộng cho bất kỳ tội phạm nghiêm trọng có liên quan đến bằng chứng điện tử.
Tội Danh & Định Nghĩa	Định nghĩa mơ hồ và bao quát, bao gồm "tuyên truyền chống Nhà nước," "xuyên tạc lịch sử," "gây chia rẽ," "đưa tin sai sự thật." Cũng bao gồm một số tội phạm mạng truyền thống, nhưng nhấn mạnh yếu tố tư tưởng, chính trị.	Xác định các tội phạm mạng cốt lõi như xâm nhập trái phép, gian lận mạng, CSAM. Loại bỏ một số đề xuất mơ hồ (như "chủ nghĩa cực đoan"). Cho phép điều tra các tội phạm nghiêm trọng do mỗi quốc gia xác định, kể cả những hành vi không mang tính kỹ thuật số rõ rệt.
Thẩm Quyền Tài Phán	Áp dụng cho tất cả mạng lưới và dịch vụ hoạt động tại Việt Nam. Yêu cầu các nền tảng nước ngoài phải đặt văn phòng đại diện và máy chủ tại Việt Nam nếu phục vụ người dùng Việt. Chủ yếu là tài phán nội địa, nhưng áp dụng rộng qua việc kiểm soát hạ tầng xuyên biên giới.	Cho phép tài phán mở rộng. Điều 22 cho phép khởi tố các hành vi phạm pháp ở nước ngoài nếu gây tổn hại đến công dân trong nước (tài phán thụ động theo quốc tịch). Cũng hỗ trợ các cơ sở tài phán truyền thống như lãnh thổ và quốc tịch. Mở rộng đáng kể phạm vi truy tố trong không gian mạng.
Nghĩa Vụ Đặt Ra	Đặt nghĩa vụ trực tiếp lên các công ty tư nhân: lưu trữ dữ liệu tại Việt Nam, xác minh danh tính người dùng, gỡ bỏ nội dung bị cho là "vi phạm" trong vòng 24 giờ, và cung cấp thông tin người dùng theo yêu cầu không cần lệnh tòa.	Đặt nghĩa vụ lên quốc gia thành viên: hình sự hóa các tội danh quy định, ban hành thủ tục điều tra (như lưu trữ và thu giữ dữ liệu), thiết lập cơ chế hợp tác quốc tế như tương trợ tư pháp và dẫn độ. Không áp đặt nghĩa vụ trực tiếp lên công ty tư nhân ở cấp hiệp ước.
Cơ Quan Thực Thi	Bộ Công An, đặc biệt là Cục An Ninh Mạng (A05), và các đơn vị quân đội như Lực lượng 47. Có quyền yêu cầu dữ liệu và kiểm duyệt nội dung mà không cần lệnh tư pháp. Tòa án trong nước xử lý các vụ việc theo luật an ninh quốc gia.	Do các cơ quan thực thi pháp luật và tư pháp của mỗi quốc gia thành viên đảm trách. Phải chỉ định cơ quan trung ương và điểm liên lạc 24/7 để xử lý yêu cầu hợp tác. Không có cơ quan cảnh sát quốc tế riêng – UNODC chỉ đóng vai trò hỗ trợ kỹ thuật và điều phối.
Cơ Chế Giám Sát & Bảo Vệ	Giám sát mang tính nội bộ và chính trị – Đảng Cộng Sản nắm quyền tối hậu. Không có cơ chế giám sát độc lập. Yêu cầu cung cấp dữ liệu không cần tòa án phê chuẩn. Quyền tự do bị đặt dưới "lợi ích chính trị của nước CHXHCN Việt Nam."	Có điều khoản tổng quát về nhân quyền (Điều 6.2), nhưng phần lớn bảo vệ pháp lý được giao về luật quốc gia. Không thiết lập cơ chế giám sát độc lập. Các yêu cầu hợp tác có thể giữ bí mật, và không bắt buộc phải thông báo cho cá nhân bị theo dõi hoặc thu thập dữ liệu.

3. Cơ Chế Thực Thi: Cưỡng Hành, Thủ Tục, và Giám Sát

Cơ Chế Thực Thi của Việt Nam

Cơ Quan Cưỡng Hành:

Chế độ an ninh mạng tại Việt Nam chủ yếu được cưỡng hành bởi Bộ Công An (BCA), đặc biệt là các đơn vị chuyên trách về an ninh mạng và phòng chống tội phạm công nghệ cao. Luật An Ninh Mạng do chính Bộ Công An soạn thảo và trao quyền rộng rãi cho các cơ quan an ninh trong việc kiểm soát nội dung và hành vi trên không gian mạng. Trong nội bộ Bộ Công An, Cục An Ninh Mạng và Phòng, Chống Tội Phạm Sử Dụng Công Nghệ Cao – thường được gọi là A05 – đóng vai trò nòng cốt trong công tác điều tra và buộc các doanh nghiệp phải tuân thủ luật pháp. Bên cạnh đó, quân đội cũng tham gia tích cực: Lực lượng 47 – một đơn vị chiến tranh mạng thuộc Quân đội Nhân dân với quân số khoảng 10.000 người được thành lập từ năm 2016 – có nhiệm vụ theo dõi mạng xã hội và phản bác các quan điểm bị xem là "chống đối chế độ." Các cơ quan này đều hoạt động dưới sự chỉ đạo trực tiếp của Đảng Cộng Sản, bởi luật đã quy định rằng an ninh mạng phải được đặt dưới "sự lãnh đạo của Đảng Cộng sản Việt Nam."

Quyền Hạn Thủ Tục:

Luật An Ninh Mạng trao cho cơ quan chức năng một loạt thẩm quyền cưỡng hành mà không cần sự chuẩn thuận của tư pháp. Các lệnh yêu cầu gỡ bỏ nội dung có thể được ban hành bởi Bộ Thông Tin và Truyền Thông hoặc Bộ Công An, buộc các nhà cung cấp dịch vụ phải xóa bỏ nội dung bị cho là "vi phạm" trong vòng 24 giờ. Quyền truy cập và thu giữ dữ liệu được hỗ trợ thông qua các quy định buộc doanh nghiệp phải lưu trữ và "cung cấp thông tin người dùng," kể cả "dấu vết liên quan" (metadata), cho các đơn vị chuyên trách khi có yêu cầu. Đáng lưu ý, các yêu cầu này không cần lệnh tòa án theo quy định hiện hành, tức là lực lượng công an có thể trực tiếp buộc các nền tảng giao nộp dữ liệu nhân danh an ninh mạng.

Luật cũng cho phép giám sát mạng và lọc nội dung – kế thừa từ các nghị định trước đó như Nghị định 72 về quản lý thông tin trên Internet. Nhằm siết chặt kiểm soát dữ liệu, Việt Nam đã ban hành Nghị định 53 (2022) để hướng dẫn thi hành: nghị định này bắt buộc các nhà cung cấp dịch vụ trên mạng – cả trong nước lẫn nước ngoài – phải lưu trữ dữ liệu tại Việt Nam và, khi được Bộ Công An thông báo, phải thiết lập văn phòng đại diện trong nước nếu dịch vụ của họ bị cho là vi phạm Luật An Ninh Mạng.

Theo Nghị định 53, nếu một nền tảng không tuân thủ (thí dụ: không xóa nội dung bị cấm hoặc không hợp tác điều tra), Bộ Công An có thể buộc họ phải lưu trữ dữ liệu người dùng tại Việt Nam trong vòng 12 tháng và giữ dữ liệu đó ít nhất 24 tháng. Quy định này tạo điều kiện thuận lợi cho việc cưỡng hành, bởi dữ liệu đặt trên lãnh thổ Việt Nam dễ bị nhà cầm quyền thu giữ. Ngoài ra, luật còn cho phép chặn truy cập đến các dịch vụ không tuân thủ – trên thực tế, đây là công cụ để kiểm duyệt hoặc buộc đóng cửa nền tảng.

Giám Sát và Khiếu Nại:

Việc giám sát thi hành Luật An Ninh Mạng tại Việt Nam chủ yếu tập trung trong hệ thống hành pháp và an ninh – không có cơ quan độc lập nào làm nhiệm vụ giám sát hay thẩm định mức độ hợp hiến, hợp pháp của các biện pháp cưỡng hành trong từng trường hợp cụ thể. Thay vào đó, các điều khoản mơ hồ trong luật trao quyền quyết định rất lớn cho nhà chức trách trong việc xác định đâu là hành vi vi phạm hoặc mối đe dọa. Mức độ tùy tiện này đã làm dấy lên nhiều lo ngại rằng luật không đơn thuần nhằm bảo vệ an ninh, mà được thiết kế như một công cụ chính trị để bảo vệ chế độ.
Các tổ chức nhân quyền quốc tế ghi nhận rằng Việt Nam gần như không có cơ chế bảo vệ quyền riêng tư đáng kể, và Luật An Ninh Mạng có thể "khiến việc nhận diện và truy tố những người hoạt động ôn hòa trên mạng trở nên dễ dàng hơn" cho nhà cầm quyền. Thực tế cho thấy kể từ khi luật có hiệu lực, nhiều nhà hoạt động và blogger đã bị bắt giữ và kết án theo các điều khoản liên quan (chẳng hạn điều luật về "tuyên truyền chống Nhà nước"), cho thấy việc cưỡng hành đã nhắm trực tiếp vào giới bất đồng chính kiến.
Tất cả các hình thức "giám sát" nếu có, chỉ mang tính nội bộ – thí dụ như việc đánh giá nội bộ do Đảng hoặc các cơ quan nhà nước thực hiện – và hoàn toàn không minh bạch. Vì thế, gần như không có cơ chế bên ngoài nào đủ khả năng kiểm soát hoặc ngăn chặn việc lạm dụng quyền lực cưỡng hành – điều mà giới chỉ trích cho rằng chính là bản chất của Luật An Ninh Mạng: một công cụ cho kiểm duyệt và giám sát toàn diện.

