THU THẬP DẤU VẾT ĐIỆN TỬ TỪ THIẾT BỊ ĐIỆN THOẠI DI ĐỘNG TRONG ĐIỀU TRA TỘI PHẠM

HOÀNG TRỌNG LỰC*

Trong những năm qua, trên thế giới cũng như tại Việt Nam, cùng với sự phát triển không ngừng của công nghệ, điện thoại di động đang ngày càng phát triển và trở thành phương tiện giao tiếp, làm việc chủ yếu của con người. Cùng với sự gia tăng của những chiếc điện thoại thông minh đa chức năng thì số vụ án liên quan đến điện thoại di động cũng tăng lên, và hình thức vi phạm ngày càng đa dạng, tinh vi và có tổ chức. Trong nhiều vụ án, điện thoại di động được sử dụng như những công cụ phạm tội. Các đối tượng có thể sử dụng điện thoại để lưu thông tin cá nhân, trao đổi thư, chat, truy cập vào các mạng xã hội, các trang web cá cược bóng đá, chơi lô đề trực tuyến… Bài viết tập trung phân tích việc thu thập dấu vết điện tử từ thiết bị điện thoại di động trong điều tra tội phạm.

Từ khóa: Dấu vết điện tử, điện thoại di động, giám định kỹ thuật số.

Ngày nhận bài: 24/11/2021; Biên tập xong: 06/12/2021; Duyệt đăng: 10/02/2022

In recent years, in the world and in Vietnam, along with the continuous development of technology, mobile phones are increasingly developing and becoming the main means of communication and work of people. Along with the development of multi-function smartphones, the number of cases related mobile phones has also increased, and the forms of violations are increasingly diverse, sophisticated and organized. In many cases, mobile phones are used as tools of crime. Criminals can use mobile phones to save personal information, exchange mail, chat, access social networks, football betting sites, play online lottery... The article focuses on analyzing the collection of electronic traces from mobile phones in criminal investigation.

Keywords: Electronic traces, mobile phones, digital inspection.

Ở nước ta trong một số vụ án gần đây, qua việc thu thập, khai thác các thông tin từ thiết bị di động của đối tượng có thể tìm ra được nhiều chứng cứ quan trọng mà phương pháp điều tra truyền thống không thể có được. Vì vậy, việc hiểu rõ cách thức lưu trữ dữ liệu, hệ điều hành đang được sử dụng trong các loại điện thoại hiện nay sẽ giúp ích cho việc khai thác, thu thập dữ liệu, qua đó nâng cao hiệu quả trong công tác đấu tranh phòng, chống tội phạm.

Hiện nay, dữ liệu điện tử trong điện thoại rất đa dạng nên có nhiều tiêu chí để phân loại nhằm nâng cao công tác thu thập và phân tích dữ liệu phục vụ công tác điều tra. Một trong những cách phân loại phổ biến là căn cứ vào hệ điều hành của điện thoại có thể phân ra các loại điện thoại sử dụng hệ điều hành như: IOS, ANDROID, WINDOWPHONE, BLACKBERRY, FUNTOUCH… Hay có thể căn cứ vào vị trí lưu trữ dữ liệu có thể phân thành dữ liệu bộ nhớ trong, dữ liệu bộ nhớ trên SIM, dữ liệu trong các thẻ nhớ, hoặc cũng có thể dựa vào hình thức tồn tại của dữ liệu điện thoại mà phân thành dữ liệu dưới dạng ký hiệu, dữ liệu dạng hình ảnh, dữ liệu dạng âm thanh… Ngoài ra, còn nhiều cách phân loại khác dựa trên các tiêu chí cụ thể như: Căn cứ vào loại dữ liệu trích xuất, khôi phục (tin nhắn, hình ảnh, vị trí, lịch sử cuộc gọi…); căn cứ vào tình trạng dữ liệu điện tử (ẩn, xóa, tồn tại) hay cũng có thể

** Phó giáo sư, Tiến sĩ, Phó trưởng khoa Kỹ thuật hình sự, Học viện Cảnh sát nhân dân*

căn cứ vào mục đích sử dụng dữ liệu (dữ liệu truyền đi, dữ liệu chuyển đến).

Tại khoản 1 Điều 99 Bộ luật Tố tụng hình sự năm 2015 (BLTTHS năm 2015) thì khái niệm về dữ liệu điện tử được định nghĩa 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.

