

# MỘT SỐ GIẢI PHÁP GÓP PHẦN HOÀN THIỆN PHÁP LUẬT VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TẠI VIỆT NAM

✍ TS. BÙI THỊ NGUYỆT THU

**Tóm tắt:** Môi trường số hóa trong thời đại công nghệ phát triển ở hầu hết các lĩnh vực đời sống xã hội kéo theo sự rò rỉ dữ liệu cá nhân, có thể gây ra một số hậu quả nghiêm trọng cho người dùng, bao gồm việc lạm dụng thông tin cá nhân, việc gian lận tài chính và việc đánh cắp danh tính. Vì vậy, việc hoàn thiện pháp luật được coi là một trong những giải pháp cần thiết. Bài viết đề cập một số vấn đề lý luận, thực trạng bảo vệ dữ liệu cá nhân ở Việt Nam hiện nay, đề xuất một số giải pháp hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân trong thời gian tới.

**Từ khóa:** Dữ liệu cá nhân, bảo vệ dữ liệu cá nhân, pháp luật về bảo vệ dữ liệu cá nhân

## 1. Khái quát về bảo vệ dữ liệu cá nhân tại Việt Nam hiện nay

### 1.1. Khái niệm và đặc điểm về dữ liệu cá nhân

Dữ liệu cá nhân, hiểu một cách khái quát nhất là bất kỳ thông tin nào liên quan đến nhận dạng của cá nhân. Theo Quy định chung về Bảo vệ dữ liệu cá nhân (BVDLCN) của Liên minh Châu Âu (GDPR), dữ liệu cá nhân được định nghĩa là “bất kỳ thông tin gì liên quan đến một người nhận dạng được hoặc một người có thể được nhận dạng (“chủ thể dữ liệu”); một người có thể được nhận dạng là người có thể được nhận dạng trực tiếp hay gián tiếp bằng việc tham chiếu số định danh hay một hoặc nhiều các đặc điểm nhận dạng về vật lý, sinh học, gen di truyền, tâm thần, kinh tế, văn hóa và xã hội của người đó”<sup>1</sup>. Dữ liệu cá nhân bao gồm: tên và tên đệm, địa chỉ

nơi cư trú, địa chỉ email, số thông tin thẻ công dân, địa điểm dữ liệu (như địa chỉ khu vực của số điện thoại), địa chỉ IP truy cập internet, dữ liệu do bệnh viện hoặc bác sĩ nắm giữ (có thể là biểu tượng nhân dạng duy nhất của cá nhân).

Ở Hoa Kỳ, khái niệm “dữ liệu cá nhân” được sử dụng song song với khái niệm “thông tin cá nhân”, “bất kỳ thông tin nào về một cá nhân được duy trì bởi một cơ quan, bao gồm (1) bất kỳ thông tin nào mà có thể sử dụng để phân biệt hoặc theo dõi danh tính của một cá nhân, như tên, số an sinh xã hội, ngày và nơi sinh, tên, thông tin y tế, và (2) bất kỳ thông tin nào có liên quan hoặc liên kết với một cá nhân, như thông tin y tế, giáo dục, tài chính và việc làm”<sup>2</sup>.

Ở Việt Nam, theo Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về Bảo vệ dữ liệu cá nhân thì dữ liệu cá nhân được hiểu là “thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên

1. Điều 4, GDPR: “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

2. Nation Institute of Standards and Technology (2010), “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800 – 122 Natl. Inst. Stand. Technol. Spec. Publ. 800-122

môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể". Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.<sup>1</sup> Định nghĩa này khá tương thích với cách tiếp cận của các quốc gia Châu Âu, phù hợp và tương thích với xu thế phát triển của công nghệ thông tin hiện nay, trong đó có dữ liệu điện tử.

### Đặc điểm của dữ liệu cá nhân

Dữ liệu cá nhân là một loại dữ liệu được thể hiện dưới nhiều hình thức và được khai thác bằng nhiều cách, nên đặc điểm của dữ liệu cá nhân có một số điểm khác biệt so với các loại dữ liệu khác, được xác định theo một số yếu tố sau:

*Thứ nhất*, dữ liệu cá nhân mang tính cá biệt. Dữ liệu cá nhân là tập hợp các thông tin gắn với một con người cụ thể, phân biệt với những người khác trong xã hội. Tính cá biệt loại trừ những trường hợp của chủ thể khác như thông tin của tổ chức, thông tin của người đã chết.

