TỘI PHẠM MẠNG VÀ VIỆC KHAI THÁC DỮ LIỆU ĐIỆN TỬ PHỤC VỤ BUỘC TỘI, TRANH TỤNG TẠI PHIÊN TÒA HÌNH SỰ

NGUYỄN ĐỨC HẠNH*

Bộ luật tố tụng hình sự (BLTTHS) năm 2015 đã có những quy định về việc bổ sung dữ liệu điện tử là một nguồn chứng cứ mới. Điều này có ý nghĩa rất quan trọng đối với các chủ thể tham gia tiến hành tố tụng, đặc biệt là Viện kiểm sát nhân dân (VKSND) trong việc khai thác dữ liệu điện tử phục vụ cho quá trình buộc tội, tranh tụng tại phiên tòa. Bài viết phân tích về tội phạm mạng, vai trò của dữ liệu điện tử trong quá trình tiến hành tố tụng hình sự; nêu lên những khó khăn, thách thức trong việc khai thác nguồn dữ liệu này và đề xuất các giải pháp khắc phục.

Từ khóa: Dữ liệu điện tử, tội phạm mạng, Bộ luật tố tụng hình sự năm 2015.

Ngày nhận bài: 22/12/2020; Biên tập xong: 12/01/2020; Duyệt đăng: 15/01/2021

The 2015 Criminal Procedure Code has supplemented specific regulations that electronic data is one source of evidence. That is very important for participants in the procedures, especially for the People's Procuracy in using electronic data for accusation and ligitation in trail. The article clarifies cybercrime, the role of electronic data in the criminal proceedings; points out difficulities in using electronic data and proposed solutions.

Keywords: Electronic data, cybercrime, the 2015 Criminal Procedure Code.

1. Khái niệm tội phạm mạng và phân loại tội phạm mạng

1.1. Khái niệm tội phạm mạng và đặc điểm cơ bản

Tội phạm mạng là một khái niệm hiện nay đã được dùng tương đối phổ biến trong đời sống xã hội. Đề cập đến khái niệm này có nhiều nghiên cứu khác nhau, nhưng nhìn chung, có thể hiểu *Tội phạm mạng* là một hành vi gây nguy hiểm đáng kể cho xã hội, vi phạm pháp luật, được thực hiện bằng cách sử dụng công nghệ thông tin và truyền thông (ICT- *information and communication technology*) để nhắm vào các mục tiêu là mạng máy tính, hệ thống, dữ liệu, trang web hoặc thông qua các công nghệ thông tin và truyền thông (ICT) tạo tiền đề, điều kiện để thực hiện hành vi phạm tội thông thường.[1, 2, 3, 4, 5]. Khoản 7 Điều 2 Luật an ninh mạng năm 2018 cũng nêu khái niệm về *Tội phạm mạng*. Đó là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật hình sự.

Một cách khái quát, có thể thấy tội phạm mạng có các đặc điểm cơ bản rất khác so với tội phạm truyền thống, đó là:

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

[1] Goodman, Marc D. and Brenner, Susan W. (2002). "*The Emerging Consensus on Criminal Conduct in Cyberspace*", International Journal of Law and Information Technology, Vol. 10, No. 2, 139-223

[2] Wall, David. (2007) "*Cybercrime: The Transformation of Crime in the Information Age Polity*"

[3] Wilson, Clay. (2008), "*Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*"

[4] Maras, Marie-Helen. (2014) "*Computer Forensics: Cybercriminals, Laws and Evidence,second edition*", Jones and Bartlett;

[5] Maras, Marie-Helen. (2016). "*Cybercriminology*", Oxford University Press;

- Tội phạm mạng không bị giới hạn bởi ranh giới địa lý hoặc vật lý;

- Tội phạm mạng khi thực hiện thường dễ dàng hơn, nhanh hơn và mất ít công sức thực hiện hơn so với tội phạm truyền thống;

- Để thực hiện được tội phạm mạng thì bắt buộc phải có máy tính, mạng máy tính, các hình thức công nghệ truyền thông khác làm công cụ, phương tiện thực hiện tội phạm;

- Để thực hiện được tội phạm bắt buộc phải thông qua không gian mạng, sử dụng Internet, công nghệ kỹ thuật số như là một phương thức thực hiện tội phạm cho dù nó là tội phạm truyền thống. Điều đó có nghĩa vai trò của công nghệ thông tin và truyền thông (ICT) đối với hành vi phạm tội là hết sức quan trọng. Công nghệ thông tin và truyền thông (ICT) có thể là mục tiêu của hành vi phạm tội nhưng cũng có thể là phương thức để thực hiện tội phạm.

