

TỘI PHẠM ĐƯA HOẶC SỬ DỤNG TRÁI PHÉP THÔNG TIN MẠNG MÁY TÍNH, MẠNG VIỄN THÔNG - NHỮNG KHÓ KHĂN, VƯỚNG MẮC TRONG PHÁT HIỆN, ĐIỀU TRA, XỬ LÝ VÀ GIẢI PHÁP KHẮC PHỤC

TRẦN QUANG TÙNG*

Trên cơ sở nghiên cứu lý luận và thực tiễn, bài viết làm rõ những khó khăn, vướng mắc trong phát hiện, điều tra, xử lý và đưa ra giải pháp khắc phục nhằm nâng cao hiệu quả phòng, chống tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính (MMT), mạng viễn thông (MVT).

Từ khóa: Tội phạm, công nghệ cao, mạng máy tính, mạng viễn thông.

Ngày nhận bài: 23/4/2021; Biên tập xong: 23/4/2021; Duyệt đăng: 23/4/2021

Based on theoretical research and practical experience, the article analyses the obstacles in the detection and investigation processes of the crime of illegal upload or use of information on computer networks or telecommunications networks, then proposes solutions to improve the effectiveness in preventing that kind of crime.

Keywords: Crime, high technology, computer networks, telecommunication networks.

Trong số những hành vi phạm tội sử dụng công nghệ cao, nổi lên là hành vi đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông được quy định tại Điều 288 Bộ luật hình sự năm 2015, sửa đổi, bổ sung năm 2017 (BLHS năm 2015). Đây là những hành vi đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật, mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu thông tin đó hoặc các hành vi sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông.

Theo báo cáo tổng kết năm 2020 của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an cho thấy, riêng trong năm 2020, trên thế giới (trong đó có Việt Nam) ghi nhận thông tin của 235 triệu tài khoản Instagram, TikTok, YouTube; 6000 nhân viên của Boeing; 150 triệu người dân Mỹ; 26.000 dữ liệu khách hàng của Honda bị rò rỉ trên mạng; 267 triệu tài khoản Facebook bị đánh cắp. Những thông tin cá nhân bị các đối tượng đăng tải trái phép lên mạng Internet nhằm thu lợi bất chính và nhiều mục đích phạm tội khác.

Một số khó khăn, vướng mắc trong quá trình phát hiện, điều tra, xử lý loại tội phạm này là:

Thứ nhất, khó khăn, vướng mắc trong áp dụng các quy định của BLHS năm 2015 đối với tội đưa

hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông

Hiện nay chưa có hướng dẫn cụ thể về “thông tin trái với quy định của pháp luật” tại điểm a, khoản 1, Điều 288 BLHS năm 2015. Qua nghiên cứu cho thấy, mỗi văn bản pháp luật lại tiếp cận nội dung này dưới những khía cạnh và phạm vi khác nhau, có thể kể đến như: Điều 21 Hiến pháp năm 2013 quy định “Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình”. Bộ luật dân sự năm 2015 có Điều 32 quy định về: “Quyền cá nhân đối với hình ảnh” và Điều 38 quy định: “Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình”. Luật An ninh mạng, tại các điều 8, 16, 17 và 18 quy định về cách hành vi xâm phạm An ninh quốc gia, trật tự an toàn xã hội trên không gian mạng. Nghị định 72/2013/NĐ-CP ngày 15/7/2013 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng (sửa đổi, bổ sung một số điều bởi Nghị định số 27/2018/NĐ-CP ngày 01/3/2018) tại khoản 1 Điều 5 cũng đưa ra các hành vi bị cấm trên mạng Internet. Điều 102 Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện quy định về xử phạt: “Vi phạm quy

* *Thạc sĩ, Khoa Toán - Tin học và Ứng dụng khoa học công nghệ trong phòng chống tội phạm, Học viện Cảnh sát nhân dân*

định về lưu trữ, cho thuê, truyền đưa, cung cấp, truy nhập, thu thập, xử lý, trao đổi và sử dụng thông tin”.

