KINH NGHIỆM QUỐC TẾ VỀ XỬ LÝ TỘI PHẠM CÔNG NGHỆ CAO VÀ MỘT SỐ KHUYẾN NGHỊ CHO VIỆT NAM

NGUYỄN HOÀNG CHI MAI *

Từ khóa: Tội phạm công nghệ cao; an ninh mạng.

Nhận bài : 20/7/2022.
Biên tập xong : 27/7/2022.
Duyệt bài : 29/7/2022.

“Nhận thức về tính chất nguy hiểm và phức tạp của tội phạm công nghệ cao, các quốc gia phát triển trên thế giới đã sớm thiết lập hành lang pháp lý chặt chẽ để xử lý và ngăn chặn hiệu quả tội phạm này. Bài viết giới thiệu kinh nghiệm của một số quốc gia tiêu biểu trong xử lý tội phạm công nghệ cao và đưa ra một số khuyến nghị cho Việt Nam.”

1. Kinh nghiệm quốc tế về xử lý tội phạm công nghệ cao

Mặc dù có sự khác biệt trong các quan điểm, nhưng về cơ bản, tội phạm công nghệ cao theo pháp luật quốc tế được hiểu là hành vi phạm tội xâm nhập đến máy tính một cách trái phép để tấn công, phá hoại hoặc chiếm hữu dữ liệu nhằm mục đích vụ lợi; chống lại cá nhân; chống lại tổ chức hoặc chống lại xã hội. Cho đến nay, nhân loại chứng kiến sự phát triển và bùng nổ của internet và công nghệ thông tin, theo đó, tạo điều kiện cho sự gia tăng về số lượng và quy mô của tội phạm công nghệ cao, đòi hỏi khung pháp lý phải liên tục được rà soát, hoàn thiện để điều chỉnh, xử lý. Dưới đây là pháp luật của một số quốc gia tiêu biểu về xử lý tội phạm công nghệ cao.

1.1. Pháp luật Trung Quốc

Là quốc gia lớn và đông dân nhất thế giới, năm 2018, Trung Quốc đã có số lượng người sử dụng máy tính đạt mức 802 triệu người, giúp củng cố vị trí của nước này là

* *Viện Khoa học pháp lý, Bộ Tư pháp.*

cộng đồng trực tuyến lớn nhất thế giới[1]. Theo báo cáo của Symantec - nhà cung cấp phần mềm bảo mật máy tính, Trung Quốc là nước có các hoạt động tấn công mạng bằng phần mềm độc hại phát triển mạnh nhất trong khu vực[2]; đồng thời, tồn tại nhiều hình thức tấn công do tội phạm mạng gây ra. Trước thực tế đó, Chính phủ Trung Quốc đã tiến hành các biện pháp nhằm ngăn chặn và xử lý loại tội phạm nguy hiểm này.

Ngày 07/11/2016, Ủy ban Thường vụ Đại hội Đại biểu nhân dân toàn quốc Cộng hòa nhân dân Trung Hoa đã ban hành Luật an ninh mạng nước Cộng hòa nhân dân Trung Hoa (gọi tắt là Luật ANM) có hiệu lực từ ngày 01/6/2017[3]. Bộ luật gồm 79 điều, chia làm 07 chương. Mục đích Chính phủ Trung Quốc hướng đến khi xây dựng bộ luật này được cụ thể hóa bằng các hành động: (1) Bảo vệ chủ quyền không gian mạng; (2) Xác định nghĩa vụ bảo mật của các nhà cung cấp sản phẩm và dịch vụ internet; (3) Hoàn thiện các quy tắc bảo vệ thông tin cá nhân; (4) Thiết lập hệ thống bảo mật cho cơ sở hạ tầng thông tin quan trọng; (5) Thiết lập các quy tắc cho việc truyền dữ liệu xuyên quốc gia tại cơ sở hạ tầng thông tin quan trọng[4]. Có thể thấy, Luật ANM đề cao vai trò và sự quản lý của nhà nước trong việc kiểm soát hoạt động của các nhà cung cấp mạng và người sử dụng mạng internet. Các quy định của luật cũng nêu rõ, Chính phủ Trung Quốc có quyền ban hành các biện pháp nhằm giám sát, ngăn chặn và xử lý các rủi ro, đe dọa an ninh mạng phát sinh từ trong và ngoài lãnh thổ quốc gia này[5].