1.2. Phân loại tội phạm mạng phổ biến

Tội phạm mạng gắn với nhiều yếu tố xã hội, tự nhiên, pháp lý nên có thể được phân ra làm rất nhiều loại khác nhau dựa trên các tiêu chí khác nhau như căn cứ vào tính chất, quy mô; căn cứ vào động cơ, mục đích; căn cứ vào điều luật… Tuy nhiên, trong bài viết này, để phục vụ cho việc khai thác chứng cứ từ nguồn dữ liệu điện tử xuất hiện khi tội phạm mạng được chuẩn bị, thực hiện, che giấu, với tiêu chí là vai trò của không gian mạng đối với việc hình thành tính nguy hiểm cho xã hội, có thể chia tội phạm mạng thành hai loại chính là: Tội phạm được hình thành từ hành vi gây nguy hiểm cho không gian mạng và tội phạm được hình thành bằng việc thực hiện các hành vi phạm tội truyền thống có sử dụng không gian mạng và công nghệ thông tin để phạm tội.

Chúng ta biết rằng, khi ICT là mục tiêu của hành vi phạm tội, tính nguy hiểm của hành vi phạm tội gây ảnh hưởng tiêu cực đến *tính bảo mật, tính toàn vẹn, tính khả dụng* của dữ liệu hoặc hệ thống máy tính[6]. Nói một cách đơn giản, thông tin cá nhân phải ở chế độ riêng tư, không được thay đổi nếu không có sự cho phép của chủ sở hữu và dữ liệu, dịch vụ và hệ thống nên được chủ sở hữu truy cập mọi lúc. Tội phạm này có các hành vi đặc trưng như tấn công mạng, gián điệp mạng. Trong đó, *Tấn công mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử. *Gián điệp mạng* là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của cơ quan, tổ chức, cá nhân.

Khi ICT là phương thức, phương tiện thực hiện hành vi phạm tội thì tính nguy hiểm của hành vi phạm tội chính là tính nguy hiểm của tội phạm truyền thống mà thông qua ICT để thực hiện[6]. Ví dụ: Hành vi sử dụng Internet, các công nghệ kỹ thuật số để lừa đảo, trộm cắp, khủng bố, tài trợ khủng bố...

2. Dữ liệu điện tử, sự xuất hiện và phân loại dữ liệu điện tử khi tội phạm mạng được thực hiện

2.1. Khái niệm dữ liệu điện tử

Điều 99 BLTTHS năm 2015 quy định: *"1. Dữ liệu điện tử là ký hiệu, chữ viết, chữ số,*

[6] UNODC (2013) *"Comprehensive Study on Cybercrime"*

hình ảnh, âm thanh hoặc dạng tương tự được tạo ra, lưu trữ, truyền đi hoặc nhận được bởi phương tiện điện tử. 2. Dữ liệu điện tử được thu thập từ phương tiện điện tử, mạng máy tính, mạng viễn thông, trên đường truyền và các nguồn điện tử khác".

Tuy nhiên, chúng tôi cho rằng đối với các ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự, con người chỉ có thể nhận biết được thông qua các thiết bị, phương tiện điện tử, phần mềm thích hợp bởi nó tồn tại dưới dạng kỹ thuật số gồm các số "0" và số "1" trong các thiết bị được chứa bằng các đơn vị nhớ là byte, bit, mà ở trạng thái tự nhiên chúng ta không thể nhìn thấy, nghe thấy hoặc nhận biết những dữ liệu trong các thiết bị chứa đựng nó. Ví dụ: Bộc lộ một thẻ nhớ bằng trực quan chúng ta không thể thấy được hình ảnh, âm thanh, ký tự… nhưng khi lắp vào máy tính, sử dụng phần mềm thích hợp để đọc thẻ nhớ chúng ta có thể thấy, nhận biết được các âm thanh, hình ảnh, ký tự… hoặc nếu sử dụng phần mềm không thích hợp thì mặc dù vẫn máy tính đó, thẻ nhớ đó nhưng cũng không thể thấy, nhận biết được các âm thanh, hình ảnh… Bên cạnh đó, còn đòi hỏi có chuyên gia biết sử dụng các phần mềm này.

Khoản 1 Điều 87 BLTTHS năm 2015 quy định dữ liệu điện tử là một trong các nguồn chứng cứ. Đây là một trong những cơ sở để những người có thẩm quyền tiến hành tố tụng có thể khai thác chứng cứ dùng để chứng minh tội phạm, kết tội đối người bị buộc tội và cũng là căn cứ để người bị buộc tội, người bào chữa khai thác chứng cứ nhằm tranh tụng, bào chữa trong tiến trình tố tụng.

