

THU THẬP CHỨNG CỨ ĐIỆN TỬ TRONG TỔ TỤNG HÌNH SỰ VIỆT NAM

LÊ NGUYỄN THANH

Hội Thẩm nhân dân, Tòa án nhân dân TP. Hồ Chí Minh

People's Jury, People's Court of Ho Chi Minh City

Email: lnthanh@hcmulaw.edu.vn

Tóm tắt

Pháp luật tố tụng hình sự Việt Nam hiện nay chưa quy định cụ thể về thủ tục thu thập chứng cứ điện tử, do đó thực tiễn áp dụng còn tùy nghi, làm ảnh hưởng đến giá trị chứng minh của chứng cứ. Bài viết phân tích các vấn đề pháp lý về thủ tục thu thập chứng cứ điện tử và đề xuất giải pháp hoàn thiện.

Từ khóa: chứng cứ, chứng cứ điện tử, dữ liệu điện tử, thu thập chứng cứ

Abstract

To collect electronic evidence, persons authorized to conduct criminal proceedings can use investigative measures specified in the Criminal Procedure Code including search, scene examination, electronic data assessment, evidence reception, special procedural investigative measures. The article analyzes legal issues related to electronic evidence collection procedures and proposes solutions for improvement.

Keywords: evidence, electronic evidence, electronic data, collect evidence

Ngày nhận bài: 25/11/2023

Ngày duyệt đăng: 15/01/2024

Ngày nay, tội phạm có sử dụng công nghệ thông tin không chỉ xâm phạm đến sự an toàn của hệ thống mạng máy tính, mạng viễn thông, các phương tiện điện tử mà còn sử dụng các phương tiện điện tử để thực hiện nhiều nhóm tội phạm khác. Ở Việt Nam, thời gian gần đây, theo báo cáo của Bộ Công an, từ đầu năm 2022 đến nay (8/2023), lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao toàn quốc đã phát hiện, khởi tố 474 vụ án, 1.071 bị can liên quan các loại tội phạm sử dụng công nghệ cao xâm phạm trật tự an toàn xã hội.¹ Tất nhiên, để chứng minh tội phạm trong các vụ án này, ngoài việc thu thập và sử dụng chứng cứ trong lời khai, lời trình bày, vật chứng... cần phải thu thập và sử dụng chứng cứ từ nguồn dữ liệu điện tử.

Thu thập chứng cứ trong tố tụng hình sự là việc sử dụng các biện pháp do pháp luật tố tụng hình sự quy định để phát hiện, thu giữ, ghi nhận, bảo quản chứng cứ nhằm chứng minh vụ án hình sự. Đối với chứng cứ điện tử, loại chứng cứ này được thu thập từ nguồn chứng cứ là dữ liệu điện tử. Theo khoản 1 Điều 99 Bộ luật Tố tụng hình sự (BLTTHS) năm 2015, dữ liệu điện tử là ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự được tạo ra, lưu trữ, truyền đi hoặc nhận được bởi phương tiện điện tử. Các loại dữ liệu điện tử được lưu trữ trong các phương tiện điện tử hoặc được lưu trữ online trên đám mây điện tử (Google Drive, Dropbox, OneDrive, iCloud...) và trên đường truyền của mạng máy tính, mạng internet, mạng viễn thông. Lý luận và thực

1 Văn Chúc, “Bộ Công an triển khai nhiều giải pháp xử lý nghiêm tội phạm công nghệ cao”, *Báo Nhân dân điện tử*, 2023, <https://nhandan.vn/bo-cong-an-trien-khai-nhieu-giai-phap-xu-ly-nghiem-toi-pham-cong-nghe-cao-post709689.html>, truy cập 18/10/2023.

tiên cho thấy, ngoài những đặc điểm, thuộc tính chung của chứng cứ, chứng cứ điện tử còn có những đặc điểm riêng biệt (như khó nhận biết bằng mắt thường mà không có chuyên môn về công nghệ thông tin; có tính “di động” - không bị hạn chế bởi yếu tố biên giới, địa lý; tính dễ nhân bản, sao chép, xóa, ẩn...). Do đó, để thu thập chứng cứ điện tử cần có những yêu cầu riêng về thủ tục, đòi hỏi trình độ hiểu biết công nghệ thông tin của chủ thể và phương tiện điện tử hỗ trợ. Đây là vấn đề khá phức tạp cần được nghiên cứu trong bài viết này.

1. Các biện pháp thu thập chứng cứ điện tử

Việc tiến hành các biện pháp để thu thập chứng cứ điện tử trước hết phải tuân thủ các quy định chung về căn cứ, thẩm quyền và thủ tục thu thập chứng cứ của từng biện pháp. Ngoài ra, khi tiến hành thu thập chứng cứ điện tử, mỗi biện pháp cần có yêu cầu riêng.

1.1. Thu thập chứng cứ điện tử bằng biện pháp khám xét

Biện pháp đầu tiên là thu thập chứng cứ điện tử bằng biện pháp khám xét. Khoản 1 Điều 192 BLTTTHS năm 2015 quy định chung việc khám xét người, chỗ ở, nơi làm việc, địa điểm, phương tiện chỉ được tiến hành “khi có căn cứ để nhận định trong người, chỗ ở, nơi làm việc, địa điểm, phương tiện có công cụ, phương tiện phạm tội, tài liệu, đồ vật, tài sản do phạm tội mà có hoặc đồ vật, dữ liệu điện tử, tài liệu khác có liên quan đến vụ án”. Người tiến hành khám xét có quyền thu giữ, niêm phong các phương tiện điện tử để thu thập chứng cứ điện tử. Điều 107 BLTTTHS năm 2015 quy định cụ thể cách thức thu giữ phương tiện điện tử: “Phương tiện điện tử phải được thu giữ kịp thời, đầy đủ, mô tả đúng thực trạng và niêm phong ngay sau khi thu giữ. Việc niêm phong, mở niêm phong được tiến hành theo quy định của pháp luật”. Đối với những phương tiện điện tử như máy tính, điện thoại thông minh, máy tính bảng, đĩa mềm, đĩa quang và các thiết bị ngoại vi khác... chứa các dữ liệu điện tử được thu giữ thì áp dụng thủ tục thu giữ vật chứng của vụ án.