Cơ Chế Thực Thi của Công Ước Liên Hiệp Quốc về Tội Phạm Mạng

Cơ Quan Cưỡng Hành:

Việc thi hành Công Ước Liên Hiệp Quốc về Tội Phạm Mạng được thực hiện thông qua các cơ quan thực thi pháp luật và hệ thống tư pháp của từng quốc gia thành viên. Khi tham gia Công Ước, mỗi quốc gia phải chỉ định cơ quan đầu mối có thẩm quyền (thường là Bộ Tư Pháp hoặc cơ quan tương trợ tư pháp quốc tế) và một điểm liên lạc 24/7 để xử lý các yêu cầu khẩn cấp liên quan đến tội phạm mạng – cơ chế này tương tự như mô hình của Công Ước Budapest (do Hội Đồng Âu Châu khởi xướng). Công Ước không thiết lập một lực lượng cảnh sát quốc tế; thay vào đó, nó tạo dựng các kênh liên lạc và hợp tác để các quốc gia phối hợp điều tra và truy tố.

Ví dụ, một đơn vị tội phạm mạng trong Bộ Công An Việt Nam (nếu Việt Nam gia nhập Công Ước) có thể liên lạc trực tiếp với cơ quan đồng cấp tại quốc gia khác để yêu cầu bằng chứng, thông tin, hoặc hỗ trợ pháp lý – mà không cần phải qua các thủ tục ngoại giao phức tạp như trước. Văn phòng Liên Hiệp Quốc về Ma Túy và Tội Phạm (UNODC) giữ vai trò hỗ trợ kỹ thuật, huấn luyện và điều phối, nhưng không trực tiếp thực thi hoặc điều tra.

Công Ước cũng dự kiến sẽ thành lập các cuộc họp thường kỳ giữa các quốc gia thành viên (tương tự các "Hội nghị các bên" trong các hiệp ước khác), qua đó các quốc gia có thể đánh giá việc thi hành và chia sẻ kinh nghiệm. Đây có thể trở thành một hình thức giám sát lỏng lẻo ở cấp tập thể.

Thẩm Quyền Thủ Tục:

Công Ước quy chuẩn hóa một loạt thẩm quyền thủ tục mà mỗi quốc gia thành viên phải cam kết đưa vào pháp luật quốc nội nhằm phục vụ công tác điều tra tội phạm mạng. Các thẩm quyền này bao gồm khả năng:

- bảo toàn dữ liệu điện tử,
- tìm kiếm và thu giữ dữ liệu máy tính,
- chặn và theo dõi thông tin liên lạc,
- và thu thập dữ liệu truy cập theo thời gian thực, v.v.

Những biện pháp này phần lớn tương đồng với các quyền hạn đã được quy định trong Công Ước Budapest của Hội Đồng Âu Châu về Tội Phạm Mạng.

Điều đặc biệt đáng lưu ý là Công Ước mở rộng việc áp dụng các quyền hạn trên không chỉ đối với các tội danh mạng được định nghĩa trong văn bản, mà còn cho cả nhóm tội phạm rộng hơn được gọi là "tội phạm nghiêm trọng" nếu có yếu tố liên quan đến bằng chứng điện tử. Điều này có nghĩa là, ví dụ, nếu một quốc gia đang điều tra

một hành vi không phải là tội phạm mạng (chẳng hạn tội tài chính hoặc hành vi phát biểu bị hình sự hóa) mà có liên quan đến bằng chứng số như email hay nội dung trên mạng xã hội, quốc gia đó vẫn có thể sử dụng toàn bộ các công cụ giám sát và thu thập dữ liệu được cấp cho việc điều tra tội phạm mạng.

Công Ước cũng đặt ra nghĩa vụ hợp tác xuyên biên giới: các quốc gia phải hỗ trợ lẫn nhau trong việc chia sẻ bằng chứng điện tử và trả lời các yêu cầu hợp tác. *Điều 35* (về hợp tác quốc tế) về thực chất buộc các quốc gia phải thu thập, bảo toàn và chia sẻ dữ liệu theo yêu cầu của một quốc gia khác đối với bất kỳ tội danh nào có khung hình phạt từ 4 năm tù trở lên theo luật của quốc gia yêu cầu. Điều này có thể bao gồm cả:

- việc *thi hành lệnh từ quốc gia khác* (ví dụ: cơ quan điều tra của nước A yêu cầu nhà cung cấp dịch vụ ở nước B giao nộp dữ liệu),
- và yêu cầu bảo toàn dữ liệu khẩn cấp.

Chương thủ tục của Công Ước có cố gắng cân bằng giữa nhu cầu điều tra của cơ quan công lực và quyền riêng tư của công dân bằng cách đưa vào Điều 24 về "điều kiện và biện pháp bảo vệ." Tuy nhiên, các nhà phê bình cho rằng những biện pháp bảo vệ này là yếu và không đủ cụ thể: Điều 24 chỉ yêu cầu các quốc gia phải "tôn trọng nhân quyền và nguyên tắc tương xứng" một cách chung chung, nhưng không quy định rõ các yếu tố thiết yếu như tính cần thiết và hợp pháp của biện pháp giám sát, mà để hoàn toàn cho pháp luật nội địa quyết định.

Ví dụ: mặc dù Công Ước khuyến khích có sự giám sát của tư pháp đối với việc nghe lén hoặc chặn dữ liệu, nhưng không bắt buộc phải có nếu pháp luật của quốc gia đó không quy định điều này.

Hơn nữa, Công Ước áp dụng *nguyên tắc "mặc định giữ bí mật"* trong việc hợp tác: các yêu cầu cung cấp dữ liệu và bản thân hoạt động thu thập dữ liệu có thể được giữ kín, kể cả đối với bên cung cấp dịch vụ (có thể bị áp đặt lệnh "cấm tiết lộ"), và không có nghĩa vụ phải thông báo cho cá nhân liên quan rằng dữ liệu của họ đã bị truy xuất hoặc sử dụng.

Những quy định về thủ tục này trao cho các quốc gia một hệ thống công cụ rất mạnh về mặt giám sát và điều tra – không chỉ phục vụ các vụ án trong nước mà còn trong khuôn khổ hợp tác quốc tế – nhằm theo đuổi các hành vi phạm pháp trong lĩnh vực tội phạm mạng và các lĩnh vực liên quan.

Giám Sát và Tuân Thủ:

Khác với nhiều công ước quốc tế về nhân quyền, Công Ước về Tội Phạm Mạng không thiết lập một cơ quan giám sát độc lập để theo dõi việc các quốc gia thành viên thi hành và tuân thủ cam kết. Không có một "ủy ban hiệp ước" hay cơ cấu thường trực nào có thẩm quyền xét duyệt liệu một quốc gia có đang lạm dụng các quyền hạn mà Công Ước cho phép hay không.

Biện pháp kiểm soát duy nhất có trong văn bản là nguyên tắc tổng quát tại Điều 6.2, theo đó Công Ước không được hiểu là cho phép các hành vi vi phạm nhân quyền. Tuy nhiên, điều khoản này không đặt ra nghĩa vụ cụ thể cho những quốc gia chưa tham gia các công ước quốc tế khác về quyền con người. Trong quá trình đàm phán, một số quốc gia còn khẳng định rõ rằng Điều 6.2 "không tạo ra nghĩa vụ pháp lý" đối với những nước không ký các văn kiện nhân quyền riêng biệt.

Hệ quả là các quốc gia có khuynh hướng độc tài có thể tuân thủ hình thức nội dung của Công Ước, nhưng lại vi phạm tinh thần của nó – bằng cách sử dụng các quyền hạn mới được trao mà không lo ngại bị chế tài hay truy cứu trách nhiệm pháp lý quốc tế.

Việc giám sát việc thi hành Công Ước nhiều khả năng sẽ chỉ diễn ra trong các diễn đàn chính trị – chẳng hạn như Đại Hội về Tội Phạm (Crime Congress) hay Ủy Ban Liên Hiệp Quốc về Phòng Chống Tội Phạm và Tư Pháp Hình Sự – hoặc thông qua các báo cáo tự nguyện từ các quốc gia thành viên. Tuy nhiên, đây đều là những hình thức giám sát yếu, thiếu tính cưỡng hành và không có quyền xét xử độc lập.

Về mặt khắc phục tư pháp, nếu quyền lợi của một cá nhân bị xâm phạm do hậu quả của hợp tác quốc tế dựa trên Công Ước (thí dụ như bị theo dõi bất hợp pháp hoặc bị dẫn độ sai), thì người đó không có cơ chế khiếu nại nào trong khuôn khổ Công Ước này. Mọi sự đòi hỏi công lý hoặc bồi thường đều phải dựa vào luật pháp trong nước của quốc gia liên quan, hoặc các cơ chế nhân quyền khác đã tồn tại từ trước – chứ không thể dựa vào chính Công Ước Tội Phạm Mạng.

Công Ước không hề đưa ra bất kỳ điều khoản nào cho phép cá nhân nạn nhân được quyền khiếu kiện, hay thiết lập một cơ chế độc lập để xét duyệt cách các quốc gia áp dụng các quyền điều tra do Công Ước quy định. Chính vì lẽ đó, một liên minh gồm nhiều tổ chức xã hội dân sự quốc tế đã đồng loạt lên tiếng phản đối, cho rằng Công Ước "đã thất bại trong việc thiết lập cơ chế giám sát tuân thủ các tiêu chuẩn nhân quyền quốc tế," và cảnh báo rằng những công cụ cưỡng hành mạnh mẽ trong Công Ước rất dễ bị lạm dụng nếu không có kiểm soát đầy đủ.