Như vậy, nếu xem xét dưới góc độ khả năng nhận biết về dữ liệu điện tử bằng các giác quan của con người gắn với ý nghĩa khai thác, sử dụng trong việc tranh tụng, buộc tội, có thể đưa ra khái niệm về dữ liệu điện tử như sau: "*Dữ liệu điện tử là một trong các nguồn chứng cứ được quy định trong Bộ luật tố tụng hình sự ở trạng thái tự nhiên; dữ liệu điện tử có trong các thiết bị, phương tiện điện tử hoặc được truyền đi, tiếp nhận từ các thiết bị, phương tiện điện tử, khi thông qua một phần mềm thích hợp các dữ liệu điện tử sẽ biểu hiện dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự mà con người có thể nhận biết được bằng các giác quan*".

2.2. Sự xuất hiện của dữ liệu điện tử khi tội phạm mạng được thực hiện, trong tiến trình tố tụng và phân loại dữ liệu điện tử

Dữ liệu điện tử, thông qua phần mềm thích hợp và phương tiện điện tử thích hợp, có thể biểu hiện dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự mà con người có thể nhận biết được bằng các giác quan.

Để thực hiện một tội phạm mạng, ngoài yếu tố con người, còn có ba yếu tố cần thiết bao gồm: Các thiết bị phần cứng, phần mềm và mạng Internet có khả năng truy cập của các thiết bị[7]. Trường hợp tội phạm tấn công mạng máy tính, ngoài các hành vi tác động mang tính vật lý thì những đối tượng phạm tội sử dụng thiết bị điện tử thông qua đường mạng Internet cùng với các phần mềm điều khiển hệ thống máy tính để tiếp cận đối tượng tấn công và can thiệp vào các đối tượng này làm mất tính năng sử dụng, hoạt động như vốn có ban đầu của nó. Quá trình này diễn ra luôn có các dữ liệu điện tử trong không gian mạng, trên đường truyền và trong các thiết bị máy tính (phần cứng) của đối tượng thực hiện hành vi phạm tội và thiết bị máy tính là đối tượng tấn công của tội phạm. Tương tự như vậy, khi một tội phạm truyền

[7] Marco Gercke (2009), *"An introduction to cybercrime"*, Resource Material series No. 79, UNAFEI, 8

thống được thực hiện như tội lừa đảo qua mạng, đối tượng phạm tội thông qua không gian mạng để tiếp cận người bị hại thực hiện hành vi gian dối để người bị hại chuyển tiền cho đối tượng bằng trực tuyến hoặc ngoại tuyến thì dữ liệu điện tử cũng luôn có trong không gian mạng, thiết bị máy tính của đối tượng phạm tội, người bị hại và các phần mềm giúp đối tượng phạm tội và người bị hại giao dịch, trao đổi, giao tiếp với nhau.

Sau khi tội phạm được thực hiện, trong quá trình giải quyết vụ án, các cơ quan có thẩm quyền tiến hành tố tụng có thể áp dụng các biện pháp điều tra nhằm phát hiện và thu thập chứng cứ như trưng cầu giám định, thực nghiệm điều tra, ghi âm, ghi hình, các biện pháp điều tra bằng phương pháp kỹ thuật số (ghi âm, ghi hình có âm thanh khi lấy lời khai, hỏi cung bị can), áp dụng các biện pháp điều tra đặc biệt… Kết quả của việc áp dụng các biện pháp điều tra này cũng có thể tạo ra, hình thành các dữ liệu điện tử là nguồn chứng cứ có khả năng xác định sự thật khách quan của vụ án.

Như vậy, có thể thấy, trong quá trình giải quyết một vụ án hình sự, dữ liệu điện tử có thể được hình thành từ khi tội phạm được chuẩn bị, thực hiện, che giấu hoặc dữ liệu cũng có thể được hình thành khi các cơ quan tiến hành tố tụng, các cơ quan, tổ chức, cá nhân khác tạo ra sau khi tội phạm đã được thực hiện nhằm góp phần giải quyết vụ án hình sự.

Căn cứ vào mức độ khách quan, độ tin cậy của các dữ liệu điện tử trong việc khai thác thông tin từ nguồn dữ liệu điện tử nhằm giải quyết vụ án hình sự, có thể chia dữ liệu điện tử thành các loại sau:

- Dữ liệu điện tử do máy tính tự động tạo ra như: "Cookies", "URL", E-mail logs, web server logs, IP, thông tin truy cập tài khoản, website… Đặc điểm của các dạng dữ liệu này là mang tính khách quan, không phụ thuộc vào ý thức của người bị hại hoặc các đối tượng sử dụng các thiết bị, phương tiện điện tử nếu không phải là đối tượng quản lý có khả năng điều chỉnh các thiết bị, phương tiện điện tử này.