Thông thường, thu thập chứng cứ điện tử bằng biện pháp khám xét được bắt đầu từ việc tiến hành khám xét và thu giữ phương tiện điện tử. Sau khi thu giữ phương tiện điện tử sẽ bàn giao phương tiện điện tử đã được niêm phong về nơi bảo quản. Sau đó, cơ quan có thẩm quyền tiến hành mở niêm phong phương tiện điện tử để xử lý thông tin thành chứng cứ dạng đọc, nghe, nhìn được. Thành phần tham gia mở niêm phong cùng với việc sao chép dữ liệu điện tử sang phương tiện điện tử khác giống như thành phần khi tiến hành khám xét. Mọi thao tác xử lý thông tin dữ liệu điện tử tiếp theo để thu thập chứng cứ được thực hiện trên bản sao, còn dữ liệu gốc được bảo quản để bảo vệ các chứng cứ không bị hư hỏng. Dữ liệu điện tử trong bản sao phải bảo đảm toàn vẹn như bản gốc.

Ngoài ra, biện pháp chuyển hóa dữ liệu điện tử (dữ liệu ảnh, ký tự, ký hiệu) sang nguồn tài liệu giấy cũng được sử dụng. Trong trường hợp đơn giản,

hoạt động này cũng có thể được tiến hành tại chỗ bằng cách in (có thể yêu cầu người vi phạm trực tiếp thao tác in) dữ liệu dạng file điện tử ra giấy những nội dung dạng ký tự, ký hiệu, ảnh có liên quan đến vụ án, đồng thời yêu cầu người chủ dữ liệu điện tử xác nhận vào từng trang giấy chứa thông tin chứng cứ được in ra, đồng thời ghi rõ: “Đây là tài liệu được in ra từ máy tính (hoặc e-mail, thiết bị số...) của tôi”.² Việc yêu cầu chủ dữ liệu điện tử in các dữ liệu ra giấy cũng thích hợp với nhu cầu thu thập chứng cứ điện tử được lưu trữ trực tuyến (*online*), vì họ có thể dùng tài khoản và mật khẩu đăng nhập để truy cập dữ liệu điện tử. Biên bản chuyển hóa dữ liệu điện tử sang tài liệu giấy và bản giấy in được đưa vào hồ sơ vụ án. Cách chuyển hóa chứng cứ từ nguồn dữ liệu điện tử sang tài liệu giấy thuận tiện bởi việc truy cập vào file dữ liệu điện tử có thể do chính người chủ tài khoản thực hiện, đồng thời ngăn ngừa trường hợp mất hoặc hư hỏng dữ liệu mà vẫn bảo đảm giá trị chứng minh. Thủ tục chuyển hóa dữ liệu điện tử bằng cách in ra bản giấy, có xác nhận của chủ dữ liệu điện tử trong vụ án mặc dù đang được áp dụng phổ biến trong thực tiễn nhưng chưa được quy định cụ thể về trường hợp áp dụng cũng như thủ tục.

BLTTTHS năm 2015 còn quy định: “Trường hợp không thể thu giữ phương tiện lưu trữ dữ liệu điện tử thì cơ quan có thẩm quyền tiến hành tố tụng sao lưu dữ liệu điện tử đó vào phương tiện điện tử và bảo quản như đối với vật chứng” (khoản 1 Điều 107). Việc thu giữ phương tiện điện tử, dữ liệu điện tử do người có thẩm quyền tiến hành tố tụng thực hiện và có thể mời người có chuyên môn liên quan tham gia. Khi thu giữ các phương tiện điện tử có thể thu thiết bị ngoại vi kèm theo và các tài liệu có liên quan (Điều 196).

Như vậy, thu thập chứng cứ điện tử bằng biện pháp khám xét trước hết là thu giữ phương tiện điện tử để phát hiện chứng cứ; có thể chuyển hóa sang tài liệu giấy hoặc sao lưu sang phương tiện điện tử khác. Quá trình thu thập, sao lưu dữ liệu điện tử từ phương tiện điện tử bị thu giữ do cơ quan có thẩm quyền tiến hành tố tụng thực hiện phải lập biên bản và đưa vào hồ sơ vụ án theo quy định tại khoản 2 Điều 107 BLTTTHS năm 2015.

Ngoài việc thu thập chứng cứ từ phương tiện điện tử cố định, còn có biện pháp chặn thu dữ liệu điện tử trên đường truyền của mạng máy tính, mạng viễn thông, mạng internet. Chặn thu dữ liệu trên đường truyền (giữa máy chủ - máy chủ, máy tính cá nhân - máy chủ, dữ liệu truyền bằng ADSL, 3G, vệ tinh) được xem là một trong những cách thu thập dữ liệu điện tử hiện nay.³ Không giống như các dữ liệu điện tử chứa chứng cứ được lưu trữ trong các phương tiện điện tử cố định được thu giữ khi khám xét, còn nhiều dữ liệu điện tử khác chỉ tồn tại một lần trên đường truyền và phải chặn thu trên

2 Trường Đào tạo, Bồi dưỡng nghiệp vụ kiểm sát TP. Hồ Chí Minh, Tài liệu tập huấn: *Nâng cao hiệu quả công tác thực hành quyền công tố, kiểm sát điều tra, kiểm sát xét xử các vụ án về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông*, 2023, tr. 19.

3 Trần Văn Hòa, “Vấn đề chứng cứ điện tử”, trong *Những nội dung mới trong Bộ luật Tố tụng hình sự năm 2015*, Nguyễn Hòa Bình (chủ biên), Nxb. CTQG, 2016, tr. 231.

