TỘI PHẠM MẠNG TRONG PHÁP LUẬT HÌNH SỰ MỘT SỐ QUỐC GIA VÀ KINH NGHIỆM CHO VIỆT NAM

● **BÙI THỊ PHƯƠNG QUỲNH[1] - TRƯƠNG VĂN TIẾN[2]**
[1] Giảng viên Khoa Luật học, Trường Đại học Vinh
[2] Lớp 63B3 Luật Kinh tế, Trường Đại học Vinh

TÓM TẮT:

Trong bối cảnh toàn cầu hóa và phát triển mạnh mẽ của công nghệ thông tin, internet trở thành hạ tầng thiết yếu nhưng đồng thời gia tăng nguy cơ an ninh, trật tự, đặc biệt là tội phạm mạng. Với đặc trưng phi lãnh thổ, nặc danh và biến đổi nhanh, tội phạm mạng đặt ra thách thức lớn cho hệ thống pháp luật hình sự, trong đó có Việt Nam. Trước yêu cầu hoàn thiện thể chế trong "kỷ nguyên số", nghiên cứu pháp luật hình sự về tội phạm mạng trở nên cấp thiết. Bài viết phân tích quy định pháp luật hình sự của Mỹ, Đức, Anh và các chuẩn mực quốc tế để rút ra kinh nghiệm, từ đó đề xuất giải pháp hoàn thiện pháp luật hình sự về tội phạm mạng tại Việt Nam, góp phần tăng cường hiệu quả phòng ngừa, xử lý và bảo vệ an ninh mạng trong bối cảnh hiện nay.

Từ khóa: tội phạm mạng, pháp luật hình sự, an ninh mạng, Việt Nam.

1. Đặt vấn đề

Trong bối cảnh kỷ nguyên số ngày càng phát triển, tội phạm mạng không còn là hiện tượng riêng lẻ mà đã trở thành một dạng tội phạm điển hình của không gian số, vượt ra ngoài khuôn khổ điều chỉnh truyền thống của pháp luật hình sự. Thời gian qua, công tác phòng, chống tội phạm mạng (TPM) được triển khai quyết liệt, đồng bộ và toàn diện, góp phần đạt được nhiều kết quả quan trọng trong thực tiễn.

Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung 2017) đã quy định về tội phạm mạng một cách đầy đủ, rõ ràng và chặt chẽ hơn trước. Nhiều quy định về tội phạm đã được sửa đổi, bổ sung cho phù hợp với các chuẩn mực quốc tế và thực tiễn, tạo điều kiện cho các cơ quan bảo vệ pháp luật đấu tranh phòng, chống tội phạm ngày càng đạt hiệu quả. Tuy nhiên, tội phạm mạng ở Việt Nam vẫn đang có xu hướng gia tăng, đồng thời xuất hiện nhiều hình thức phạm tội mới với những thủ đoạn thực hiện ngày càng tinh vi (Hồng Vinh, 2024). Bên cạnh đó, do đặc trưng của loại tội phạm này là khó phát hiện, khó truy lùng dấu vết khiến cho hậu quả để lại đặc biệt nghiêm trọng. Trong khi nhiều quốc gia đã có những bước tiến đáng kể trong việc xây dựng hệ thống pháp luật để xử lý tội phạm, thì Việt Nam, mặc dù đã có những hành động và quy định pháp lý trong lĩnh vực này, nhưng vẫn đang đối mặt với nhiều thách thức trong việc áp dụng pháp luật hiệu quả. Đặc biệt, Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017) đã có hiệu lực thi hành được 8 năm, nên cần có những

nghiên cứu để đánh giá tính hiệu quả của quy định pháp luật. Điều này đòi hỏi Việt Nam cần phải tham khảo, học hỏi kinh nghiệm từ các quốc gia đi trước để hoàn thiện và cải thiện hệ thống pháp luật hình sự của mình trong lĩnh vực tội phạm mạng.