Như vậy, do có nhiều văn bản pháp luật quy định khác nhau về các hành vi bị cấm trên không gian mạng nên chưa có sự thống nhất trong công tác đấu tranh phòng, chống tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. Điều này gây nhiều khó khăn trong quá trình phát hiện, điều tra về hành vi phạm tội này.

Đồng thời, về vấn đề xác định hậu quả phi vật chất, theo quy định tại Điều 288 BLHS năm 2015, hậu quả của tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông là một tình tiết định tội và định khung. Điều này có nghĩa là hành vi phạm tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông phải gây hậu quả nhất định thì mới cấu thành tội phạm. Hậu quả của hành vi phạm tội này được xem xét trên hai khía cạnh là hậu quả vật chất và hậu quả phi vật chất. Hậu quả vật chất được xác định dựa trên số tiền “thu lợi bất chính” hoặc số tiền “gây thiệt hại” do đối tượng thực hiện hành vi phạm tội gây ra. Theo đó, để cấu thành tội phạm này, số tiền thu lợi bất chính của đối tượng phạm tội phải từ 50.000.000 đồng và số tiền gây thiệt hại phải từ 100.000.000 đồng trở lên. Một số hậu quả phi vật chất như: “gây dư luận xấu làm giảm uy tín của cơ quan, tổ chức, cá nhân”, “xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát”, “gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội hoặc quan hệ đối ngoại của Việt Nam”, “dẫn đến biểu tình”. Tuy nhiên, bản thân điều luật và văn bản hướng dẫn thi hành quy định còn chung chung về hậu quả và các mức độ để đánh giá tính nghiêm trọng của các hậu quả phi vật chất này. Điều này gây khó khăn trong quá trình xác định hành vi phạm tội và áp dụng các tình tiết định khung với tội phạm này.

Thứ hai, khó khăn, vướng mắc trong thu thập thông tin, tài liệu tồn tại dưới dạng dữ liệu điện tử để đấu tranh, xử lý với đối tượng

Với tính chất của một loại tội phạm sử dụng công nghệ cao, những thông tin tài liệu phản ánh về hành vi phạm tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông cũng tồn tại dưới dạng dữ liệu điện tử và rất dễ bị xóa bỏ, thay đổi, làm ẩn, mã hoá. Với chủ ý phạm tội, bằng khả năng kỹ thuật và sự hỗ trợ của các phần mềm được cung cấp

rất phổ biến trên các trang mạng, các đối tượng không khó khăn để thay đổi ngay từ đầu các dữ liệu điện tử liên quan đến quá trình phạm tội như thay đổi địa chỉ IP (fake IP), giả địa chỉ thư điện tử (fake email)... Đối tượng cũng có thể dễ dàng tiêu huỷ các thiết bị lưu trữ, gây ra những hỏng hóc về mặt vật lý khiến cho việc phục hồi dữ liệu vô cùng khó khăn, hoặc nếu có phục hồi thì cũng cần những phương tiện chuyên dụng cao cấp và tốn nhiều thời gian.

Thứ ba, khó khăn trong xác định người đăng tải thông tin trái với quy định của pháp luật và hình thức xử lý đối với người chia sẻ những thông tin vi phạm

Một thực tế đang diễn ra trên không gian mạng là có nhiều thông tin trái với quy định của pháp luật, thông tin sai sự thật nhưng lại được chia sẻ rất nhiều. Việc chia sẻ tin của mỗi người có thể xuất phát từ những lý do khác nhau, có người vì mục đích câu “view”, câu “like”, có người vì vô tình không biết là thông tin sai, tin giả hoặc cho rằng đó là thông tin hữu ích... Việc những thông tin được lan truyền rất nhanh chóng trên mạng Internet và được nhiều người chia sẻ lại đã gây khó khăn trong việc truy nguyên nguồn gốc thông tin đó. Tuy vậy, hệ thống pháp luật hiện hành cũng như thực tiễn phát hiện, điều tra, xử lý đối với tội phạm này cũng chưa đặt ra trách nhiệm xử lý đối với những người chia sẻ thông tin, trong khi đây mới chính là những người khiến những thông tin trái quy định của pháp luật, thông tin sai sự thật bị lan truyền một cách nhanh chóng và để lại nhiều hậu quả khi có nhiều người tiếp cận với những thông tin này.