Nguy cơ toàn cầu đối với quyền tự do dân sự và các mối lo ngại từ các bên liên quan:

Các tổ chức xã hội dân sự, chuyên gia pháp lý và các nhà hoạt động nhân quyền cảnh báo rằng Công ước Liên Hợp Quốc về tội phạm mạng không chỉ đe dọa quyền tự do trên mạng tại các chế độ độc tài, mà còn tạo ra mối nguy toàn cầu đối với quyền tự do ngôn luận, quyền riêng tư và quyền được xét xử công bằng.

Bằng cách cho phép dẫn độ và hợp tác xuyên biên giới đối với bất kỳ "tội phạm nghiêm trọng" nào có liên quan đến bằng chứng điện tử—mà không yêu cầu tội danh đó phải có tính chất mạng—Công ước này trao cho các chế độ độc tài quyền truy đuổi những người bất đồng chính kiến và các nhà hoạt động ở nước ngoài. Định nghĩa "tội phạm nghiêm trọng" được hoàn toàn giao cho luật quốc gia quyết định, đồng nghĩa với việc các quốc gia như Việt Nam có thể yêu cầu dẫn độ những người chỉ trích ôn hòa dưới các danh nghĩa mơ hồ như "tuyên truyền chống nhà nước" hoặc "xuyên tạc chính quyền," miễn là hình phạt quy định từ bốn năm tù trở lên.

Kết quả là, Công ước có nguy cơ thiết lập một hệ thống "bàn tay vô hình" của công lý độc tài, trong đó các chính phủ có thể yêu cầu hỗ trợ từ nước ngoài—bao gồm cung cấp dữ liệu, theo dõi, hoặc thậm chí dẫn độ—mà không cần thông qua quy trình pháp lý, không có các biện pháp bảo vệ đầy đủ hay cơ chế rà soát nhân quyền thực thụ. Mối đe dọa này không chỉ giới hạn đối với công dân sống trong các quốc gia độc tài, mà còn mở rộng đến các nhà báo, nhà hoạt động và cư dân mạng trên toàn thế giới.

Công ước không đưa ra bất kỳ quy định rõ ràng nào để bảo vệ quyền tự do biểu đạt kỹ thuật số hoặc danh tính ẩn danh, tạo điều kiện cho các nhà cầm quyền hình sự hóa cả việc sở hữu hoặc lan truyền những nội dung nhạy cảm về chính trị. Ví dụ, chỉ cần có một tài khoản email, chia sẻ một bài viết trên blog, hoặc điều hành một diễn đàn trực tuyến cũng có thể bị diễn giải là hành vi phạm tội liên quan đến mạng theo luật quốc gia, từ đó kích hoạt các cơ chế hợp tác quốc tế. Việc thiếu các biện pháp bảo vệ nhân quyền bắt buộc trong các yêu cầu dẫn độ hoặc giám sát càng làm nguy cơ trầm trọng thêm.

Khác với các điều ước quốc tế về nhân quyền, Công ước về tội phạm mạng không thiết lập một ủy ban giám sát hay cơ chế khiếu nại. Các yêu cầu hợp tác có thể được thực hiện một cách bí mật và tiến hành mà không cần thông báo cho người bị ảnh hưởng hoặc tạo điều kiện cho họ phản bác. Công ước này trao vỏ bọc pháp lý mạnh mẽ cho các hành vi đàn áp mà không có khả năng kháng án hoặc phản biện.

Những lo ngại này đã được Báo cáo viên đặc biệt của Liên Hợp Quốc về quyền tự do ngôn luận, Cao ủy Nhân quyền Liên Hợp Quốc và hơn hai chục tổ chức xã hội dân sự đồng loạt lên tiếng, cảnh báo rằng mặc dù được trình bày như một công cụ chống tội phạm mạng, Công ước này có thể bị các quốc gia lợi dụng để phục vụ cho mục tiêu kiểm soát chính trị và đàn áp ngoài biên giới trong không gian kỹ thuật số.

4. Tác Động Địa Chính Trị và Mức Độ Tương Hợp với Các Chuẩn Mực Quốc Tế

Chính sách an ninh mạng của Việt Nam cũng như việc chuẩn bị tham gia Công Ước Liên Hiệp Quốc về Tội Phạm Mạng đều mang hàm ý địa chính trị sâu sắc, đặc biệt là trong tương quan giữa thực tiễn quốc nội và các chuẩn mực pháp lý quốc tế.

Luật An Ninh Mạng của Việt Nam dưới góc nhìn quốc tế

Khi Việt Nam thông qua Luật An Ninh Mạng vào năm 2018, nhiều chính phủ nước ngoài và các công ty công nghệ lớn đã lập tức bày tỏ quan ngại. Luật này còn được so sánh với mô hình "chủ quyền mạng" (cyber sovereignty) mà Trung Cộng và Nga vốn cổ xúy – tức là khẳng định quyền kiểm soát toàn diện không gian mạng trong phạm vi lãnh thổ, đi kèm với các biện pháp kiểm duyệt và cô lập kỹ thuật số.

Các quy định khắt khe về lưu trữ dữ liệu trong nước và kiểm duyệt nội dung của Việt Nam được nhìn nhận là đang nối gót xu hướng của các quốc gia có khuynh hướng độc tài, muốn siết chặt kiểm soát internet. Cách tiếp cận này đi ngược với các chuẩn mực quốc tế vốn đề cao một môi trường mạng tự do, cởi mở và đa thành phần, trong đó không chỉ chính phủ mà cả xã hội dân sự, doanh nghiệp và giới chuyên môn cùng tham gia quản trị mạng.

Các chính phủ phương Tây – như Hoa Kỳ và Liên Hiệp Âu Châu – cùng với các tổ chức bảo vệ quyền tự do internet đã lên án mạnh mẽ Luật An Ninh Mạng của Việt Nam, xem đây là một bước lùi nghiêm trọng đối với quyền tự do ngôn luận và quyền tiếp cận thông tin. Có ý kiến cho rằng luật này "bị giới dân chủ và giới công nghệ chỉ trích nặng nề" như một văn kiện mang tính áp chế.

Luật này cũng bị cho là xung đột với một số cam kết quốc tế của Việt Nam, đặc biệt là trong các hiệp định thương mại tự do có điều khoản về thương mại kỹ thuật số – thí dụ như chương về thương mại điện tử trong Hiệp định CPTPP, vốn khuyến cáo hạn chế yêu cầu lưu trữ dữ liệu tại chỗ (dù Việt Nam đã đạt được một số ngoại lệ trong đàm phán).

Về mặt địa chính trị, Việt Nam đã tìm cách cân bằng giữa việc hội nhập toàn cầu và duy trì kiểm soát chính trị nội bộ. Tuy nhiên, Luật An Ninh Mạng rõ ràng cho thấy nhà cầm quyền nghiêng về ưu tiên ổn định chế độ hơn là tuân thủ các chuẩn mực dân chủ và tự do.

Dù vậy, Việt Nam vẫn rất nhạy cảm với hình ảnh quốc tế của mình – nhà cầm quyền đã tuyên truyền rằng luật này là cần thiết để bảo vệ "an ninh quốc gia" và tương đồng với thông lệ quốc tế, mặc dù trên thực tế, nhiều điều khoản vượt xa giới hạn mà các quốc gia dân chủ chấp nhận trong lĩnh vực an ninh mạng.

Việc áp đặt yêu cầu đối với các công ty công nghệ nước ngoài – chẳng hạn phải đặt văn phòng đại diện và máy chủ trong nước – khiến chính sách này càng giống với mô hình kiểm soát của Trung Cộng, và đồng thời tạo tiền lệ nguy hiểm cho khu vực Đông Nam Á trong việc thiết lập cái gọi là "chủ quyền kỹ thuật số."

Hệ quả là, nhiều quốc gia ASEAN khác đã quan sát kỹ lưỡng cách Việt Nam áp dụng luật này, và có quốc gia đã bắt đầu mô phỏng hoặc xây dựng các đạo luật tương tự, qua đó hạ thấp tiêu chuẩn nhân quyền trong quá trình hình thành các chuẩn mực khu vực về không gian mạng.

Công Ước Tội Phạm Mạng của Liên Hiệp Quốc và Chuẩn Mực Toàn Cầu

Quá trình hình thành Công Ước về Tội Phạm Mạng của Liên Hiệp Quốc chính là một câu chuyện về sự tranh giành ảnh hưởng địa chính trị trong lĩnh vực luật pháp quốc tế. Suốt nhiều năm, Công Ước Budapest năm 2001 của Hội Đồng Âu Châu là văn kiện quốc tế chủ đạo về chống tội phạm mạng. Tuy nhiên, các cường quốc như Nga, Trung Cộng và cả Việt Nam đều từ chối gia nhập, với lý do rằng công ước này mang tính "Âu-Mỹ" và không phản ánh đầy đủ quan điểm của các quốc gia đang phát triển hay ngoài phương Tây.

Năm 2019, với sự hậu thuẫn mạnh mẽ từ Nga (và được Việt Nam cùng nhiều nước khác ủng hộ qua lá phiếu), Đại Hội Đồng Liên Hiệp Quốc đã thông qua nghị quyết khởi động đàm phán một công ước mới về tội phạm mạng – ngầm tạo ra một "phương án thay thế" cho khung pháp lý của Budapest.

Văn kiện được thông qua năm 2024 là kết quả của một cuộc thỏa hiệp khó khăn giữa hai tầm nhìn đối nghịch:

- Khối phương Tây cố gắng giới hạn nội dung công ước vào những tội phạm thuần túy về công nghệ (cyber-dependent crimes) và kèm theo các biện pháp bảo vệ nhân quyền.
- Trong khi đó, phe Nga – Trung và các quốc gia đồng minh lại thúc đẩy mở rộng phạm vi công ước sang các hành vi liên quan đến nội dung, đồng thời khẳng định mạnh mẽ chủ quyền nhà nước trong không gian mạng.

