

ĐẤU TRANH PHÒNG, CHỐNG TỘI PHẠM CÔNG NGHỆ CAO TẠI NIGERIA VÀ KINH NGHIỆM CHO VIỆT NAM

TRẦN XUÂN THIÊN AN*

Trước đây, Nigeria là một trong những quốc gia có tỉ lệ tội phạm công nghệ cao cao nhất trên thế giới. Tuy nhiên, nhờ sự quan tâm kịp thời của chính phủ Nigeria thông qua việc thực hiện hiệu quả các giải pháp như: Tăng cường việc ban hành, sửa đổi, bổ sung nhiều đạo luật; tăng mức hình phạt với từng tội danh có liên quan đến tội phạm công nghệ cao; thành lập các cơ quan chuyên môn trong lĩnh vực bảo đảm an ninh mạng, do đó loại tội phạm này trong thời gian gần đây đã được phát hiện và xử lý kịp thời.

Từ khoá: Tội phạm công nghệ cao tại Nigeria; Bộ luật Hình sự Nigeria; Đạo luật chứng cứ Nigeria.

Nhận bài: 18/11/2021; biên tập xong: 05/12/2021; duyệt bài: 12/12/2021

1. Các loại hình tội phạm công nghệ cao phổ biến ở Nigeria và hình phạt tương ứng

(1) Lừa đảo chiếm đoạt tài sản qua thư điện tử, thư rác (spam), tin nhắn văn bản (SMS):

Đây là một trong những loại hình tội phạm công nghệ cao phổ biến ở Nigeria với hình thức, nội dung, đề tài thu hút hoặc các dự án, mô hình đầu tư tài chính sinh lời

nhanh được chuyển đến bị hại - đa phần là cá nhân¹.

Tại khoản 2 Điều 12 Luật tội phạm mạng năm 2015 của Nigeria quy định mức hình phạt cho hành vi này là phạt tù, thời hạn không dưới 05 năm hoặc phạt tiền

* Khoa kiểm sát hình sự, Trường đào tạo, bồi dưỡng nghiệp vụ kiểm sát tại Thành phố Hồ Chí Minh.

không dưới 10 triệu naira hoặc cả hai hình phạt trên.

(2) Rình rập, quấy rối trên mạng:

Điều 15 Luật tội phạm mạng Nigeria năm 2015 quy định hình phạt cho tội phạm này là phạt tiền không dưới 02 triệu naira hoặc phạt tù không dưới 01 năm hoặc cả hai hình phạt trên đối với hành vi nêu tại khoản 1, hoặc phạt tù không dưới 10 năm hoặc phạt tiền không dưới 25 triệu naira hoặc cả hai hình phạt trên đối với trường hợp hành vi thuộc điểm a, b khoản 2; bị phạt tù có thời hạn không ít hơn 05 năm hoặc phạt tiền không dưới 15 triệu naira hoặc cả hai hình phạt trên đối với hành vi thuộc điểm c khoản 2 Điều này.

(3) Chiếm dụng tên miền:

Theo Điều 16 Luật tội phạm mạng Nigeria năm 2015 thì: Người nào cố ý sử dụng tên, tên doanh nghiệp, nhãn hiệu, tên miền hoặc từ, cụm từ khác được đăng ký,

1. Đối tượng phạm tội gửi e-mail nói rằng nạn nhân là người được thụ hưởng một khoản tiền, tài sản hoặc quyền tài sản được nêu trong di chúc của một người (có thể là người thân thiết hoặc không quen biết với nạn nhân) trị giá hàng trăm triệu naira (tiền Nigeria); gửi e-mail cho các nạn nhân nhằm gây quỹ và xin hỗ trợ cho các tổ chức từ thiện không tồn tại trên thực tế; tự xưng là quan chức, doanh nhân hoặc vợ, chồng của các quan chức chính phủ ở Nigeria hoặc bất kỳ quốc gia nào khác, đồng thời cam kết sẽ lợi dụng mối quan hệ của mình để giúp đỡ nạn nhân những việc họ mong muốn sau khi họ chuyển một khoản phí nhất định.