- Dữ liệu điện tử do đối tượng thực hiện hành vi phạm tội hoặc người bị hại tạo ra như: Các văn bản, bảng biểu, hình ảnh, thông tin… là nội dung của các thông điệp điện tử như email, chat, các dữ liệu tải xuống (download) và tải lên (upload) mạng... Các dữ liệu này có thể mang tới những thông điệp thông tin như nó vốn có nhưng cũng có thể mang lại những thông điệp thông tin không đúng với bản chất sự vật, hiện tượng bởi sự chỉnh sửa, xóa bỏ bớt dữ liệu hoặc bổ sung thêm vào dữ liệu.

- Dữ liệu điện tử do các cơ quan chức năng hoặc cơ quan có thẩm quyền tố tụng tạo ra như: Dữ liệu trong các thiết bị, phương tiện điện tử khi tiến hành các biện pháp điều tra tố tụng đặc biệt, ghi lại việc thực nghiệm điều tra, khám nghiệm hiện trường, hỏi cung bị can…

3. Khái niệm chứng cứ điện tử và việc khai thác chứng cứ điện tử phục vụ việc buộc tội, tranh tụng tại phiên tòa

3.1. Khái niệm chứng cứ điện tử

Trong quá trình giải quyết vụ án hình sự, các chủ thể tiến hành và tham gia tố tụng bắt buộc phải sử dụng chứng cứ để đưa ra các quyết định và hành vi tố tụng, có như vậy mới phù hợp với quy định của pháp luật và thực hiện tốt chức năng, nhiệm vụ của các chủ thể được Luật tố tụng hình sự quy định. Trong quá trình tham gia tố tụng, không chỉ Viện kiểm sát mà ngay cả đối với các chủ thể khác, để có thể buộc tội và tranh tụng thành công thì chứng cứ là "vũ khí" quyết định thắng lợi. Nếu không có chứng cứ, không đủ chứng

cứ tất yếu sẽ dẫn đến oan, sai và bỏ lọt tội phạm, đồng thời cũng không có đủ lý lẽ đối đáp khi tranh tụng. BLTTHS năm 2015 lần đầu tiên quy định dữ liệu điện tử là một trong số những nguồn chứng cứ, đòi hỏi các chủ thể tiến hành và tham gia tố tụng muốn thực hiện tốt chức năng, nhiệm vụ của mình phải hiểu biết và khai thác tốt chứng cứ từ nguồn này, cũng như hiểu được mối tương quan giữa dữ liệu điện tử và các nguồn chứng cứ khác.

Theo quy định của Điều 86 BLTTHS năm 2015 thì: *"Chứng cứ là những gì có thật, được thu thập theo trình tự, thủ tục do Bộ luật này quy định, được dùng làm căn cứ để xác định có hay không có hành vi phạm tội, người thực hiện hành vi phạm tội và những tình tiết khác có ý nghĩa trong việc giải quyết vụ án"*. Trong đó, "những gì" ở đây có thể hiểu là những thông tin mà mọi người có thể nhận biết được trực tiếp bằng các giác quan hoặc thông qua một phương tiện nhất định. Những thông tin này có thật, tức là nó phản ánh khách quan về một sự vật, hiện tượng cụ thể, đồng thời có liên quan đến việc giải quyết vụ án hình sự và đảm bảo tính hợp pháp thông qua việc được thu thập theo trình tự, thủ tục do Luật tố tụng hình sự quy định.

Để có được chứng cứ, những chủ thể có thẩm quyền thu thập chứng cứ chỉ được tìm kiếm, phát hiện và thu thập từ các nguồn chứng cứ được quy định tại khoản 1 Điều 87 BLTTHS năm 2015, trong đó có nguồn chứng cứ là dữ liệu điện tử. Mặc dù BLTTHS năm 2015 không đề cập đến thuật ngữ *"chứng cứ điện tử"* và không đưa ra khái niệm về *"chứng cứ điện tử"*, nhưng trong thực tiễn hoạt động tố tụng, trong nghiên cứu khoa học, nhiều người vẫn sử dụng thuật ngữ này. Chúng tôi đồng tình với việc sử dụng thuật ngữ này với ý nghĩa như là một trường hợp đặc biệt của chứng cứ và có thể đưa ra khái niệm về *"chứng cứ điện tử"*, đó là chứng cứ được khai thác hoặc thu thập được từ nguồn dữ liệu điện tử.