Công Ước sau cùng đã loại bỏ một số đề xuất gây tranh cãi nhất – chẳng hạn như ngôn ngữ do Nga đưa ra trước đây nhằm hình sự hóa hành vi "cực đoan" trên mạng với định nghĩa mơ hồ. Tuy nhiên, văn kiện này vẫn vượt quá các chuẩn mực quốc tế hiện hành trên nhiều phương diện: nó hợp pháp hóa mức độ giám sát xuyên quốc gia và hợp tác cưỡng chế giữa các chính phủ ở quy mô chưa từng có, áp dụng cho một loạt các loại tội phạm, không chỉ riêng tội phạm mạng.

Theo một phân tích chung của nhiều tổ chức xã hội dân sự, những cơ chế này "rất dễ bị các chính quyền lợi dụng để đàn áp những tiếng nói bất đồng chính kiến." Bằng cách cho phép hợp tác quốc tế về bất kỳ tội phạm nghiêm trọng nào – theo định nghĩa riêng của từng quốc gia – hiệp ước này tạo ra nguy cơ liên kết các cơ quan cưỡng chế quốc tế chống lại các hành vi mà một nước xem là tội phạm nhưng nước khác lại không (chẳng hạn như các hành vi liên quan đến tự do ngôn luận hay phản biện chính trị).

Điều này dẫn đến khả năng xung đột trực tiếp với các nguyên tắc nhân quyền quốc tế: nếu một quốc gia xem chỉ trích nhà cầm quyền là "tội phạm mạng nghiêm trọng" và một quốc gia khác, do bị ràng buộc bởi Công Ước, chấp thuận điều tra hay dẫn độ nghi can về nước để truy tố, thì hậu quả là phá vỡ truyền thống bảo vệ người bị truy tố chính trị (vốn từ lâu được coi là lý do chính đáng để từ chối dẫn độ trong luật quốc tế).

Cao Ủy Nhân Quyền Liên Hiệp Quốc cùng với các Báo Cáo Viên đặc biệt đã công khai cảnh báo rằng phạm vi quá rộng và thiếu các biện pháp bảo đảm của Công Ước có thể mở đường cho việc đàn áp các nhà báo và các nhà hoạt động xã hội.

Tóm lại, dù Công Ước này được xây dựng với mục tiêu thiết lập một khuôn khổ chuẩn mực toàn cầu trong cuộc chiến chống tội phạm mạng, nhưng trên thực tế, nó có nguy cơ đẩy các chuẩn mực quốc tế đi lệch hướng – theo chiều hướng củng cố quyền lực giám sát của nhà nước, mà không đi kèm với những cam kết tương xứng về bảo vệ các quyền tự do căn bản và nhân phẩm.

Việt Nam: Hòa Hợp Hay Dị Hướng Với Chuẩn Mực Quốc Tế?

Việt Nam hiện đang tự định vị mình như một nước ủng hộ tích cực Công Ước Liên Hiệp Quốc về Tội Phạm Mạng – thậm chí đã tình nguyện đăng cai lễ ký kết chính thức dự kiến diễn ra vào tháng 10 năm 2025 tại Hà Nội. Đây là một động thái mang ý nghĩa ngoại giao đáng kể: nó cho thấy tham vọng của Hà Nội muốn được nhìn nhận như một quốc gia dẫn đầu trong lĩnh vực quản trị không gian mạng toàn cầu, thể hiện sự hòa nhập vào "đồng thuận quốc tế" (Công Ước đã được toàn thể ủy ban của LHQ thông qua), đồng thời xoa dịu phần nào các chỉ trích trước đây bằng cách thể hiện thái độ cởi mở hơn với hợp tác đa phương.

Bề ngoài, có thể thấy sự hòa hợp nhất định: ưu tiên của Việt Nam trong việc trấn áp các tội phạm mạng và "thành phần xấu" trên không gian mạng dường như trùng hợp với mục tiêu của Công Ước là tăng cường hợp tác quốc tế chống lại tội phạm mạng.

Tuy nhiên, ẩn bên dưới là những mâu thuẫn sâu sắc với các chuẩn mực tự do của thế giới dân chủ. Việt Nam định nghĩa rất rộng về "đe dọa an ninh mạng", bao gồm cả những hình thức phát biểu ôn hòa có tính chính trị, điều này đi ngược lại nguyên tắc – tuy chỉ mang tính hình thức trong Công Ước nhưng lại là nền tảng lâu đời trong luật nhân quyền quốc tế – rằng biểu đạt tư tưởng trên mạng cần được bảo vệ.

Theo đúng tinh thần Điều 6.2 của Công Ước, Việt Nam sẽ không được phép sử dụng các công cụ do hiệp ước này tạo ra để đàn áp giới bất đồng chính kiến. Nhưng trên thực tế, Việt Nam có thể sẽ viện dẫn điều khoản "tôn trọng luật pháp quốc gia" trong Công Ước để quốc tế hóa nỗ lực trấn áp những người chỉ trích chế độ.

Thí dụ: nếu một nhà hoạt động lưu vong bị cáo buộc "tuyên truyền chống Nhà nước" qua mạng – một hành vi có thể bị kết án hơn 4 năm tù theo Bộ Luật Hình Sự Việt Nam (đáp ứng điều kiện "tội nghiêm trọng" trong Công Ước) – thì Hà Nội có thể sử dụng Công Ước này để yêu cầu quốc gia nơi người đó cư trú hợp tác trong việc thu thập dữ liệu, thậm chí dẫn độ. Những yêu cầu như vậy, nếu thiếu một công cụ pháp lý quốc tế, thường sẽ bị xem là nhạy cảm về chính trị và khó được chấp thuận. Nhưng dưới danh nghĩa Công Ước của Liên Hiệp Quốc, các yêu cầu ấy sẽ được ngụy trang bằng tính chính danh pháp lý quốc tế, khiến việc từ chối trở nên khó xử hơn về mặt ngoại giao.

Tình huống như vậy sẽ đặt ra phép thử thực tế cho các quốc gia phương Tây: họ có thể viện lý do "tội phạm chính trị" để từ chối dẫn độ hay hợp tác, nhưng việc đã đặt bút ký vào một hiệp ước không cấm rõ ràng những hành vi lạm dụng như vậy sẽ khiến họ rơi vào thế tiến thoái lưỡng nan về mặt ngoại giao và pháp lý.

Ở một khía cạnh khác, việc Việt Nam tham gia vào tiến trình thương thảo Công Ước của Liên Hiệp Quốc cũng đồng nghĩa với việc nhà cầm quyền Hà Nội buộc phải công khai thừa nhận các chuẩn mực quốc tế. Nhiều quan chức Việt Nam đã tuyên truyền về các nỗ lực hoàn thiện luật an ninh mạng trong nước và khẳng định rằng Việt Nam đang "tăng cường hợp tác quốc tế" phù hợp với xu thế toàn cầu.

Trong phạm vi khu vực, động thái của Việt Nam có thể khuyến khích các quốc gia láng giềng cùng gia nhập Công Ước (thay vì chọn Công Ước Budapest của Âu Châu) và ban hành các đạo luật tương tự. Hệ quả có thể là tăng cường năng lực chống tội phạm mạng thực sự, hoặc gây ra hiệu ứng lan tỏa tiêu chuẩn, làm hợp thức hóa mô hình luật an ninh mạng mang tính áp chế – điều mà nhiều tổ chức nhân quyền đang lo ngại.

Trên thực tế, sự tồn tại của Công Ước có thể được Việt Nam sử dụng để biện minh cho luật an ninh mạng của mình. Hà Nội có thể lập luận rằng: các yêu cầu về lưu trữ dữ liệu trong nước hay buộc gỡ bỏ nội dung "xấu độc" là quyền chủ quyền chính đáng, phù hợp với tinh thần hợp tác mà cộng đồng quốc tế đang thúc đẩy qua hiệp ước này.

Nói cách khác, Việt Nam lật ngược thế cờ trước những lời chỉ trích trước đây, bằng cách tuyên bố:

"Chúng tôi đang dẫn đầu nỗ lực quốc tế chống tội phạm mạng – bằng chứng là Việt Nam là nước đăng cai lễ ký kết Công Ước – cho nên luật trong nước của chúng tôi cũng là một phần của nỗ lực đó."

Về mặt địa chính trị, Việt Nam đang đứng giữa hai bờ: một mặt hợp tác với Liên Hiệp Quốc (cũng là đối tác của các nước phương Tây), mặt khác vẫn duy trì mô hình kiểm soát không gian mạng mang đậm dấu ấn của các chế độ độc tài.

Việc hai hệ thống luật này sẽ hội tụ hay xung đột trong thực tế còn tùy thuộc vào quá trình thực thi. Nếu nhiều quốc gia phê chuẩn Công Ước này, thì các điều khoản mơ hồ và rộng rãi trong đó có thể hợp thức hóa một phần các chính sách của Việt Nam ở cấp độ toàn cầu. Ngược lại, việc hội nhập quốc tế sâu hơn có thể tạo áp lực buộc Hà Nội phải thu hẹp định nghĩa về "tội phạm mạng", loại trừ các hình thức phát biểu chính trị thuần túy. Tuy nhiên, vào thời điểm hiện tại, lập trường và chính sách của Việt Nam vẫn còn xung khắc với các chuẩn mực tự do quốc tế về quyền kỹ thuật số, dù về hình thức đã có sự "hội nhập" vào các xu hướng mới về hợp tác an ninh toàn cầu – vốn ngày càng thiên về tăng cường quyền lực cho nhà cầm quyền và mở rộng quyền truy xét xuyên quốc gia.