Bên cạnh việc tạo ra quyền lực nhà nước trong hoạt động quản lý mạng, Chính phủ Trung Quốc còn đặt ra các quy định cho nhà cung cấp mạng yêu cầu các hoạt động kinh doanh và dịch vụ mạng phải tuân thủ luật pháp và các quy định hành chính, tôn trọng đạo đức xã hội, tuân thủ đạo đức thương mại, trung thực và đáng tin cậy, thực hiện nghĩa vụ bảo vệ an ninh mạng, chấp nhận sự giám sát của Chính phủ và công chúng; đồng thời chịu trách nhiệm xã hội[6]. Các yêu cầu này được cụ thể hóa như sau: (1) Xây dựng hệ thống quản lý an ninh nội bộ và quy tắc hoạt động, xác định những người chịu trách nhiệm về an ninh mạng và thực hiện trách nhiệm bảo vệ an ninh mạng; (2) Áp dụng các biện pháp kỹ thuật để ngăn chặn virus máy tính, tấn công mạng, xâm nhập mạng và các hành động khác gây nguy hiểm cho an ninh

1. Báo cáo của Trung tâm thông tin Internet Trung Quốc (CNNIC).

2. Symantec Security Summary - December 2021, xem tại đường dẫn: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-december-2021.

3. Xem tại đường dẫn: https://www.informatica-juridica.com/ley/data-security-law-of-the-peoples-republic-of-chinadsl/#:~:text=The%20provisions%20of%20the%20Cybersecurity,data%20handlers%20collecting%20or%20producing.

4. Nick Beckett (2017), "A guide for businesses to China's first cyber security law", xem tại đường dẫn: https://www.computerweekly.com/opinion/Chinas-first-cyber-security-law-what-it-means-for-companies.

5. Điều 5 Luật an ninh mạng nước Cộng hòa nhân dân Trung Hoa.

6. Điều 9 Luật an ninh mạng nước Cộng hòa nhân dân Trung Hoa.

mạng; (3) Áp dụng các biện pháp kỹ thuật để theo dõi, ghi lại trạng thái hoạt động mạng, sự cố an ninh mạng và tuân theo các quy định lưu trữ nhật ký mạng trong ít nhất 06 tháng; (4) Áp dụng các biện pháp phân loại dữ liệu, sao lưu dữ liệu quan trọng và mã hóa; (5) Các nghĩa vụ khác được cung cấp bởi pháp luật hoặc các quy định hành chính.

Như vậy, Luật ANM đã tạo nên một hệ thống các quy định và chế tài chặt chẽ nhằm đề phòng và xử lý sự tấn công của tội phạm công nghệ cao. Với số lượng người sử dụng mạng internet đông nhất Châu Á, việc ban hành các quy định này của Chính phủ Trung Quốc mang lại hiệu quả tích cực, giúp giảm thiểu một cách rõ rệt số lượng tội phạm công nghệ cao.

Bên cạnh ưu điểm, Luật ANM của quốc gia này vẫn tồn tại những bất cập nhất định, ví dụ: Internet ở Trung Quốc đang dần mất tính lưu trữ thông tin và phát triển ứng dụng tự do khi chính phủ kiểm soát chặt chẽ cả về nội dung, mạng lưới kết nối, ứng dụng và các kênh giao tiếp. Có một số quy định "cực đoan" được cho là xâm phạm quyền riêng tư về lưu trữ thông tin, liên lạc cá nhân như: Người dùng mạng xã hội khi chia sẻ thông tin và bình luận nhạy cảm có thể bị phạt tù; các công ty nước ngoài phải lắp đặt máy chủ tại Trung Quốc chứa dữ liệu của người Trung Quốc; người dùng internet phải đăng ký các dịch vụ trên mạng với tên thật, và dự kiến gắn liền với nó là hệ thống chấm điểm công dân; các trang web không được cấp phép bị cấm đăng bất kỳ tin tức gì trên mạng...

1.2. Pháp luật Hoa Kỳ

Phát triển internet từ rất sớm, Hoa Kỳ đồng thời cũng phải đối mặt với hậu quả do tội phạm công nghệ cao gây ra. Thống kê của FBI (Cục điều tra liên bang Hoa Kỳ) cho biết, năm 2020, tội phạm trên không gian mạng gây thiệt hại cho ngành công nghiệp công nghệ thông tin nước này vào khoảng 402 tỉ USD[7] với những nhóm tội phạm có tổ chức (chuyên ăn cắp thông tin cá nhân, thẻ tín dụng và những kẻ xây dựng hệ thống mạng botnet). Các nhà lập pháp Hoa Kỳ đã ban hành các đạo luật nhằm ngăn chặn, phòng chống kịp thời hậu quả tội phạm công nghệ cao gây ra.