đường truyền như sử dụng dịch vụ truyền thông được cung cấp trực tiếp đến người xem thông qua Internet (*over-the-top*, OTT), mua hàng qua mạng, đánh bạc (cá độ) qua mạng Internet... Nếu không chặn thu kịp thời sẽ rất khó để thu thập chứng cứ do người nắm quyền quản trị gỡ, xóa. Nếu đã bị gỡ, xóa trong máy chủ thì điều tra viên chỉ có thể sử dụng dữ liệu điện tử đã thu trong giai đoạn trinh sát và chuyển hóa thành chứng cứ theo thủ tục tố tụng.⁴

Biện pháp “chặn thu” dữ liệu điện tử là biện pháp điều tra công khai, khác với biện pháp điều tra tố tụng đặc biệt hoặc biện pháp trinh sát nghiệp vụ khác. Vì vậy, khi thu thập chứng cứ điện tử phải lập biên bản và đưa vào hồ sơ vụ án (khoản 2 Điều 107 BL TTHS năm 2015) mà không thể tiến hành như biện pháp trinh sát. Dữ liệu điện tử tồn tại trên mạng máy tính, mạng viễn thông hoặc trên đường truyền có tính di động cao, dễ gỡ bỏ và tác động làm thay đổi, được lưu ở máy chủ của nhà cung cấp dịch vụ trực tuyến. Vì thế biện pháp chặn thu cần thực hiện nhanh chóng mà vẫn phải bảo đảm tính nguyên vẹn của chứng cứ. Mọi hoạt động chặn thu đều tiến hành lập biên bản, có sao lưu vào phương tiện điện tử để bảo quản với thành phần tham gia giống như hoạt động khám xét. Có thể chặn thu dữ liệu điện tử bằng việc tải, chia sẻ, sao chép hoặc chụp ảnh các dữ liệu điện tử trên màn hình thiết bị đang hoạt động và sao lưu vào phương tiện điện tử khác như quy định tại khoản 1 Điều 107 BL TTHS năm 2015.

Tuy nhiên, để bảo đảm giá trị chứng minh, cần kết hợp với các biện pháp điều tra khác như lấy lời khai của người liên quan đến dữ liệu này. Trong một số vụ án xảy ra gần đây, cơ quan có thẩm quyền chủ động thu thập chứng cứ điện tử bằng biện pháp chặn thu trên đường truyền thông qua các tài khoản mạng xã hội như Facebook, Zalo, Tiktok... với các dòng trạng thái, hình ảnh, clip có nội dung vi phạm pháp luật. Ví dụ, vụ án do Nguyễn Hữu M, phạm tội lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của nhà nước, quyền, lợi ích hợp pháp của tổ chức cá nhân. Từ 11/2019 đến đầu tháng 02/2020, Nguyễn Hữu M sử dụng tài khoản Facebook “Nguyễn Hữu M” do mình lập từ năm 2012 được đăng ký bằng gmail trên phương tiện điện thoại Iphone 6S đăng tải 86 bài viết, hình ảnh có nội dung xâm phạm đến uy tín, danh dự của lực lượng công an và chính quyền Thành phố Hà Nội, Bộ Y tế.⁵ Hầu hết chứng cứ và dữ liệu điện tử này được thu trên đường truyền.

Ngoài ra, trong thực tiễn, chủ thể thu thập chứng cứ có thể tổ chức ghi hình, ghi âm trực tiếp các dữ liệu đang phát trên đường truyền vào phương tiện điện tử khác, quá trình này cũng được lập biên bản và đưa vào hồ sơ vụ án. Việc bảo quản các phương tiện điện tử có sao lưu dữ liệu điện tử tương tự như bảo quản vật chứng. Tuy nhiên, những kỹ thuật chặn thu chứng cứ, dữ liệu điện tử này được tiến hành phù hợp với điều kiện thực tế mang tính

4 Trần Văn Hòa, *ltd*, 2016, tr. 234.

5 Bản án số 13/2020/HS-ST ngày 07/09/2020 của Tòa án nhân dân huyện N.H, tỉnh Q. N.

“sáng tạo” của từng đơn vị, cá nhân của chủ thể có thẩm quyền mà chưa có những hướng dẫn thống nhất.

1.2. Thu thập chứng cứ điện tử bằng biện pháp khám nghiệm hiện trường

Đối với việc thu thập chứng cứ điện tử bằng biện pháp khám nghiệm hiện trường, BLTTTHS năm 2015 quy định thủ tục chung tại Điều 201, trong đó nêu rõ khám nghiệm nơi xảy ra, nơi phát hiện tội phạm để phát hiện dấu vết của tội phạm, thu giữ vật chứng, tài liệu, đồ vật, dữ liệu điện tử khác liên quan và làm sáng tỏ những tình tiết có ý nghĩa đối với việc giải quyết vụ án. BLTTTHS không có quy định riêng về thủ tục khám nghiệm các hiện trường riêng biệt của từng loại vụ án (như hiện trường vụ án có sử dụng phương tiện điện tử để phạm tội; vụ án vi phạm an toàn giao thông; vụ án cháy nổ; vụ án cướp tài sản; vụ án trộm cắp tài sản; vụ án giết người...). Có hiện trường chỉ có một hoặc một vài phương tiện điện tử hiện diện có chứa dữ liệu điện tử như điện thoại thông minh, hộp đen, camera hành trình... Tuy nhiên, cũng có hiện trường vụ án xâm phạm hoạt động bình thường của phương tiện điện tử, mạng viễn thông, mạng internet hoặc sử dụng các phương tiện điện tử để phạm tội, điển hình như các vụ án tổ chức đánh bạc trực tuyến.⁶

Mặc dù bản chất loại hiện trường có những phương tiện điện tử dùng vào mục đích phạm tội vẫn là hiện trường vật lý bình thường, không phải hiện trường kỹ thuật số, nhưng vẫn đặt ra yêu cầu riêng về cách thức tiếp cận hiện trường, bảo vệ hiện trường, tiến hành vẽ sơ đồ hiện trường bố trí các phương tiện điện tử và cách thức thu giữ các loại phương tiện điện tử, trình tự tiếp cận các dữ liệu điện tử bảo đảm không bị mất thông tin, không giống như thu giữ vật chứng, tài liệu, đồ vật thông dụng khác⁷. Hiện nay, những quy định chung trong BLTTTHS chưa đủ chi tiết để hướng dẫn riêng khám nghiệm hiện trường vụ án có sử dụng các phương tiện điện tử để phạm tội.

