CHỨNG CỨ TỪ NGUỒN DỮ LIỆU ĐIỆN TỬ VÀ KIẾN NGHỊ HOÀN THIỆN QUY ĐỊNH PHÁP LUẬT CÓ LIÊN QUAN

■ HOÀNG THỊ THẢO *

Tóm tắt: *Bài viết khái quát về dữ liệu điện tử, phân tích điều kiện để nguồn dữ liệu điện tử trở thành chứng cứ và đưa ra một số kiến nghị hoàn thiện quy định của pháp luật Việt Nam liên quan đến chứng cứ từ nguồn dữ liệu điện tử.*

Abstract: *The article provides an overview of electronic data, analyzes the conditions for electronic data sources to become evidence, and makes some recommendations to improve regulations of Vietnamese law related to evidence from electronic data sources.*

1. Khái quát về dữ liệu điện tử

1.1. Định nghĩa dữ liệu điện tử

Cùng với sự bùng nổ của công nghệ thông tin, đặc biệt là trí tuệ nhân tạo, có nhiều hành vi vi phạm pháp luật được thực hiện trên không gian mạng, hoặc người thực hiện hành vi vi phạm pháp luật lợi dụng các thiết bị điện tử, các nền tảng trực tuyến để thực hiện hành vi phi pháp. Trong những trường hợp này, chứng cứ từ nguồn dữ liệu điện tử là một yếu tố quan trọng để xác định hành vi vi phạm pháp luật.

Pháp luật tố tụng hình sự và pháp luật tố tụng dân sự đều ghi nhận giá trị dùng làm chứng cứ của nguồn dữ liệu điện tử (khoản 1 Điều 94 Bộ luật Tố tụng dân sự năm 2015 và điểm c khoản 1 Điều 87 Bộ luật Tố tụng hình sự năm 2015). Điều 99 Bộ luật Tố tụng hình sự năm 2015 định nghĩa dữ liệu điện tử như sau:

"1. 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.

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".

Định nghĩa trên thống nhất với cách hiểu về dữ liệu điện tử quy định tại khoản 5 Điều 4 Luật Giao dịch điện tử năm 2005 và khoản 6, khoản 7 Điều 3 Luật Giao dịch điện tử năm 2023 (có hiệu lực thi hành từ ngày 01/7/2024): "Dữ liệu là ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự khác"; "Dữ liệu điện tử là dữ liệu được tạo ra, xử lý, lưu trữ bằng phương tiện điện tử".

Tuy nhiên, hiện nay, trí tuệ nhân tạo (AI) và công nghệ học máy (machine learning) ngày càng phát triển, có nhiều nguồn dữ liệu điện tử do AI tạo ra dựa trên các dữ liệu do con người cung cấp cho AI hoặc dữ liệu do chính AI thu thập được. Ví dụ, AlphaGo là một chương trình máy tính được Google DeepMind phát triển để chơi cờ vây. AlphaGo ban đầu được huấn luyện để bắt chước lối chơi của con người bằng cách học khoảng 30 triệu nước đi từ 160.000 ván cờ. Tuy nhiên, khi AlphaGo đã đạt đến một mức độ thành thạo nhất định, nó sẽ được huấn luyện thêm bằng cách sử dụng phương pháp học tăng cường (reinforcement learning) để cải thiện lối chơi của nó. Chính vì vậy, một trong các nhà sáng lập của AlphaGo phải

* Công ty cổ phần Du lịch Việt Nam VNTravel

thừa nhận rằng, mặc dù DeepMind đã lập trình AlphaGo chơi cờ vây nhưng họ không biết nó sẽ thực hiện những nước đi gì. Những nước đi của AlphaGo nằm ngoài tầm kiểm soát của DeepMind và tốt hơn nhiều so với những gì mà người chơi cờ vây có thể nghĩ ra[1]. Như vậy, AI đã được đào tạo để tự học hỏi và đưa ra các quyết định mà chính các lập trình viên cũng không ngờ đến. Tuy nhiên, AI hoặc robot có thể sẽ đưa ra các quyết định gây thiệt hại cho con người, mà những quyết định này nằm ngoài tầm kiểm soát và dự đoán của các lập trình viên và đây cũng là một nguồn dữ liệu quan trọng cần xem xét trong quá trình giải quyết các vụ án, các vụ việc sử dụng AI hoặc robot. Do vậy, tác giả đề nghị sửa đổi định nghĩa dữ liệu điện tử như sau: "Dữ liệu điện tử là các ký hiệu, chữ viết, chữ số, hình ảnh, âm thành hoặc dạng tương tự khác, được tạo ra bởi các thiết bị điện tử, phương tiện điện tử và các công nghệ mới hoặc thông qua việc sử dụng các thiết bị điện tử, phương tiện điện tử; được xử lý, lưu trữ, truyền nhận thông qua các phương tiện điện tử".