5. Phản Ứng Từ Giới Quan Sát Quốc Tế và Giới Chuyên Gia

Cả Luật An Ninh Mạng của Việt Nam lẫn Công Ước Tội Phạm Mạng của Liên Hiệp Quốc đều đã gây ra những phản ứng mạnh mẽ từ nhiều giới quan tâm – bao gồm các tổ chức nhân quyền, các nhóm bảo vệ quyền tự do kỹ thuật số, giới học giả, chính phủ các nước dân chủ, cũng như các công ty công nghệ lớn.

Phản Ứng Đối Với Luật An Ninh Mạng Của Việt Nam

Phản Ứng Trong Nước và Khu Vực:

Tại Việt Nam, do môi trường chính trị bị kiểm soát nghiêm ngặt, nên ít có sự phản đối công khai đối với đạo luật này. Tuy nhiên, nhiều nhà hoạt động và một số hiệp hội doanh nghiệp đã kín đáo bày tỏ lo ngại về ảnh hưởng của luật đối với quyền tự do công dân và sự phát triển của kinh tế số. Dù vậy, Quốc Hội bù nhìn Việt Nam vẫn thông qua đạo luật này với tỉ lệ áp đảo.

Tại Đông Nam Á, các nước láng giềng theo dõi sát động thái của Việt Nam. Một số chính phủ có khuynh hướng độc tài đã tán dương lập trường cứng rắn của Hà Nội trong việc kiểm soát thông tin mạng, trong khi các nước như Indonesia và Malaysia, đang trong quá trình thảo luận các dự luật tương tự, đã tham khảo mô hình của Việt Nam vừa để áp dụng, vừa để rút kinh nghiệm.

Phản Ứng Của Các Tổ Chức Nhân Quyền Quốc Tế:

Các tổ chức nhân quyền quốc tế đồng loạt lên án đạo luật này như một công cụ đàn áp toàn diện dưới danh nghĩa "an ninh mạng".

Tổ chức Human Rights Watch (HRW) gọi dự luật này là "mơ hồ và bao quát một cách nguy hiểm", đồng thời cảnh báo rằng "mục tiêu thật sự dường như là bảo vệ độc quyền quyền lực của Đảng Cộng Sản không kém gì bảo vệ hệ thống mạng." HRW nhấn mạnh rằng luật này "trực tiếp nhắm vào quyền tự do biểu đạt và tiếp cận thông tin", đồng thời trao cho nhà cầm quyền "thêm một vũ khí… để đàn áp các tiếng nói đối lập." Tổ chức này cũng chỉ rõ rằng việc hình sự hóa hành vi "tuyên truyền chống Nhà nước" và buộc các công ty công nghệ cung cấp dữ liệu người dùng đã vi phạm quyền riêng tư và trái với các cam kết quốc tế của Việt Nam, trong đó có Công Ước Quốc Tế về Các Quyền Dân Sự và Chính Trị (ICCPR) mà Việt Nam là thành viên.

Ân Xá Quốc Tế (Amnesty International) lập luận rằng các điều khoản của luật — đặc biệt là yêu cầu lưu trữ dữ liệu trong nước và buộc gỡ bỏ nội dung — đã góp phần hình thành một nhà nước giám sát hà khắc. Tổ chức này kêu gọi các công ty công nghệ không nên tuân thủ những quy định đàn áp như vậy. Tuy nhiên, trên thực tế, các tập đoàn như Facebook và Google tuy ban đầu có chống đối các yêu sách của phía Việt Nam, nhưng theo thời gian đã dần chấp thuận nhiều yêu cầu kiểm duyệt nội dung từ phía nhà cầm quyền. Ân Xá Quốc Tế lên án diễn biến này, cảnh báo rằng các công ty tư nhân đang bị biến thành công cụ tiếp tay cho bộ máy kiểm duyệt của nhà cầm quyền độc tài.

Quyền Kỹ Thuật Số và Giới Học Thuật:

Các tổ chức tranh đấu cho quyền kỹ thuật số như Access Now và ARTICLE 19 đã chỉ rõ rằng Luật An Ninh Mạng của Việt Nam là một điển hình cho việc luật an ninh mạng hay phòng chống tội phạm mạng có thể bị lạm dụng để chà đạp quyền con người. Trong một bản phân tích, ARTICLE 19 nhận định rằng các định nghĩa trong luật này — chẳng hạn như "gián điệp mạng" — được diễn giải quá rộng, đến mức có thể hình sự hóa những hành vi rất thông thường như sử dụng VPN để truy cập thông tin.

Nhiều học giả đăng bài trên các tạp chí chuyên ngành đã ghi nhận rằng việc viện dẫn "an ninh quốc gia" trong luật này phản ánh đúng mô hình kiểm soát internet theo kiểu Trung Cộng và Nga, nghĩa là đặt không gian mạng hoàn toàn dưới quyền kiểm soát của nhà nước, đi ngược lại mô hình internet mở và đa nguyên của cộng đồng quốc tế.

Một số học giả pháp lý trong khu vực cũng bày tỏ lo ngại rằng cách tiếp cận này của Việt Nam có thể khiến nền kinh tế số của quốc gia bị cô lập. Với các quy định ép buộc dữ liệu phải được lưu trữ trong lãnh thổ Việt Nam và đe dọa chặn các dịch vụ không tuân thủ, luật này có thể làm nản lòng các nhà đầu tư nước ngoài, và thậm chí đẩy Việt Nam đến tình trạng "mạng riêng biệt" — tức tách rời khỏi hệ thống internet toàn cầu ("splinternet").

Trong khi đó, những người cổ súy cho tự do ngôn luận cảnh báo về tác động tiêu cực của luật đối với diễn đàn xã hội trực tuyến tại Việt Nam, vốn là một trong những nơi hiếm hoi người dân có thể chia sẻ thông tin độc lập và quan điểm chính trị. Từ khi luật có hiệu lực, nhiều blogger và công dân mạng đã bị bắt giữ, bị truy tố và kết án với những điều khoản phù hợp với luật này.

Bộ Ngoại Giao Hoa Kỳ và các viên chức Liên Âu đều đã công khai chỉ trích luật, ngay khi nó được Quốc Hội CSVN thông qua. Đại Sứ Quán Hoa Kỳ tại Hà Nội khi đó đã bày tỏ "thất vọng sâu sắc" và cảnh báo rằng các điều khoản như ép buộc lưu trữ dữ liệu trong nước có thể cản trở nghiêm trọng các mục tiêu về an ninh mạng và đổi mới kỹ thuật số của Việt Nam — một cách nói ngoại giao cho thấy cả lo ngại về thương mại lẫn chiến lược an ninh.

Tóm lại, phản ứng chủ đạo từ cộng đồng quốc tế đối với Luật An Ninh Mạng của Việt Nam là xem đây như một công cụ đàn áp và đi ngược lại các chuẩn mực nhân quyền toàn cầu, và có nguy cơ trở thành một hình mẫu nguy hiểm để các chế độ độc tài khác noi theo.

Phản Ứng Đối Với Công Ước Tội Phạm Mạng Của Liên Hiệp Quốc

Liên minh phản biện rộng khắp:

Khác với thông lệ của phần lớn các hiệp ước quốc tế do Liên Hiệp Quốc ban hành, Công Ước Tội Phạm Mạng này đã gặp phải làn sóng phản đối mạnh mẽ ngay cả sau khi được thông qua. Một liên minh đa dạng bao gồm các tổ chức nhân quyền, cơ quan bảo vệ tự do truyền thông, giới chức LHQ về nhân quyền, hiệp hội kỹ nghệ công nghệ, và các nhà nghiên cứu an ninh mạng đều lên tiếng cảnh báo về những hệ lụy nguy hiểm của văn kiện này.

Trong giai đoạn trước khi Đại Hội Đồng LHQ biểu quyết, 29 tổ chức và chuyên gia — trong đó có Human Rights Watch, Electronic Frontier Foundation (EFF), Access Now và nhiều đơn vị khác — đã cùng ký một bức thư ngỏ kêu gọi các quốc gia, đặc biệt là các nước dân chủ trong khối Liên Âu, hãy bỏ phiếu "phản đối" Công Ước.

Lá thư này cảnh báo rằng Công Ước "sẽ làm suy yếu nền dân chủ, quyền con người và pháp quyền, đồng thời đe dọa sự an toàn và quyền riêng tư của người sử dụng internet trên toàn thế giới." Các mối quan ngại chính bao gồm:

- Phạm vi điều chỉnh tội phạm quá rộng;
- Các biện pháp giám sát cực kỳ mạnh mẽ, nhưng thiếu vắng cơ chế kiểm soát độc lập và hiệu quả.

Một điểm đặc biệt bị chỉ trích là Điều 35 của Công Ước — yêu cầu các quốc gia thành viên phải chia sẻ dữ liệu và hợp tác điều tra đối với bất kỳ "tội phạm nghiêm trọng" nào, miễn là tội danh đó có mức án từ 4 năm tù trở lên theo luật của nước yêu cầu. Điều này tạo ra kẽ hở lớn để các nhà cầm quyền lạm dụng, dùng Công Ước như công cụ để đàn áp tiếng nói bất đồng, chỉ cần hình sự hóa hành vi ấy trong luật nội địa của mình.

Electronic Frontier Foundation (EFF) đã gọi bản dự thảo này là "một tấm ngân phiếu trắng cho lạm quyền giám sát", và ví von Công Ước như một "hiệp ước hợp pháp hóa gián điệp xuyên quốc gia". Tạp chí Scientific American, trong một bài viết có tiêu đề "Hiệp Ước Tội Phạm Mạng Mới Của LHQ Có Thể Đe Dọa Quyền Con Người", cũng cảnh báo rằng Công Ước có thể được áp dụng cho hầu như mọi loại tội phạm hiện nay, vì gần như mọi hành vi đều có yếu tố công nghệ, từ đó mở đường cho sự toàn cầu hóa quyền lực điều tra mà không đi kèm kiểm soát mạnh mẽ.