thuộc sở hữu hoặc sử dụng bởi bất kỳ cá nhân, công ty, cơ quan thuộc Chính quyền liên bang, tiểu bang hoặc chính quyền địa phương ở Nigeria, thông qua internet hoặc bất kỳ mạng máy tính nào khác, mà không có thẩm quyền hoặc quyền can thiệp sử dụng được cho phép bởi chủ sở hữu, người đăng ký hoặc người dùng trước hợp pháp là phạm tội chiếm dụng tên miền với mức án tù có thời hạn không dưới hai năm hoặc phạt tiền không dưới 05 triệu naira hoặc bị áp dụng cả hai hình phạt trên.

(4) Khủng bố mạng:

Hành vi này liên quan đến việc sử dụng mạng internet để thực hiện hành vi khủng bố hoặc kích động, tuyển mộ xây dựng lực lượng cho các cuộc tấn công khủng bố. Đây được xem là một trong những phương thức mới mà những phiến quân nổi dậy hoặc những phần tử tôn giáo cực đoan sử dụng để tuyển mộ thành viên mới và xây dựng kế hoạch chống phá an ninh quốc gia. Tội phạm này được quy định tại Điều 17 Luật tội phạm mạng Nigeria năm 2015 với mức hình phạt cao nhất lên đến chung thân.

(5) Phát tán, tàng trữ nội dung khiêu dâm trẻ em thông qua Internet:

Khoản 1 Điều 14 Luật tội phạm mạng Nigeria năm 2015 quy định: Người nào cố tình sử dụng bất kỳ máy tính hoặc hệ thống mạng nào nhằm: (a) Sản xuất nội dung khiêu dâm trẻ em nhằm mục đích phân

phối; (b) Cung cấp nội dung khiêu dâm trẻ em; (c) Phát tán hoặc truyền hình ảnh khiêu dâm trẻ em; (d) Mua bán nội dung khiêu dâm trẻ em cho chính mình hoặc cho người khác; (e) Tàng trữ nội dung khiêu dâm trẻ em trong hệ thống máy tính hoặc trên các phương tiện lưu trữ sẽ bị phạt tù với thời hạn 10 năm hoặc phạt tiền không dưới 20 triệu naira hoặc cả hai hình phạt trên (đối với trường hợp tại điểm a,b,c); bị phạt tù không dưới 05 năm hoặc bị phạt tiền không dưới 10 triệu naira hoặc cả hai hình phạt trên (đối với trường hợp tại điểm d,e).

(6) Đánh cắp danh tính và mạo danh:

Điều này đề cập đến hành vi phạm tội trộm cắp danh tính và sử dụng nhân dạng của người khác để thực hiện nhiều hành vi phạm tội khác nhau được quy định tại Điều 13 Luật tội phạm mạng Nigeria năm 2015: Bất kỳ ai trong quá trình sử dụng máy tính, hệ thống máy tính hoặc mạng nhằm: (a) Cố ý có được hoặc sở hữu thông tin nhận dạng người khác hoặc đối tượng khác với ý định lừa gạt, hoặc (b) Mạo danh đối tượng hoặc người khác, sống hoặc đã chết, nhằm mục đích: (i) Vụ lợi cho bản thân hoặc cho người khác; (ii) Chiếm đoạt tài sản hoặc bất kỳ lợi ích nào; (iii) Gây bất lợi cho đối tượng hoặc người bị mạo danh hay người khác; (iv) Nhằm tránh bị truy bắt hoặc truy tố, cản trở hoạt động điều tra sẽ bị coi là phạm tội này và bị phạt tù

không dưới 03 năm hoặc phạt tiền không dưới 07 triệu naira hoặc bị áp dụng cả hai hình phạt trên.