Khi các dữ liệu điện tử được thu thập tuân thủ các quy định của pháp luật tố tụng thì các dữ liệu điện tử được coi là chứng cứ điện tử. Tuy pháp luật Việt Nam hiện hành chưa có khái niệm về "chứng cứ điện tử", nhưng về mặt khoa học pháp lý, có thể hiểu, "chứng cứ điện tử là bất kỳ bằng chứng nào có nguồn gốc từ dữ liệu được lưu trữ trong hoặc được tạo ra bởi thiết bị mà hoạt động của thiết bị này phụ thuộc vào các phần mềm và các dữ liệu được lưu trữ trong hoặc được truyền nhận thông qua hệ thống máy tính hoặc hệ thống mạng"[2].

1.2. Phân loại dữ liệu điện tử

Dữ liệu điện tử có thể là văn bản, video, hình ảnh, bản ghi âm, ký hiệu, chữ số, đoạn code... được lưu trữ trong các thiết bị điện tử như máy tính, điện thoại di động, đồng hồ thông minh, máy ghi âm, đĩa CD, ổ cứng máy tính...

Dữ liệu có thể được thể hiện qua các phương tiện điện tử như email, tin nhắn điện thoại, tin nhắn trên các ứng dụng nhắn tin, mạng xã hội, các phần mềm và ứng dụng di động...

Dữ liệu điện tử có thể do con người tạo ra như nội dung email, nội dung một hợp đồng điện tử... Dữ liệu điện tử cũng có thể do AI, robot và các công nghệ mới tạo ra như ví dụ về AlphaGo ở trên.

1.3. Đặc điểm của dữ liệu điện tử

Thứ nhất, dữ liệu điện tử không thể nhìn thấy bằng mắt thường, không thể tồn tại một cách độc lập mà phải phụ thuộc vào các thiết bị điện tử hoặc các phần mềm ứng dụng.

Với các nguồn chứng cứ truyền thống như văn bản, thiết bị... các bên tham gia tố tụng có thể dễ dàng truy cập, đọc được thông tin. Tuy nhiên, với dữ liệu điện tử, các bên cần sự hỗ trợ của phần cứng và phần mềm phù hợp. Người dùng không thể tạo hoặc thực hiện bất kỳ thao tác gì với dữ liệu điện tử nếu không có phần cứng hoặc phần mềm thích hợp. Bên cạnh đó, dữ liệu ở dạng điện tử (ví dụ như các đoạn code hoặc các ký hiệu) phải được chuyển sang dạng con người có thể đọc được thông qua sự hỗ trợ của các sản phẩm công nghệ hoặc các chuyên gia.

Thứ hai, dữ liệu điện tử có thể dễ dàng được sao chép, phát tán, thay đổi hoặc xóa.

Không giống như các loại nguồn chứng cứ truyền thống khác, dữ liệu điện tử có thể được thay đổi nhanh chóng thông qua các thiết bị điện tử như máy tính, điện thoại hoặc thông qua các phần mềm. Một số phần mềm còn cho phép người dùng có thể thay đổi nội dung dữ liệu có trên một máy tính ở vị trí khác (ví dụ như phần mềm teamview

cho phép một người có thể truy cập và thực hiện các tác vụ trên một máy tính ở cách xa họ). Với dữ liệu điện tử, hành động đơn thuần là khởi động máy tính và mở tài liệu sẽ thay đổi thông tin của dữ liệu điện tử đó, chẳng hạn như thông tin về dấu thời gian[3] (timestamp), thông tin về lần đăng nhập gần nhất vào dữ liệu. Điều này sẽ làm thay đổi tính toàn vẹn của dữ liệu và có thể là lý do để các cơ quan tiến hành tố tụng không chấp nhận giá trị chứng cứ của dữ liệu điện tử này.