Thay vì sửa đổi Bộ luật Hình sự để giải thích, quy định thêm về các tội liên quan đến tội phạm công nghệ cao, Quốc hội Mỹ đã ban hành Đạo luật lạm dụng và gian lận máy tính (CFAA) năm 1986, với mục đích sửa đổi, bổ sung các quy định hiện hành còn thiếu sót trong việc xử lý hành vi gian lận máy tính, vốn đã được quy định trong Đạo luật kiểm soát tội phạm toàn diện năm 1984. Mục đích của CFAA là để bảo vệ thông tin mật, hồ sơ tài chính, thông tin tín dụng của Chính phủ và các tổ chức tài chính. Sau nhiều lần sửa đổi, đạo luật đã thêm hình phạt bổ sung cho hành vi gian lận và các hành vi khác liên quan đến kết nối và truy cập máy tính. Đạo luật cũng hình sự hóa các hành vi liên quan đến máy tính khác bao gồm các quy định xử phạt hành vi trộm cắp tài sản thông qua

7. Xem tại đường dẫn: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/.

máy tính để xử phạt những người gây thiệt hại và cố ý thay đổi dữ liệu thông tin của người khác.

Đạo luật CFAA áp dụng cho bất kỳ chủ thể nào trong phạm vi quyền tài phán của lãnh thổ Hoa Kỳ và các phán quyết, hoạt động điều tra sẽ được thi hành bởi bộ Tư pháp (DOJ), Cơ quan mật vụ Hoa Kỳ (SS) và Cục điều tra Liên bang (FBI). Đạo luật đã được sửa đổi nhiều lần nhằm theo kịp xu hướng phát triển của tội phạm công nghệ cao và gần đây nhất năm 2008. Theo đó, đạo luật cấm việc truy cập trái phép hoặc truy cập vượt quá ủy quyền để có được thông tin từ các máy tính của tổ chức tài chính, máy tính của Chính phủ Hoa Kỳ hoặc máy tính được bảo vệ; cấm các hành động khác với dữ liệu được bảo vệ hoặc hạn chế nhất định ảnh hưởng đến lợi ích quốc gia hoặc tạo lợi thế cho bất kỳ quốc gia nào. CFAA đã xử lý được rất nhiều vụ án lớn về tội phạm công nghệ cao trong nhiều lĩnh vực. Điển hình là vụ án Palpay 14[8] - do một nhóm tập thể nam nữ ẩn danh phá vỡ quyền truy cập vào trang web thanh toán Palpay (13 người trong số đó đã nhận tội trong một Tòa án ở California, Hoa Kỳ). Trong một số trường hợp, CFAA cho phép một cá nhân bị thiệt hại phải đưa ra một vụ kiện dân sự để bồi thường thiệt hại hoặc giảm nhẹ trách nhiệm đối với người vi phạm. Theo CFAA, hình phạt thấp nhất của tội phạm công nghệ cao là 01 năm và cao nhất là 10 năm; tăng nặng 20 năm trong trường hợp tội phạm chịu hai bản án. Ngoài ra, những tài sản được sử dụng để tạo điều kiện hoặc thực hiện hành vi phạm tội và tài sản mà tội phạm thu được sẽ bị tịch thu. Mặt khác, còn tồn tại một số bất cập như việc sử dụng các khái niệm công nghệ lỗi thời trong các hoạt động hàng ngày gây ảnh hưởng đến quá trình xét xử. Các định nghĩa mơ hồ của CFAA cung cấp một cách thụ động quyết định truy tố rộng rãi có thể biến hàng triệu người dùng internet hàng ngày thành tội phạm, ngay cả trong các trường hợp vi phạm phổ biến thỏa thuận điều khoản dịch vụ trực tuyến.

Bên cạnh CFAA, Luật hình sự Hoa Kỳ cũng đưa ra khung pháp lý cho tội phạm công nghệ cao. Những hành vi bị xét xử hình sự bao gồm: Truy cập bất hợp pháp vào dữ liệu lưu trữ truyền thông, trộm cắp danh tính, lừa đảo qua đường dây, qua các phương tiện truyền thông. Tòa án có thể áp dụng các bản án cao hơn 05 năm nếu hành vi phạm tội tạo điều kiện cho tội phạm buôn bán ma túy, tội phạm bạo lực hoặc hành vi khủng bố, hoặc nếu người phạm tội có tiền án. Tòa án cũng có thể ra lệnh cho người phạm tội trả tiền bồi thường cho nạn nhân của hành vi trộm cắp danh tính với số tiền bằng với giá trị mà nạn nhân nỗ lực khắc phục dự định hoặc thiệt hại thực tế gây ra bởi hành vi phạm tội.