Ngay cả Báo cáo viên Đặc biệt của LHQ về Tự do Ngôn luận và Cao Ủy Nhân Quyền LHQ cũng đã can thiệp trong quá trình đàm phán, kêu gọi siết chặt các biện pháp bảo vệ quyền con người và bày tỏ quan ngại sâu sắc trước các điều khoản mơ hồ về các khái niệm như "khủng bố" hay "cực đoan", vì chúng có thể dễ dàng bị lợi dụng để bóp nghẹt quyền tự do biểu đạt. Mặc dù một số điều khoản mơ hồ nhất đã bị loại bỏ khỏi bản cuối cùng, nhiều chuyên gia nhân quyền vẫn cho rằng văn kiện này còn lâu mới đạt chuẩn mực nhân quyền, và tiềm ẩn nguy cơ bị các chế độ độc tài khai thác để củng cố đàn áp trong nước dưới danh nghĩa hợp tác quốc tế.

Quan Điểm Của Các Bên Ủng Hộ:

Ở chiều ngược lại, Công Ước Tội Phạm Mạng của Liên Hiệp Quốc đã nhận được sự ủng hộ mạnh mẽ từ nhiều chính phủ, và đã được Ủy Ban Soạn Thảo thông qua với sự nhất trí tuyệt đối. Những quốc gia như Nga, Trung Cộng, cùng với nhiều nước đang phát triển, hoan nghênh văn kiện này như một "bước ngoặt lịch sử" và là "hiệp ước chống tội phạm đa phương đầu tiên trong hơn hai thập niên." Họ nhấn mạnh đến lợi ích từ việc hợp tác toàn cầu để đối phó với tội phạm mạng, một hiện tượng có tính chất xuyên quốc gia, vượt ngoài khả năng kiểm soát của từng quốc gia riêng lẻ.

Các quốc gia ủng hộ cho rằng Công Ước đã giải quyết một số vấn nạn nghiêm trọng như khai thác tình dục trẻ em trên mạng, lừa đảo tài chính, và các cuộc tấn công mạng quy mô lớn. Ngoài ra, Công Ước còn bao gồm các điều khoản về hỗ trợ kỹ thuật và nâng cao năng lực, điều mà các nước nghèo hơn kỳ vọng sẽ giúp họ củng cố hệ thống phòng thủ mạng của mình.

Việt Nam, chẳng hạn, đã khẳng định sự ủng hộ của mình trên lập trường rằng đây là cơ hội để thể hiện vai trò là đối tác quốc tế tích cực, đồng thời cải thiện khung pháp luật nội địa sao cho tiệm cận với chuẩn mực toàn cầu. Một số chuyên gia pháp lý từ các nước ủng hộ Công Ước cho rằng những chỉ trích là phóng đại, và Công Ước thực chất chỉ cung cấp công cụ pháp lý, còn việc sử dụng ra sao hoàn toàn phụ thuộc vào thiện chí chính trị của từng chính phủ. Họ cũng chỉ ra rằng, ngôn ngữ về quyền con người đã được lồng vào Công Ước (Điều 6.2 và Điều 24) — điều không hề được bảo đảm từ đầu — là kết quả của sự thương lượng.

Giới công lực và cơ quan thực thi pháp luật quốc tế nhìn chung đánh giá Công Ước theo hướng tích cực, đặc biệt nhấn mạnh rằng văn kiện này sẽ giúp đơn giản hóa các thủ tục hợp tác điều tra xuyên biên giới, vốn từ lâu đã gặp bế tắc do thiếu một khuôn khổ chung (nhất là với các quốc gia không ký Công Ước Budapest). Các viên chức thuộc Interpol và Văn phòng Liên Hiệp Quốc về Ma Túy và Tội Phạm (UNODC) cũng đã lên tiếng cho rằng Công Ước lấp đầy khoảng trống pháp lý hiện tại và cẩn trọng nhấn mạnh rằng quyền con người cần được tôn trọng trong quá trình thi hành. Tuy vậy, những trấn an này vẫn chưa đủ sức xoa dịu làn sóng chỉ trích.

Giới Học Giả Luật Pháp và Các Phân Tích Chuyên Môn:

Nhiều nhà phân tích luật pháp trên các diễn đàn chuyên ngành như Just Security và Lawfare đã cẩn trọng mổ xẻ văn kiện Công Ước và đa phần đồng thuận với các mối lo ngại mà xã hội dân sự đã nêu ra. Trong một bài phân tích tháng 8 năm 2024, luật gia Katitza Rodriguez của tổ chức Electronic Frontier Foundation (EFF) nhận định rằng những điều khoản bảo vệ nhân quyền trong Công Ước "rất chung chung, và ở các điểm then chốt lại phó mặc cho luật nội địa – vốn thường thiếu chuẩn mực", đặc biệt là khi không có cơ chế giám sát hay bắt buộc tuân thủ theo các công ước nhân quyền quốc tế. Bà cảnh báo rằng "các công cụ hợp tác toàn cầu" mà Công Ước thiết lập rất dễ bị lạm dụng.

Một nhà bình luận khác, Eli Scher-Zagier, viết trên Lawfare đã nhấn mạnh mức độ bao trùm quyền tài phán của Công Ước. Ông chỉ rõ rằng văn kiện này "hợp thức hóa việc các quốc gia đem luật hình sự nội địa áp dụng ra nước ngoài, rồi dựa vào đó truy lùng công dân nước khác đang sống ở hải ngoại" – một tiền lệ đặc biệt nguy hiểm đối với những người lưu vong, ký giả độc lập, và giới hoạt động sống ngoài nước. Bài viết cảnh báo rằng việc Công Ước thừa nhận nguyên tắc "thụ động chủ thể" (passive personality jurisdiction) sẽ dẫn tới "quyền truy tố gần như vô hạn của các nhà nước độc tài", nếu không được kềm chế.

Ở một góc nhìn tích cực hơn, một số học giả công nhận rằng việc có một công ước toàn cầu dưới khuôn khổ Liên Hiệp Quốc có thể giúp các quốc gia phối hợp hiệu quả hơn trong việc đối phó với các mối đe dọa nghiêm trọng thực sự, chẳng hạn như ransomware hay lừa đảo xuyên quốc gia – những loại tội phạm không nước nào có thể xử lý một mình. Tuy nhiên, ngay cả những ý kiến ôn hoà này cũng thường kết luận rằng nếu không có các cơ chế bảo vệ quyền riêng tư vững chắc, thì Công Ước có thể gây hại nhiều ngang bằng với lợi ích mà nó mang lại.

Giới kỹ nghệ công nghệ – bao gồm các tập đoàn lớn và hiệp hội – cũng đã lên tiếng công khai. Các công ty như Apple, Google và Meta, thông qua các nhóm vận động, đã yêu cầu làm rõ các điều khoản bảo vệ dữ liệu cá nhân, đồng thời bày tỏ lo ngại rằng việc mỗi quốc gia diễn giải và áp dụng Công Ước theo cách riêng sẽ khiến họ bị buộc phải tuân theo các yêu sách dữ liệu mang tính đàn áp của một số chính quyền.

Tính đến giữa năm 2025, nhiều công ty đang đánh giá lại cách tổ chức hoạt động toàn cầu của họ nếu Công Ước chính thức có hiệu lực, và một số có thể chọn giải pháp giảm lưu trữ dữ liệu người dùng hoặc gia tăng sử dụng mã hóa, nhằm hạn chế nguy cơ bị ép giao nộp thông tin.

Tóm lược:

Phản ứng đối với Công Ước Tội Phạm Mạng của Liên Hiệp Quốc đã cho thấy sự chia rẽ sâu sắc trên trường quốc tế. Một liên minh hiếm hoi giữa các tổ chức nhân quyền, giới kỹ nghệ công nghệ, các chuyên gia độc lập và thậm chí một số chính phủ dân chủ đều bày tỏ lo ngại rằng Công Ước sẽ bị lợi dụng để hợp thức hóa các hoạt động giám sát và đàn áp tiếng nói bất đồng, vượt ra ngoài biên giới quốc gia.

Việt Nam – với sự ủng hộ sốt sắng – đã trở thành ví dụ điển hình trong mắt các nhà phê bình, rằng đây là một quốc gia có thể tận dụng các công cụ do Công Ước cung cấp để mở rộng nghị trình kiểm soát không gian mạng theo chiều hướng độc đoán. Trái lại, phía Hà Nội lại trình bày sự tham gia của mình như là bằng chứng cho thấy Việt Nam là "một thành viên có trách nhiệm" trong cộng đồng quốc tế về quản trị mạng.

Những năm sắp tới – khi Công Ước được chính thức ký kết và phê chuẩn (cần 40 quốc gia để có hiệu lực) – sẽ là giai đoạn quyết định để xem các mối lo ngại có trở thành hiện thực hay không. Đồng thời, nhiều chuyên gia cũng đã kêu gọi bổ sung thêm các nghị định thư tùy chọn về nhân quyền, nhằm điều chỉnh và bảo đảm rằng khung pháp lý toàn cầu này không trở thành công cụ đàn áp, mà thực sự phục vụ cho công lý và tự do trong kỷ nguyên kỹ thuật số.

6. Diễn Biến Gần Đây và Viễn Ảnh Sắp Tới

Tiến Trình Đàm Phán Công Ước tại Liên Hiệp Quốc (2024–2025)

Công Ước Liên Hiệp Quốc về Tội Phạm Mạng đã được Đại Hội Đồng LHQ chính thức thông qua vào ngày 24 tháng 12 năm 2024, theo Nghị Quyết số 79/243. Văn kiện sau cùng gồm chín chương, đề cập đến các nội dung như hình sự hóa hành vi phạm pháp trên mạng, biện pháp phòng ngừa, thủ tục điều tra, hợp tác quốc tế, hỗ trợ kỹ thuật và cơ chế thi hành.