Đặc tính dễ dàng thay đổi của dữ liệu điện tử cũng ảnh hưởng tới tính chính xác của nó với tư cách là một chứng cứ. Một ví dụ điển hình với người dùng internet là khi truy cập vào một trang web tại các thời điểm khác nhau thì nội dung và hình ảnh hiển thị có thể khác nhau.

Hiện nay, nhiều người dùng máy tính thường xuyên tải các dữ liệu của họ như hình ảnh, thông tin cá nhân... lên các trang mạng xã hội, các nền tảng lưu trữ trực tuyến như Google Drive. Việc tự động tải dữ liệu lên mạng cũng đồng nghĩa với việc người dùng mất quyền kiểm soát thông tin mình đã tạo. Các thông tin này có thể bị kẻ xấu lợi dụng để thực hiện các mục đích phi pháp. Tính dễ dàng sao chép của các dữ liệu này gây khó khăn trong việc xác định ai là người đã sử dụng dữ liệu điện tử để thực hiện hành vi vi phạm pháp luật.

Khả năng chuyển giao nhanh chóng và đặc tính dễ dàng sao chép cũng có thể tạo ra các vấn đề liên quan đến quyền tài phán. Dữ liệu kinh doanh thường được các tổ chức xử lý bằng công nghệ điện toán đám mây (cloud computing), bao gồm việc thuê máy chủ của bên thứ ba không do công ty sở hữu và kiểm soát và có thể được đặt khắp nơi trên thế giới. Tính linh hoạt về mặt địa lý do mạng máy tính quốc tế cung cấp đã được các ngân hàng và sòng bạc nước ngoài sử dụng để chọn khu vực pháp lý phù hợp với họ. Điện toán đám mây cho phép các công ty này giao dịch với khách hàng sử dụng máy móc ở các quốc gia có ít biện pháp bảo vệ người tiêu dùng, lưu trữ thông tin chi tiết về khách hàng ở các quốc gia không có yêu cầu cao về quyền riêng tư và gửi lợi nhuận vào ngân hàng ở các quốc gia có thuế thấp và có tiêu chuẩn bảo mật thông tin ngân hàng cao. Việc xác định thẩm quyền để khởi kiện một công ty như vậy có thể rất phức tạp[4].

Thứ ba, dữ liệu điện tử khó thu thập và phân tích.

Dữ liệu điện tử thường được được mã hóa nên việc thu thập và phân tích cần sự hỗ trợ của công nghệ và các chuyên gia. Đặc điểm này đặt ra một thách thức đối với các cơ quan tiến hành tố tụng và các cá nhân, tổ chức có nghĩa vụ chứng minh trong hoạt động tố tụng dân sự, do họ cần phải có các trang thiết bị kỹ thuật cần thiết để mã hóa, phân tích các dữ liệu điện tử này hoặc chuyển dữ liệu điện tử sang dạng mà con người có thể đọc được.

Dữ liệu điện tử thường được tạo ra trên không gian ảo và không có tính biên giới, lãnh thổ. Vì vậy, việc thu thập và đánh giá nhằm xác định giá trị chứng cứ của các dữ liệu này sẽ gặp nhiều khó khăn. Đặc tính xuyên biên giới của dữ liệu điện tử buộc các nước phải hợp tác để có thể thu thập được các dữ liệu này. Ngày 28/7/2023, Liên minh châu Âu (EU) đã thông qua quy định về việc cung cấp các chứng cứ điện tử xuyên biên giới phục vụ cho hoạt động tố tụng hình sự. Quy định này sẽ cho phép chính quyền quốc gia thành viên của EU được quyền yêu cầu các nhà cung cấp dịch vụ ở quốc gia thành viên khác phải cung cấp bằng chứng điện tử hoặc yêu cầu dữ liệu điện tử được lưu giữ trong tối đa 60 ngày để dữ liệu liên quan không bị phá hủy hoặc bị mất[5].

Thứ tư, dữ liệu điện tử bị ảnh hưởng mạnh mẽ bởi sự thay đổi của công nghệ.

