

THỦ ĐOẠN SỬ DỤNG CÁC ỨNG DỤNG MẠNG CÔNG NGHỆ THÔNG TIN, TRUYỀN THÔNG ĐỂ PHẠM TỘI MUA BÁN NGƯỜI VÀ VIỆC PHÒNG NGỪA, PHÁT HIỆN, XỬ LÝ

NGUYỄN ĐỨC HẠNH*

Trong những năm gần đây, bên cạnh cách thức tổ chức và thực hiện tội phạm truyền thống của tội phạm mua bán người, các đối tượng còn sử dụng các phương tiện, công nghệ thông tin truyền thông trong việc chuẩn bị thực hiện tội phạm, tổ chức thực hiện tội phạm và che giấu tội phạm. Điều này khiến mức độ nguy hiểm của tội phạm tăng lên, số lượng người bị hại nhiều hơn, sau khi thực hiện tội phạm để trốn tránh pháp luật hơn. Vì vậy, yêu cầu trong việc nghiên cứu thủ đoạn phạm tội giúp phòng ngừa, phát hiện tội phạm ứng dụng mạng công nghệ thông tin và truyền thông là hết sức cần thiết, cấp bách hiện nay.

Từ khóa: Tội phạm mua bán người; công nghệ thông tin; phòng, chống mua bán người.

Ngày nhận bài: 22/6/2021; Biên tập xong: 28/6/2021; Duyệt đăng: 30/6/2021

In recent years, in addition to the traditional modes of organizing and carrying out human trafficking, criminals also use technology to facilitate, organize and hide their illegal activities. This increases the seriousness of the crimes and the number of victims. Also, after committing the crimes, with the support of technology, it is easier for criminals to abscond the law. This article explores how human traffickers use technology to expand their networks, and how technology can be used to prevent, detect and handle trafficking in persons cases.

Keywords: Human trafficking crimes, information technology, human trafficking prevention.

Tội phạm mua bán người (MBN) trong những năm gần đây diễn biến phức tạp với tính chất, quy mô và thủ đoạn hoạt động phạm tội ngày càng tinh vi, xảo quyệt, có tổ chức chặt chẽ giữa người mua và người bán, môi giới, dẫn dắt, hình thành các đường dây tội phạm liên tỉnh và xuyên quốc gia. Tội phạm MBN đã được phát hiện xảy ra trên phạm vi 63 tỉnh, thành phố; nạn nhân không chỉ là phụ nữ, trẻ em mà đã xuất hiện tình trạng mua bán nam giới, trẻ sơ sinh, bào thai, mua bán nội tạng, đẻ thuê...¹ Mặc dù giảm về số lượng bị phát hiện, xử lý nhưng tình hình tội phạm

MBN vẫn diễn biến phức tạp, thủ đoạn tội phạm hết sức tinh vi, xảo quyệt với sự tham gia của các đối tượng được tổ chức thành đường dây; có sự phân công, phối hợp chặt chẽ và rất chuyên nghiệp gây khó khăn cho các cơ quan chức năng trong quá trình điều tra, truy tố².

Bên cạnh cách thức tổ chức và thực hiện tội phạm truyền thống, các đối tượng MBN còn sử dụng các phương tiện, công nghệ thông tin truyền thông trong việc chuẩn bị thực hiện tội phạm, tổ chức thực hiện tội phạm và che giấu tội phạm khiến mức độ nguy hiểm

¹ Báo cáo Bộ Công an “Tình hình thực hiện pháp luật về phòng chống mua bán người giai đoạn 2012-2017”.

* Phó Giáo sư, Tiến sĩ, Phó Hiệu trưởng Trường Đại học Kiểm sát Hà Nội

² Báo cáo Ban chỉ đạo 138/CP năm 2019.

của tội phạm tăng lên, số lượng người bị hại nhiều hơn, sau khi thực hiện tội phạm để trốn tránh pháp luật hơn. Ví dụ như việc các đối tượng phạm tội sử dụng Internet để tìm kiếm, phát hiện nạn nhân; sử dụng điện thoại di động, Email, Facebook, Zalo... để liên lạc đưa nạn nhân di chuyển trong lãnh thổ, ra nước ngoài; sử dụng chứng minh thư giả để mở tài khoản, dùng hình thức thanh toán trực tuyến chuyển và rút tiền; lập các trang web đen để quảng cáo, tiếp thị, tìm kiếm khách hàng; giả danh lực lượng chức năng để lừa gạt, cưỡng ép nạn nhân nhằm bán sang biên giới³. Thậm chí, có những trường hợp dùng tên, hình ảnh đại diện giả trên Facebook mặc lễ phục Công an, Bộ đội Biên phòng làm quen, kết bạn và lừa bán nạn nhân bên cạnh chiêu trò lừa đảo yêu đương...