(7) Gian lận thẻ tín dụng (ATM, VISA, Mastercard...):

Các đối tượng phạm tội đánh cắp mã PIN của người dùng và sử dụng thẻ đã đánh cắp để rút tất cả tiền trong tài khoản hoặc tiêu xài cá nhân. Hình phạt cho hành vi này được quy định tại khoản 1 Điều 12 Luật tội phạm mạng Nigeria năm 2015 là phạt tù không dưới 03 năm hoặc phạt tiền không dưới 07 triệu naira hoặc cả hai hình phạt trên.

(8) Vi phạm bản quyền:

Đây được xem như hành vi vi phạm quyền sở hữu trí tuệ. Công nghệ kỹ thuật số và nền tảng công nghệ hiện đại ngày nay đã giúp việc sao chép các sản phẩm sáng tạo như âm nhạc, phim ảnh trở nên dễ dàng, hoàn hảo nhờ sự cung cấp miễn phí và ẩn danh của internet nhằm truyền và trao đổi những sản phẩm “lậu” trên khắp thế giới.

(9) Hack mạng:

Về bản chất, đây là hành vi xâm phạm nghiêm trọng đến quyền riêng tư, bảo mật thông tin cá nhân, cơ quan, tổ chức. Luật tội phạm mạng Nigeria năm 2015 quy định nhiều loại tội phạm liên quan đến hành vi này tại các Điều 5 - Hành vi phạm tội đối với cơ sở hạ tầng thông tin quốc gia; Điều

6 - Truy cập bất hợp pháp vào máy tính; Điều 7 - Can thiệp bất hợp pháp vào thông tin liên lạc; Điều 8 - Sửa đổi trái phép dữ liệu với khung hình phạt đa dạng từ phạt tiền, phạt tù có thời hạn, chung thân đến tử hình tương xứng với hậu quả của từng hành vi.

2. Khung pháp lý trong đấu tranh phòng, chống tội phạm công nghệ cao tại Nigeria

Luật tội phạm mạng năm 2015: Được thông qua tháng 5/2015, là đạo luật đầu tiên ở Nigeria liên quan đến an ninh mạng. Luật này buộc các văn phòng của Cơ quan cố vấn an ninh Quốc gia (NSA) và Tổng chương lý Liên bang (AGF) chịu trách nhiệm phối hợp thực thi và thành lập Hội đồng tư vấn về tội phạm mạng, Quỹ an ninh mạng Quốc gia với sự giám sát của NSA. Các hành vi phạm tội và hình phạt bao gồm: Truy cập bất hợp pháp vào máy tính (Điều 6), can thiệp bất hợp pháp vào thông tin liên lạc (Điều 12), sửa đổi dữ liệu trái phép (Điều 16), lạm dụng dữ liệu, can thiệp hệ thống (Điều 8), lừa đảo liên quan đến máy tính (Điều 14), giả mạo liên quan đến máy tính (Điều 13)... Bên cạnh đó, Luật cũng quy định cụ thể chức năng, nhiệm vụ của Hội đồng tư vấn về tội phạm mạng (Phần V), việc truy tìm, bắt giữ và truy tố (Phần VI); việc xét xử và hợp tác quốc tế (Phần VII).

Luật tổ chức Ủy ban tội phạm kinh tế và tài chính năm 2004: Ủy ban tội phạm kinh tế và tài chính (EFCC) là một cơ quan thực thi pháp luật Nigeria điều tra các tội phạm tài chính như gian lận thuế phí và rửa tiền... EFCC có thẩm quyền điều tra tất cả các tội phạm tài chính bao gồm gian lận thuế, phí, rửa tiền, làm giả, chuyển tiền bất hợp pháp, gian lận thẻ tín dụng máy tính, lừa đảo hợp đồng,... bao gồm cả các loại tội phạm có liên quan đến lĩnh vực trên thực hiện qua mạng².