3.2. Khai thác chứng cứ điện tử phục vụ việc buộc tội, tranh tụng tại phiên tòa xét xử vụ án hình sự

Trên cơ sở khái niệm chứng cứ điện tử nêu trên, có thể hiểu khai thác chứng cứ điện tử là việc các chủ thể có thẩm quyền tiến hành tố tụng và chủ thể tham gia tố tụng, trong đó có Viện kiểm sát lựa chọn những thông tin có được từ nguồn dữ liệu điện tử để bảo vệ quan điểm của mình đối với quá trình giải quyết vụ án hình sự nhằm thực hiện chức năng tố tụng hình sự của chủ thể đó. VKSND tham gia tố tụng có hai chức năng là thực hành quyền công tố và kiểm sát việc giải quyết vụ án hình sự. Do đó, Viện kiểm sát khai thác chứng cứ từ nguồn dữ liệu điện tử nhằm mục đích chủ yếu là buộc tội người thực hiện hành vi nguy hiểm cho xã hội bị coi là tội phạm, thực hiện việc tranh tụng với các chủ thể đối tụng khác bằng việc bảo vệ quan điểm truy tố, bác bỏ những luận điểm bào chữa của người bào chữa không chính xác, không có căn cứ và bảo đảm việc giải quyết vụ án hình sự được nhanh chóng, kịp thời, đúng người, đúng tội, đúng pháp luật, không làm oan người vô tội, không bỏ lọt tội phạm, phát hiện và làm rõ những vi phạm thiếu sót trong hoạt động giải quyết vụ án hình sự để có những yêu cầu, kiến nghị, kháng nghị nhằm khắc phục vi phạm.

Buộc tội và tranh tụng tại phiên tòa xét xử vụ án hình sự là một trong những hoạt động thực hành quyền công tố của VKSND, sử dụng các chứng cứ đã thu thập được từ các nguồn chứng cứ khác nhau nhằm truy cứu trách nhiệm hình sự đối với bị cáo tại phiên tòa và bảo vệ quan điểm truy tố của Viện kiểm sát, phản bác lại những luận cứu bào chữa của bị cáo

và người bào chữa. Dữ liệu điện tử có ý nghĩa hết sức quan trọng đối với VKSND trong việc buộc tội, tranh tụng tại phiên tòa, bởi đây là một trong số nguồn chứng cứ đã được BLTTHS ghi nhận. Để dữ liệu điện tử thực sự trở thành nguồn chứng cứ hữu dụng trong quá trình tiến hành tố tụng cần lưu ý một vài điểm như sau:

+ Dữ liệu điện tử luôn được chứa đựng hoặc truyền, phát, tiếp nhận bởi các thiết bị, phương tiện điện tử nên các thiết bị, phương tiện điện tử này tất yếu sẽ trở thành vật chứng của vụ án hình sự. Để thu giữ, kiểm tra, xem xét, đánh giá đối với dữ liệu điện tử, đôi khi các cơ quan tiến hành tố tụng phải lập biên bản đối với từng hoạt động và như vậy, nguồn chứng cứ là biên bản phản ánh các hoạt động tố tụng đã song hành và củng cố, thống nhất với dữ liệu điện tử, tạo thành sự thống nhất, phù hợp giữa hệ thống chứng cứ mà Viện kiểm sát có thể khai thác để buộc tội và tranh tụng.

+ Do dữ liệu điện tử có thuộc tính khôi phục sau khi bị xóa nên thông qua những phần mềm chuyên biệt, với những thiết bị, phương tiện điện tử nhất định, các chuyên gia có thể khôi phục lại dữ liệu điện tử. Có thể lý giải điều này là việc đưa dữ liệu điện tử trở về trạng thái ban đầu mà khi thông qua thiết bị, phương tiện điện tử, phần mềm có thể biểu hiện thành các thông điệp chứa đựng thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự mà con người có thể nhận biết được như trước khi bị xóa. Từ đó, Cơ quan điều tra, Viện kiểm sát có thể trưng cầu chuyên gia khôi phục lại dữ liệu điện tử bị xóa trong các thiết bị và phương tiện điện tử thu giữ được.

+ Dữ liệu điện tử có thể được sao chép từ dữ liệu điện tử gốc thành nhiều dữ liệu điện tử mới có cùng thuộc tính, nội dung và khi thông qua thiết bị, phương tiện điện tử có cùng thuộc tính, tiêu chuẩn với cùng một loại phần mềm thì sẽ có các thông điệp chứa đựng thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự mà con người có thể nhận biết, cảm nhận được. Do đó, Cơ quan điều tra, Viện kiểm sát có thể sao chép các dữ liệu từ hệ thống máy chủ, nhà mạng, đám mây… phục vụ cho việc giải quyết vụ án hình sự.