1.3. Thu thập chứng cứ điện tử bằng biện pháp giám định dữ liệu điện tử

Có thể xem đây là biện pháp thu thập chứng cứ tiếp theo sau khi khám xét, khám nghiệm hiện trường có thu giữ phương tiện điện tử, dữ liệu điện tử nhưng khó phát hiện, kiểm tra, đánh giá chứng cứ, người giám định dữ liệu điện tử vận dụng sự hiểu biết về chuyên môn khoa học và công nghệ số để thu thập chứng cứ điện tử. Hiện nay, giám định dữ liệu điện tử là loại giám

6 Ví dụ, vụ tổ chức đánh bạc, cá độ xuyên quốc gia tại Khu đô thị Our City (Hải Phòng) bị bắt vào ngày 27/7/2019. Chỉ hơn 30 giây, gần 400 con bạc bị lực lượng công an khống chế, bắt quả tang khiến họ không kịp trở tay để có thể ngắt cầu dao, hủy dữ liệu hay chạy thoát thân. Qua khám xét, có quan công an thu giữ gần 2.000 điện thoại di động thông minh, 533 máy tính các loại, nhiều thẻ ngân hàng, tiền mặt cùng đồ vật, tài liệu liên quan đến vụ án. Số tiền tổ chức cờ bạc này giao dịch trên hệ thống là trên 3,6 tỷ Nhân dân tệ, tương đương hơn 12.000 tỷ đồng. Xem: Minh Khang - Nguyễn Huệ, *30 giây đột kích sào huyệt cờ bạc nửa tỷ USD*, <https://vtc.vn/30-giay-dot-kich-sao-huyet-co-bac-nua-ty-usd-ar737208.html>, truy cập 30/10/2023.

7 Tham khảo quy trình khám nghiệm hiện trường có phương tiện điện tử trong tài liệu Trần Văn Hòa, *An toàn thông tin và công tác phòng chống tội phạm sử dụng công nghệ cao*, Nxb. Công an nhân dân, 2011, tr. 369 – 373.

định kỹ thuật hình sự, tuy nhiên trường hợp nào cần trưng cầu giám định vẫn chưa được quy định cụ thể trong pháp luật tố tụng hình sự. Theo Điều 206 của BLTTHS năm 2015, giám định dữ liệu điện tử không phải là trưng cầu giám định. Có tác giả cho rằng “hoạt động giám định dữ liệu điện tử do giám định viên tư pháp sử dụng thiết bị, công nghệ phù hợp thực hiện việc sao chép, phục hồi, giải mã, phân tích và tìm kiếm dữ liệu lưu trong tang vật là thiết bị lưu trữ.⁸ Đối chiếu với quy định tại khoản 3 Điều 107 của BLTTHS năm 2015: “Khi nhận được quyết định trưng cầu giám định của cơ quan có thẩm quyền tiến hành tố tụng thì cá nhân, tổ chức có trách nhiệm thực hiện phục hồi, tìm kiếm, giám định dữ liệu điện tử” và “kết quả phục hồi, tìm kiếm, giám định phải chuyển sang dạng có thể đọc, nghe hoặc nhìn được” (khoản 4 Điều 107 của BLTTHS năm 2015), từ đó suy ra trưng cầu giám định dữ liệu điện tử khi cần phục hồi, tìm kiếm, giám định dữ liệu điện tử. Nếu các dữ liệu điện tử trước đó đã bị xóa, bị ẩn, bị ghi đè hoặc nghi ngờ có sửa chữa, cắt ghép hoặc được mã hóa mà không thể đọc, nghe hoặc nhìn được nhưng cần sử dụng để chứng minh vụ án thì mới trưng cầu giám định. Nếu dữ liệu điện tử ở dạng đọc, nghe, nhìn được hoặc có chứng cứ khác thay thế thì không cần phải trưng cầu giám định dữ liệu điện tử để thu thập chứng cứ.

Trong điều tra bằng biện pháp kỹ thuật số nói chung và giám định dữ liệu điện tử nói riêng, các phần mềm chuyên dụng có vai trò rất lớn để phát hiện, sao chép, giải mã, phục hồi chứng cứ điện tử. Các phần mềm này cần được các cơ quan liên ngành công nhận để thống nhất sử dụng trong trường hợp sao chép chống ghi (*read only*), khi cần trích xuất thông tin, giải mã thông tin và phục hồi dữ liệu điện tử/chứng cứ điện tử bị xóa, bị thay đổi nhằm bảo đảm tính khách quan, toàn vẹn của chứng cứ thu thập được.⁹ Theo quy định, để bảo vệ dữ liệu gốc, việc phục hồi, tìm kiếm, giám định dữ liệu điện tử chỉ được thực hiện trên bản sao (khoản 4 Điều 107 của BLTTHS năm 2015), tất nhiên nội dung bản sao phải nguyên vẹn như bản gốc. Vì thế, để bảo đảm khách quan, quá trình sao chép dữ liệu điện tử từ bản gốc sang bản sao để xử lý thông tin cần có sự chứng kiến của chủ dữ liệu (người phạm tội), người bào chữa. Hiện nay, thủ tục này chưa được quy định cụ thể nên không

8 Cao Anh Đức, Ngô Thị Bích Thu, “Biện pháp thu thập, chuyển hóa, sử dụng chứng cứ điện tử trong vụ án sử dụng công nghệ cao”, *Công thông tin điện tử Viện kiểm sát nhân dân tối cao*, 2021, <https://www.vksndtc.gov.vn/tin-tuc/cong-tac-kiem-sat/bien-phap-thu-thap-chuyen-hoa-su-dung-chung-cu-die-d10-t9873.html?Page=1#new-related>, truy cập ngày 13/10/2023.

9 Hiện nay, theo tìm hiểu của tác giả, phần mềm XRY của hãng Micro Systemation (Thụy Điển) và phần mềm UFED của hãng Cellebrite (Israel) được sử dụng để trích xuất dữ liệu và mật khẩu thiết bị điện thoại di động, bao gồm xuất các dữ liệu quan trọng như nhật ký cuộc gọi, danh bạ, tin nhắn văn bản (SMS), hình ảnh, video, tệp âm thanh, ESN IMEI, thông tin ICCID (mã số định danh của SIM) và IMSI và hơn thế nữa, từ một loạt các thiết bị di động; trích xuất dữ liệu lịch sử duyệt web, facebook, facebook messenger, skype, whatsapp, các ứng dụng của Google (Drive, Email, Calendar, Docs, Duo, Photo,...); trích xuất dữ liệu từ thiết bị của nhiều hệ điều hành: Apple iOS, Blackberry, Android, Symbian, Microsoft Mobile và Palm OS. Phần mềm EnCase của Công ty Guidance (Mỹ) được nhiều cơ quan, chính phủ và các công ty trên thế giới sử dụng chuyên khôi phục, phân tích chứng cứ điện tử và giải pháp khắc phục sự cố khẩn cấp. Xem Trần Văn Hòa, *ltd*, tr. 468.

tránh khỏi thắc mắc, nghi ngờ từ phía người bào chữa và người bị buộc tội về tính đúng đắn của việc sao chép dữ liệu điện tử sang bản sao.