*Thứ hai*, dữ liệu cá nhân mang tính xác thực - liên kết của thông tin. Dữ liệu cá nhân được sử dụng để nhận dạng và định danh cá nhân trong các mối quan hệ xã hội. Như thông tin của căn cước công dân, số tài khoản ngân hàng, hoặc địa chỉ email có thể dùng để xác định và liên kết với một người cụ thể.

*Thứ ba*, dữ liệu cá nhân mang tính đa dạng về nội dung và hình thức, không chỉ bao gồm thông tin cơ bản như tên và địa chỉ, mà còn có thể bao gồm hình ảnh, video, tài liệu, thông tin về hành vi trực tuyến, và nhiều loại dữ liệu khác. Điều này phản ánh sự đa dạng và phong phú của dữ liệu cá nhân.

*Thứ tư*, dữ liệu cá nhân mang dấu hiệu nhận diện của một loại quyền tài sản mới, vì dữ liệu cá nhân không chỉ liên quan đến quyền riêng tư của một người mà còn có giá trị kinh tế nhất định. Nó có thể được sử dụng để tạo ra giá trị trong nhiều ngữ cảnh, bao gồm tiếp thị, nghiên cứu thị trường, phát triển sản phẩm và dịch vụ mới.

## 1.2. Khái niệm bảo vệ dữ liệu cá nhân

Theo Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân thì "Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật"<sup>2</sup>. Như vậy, có thể hiểu bảo vệ dữ liệu cá nhân là việc thực hiện các hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý các hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật nhằm bảo đảm dữ liệu cá nhân được an toàn.

## 2. Quy định pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam hiện nay

Hiện nay bảo vệ dữ liệu cá nhân được thể hiện trước hết trong các văn bản pháp lý. Hiến pháp 2013 đặt ra nguyên tắc cơ bản về quyền riêng tư và bảo vệ dữ liệu cá nhân của mỗi công dân tại Điều 21: "1. Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình. Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn". Như vậy, Hiến pháp xác định được tầm quan trọng của việc bảo vệ thông tin cá nhân và tạo ra cơ sở pháp lý mạnh mẽ ở tầm hiến định để đảm bảo tính riêng tư và an toàn của dữ liệu cá nhân của mọi công dân. Quyền bảo vệ dữ liệu cá nhân còn được thể hiện tại các văn bản pháp lý khác như Bộ luật Dân sự 2015: "1. Đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ; Việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến đời sống riêng tư, bí mật cá nhân phải được người đó đồng ý, việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến bí mật gia đình phải được các thành viên gia đình đồng ý, trừ trường hợp luật có quy định khác" (Điều 38).

Việc thừa nhận dữ liệu cá nhân như một phần của quyền riêng tư cho phép công dân được bảo vệ khỏi sự can thiệp trái phép của các bên thứ ba. Nó tạo nền tảng pháp lý để ngăn chặn việc thu thập, sử dụng, hoặc tiết lộ dữ liệu cá nhân mà không có sự đồng ý hoặc không dựa trên cơ sở pháp lý. Điều này đảm bảo rằng mọi người có quyền kiểm soát thông tin cá

1. Điều 2, Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về Bảo vệ dữ liệu cá nhân

2. Khoản 5, Điều 2, Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân

nhân của họ và không bị xâm phạm trong việc tiết lộ thông tin cá nhân mà họ không muốn. Điều này có ý nghĩa quan trọng trong việc xây dựng một hệ thống pháp luật dân sự đáng tin cậy để bảo vệ dữ liệu cá nhân và đảm bảo tính riêng tư của mọi công dân.

Pháp luật hành chính và pháp luật hình sự đặt cơ sở cho việc bảo vệ dữ liệu cá nhân thông qua việc thiết lập các biện pháp quản lý hành chính và các biện pháp hình sự đối với những hành vi vi phạm dữ liệu cá nhân<sup>1</sup>. Pháp luật hành chính thiết lập các quy định và yêu cầu về bảo mật nhằm xác định và quy định cách thức quản lý và giám sát việc thu thập và sử dụng dữ liệu cá nhân. Pháp luật hình sự đưa ra cơ chế xử lý các hành vi xâm phạm dữ liệu cá nhân thông qua các biện pháp hình sự, bao gồm truy cứu trách nhiệm hình sự cho những người hoặc tổ chức thực hiện việc thu thập hoặc sử dụng dữ liệu cá nhân một cách trái phép hoặc không có sự đồng ý của chủ sở hữu thông tin cá nhân. Những hình phạt này có thể bao gồm phạt tiền hoặc phạt tù, nhằm đảm bảo tính riêng tư và bảo vệ dữ liệu cá nhân của công dân.