+ Dữ liệu điện tử có thể truyền trong không gian từ thiết bị, phương tiện điện tử này đến thiết bị, phương tiện điện tử khác trong một khoảng thời gian mà không cần dây dẫn, với khoảng cách xa nên Cơ quan điều tra, Viện kiểm sát có thể tìm kiếm, phát hiện và thu giữ các dữ liệu điện tử này trong không gian khi đang được truyền phát mà không cần phải thu giữ được thiết bị thu, phát. Việc phát hiện, thu giữ dữ liệu điện tử khi cần thiết sẽ cần đến sự trợ giúp từ những cán bộ có chuyên môn nghiệp vụ và cần phải tuân theo những quy định cụ thể có trong BLTTHS.

Lời khai, lời trình bày của bị can, bị hại, nhân chứng… trong nhiều trường hợp được ghi âm, ghi hình có âm thanh hoặc việc ghi hình, chụp ảnh việc khám nghiệm hiện trường, thực nghiệm điều tra…, tức là được lưu trữ dưới dạng dữ liệu điện tử có ý nghĩa trong việc buộc tội và tranh tụng đối với Viện kiểm sát. Đặc biệt là trong trường hợp sau khi khai nhận, bị can, bị cáo và những người được lấy lời khai phản cung, thay đổi lời khai tại phiên tòa.

Để đưa ra những kết luận giám định khách quan, chính xác, các giám định viên có thể phải tiến hành thực nghiệm, phải so sánh các mẫu vật, cũng như có nhiều hoạt động khác sử dụng các thiết bị, phương tiện điện tử nên sẽ khởi tạo ra các dữ liệu điện tử. Khi đó, các thiết bị, phương tiện

điện tử càng hiện đại, tiện nghi thì kết quả giám định càng khách quan, chính xác, giúp cho việc buộc tội là đúng đắn và quá trình tranh tụng của Viện kiểm sát được thuyết phục, đầy đủ, thuận lợi.

Có những trường hợp kết quả ủy thác tư pháp hình sự và hợp tác quốc tế giữa các quốc gia, cơ quan tư pháp được trao đổi, thực hiện thông qua các thiết bị, phương tiện điện tử để hạn chế chi phí tố tụng và rút ngắn thời gian thực hiện nên sẽ có các dữ liệu điện tử chứa đựng kết quả này, hỗ trợ tích cực cho việc buộc tội và tranh tụng của Viện kiểm sát tại các phiên tòa xét xử vụ án hình sự. Ví dụ, có thể sử dụng cầu truyền hình, email... để lấy lời khai nhân chứng, bị hại.

Thông qua dữ liệu điện tử liên quan trực tiếp đến hành vi phạm tội khi tội phạm được chuẩn bị, thực hiện hoặc che giấu mà Cơ quan điều tra, Viện kiểm sát có thể tìm kiếm, phát hiện, thu thập, củng cố các nguồn chứng cứ khác và ngược lại, cụ thể như:

+ Trong quá trình giải quyết vụ án hình sự, các cơ quan tiến hành tố tụng thường xuyên thông qua dữ liệu điện tử để phát hiện ra nguồn chứng cứ khác và ngược lại. Ví dụ: Đối tượng lạ mặt vào nhà nạn nhân để hiếp dâm sau đó bỏ trốn, Cơ quan điều tra đã trích xuất camera an ninh nhà hàng xóm để nhận diện đối tượng, trên cơ sở đó tiến hành lập biên bản ghi lời khai các đối tượng hiềm nghi *(Đây là trường hợp thông qua nguồn dữ liệu điện tử để phát hiện nguồn chứng cứ khác).*

+ Khi lấy lời khai, đối tượng hiềm nghi trình bày rằng: Trước đó đã gọi điện cho nạn nhân bằng sim điện thoại rác để hẹn gặp, sau đó đã khống chế nạn nhân và đưa nạn nhân về nhà đối tượng để thực hiện hành vi hiếp dâm và có dùng điện thoại ghi lại. Căn cứ vào lời khai này, Cơ quan điều tra đã trích xuất các camera dọc tuyến đường mà đối tượng di chuyển cùng nạn nhân, rút lists (danh sách) điện thoại di động theo số thuê bao của nạn nhân và đối tượng, thu thập các video clips (băng ghi hình) được ghi lại trong điện thoại của đối tượng để chứng minh hành vi phạm tội *(Đây là trường hợp thông qua các nguồn chứng cứ khác để phát hiện dữ liệu điện tử),* củng cố chứng cứ chứng minh hành vi phạm tội. Ngay cả khi bị cáo phản cung vẫn có đủ chứng cứ để buộc tội.

Nói cách khác, chứng cứ điện tử có khả năng củng cố các chứng cứ có được từ các nguồn chứng cứ khác và ngược lại, các chứng cứ có được từ các nguồn chứng cứ khác cũng có khả năng củng cố chứng cứ thu thập được từ nguồn dữ liệu điện tử, giúp cho việc buộc tội và tranh tụng của Viện kiểm sát dễ dàng, thuyết phục và chính xác. Nắm vững và khai thác tốt mối quan hệ này còn giúp Viện kiểm sát có căn cứ vững chắc buộc tội, tranh tụng và đề nghị giải quyết các vấn đề khác của vụ án hình sự ngay cả khi có việc phản cung hoặc thay đổi lời khai trước đó.