Công nghệ thay đổi nhanh chóng, các doanh nghiệp thường xuyên cập nhật hệ điều hành, phần mềm ứng dụng. Khi phát hành các phần mềm mới hoặc cập nhật hệ điều hành, các phần mềm và hệ điều hành cũ thường hết giá trị sử dụng sau một khoảng thời gian nhất định. Kết quả là, dữ liệu ở dạng kỹ thuật số không thể đọc hoặc không sử dụng được bằng phần mềm hoặc hệ điều hành mới. Ví dụ, một công ty phần mềm có thể không còn sản xuất phần mềm tương thích (khi các phiên bản phần mềm mới có thể hoạt động trên các thiết bị điện tử cũ). Sự lỗi thời về mặt kỹ thuật là một vấn đề lớn ảnh hưởng đến mọi khía cạnh của quy trình pháp lý, đặc biệt vì tốc độ thay đổi hiện nay đã trở nên quá nhanh.

2. Điều kiện để nguồn dữ liệu điện tử trở thành chứng cứ

Khoản 3 Điều 99 Bộ luật Tố tụng hình sự năm 2015 quy định: "Giá trị chứng cứ của dữ liệu điện tử được xác định căn cứ vào cách thức khởi tạo, lưu trữ hoặc truyền gửi dữ liệu điện tử; cách thức bảo đảm và duy trì tính toàn vẹn của dữ liệu điện tử; cách thức xác định người khởi tạo và các yếu tố phù hợp khác".

Để một dữ liệu điện tử có thể trở thành chứng cứ điện tử, dữ liệu điện tử phải đáp ứng các yêu cầu, điều kiện chung của chứng cứ, cụ thể là: Tính xác thực và tin cậy, tính liên quan, tính hợp pháp. Ngoài ra, do đặc điểm riêng của dữ liệu điện tử như đã phân tích ở trên, dữ liệu điện tử phải có tính toàn vẹn để có thể có giá trị chứng cứ trong các hoạt động tố tụng.

***Thứ nhất,** tính xác thực, tin cậy:* Dữ liệu điện tử phải có tính xác thực, tức là nó phản ánh các tình huống, sự kiện có thật đã xảy ra. Đối với dữ liệu điện tử, tính xác thực và tin cậy không chỉ được phản ánh ở nội dung của chính dữ liệu, mà còn được thể hiện ở kỹ thuật thu thập, lưu trữ dữ liệu đó.

Việc chứng minh tính xác thực và tin cậy của dữ liệu điện tử có thể cần sự trợ giúp của công nghệ hoặc chuyên gia. Ví dụ, khi xác thực một giọng nói trong file ghi âm, các cơ quan có thẩm quyền có thể yêu cầu xác thực từ: (i) Người có quen biết, có khả năng nhận diện được giọng nói trong file ghi âm; (ii) Bằng chứng chuyên môn sử dụng phân tích thính giác hoặc phân tích âm thanh[6].

Ngày nay, việc sử dụng siêu dữ liệu (metadata) để xác thực dữ liệu điện tử rất phổ biến. Siêu dữ liệu luôn đi kèm với dữ liệu điện tử và thường không được hiển thị với người dùng. Các siêu dữ liệu rất đa dạng, phụ thuộc vào từng loại dữ liệu. Ví dụ, hai công ty ký kết một hợp đồng điện tử, thông qua một nền tảng ký kết hợp đồng trực tuyến. Nhân viên của hai công ty có thể đóng, mở, truy cập vào tệp này rất nhiều lần. Siêu dữ liệu của tệp kỹ thuật số này có thể thay đổi liên tục, ghi nhận số lần, thời gian, địa điểm thực hiện thay đổi, chỉnh sửa tài liệu.

Ngoài ra, do đặc điểm của dữ liệu điện tử được thực hiện trên hệ thống mạng hoặc hệ thống máy tính, để chứng minh tính xác thực của dữ liệu điện tử, có thể sử dụng quy trình hệ thống mạng hoặc hệ thống công nghệ. Ví dụ, hiện nay, các công ty công nghệ hoặc tập đoàn lớn thường sử dụng intranet để thực hiện công việc (intranet là mạng nội bộ, chỉ được sử dụng bởi nhân viên công ty, thường được phân quyền, ủy quyền cho từng bộ phận hoặc nhân viên thực hiện các tác vụ cụ thể

trên intranet). Một công ty muốn chứng minh một nhân viên của mình đã lấy thông tin bảo mật từ intranet và tiết lộ ra bên ngoài, cần xác minh được rằng, hệ thống intranet của công ty chỉ phân quyền cho một mình nhân viên đó được tiếp cận các thông tin bảo mật hoặc tại thời điểm thông tin bị tiết lộ, chỉ có một mình nhân viên đó sử dụng hệ thống intranet của công ty. Để làm được việc này, công ty cần dựa vào lịch sử truy cập vào hệ thống intranet, IP đã truy cập vào hệ thống intranet, các tác vụ người dùng đã thực hiện trên intranet...