Để góp phần nâng cao hiệu quả phát hiện, xử lý tội phạm MBN có sử dụng công nghệ thông tin, truyền thông, bài viết trình bày, phân tích những yếu tố của mạng thông tin, truyền thông mà các đối tượng phạm tội MBN có thể khai thác, thực hiện tội phạm cũng như những nội dung liên quan đến việc sử dụng công nghệ thông tin, truyền thông để phòng ngừa và chống tội phạm MBN. Từ đó, tác giả đưa ra một số kiến nghị, đề xuất nhằm nâng cao năng lực phòng ngừa, phát hiện và xử lý tội phạm MBN có sử dụng công nghệ thông tin, truyền thông.

³ Ngày 10/9/2020, Công an Lào Cai khởi tố Sùng A Chó (SN 1991, trú tại xã Mường Toong, huyện Mường Nhé, tỉnh Điện Biên); Thảo Seo Hòa (SN 1976, trú tại huyện Hàm Yên, tỉnh Tuyên Quang); Chang A Vương (SN 1987, trú tại huyện Tam Đường, tỉnh Lai Châu) cùng đồng bọn về 02 hành vi mua bán người và mua bán người dưới 16 tuổi.

1. Một số yếu tố gắn với mạng công nghệ thông tin, truyền thông mà các đối tượng phạm tội mua bán người thường khai thác sử dụng trong việc thực hiện hành vi phạm tội

- Mạng thông tin, truyền thông có khả năng giúp cho việc giao tiếp, trao đổi thông tin giữa người dùng với tốc độ cao, dễ dàng vượt qua biên giới quốc gia mà không chịu sự kiểm soát của các cơ quan chức năng. Lợi dụng đặc điểm này, các đối tượng phạm tội MBN đã sử dụng mạng thông tin, truyền thông để kết nối với các nạn nhân trên khắp các quốc gia và vùng lãnh thổ trên thế giới.

- Việc thiết lập và sử dụng các trang web bất hợp pháp dễ dàng, các hồ sơ trực tuyến ẩn danh, các thiết bị dùng một lần luôn sẵn có đã tạo điều kiện thuận lợi cho việc che giấu các giao tiếp, giao dịch thông qua môi trường mạng khi các mạng lưới tội phạm được thực hiện, giúp các đối tượng này dễ dàng che giấu tội phạm, trốn tránh sự phát hiện của cơ quan chức năng. Do đó, các đối tượng MBN thường khai thác triệt để yếu tố này để tiếp cận nạn nhân, tránh sự phát hiện, can thiệp của gia đình và cơ quan chức năng.

- Việc phát hiện, thu thập dữ liệu điện tử để có chứng cứ chứng minh hành vi phạm tội thông qua môi trường mạng đòi hỏi phải có các nguồn lực và thiết bị công nghệ thông tin, truyền thông hiện đại. Vì vậy, với các quốc gia kém phát triển và đang phát triển (thường là các quốc gia có nạn nhân bị mua bán), đây là một thách thức không nhỏ khiến các đối tượng MBN không ngừng khai thác tính năng này khi thực hiện tội phạm.

- Thủ đoạn phổ biến mà các đối tượng phạm tội MBN có thể khai thác, sử dụng công nghệ thông tin, truyền thông khi thực hiện các hành vi phạm tội là:

+ Thông qua mạng thông tin, truyền thông, các đối tượng MBN dễ dàng tìm kiếm, xác định các khu vực có thể có nạn nhân để tuyển mộ, khống chế, kiểm soát khi vận chuyển, chứa chấp, tiếp nhận và chuyển giao. Việc sử dụng công nghệ thông tin của các đối tượng tội phạm có thể từ những giai đoạn đầu tiên nhằm xác định những nạn nhân tiềm năng thông qua các quảng cáo trên mạng đến những giai đoạn cuối cùng là che giấu hành vi phạm tội. Rửa tiền có thể được thực hiện từ hành vi phạm tội này.

+ Việc sử dụng công nghệ có thể áp dụng cho tất cả các hình thức MBN như Internet giúp cho những đối tượng MBN có thể tiếp cận với số lượng lớn các nạn nhân tiềm năng so với việc thực hiện thông qua điện thoại, tin nhắn, liên hệ trực tiếp.