Đầu năm 2025, Việt Nam đã chủ động có những bước đi nổi bật để chuẩn bị cho việc ký kết: Tại kỳ họp tháng 5 năm 2025 của Ủy Ban Phòng, Chống Tội Phạm thuộc Liên Hiệp Quốc tại Vienna, phái đoàn Việt Nam đã công bố sẽ nhận trách nhiệm tổ chức lễ ký kết chính thức vào các ngày 25–26 tháng 10 năm 2025 tại Hà Nội.

Việt Nam đã gửi thư mời đến nguyên thủ quốc gia của tất cả các nước thành viên Liên Hiệp Quốc, cho thấy tầm quan trọng chính trị đặc biệt mà Hà Nội dành cho sự kiện này. Buổi lễ – được đặt tên là "Lộ Trình Tiến Về Hà Nội" (The Road to Hanoi) – sẽ do Chủ Tịch Nước Việt Nam và Tổng Thư Ký Liên Hiệp Quốc đồng chủ tọa, phối hợp tổ chức cùng với Văn Phòng Ma Túy và Tội Phạm LHQ (UNODC). Việc tổ chức như vậy đã nâng vị thế của Việt Nam lên hàng nước chủ chốt trong quá trình vận động cho Công Ước.

Sau tháng 10 năm 2025, Công Ước sẽ tiếp tục mở rộng cho các quốc gia ký kết tại trụ sở LHQ ở New York cho đến hết năm 2026. Tính đến giữa năm 2025, nhiều quốc gia đang tiến hành xét duyệt nội bộ để quyết định có tham gia hay không; phần lớn được dự đoán sẽ ký tại Hà Nội, tuy nhiên một số quốc gia châu Âu và các nền dân chủ khác vẫn đang cân nhắc các mối quan ngại đã nêu.

Tại Liên Âu, các cuộc thảo luận đang diễn ra về việc ban hành các tuyên bố diễn giải hoặc bảo lưu khi ký, nhằm làm rõ cách thức các quốc gia thành viên sẽ thi hành Công Ước phù hợp với các cam kết về nhân quyền. Ngoài ra, một nghị định thư bổ sung (supplementary protocol) cũng đang được cân nhắc – như đã được đề cập trong thư ngỏ của các tổ chức xã hội dân sự – với khả năng sẽ bổ sung thêm các tội danh trong tương lai, cho thấy Công Ước được xem là một văn kiện "sống", có thể mở rộng. Chính yếu tố này là một trong các lý do khiến giới quan sát kêu gọi sự thận trọng cao độ.

Chính sách An ninh mạng trong nước của Việt Nam (2019–2025)

Kể từ khi Luật An ninh mạng chính thức có hiệu lực vào đầu năm 2019, nhà cầm quyền Cộng sản Việt Nam đã không ngừng siết chặt việc thi hành và đồng thời mở rộng các quy định liên quan. Một bước phát triển đáng chú ý là Nghị định 53 ban hành năm 2022, như đã đề cập trước đó, nhằm hiện thực hóa việc lưu trữ dữ liệu tại chỗ (data localization), với thời hạn chót là tháng 10 năm 2022. Đến năm 2023, nhiều bản tin cho biết các công ty công nghệ lớn của nước ngoài đã bắt đầu có những bước đi nhằm "tuân thủ từng phần". Chẳng hạn, Apple được cho là đã đồng ý lưu trữ dữ liệu iCloud của người dùng Việt Nam trên các máy chủ đặt tại Việt Nam thông qua một nhà cung cấp dịch vụ điện toán đám mây trong nước; trong khi đó, Google và Meta (Facebook) đã tăng cường hợp tác trong việc xử lý các yêu cầu gỡ bỏ nội dung, dù vẫn tuyên bố rằng họ chỉ hành động đối với các nội dung vi phạm chính sách nội bộ hoặc luật pháp Việt Nam.

Về phía nhà cầm quyền, họ không hề che giấu việc tận dụng triệt để Luật An ninh mạng như một công cụ áp chế: vào năm 2020, Facebook từng bị đe dọa sẽ bị chặn truy cập tại Việt Nam nếu không kiểm duyệt thêm các bài viết chống nhà cầm quyền – một yêu sách được hậu thuẫn bằng "cơ sở pháp lý" từ Luật mới ban hành. Trước áp lực này, Facebook đã nhượng bộ và gia tăng đáng kể việc hạn chế nội dung tại Việt Nam, theo các báo cáo minh bạch. Tổ chức Ân xá Quốc tế (Amnesty International) đã lên tiếng phản đối sự nhượng bộ này, cho rằng Facebook đã "đồng lõa với chế độ kiểm duyệt".

Cùng lúc, Việt Nam ban hành Nghị định Bảo vệ Dữ liệu Cá nhân (2023), được xem là phần bổ sung cho Luật An ninh mạng, nhằm kiểm soát chặt chẽ hơn việc thu thập, xử lý dữ liệu cá nhân – trong đó có điều khoản gây tranh cãi là cấm sử dụng tên giả hay ẩn danh trong một số tương tác trực tuyến, về thực chất là củng cố thêm chính sách "tên thật" vốn đã được nêu trong Luật An ninh mạng.

Việc cưỡng chế cũng ngày càng khốc liệt hơn: từ năm 2019 đến 2023, hàng chục blogger, người dùng Facebook và Youtuber đã bị bắt giam, truy tố và kết án với các tội danh liên quan đến "an ninh quốc gia" hoặc "tuyên truyền chống phá nhà nước", dựa trên các phát biểu hoặc nội dung đăng tải trên mạng. Luật An ninh mạng đóng vai trò là cơ sở pháp lý để tiến hành giám sát, thu thập chứng cứ và truy cứu trách nhiệm hình sự đối với các cá nhân này.

Đến tháng 4 năm 2023, báo chí nhà nước Việt Nam loan tin rằng mức độ hợp tác giữa các nền tảng công nghệ nước ngoài và nhà cầm quyền đã "được cải thiện rõ rệt", dẫn chứng hàng ngàn video và trang mạng bị gỡ bỏ theo yêu cầu – điều mà giới chức gọi là thành tựu của chính sách an ninh mạng trong việc "làm sạch" không gian mạng. Tuy nhiên, các bản phúc trình "Tự do Internet" của tổ chức Freedom House vẫn tiếp tục xếp hạng Việt Nam là quốc gia "Không Tự Do", với lý do chính là những vi phạm quyền tự do ngôn luận được thể chế hóa qua Luật An ninh mạng 2018.

Triển Vọng Tương Lai

Trong thời gian tới, mối tương tác giữa luật pháp quốc gia của Việt Nam và Công Ước quốc tế về tội phạm mạng sẽ là một diễn biến quan trọng cần theo dõi chặt chẽ. Rất có khả năng nhà cầm quyền Hà Nội sẽ nhanh chóng phê chuẩn Công Ước này ngay sau lễ ký kết, trở thành một trong những quốc gia đầu tiên gia nhập. Sau đó, các cơ quan công an và an ninh của Việt Nam có thể bắt đầu sử dụng các cơ chế hợp tác quốc tế mà Công Ước thiết lập để truy cứu các vụ án "tội phạm mạng".

Ở một mặt tích cực, điều này có thể giúp tăng cường khả năng phối hợp truy bắt các tổ chức tin tặc xuyên quốc gia – nhất là trong bối cảnh Việt Nam cũng từng là nạn nhân của các cuộc tấn công mạng vào ngành ngân hàng, cũng như hàng loạt vụ lừa đảo trực tuyến nhắm vào công dân Việt Nam từ các đường dây quốc tế. Nếu sử dụng đúng, cơ chế hợp tác của Công Ước có thể góp phần cải thiện an ninh mạng một cách thiết thực.

Tuy nhiên, ở mặt tiêu cực – và cũng là điều khiến nhiều người lo ngại – là việc Hà Nội có thể thử nghiệm ranh giới của Công Ước bằng cách yêu cầu hỗ trợ quốc tế đối với các trường hợp mà họ gọi là "tội phạm mạng", nhưng cộng đồng quốc tế nhận ra thực chất chỉ là những hành vi hoạt động ôn hòa, thể hiện chính kiến. Phản ứng của các nền dân chủ tự do trước những yêu cầu như vậy – từ chối hay đáp ứng – sẽ tạo ra tiền lệ ảnh hưởng đến tính chính danh và tương lai áp dụng của Công Ước. Các trường hợp ban đầu sẽ rất quan trọng để xác lập các chuẩn mực thực hành, và có thể sẽ xuất hiện nhu cầu hình thành các hướng dẫn nội bộ hoặc thông lệ quốc tế nhằm xử lý những yêu cầu mang tính chính trị nhạy cảm.

Về mặt đối nội, Luật An ninh mạng tại Việt Nam không có dấu hiệu sẽ được nới lỏng; ngược lại, việc thi hành có thể ngày càng trở nên hệ thống hóa và chặt chẽ hơn. Việc thành lập lực lượng an ninh mạng đông đảo và việc thể chế hóa bộ máy theo dõi dư luận qua các đơn vị như "Lực lượng 47" và đội ngũ "định hướng dư luận" cho thấy nhà cầm quyền có chiến lược lâu dài để kiểm soát không gian mạng và định hình dư luận xã hội. Không gian dân sự trong nước tiếp tục bị thu hẹp nghiêm trọng, và Luật An ninh mạng đang góp phần củng cố tình trạng tự kiểm duyệt trong cộng đồng mạng, khi người dân lo sợ phải đối mặt với các bản án nặng nề nếu "vượt ranh giới đỏ".