Khi xem xét tính xác thực và tin cậy của dữ liệu điện tử, phải đánh giá được phương pháp kỹ thuật sử dụng để thu thập chứng cứ này như: Kỹ thuật hoặc công nghệ thu thập đã được pháp luật chấp nhận chưa hoặc đã có bằng chứng khoa học về mức độ tin cậy của phương pháp này chưa; tỷ lệ lỗi (nếu có) của biện pháp công nghệ này.

Thứ hai, *tính liên quan:* Dữ liệu điện tử để trở thành chứng cứ thì phải có liên quan tới vụ việc, vụ án đang được xử lý, bao gồm liên quan định danh và liên quan về nội dung. Khác với các dữ liệu truyền thống, việc xác định tính liên quan về định danh cần dựa vào các dấu vết (trace) mà người dùng để lại trên các phương tiện điện tử hoặc thiết bị điện tử như: Thông tin tên đăng nhập và mật khẩu vào phần mềm, dấu thời gian thể hiện số lần và thời gian đăng nhập vào một thiết bị hoặc một ứng dụng... Tính liên quan về nội dung sẽ được các bên liên quan xác định dựa trên từng tình huống cụ thể.

Thứ ba, *tính hợp pháp:* Điều 86 Bộ luật Tố tụng hình sự năm 2015 quy định: "Chứng cứ là những gì có thật, được thu thập theo trình tự, thủ tục do Bộ luật này quy định". Như vậy, để bảo đảm tính hợp pháp, trước hết dữ liệu điện tử phải được thu thập phù hợp với quy định của pháp luật tố tụng. Do bản chất của dữ liệu điện tử thường chứa một lượng lớn thông tin, nên trong quá trình thu thập thông tin, cơ quan tiến hành tố tụng hoặc bên thứ ba có thể được tiếp cập với các thông tin riêng tư, bí mật cá nhân, nằm ngoại phạm vi của vụ việc, vụ án đang giải quyết. Pháp luật cần có quy định cụ thể về giám định pháp y kỹ thuật số để bảo đảm tuân thủ quy định của Hiến pháp trong việc bảo vệ thông tin cá nhân[7]. Việc thu thập dữ liệu điện tử cần bảo đảm không vi phạm quy định về bảo vệ thông tin cá nhân, xâm phạm quyền riêng tư. Tuy nhiên, một câu hỏi khó được đặt ra khi bằng chứng điện tử được thu thập mà một người không hề biết và chấp nhận, nhưng nó lại cho thấy người đó đã phạm tội. Ví dụ, nếu công ty đặt camera ẩn, không cho nhân viên biết, thông qua camera đó, công ty phát hiện hành vi trộm cắp của nhân viên. Dữ liệu điện tử thu thập được trong trường hợp này đã vi phạm quy định về quyền riêng tư của cá nhân, nhưng lại chứng minh cá nhân đó có vi phạm. Về trường hợp này, pháp luật Tây Ban Nha đã có một vụ việc tương tự và Tòa án Tây Ban Nha cho rằng, việc giám sát nhân viên bằng camera ẩn (mà nhân viên không biết) là phù hợp với quyền riêng tư vì đoạn phim chỉ được sử dụng để truy tìm những người chịu trách nhiệm về việc mất hàng hóa từ cửa hàng và áp dụng các biện pháp kỷ luật đối với họ. Tuy nhiên, Tòa án đã đưa ra phán quyết dựa trên phân tích rằng, công ty đã tuân thủ các quy định của pháp luật quốc gia về các biện pháp bảo vệ thông tin cá nhân và quyền riêng tư trong trường hợp này[8].