+ Các thủ đoạn tuyển mộ của những đối tượng MBN có thể được thực hiện thông qua sử dụng các trang web để thiết lập liên hệ ban đầu với nạn nhân trên phạm vi rộng, nhiều nhóm người dùng Internet. Các trang web này có thể giúp trò chuyện, trao đổi thông tin dưới dạng tin nhắn, văn bản, video, trao đổi hình ảnh, hẹn hò và các hoạt động khác. Ngoài ra, những diễn đàn mạng cũng cung cấp cho kẻ mua bán người thông tin về các lỗ hổng từ máy tính của nạn nhân, cơ sở dữ liệu của nạn nhân để có thể khai thác nhằm lấy được lòng tin và sự tự tin của nạn nhân.

+ Trên các trang web và ứng dụng mạng xã hội, các đối tượng MBN có thể

ngghiên cứu, tìm hiểu về nạn nhân và dễ dàng theo dõi những lượt thích và không thích. Điều này giúp những đối tượng MBN có thể điều chỉnh cách tiếp cận với từng nạn nhân và khai thác điểm yếu của nạn nhân. Nắm bắt nhu cầu lao động, các nạn nhân có thể được tuyển mộ thông qua các lời mời làm việc, thường là thông qua các trang web tuyển dụng giả mạo, quảng cáo trực tuyến, các cơ quan tuyển dụng giả hay thông qua các trang mạng xã hội.

+ Các đối tượng MBN thường xác định nạn nhân nhờ điện thoại thông minh (smartphone) bởi hầu hết ở các quốc gia, điện thoại thông minh đều có khả năng truy cập Internet. Trong khi tùy thuộc vào kiến thức của người dùng mà việc sử dụng các cài đặt quyền riêng tư, bảo mật là rất khác nhau, nhiều nạn nhân không biết cách cài đặt nên đã bị các đối tượng phạm tội có thể khai thác, lấy cắp thông tin và tìm cách tiếp cận. Các ứng dụng, phương tiện truyền thông xã hội và các nền tảng trực tuyến khác cung cấp cho những đối tượng MBN quyền truy cập vào một loạt thông tin hữu ích có thể được sử dụng nhằm đánh lừa nạn nhân, bao gồm: Dữ liệu về vị trí, thông tin chi tiết nhận dạng, lối sống, thói quen, hình ảnh, địa chỉ liên lạc... Ở các quốc gia phát triển, điện thoại thông minh được thanh thiếu niên sử dụng phổ biến và trong một số trường hợp, các ứng dụng trong điện thoại thông minh đã giúp các đối tượng phạm tội dễ tiếp cận và khống chế các nạn nhân nhỏ tuổi hơn.

Dưới đây là bảng thông tin tổng quan về các trang web tuyển dụng và kết nối thường được những đối tượng MBN sử dụng:

	Xem & bình luận trang web	Các địa điểm chuyển đổi	Các trang web	Các trang web quảng cáo và bán hàng
Các trang web thường được sử dụng	Facebook, Instagram (đăng ảnh lên trang cá nhân của chúng, có thể bình luận về ảnh khác, nhận tin nhắn riêng tư và có tài khoản thứ hai mà cha mẹ không biết gọi là “finstagram” hoặc instagram giả), Snapchat (nhắn tin và đăng ảnh công khai, biến mất sau khi đã mở và chức năng chia sẻ tin nhắn/hình ảnh/video riêng tư)	Tinder (ứng dụng hẹn hò để trò chuyện với những người bạn phù hợp, tin nhắn riêng tư để liên lạc, gặp gỡ và hẹn hò); Blindr (ứng dụng hẹn hò với trò chuyện riêng tư, định vị GPS để định vị người khác); WhatsApp (ứng dụng nhắn tin được mã hóa nơi các nhà cung cấp dịch vụ không lưu bản sao tin nhắn của họ trên máy chủ và chỉ hai người đang giao tiếp mới có thể truy cập các tin nhắn đó); KIK (ứng dụng nhắn tin không được kết nối với số điện thoại, tin nhắn không được lưu trên máy chủ để truy cập bên ngoài cuộc trò chuyện).	Trò chuyện roulette hoặc Omegle (webcam với người lạ một cách riêng biệt, người dùng có thể xoay qua nhiều người lạ và webcam có hộp trò chuyện riêng tư dưới màn hình webcam)	Hướng dẫn thành phố (rao vặt, trang đi kèm với quảng cáo) Skipthegames, Bedpage (đi kèm trang web với cá nhân quảng cáo dịch vụ) Seekingarrangement (hẹn hò, trang web thông tin tương tự như hồ sơ hẹn hò có nhắn tin); Sugar-baby (trang web quảng cáo cho cô gái có hồ sơ cho các johns / sugar daddies duyệt và nhắn tin)
Các trang web ít phổ biến hơn	YikYak (đăng bài ẩn danh với phần bình luận, vị trí GPS cho phép người khác xác định vị trí của người dùng trong một bán kính nhất định); Whisper (đăng bài ẩn danh với khả năng bình luận và gửi tin nhắn ẩn danh cho người dùng)	Màu vàng (ứng dụng hẹn hò / bạn bè dành cho giới trẻ có chức năng vuốt, “tinder cho trẻ em”); # 1 Chat Avenue (phòng trò chuyện dành cho trẻ em với người lạ trong một nhóm lớn, một người có thể nhắn tin trong một nhóm lớn hoặc nhắn tin riêng tư)	Monkey (webcam với người lạ trong số giây có hạn, thanh niên cần tìm người dùng khác làm bạn trong thời gian không giới hạn, được quảng cáo dành riêng cho giới trẻ)	Các trang web ít phổ biến hơn không thể xác định vì đã có nhiều thay đổi
Quá trình	Những đối tượng MBN có thể thực hiện các thao tác thông qua mạng như thích, nhận xét, đề nghị kết bạn và thu thập thông tin mà sau đó sử dụng để tuyển mộ và thu hút thanh niên.	Trò chuyện với người trẻ, có thể sau khi thu thập thông tin trên một trang web xem và nhận xét. Việc tán tỉnh, gạ gẫm có thể xảy ra trên các ứng dụng và trang web nhắn tin này, thuyết phục ai đó gửi một bức ảnh nhạy cảm và sau đó sử dụng nó để tống tiền họ.	Lấp các lỗ hổng, xây dựng lòng tin và khiến họ chia sẻ nhiều hơn về cơ thể của họ bằng hình ảnh. Di chuyển chúng từ trang được giám sát sang trang ít được giám sát hơn.	Chuyển họ từ chia sẻ sang bán ảnh trực tuyến của chính họ.