1.3. Pháp luật Anh quốc

Là một trong những nền kinh tế lớn nhất thế giới, nổi tiếng với sức mạnh dịch vụ tài chính, khiến Vương quốc Anh trở thành mục tiêu hàng đầu cho các tin tặc

8. Aarti Shahani (2013), "US puts Internet protests on trial as part of PayPal 14 prosecution" (Tạm dịch: Các cơ quan chức năng khởi tố vụ án Paypal 14), xem tại đường dẫn: http://america.aljazeera.com/articles/2013/10/29/prosecutors-put-paypal14andinternetprotestontrial.html.

tham vọng nhất thế giới. Để nâng cao hiệu quả trong hoạt động ngăn chặn và xử lý tội phạm công nghệ cao, Vương quốc Anh vốn là quốc gia theo hệ thống thông luật (common law), chủ yếu sử dụng án lệ thì nay cũng đã xây dựng hành lang pháp luật hoàn thiện và đầy đủ nhất nhằm điều chỉnh loại tội phạm nguy hiểm này.

Đạo luật lạm dụng máy tính năm 1990[9] là đạo luật quy định rõ nhất các hành vi phạm tội của tội phạm công nghệ cao cũng như thực hiện xác định thẩm quyền, phạm vi xét xử với loại tội phạm này. Đạo luật gồm 18 điều, 03 chương. Chương 1 gồm các quy định định nghĩa hành vi bị xem là phạm tội hình sự liên quan đến công nghệ cao. Chương 2 xác định thẩm quyền của các cơ quan nhà nước trong hoạt động xử lý tội phạm công nghệ cao, đồng thời, chỉ rõ phạm vi xét xử của các cơ quan tài phán. Chương 3 là các quy định hướng dẫn dành cho các quốc gia thành viên như Scotland, Bắc Ireland trong hoạt động phối hợp nhằm nâng cao chất lượng hoạt động ngăn chặn xử lý tội phạm công nghệ cao. Các quy định trong Đạo luật bước đầu đã hạn chế được những hành vi phổ biến của tội phạm công nghệ cao như truy cập trái phép vào dữ liệu máy tính hay những hành vi gây thiệt hại nghiêm trọng. Đạo luật này đã góp phần đáng kể trong việc giảm sự gia tăng của tội phạm công nghệ cao ở Vương quốc Anh. Tuy chưa phân biệt đầy đủ các loại tội phạm mạng, nhưng được xem là vừa có tính răn đe, vừa linh hoạt nên các quốc gia khác như Canada và Cộng hòa Ireland đã dựa trên nội dung của đạo luật này để phát triển đạo luật riêng.

Năm 2015, Đạo luật lạm dụng máy tính năm 1990 đã được sửa đổi và đưa vào Đạo luật tội phạm nghiêm trọng năm 2015. Phần về tội phạm công nghệ cao được sửa đổi và đưa vào Phần II của Đạo luật. Đạo luật mới đã mở rộng phạm vi xác định hành vi phạm tội của tội phạm công nghệ cao, bao gồm cả việc cung cấp công cụ để thực hiện hành vi phạm tội, bất kể ý định cung cấp công cụ đó là gì, qua đó, việc bắt giữ cá nhân sử dụng các công cụ để thực hiện hành vi phạm tội về máy tính trở nên dễ dàng hơn. Đạo luật tội phạm nghiêm trọng năm 2015 đã mở rộng phạm vi lãnh thổ trong việc xét xử bằng cách quy định rõ hơn về "quốc tịch Anh" vào quyền tài phán. Điều này cung cấp cơ sở pháp lý vững vàng để truy tố một công dân mang quốc tịch Anh thực hiện bất kỳ hành vi phạm tội nào bên ngoài lãnh thổ, nơi không liên quan đến Vương quốc Anh, với điều kiện là hành vi phạm tội đã diễn ra ở quốc gia đó.