2. Bài học kinh nghiệm từ các quốc gia

2.1. Bài học kinh nghiệm từ Mỹ

Kinh nghiệm của Mỹ cho thấy cách tiếp cận sớm, rõ ràng và có tính hệ thống trong xây dựng pháp luật về tội phạm mạng. Mỹ đã ban hành các đạo luật nền tảng như Đạo luật về gian lận và lạm dụng máy tính (CFAA), đồng thời thiết lập hệ thống pháp luật bổ trợ liên quan đến an ninh mạng và bảo vệ dữ liệu. Điểm đáng chú ý là Mỹ không xây dựng một khái niệm chung về tội phạm mạng mà phân loại cụ thể từng hành vi vi phạm. Cách tiếp cận này giúp pháp luật trở nên linh hoạt hơn khi xử lý các trường hợp cụ thể.

Bên cạnh đó, Mỹ đã ký các công ước với các quốc gia trong việc hợp tác đấu tranh xử lý TPM theo đó Công ước Budapest và Công ước Palermo là 2 công cụ quan trọng trong việc hỗ trợ hợp tác quốc tế trong xử lý tội phạm công nghệ cao (Nguyễn Hoàng Chi Mai, 2023), từ đó tạo cơ sở pháp lý cho hoạt động dẫn độ, tương trợ tư pháp và phối hợp điều tra trong các vụ án xuyên quốc gia.

Về thực tiễn, Mỹ chú trọng xây dựng lực lượng chuyên trách với trình độ cao thông qua các cơ quan như Cục Điều tra Liên bang (FBI) và Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA), đồng thời triển khai các chương trình đào tạo chuyên sâu và liên tục. Ngoài ra, Mỹ đẩy mạnh ứng dụng công nghệ hiện đại như trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data) và hệ thống giám sát an ninh mạng nhằm nâng cao hiệu quả phát hiện và xử lý tội phạm. Công tác tuyên truyền, nâng cao nhận thức xã hội cũng được triển khai rộng rãi, góp phần phòng ngừa tội phạm từ sớm.

2.2. Bài học kinh nghiệm từ Đức

Đức xây dựng hệ thống pháp luật về tội phạm mạng theo hướng chi tiết nhưng linh hoạt, phù hợp với sự phát triển nhanh chóng của công nghệ thông tin. Hệ thống pháp luật không chỉ điều chỉnh các hành vi truyền thống mà còn bao quát các hành vi mới phát sinh trong môi trường số, gắn với các quy định về bảo vệ dữ liệu và an ninh thông tin, chẳng hạn Luật Bảo vệ dữ liệu Liên bang Đức (BDSG) và Quy định Chung về Bảo vệ Dữ liệu của EU (GDPR). Từ đó cho thấy, pháp luật cần có khả năng cập nhật thường xuyên để thích ứng với thực tiễn.

Đức cũng đặc biệt coi trọng hợp tác quốc tế, nhất là trong khuôn khổ Liên minh châu Âu và các điều ước quốc tế về tương trợ tư pháp. Cơ chế hợp tác này giúp nâng cao hiệu quả điều tra, truy tố và xét xử các vụ án có yếu tố xuyên biên giới.

Về thực tiễn, Đức xây dựng cơ chế điều phối tập trung thông qua Cơ quan Cảnh sát Hình sự Liên bang (BKA), đồng thời tăng cường hợp tác với Europol, Interpol và các đối tác quốc tế. Ngoài ra, Đức thiết lập cơ chế phối hợp chặt chẽ giữa cơ quan nhà nước và khu vực tư nhân, qua đó nâng cao khả năng chia sẻ thông tin và ứng phó với các mối đe dọa an ninh mạng. Việc ứng dụng công nghệ như AI và Big Data cũng được chú trọng nhằm phát hiện sớm và xử lý hiệu quả các hành vi phạm tội.