Nguồn: Ryan Kunz, Meredith Baughman, Rebecca Yarnell and Celia Williamson (2018), Social Media and Sex Trafficking Responses, University of Toledo

- Một xu hướng liên quan khác trong việc tuyển mộ nạn nhân là việc sử dụng các nền tảng chơi game trực tuyến. Máy chơi game tiên tiến cung cấp chức năng tương tự như máy tính để bàn và ngày càng được sử dụng nhiều hơn trong các vụ phạm tội. Bên cạnh đó, còn xuất hiện những thủ đoạn khác như:

+ Việc kiểm soát, khống chế nạn nhân có thể diễn ra dưới nhiều hình thức, trong đó có ép buộc, dụ dỗ và đưa các nạn nhân rời khỏi nhà của họ, kiểm soát tài chính và tổng tiền. Các đối tượng MBN sử dụng công nghệ để tránh tiếp xúc trực tiếp với nạn nhân. Đây cũng là thách thức khiến việc điều tra tội phạm MBN ngày càng trở nên khó khăn hơn. Tuy nhiên, “kiểm soát ảo” nạn nhân là một công cụ phổ biến. Việc kiểm soát có thể bao gồm theo dõi nạn nhân thông qua kiểm tra thủ công hồ sơ điện thoại hoặc truy cập các ứng dụng điện thoại thông qua các ứng dụng dựa trên đám mây hoặc bằng cách triển khai phần mềm gián điệp. Ngay cả sau khi nạn nhân không còn nằm trong tầm kiểm soát của những đối tượng MBN (ví dụ như họ đã trốn thoát được), họ vẫn có thể bị theo dõi bằng các ứng dụng theo dõi vị trí trên điện thoại di động của mình. Những đối tượng MBN cũng có thể gửi thông tin liên lạc đe dọa đến những nạn nhân tìm cách trốn thoát nhằm duy trì hoặc giành lại quyền kiểm soát họ.

+ Sử dụng mạng để lừa đảo, đe dọa và thực hiện hành vi gian dối khác có thể được những đối tượng MBN áp dụng khi có được những thông tin có thể gây tổn hại cho nạn nhân (hình ảnh hoặc video) như một phương tiện để giành quyền khống chế, kiểm soát. Ví dụ, bằng cách hứa hẹn công việc người mẫu và yêu cầu chụp ảnh khỏa thân từ các người mẫu, các đối tượng đưa ra những lời đe dọa. Điều

này không đòi hỏi phải có sự tiếp xúc trực tiếp giữa những kẻ MBN và nạn nhân mà mọi thứ có thể đạt được trong không gian ảo. Một thủ đoạn khác là những đối tượng MBN chiếm đoạt mạng xã hội của nạn nhân và thêm nội dung gợi ý sự đồng ý khai thác, cùng với nội dung khiêu dâm để làm tổn hại danh tiếng và uy tín của nạn nhân hoặc xâm nhập giả tạo tư cách người khiếu nại, khiến tài khoản của họ bị nhà cung cấp dịch vụ đóng, bị cô lập, mất danh tính kỹ thuật số và mất liên lạc với gia đình và cộng đồng.

