IPS Viện Nghiên cứu Chính sách và Phát triển Truyền thông

ĐÁNH GIÁ BAN ĐẦU

THỰC THI NGHỊ ĐỊNH BẢO VỆ DỮ LIỆU CÁ NHÂN

KHUYẾN NGHỊ HOÀN THIỆN DỰ THẢO LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN

THÁNG 04 NĂM 2025

A: 18th Floor, VTC Online Building, 18 Tam Trinh, Hanoi
T: (+84) 373 643 601 | E: contact@ips.org.vn | W: https://ips.org.vn/

Giới thiệu về Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS)

Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS) là tổ chức nghiên cứu, tư vấn chính sách độc lập thuộc Hội Truyền thông số Việt Nam. IPS cung cấp các phân tích và giải pháp chính sách nhằm tối ưu tiềm năng của công nghệ số, góp phần thúc đẩy thịnh vượng kinh tế và củng cố an toàn số cho đất nước, người dân Việt Nam. Lĩnh vực nghiên cứu, tư vấn chính sách của IPS gồm kinh tế số, chính phủ số và xã hội số.

Về kinh tế số, IPS tập trung vào nghiên cứu và tư vấn về: (1) chính sách về hạ tầng cho kinh tế số như cáp quang biển, vệ tinh, trung tâm dữ liệu, phát triển trí tuệ nhân tạo; (2) chính sách điều tiết thị trường dịch vụ số, nhằm tăng cường giao lưu thương mại, văn hóa, kinh tế giữa Việt Nam với các nước trên thế giới. Về xã hội số, IPS đi sâu nghiên cứu thực tiễn bảo vệ quyền trên môi trường số, khuyến khích sự tham gia của công dân vào quản trị công. Về chính phủ số, IPS nghiên cứu và tư vấn về quản trị dữ liệu, thúc đẩy dữ liệu mở và nâng cao hiệu quả dịch vụ công, ứng dụng AI trong khu vực công, những giải pháp nhằm mang lại lợi ích cho người dân.

1. Giới thiệu chung

Tháng 04/2023, Nghị định 13/2023/NĐ-CP Bảo vệ dữ liệu cá nhân (sau đây viết tắt là Nghị định 13) được ban hành, đặt ra nhiều nghĩa vụ cho các chủ thể thực thi nhằm bảo vệ an toàn dữ liệu cá nhân. Dự thảo Luật Bảo vệ dữ liệu cá nhân sắp tới cũng được xây dựng dựa trên các quy định hiện có của Nghị định 13/2023/NĐ-CP, tạo điều kiện thuận lợi cho tổ chức, cá nhân trong việc tuân thủ các quy định.

Nghị định 13 có những tác động tích cực trên thực tế, bao gồm nâng cao nhận thức và thực hành bảo vệ dữ liệu của cả doanh nghiệp và người dùng, hạn chế các hoạt động mua bán, khai thác trái phép dữ liệu cá nhân. Bên cạnh đó, thời gian qua có không ít tổ chức phản ánh về vướng mắc, khó khăn trong việc tuân thủ các quy định của Nghị định 13. Dựa trên khảo sát 4.935 đơn vị, tổ chức tại Việt Nam, báo cáo tổng kết An ninh mạng 2024 do Hiệp hội An ninh mạng Quốc gia (NCA) kết luận, có tới 58,82% tổ chức, đơn vị cho biết gặp nhiều vướng mắc trong vấn đề thủ tục, quy trình và pháp lý. 17,65% đơn vị cho biết đang thiếu biện pháp kỹ thuật bảo vệ dữ liệu[1].

Tài liệu này tổng hợp kết quả khảo sát, làm rõ những khó khăn, vướng mắc của các tổ chức, bao gồm doanh nghiệp và tổ chức phi lợi nhuận trong việc tuân thủ các nghĩa vụ được đặt ra trong Nghị định 13 và dự thảo Luật Bảo vệ dữ liệu cá nhân. Khảo sát thu thập ý kiến từ hơn 60 tổ chức, doanh nghiệp, trong đó tập trung vào các tổ chức, doanh nghiệp nắm giữ nhiều dữ liệu nhạy cảm như y tế, viễn thông, ngân hàng và tổ chức tín dụng. Trên cơ sở tìm hiểu nguyên nhân khó khăn, vướng mắc của tổ chức, doanh nghiệp, từ cả khía cạnh khách quan lẫn chủ quan, Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS) đưa ra một số đề xuất cụ thể đối với dự thảo Luật Bbảo vệ dữ liệu cá nhân và các định hướng để xây dựng văn bản hướng dẫn thi hành Luật này trong tương lai, hướng đến một đạo luật bảo vệ dữ liệu cá nhân hiệu quả, vừa bảo vệ được lợi ích của cá nhân, vừa hài hòa được lợi ích của tổ chức, doanh nghiệp, đảm bảo môi trường kinh doanh lành mạnh, thúc đẩy phát triển kinh tế số.