Nhìn chung, để bắt kịp xu hướng phát triển của tội phạm công nghệ cao về số lượng và về phương thức thủ đoạn, Vương quốc Anh cũng đã mở rộng đối tượng phạm tội, phạm vi xét xử nhằm kiểm soát tốt hơn không gian mạng, tránh bỏ lọt tội phạm, đặc biệt, trong bối cảnh phát triển mạnh mẽ của cuộc Cách mạng công nghiệp 4.0 như hiện nay.

2. Một số khuyến nghị

Thứ nhất, tiếp tục sửa đổi, bổ sung Bộ

9. Computer Misuse Act 1990 of the Parliament of the United Kingdom, xem tại đường dẫn: https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990.

luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017 có liên quan đến nhóm tội phạm công nghệ cao với những tội danh cụ thể hơn. Qua tham khảo Bộ luật Hình sự các quốc gia trên, Bộ luật Hình sự Việt Nam hiện hành cần nghiên cứu bổ sung các tội danh mới liên quan đến tội phạm công nghệ cao cũng như ban hành kịp thời các hướng dẫn thi hành nhằm giúp các cơ quan tố tụng xác định rõ hành vi vi phạm, có trách nhiệm phối hợp trong công tác phát hiện, đấu tranh, phòng ngừa và xử lý hành vi vi phạm. Nội dung sửa đổi nên phân loại tội phạm mạng/tội phạm sử dụng công nghệ cao để phục vụ công tác phát hiện, xử lý, đấu tranh và phòng ngừa loại tội phạm này cụ thể hơn; xây dựng chương riêng về tội phạm mạng/tội phạm sử dụng công nghệ cao. Đối với nhóm các tội phạm về tài chính; tuyên truyền văn hóa phẩm đồi trụy (Điều 253 Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017), cần có điều khoản tăng nặng với tội phạm sử dụng công nghệ cao để thực hiện hành vi phạm tội.

Ngoài ra, cần tiếp tục sửa đổi các quy định của Bộ luật Tố tụng hình sự, Luật giao dịch điện tử, Luật xử lý vi phạm hành chính, Luật viễn thông hiện hành... phù hợp với đặc thù và yêu cầu của công tác đấu tranh phòng, chống tội phạm công nghệ cao.

Thứ hai, tăng cường công tác phòng ngừa loại tội phạm về công nghệ thông tin. Các biện pháp phòng ngừa cơ bản bao gồm: (i) Sử dụng các công cụ kỹ thuật để ngăn chặn các vụ truy cập trái phép, lây lan virus, lấy cắp dữ liệu..., phòng ngừa, bảo vệ cho các server, website, cơ sở dữ liệu, bằng các thiết bị an ninh mạng (phần cứng), các phần mềm chống virus, spyware, spam, trojan horse...; (ii) Xây dựng các phần mềm quản trị hệ thống, phân quyền cho người sử dụng cơ sở dữ liệu phù hợp, có biện pháp bảo đảm an ninh mạng, không để bị tấn công từ bên trong; (iii) Tăng cường công tác tuyên truyền, giáo dục, phổ biến pháp luật trong lĩnh vực công nghệ thông tin (đặc biệt với đối tượng học sinh, sinh viên trong lĩnh vực công nghệ thông tin).

Thứ ba, nâng cao chất lượng đội ngũ cán bộ trực tiếp làm công tác đấu tranh phòng, chống tội phạm sử dụng công nghệ cao. Lực lượng Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao cần nghiên cứu triển khai áp dụng hình thức "tuần tra trên mạng"; cụ thể, phân công trinh sát công nghệ thông tin thường xuyên truy cập vào các trang mạng, diễn đàn công nghệ thông tin, nhất là các diễn đàn của giới tội phạm mạng công nghệ cao để chủ động tìm hiểu phương thức, thủ đoạn hoạt động của tội phạm, các công cụ, phương tiện do các đối tượng phạm tội sử dụng; tiếp tục thực hiện hiệu quả hợp tác quốc tế trong phòng, chống tội phạm công nghệ cao và đảm bảo an toàn thông tin, an ninh mạng; tranh thủ nguồn nhân lực và học hỏi kinh nghiệm của các nước trong đấu tranh phòng, chống tội phạm công nghệ cao, kinh nghiệm về quản trị, vận hành hệ thống mạng; tiếp tục đầu tư cơ sở hạ tầng, nâng cấp và hiện đại hóa các trang thiết bị nghiệp vụ, thiết bị chuyên dụng theo các dự án đã được Chính phủ phê duyệt, phù hợp với đặc điểm, tính chất công tác của lực lượng Cảnh sát phòng, chống tội phạm công nghệ cao.❐