+ Thông qua mạng Internet, các đối tượng MBN rao bán người trực tuyến với những quảng cáo được đăng tải trên các trang web không chính thống, nội dung thường được bảo vệ bằng mật khẩu và mã hóa. Hành vi này đã được sử dụng cho các hoạt động bất hợp pháp và gây ra những cản trở không nhỏ đối với hoạt động điều tra của cơ quan tố tụng về hành vi MBN. Trường hợp khác, đối tượng phạm tội cũng có thể rao bán người trên các trang web thông thường khác bằng cách núp dưới dạng dịch vụ mát-xa với việc sử dụng tiếng “lóng”. Ví dụ: Biểu tượng cảm xúc (chẳng hạn như hoa anh đào để xác định nạn nhân là một trinh nữ) và các cụm từ khác trong mô tả của các quảng cáo ngấm hiểu làm hoạt động mại dâm (ví dụ: “trải nghiệm bạn gái”) hoặc trẻ vị thành niên được quảng cáo với cụm từ “tôi có một người bạn trẻ hơn”.

+ Lợi nhuận mà các đối tượng MBN có được có thể chuyển dưới dạng tiền điện tử như đồng tiền điện tử Bitcoin để dễ thanh khoản, dễ cất giấu hơn so với tiền tệ thật bởi chúng không bị quản lý và không được hỗ trợ bởi các ngân hàng. Mặt khác, các đối tượng sử dụng tiền kỹ thuật số sẽ không bị phụ thuộc vào biên giới quốc gia và có thể phục vụ trao đổi với cả các tổ

chức tội phạm khác, thực hiện các loại tội phạm khác không phải MBN. Các loại tiền kỹ thuật số mà các đối tượng phạm tội có được không cần phải thực hiện hành vi rửa tiền, vốn khó khăn hơn ở hầu hết các quốc gia do các quy định về báo cáo tiền mặt ngày càng nghiêm ngặt và tuân thủ quy định chống rửa tiền. Các khoản tiền ở dạng kỹ thuật số có thể được vận chuyển qua biên giới một cách dễ dàng, do đó vượt qua giới hạn chuyển tiền mặt giữa các khu vực pháp lý. Việc sử dụng nhiều “ví tiền” kỹ thuật số (mỗi ví tiền riêng cho mỗi giao dịch) tạo thêm thách thức cho cảnh sát và cơ quan chống rửa tiền trong việc theo dõi và giám sát các giao dịch. Các loại tiền kỹ thuật số cung cấp tính ẩn danh tương đối. Việc sử dụng tiền điện tử liên quan đến các yếu tố khác chẳng hạn như “nhà giao dịch tiền điện tử”, “người trộn tiền điện tử”, “người trao đổi tiền điện tử” và “sàn giao dịch tiền điện tử”... Nếu các nhà hoạch định chính sách và thực thi pháp luật trên toàn cầu chưa bổ sung các quy định điều chỉnh quan hệ này thì việc điều tra, xử lý sẽ gặp phải nhiều thách thức.

- Sử dụng công nghệ trong thực hiện hành vi đưa người di cư trái phép trước khi thực hiện hành vi phạm tội MBN

+ Theo số liệu của Ủy ban Châu Âu, năm 2016, “việc sử dụng mạng xã hội để thực hiện việc đưa người di cư trái phép đã tăng trưởng theo cấp số nhân trong những năm gần đây”. Năm 2016, 10 quốc gia thành viên Liên minh Châu Âu (EU) đã xác nhận mạng xã hội được sử dụng để quảng cáo các dịch vụ đưa người di cư trái phép, cung cấp thông tin về các tuyến đường di cư và tạo điều kiện giao tiếp giữa những đối tượng thực hiện hành vi đưa người di cư trái phép và các nạn nhân. Năm 2017, Cao ủy Liên Hợp Quốc về người tị nạn (UNHCR) đã công

bố nghiên cứu về việc sử dụng mạng xã hội của người nói tiếng Ả Rập, cũng như người tị nạn và di cư Afghanistan. Các nhà nghiên cứu đã theo dõi hàng trăm trang Facebook trong khoảng thời gian 10 tháng, ghi lại dữ liệu định tính về trao đổi thông tin giữa những người di cư, lời đề nghị của những kẻ tổ chức đưa người di cư trái phép - đối tượng rất dễ trở thành nạn nhân của tội phạm MBN và trên thực tế đã có nhiều người di cư trái phép trở thành nạn nhân của tội phạm MBN.