1.4. Tiếp nhận chứng cứ điện tử

Tiếp nhận chứng cứ cũng là một hình thức thu thập chứng cứ thụ động. Điều 88 BLTTHS năm 2015 quy định chung về hình thức thu thập và tiếp nhận chứng cứ: “Để thu thập chứng cứ, người bào chữa có quyền gặp người mà mình bào chữa, bị hại, người làm chứng và những người khác biết về vụ án để hỏi, nghe họ trình bày về những vấn đề liên quan đến vụ án; đề nghị cơ quan, tổ chức, cá nhân cung cấp tài liệu, đồ vật, dữ liệu điện tử liên quan đến việc bào chữa” (khoản 2); “Những người tham gia tố tụng khác, cơ quan, tổ chức hoặc bất cứ cá nhân nào đều có thể đưa ra chứng cứ, tài liệu, đồ vật, dữ liệu điện tử và trình bày những vấn đề có liên quan đến vụ án” (khoản 3).

Điều luật cũng quy định thủ tục tiếp nhận chứng cứ: Khi tiếp nhận chứng cứ, tài liệu, đồ vật, dữ liệu điện tử liên quan đến vụ án do những người quy định tại khoản 2 và khoản 3 Điều 88 cung cấp, cơ quan có thẩm quyền tiến hành tố tụng phải lập biên bản giao nhận và kiểm tra, đánh giá theo quy định của BLTTHS năm 2015.

Vướng mắc phát sinh khi các dữ liệu điện tử do các cá nhân, cơ quan, tổ chức phát hiện, giao nộp nhưng chưa có đầy đủ thông tin về quá trình thu giữ cũng như nguồn gốc, xuất xứ của các dữ liệu này. Nếu dữ liệu điện tử không bị mã hóa, có thể trực tiếp nhìn, nghe, đọc được thì cũng cần kết hợp với các biện pháp thu thập chứng cứ khác như lấy lời khai, đối chất, nhận dạng, thực nghiệm điều tra... để kiểm tra chứng cứ điện tử. Nếu có sự nghi ngờ nguồn gốc của dữ liệu điện tử do các cá nhân, tổ chức, cá nhân cung cấp hoặc nghi ngờ tính khách quan của chứng cứ điện tử thì trưng cầu giám định để thu thập chứng cứ. Điều 88 BLTTHS năm 2015 không quy định trường hợp từ chối tiếp nhận chứng cứ, tài liệu đồ vật, dữ liệu điện tử nếu người có thẩm quyền cho rằng không liên quan đến vụ án, không được thu thập hợp pháp hoặc không cần thiết sử dụng để chứng minh vụ án.

Như vậy, việc tiếp nhận dữ liệu điện tử do các cá nhân, tổ chức, cơ quan cung cấp cũng là biện pháp thu thập chứng cứ điện tử. Để bảo đảm tính khách quan của chứng cứ, cần kết hợp thực hiện các biện pháp điều tra khác, kể cả phải giám định dữ liệu điện tử.

1.5. Thu thập chứng cứ điện tử bằng biện pháp điều tra tố tụng đặc biệt

Điều 223 BLTTHS năm 2015 quy định các biện pháp điều tra tố tụng đặc biệt: “Sau khi khởi tố vụ án, trong quá trình điều tra, người có thẩm quyền tiến hành tố tụng có thể áp dụng các biện pháp điều tra tố tụng đặc biệt: 1. Ghi âm, ghi hình bí mật; 2. Nghe điện thoại bí mật; 3. Thu thập bí mật dữ liệu điện tử”. Trường hợp áp dụng biện pháp điều tra tố tụng đặc biệt để thu thập chứng cứ điện tử được áp dụng đối với các tội: Tội xâm phạm an ninh quốc gia, tội phạm

về ma túy, tội phạm về tham nhũng, tội khủng bố, tội rửa tiền; Tội phạm khác có tổ chức thuộc loại tội phạm đặc biệt nghiêm trọng (Điều 224 BLTTHS năm 2015). Có thể nhận thấy các biện pháp điều tra tố tụng đặc biệt được quy định tại Điều 223 của BLTTHS năm 2015 đều ít nhiều liên quan đến dữ liệu điện tử. Có thể là dữ liệu điện tử có chứa các chứng cứ được cơ quan có thẩm quyền tiến hành tố tụng chủ động và bí mật ghi lại trong phương tiện điện tử như tiến hành ghi âm, ghi hình bí mật. Đối với các dữ liệu điện tử do người phạm tội hoặc người khác khởi tạo, lưu trữ, truyền đi hoặc nhận thì việc thu thập được tiến hành bí mật để thu giữ, chặn thu các dữ liệu điện tử đó.

Đặc điểm của hoạt động thu thập chứng cứ bằng biện pháp điều tra tố tụng đặc biệt là biện pháp điều tra được tiến hành bí mật nhưng có sự kiểm sát của Viện kiểm sát ngay từ khi bắt đầu áp dụng. Đặc điểm này cũng cho thấy biện pháp điều tra tố tụng đặc biệt khác với biện pháp thu thập chứng cứ điện tử bằng biện pháp trình sát nghiệp vụ, tuy nhiên cách thức thực hiện có thể giống nhau. Quy định biện pháp điều tra trong BLTTHS năm 2015 cũng là minh chứng cho việc thực hiện các cam kết quốc tế về tăng cường đấu tranh với một số loại tội phạm nghiêm trọng trên cơ sở vẫn bảo đảm quyền con người, quyền công dân, tạo điều kiện tốt cho việc hội nhập và hợp tác quốc tế.¹⁰ Đây cũng là thách thức khi thu thập chứng cứ điện tử bằng biện pháp điều tra tố tụng đặc biệt mà “quyền con người và quyền công dân chỉ có thể bị hạn chế theo quy định của luật trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng” (Điều 14 của Hiến pháp năm 2013), cụ thể có thể hạn chế quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; quyền bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác được quy định tại Hiến pháp (Điều 21 của Hiến pháp năm 2013). Để hạn chế việc lạm dụng biện pháp, quyết định áp dụng biện pháp điều tra tố tụng đặc biệt ghi rõ thông tin cần thiết về đối tượng bị áp dụng, tên biện pháp được áp dụng, thời hạn, địa điểm áp dụng, cơ quan tiến hành biện pháp điều tra tố tụng đặc biệt (khoản 2 Điều 225 của BLTTHS năm 2015). Quyết định áp dụng biện pháp điều tra tố tụng đặc biệt phải được Viện trưởng Viện kiểm sát cùng cấp phê chuẩn trước khi thi hành. Thủ trưởng Cơ quan điều tra đã ra quyết định áp dụng có trách nhiệm kiểm tra chặt chẽ việc áp dụng biện pháp này, kịp thời đề nghị Viện kiểm sát hủy bỏ nếu xét thấy không còn cần thiết (khoản 3 Điều 225 của BLTTHS năm 2015); tài liệu không liên quan đến vụ án phải tiêu hủy kịp thời (Điều 227 của BLTTHS năm 2015).