Thứ tư, khó khăn trong phối hợp với các nhà cung cấp dịch vụ đề nghị cung cấp thông tin phục vụ công tác điều tra, xử lý

Khoản 4 Điều 5 Bộ luật tố tụng hình sự (BLTTHS) năm 2015 quy định về trách nhiệm của cơ quan nhà nước, tổ chức và cá nhân trong đấu tranh phòng, chống tội phạm nêu rõ: “Cơ quan nhà nước, tổ chức và cá nhân có trách nhiệm thực hiện yêu cầu và tạo điều kiện để cơ quan, người có thẩm quyền tiến hành tố tụng thực hiện nhiệm vụ”. Điều 168 BLTTHS năm 2015 có quy định yêu cầu các cơ quan, tổ chức, cá nhân có trách nhiệm thực hiện các yêu cầu của Cơ quan điều tra, cơ quan được giao nhiệm vụ tiến hành một số hoạt động điều tra, Viện kiểm sát trong giai đoạn điều tra vụ án hình sự; trường hợp không chấp hành mà không vì lý do bất khả kháng hoặc không do

trở ngại khách quan thì bị xử lý theo quy định của pháp luật.

Tuy nhiên, Điều 382, 383 BLHS năm 2015 mới chỉ dừng lại ở việc xử lý đối với hành vi từ chối cung cấp tài liệu, cung cấp tài liệu sai sự thật của người làm chứng, người giám định, người định giá tài sản, người phiên dịch, người dịch thuật, người bào chữa; còn các cá nhân, tổ chức, cơ quan khác thì chưa có chế tài xử lý trong trường hợp không cung cấp hoặc cung cấp tài liệu sai sự thật. Chính vì vậy, trong thời gian qua, việc cung cấp thông tin về dữ liệu khách hàng của các nhà cung cấp dịch vụ như nhà mạng viễn thông, ngân hàng, nhà cung cấp dịch vụ trên mạng Internet, mạng xã hội (Facebook, Zalo...) cho cơ quan chức năng còn chậm và còn nhiều trường hợp từ chối cung cấp thông tin mà không có lý do hợp lý.

Thứ năm, khó khăn trong việc gỡ bỏ những thông tin vi phạm trên không gian mạng đối với các nhà cung cấp thông tin công cộng qua biên giới

Hiện nay, quy định về việc gỡ bỏ thông tin vi phạm trên không gian mạng chủ yếu được căn cứ vào quy định tại Luật An ninh mạng năm 2018, Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử và Thông tư số 38/2016/TT-BTTTT ngày 26/12/2016 của Bộ Thông tin và Truyền thông quy định chi tiết về việc cung cấp thông tin công cộng qua biên giới. Theo đó, với các nhà cung cấp dịch vụ nước ngoài ở Việt Nam phổ biến như Facebook, Google, công tác phối hợp của cơ quan chức năng Việt Nam trong kiểm soát và gỡ bỏ các thông tin vi phạm vẫn còn rất hạn chế. Một phần nguyên nhân là vì chính sách pháp luật chưa đưa ra những chế tài xử lý cứng rắn với những nhà cung cấp dịch vụ này khi họ từ chối nghĩa vụ kiểm soát và ngăn chặn, gỡ bỏ những thông tin vi phạm.

Bên cạnh đó, căn cứ điểm b khoản 2 Điều 26 Luật An ninh mạng năm 2018 và khoản 1 Điều 5 Thông tư số 38/2016/TT-BTTTT ngày 26/12/2016 của Bộ Thông tin và Truyền thông thì trong vòng 24 giờ, các nhà cung cấp dịch vụ nước ngoài phải gỡ bỏ những thông tin vi phạm theo đề nghị từ lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông. Có thể thấy, kể cả trong trường hợp những nhà cung cấp dịch vụ này đồng ý

gỡ bỏ thông tin vi phạm thì trong khoảng thời gian đó, những thông tin đã được nhiều người khác chia sẻ lại và lan truyền nhanh chóng trên mạng Internet.