+ Đối với việc quảng cáo đưa người di cư trái phép, các đối tượng phạm tội có thể chọn tiếp thị dịch vụ của họ trực tuyến thông qua các trang mạng xã hội và quảng cáo “truyền miệng” giữa người di cư hay những đối tượng tổ chức sử dụng điện thoại thông minh. Những đối tượng phạm tội quảng cáo dịch vụ trên Facebook giống như “bất kỳ công ty du lịch hợp pháp nào”. Nghiên cứu của UNHCR năm 2017 cho thấy, có hàng trăm trang Facebook cung cấp cả dịch vụ hợp pháp và bất hợp pháp với đầy đủ thông tin liên lạc. Công nghệ giúp các đối tượng phạm tội tiếp cận nạn nhân trong phạm vi cộng đồng rộng lớn hơn mà không nhất thiết các đối tượng này phải có sự hiện diện thực tế. Sau khi những người di cư tự mình di chuyển ra nước ngoài, các đối tượng MBN tiếp tục thực hiện các công đoạn phạm tội khác như cách truyền thống.

+ Điện thoại thông minh, email, nền tảng mạng xã hội và ứng dụng được những đối tượng phạm tội sử dụng để liên lạc với người di cư và cho phép chúng tạo điều kiện thuận lợi hơn cho quá trình đưa người qua biên giới, phản ứng, đối phó với các cơ quan chức năng dễ hơn. Thậm chí, những đối tượng đưa người di cư trái phép không phải đi cùng những người di cư qua lại giữa các biên giới. Giao

tiếp điện tử cũng cho phép những người di cư trái phép (và những người chuẩn bị di cư trái phép) biết được các thông tin của những kẻ tổ chức thông qua các trang mạng xã hội trực tuyến, mức độ an toàn của tuyến đường sẽ được sử dụng, mong muốn của quốc gia đến và tình hình kiểm soát biên giới.

+ Bên cạnh việc thanh toán bằng tiền mặt thông qua sử dụng người bảo lãnh là bên thứ ba (thành viên gia đình) thì phương thức thanh toán còn có thể được thực hiện bằng trả góp trên các hệ thống thanh toán trực tuyến. Tiền điện tử có thể giúp những đối tượng phạm tội và các nhóm tội phạm có tổ chức dễ dàng nhận việc thanh toán, cất giấu và chuyển tiền, hỗ trợ rửa tiền hay chuyển tiền qua biên giới quốc gia mà tránh bị chính quyền điều tra và bắt giữ bởi tiền điện tử có tính năng ẩn danh; mặt khác, giúp người di cư không cần thiết phải mang theo số lượng lớn tiền mặt.

+ Những đối tượng tổ chức đưa người di cư trái phép và người di cư cũng có thể sử dụng công nghệ thông tin và truyền thông để cung cấp, trao đổi thông tin khi tội phạm được chuẩn bị thực hiện. Ví dụ: Xác định các loại dịch vụ được cung cấp, thời gian, ngày tháng và giá cả của dịch vụ, nghiên cứu biên giới nào có tình hình an ninh lỏng lẻo/nghiêm ngặt hơn và thời gian đến trong ngày để thu hút ít sự chú ý nhất...

+ Công nghệ trong chừng mực nhất định làm mờ ranh giới giữa người nhập cư trái phép và đối tượng tổ chức di cư trái phép.

2. Việc sử dụng công nghệ thông tin, truyền thông để phòng ngừa và phát hiện, xử lý tội phạm mua bán người

- Những tiến bộ trong công nghệ, đặc biệt là công nghệ truyền thông thông tin

nhờ điện thoại thông minh và Internet đã được các đối tượng phạm tội MBN tận dụng triệt để, tạo ra rào cản, khó khăn, thách thức trong việc phát hiện và điều tra. Tuy nhiên, sự phát triển này cũng góp phần không nhỏ trong việc giúp các cơ quan tố tụng khai thác tính năng, tác dụng nhằm ngăn chặn, phát hiện tội phạm MBN như:

+ Công nghệ ngày càng được ứng dụng, triển khai mạnh mẽ trong việc giúp quản lý đường biên giới, cửa khẩu tại các khu vực biên giới. Hỗ trợ các cơ quan thực thi pháp luật, cơ quan tố tụng phát hiện những đối tượng di chuyển trái phép qua biên giới, hơn nữa giúp ghi lại, lưu trữ, phân tích và trao đổi thông tin liên quan đến các nạn nhân bị mua bán.