4. Khó khăn, vướng mắc và thách thức trong việc khai thác nguồn dữ liệu điện tử phục vụ việc buộc tội, tranh tụng tại phiên tòa

Mặc dù dữ liệu điện tử rất quan trọng và có ý nghĩa trong việc khai thác nhằm phục vụ việc buộc tội, tranh tụng tại phiên tòa xét xử hình sự, nhưng trong thực tiễn hiện nay, việc tổ chức thực hiện áp dụng các quy định pháp luật có liên quan và việc triển khai hoạt động khai thác dữ liệu điện tử nhằm phục vụ việc buộc tội, tranh tụng tại phiên tòa hình sự gặp không ít khó khăn, vướng mắc. Có thể kể đến như:

- Hiện nay, hệ thống các khung pháp lý quy định về việc khai thác dữ liệu điện tử nhằm phục vụ việc buộc tội, tranh tụng tại phiên tòa xét xử hình sự chưa được

ban hành một cách đầy đủ, thống nhất. Chưa có một quy trình chuẩn để thực hiện việc ghi âm, ghi hình có âm thanh bằng kỹ thuật số khi hỏi cung bị can, lấy lời khai, thực nghiệm điều tra, đối chất, nhận dạng… Chưa có các văn bản quy định về cách thức, tiểu chuẩn khi khôi phục dữ liệu điện tử bị xóa từ các thiết bị điện tử, phương tiện điện tử. Chưa có quy định về việc bảo quản, sao chép, lưu trữ các dữ liệu điện tử hình thành từ các hoạt động tố tụng hình sự.

- Các Kiểm sát viên chưa được đào tạo một cách bài bản, đầy đủ để có hiểu biết sâu sắc về dữ liệu điện tử, thiết bị, phương tiện điện tử, phần mềm ứng dụng trên các thiết bị, phương tiện điện tử để có thể khai thác đầy đủ, triệt để các dữ liệu điện tử nhằm phục vụ việc buộc tội, tranh tụng tại phiên tòa xét xử hình sự.

- Các điều kiện đảm bảo, hỗ trợ việc khai thác dữ liệu điện tử phục vụ việc giải quyết các vụ án theo quy định của tố tụng hình sự vẫn còn nhiều hạn chế. Hầu hết các Cơ quan điều tra, Viện kiểm sát, Tòa án chưa được trang bị các thiết bị, phương tiện điện tử và phần mềm tương thích phục vụ cho các hoạt động tố tụng hình sự.

- Việc nhận thức và tổ chức thực hiện các quy định liên quan đến dữ liệu điện tử phục vụ hoạt động điều tra, truy tố, xét xử đến nay vẫn chưa được các cấp, các ngành, các cơ quan tư pháp đánh giá cao và quan tâm một cách đúng mức. Trong phạm vi cả nước, có nhiều khu vực trình độ dân trí còn thấp, kém nên còn xa lạ với các thiết bị, phương tiện điện tử, kỹ thuật số.

- Ngoài những khó khăn nêu trên, còn tồn tại một số thách thức, khó khăn mà nhiều nước trên thế giới cũng gặp phải khi khai thác nguồn dữ liệu điện tử phục vụ việc điều tra, giải quyết vụ án như[8]:

+ Chưa có quy định và sự thống nhất trong việc quy định nghĩa vụ của các công ty viễn thông, các nhà cung cấp dịch vụ mạng máy tính, mạng viễn thông. Những đơn vị này phải cung cấp cho các cơ quan thực thi pháp luật dữ liệu điện tử về người dùng bao gồm nội dung về hoạt động của họ và địa chỉ IP, các thông tin khác không thuộc nội dung sử dụng dịch vụ hoặc không có quy định thống nhất về trách nhiệm lưu giữ các dữ liệu này trong khoảng thời gian là bao lâu. Do đó, trong trường hợp tội phạm sử dụng các phần mềm, trang Web có máy chủ đặt bên ngoài quốc gia mà hành vi phạm tội được diễn ra, các cơ quan tố tụng càng khó thu thập được các dữ liệu điện tử từ nhà mạng.

+ Việc quy định người dùng Internet bắt buộc phải thể hiện rõ danh tính không được sự thống nhất ở các quốc gia, nhiều quốc gia cho phép người dùng có thể ẩn danh (không phải đăng ký tên khi sử dụng). Điều này cũng khiến công tác điều tra, phát hiện tội phạm và buộc tội gặp khó khăn hơn.