Tại Điều 107 BLTTHS năm 2015 có hiệu lực thi hành từ ngày 01/01/2018 có quy định: "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".

Như vậy, chúng ta có thể thấy rằng phương tiện điện tử và cụ thể ở đây là điện thoại đi động phải được thu thập đúng luật, trong cả quá trình khám xét, thu giữ vật chứng, sử dụng công nghệ (thiết bị phần cứng và phần mềm) được cơ quan pháp luật công nhận, từ đó điện thoại di động mới được sử dụng để khai thác dữ liệu điện tử tồn tại bên trong và tiến hành sao lưu dữ liệu, bảo quản, phục hồi, phân tích, tìm kiếm và giám định dữ liệu làm chứng cứ. Cơ quan điều tra phải thu thập theo đúng thủ tục tố tụng hình sự: Dữ liệu thu được từ điện thoại di động phải được ghi vào biên bản, niêm phong theo đúng quy định, không bị tác động làm thay đổi dữ liệu kể từ khi thu giữ hợp pháp và không thể can thiệp để thay đổi. Chuyên gia phục hồi dữ liệu sử dụng công nghệ và phần mềm phục hồi dữ liệu, như thiết bị chống ghi (Read Only - chỉ đọc) sao chép dữ liệu và chỉ sử dụng bản sao này để phục hồi, phân tích, tìm kiếm dữ liệu, chuyển thành dạng đọc được, nghe được, nhìn thấy được.

Bên cạnh đó, từ khái niệm được đưa vào tại khoản 1 Điều 99 BLTTHS năm 2015, chúng ta thấy rằng xét về bản chất, 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, có thể phục hồi, phân tích, tìm được dữ liệu, kể cả đã bị xóa, bị ghi đè, dưới dạng ẩn, đã mã hóa và làm cho có thể đọc được, nhìn thấy được, ghi lại và có thể sử dụng làm chứng cứ.

Vì vậy, để nâng cao hiệu quả trong việc phát hiện, thu thập dữ liệu điện tử từ điện thoại đi động, trước hết chúng ta cần phải hiểu được cơ chế hình thành và đặc điểm của dữ liệu điện tử trên điện thoại di động.

Cơ chế hình thành dữ liệu điện tử trên điện thoại được hình thành do sự tác động giữa những đối tượng vật chất, đó là kết quả của những thao tác trên điện thoại với việc sử dụng các phần mềm để xử lý các dữ liệu do người dùng đưa vào.

Các giai đoạn chính của quá trình thực hiện hành vi của tội phạm:

- *Giai đoạn nhập dữ liệu:* Đây là giai đoạn tiếp nhận thông tin từ ngoài đưa vào điện thoại di động bằng bàn phím, camera, micro… Hầu hết dấu vết điện tử của các hành vi vi phạm pháp luật được hình thành trong giai đoạn này.

- *Giai đoạn phần mềm xử lý dữ liệu:* Trong giai đoạn này, phần mềm có thể tự tạo ra các dữ liệu để lưu tạm dữ liệu trong quá trình xử lý và có thể ghi lại các kết quả trung gian, hoặc ghi lại quá trình xử lý. Giai đoạn này hình thành những dấu vết điện tử rất khách quan mà người dùng có thể không hay biết. Kết thúc của giai đoạn này là việc *lưu dữ liệu đã qua xử lý vào bộ nhớ* điện tử trên điện thoại hoặc được truyền đi.

- *Giai đoạn truyền dữ liệu:* Đây là giai đoạn dữ liệu điện tử được truyền từ điện thoại này sang điện thoại khác hoặc thiết bị điện tử khác thông qua mạng viễn thông hay mạng Internet. Giai đoạn này

tội phạm có thể sử dụng nhiều phương thức và thủ đoạn khác nhau để truy cập bất hợp pháp vào điện thoại, làm biến dạng dữ liệu, sai lệch chương trình điều khiển, truyền virus vào hệ thống để thực hiện mục đích phạm tội.

- *Giai đoạn xuất hiện dữ liệu:* Dữ liệu lưu trong bộ nhớ có thể được chuyển sang dạng có thể đọc được, hiểu được. Giai đoạn này rất ít bị phá hoại ngầm nhưng khi có những vụ trộm dữ liệu đã được thực hiện thì người phạm tội có thể lấy được những thông tin có giá trị khi hiển thị hoặc in ra.