2.3. Bài học kinh nghiệm từ Anh

Anh xây dựng hệ thống pháp luật tương đối hoàn chỉnh với các đạo luật chuyên biệt như Đạo luật Sử dụng sai mục đích máy tính, đồng thời thường xuyên cập nhật để phù hợp với thực tiễn. Hệ thống pháp luật của Anh chú trọng tính thống nhất, tính ràng buộc và khả năng cụ thể hóa các cam kết quốc tế thành quy định pháp lý trong nước.

Một điểm đáng chú ý là Anh tiếp cận theo hướng phân loại rõ ràng các hành vi tội phạm mạng, qua đó nâng cao tính minh bạch và khả năng áp dụng pháp luật. Đồng thời, Anh đặc biệt chú trọng xây dựng cơ chế hợp tác quốc tế, bao gồm các quy định về dẫn độ, tương trợ tư pháp và truy xuất dữ liệu xuyên biên giới, điển hình là việc tham gia Công ước Budapest và ký kết các hiệp định song phương.

Về thực tiễn, Anh áp dụng nguyên tắc quyền tài phán mở rộng, cho phép xử lý các hành vi phạm tội có yếu tố nước ngoài nhưng liên quan đến công dân hoặc tổ chức trong nước. Ngoài ra, Anh đẩy mạnh ứng dụng công nghệ hiện đại trong giám sát và phát hiện

tội phạm, đồng thời xây dựng các chương trình đào tạo chuyên sâu cho lực lượng thực thi pháp luật. Việc tăng cường hợp tác quốc tế và phát triển các công cụ kỹ thuật số cũng góp phần nâng cao hiệu quả phòng, chống tội phạm mạng.

3. Đề xuất và giải pháp hoàn thiện pháp luật hình sự về tội phạm mạng tại Việt Nam trong bối cảnh mới

Trên cơ sở đối chiếu giữa Bộ luật Hình sự 2015 (sửa đổi, bổ sung 2017) và Luật An ninh mạng 2025 (có hiệu lực từ ngày 01/7/2026), có thể nhận thấy một vấn đề mang tính bản chất: Luật An ninh mạng đã bước đầu nhận diện tương đối đầy đủ các hành vi nguy hiểm trong không gian mạng, nhưng phần lớn các hành vi này chưa được "chuyển hóa" tương ứng thành tội phạm trong luật Hình sự. Điều này tạo ra khoảng trống pháp lý giữa "hành vi bị cấm" và "hành vi bị xử lý hình sự".

Vì vậy, việc hoàn thiện Bộ luật Hình sự cần đi theo hướng nội luật hóa trực tiếp các hành vi đã được xác định trong Luật An ninh mạng, đồng thời cụ thể hóa thành các cấu thành tội phạm rõ ràng, có khả năng áp dụng trong thực tiễn.

3.1.Pháp luật Việt Nam cần bổ sung quy định về một số hành vi tội phạm mạng mới.

Một là, cần xem xét, bổ sung quy định về tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản tại Điều 290 của Bộ luật Hình sự 2015 (sửa đổi, bổ sung 2017) theo hướng mở rộng phạm vi điều chỉnh đối với các hành vi sử dụng công nghệ mới. Cụ thể, đề xuất bổ sung điểm e khoản 1 Điều 290 mới quy định: "Sử dụng công nghệ thông tin, phương tiện điện tử, trí tuệ nhân tạo hoặc công nghệ số khác để tạo lập, giả mạo hình ảnh, âm thanh, dữ liệu nhận dạng của cá nhân, tổ chức nhằm thực hiện hành vi chiếm đoạt tài sản". Quy định này nhằm trực tiếp hình sự hóa hành vi lừa đảo bằng công nghệ giả mạo (deepfake), vốn đang trở thành xu hướng phổ biến và có mức độ nguy hiểm cao.