Luật Bảo vệ người tiêu dùng quy định «Người tiêu dùng được bảo đảm an toàn, bí mật thông tin của mình khi tham gia giao dịch, sử dụng hàng hóa, dịch vụ, trừ trường hợp cơ quan nhà nước có thẩm quyền yêu cầu»<sup>2</sup>; Luật An toàn thông tin mạng cũng quy định «cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng»<sup>3</sup>. Như vậy, bên cạnh quy định về quyền của người tiêu dùng khi tham gia các giao dịch thì pháp luật cũng đã quy định về trách nhiệm của mỗi cá nhân trong việc bảo vệ thông tin của chính mình.

Luật Viễn thông 2009 có đề cập đến: «Doanh nghiệp viễn thông không được tiết lộ thông tin riêng liên quan đến người sử dụng dịch vụ viễn thông, bao gồm tên, địa chỉ, số máy gọi, số máy được gọi, vị trí máy gọi, vị trí máy được gọi,

thời gian gọi và thông tin riêng khác mà người sử dụng đã cung cấp khi giao kết hợp đồng với doanh nghiệp»<sup>4</sup>.

Luật Các tổ chức tín dụng năm 2010 cũng quy định về bảo mật thông tin: «3. Tổ chức tín dụng, chi nhánh ngân hàng nước ngoài không được cung cấp thông tin liên quan đến tài khoản, tiền gửi, tài sản gửi, các giao dịch của khách hàng tại tổ chức tín dụng, chi nhánh ngân hàng nước ngoài cho tổ chức, cá nhân khác, trừ trường hợp có yêu cầu của cơ quan nhà nước có thẩm quyền theo quy định của pháp luật hoặc được sự chấp thuận của khách hàng»<sup>5</sup>.

Tuy nhiên các qui định trên mới chỉ điều chỉnh ở mức độ khái quát và nằm rải rác ở các văn bản luật khác nhau, do đó cần thiết phải có một văn bản pháp lý chuyên biệt điều chỉnh trực tiếp về bảo vệ dữ liệu cá nhân. Ngày 17 tháng 4 năm 2023 Chính phủ ban hành Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, có hiệu lực từ ngày 01/7/2023. Nghị định ra đời nhằm khắc phục những vướng mắc của pháp luật ở lĩnh vực này. Nghị định đã đưa ra được định nghĩa cụ thể về dữ liệu cá nhân, phân loại dữ liệu cá nhân gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm, và các vấn đề liên quan đến bảo vệ dữ liệu cá nhân.

So với các văn bản trước đây, Nghị định 13/2023/NĐ-CP đã cung cấp một khung pháp lý rõ ràng về quyền và nghĩa vụ của chủ thể dữ liệu. Chủ thể dữ liệu có quyền kiểm soát thông tin cá nhân của họ, bao gồm quyền truy cập, chỉnh sửa và từ chối việc thu thập thông tin. Nghị định cũng tập trung vào việc xác định quy trình bảo vệ dữ liệu cá nhân trong quá trình xử lý, đồng thời yêu cầu đánh giá tác động trước khi chuyển dữ liệu cá nhân ra nước ngoài, nhằm làm giảm nguy cơ dữ liệu cá nhân có thể rơi vào tay của các bên không có quyền. Các biện pháp và điều kiện để bảo đảm an toàn dữ liệu cá nhân cũng được quy định cụ thể. Đặc biệt, Nghị định đề cập đến trách nhiệm của các cơ quan, tổ chức và cá nhân trong việc quản lý và bảo vệ dữ liệu cá nhân. Các tổ chức cần tuân thủ các quy định bảo vệ dữ liệu và thiết lập cơ chế giám

1. Hùng Quân, Cảnh giác với thủ đoạn lợi dụng công nghệ Deepfake để lừa đảo, <https://cand.com.vn/Cong-nghe/canh-giac-voi-thu-doan-loi-dung-cong-nghe-deepfake-de-lua-dao-i688571/>, truy cập ngày 12/4/2024.