Các đối tác thương mại quốc tế sẽ tiếp tục vận động nhà nước Việt Nam điều chỉnh một số điểm cụ thể – chẳng hạn như yêu cầu lưu trữ dữ liệu trong nước, vốn là điểm bế tắc đối với các công ty ngoại quốc. Tuy nhiên, trừ phi có áp lực mạnh mẽ từ bên ngoài hoặc có cải tổ thực sự từ bên trong, Luật này nhiều khả năng sẽ vẫn được duy trì. Đáng chú ý là năm 2026 sẽ diễn ra kỳ Đại hội Đảng toàn quốc định kỳ tại Việt Nam – một thời điểm mà thông tin và an ninh mạng thường bị siết chặt hơn, để bảo đảm tính "ổn định chính trị" cho giới cầm quyền.

Tóm lại, Luật An ninh mạng của Việt Nam và Công Ước Tội phạm mạng của Liên Hiệp Quốc – thường được gọi là "Công Ước Hà Nội" – tượng trưng cho hai tầng nấc của một trật tự toàn cầu đang chuyển dịch. Ở cấp quốc gia, Việt Nam cho thấy cách mà danh nghĩa "an ninh mạng" có thể bị lợi dụng làm bình phong cho chế độ kiểm soát độc đoán. Ở cấp quốc tế, Công Ước mới của LHQ phản ánh nỗ lực toàn cầu trong việc đối phó với các hiểm họa mạng, nhưng lại có nguy cơ đánh đổi quá nhiều cho lợi ích của các nhà nước chuyên chế – mà quên đi quyền tự do và phẩm giá của con người.

Nếu xu hướng hiện nay tiếp tục, sự kết hợp giữa mô hình kiểm soát mạng của Việt Nam và một công ước quốc tế dễ bị khai thác sẽ đặt nền móng cho một trật tự mạng mang màu sắc phi tự do – nơi ranh giới giữa "tội phạm mạng thực sự" và "bất đồng chính kiến ôn hòa" ngày càng trở nên mờ nhạt – không chỉ tại Việt Nam, mà còn trên bình diện toàn cầu.

TÀI LIỆU THAM KHẢO

- Tổ chức Theo dõi Nhân quyền (Human Rights Watch). “Việt Nam: Hãy rút lại Luật An ninh mạng đầy vấn đề.” 7 tháng 6, 2018. www.hrw.org/news/2018/06/07/vietnam-withdraw-problematic-cyber-security-law.
- Báo Nhân Dân. “Việt Nam công bố thời gian tổ chức lễ ký Công Ước Liên Hiệp Quốc về tội phạm mạng.” 25 tháng 12, 2024. en.nhandan.vn/viet-nam-announces-date-for-signing-ceremony-of-un-convention-against-cybercrime-post148265.html.
- Benítez-Mongelós, Sara. “Công Ước về Tội phạm Mạng của LHQ: Vì sao nó đe dọa các nhà báo và người bảo vệ nhân quyền.” Global Campus of Human Rights, tháng 3, 2025. www.gchumanrights.org/preparedness/the-un-cybercrime-convention-why-it-endangers-human-rights-defenders-and-journalists.
- Rodriguez, Katitza. “Công Ước về Tội phạm Mạng: Thiếu sót trong bảo vệ nhân quyền.” Just Security, 21 tháng 3, 2024. www.justsecurity.org/98738/cybercrime-convention-human-rights.
- Scher-Zagier, Eli. “Công Ước Mới của LHQ về Tội phạm Mạng quan trọng hơn cả những gì giới phê bình nhận ra.” Lawfare, 20 tháng 3, 2025. www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-deal-than-even-its-critics-realize.
- Cơ quan Quản lý Thương mại Quốc tế Hoa Kỳ (ITA). “Yêu cầu nội địa hóa dữ liệu theo Luật An ninh mạng Việt Nam.” 1 tháng 9, 2022. www.trade.gov/market-intelligence/vietnam-cybersecurity-data-localization-requirements.
- Ratcliffe, Rebecca. “Luật Internet mới của Việt Nam bị chỉ trích là ‘hà khắc’.” The Guardian, 23 tháng 12, 2024. www.theguardian.com/world/2024/dec/23/vietnam-identity-verification-internet-law-reactions-decree-147-censorship.
- Tổ chức Ân xá Quốc tế (Amnesty International). “Việt Nam: Nhóm tin tặc nhắm vào các nhà hoạt động bằng phần mềm gián điệp.” 10 tháng 2, 2021. www.amnesty.org/en/latest/press-release/2021/02/viet-nam-hacking-group-targets-activist.
- Human Rights Watch. “Các nước EU nên bỏ phiếu chống Công Ước về Tội phạm Mạng của LHQ.” 21 tháng 10, 2024. www.hrw.org/news/2024/10/21/eu-member-states-should-vote-no-un-cybercrime-treaty.
- Electronic Frontier Foundation (EFF). “Mối lo ngại của EFF về dự thảo Công Ước về Tội phạm Mạng của LHQ.” 24 tháng 7, 2024. www.eff.org/deeplinks/2024/07/effs-concerns-about-un-draft-cybercrime-convention.

- Freedom House. “Việt Nam: Tự do Internet năm 2019.” 2019. freedomhouse.org/country/vietnam/freedom-net/2019.
- Lumb, David. “Luật An ninh mạng mới của Việt Nam làm dấy lên lo ngại về hạn chế tự do ngôn luận.” TechCrunch, 12 tháng 6, 2018. techcrunch.com/2018/06/12/vietnams-new-cyber-security-law-draws-concern-for-restricting-free-speech.
- Amnesty International. “Luật An ninh mạng mới của Việt Nam: Một cú đánh nặng nề vào tự do biểu đạt.” 12 tháng 6, 2018. www.amnesty.org/en/press-releases/2018/06/viet-nam-cybersecurity-law-devastating-blow-freedom-of-expression.
- Đỗ Việt Cường và Nguyễn Quang Hà. “Công Ước Hà Nội về Tội phạm Mạng: Một cột mốc cho thế giới và Việt Nam.” Tạp chí Pháp luật Việt Nam, 3 tháng 4, 2025. vietnamlawmagazine.vn/hanoi-convention-against-cybercrime-a-milestone-for-the-world-and-vietnam-73746.html.
- Gia Nghi và Ngọc Nguyễn. “Hà Nội sẽ đăng cai lễ ký Công Ước về Tội phạm Mạng năm 2025.” Thời Báo Kinh Tế Sài Gòn, 25 tháng 12, 2024. english.thesaigontimes.vn/hanoi-to-host-un-cybercrime-convention-signing-in-2025.
- Human Rights Watch. “Việt Nam: Hủy bỏ các đạo luật Internet gây hại.” 10 tháng 12, 2024. www.hrw.org/news/2024/12/11/vietnam-repeal-harmful-internet-laws.
- Lương Hải Thành. “Việt Nam cần hợp tác thực chất để triệt phá mạng lưới tội phạm mạng.” East Asia Forum, 26 tháng 3, 2025. eastasiaforum.org/2025/03/26/vietnam-needs-committed-collaboration-to-dismantle-cybercrime-networks.
- Parameswaran, Prashanth. “Tương lai nào cho Luật An ninh mạng mới của Việt Nam năm 2019?” The Diplomat, 3 tháng 1, 2019. thediplomat.com/2019/01/what-lies-ahead-for-vietnams-new-cyber-law-in-2019.
- Propp, Kenneth và Kennedy-Mayo, DeBrae. “Từ Budapest đến Hà Nội: So sánh Công Ước về Tội phạm mạng của Hội đồng Âu Châu và Liên Hiệp Quốc.” Lawfare, 8 tháng 5, 2025. www.lawfaremedia.org/article/from-budapest-to-hanoi--comparing-the-coe-and-un-cybercrime-conventions.
- Văn phòng Ma túy và Tội phạm Liên Hiệp Quốc (UNODC). “Công Ước Liên Hiệp Quốc về Tội phạm Mạng: Tăng cường hợp tác quốc tế để chống lại một số tội phạm sử dụng công nghệ thông tin và chia sẻ chứng cứ điện tử trong các vụ án nghiêm trọng.” 2025. www.unodc.org/unodc/en/cybercrime/convention/home.html.

VỀ TÁC GIẢ

Luật sư Linh Nguyễn là một nhà hoạt động cho Tự do Tôn giáo và Nhân quyền. Bà từng đảm nhiệm vai trò cố vấn cho Tòa Công Lý Duy Ngô Nhĩ (Uyghur Tribunal), do Ngài Geoffrey Nice, QC, chủ toạ.

Trong các năm 2021 và 2023, bà đã tham gia các cuộc tham vấn với chính phủ Hoa Kỳ nhằm chuẩn bị cho các Hội nghị Thượng đỉnh về Dân chủ, đóng góp vào các vấn đề then chốt như: yểm trợ phong trào dân chủ, bài trừ tham nhũng, bảo vệ sự trong sạch của tiến trình bầu cử, cổ xúy một nền hành chánh bao gồm mọi giới, và bảo vệ quyền lợi của giới lao động. Năm 2024, bà đảm nhiệm vai trò điều hợp viên tại Hội nghị Thượng đỉnh Dân chủ Á Châu, tổ chức tại thủ đô Hán Thành, Đại Hàn, trong khuôn khổ Thượng đỉnh Dân chủ Toàn cầu.

Là một diễn giả được chú ý trên trường quốc tế, bà từng phát biểu tại Ngày Quốc tế Dân chủ năm 2023 tại trụ sở Liên Hiệp Quốc, và được mời thuyết trình tại Hội nghị Thượng đỉnh Tương Lai do Đại Hội Đồng LHQ tổ chức. Quan điểm và phân tích của bà đã được phổ biến rộng rãi trên các cơ quan truyền thông uy tín như Đài Á Châu Tự Do, Đài Tiếng Nói Hoa Kỳ, và nhật báo South China Morning Post.

2025

Chi tiết liên lạc

info@endcommunism.net

allianceforvietnamsdemocracy.org