Hai là, các hành vi tội phạm liên quan đến blockchain và tiền mã hóa, như rửa tiền và lừa đảo qua giao dịch tiền mã hóa, cũng cần được pháp luật quy định rõ ràng để bảo vệ an ninh tài chính quốc gia. Nhóm nghiên cứu đề xuất bổ sung điểm i khoản 2 Điều 324: Tội rửa tiền "sử dụng mạng máy tính, mạng viễn thông hoặc phương tiện điện tử để phạm tội".

Ba là, các hành vi lạm dụng dữ liệu cá nhân, vi phạm quyền riêng tư, phát tán thông tin sai lệch và tội phạm liên quan đến Internet of Things (IoT) cần được điều chỉnh chặt chẽ hơn.

3.2. Việt Nam cần sửa đổi, bổ sung các quy định của pháp luật hình sự về tội phạm mạng theo hướng khắc phục những hạn chế nội tại và bảo đảm sự tương thích với các chuẩn mực pháp lý quốc tế.

Một là, đối với Điều 286 về tội phát tán chương trình tin học gây hại, cần bổ sung dấu hiệu về đối tượng tác động vào cấu thành tội phạm cơ bản, theo đó xác định rõ các hệ thống thông tin có tính chất đặc biệt quan trọng như: hệ thống dữ liệu thuộc bí mật nhà nước, hệ thống thông tin phục vụ quốc phòng, an ninh. Khi hành vi phát tán chương trình độc hại được thực hiện nhằm vào các hệ thống này, tội phạm cần được coi là hoàn thành ngay tại thời điểm thực hiện hành vi, không phụ thuộc vào việc hậu quả đã xảy ra hay chưa. Đồng thời, hậu quả thực tế (nếu có) hoặc yếu tố tái phạm cần được chuyển hóa thành các tình tiết định khung tăng nặng, nhằm bảo đảm sự phân hóa trách nhiệm hình sự.

Hai là, đối với Điều 287 về tội cản trở hoặc gây rối loạn hoạt động của hệ thống thông tin, cần mở rộng phạm vi các đối tượng được bảo vệ trong cấu thành cơ bản, bao gồm: cơ sở hạ tầng thông tin trọng yếu quốc gia như hệ thống điều hành lưới điện, hệ thống tài chính - ngân hàng, hệ thống điều khiển giao thông, cũng như các hệ thống thông tin phục vụ quốc phòng, an ninh. Việc tác động trái phép đến các hệ thống này, xét về bản chất, đã đủ để cấu thành hành vi nguy hiểm cho xã hội ở mức độ cao, do đó cần được xử lý hình sự ngay cả khi chưa phát sinh hậu quả cụ thể. Cách tiếp cận này phù hợp với yêu cầu bảo vệ an ninh mạng quốc gia trong Luật An ninh mạng năm 2025, đồng thời tiệm cận với thông lệ quốc tế về bảo vệ hạ tầng thông tin trọng yếu.

Ba là, đối với Điều 288 về tội đưa hoặc sử dụng trái phép thông tin trên mạng, cần bổ sung dấu hiệu "thông tin có tác hại lớn cho xã hội" vào cấu thành tội phạm cơ bản. Quy định này nhằm xử lý kịp thời các hành vi phát tán thông tin nguy hiểm, đặc biệt là thông tin sai lệch có khả năng gây bất ổn xã hội, ảnh hưởng đến an ninh quốc gia hoặc trật tự công cộng, ngay cả khi hậu quả cụ thể chưa xảy ra hoặc chưa thể định lượng. Tuy nhiên, để bảo đảm tính minh bạch và tránh nguy cơ áp dụng tùy tiện, cần thiết phải xây dựng các tiêu chí pháp lý rõ ràng để xác định "tác hại lớn cho xã hội", có thể dựa trên các yếu tố như phạm vi lan truyền, mức độ ảnh hưởng đến cộng đồng, và khả năng gây phương hại đến các lợi ích được pháp luật bảo vệ.