2. Một số khó khăn, thách thức khi thu thập chứng cứ điện tử

Thứ nhất, hợp tác thu thập chứng cứ với các nhà mạng có máy chủ ở

10 Trần Đình Nhã, “Biện pháp điều tra tố tụng đặc biệt”, trong *Những nội dung mới trong Bộ luật Tố tụng hình sự năm 2015*, Nguyễn Hòa Bình (chủ biên), Nxb. CTQG, 2016, tr. 290 - 291.

nước ngoài là thách thức cho các cơ quan có thẩm quyền tiến hành tố tụng, bởi phần lớn các nhà cung cấp dịch vụ trực tuyến lớn có máy chủ ở nước ngoài, phổ biến như Google, Facebook, Youtube, Tiktok, Intergram... Vấn đề khó khăn này cũng gặp ở các nước châu Âu, “có quan chức năng có thể yêu cầu và thu thập các tài liệu cần thiết để điều tra tội phạm trong phạm vi quốc gia của họ, nhưng chứng cứ điện tử được lưu trữ trực tuyến bởi các nhà cung cấp dịch vụ thường có trụ sở tại một quốc gia khác với điều tra viên, ngay cả khi tội phạm chỉ xảy ra ở một quốc gia”.¹¹ Do đó, “để thu thập dữ liệu phải có sự phối hợp với nhà cung cấp dịch vụ qua kênh hợp tác quốc tế; tuy nhiên hoạt động này rất khó khăn do sự khác biệt về quy định pháp luật giữa các quốc gia, rào cản về ngôn ngữ, các nhà dịch vụ thường lấy lý do bảo vệ bí mật khách hàng để từ chối cung cấp hoặc không trả lời”.¹²

Thứ hai, vấn đề thu thập, xử lý chứng cứ điện tử vốn nhạy cảm vì có thể xâm phạm quyền cá nhân và riêng tư của con người, đặc biệt khi áp dụng các biện pháp điều tra tố tụng đặc biệt. Hầu hết các biện pháp này “trong chừng mực khác nhau đều hạn chế một số quyền con người, quyền công dân nào đó”.¹³ Ngoài ra, trong dữ liệu điện tử, phương tiện điện tử có thể chứa các thông tin cá nhân khác (hình ảnh, tài liệu, kể cả sản phẩm trí tuệ) của chủ dữ liệu nhưng không liên quan đến tội phạm. Hiện nay, vẫn chưa có quy định cụ thể trong luật tố tụng hình sự để bảo vệ dữ liệu cá nhân (như yêu cầu được bảo mật; yêu cầu được sao chép để bảo vệ dữ liệu để không bị mất, không bị khai thác trái pháp luật).

Thứ ba, các thành tựu trong lĩnh vực công nghệ số phát triển nhanh, vì vậy mà dữ liệu điện tử và chứng cứ điện tử được khởi tạo, lưu trữ, truyền, nhận từ các phương tiện điện tử ngày càng tinh vi và đa dạng. Từ đó, các cơ quan có thẩm quyền tiến hành tố tụng cần trang bị, sử dụng các phương tiện điện tử hỗ trợ, các phần mềm hiện đại để có thể xử lý, thu thập chứng cứ điện tử. Thách thức này có thể nhận thấy trong cuộc cách mạng công nghiệp lần thứ 4 (từ sau 2013). Trong thời gian ngắn, thế giới được chứng kiến các thành tựu công nghệ số có giá trị vượt bậc như trí tuệ nhân tạo (*artificial intelligence*, AI), vạn vật kết nối (*internet of things*, IOT) và dữ liệu lớn (*big data*), cùng với

11 European Commission, “*Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence*”, 2019, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_19_863/MEMO_19_863_EN.pdf, truy cập ngày 16/10/2023.

12 Cao Anh Đức, Ngô Thị Bích Thu, *tlđđ*, 2021.

13 Trần Đình Nhã, *tlđđ*, 2016, tr. 291; Nguyen Phuong Thao, “The Use of Artificial Intelligence in Criminal Investigation and Trials in Europe and Some Countries: Experience for Vietnam”, *Vietnamese Journal of Legal Sciences*, Vol. 8, No. 1, 2023, <https://doi.org/10.2478/vjls-2023-0003>, tr. 55-77; Ngo Nguyen Thao Vy, “AI Implementation in ODR: A Game-Changer or a Troublemaker of Data Protection”, *Vietnamese Journal of Legal Sciences*, Vol. 8, No. 1, 2023, <https://doi.org/10.2478/vjls-2023-0001>, tr. 1-24; Mathias Artzt and Tran Viet Dung, “Artificial intelligence and data protection: How to reconcile both areas from the European law perspective”, *Vietnamese Journal of Legal Sciences*, Vol. 7, No. 2, 2022, <https://doi.org/10.2478/vjls-2022-0007>, tr. 39-57

sự xuất hiện của mạng xã hội, điện toán đám mây, đặc biệt với sự ra đời của robot có trí tuệ nhân tạo. Sự phát triển nhanh của công nghệ số không chỉ đòi hỏi về các thiết bị, phần mềm chuyên dụng được cập nhật kịp thời để có khả năng phục hồi dữ liệu điện tử, phát hiện chứng cứ mà còn yêu cầu về trình độ sử dụng công nghệ của những người có thẩm quyền tiến hành tố tụng. Dù vậy, hiện nay, những thiết bị, phần mềm chuyên dụng thường có giá thành rất cao, kinh phí điều tra chưa đáp ứng được”.¹⁴