+ Khung pháp lý trong việc bảo quản, thu giữ dữ liệu điện tử theo yêu cầu của quốc gia khác vẫn còn là vấn đề nhạy cảm, hoạt động gián điệp thông qua hệ thống mạng máy tính chưa có những quy định thống nhất giữa các quốc gia, chưa có những Công ước quốc tế điều chỉnh cụ thể vấn đề này.

5. Giải pháp nhằm nâng cao chất lượng việc khai thác nguồn dữ liệu điện tử phục vụ việc buộc tội, tranh tụng tại phiên tòa

- Hoàn thiện hệ thống pháp luật liên quan đến việc triển khai thực hiện, quản lý, khai thác dữ liệu điện tử phục vụ việc buộc tội, tranh tụng tại phiên tòa hình sự.

[8] Group 2 (2009) *"Challenges and best practices in cybercrime investigation"*, Resource Material series No. 79, UNAFEI, 107-112

- Sớm số hóa các tài liệu thông thường, các tàng thư tội phạm, thông tin về công dân Việt Nam, người không có quốc tịch, công dân nước ngoài nhập cảnh, xuất cảnh, các kết luận điều tra, cáo trạng, bản án… Hình thành những kho dữ liệu điện tử hỗ trợ việc khai thác để phục vụ việc điều tra, truy tố, xét xử các vụ án hình sự.

- Tổ chức đào tạo, bồi dưỡng, tập huấn để những người có thẩm quyền tố tụng đều hiểu biết sâu sắc về dữ liệu điện tử và chứng cứ điện tử như:

+ Đưa vào chương trình giảng dạy tại các cơ sở đào tạo về tư pháp hình sự chuyên đề chuyên sâu về dữ liệu điện tử, chứng cứ điện tử.

+ Triển khai bồi dưỡng, tập huấn cho lực lượng có thẩm quyền tố tụng đang thực thi pháp luật mà chưa được đào tạo về dữ liệu điện tử, chứng cứ trước đây.

- 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. Đồng thời, củng cố các chứng cứ khác thông qua chứng cứ điện tử và ngược lại.

- Hình thành đội ngũ hỗ trợ và bổ trợ tư pháp có kiến thức chuyên môn sâu, có khả năng sử dụng các trang thiết bị điện tử, phương tiện điện tử, phần mềm để có thể phát hiện các dấu vết phi truyền thống, dấu vết điện tử… nhằm thu thập, bảo quản, giám định, khai thác tốt nhất nguồn chứng cứ điện tử phục vụ giải quyết vụ án.

- 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…

- Hoàn thiện các quy định của tố tụng hình sự trong việc tìm kiếm, phát hiện, ghi nhận, thu thập, bảo quản, đánh giá, sử dụng chứng cứ điện tử bởi loại chứng cứ này có rất nhiều đặc điểm khác biệt so với chứng cứ truyền thống.

- Tăng cường hợp tác quốc tế, chia sẻ thông tin, hiểu biết về dữ liệu điện tử, chứng cứ điện tử trong việc điều tra, truy tố, xét xử các vụ án hình sự; việc sử dụng các thành tựu khoa học kỹ thuật hình sự đặc biệt là kỹ thuật số, kỹ thuật điện tử, trí tuệ nhân tạo trong phát hiện và đấu tranh với các loại tội phạm.

- Sử dụng các phương tiện điện tử, thiết bị điện tử để hỗ trợ việc tương trợ tư pháp hình sự và hợp tác quốc tế trong điều tra, truy tố, xét xử các vụ án hình sự có nhiều đối tượng phạm tội ở các quốc gia khác nhau, tội phạm xuyên quốc gia, tội phạm mạng, tội phạm công nghệ cao… nhằm giảm các chi phí tố tụng, rút ngắn thời gian giải quyết vụ án nhưng vẫn đạt được hiệu quả như mong muốn.

- Các quốc gia trên thế giới cần thống nhất đối với quy định về việc lưu trữ thông tin của nhà cung cấp dịch vụ và kiểm soát thông tin về người dùng, cụ thể[9]:

+ Quy định các nhà cung cấp dịch vụ có nghĩa vụ lưu giữ dữ liệu điện tử liên quan đến người dùng Internet trong thời gian tối thiểu là 180 ngày.

+ Quy định việc yêu cầu xác định người truy cập Internet thông qua các thiết bị đầu cuối tại nơi công cộng thì buộc chủ sở hữu hoặc người phụ trách xác định những thông tin của các cá nhân này./.

[9] Group 1 (2009) *"Issues and measure concerning the legal framework to combat cybercrime"*, Resource Material series No. 79, UNAFEI, 98-106