Ngày nay, rất nhiều dữ liệu điện tử được lưu trữ tại khối tư nhân, đặc biệt là ở các công ty công nghệ. Các công ty công nghệ khi thu thập thông tin

của người dùng đều có cam kết sẽ bảo mật thông tin và chỉ được sử dụng trong những hoạt động nhất định. Chính vì vậy, pháp luật cần có quy định và chế tài cụ thể, yêu cầu các công ty cung cấp dữ liệu điện tử phục vụ cho hoạt động tố tụng, bảo đảm phòng ngừa và xử lý hành vi vi phạm pháp luật. Nội dung này cần được luật hóa cụ thể để tránh trường hợp lạm dụng thông tin cá nhân hoặc việc thu thập dữ liệu điện tử vi phạm quyền của các tổ chức, cá nhân.

Do đặc điểm xuyên biên giới của dữ liệu điện tử, pháp luật cần xem xét đến tình huống: Nếu dữ liệu điện tử được thu thập theo quy định của một hệ thống pháp luật khác, dữ liệu điện tử đó có được cơ quan có thẩm quyền chấp nhận làm chứng cứ không.

Để bảo đảm tính xác thực và hợp pháp, mỗi loại dữ liệu điện tử cần có một quy định riêng, yêu cầu riêng trong quá trình thu thập. Ví dụ, khi thu thập dữ liệu điện tử là một đoạn code, có thể phải sử dụng phương tiện điện tử thích hợp để lưu trữ, đồng thời giám sát để người thu thập code không làm thay đổi nội dung đoạn code. Cách thức lấy thu thập dữ liệu điện tử có ảnh hưởng trực tiếp tới độ tin cậy của bằng chứng, vì dữ liệu điện tử rất dễ bị thay đổi hoặc hủy bỏ.

Thứ tư, tính toàn vẹn: Vì đặc tính dễ thay đổi, chỉnh sửa của dữ liệu điện tử, để trở thành chứng cứ, dữ liệu điện tử phải bảo đảm tính toàn vẹn. Tính toàn vẹn của dữ liệu điện tử được hiểu là[9]: Dữ liệu điện tử được giữ nguyên trạng thái và nội dung từ thời điểm thu thập đến thời điểm sử dụng; dữ liệu điện tử được bảo vệ khỏi sự làm giả hoặc thao túng từ thời điểm thu thập đến thời điểm sử dụng; mỗi lần truy cập vào dữ liệu điện tử phải lưu thông tin truy cập (siêu dữ liệu) và không được làm thay đổi nội dung của dữ liệu; phương tiện lưu trữ phải được bảo vệ khỏi sự can thiệp từ bên ngoài; phải tạo và lưu giữ dấu vết kiểm tra hoặc hồ sơ về tất cả các quy trình áp dụng cho bằng chứng điện tử trên máy tính. Bên thứ ba có thể lặp lại các quy trình này và tái tạo kết quả.

Xác định tính toàn vẹn của dữ liệu điện tử là một vấn đề khó, hiện nay, pháp luật Việt Nam chưa có quy định cụ thể. Như ví dụ đã nêu ở trên, một hợp đồng điện tử được ký kết bởi hai công ty, siêu dữ liệu của tệp này ghi nhận hành động mở và đóng tệp của các nhân viên mà không làm thay đổi nội dung của tệp. Trong trường hợp này, siêu dữ liệu của tệp có thể đã bị thay đổi nhưng nội dung của tệp được đề cập vẫn không bị ảnh hưởng, vậy có thể coi dữ liệu điện tử này vẫn bảo đảm tính toàn vẹn để trở thành chứng cứ trong hoạt động tố tụng không?

Để đánh giá được tính toàn vẹn của dữ liệu điện tử, pháp luật cần quy định cụ thể về trạng thái, điều kiện của từng thiết bị, phương tiện điện tử, hệ thống máy tính. Đồng thời, pháp luật nên có quy định về việc cho phép sử dụng các công nghệ mới để bảo đảm tính toàn vẹn của dữ liệu điện tử. Tòa án Hàng Châu, Trung Quốc, sau đó là Tòa án tối cao Trung Quốc đã công nhận công nghệ blockchain như một phương pháp để thu thập dữ liệu điện tử bảo đảm tính xác thực và toàn vẹn[10]. Blockchain vốn có khả năng chống lại việc sửa đổi dữ liệu. Điều này làm cho blockchain phù hợp với mục đích chứng minh tính toàn vẹn của dữ liệu điện tử[11].