Ngoài ra, mặc dù hợp tác trong gỡ bỏ thông tin vi phạm nhưng nhiều nhà cung cấp dịch vụ nước ngoài vẫn cho phép các chủ kênh vi phạm này đăng tải lại các clip đã gỡ. Điều này lý giải nhiều video vi phạm đã được gỡ sau đó lại tiếp tục xuất hiện trở lại, thậm chí còn cho phép chủ các kênh này tiếp tục sử dụng tính năng “gợi ý nội dung” để quảng bá, phát tán nội dung thông tin vi phạm.

Để khắc phục những khó khăn, vướng mắc trong phát hiện, điều tra, xử lý nhằm nâng cao hiệu quả phòng, chống loại tội phạm này, tác giả đề xuất một số giải pháp sau:

Một là, kiến nghị, tham mưu hoàn thiện chính sách pháp luật

Cần tham mưu cho Bộ Công an, các cơ quan có thẩm quyền nghiên cứu xây dựng và ban hành một văn bản hướng dẫn áp dụng các quy định của BLHS năm 2015 về một số tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, trong đó có tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. Theo đó, nội dung hướng dẫn cần giải quyết một số vấn đề cụ thể liên quan đến công tác đấu tranh phòng, chống tội phạm sử dụng công nghệ cao nói chung và tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông nói riêng như sau:

+ Cần thống nhất việc định nghĩa, giải thích về “thông tin trái với quy định của pháp luật” và cụ thể các hành vi phạm tội của tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông làm cơ sở để nhận diện và đấu tranh với loại tội phạm này.

+ Đối với vấn đề xác định hậu quả phi vật chất, bản thân điều luật và văn bản hướng dẫn thi hành quy định còn chung chung về hậu quả và các mức độ để đánh giá tính nghiêm trọng của các hậu quả phi vật chất này. Khi xem xét hậu quả phi vật chất, có thể cần nhắc đến những vấn đề sau: Tần suất (số lần), khoảng thời gian người phạm tội thực hiện việc gửi, phát tán, cung cấp nội dung vi phạm; Những ảnh hưởng tới tinh thần và hành vi của nạn nhân là cá nhân do hành vi phạm tội gây ra như lo sợ, sang chấn, bế tắc tâm lý, tự tử, tự gây thương tích... Cần chú ý đến đặc điểm tâm lý, hoàn cảnh của nạn nhân để đánh giá mức

độ tác động ảnh hưởng cho phù hợp; Uy tín của tổ chức, doanh nghiệp bị ảnh hưởng bởi hành vi tội phạm; Thái độ nạn nhân đối với những thông tin có liên quan đến mình được người phạm tội gửi đến hoặc phát tán trên mạng; Số người kết nối, người viết bình luận, đưa ra những đánh giá và phát tán lại các nội dung vi phạm; Những ảnh hưởng của sự việc đến dư luận xã hội, cộng đồng mạng...

+ Cần hướng dẫn cụ thể về nguyên tắc, cách thức và quy trình thu thập, phân tích, bảo quản dữ liệu điện tử có liên quan đến hành vi phạm tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. Bởi lẽ, các quy định liên quan đến dữ liệu điện tử tại các điều 87, 99 và 107 BLTTHS năm 2015 mới chỉ mang tính chất khái quát nên thực tế quá trình thu thập, phân tích, bảo quản dữ liệu điện tử còn chưa thống nhất và dễ xảy ra sai sót.

+ Xác định rõ trách nhiệm, nghĩa vụ, thời gian cung cấp thông tin của các nhà cung cấp dịch vụ trên mạng Internet khi có yêu cầu đề nghị từ cơ quan chức năng, đảm bảo quá trình điều tra, xử lý hành vi phạm tội kịp thời, đúng luật.