2. Khoản 1 Điều 6 quy định Luật Bảo vệ người tiêu dùng

3. Khoản 1 Điều 16 Luật An toàn thông tin mạng

4. Khoản 4 Điều 6 Luật Viễn thông năm 2009

5. Điều 14 Luật Các tổ chức tín dụng năm 2010

sát để đảm bảo rằng quyền riêng tư của chủ thể dữ liệu không bị vi phạm.

Như vậy, nhìn một cách tổng thể, hệ thống pháp luật Việt Nam về cơ bản đã ghi nhận quyền được bảo vệ dữ liệu cá nhân của mỗi người, đồng thời cũng quy định rõ trách nhiệm của mỗi cá nhân về việc tự bảo vệ thông tin cá nhân của mình.

### 3. Thực trạng về bảo vệ dữ liệu cá nhân ở Việt Nam hiện nay

Mặc dù có nhiều văn bản pháp luật đã qui định như đã nêu ở trên, tuy nhiên, tình trạng vi phạm pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam vẫn diễn ra khá phổ biến, các hành vi này có thể đến từ cơ quan nhà nước, cơ quan báo chí, truyền thông hoặc từ các doanh nghiệp, từ các cá nhân. Có thể dẫn chứng qua một số vụ việc điển hình sau đây:

Đầu năm 2023, anh N.H.K, trú tại phường Quỳnh Lôi, quận Hai Bà Trưng, Hà Nội đã bị mất giấy tờ cá nhân, trong đó có thẻ Căn cước công dân. Khoảng vài tháng sau đó, anh K bất ngờ nhận được tin nhắn yêu cầu trả khoản vay của một ứng dụng vay tiền online, mặc dù anh không hề vay tiền qua ứng dụng này<sup>1</sup>. Tình huống mất cảnh giác của anh N.H.K là một ví dụ cụ thể về cách mà thông tin cá nhân có thể bị lợi dụng và sử dụng sai mục đích trong thời đại số hóa. Điều này đặt ra một loạt vấn đề về an ninh mạng và bảo vệ thông tin cá nhân.

Hoặc vụ việc của ca sĩ V.M.H đã bị rò rỉ và lan truyền rộng rãi hình ảnh nhạy cảm trên môi trường mạng Internet. Dưới góc nhìn của một chuyên gia bảo mật, ông Võ Đỗ Thắng – Giám đốc Trung tâm An ninh mạng Athena – cho rằng, trong vụ rò rỉ hình ảnh nhạy cảm nghi của ca sĩ V.M.H, có ba khả năng dẫn đến tình trạng trên. Khả năng thứ nhất là chất lượng các sản phẩm camera kém, hệ điều hành không đảm bảo độ bảo mật cao, sẽ có những công cụ có thể quét và tìm ra đường để xâm nhập vào, lấy cắp thông tin, hình ảnh riêng tư để phát tán, trục lợi... Khả năng thứ hai là từ phía nhà cung cấp thiết bị và dịch vụ camera an ninh. Sau khi

lắp đặt, kĩ thuật viên không chuyển giao lại mật khẩu (password) và các thông số kĩ thuật khác. Chủ sở hữu cũng không quan tâm hoặc không biết để yêu cầu chuyển giao để sau đó thay đổi mật khẩu. Từ đó, kĩ thuật viên có thể có mật khẩu để vào tài khoản và theo dõi chủ sở hữu. Khả năng thứ ba, là tài khoản được chia sẻ với người khác để cùng hỗ trợ trong việc quản lý nhà cửa, và những người được chia sẻ không bảo mật tốt nên để rò rỉ mật khẩu cho đối tượng xấu và từ đó đối tượng xâm nhập để theo dõi và lấy cắp thông tin, hình ảnh.<sup>2</sup>

Thêm vào đó, sự ra đời và phát triển mạnh mẽ của công nghệ Deepfake kết hợp với sự rò rỉ dữ liệu cá nhân đã làm “nở rộ” làn sóng lừa đảo online không chỉ ở Việt Nam mà ở phạm vi toàn cầu. Theo các chuyên gia công nghệ, những đối tượng xấu đã sử dụng công nghệ Deepfake AI, tạo ra các sản phẩm công nghệ âm thanh, hình ảnh, video làm giả người ngoài đời thực với độ chính xác tương đối cao<sup>3</sup> phục vụ cho kịch bản lừa đảo.