3. Một số kiến nghị hoàn thiện quy định của pháp luật Việt Nam liên quan đến chứng cứ từ nguồn dữ liệu điện tử

Thứ nhất, *sửa đổi định nghĩa về dữ liệu điện tử và quy định chi tiết tiêu chí của chứng cứ điện tử.*

Các quy định của pháp luật liên quan tới hoạt động tố tụng nên sử dụng thống nhất một khái niệm dữ liệu điện tử và chứng cứ điện tử. Như đã phân tích tại mục 1, khái niệm dữ liệu điện tử do Bộ luật Tố tụng hình sự năm 2015 quy định chưa xác định rõ ràng các dữ liệu do phương tiện điện tử hoặc công nghệ mới như AI tạo ra. Tuy nhiên, hiện tại, đây lại là nguồn dữ liệu quan trọng và xuất hiện thường xuyên trong đời sống và hoạt động kinh doanh. Tác giả cho rằng, nên sửa đổi khái niệm dữ liệu điện tử theo hướng, dữ liệu điện tử bao gồm cả các dữ liệu do AI hoặc các công nghệ mới tạo ra dựa trên thông tin do con người cung cấp hoặc thông tin do chính các công nghệ này tự thu thập.

Pháp luật Việt Nam chưa có quy định rõ ràng về tính toàn vẹn của dữ liệu điện tử và các tiêu chí để xác định tính toàn vẹn của dữ liệu. Việc thiếu các hướng dẫn cụ thể sẽ khiến các cơ quan, tổ chức, cá nhân tham gia tố tụng gặp khó khăn trong việc đưa ra chứng cứ để chứng minh cho yêu cầu của mình.

Thứ hai, *xây dựng quy định về các yêu cầu cần tuân thủ khi thu thập, xử lý, chuyển giao, chuyển đổi các loại dữ liệu điện tử khác nhau.*

Mỗi loại dữ liệu điện tử có yêu cầu kỹ thuật riêng trong quá trình thu thập, xử lý, chuyển giao và chuyển đổi thành dạng có thể đọc được. Do vậy, các nhà làm luật nên sớm ban hành tiêu chuẩn áp dụng với những dữ liệu này để bảo đảm: (i) Quá trình thu thập và xử lý dữ liệu diễn ra hợp pháp; (ii) Tòa án và các cơ quan tiến hành tố tụng khác sẽ có căn cứ cụ thể để chấp thuận hoặc từ chối giá trị chứng cứ của các dữ liệu điện tử này.

Các hướng dẫn cụ thể với từng loại dữ liệu điện tử nếu được áp dụng sẽ là căn cứ để xác định tính xác thực, tính tin cậy và tính toàn vẹn của chứng cứ điện tử.

Thứ ba, *xây dựng quy định pháp luật về việc thu thập, sử dụng và chuyển giao dữ liệu điện tử xuyên biên giới.*

Bản chất toàn cầu của internet và việc sử dụng ngày càng tăng các dịch vụ đám mây khiến việc truy cập hoặc xử lý dữ liệu xuyên biên giới ngày càng phổ biến. Vấn đề là có sự khác biệt đáng kể giữa các quy định của các quốc gia trong việc thu thập dữ liệu điện tử, chứng cứ điện tử ở nước ngoài. Với các dữ liệu điện tử xuyên biên giới, pháp luật cần có quy định cụ thể về việc thu thập chứng cứ và đưa ra các tiêu chí cụ thể để xác định giá trị chứng cứ của các dữ liệu điện tử được thu thập ở các khu vực tài phán khác.

Thứ tư, *xây dựng các quy định về việc thu thập dữ liệu điện tử do khối tư nhân sở hữu, quản lý.*

Khu vực tư nhân sở hữu một lượng lớn các dữ liệu điệu tử có thể ảnh hưởng tới kết quả của hoạt động tố tụng. Cơ quan có thẩm quyền cần sớm ban hành các quy định để phục vụ cho việc thu thập dữ liệu điện tử do khối tư nhân sở hữu, quản lý.