3.3. Thứ ba, cần bổ sung quy định thêm về trách nhiệm hình sự đối với pháp nhân thương mại trong tội phạm mạng.

Theo đó, tại điều 76 Bộ luật Hình sự năm 2015 chưa có quy định pháp nhân thương mại phải chịu trách nhiệm hình sự về tội phạm mạng hay tội phạm trong lĩnh vực công nghệ thông tin, mạng vi tính. Cần quy định trách nhiệm hình sự đối với pháp nhân là một bước tiến quan trọng trong việc củng cố hệ thống pháp luật, vì trong thực tế, các tổ chức, công ty, doanh nghiệp không chỉ có nguồn lực lớn mà còn nắm giữ một lượng lớn dữ liệu và thông tin quan trọng đồng nghĩa với đó nếu gây ra hậu quả sẽ rất lớn. Việc truy cứu trách nhiệm hình sự đối với pháp nhân trong các tội phạm mạng sẽ giúp giải quyết những vấn đề như:

Một là, tạo sự công bằng trong xử lý tội phạm, vì trong nhiều vụ việc tội phạm mạng, hành vi vi phạm có thể xuất phát từ sự thiếu sót trong việc quản lý, giám sát và bảo vệ an ninh mạng của pháp nhân. Nếu pháp nhân không phải chịu trách nhiệm hình sự, các hành vi này có thể không bị xử lý nghiêm túc. Việc truy cứu trách nhiệm hình sự đối với pháp nhân sẽ tạo ra một cơ chế công bằng, giúp cả cá nhân lẫn tổ chức phải chịu trách nhiệm nếu hành vi của họ gây thiệt hại cho xã hội.

Hai là, tăng cường trách nhiệm của tổ chức, doanh nghiệp khi pháp nhân phải chịu trách nhiệm hình sự, điều này sẽ khuyến khích các tổ chức, doanh nghiệp phải nghiêm túc hơn trong việc xây dựng các chính sách bảo mật, phòng ngừa tội phạm mạng. Các công ty sẽ phải đầu tư vào cơ sở hạ tầng bảo mật, đào tạo nhân viên và thiết lập các quy trình phòng ngừa nhằm hạn chế tối đa các rủi ro từ tội phạm mạng.

3.4. Giải pháp tăng cường hiệu quả thực thi pháp luật

Thứ nhất, để phòng chống tội phạm mạng hiệu quả, một trong những biện pháp quan trọng là tăng cường cơ sở hạ tầng hệ thống bảo mật cao. Việc này không chỉ giúp ngăn chặn các mối đe dọa từ tội phạm mạng mà còn bảo vệ thông tin cá nhân, tài sản và các hệ thống quan trọng của quốc gia. Đầu tiên, cần đầu tư vào các công nghệ bảo mật tiên tiến như mã hóa dữ liệu, xác thực đa yếu tố và các công cụ giám sát mạng để phát hiện và ngăn chặn kịp thời các cuộc tấn công mạng. Bên cạnh việc đầu tư vào công nghệ, cũng cần xây dựng các quy trình bảo mật chặt chẽ. Đồng thời, các tổ chức và cơ quan nhà nước cần phối hợp với các doanh nghiệp và các chuyên gia an ninh mạng để thiết lập các kế hoạch phản ứng nhanh khi có sự cố an ninh xảy ra, giúp giảm thiểu thiệt hại và khôi phục hệ thống nhanh chóng.