Từ việc nghiên cứu cơ chế hình thành, có thể thấy dữ liệu điện tử trên điện thoại có những đặc điểm là không tồn tại ở các dạng vật chất thông thường mà tồn tại dưới dạng các thông tin điện tử và được lưu trữ trong bộ nhớ của điện thoại. Bên cạnh đó, dữ liệu điện tử có bản chất động. Bản chất động của dữ liệu điện tử thể hiện ở khả năng sao chép, dịch chuyển từ vị trí này sang vị trí khác, từ điện thoại này sang điện thoại khác hoặc thiết bị phương tiện khác, từ định dạng này sang định dạng khác… Bản chất động của dữ liệu điện tử còn thể hiện ở khả năng dễ dàng chỉnh sửa, xóa bỏ, có thể được mã hoá hoặc ẩn đi. Bên cạnh đó, một đặc điểm rất quan trọng đó là dữ liệu điện tử có khả năng khôi phục được dù bị xóa đi bởi nguyên nhân chủ quan của con người hoặc do các nguyên nhân khách quan. Các đặc điểm này ảnh hưởng rất lớn đến việc phát hiện, thu giữ và bảo quản dấu vết điện tử từ điện thoại.

Trong hoạt động điều tra và xử lý tội phạm, việc tìm kiếm dữ liệu điện tử từ điện thoại thường bắt đầu bằng cách kiểm tra trực tiếp trên điện thoại đã thu giữ của đối tượng, để tìm ra những tập tin, tệp chứa đựng những thông tin có ý nghĩa trong việc chứng minh sự thật của vụ án. Cần đặc biệt chú ý các văn bản, bảng biểu, hình ảnh, thông tin, email, chat, các dữ liệu phản ánh việc đăng tải và tải về của đối tượng. Đây có thể là những tài liệu chứng cứ có giá trị trong việc buộc tội hoặc để đấu tranh buộc đối tượng phải khai nhận về hành vi phạm tội của mình.

Thu thập dữ liệu là việc khai thác tất cả những thông tin có trên điện thoại, bao gồm cả những thông tin đang lưu trên máy và những thông tin đã xóa nhằm tạo điều kiện cho quá trình khai thác thông tin. SIM điện thoại cũng là một thiết bị lưu trữ nhiều thông tin. Trên SIM thường lưu những tin nhắn SMS, danh bạ… Vì vậy, trong quá trình khai thác dữ liệu, khai thác SIM cũng là một khâu quan trọng. Việc khai thác dữ liệu trên SIM có thể được tiến hành trực tiếp thông qua điện thoại hoặc kết nối với máy tính bằng một đầu đọc thẻ SIM. Đối với mỗi loại điện thoại sẽ có một phương pháp khai thác dữ liệu khác nhau, tùy thuộc vào từng loại điện thoại thu được mà cán bộ kỹ thuật sẽ quyết định nên khai thác theo phương pháp nào. Tuy nhiên để khai thác một cách có hiệu quả thì các phương pháp đều phải tuân theo trình tự sau:

Bước 1: Tiến hành thu giữ điện thoại theo đúng quy trình để tránh làm mất thông tin trên điện thoại và đảm bảo đúng thủ tục pháp lý.

Bước 2: Khi ở trạng thái tiết kiệm năng lượng điện thoại giống như đang tắt, nhưng trên thực tế điện thoại đang bật. Để kiểm tra trạng thái của điện thoại có thể ấn một nút bất kỳ trên điện thoại.

Bước 3: Kiểm tra xem điện thoại có dùng SIM không. Nếu điện thoại dùng SIM thì chuyển sang quy trình khai thác SIM. Nếu điện thoại sử dụng công nghệ CDMA thì việc khai thác dữ liệu chỉ tiến hành trên máy điện thoại.

Bước 4: Bật nguồn lên và tiến hành các bước tiếp theo để khai thác thông tin trên điện thoại.

Bước 5: Kiểm tra các đặc điểm của điện thoại, nắm rõ các đặc điểm kỹ thuật để có thể đưa ra phương pháp thu thập dữ liệu hợp lý. Bước này đòi hỏi cán bộ kỹ thuật phải có kiến thức, am hiểu về các loại điện thoại và đặc điểm của chúng.

Bước 6: Lập kế hoạch khai thác.