3. Một số kiến nghị nhằm bảo đảm hiệu quả của việc thu thập chứng cứ điện tử

Với mô hình tố tụng Việt Nam hiện nay thì phần lớn chứng cứ và kết quả chứng minh ở giai đoạn tố tụng trước được giai đoạn tố tụng sau kế thừa. Thực tế, chứng cứ điện tử nói riêng và chứng cứ nói chung được thu thập ở giai đoạn điều tra có giá trị chứng minh cao, nhiều khả năng được Viện kiểm sát và Tòa án chấp nhận. Ở giai đoạn xét xử khó có điều kiện thu thập chứng cứ mới cũng như kiểm tra chứng cứ điện tử do thiếu phương tiện để thực hiện. Vì vậy, để Cơ quan điều tra, Viện kiểm sát, Tòa án, người bào chữa có cơ sở chung thừa nhận tính xác thực, tính liên quan và tính hợp pháp của chứng cứ điện tử, cần bổ sung và hướng dẫn chi tiết các trình tự, thủ tục thu thập chứng cứ điện tử. Đề xuất này cũng dựa trên thực tiễn thu thập chứng cứ điện tử, cụ thể như sau:

Thứ nhất, cần hướng dẫn áp dụng một số quy định về thủ tục và biện pháp thu thập chứng cứ điện tử. Thủ tục chuyển hóa dữ liệu điện tử bằng cách in ra tài liệu giấy cần có sự chứng kiến và xác nhận của chủ dữ liệu điện tử. Nếu dữ liệu ở dạng đọc, nghe, nhìn được thì trong quá trình khám xét, khám nghiệm hiện trường có thể in ra tài liệu giấy và yêu cầu chủ dữ liệu điện tử xác nhận từng trang tài liệu giấy. Về biện pháp “chặn thu” dữ liệu điện tử với những dữ liệu công khai trên đường truyền, cơ quan có thẩm quyền thu thập chứng cứ điện tử có thể được thực hiện bằng cách tải (*download*), chia sẻ (*share*), sao chép (*copy*), chụp ảnh các dữ liệu điện tử đang hiển thị và được sao lưu vào phương tiện điện tử khác. Ngoài ra, có thể tổ chức ghi hình, ghi âm các dữ liệu đang phát trực tiếp trên đường truyền vào phương tiện điện tử khác, quá trình này cũng được lập biên bản và đưa vào hồ sơ vụ án. Việc bảo quản các phương tiện điện tử có sao lưu dữ liệu điện tử tương tự như bảo quản vật chứng. Thủ tục sao chép bản gốc dữ liệu điện tử sang bản sao để xử lý thông tin phải có người chủ dữ liệu điện tử chứng kiến và được nhà chuyên môn thực hiện bằng các phần mềm chống ghi (*read only*). Phần mềm này được các cơ quan liên ngành thừa nhận. Thủ tục này bảo đảm tính khách quan, toàn vẹn của bản sao dữ liệu điện tử như bản gốc.

Ngoài ra, cần hướng dẫn chi tiết thủ tục khám nghiệm hiện trường vụ án

14 Cao Anh Đức, Ngô Thị Bích Thu, *ltd*, 2021.

có sử dụng các phương tiện điện tử để phạm tội. Trong đó, cần xác định cách thức bảo vệ hiện trường; vẽ sơ đồ hiện trường các phương tiện điện tử; các loại phương tiện điện tử cần thu giữ; các thao tác thu giữ từng loại phương tiện điện tử (đang hoạt động hoặc đã tắt) sao cho bảo đảm nguyên vẹn thông tin; các thiết bị bảo quản phương tiện điện tử được sử dụng (túi “chống kết nối” như túi Faraday). Về trường hợp cần thiết trưng cầu giám định dữ liệu điện tử, cần quy định là các trường hợp cần phục hồi, tìm kiếm, giám định dữ liệu điện tử, nếu các dữ liệu này bị xóa, bị ẩn, ghi đè hoặc nghi ngờ có sửa chữa, cắt ghép hoặc được mã hóa/định dạng mà không thể đọc, nghe hoặc nhìn được.

Thứ hai, cần bổ sung quy định quyền chủ dữ liệu điện tử được yêu cầu bảo vệ dữ liệu điện tử cá nhân không liên quan đến vụ án được lưu trong phương tiện điện tử bị thu giữ; quyền được sao chép dữ liệu cá nhân không liên quan đến vụ án.

Thứ ba, bên cạnh các giải pháp hoàn thiện thủ tục thu thập chứng cứ điện tử còn có các giải pháp khác bảo đảm thu thập chứng cứ điện tử:

- Thống nhất việc sử dụng các phần mềm chuyên dụng để sao chép (chống ghi), phục hồi, trích xuất dữ liệu bảo đảm thu thập chứng cứ điện tử đáng tin cậy. Yêu cầu này làm giảm bớt sự hoài nghi về tính toàn vẹn và khách quan của các chứng cứ điện tử thu thập được, đặc biệt là khâu giám định dữ liệu điện tử. Ở Việt Nam hiện nay chưa có sự công nhận chính thức về các công cụ, phần mềm được sử dụng để điều tra kỹ thuật số. Các nước tiên tiến trên thế giới đã thực hiện tiêu chuẩn hóa công cụ pháp y kỹ thuật số từ lâu. Ở Hoa Kỳ có Viện Tiêu chuẩn và Công nghệ quốc gia (*National Institute of Standards and Technology, NIST*), Nhóm Công tác khoa học về bằng chứng kỹ thuật số và Tổ chức Tiêu chuẩn hóa quốc tế, họ đã đưa tiêu chuẩn, phương pháp để kiểm chứng các công cụ pháp y kỹ thuật số, xem đây là tiêu chuẩn kỹ thuật được luật hóa (ISO/IEC 27041, 2015).¹⁵ Ở các nước, những phần mềm điều tra (*forensic software*) có thể bao gồm các gói phần mềm phổ biến như EnCase, FTK...¹⁶ Bên cạnh đó, cần đào tạo thường xuyên các điều tra viên, kiểm sát viên, thẩm phán về kiến thức, kỹ năng phát hiện chứng cứ, sử dụng các phương tiện điện tử, phần mềm để đáp ứng nhu cầu thu thập chứng cứ điện tử.