Bộ luật Hình sự Nigeria: Được sử dụng để điều tra, truy tố, xét xử các loại tội phạm mạng. Hầu hết các hành vi của các đối tượng tội phạm công nghệ cao đều liên quan đến một số tội danh quy định trong Bộ luật Hình sự. Ví dụ, Điều 419 quy định: Bất kỳ người nào có thủ đoạn gian dối nhằm lừa đảo chiếm đoạt tài sản bất kỳ từ người nào khác, hoặc lừa dối khiến họ giao khác giao tài sản đều phạm tội nghiêm trọng và có thể bị phạt tù 03 năm. Mục 418 định nghĩa: Thủ đoạn gian dối là bất kỳ hành vi nào được thực hiện bằng lời nói, bằng văn bản hoặc hành vi khác - quy định này có thể hiểu bao gồm việc thực hiện hành vi khách quan thông qua không gian mạng.

Đạo luật chứng cứ Nigeria năm 2011: Lần đầu tiên bổ sung khái niệm “tài liệu,

2. Mục 6 của Luật tổ chức Ủy ban tội phạm kinh tế và tài chính.

chứng cứ” bao gồm cả chứng cứ, dữ liệu điện tử vào Điều 258 của đạo luật này. Bên cạnh đó, đạo luật cũng bổ sung một số quy định khác thừa nhận chứng cứ điện tử là một trong những bằng chứng có thể được thu thập trong quá trình giải quyết vụ việc. Điều 84 quy định: Một nội dung liên quan đến các vụ việc có trong tài liệu điện tử được trích xuất từ máy tính có thể được xem là bằng chứng; hồ sơ điện tử của sổ sách được lưu giữ trong quá trình kinh doanh cũng có thể được xem là bằng chứng.

Luật hình sự của tiểu bang Lagos về tội phạm máy tính 2011: Quy định hành vi sử dụng dữ liệu điện tử và máy tính một cách bất hợp pháp, cụ thể: Bất kỳ ai cố tình sử dụng máy tính nhằm thực hiện bất kỳ chức năng nào với mục đích truy cập trái phép vào bất kỳ chương trình hoặc dữ liệu nào được lưu giữ trong bất kỳ máy tính khác đều có tội và có thể bị phạt tù 02 năm (Điều 385); hoặc quy định về hành vi sửa đổi trái phép các tài liệu máy tính như sau: Bất kỳ ai cố ý thực hiện hành vi sửa đổi nội dung dữ liệu của bất kỳ máy tính nào đều phạm tội nghiêm trọng và có thể bị phạt tù 03 năm (Điều 387)...

Đạo luật tội phạm bưu chính viễn thông năm 1995: Điều chỉnh các giao dịch được thực hiện trên nền tảng thương mại điện tử, ví dụ, Điều 9 quy định: Nếu bất kỳ người nào không có thẩm quyền mà thực hiện

hành vi lừa đảo, cố ý tấn công, trì hoãn, chặn hoặc can thiệp vào bất kỳ vấn đề bưu chính hoặc thư điện tử nào nhằm mục đích tìm kiếm hoặc đánh cắp, phá hủy hoặc làm mất đi bất kỳ dữ liệu có liên quan sẽ được xem là có tội và có thể bị kết án tù không dưới 07 năm.