+ Các dữ liệu điện tử cung cấp các chứng cứ chứng minh hành vi phạm tội như sự biến động tài khoản ngân hàng, dữ liệu trong điện thoại, hình ảnh, âm thanh lưu trữ được trong các thiết bị kỹ thuật số. Những thông tin khác có được trên mạng xã hội như hình ảnh, video, địa chỉ liên hệ, vị trí và thông tin khác, lịch sử trình duyệt trên máy tính cá nhân và địa chỉ IP là nguồn chứng cứ rất quan trọng.

+ Các lực lượng chức năng có thể tạo các bẫy tội phạm có tổ chức hoạt động trực tuyến và có thể cho phép thu thập bằng chứng kỹ thuật số như một phần của cuộc điều tra. Trở ngại chính đối với các cuộc điều tra là áp lực về thời gian tiến hành điều tra phải nhanh chóng, kịp thời nên công nghệ có thể được tận dụng giúp giảm thời gian xác định đối tượng phạm tội và nạn nhân. Ví dụ, chatbot có thể được sử dụng để tham gia vào các cuộc trò chuyện với hàng nghìn kẻ lạm dụng trực tuyến cùng một lúc.

+ Dữ liệu GPS có thể được sử dụng để theo dõi vị trí và lịch sử thiết bị phục vụ hoạt động điều tra.

+ Các tổ chức chống MBN sử dụng các nền tảng truyền thông xã hội, ví dụ như Facebook và Twitter để truyền đạt thông tin về tội phạm MBN, đăng thông tin hoặc liên kết với các tổ chức khác có mục tiêu tương tự, tạo cơ hội cho mọi người dân trong xã hội tham gia vào các chiến dịch phòng ngừa và chống MBN. Các tổ chức này cũng sử dụng các nền tảng chia sẻ video (chẳng hạn như YouTube) để giáo dục người dân về tội phạm MBN. Ví dụ: Dự án Polaris - một tổ chức phi chính phủ hoạt động để chống lại và ngăn chặn nạn MBN - sử dụng các nền tảng chia sẻ video và truyền thông xã hội để nâng cao nhận thức, đồng thời ra mắt dịch vụ nhắn tin (BeFree) hoạt động 24/7 để hỗ trợ nạn nhân của tội phạm MBN được giải cứu và sống sót.

+ Cơ chế thông tin cho nhân chứng và nạn nhân qua điện thoại hoặc Internet đã được thiết lập để giúp đỡ những người từ nước ngoài đến làm việc ở nước khác hiểu được mình có đang thuộc dạng đối tượng bị bóc lột hay không.

+ Các biện pháp điều tra sử dụng mạng thông tin, truyền thông giúp xác định vị trí của các đối tượng phạm tội và nạn nhân. Ví dụ: Bahrain đã phát thẻ SIM cho người lao động khi đến nước này nhằm giúp người lao động có thể sử dụng tin nhắn văn bản để liên hệ với cơ quan quản lý ngay lập tức nếu có vấn đề liên quan đến lao động của họ. Những cách tiếp cận như vậy cũng cho phép Nhà nước theo dõi người di cư.

+ Thông qua mạng viễn thông giúp cho các cơ quan chức năng thu thập được các dữ liệu hỗ trợ việc phát hiện, điều tra

và truy tố các đối tượng phạm tội, đồng thời có thể hỗ trợ và dự đoán các hình thức tội phạm cũng như dự đoán các hoạt động với mục đích phòng, chống tội phạm. Dữ liệu được thu thập có thể giúp tăng cường hợp tác điều tra ở cấp quốc gia và đa quốc gia. Khi có sự chia sẻ dữ liệu, hợp tác giữa các cơ quan thực thi pháp luật của các nước thì hiệu quả đấu tranh phòng, chống tội phạm MBN sẽ được nâng cao.

3. Một số kiến nghị, đề xuất nhằm nâng cao năng lực phòng ngừa, phát hiện và xử lý tội phạm mua bán người có sử dụng công nghệ thông tin để phạm tội

Để nâng cao năng lực phòng ngừa, phát hiện và xử lý tội phạm MBN có sử dụng công nghệ thông tin, truyền thông như một công cụ, phương tiện khi thực hiện tội phạm, chúng tôi cho rằng cần thực hiện một số giải pháp sau:

- Các quốc gia trên thế giới và khu vực cần tăng cường phối hợp trong thực hiện các Hiệp ước đa phương, song phương về đấu tranh phòng ngừa, chống tội phạm MBN, tội phạm mạng và tội phạm công nghệ cao.