Theo quan sát của Bkav, tại Việt Nam, nhiều trang thương mại điện tử lớn, một số nền tảng giao hàng trực tuyến có nhiều người sử dụng, đã bị xâm nhập và đánh cắp dữ liệu. Theo kết quả *đánh giá an ninh mạng Bkav của Tập đoàn công nghệ Bkav, năm 2020, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã đạt kỷ lục mới, vượt mốc 1 tỷ USD (23,9 nghìn tỷ đồng)*.<sup>4</sup>

Thực trạng trên đã phản ánh phần nào những hậu quả nghiêm trọng của hành vi xâm phạm dữ liệu cá nhân ở Việt Nam. Đồng thời đặt ra yêu cầu cần tiếp tục nghiên cứu, hoàn thiện các quy định pháp luật liên quan đến bảo vệ dữ liệu cá nhân, tăng cường các giải pháp phù hợp để bảo vệ quyền và lợi ích hợp pháp của mọi chủ thể dữ liệu.

2. Thế Lâm, Văn Mai Hương nghi bị lộ clip: Chuyên gia nói về 3 lỗ hổng rò rỉ hình ảnh, <https://laodong.vn/giai-tri/van-mai-huong-nghi-bi-lo-clip-chuyen-gia-noi-ve-3-lo-hong-ro-ri-hinh-anh-775260>. Ido, truy cập ngày 18/4/2024;

3. Hùng Quân, Cảnh giác với thủ đoạn lợi dụng công nghệ Deepfake để lừa đảo, <https://cand.com.vn/Cong-nghe/canh-giac-voi-thu-doan-loi-dung-cong-nghe-deepfake-de-lua-dao-i688571/>, truy cập ngày 18/4/2024.

4. Lâm Thảo, Toàn cảnh an ninh mạng Việt Nam năm 2020: Tổn thất hơn 1 tỷ USD do virus máy tính, <https://nhandan.vn/toan-can-an-ninh-mang-viet-nam-nam-2020-ton-that-hon-1-ty-usd-do-virus-may-tinh-post632235.html>, truy cập ngày 12/4/2024

1. Triệu Quang Xuyên, Không nợ vẫn bị đòi tiền vì lộ thông tin căn cước công dân, người dân phải làm gì, [https://thanhtri.hanoi.gov.vn/cong-nghe-thong-tin-an-toan-thong-tin/-/asset\\_publisher/HgNzII7sMGQj/content/khong-no-van-bi-oi-tien-vi-lo-thong-tin-can-cuoc-cong-dan-nguoi-dan-phai-lam-gi](https://thanhtri.hanoi.gov.vn/cong-nghe-thong-tin-an-toan-thong-tin/-/asset_publisher/HgNzII7sMGQj/content/khong-no-van-bi-oi-tien-vi-lo-thong-tin-can-cuoc-cong-dan-nguoi-dan-phai-lam-gi)

#### 4. Một số khuyến nghị hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân

*Thứ nhất*, cần làm rõ khái niệm “trụ sở” trong quy định tại điểm a khoản 5 Điều 14 Nghị định 13/2023/NĐ-CP. “Trụ sở” ở đây có thể hiểu là “trụ sở chính” như Điều 42 Luật Doanh nghiệp năm 2020 đề cập: “trụ sở chính của doanh nghiệp đặt trên lãnh thổ Việt Nam, là địa chỉ liên lạc của doanh nghiệp và được xác định theo địa giới đơn vị hành chính; có số điện thoại, số fax và thư điện tử (nếu có)”<sup>1</sup> hay là địa điểm kinh doanh, chi nhánh, văn phòng đại diện.

Hiện nay, chưa có văn bản nào quy định rõ về số lượng trụ sở của doanh nghiệp. Tuy nhiên dựa vào các quy định pháp luật hiện hành, mỗi doanh nghiệp chỉ có một trụ sở chính - là địa chỉ mà doanh nghiệp đăng ký trong giấy đăng ký kinh doanh, khác với địa điểm kinh doanh, chi nhánh, văn phòng đại diện,...