3. Một số kinh nghiệm có giá trị tham khảo cho Việt Nam

Để đáp ứng yêu cầu đấu tranh phòng, chống tội phạm công nghệ cao, Việt Nam đã ban hành Luật an ninh mạng năm 2018. Trong Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017, tội phạm công nghệ cao được quy định tại Mục 2 Chương XXI (gồm 09 điều luật). Tuy nhiên, hiện nay các hành vi sử dụng công nghệ cao ngày càng tinh vi, đe dọa tới an toàn thông tin, như: Người nước ngoài vào Việt Nam sử dụng thiết bị công nghệ cao để trộm cắp cước viễn thông, sử dụng thẻ tín dụng giả, lừa đảo; các đường dây tội phạm sử dụng công nghệ cao sau khi bị phát hiện và bị xử lý quyết liệt trong thời gian qua đã chuyển qua các phương thức, thủ đoạn mới; cá độ và đánh bạc qua mạng tiếp tục diễn biến phức tạp, điển hình là vụ án “đánh bạc nghìn tỷ” tại Phú Thọ, hay vụ án Huỳnh Ngọc Lễ sử dụng mạng internet chia tài khoản thành 6 tài khoản Agen, 32 tài khoản Member để giao cho nhiều người đánh bạc với Lễ dưới hình thức cá độ bóng

đã dựa vào các trận bóng vòng chung kết giải vô địch các quốc gia châu Âu (Euro). Từ ngày 17/6/2021 đến khi bị bắt, người chơi cá cược tổng cộng 4.350 lượt với tổng số tiền tổ chức cá cược trên 50 tỷ đồng”³. Hoạt động của tội phạm sử dụng công nghệ cao ngày càng mang đậm tính chất của tội phạm có tổ chức, xuyên quốc gia.

Để đấu tranh có hiệu quả với tội phạm sử dụng công nghệ cao trong thời gian tới, đồng thời vận dụng kinh nghiệm xử lý tội phạm công nghệ cao tại Nigeria, theo tác giả, Việt Nam có thể tham khảo thực hiện một số giải pháp cơ bản sau:

Thứ nhất, các cơ quan có thẩm quyền cần tiếp tục rà soát, nghiên cứu và đề xuất hoàn thiện các văn bản quy phạm pháp luật làm cơ sở pháp lý vững chắc cho công tác đấu tranh với tội phạm công nghệ cao tại Việt Nam, như: Bộ luật Hình sự, Bộ luật Tố tụng hình sự, Luật an ninh mạng... Bên cạnh đó, Bộ luật Hình sự cần kịp thời quy định những hành vi nguy hiểm mới phát sinh trong xã hội, có tính nguy hiểm cao, nhất là nghiên cứu đưa pháp nhân thương mại trở thành

chủ thể của nhóm tội phạm này⁴.

Cần ban hành các văn bản dưới luật về công tác đấu tranh phòng ngừa và chống tội phạm, các hành vi vi phạm khác trong lĩnh vực sử dụng công nghệ cao, trong đó, cần nghiên cứu giao cho Viện kiểm sát nhân dân tối cao chủ trì, phối hợp với các bộ, ngành hữu quan như: Bộ Công an, Tòa án nhân dân tối cao, Bộ Tư pháp, Bộ Thông tin và Truyền thông, Ngân hàng Nhà nước xây dựng Thông tư liên ngành về phòng, chống tội phạm sử dụng công nghệ cao; chủ trì, phối hợp xây dựng Thông tư liên ngành giữa Bộ Công an, Viện kiểm sát nhân dân tối cao và Tòa án nhân dân tối cao hướng dẫn điều tra, truy tố, xét xử đối với 09 tội danh liên quan đến lĩnh vực sử dụng công nghệ cao trong Bộ luật Hình sự năm 2015⁵.

Thứ hai, cần đẩy mạnh công tác tuyên truyền, giáo dục phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao trong quần chúng nhân dân; đặc biệt là đối với các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ Internet, viễn thông; các doanh nghiệp hoạt động trong lĩnh vực tài chính, ngân hàng, thanh toán điện tử và thương mại điện tử. Thông qua các cơ quan thông tấn, báo chí tuyên truyền, cảnh báo

3. https://congan.com.vn/tin-chinh/nhung-thach-thuc-trong-dau-tranh-voi-toi-pham-cong-nghe-cao-va-an-ninh-mang_116033.html, truy cập ngày 11/11/2021.