Bước 7: Kiểm tra xem loại điện thoại đó có hỗ trợ kết nối với máy tính không? Có thể sử dụng công cụ khai thác dữ liệu nào?

Bước 8: Sử dụng các công cụ để thu thập, khai thác và phục hồi dữ liệu trên điện thoại. Tùy thuộc vào dữ liệu cần khai thác mà chọn công cụ khai thác hợp lý để đạt được hiệu quả cao nhất.

Bước 9: Sử dụng các phương pháp khai thác dữ liệu thực hiện quá trình khai thác dữ liệu trên điện thoại di động.

Bước 10: Sau khi khai thác hết các thông tin trên máy thì tắt nguồn và tháo SIM ra khỏi máy để chuyển sang quy trình khai thác SIM. SIM điện thoại cũng là một thiết bị lưu trữ nhiều thông tin. Trên SIM thường lưu những tin nhắn, danh bạ điện thoại và nhiều thông tin khác. Vì vậy, trong quá trình khai thác dữ liệu, khai thác SIM cũng là một khâu quan trọng. Để khai thác triệt để các thông tin trên SIM (kể cả những thông tin đã bị xóa), kết nối SIM với máy tính thông qua một đầu đọc SIM và sử dụng các phần mềm được cài trên máy tính.

Khi tạo ra một bản sao dấu vết điện tử để phân tích, cần phải sử dụng các giá trị băm được mã hóa (MD5, SHA). Mục đích của giá trị băm là xác minh tính xác thực và tính toàn vẹn của dữ liệu dưới dạng bản sao chính xác của dữ liệu gốc. Giá trị băm là rất quan trọng, đặc biệt là khi sử dụng làm chứng cứ tranh tụng trước tòa, bởi vì việc thay đổi ngay cả một chút dữ liệu nhỏ nhất sẽ tạo ra giá trị băm hoàn toàn mới. Trong quá trình phân tích, chỉ cần tạo một tệp mới hoặc chỉnh sửa một tệp hiện có trên máy tính chắc chắn sẽ tạo ra một giá trị băm mới cho tệp tin đó. Giá trị băm này và siêu dữ liệu tệp khác không hiển thị trong cửa sổ trình duyệt tệp thông thường nhưng có thể truy cập bằng phần mềm đặc biệt. Nếu giá trị băm không khớp với giá trị băm của tệp dữ liệu đã được băm trước đó chứng tỏ dữ liệu đã bị tác động, chỉnh sửa.

Tóm lại, điện thoại di động chứa đựng nhiều thông tin có ý nghĩa phục vụ hoạt động điều tra. Tuy nhiên, đây là dữ liệu dễ mất, nhiều dữ liệu chỉ cần ngắt nguồn điện, dữ liệu không còn tồn tại. Do đó, quá trình tiến hành các hoạt động điều tra như: Khám nghiệm hiện trường, khám xét, thu giữ dữ liệu điện tử… cần có sự chuẩn bị cẩn thận về con người, phương tiện kỹ thuật; quá trình tiến hành sao lưu cần thiết phải lập biên bản sao lưu với đầy đủ như: Đối tượng được sao lưu, đối tượng lưu trữ, phương pháp sao lưu và gán giá trị băm cho dữ liệu được sao lưu. Bất kỳ lỗ hổng nào trong quá trình thu thập, bảo quản đều có khả năng dẫn đến các vấn đề pháp lý phát sinh./.

TÀI LIỆU THAM KHẢO

1. Hoàng Trọng Lực, Vũ Huy Năng (2021), *Dấu vết điện tử,* Nxb. Công an nhân dân, Hà Nội;

2. Hà Lương Tín (2019), *Giám định kỹ thuật số và điện tử trong điều tra tội phạm*, Học viện Cảnh sát nhân dân, Hà Nội;

3. Đào Văn Vạn (2014), *Thu thập, đánh giá và sử dụng dấu vết điện tử phục vụ yêu cầu điều tra vụ án có sử dụng công nghệ thông tin,* Học viện Cảnh sát nhân dân, Hà Nội;

4. Baryamureeba, V. and Tushabe, F. (2004) The Enhanced Digital Investigation process Model. Digital Forensic Research Workshop.

5. Savoldi A. and Gubian P (2008). Data hiding and recovery on wince based handheld devices. In Fourth Annual IFIPWG 11.9 International Conference on Digital Forensics .