Thứ hai, cần đẩy mạnh hợp tác quốc tế trong đấu tranh phòng chống tội phạm mạng bởi hợp tác quốc tế trong việc đấu tranh phòng chống tội phạm mạng đóng vai trò cực kỳ quan trọng trong bối cảnh tội phạm mạng ngày càng trở nên tinh vi và xuyên biên giới. Các quốc gia cần phải hợp tác để chia sẻ thông tin, công nghệ, và nguồn lực nhằm đối phó với những mối đe dọa này. Thông qua các tổ chức quốc tế như Interpol và Europol, các quốc gia có thể phối hợp trong việc điều tra, truy tố và ngăn chặn các hành vi tội phạm mạng, đặc biệt là khi chúng liên quan đến các nhóm tội phạm có tổ chức và xuyên quốc gia. Ngoài ra, việc tham gia vào các công ước quốc tế như Công ước Budapest về tội phạm mạng và Công ước Palermo về phòng chống tội phạm có tổ chức giúp các quốc gia có một khuôn khổ pháp lý chung để thúc đẩy hợp tác trong việc xử lý tội phạm mạng. Thêm vào đó, các chiến dịch toàn cầu nhằm nâng cao nhận thức cộng đồng và tăng cường an ninh mạng cũng góp phần quan trọng trong việc phòng ngừa và xử lý

tội phạm mạng hiệu quả. Do đó, hợp tác quốc tế không chỉ là giải pháp hữu hiệu giúp các quốc gia đối phó với tội phạm mạng mà còn là yếu tố thiết yếu trong việc xây dựng một môi trường mạng an toàn và bảo mật trên toàn cầu.

Thứ ba, một biện pháp quan trọng trong công tác phòng chống tội phạm mạng là tuyên truyền và thông báo đến người dân về các hình thức tội phạm mới trong không gian mạng để họ có thể chủ động phòng tránh đặc biệt là vùng biên giới, vùng sâu vùng xa… từ đó giảm thiểu những thiệt hại không đáng có. Với sự phát triển nhanh chóng của công nghệ và sự xuất hiện của nhiều hình thức tội phạm mạng mới, việc nâng cao nhận thức cộng đồng là một yếu tố không thể thiếu trong chiến lược bảo vệ an ninh mạng. Các chiến dịch tuyên truyền có thể bao gồm việc cung cấp thông tin chi tiết về các loại tội phạm mạng phổ biến như lừa đảo qua email, lừa đảo qua mạng xã hội, gian lận trực tuyến, tấn công DDoS, hoặc phát tán mã độc (malware)... Các hình thức tội phạm này thường thay đổi liên tục và ngày càng tinh vi hơn, khiến người dân dễ bị lừa gạt hoặc gặp phải các mối nguy hiểm. Vì vậy, việc cung cấp những thông tin kịp thời và chính xác sẽ giúp người dân nhận diện được các mối đe dọa và cảnh giác hơn.

Ngoài ra, các chiến dịch cũng cần nhấn mạnh tầm quan trọng của việc cập nhật phần mềm và các hệ điều hành thường xuyên để bảo vệ các thiết bị cá nhân khỏi những lỗ hổng bảo mật. Việc sử dụng các phương tiện truyền thông đại chúng, từ báo chí, truyền hình, đến các mạng xã hội, sẽ giúp thông tin đến được đông đảo người dân. Đồng thời, có thể tổ chức các khóa học, hội thảo hoặc chương trình đào tạo trực tuyến để hướng dẫn người dân các kỹ năng bảo mật cơ bản, giúp họ chủ động bảo vệ thông tin cá nhân và phòng tránh các hình thức tội phạm mạng. Ngoài ra, các cơ quan nhà nước, tổ chức xã hội và doanh nghiệp cần phối hợp chặt chẽ trong việc cung cấp thông tin, khuyến khích người dân tham gia vào các chương trình bảo vệ an ninh mạng. Điều này không chỉ giúp nâng cao ý thức cộng đồng mà còn góp phần tạo ra một mạng lưới bảo mật vững chắc, giúp giảm thiểu thiệt hại do tội phạm mạng gây ra.