4. Điều 20 Luật tội phạm mạng Nigeria năm 2015 quy định pháp nhân phạm tội theo Luật này phải chịu trách nhiệm hình sự với mức phạt không dưới 10 triệu naira...

5. Lê Thị Hồng Xuân, Nguyễn Thị Thùy Linh, *Tội phạm mạng trong kỷ nguyên cách mạng công nghiệp 4.0*, Tạp chí Tòa án nhân dân, số 18 (9/2018).

các phương thức, thủ đoạn hoạt động phạm tội sử dụng công nghệ cao, cũng như kết quả đấu tranh với các vụ việc, vụ án điển hình để răn đe, nâng cao ý thức cảnh giác cho người dân. Duy trì các hòm thư tố giác tội phạm, số điện thoại “đường dây nóng”, trực ban hình sự để kịp thời tiếp nhận, xử lý thông tin về tội phạm sử dụng công nghệ cao. Đồng thời cảnh báo, phòng ngừa việc lạm dụng, thiếu hiểu biết pháp luật dẫn đến vi phạm pháp luật trong sử dụng công nghệ cao, nhất là giới học sinh, sinh viên.

Thứ ba, tăng cường thanh tra, kiểm tra liên ngành, kiểm soát việc cấp, bán tên miền quốc gia “.vn”, việc cấp giấy xác nhận đối với các trang mạng xã hội, các trang web có tên miền trong nước, xử lý nghiêm đối với chủ sở hữu các trang mạng có sai phạm⁶.

Thứ tư, xây dựng, đào tạo đội ngũ cán bộ có trình độ cao về công nghệ thông tin trong các cơ quan tiến hành tố tụng; kiện toàn tổ chức bộ máy và triển khai thành lập các đơn vị phòng, chống tội phạm sử dụng công nghệ cao trực thuộc các phòng chức năng ở các tỉnh, thành phố trực thuộc trung ương nhằm xây dựng một hệ thống lực lượng phòng, chống tội phạm trên phạm vi toàn quốc. Đồng thời, tăng cường đầu tư

trang thiết bị công nghệ đáp ứng yêu cầu bảo đảm an ninh, an toàn thông tin mạng trong tình hình mới.

Thứ năm, tăng cường hợp tác quốc tế, chia sẻ kinh nghiệm trong lĩnh vực đấu tranh phòng, chống tội phạm sử dụng công nghệ cao; tập trung trao đổi thông tin tội phạm, tranh thủ tài trợ của các chính phủ, các tổ chức phi chính phủ trong việc đầu tư, mua sắm trang thiết bị kỹ thuật, công nghệ hiện đại; tăng cường phối hợp với các đơn vị có liên quan tương ứng ở nước ngoài để giải quyết các yêu cầu phát hiện, xác minh, điều tra tội phạm một cách kịp thời, triệt để. □

Tài liệu tham khảo:

1. Bộ luật hình sự Nigeria.
2. Bộ luật Hình sự Việt Nam năm 2015 (sửa đổi, bổ sung năm 2017).
3. Luật tội phạm mạng Nigeria năm 2015.
4. Đạo luật chứng cứ Nigeria năm 2011.
5. Luật hình sự của tiểu bang Lagos về tội phạm máy tính 2011.
6. Đạo luật tội phạm buru chính viễn thông năm 1995.
7. Dr. Ibikunle Frank ft Eweniyi Odunayo, Approach to cyber security issues in Nigeria: Challenges and Solution, Department of Electrical & Information Engineering, Covenant University, Nigeria;
8. Fasuyi Olayiwola Gamaliel, The legal framework prohibiting cybercrimes in Nigeria, University of Lagos, Nigeria.

6. Anh Đức, <https://thitruongtaichinhvientien.vn/giai-phap-chong-toi-pham-cong-nghe-cao-23595.html>, truy cập ngày 11/11/2021.