- Các cơ quan chức năng Việt Nam tiếp tục có các biện pháp nhằm tuyên truyền, tổ chức thực thi một cách có hiệu quả Luật công nghệ thông tin năm 2006, Luật công nghệ cao năm 2008, Luật an toàn thông tin mạng năm 2015 và Luật an ninh mạng năm 2018 gắn với việc tuyên truyền, tổ chức thực hiện Luật Phòng, chống mua bán người năm 2011.

- Hoàn thiện các quy định pháp lý liên quan khác đến quản lý, khai thác, sử dụng dữ liệu điện tử từ các thiết bị điện tử, phương tiện điện tử, phần mềm... để đảm bảo tính liên quan, khách quan, hợp pháp của chứng cứ điện tử trong những trường

hợp dữ liệu điện tử được khôi phục sau khi bị xóa; phát hiện, bảo quản, sao lưu dữ liệu điện tử trước khi đưa đi giám định; thu giữ các dữ liệu điện tử đang truyền trong không gian mạng...

- Xây dựng cơ chế phối hợp và cung cấp thông tin giữa các công ty hoạt động trong lĩnh vực thông tin truyền thông không đặt trụ sở chính trên lãnh thổ quốc gia như Facebook, Microsoft, Instagram, Google... với các cơ quan thực thi pháp luật, cơ quan tố tụng nhằm ngăn chặn, phát hiện, xử lý các hành vi sử dụng mạng máy tính, công nghệ thông tin truyền thông để phạm tội MBN.

- Xây dựng đội ngũ chuyên gia trong các cơ quan thực thi pháp luật, cơ quan tố tụng có khả năng sử dụng những tiến bộ của công nghệ thông tin, truyền thông để phòng ngừa, phát hiện, điều tra, truy tố, xét xử tội phạm có sử dụng công nghệ cao nói chung và tội phạm MBN có sử dụng công nghệ thông tin, truyền thông nói riêng.

- Trang bị cơ sở vật chất cho các cơ quan tiến hành tố tụng, trong đó có các phương tiện điện tử, thiết bị điện tử, phần mềm uy tín để hỗ trợ việc tìm kiếm, phát hiện, ghi nhận, thu thập, bảo quản, củng cố, đánh giá, sử dụng các dữ liệu điện tử, chứng cứ điện tử trong giải quyết vụ án hình sự. Củng cố chứng cứ khai thác từ các nguồn chứng cứ khác thông qua nguồn dữ liệu điện tử và ngược lại.

- Đầu tư nguồn lực, đào tạo lực lượng trong các cơ quan thực thi pháp luật, cơ quan có thẩm quyền tiến hành tố tụng để có khả năng phát hiện, điều tra, xử lý tội phạm MBN gắn với các thủ đoạn phạm tội mới trong tương lai có thể xuất hiện như:

+ Tội phạm MBN có sử dụng trí tuệ nhân tạo để tìm kiếm bị hại, thực hiện tuyển mộ, tiếp nhận, chuyển giao và trốn tránh trách nhiệm hình sự cá nhân;

+ Các đối tượng phạm tội MBN có sử dụng trợ lý là các cá nhân ảo để thực hiện hành vi phạm tội và che giấu tội phạm;

+ Đối tượng MBN sử dụng các công cụ như robot, máy bay không người lái và phương tiện tự vận hành trong việc giám sát người lao động; đồng thời cản trở, trốn tránh việc bị các cơ quan thực thi pháp luật phát hiện, bắt giữ;

+ Khi các nền tảng và cấu trúc bảo mật ngày càng trở nên tinh vi, một tổ chức tội phạm có thể núp bóng hoạt động kinh doanh hợp pháp và khiến các cơ quan chức năng rất khó phát hiện;

+ Môi trường bóc lột trực tuyến có thể tạo ra những phương thức, thủ đoạn phạm tội mới đối với các tổ chức tội phạm, cũng như những hình thức phạm tội có tổ chức mới./.

TÀI LIỆU THAM KHẢO

1. Báo cáo của Bộ công an về “Tình hình thực hiện pháp luật về phòng chống mua bán người giai đoạn 2012-2017”;
2. Báo cáo của Ban chỉ đạo 138/CP năm 2019;
3. Nguyễn Đức Hạnh (2020), “Khai thác chứng cứ từ nguồn dữ liệu điện tử phục vụ việc buộc tội, tranh tụng của Kiểm sát viên tại phiên tòa”, Tạp chí Kiểm sát, số 2/2021, tr.42-50;
4. Ryan Kunz, Meredith Baughman, Rebecca Yarnell and Celia Williamson (2018), *Social Media and Sex Trafficking Responses*, University of Toledo;
5. UNODC (2020). *Modul 14: Link between Cybercrime, Trafficking in Persons and Smuggling of Migrants*, University Modul Series Cybercrime, E4J.