- Áp dụng đúng các biện pháp điều tra tố tụng đặc biệt với sự kiểm sát chặt chẽ của Viện kiểm sát để thu thập chứng cứ điện tử. Yêu cầu này góp phần hạn chế các trường hợp áp dụng biện pháp giống như biện pháp trình sát, do cách thức thực hiện gần giống nhau. Đề xuất này cũng nhằm bảo đảm quyền con người trong quá trình thu thập chứng cứ điện tử.

15 Lê Tấn Quan, *Pháp luật Việt Nam về chứng cứ điện tử*, Luận án Tiến sĩ Luật học, Trường Đại học Kinh tế TP. Hồ Chí Minh, 2022, tr. 109-110.

16 Marjie T. Britz, *Computer forensics and cyber-crime: An introduction*, Third Edition, Pearson Education Inc., 2013, tr. 313.

- Hợp tác với các nhà cung cấp dịch vụ trực tuyến, đặc biệt là nhà cung cấp dịch vụ có máy chủ ở nước ngoài. Thỏa thuận với các nhà cung cấp dịch vụ về điều kiện để cung cấp chứng cứ điện tử phục vụ cho hoạt động khởi tố, điều tra, truy tố, xét xử vụ án hình sự theo thông lệ chung. Mỗi yêu cầu của cơ quan tư pháp phải nêu rõ loại dữ liệu được yêu cầu và cơ sở pháp lý để yêu cầu dữ liệu. Chẳng hạn, nhà cung cấp dịch vụ TikTok, nếu yêu cầu liên quan đến dữ liệu nội dung mà không đáp ứng được các quy định hiện hành đối dữ liệu được yêu cầu thì dữ liệu sẽ không được tiết lộ¹⁷ (thường cần có lệnh tòa/tư pháp nội địa, trát hoặc tương đương). ●

Tài liệu tham khảo

- [1] Bản án số 13/2020/HS-ST, ngày 07/09/2020 của Tòa án nhân dân huyện N. H, tỉnh Q. N. [trans: Award No. 13/2020/HS-ST, dated September 7, 2020, of the People’s Court of N.H District, Q. N. Province]
- [2] Mathias Artzt and Tran Viet Dung, “Artificial intelligence and data protection: How to reconcile both areas from the European law perspective”, *Vietnamese Journal of Legal Sciences*, Vol. 7, No. 2, 2022, <https://doi.org/10.2478/vjls-2022-0007>
- [3] Marjie T. Britz, *Computer forensics and cyber-crime: An introduction*, Third Edition, Pearson Education, Inc, 2013
- [4] Trần Văn Hòa, *An toàn thông tin và công tác phòng chống tội phạm sử dụng công nghệ cao*, Nxb. CAND, 2011 [trans: Tran Van Hoa, *Information Security and High-Tech Crime Prevention*, People’s Police Newspaper Publishing House, 2011]
- [5] Trần Văn Hòa, “Vấn đề chứng cứ điện tử”, trong *Những nội dung mới trong Bộ luật Tố tụng hình sự năm 2015*, Nguyễn Hòa Bình (chủ biên), Nxb. CTQG, 2016 [trans: Tran Van Hoa, “Issues of Electronic Evidence”, *New Content in the Criminal Procedure Code of 2015*, Edited by Nguyễn Hòa Bình, National Political Publishing House, 2016]
- [6] Trần Đình Nhã, “Biện pháp điều tra tố tụng đặc biệt”, trong *Những nội dung mới trong Bộ luật Tố tụng hình sự năm 2015*, Nguyễn Hòa Bình (chủ biên), Nxb. CTQG, 2016 [trans: Tran Dinh Nha, “Special Investigative Measures”, *New Contents in the Criminal Procedure Code of 2015*, Edited by Nguyễn Hòa Bình, National Political Publishing House, 2016]
- [6] Lê Tấn Quan, *Pháp luật Việt Nam về chứng cứ điện tử*, Luận án Tiến sĩ Luật học, Trường Đại học Kinh tế TP. Hồ Chí Minh, 2022 [trans: Lê Tấn Quan, *Vietnamese Law on Electronic Evidence*, Doctoral Dissertation in Law, Ho Chi Minh City University of Economics, 2022]
- [7] Nguyễn Lâm Thanh, “Quản lý nội dung trên nền tảng TikTok tại Việt Nam”, trong tài liệu Hội nghị: *Phòng ngừa vi phạm, tội phạm trong chuyển đổi nền kinh tế số và bảo đảm an ninh thông tin mạng đối với dịch vụ nội dung số tại Việt Nam*, 2023 [trans: Nguyen Lam Thanh, “Content Management on the TikTok Platform in Vietnam”, Document from the *Conference on Prevention of Violations and Crimes in the Digital Transformation of the Economy and Ensuring Cybersecurity for Digital Content Services in Vietnam*, 2023]
- [8] Nguyen Phuong Thao, “The Use of Artificial Intelligence in Criminal Investigation and Trials in Europe and Some Countries: Experience for Vietnam”, *Vietnamese Journal of Legal Sciences*, Vol. 8, No. 1, 2023, <https://doi.org/10.2478/vjls-2023-0003>
- [9] Trường Đào tạo, Bồi dưỡng nghiệp vụ kiểm sát TP. Hồ Chí Minh, tài liệu tập huấn: *Nâng cao hiệu quả công tác thực hành quyền công tố, kiểm sát điều tra, kiểm sát xét xử các vụ án về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông*, 6/2023 [trans: Training Institute for Prosecution and Investigation Profession in Ho Chi Minh City, Training Document: *Enhancing the Effectiveness of Practicing Prosecutorial Authority, Investigative Prosecution, and Prosecutorial Examination in Cases of Crimes in the Field of Information Technology and Telecommunications*, 2023]
- [10] Ngo Nguyen Thao Vy, “AI Implementation in ODR: A Game-Changer or a Troublemaker of Data Protection”, *Vietnamese Journal of Legal Sciences*, Vol. 8, No. 1, 2023, <https://doi.org/10.2478/vjls-2023-0001>

17 Nguyễn Lâm Thanh, “Quản lý nội dung trên nền tảng TikTok tại Việt Nam”, trong tài liệu Hội nghị: *Phòng ngừa vi phạm, tội phạm trong chuyển đổi nền kinh tế số và bảo đảm an ninh thông tin mạng đối với dịch vụ nội dung số tại Việt Nam*, 2023, tr. 59-60.