Hai là, tăng cường công tác tuyên truyền, giáo dục pháp luật và nâng cao nhận thức của những người tham gia vào môi trường mạng Internet

Công tác tuyên truyền, phổ biến giáo dục pháp luật có vai trò rất quan trọng, cần thực hiện thường xuyên, liên tục nhằm giúp người dân nhận thức rõ tính hai mặt của Internet và mạng xã hội; nhận diện các thủ đoạn, nội dung thông tin vi phạm, tính chất nguy hại của nó đối với cá nhân và xã hội, tránh tình trạng vô tình tiếp tay cho các hoạt động chống phá và các hành vi tiêu cực, phản cảm, thiếu văn hóa trên không gian mạng. Đồng thời, cần tăng cường sự giám sát, phát hiện thông tin sai phạm từ cộng đồng; các thông tin sai trái trên mạng Internet cần được phản biện, phản bác công khai, kịp thời.

Bên cạnh đó, công tác tuyên truyền cần tập trung vào một số đối tượng cụ thể, như những người sở hữu tài khoản có tầm ảnh hưởng rộng rãi trên mạng Internet, mạng xã hội để góp phần định hướng thông tin đúng đắn và điều chỉnh hành vi sử dụng mạng Internet, mạng xã hội của người khác cho phù hợp.

Ba là, tăng cường mối quan hệ phối hợp với các nhà cung cấp dịch vụ trên mạng Internet, mạng viễn thông

Trong công tác đấu tranh phòng, chống tội phạm đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao cần tăng cường quan hệ phối hợp với các nhà cung cấp dịch vụ trên mạng Internet, mạng viễn thông. Mối quan hệ này có thể được thực hiện thông qua các Quy chế phối hợp, Biên bản ghi nhớ.

Đối với các nhà cung cấp dịch vụ nước ngoài, phải có sự tuân thủ pháp luật Việt Nam, đặc biệt là những quy định trong Luật An ninh mạng như thực hiện các đề nghị của lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông, phải lưu trữ dữ liệu người dùng tại Việt Nam trong thời gian theo quy định, phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam... Điều này nhằm tạo ra một cơ chế và hành lang pháp lý để nhà nước có thể quản lý những hoạt động của các nhà cung cấp dịch vụ nước ngoài tại Việt Nam, tạo sự bình đẳng giữa các nhà cung cấp trong và ngoài nước.

Bốn là, về khoảng thời gian gỡ bỏ thông tin vi phạm trên mạng máy tính, mạng viễn thông

Hiện nay, khoảng thời gian được quy định để các nhà cung cấp dịch vụ trên mạng máy tính, mạng viễn thông gỡ bỏ các thông tin vi phạm được quy định tại khoản 2 Điều 26 Luật An ninh mạng và Điều 5 Thông tư số 38/2016/TT-BTTTT ngày 26/12/2016 của Bộ Thông tin và Truyền thông. Theo đó, trong vòng 24 giờ kể từ thời điểm có đề nghị từ cơ quan chuyên trách bảo vệ an ninh mạng của Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông, các doanh nghiệp cung cấp dịch vụ trên mạng máy tính, mạng viễn thông phải gỡ bỏ các thông tin vi phạm trên nền tảng dịch vụ mà mình cung cấp. Tuy nhiên, với tốc độ lan truyền nhanh chóng của các thông tin trên mạng Internet, trong khoảng thời gian đó, các thông tin vi phạm đã được nhiều người chia sẻ hoặc sao, chụp lại và rất khó để kiểm soát thông tin.

Vì vậy, cần nghiên cứu rút ngắn khoảng thời gian yêu cầu các nhà cung cấp dịch vụ mạng máy tính, mạng viễn thông gỡ bỏ thông tin vi phạm. Việc yêu cầu này có thể được thực hiện thông qua một số phương thức như qua các phương tiện điện tử, qua Email... để đảm bảo sự nhanh chóng, kịp thời./.