Việc thu thập dữ liệu điện tử từ các công ty tư nhân cần tuân thủ thủ tục nhất định để bảo đảm: (i) Các công ty này không vi phạm cam kết bảo mật thông tin của chính họ với khách hàng, đối tác; (ii) Cơ quan có thẩm quyền không lợi dụng hoạt động tố tụng để tiếp cận các thông tin không liên quan đến vụ việc, vụ án đang xử lý; (iii) Bảo đảm việc tuân thủ quyền đối với thông tin cá nhân, bí mật cá nhân theo quy định của Hiến pháp; (iv) Không xâm phạm hoặc làm ảnh hưởng tới bí mật kinh

doanh hoặc hoạt động kinh doanh của khối tư nhân.

Việc xây dựng quy định này cũng hỗ trợ cho các cá nhân, tổ chức trong việc tự thu thập dữ liệu điện tử để chứng minh yêu cầu của mình. Nếu không có quy định pháp luật điều chỉnh việc thu thập dữ liệu điện tử khối tư nhân, sẽ rất khó để các tổ chức, cá nhân có thể yêu cầu các công ty, doanh nghiệp tư nhân cung cấp dữ liệu điện tử. Điều quan trọng là cơ quan có thẩm quyền phải có các quy tắc rõ ràng về những loại dữ liệu nào có thể được thu thập từ khu vực tư nhân và những thủ tục nào cần phải tuân theo.

Thứ năm, *xây dựng quy định về pháp y/giám định kỹ thuật số.*

Ngày nay, nguồn chứng cứ từ dữ liệu điện tử được sử phổ biến trong các hoạt động tố tụng hình sự, dân sự và hành chính. Ví dụ, người dùng máy tính để lại dấu vết kỹ thuật số khi sử dụng máy tính, thiết bị di động hoặc các phương tiện điện tử khác. Giám định viên pháp y kỹ thuật số có thể xác định nghi phạm bằng cách thu thập và phân tích các dấu vết kỹ thuật số này. Chính vì vậy, các cơ quan có thẩm quyền nên xem xét việc thành lập các tổ chức pháp y/giám định kỹ thuật số ở khu vực công và khu vực tư nhân để phục vụ cho quá trình tố tụng.

Bản chất vô hình của dữ liệu điện tử và thông tin được chứa trong các thiết bị điện tử làm cho dữ liệu điện tử dễ bị thay đổi hơn so với chứng cứ truyền thống. Do đó, cần có một quy trình thu thập với các tiêu chí, tiêu chuẩn rõ ràng. Pháp y/giám định kỹ thuật số là một nhu cầu cấp thiết, vì vậy, cần sớm ban hành các quy định pháp luật liên quan tới lĩnh vực này để tạo điều kiện cho các cá nhân, tổ chức và các cơ quan tiến hành tố tụng có thể chủ động thu thập dữ liệu điện tử làm chứng cứ ❑

---

1. https://en.wikipedia.org/wiki/AlphaGo_versus_Lee_Sedol.

2. Hướng dẫn của Ủy ban Bộ trưởng (Hội đồng châu Âu) về chứng cứ điện tử trong tố tụng dân sự và hành chính thông qua ngày 30/01/2019 theo đề xuất của Ủy ban châu Âu về hợp tác pháp lý (CDCJ), https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5.

3. Khoản 15 Điều 3 Luật Giao dịch điện tử năm 2023 quy định: "Dấu thời gian là dữ liệu điện tử gắn với thông điệp dữ liệu cho phép xác định thời gian của thông điệp dữ liệu đó tồn tại ở một thời điểm cụ thể".

4. https://www.hpl.hp.com/techreports/2009/HPL-2009-99.pdf.

5. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023L1544&qid=1696298513074; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543&qid=1696309331909.

6. Section 3.86, Electronic Evidence, 4th Edition, Editors by Stephen Mason và Daniel Seng, Insitute of Advanced Legal Studies, School of Advanced Study University of London.

7. Hiến pháp năm 2013.

8. https://utrechtlawreview.org/articles/10.36633/ulr.525.

9. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf.

10. Interpol review of digital evidence for 2019 - 2022.

11. https://www.chainsecurity.asia/EN/evidence.html#:~:text=Tamper%2DProof%20%2D%20Digital%20evidence%20integrity,gets%20synchronized%20to%20all%20nodes; Vũ Quang Minh, Lê Thị Anh, Khả năng ứng dụng công nghệ Blockchain trong việc lưu trữ chứng cứ hỗ trợ điều tra số.