4. Kết luận

Bài viết đã làm rõ đặc điểm, xu hướng phát triển của tội phạm mạng và những thách thức đặt ra đối với pháp luật hình sự trong bối cảnh chuyển đổi số. Trên cơ sở phân tích kinh nghiệm của một số quốc gia như Mỹ, Đức và Anh, bài viết rút ra những giá trị tham khảo quan trọng cho Việt Nam trong việc xây dựng và hoàn thiện pháp luật. Từ đó, bài viết đề xuất định hướng hoàn thiện pháp luật hình sự theo hướng nội luật hóa các hành vi nguy hiểm trong không gian mạng, đồng thời nâng cao hiệu quả thực thi thông qua tăng cường năng lực bảo mật, hợp tác quốc tế và nhận thức xã hội. Đây là những yêu cầu cấp thiết nhằm bảo đảm an ninh mạng và trật tự an toàn xã hội trong kỷ nguyên số ■

TÀI LIỆU THAM KHẢO:

Trần Thị Diệu Hương (2018). Án lệ trong hệ thống pháp luật thông luật Anh - Kinh nghiệm cho việc hoàn thiện quy định về án lệ ở Việt Nam. Trang điện tử Ban Nội chính Tỉnh ủy Bắc Ninh. Truy cập tại https://bannoichinh.bacninh.gov.vn/news/-/details/4295857/an-le-trong-he-thong-phap-luat-thong-luat-anh-kinh-nghiem-cho-viec-hoan-thien-quy-inh-ve-an-le-o-viet-nam

Hồng Vinh. (2024). Nhiều dữ liệu bí mật của các cơ quan, tổ chức bị đánh cắp, tăng 33% tấn công mạng. Truy cập tại https://vneconomy.vn/nhieu-du-lieu-bi-mat-cua-cac-co-quan-to-chuc-bi-danh-cap-tang-33-tan-cong-mang.htm?utm_source=chatgpt.com

Nguyễn Hoàng Chi Mai. (2023). Kinh nghiệm của Hoa Kỳ về phòng, chống tội phạm mạng. Tạp chí Kiểm sát, số 22/2023. Truy cập tại https://vksquangngai.gov.vn/kinh-nghiem-cua-hoa-ky-ve-phong-chong-toi-pham-mang-833.html

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. (2006). Luật Công nghệ thông tin 2006.

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. (2008). Luật Công nghệ cao 2008.

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. (2015). Bộ luật Hình sự 2015.

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. (2017). Bộ luật Hình sự sửa đổi, bổ sung 2017.

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. (2018). Luật An ninh mạng 2018.

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam. (2025). Luật An ninh mạng 2025.

Council of Europe. (2001). Convention on Cybercrime. Budapest, Hungary: Council of Europe. Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

United Nations. (2000). United Nations Convention against Transnational Organized Crime and the Protocols Thereto. Adopted at Palermo, Italy, 15 November 2000. Available at https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

Ngày nhận bài: 20/01/2026
Ngày phản biện đánh giá và sửa chữa: 6/02/2026
Ngày chấp nhận đăng bài: 23/02/2026

CYBERCRIME IN COMPARATIVE CRIMINAL LAW: LESSONS AND IMPLICATIONS FOR VIETNAM

● **BUI THI PHUONG QUYNH**[1]
● **TRUONG VAN TIEN**[2]
[1]Lecturer, Faculty of Law, Vinh University
[2]Student, Vinh University

ABSTRACT:

Amid globalization and the rapid advancement of information technology, the Internet has become essential infrastructure while simultaneously intensifying risks to security and public order, particularly in the form of cybercrime. Characterized by its transnational scope, anonymity, and rapid evolution, cybercrime presents substantial challenges to contemporary criminal law systems, including that of Vietnam. In response to the growing imperative to modernize legal frameworks in the digital age, this study examines criminal law provisions on cybercrime through a comparative analysis of the United States, Germany, the United Kingdom, and relevant international standards. The findings provide a comprehensive perspective on regulatory approaches and contribute to a deeper understanding of legal mechanisms for strengthening cybercrime prevention, enforcement, and cybersecurity protection in Vietnam.

Keywords: cybercrime, criminal law, cybersecurity, Vietnam.