Nếu hiểu “trụ sở” là “trụ sở chính” thì sẽ dẫn đến sự bất tiện trong việc di chuyển của chủ thể dữ liệu/người được ủy quyền khi phát sinh yêu cầu cung cấp dữ liệu. Vì các doanh nghiệp, tổ chức có thể có nhiều chi nhánh, văn phòng đại diện ở nhiều nơi trên cả nước nhưng trụ sở chính được đặt tại một địa phương khác.

Vì vậy, “trụ sở” cần được mở rộng phạm vi là địa điểm kinh doanh, chi nhánh, văn phòng đại diện. Như vậy có thể điều chỉnh điểm a khoản 5 Điều 14 Nghị định 13/2023/NĐCP là “*Chủ thể dữ liệu trực tiếp hoặc ủy quyền cho người khác đến trụ sở, chi nhánh, văn phòng đại diện, hoặc địa điểm kinh doanh của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân yêu cầu cung cấp dữ liệu cá nhân*”. Điều này tạo thuận lợi cho quy trình tiếp nhận yêu cầu của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân giải quyết khó khăn không bắt buộc người yêu cầu phải di chuyển đến trụ sở chính.

*Thứ hai*, quy định về xử lý dữ liệu cá nhân của người bị tuyên bố mất tích, đã chết theo Nghị định 13/2023/NĐ-CP đang bị bó hẹp trong phạm vi chỉ chấp nhận khi có sự đồng ý trong hàng thừa kế thứ nhất, cụ thể là vợ, chồng, con thành niên hoặc của cha, mẹ người

bị tuyên bố mất tích, đã chết. Vì vậy, có thể mở rộng thêm phạm vi quyền đồng ý xử lý dữ liệu cá nhân của người bị tuyên bố mất tích, đã chết, thực hiện theo nguyên tắc ưu tiên, có thể trao thêm quyền này cho người giám hộ, và những người nằm trong các hàng thừa kế theo quy định về hàng thừa kế tại Điều 651 Bộ luật Dân sự năm 2015.

*Thứ ba*, cần qui định thời hạn thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân tại khoản 4 Điều 23 Nghị định 13/2023/NĐ-CP đối ứng với từng ngành, từng lĩnh vực cụ thể. Vì thuật ngữ “từng đợt, từng giai đoạn” còn chung chung, dẫn đến việc xác định trách nhiệm của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân gặp khó khăn khi các chủ thể này vi phạm quy định về bảo vệ dữ liệu cá nhân. Thời hạn cụ thể cần được nghiên cứu, xem xét và đánh giá thận trọng dựa trên các tiêu chí về loại dữ liệu cá nhân bị xâm phạm (dữ liệu cá nhân nhạy cảm hay dữ liệu cá nhân cơ bản), mức độ của hành vi vi phạm và có thể xét đến cả nhóm ngành, nghề kinh doanh, hoạt động.

*Thứ tư*, cần nghiên cứu xây dựng một đạo luật riêng về bảo vệ dữ liệu cá nhân. Hiện ở Châu Âu đã có văn bản pháp luật chung của EU và nhiều nước trong khu vực ban hành văn bản quy phạm pháp luật riêng bảo vệ dữ liệu cá nhân. Ở Việt Nam, quy định pháp luật về vấn đề này còn nằm rải rác ở nhiều văn bản luật. Nghị định 13/2023/NĐ-CP được ban hành là bước tiến quan trọng nhưng hiệu lực pháp lý thấp. Vì vậy, việc xây dựng một đạo luật riêng về bảo vệ dữ liệu cá nhân là cần thiết, sẽ khắc phục tình trạng chồng chéo các quy định pháp luật và đảm bảo thực thi thống nhất trong thực tiễn.

*Thứ năm*, đối với một số ngành nghề kinh doanh có tính đặc thù về loại dữ liệu cá nhân như: tài chính ngân hàng, bảo hiểm, bất động sản, chăm sóc sức khỏe y tế, quảng cáo, truyền thông, cần có quy định bắt buộc phải mã hoá dữ liệu cá nhân để thông tin được an toàn và bảo mật hơn vì nếu bị rò rỉ sẽ gây ra những hệ lụy nghiêm trọng không chỉ cho chủ thể dữ liệu mà còn ảnh hưởng đến cá nhân, cơ quan và tổ chức khác bao gồm cả Bên Kiểm soát dữ liệu, Bên Kiểm soát và xử lý dữ liệu./.

1. Điều 42 Luật Doanh nghiệp năm 2020