[1] https://datasecurity.vn/vi/post/hon-43--to-chuc--doanh-nghiep-chua-co-nhan-su-chuyen-trach-bao-ve-du-lieu-ca-nhan-26.htm

2. Thực trạng triển khai Nghị định 13/2023/NĐ-CP tại một số tổ chức

2.1. Mức độ sẵn sàng thực thi

Trước tiên, **phần lớn đơn vị được khảo sát đều ghi nhận tầm quan trọng ngày càng tăng của bảo vệ dữ liệu cá nhân**, đặc biệt trong các lĩnh vực y tế, ngân hàng, công nghệ và viễn thông. Toàn bộ bên trả lời khảo sát đều đón nhận và ủng hộ các quy định của cơ quan soạn thảo, thực thi, nhất trí về chủ trương bảo vệ dữ liệu cá nhân mà Đảng và Nhà nước đặt ra. Đặc biệt, Nghị định 13 được nhìn nhận là tín hiệu tích cực, thúc đẩy sự chuyển biến từ nhận thức sang hành động, đồng thời tạo điều kiện để doanh nghiệp chuẩn bị hợp lý trước khi Luật Bảo vệ dữ liệu cá nhân được ban hành. Trong giai đoạn Nghị định 13 có hiệu lực, một số doanh nghiệp, tổ chức phi lợi nhuận đã chủ động rà soát quy trình xử lý dữ liệu, bổ sung quy định nội bộ, đào tạo nhân viên và phân công rõ ràng bộ phận chịu trách nhiệm tuân thủ. Đồng thời, nhóm này cũng theo dõi rất sát những thông tin lập pháp mới nhất liên quan đến dự án Luật Bảo vệ dữ liệu cá nhân để chuẩn bị tuân thủ.

Mặt khác, **mức độ sẵn sàng triển khai giữa các nhóm đối tượng khác nhau có sự chênh lệch đáng kể**. Các tập đoàn lớn, đặc biệt là doanh nghiệp có vốn đầu tư nước ngoài từng tiếp cận tiêu chuẩn quốc tế như Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (General Data Protection Regulation – GDPR), thường có lợi thế về nhân sự chuyên môn, hệ thống kỹ thuật và văn hóa tuân thủ. Trong khi đó, nhiều doanh nghiệp trong nước, nhất là doanh nghiệp nhỏ và vừa, tổ chức phi lợi nhuận trong nước còn gặp khó khăn trong việc hiểu đúng yêu cầu pháp lý và thiếu nguồn lực để triển khai bài bản. Hầu hết các doanh nghiệp, tổ chức phi lợi nhuận ở quy mô nhỏ và vừa không có cán bộ phụ trách pháp chế riêng, không có cán bộ kỹ thuật phụ trách dữ liệu riêng. Do đó, họ thiếu thông tin pháp lý lẫn thiếu nguồn lực kỹ thuật để tuân thủ.

Khối các cơ quan nhà nước cũng gặp nhiều khó khăn trong nắm bắt thông tin và thực hiện tuân thủ. Đánh giá các cổng thông tin cung cấp dịch vụ công của 63 tỉnh thành phố cho thấy gần như toàn bộ các cổng không đạt yêu cầu về tiêu chí công khai chính sách bảo vệ dữ liệu. Ví dụ, chính sách bảo vệ dữ liệu hoặc không có, hoặc được soạn thảo không đáp ứng đúng quy định pháp luật. Điều này đặt ra nghi vấn trong quá trình thu thập, xử lý dữ liệu cá nhân của cơ quan nhà nước, rất có thể, việc tuân thủ đầy đủ các quy định là chưa đạt yêu cầu.

Hơn thế nữa, kể cả những doanh nghiệp có nguồn lực, khả năng đảm bảo tuân thủ vẫn là vấn đề. Một số doanh nghiệp cho biết dù đã tích cực nghiên cứu và

triển khai các biện pháp bước đầu, nhưng vẫn không chắc liệu mình đã thực hiện đúng quy định hay chưa, do thiếu các hướng dẫn cụ thể và ví dụ minh họa từ phía cơ quan nhà nước. Tình trạng "muốn tuân thủ nhưng không biết bắt đầu từ đâu" là khá phổ biến trong cộng đồng doanh nghiệp, nhất là đối với nhóm không có phòng pháp chế hoặc không thuê ngoài dịch vụ tư vấn.

2.2. Chi phí tuân thủ

Việc thực thi các yêu cầu của Nghị định 13 đòi hỏi **các tổ chức phải đầu tư** không nhỏ **về nguồn lực tài chính, nhân sự và thời gian**. Khảo sát thực tế cho thấy, nhiều doanh nghiệp – kể cả trong lĩnh vực thâm dụng công nghệ như viễn thông – phải dành chi phí đáng kể để tổ chức đào tạo nội bộ, xây dựng quy trình xử lý dữ liệu, rà soát hợp đồng, bổ sung biểu mẫu thu thập thông tin, đồng thời thuê tư vấn pháp lý hoặc dịch vụ đánh giá kỹ thuật. Những chi phí này phát sinh do hai nhóm quy định: thứ nhất, những nghĩa vụ phải tuân thủ yêu cầu của chủ thể dữ liệu (chẳng hạn như nghĩa vụ xóa, hủy dữ liệu tại Điều 16, Điều 20, v.v), thứ hai, những nghĩa vụ phải tuân thủ yêu cầu lập báo cáo đánh giá tác động xử lý dữ liệu cá nhân và báo cáo tác động chuyển dữ liệu ra nước ngoài (Điều 24, Điều 25).

Với các doanh nghiệp quy mô lớn hoặc đã từng tuân thủ Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (General Data Protection Regulation – GDPR), hoặc các quy định pháp luật về bảo vệ thông tin cá nhân của Trung Quốc, chi phí này được xem là hợp lý và có thể tích hợp vào hệ thống hiện có. Tuy nhiên, các doanh nghiệp trên chỉ là thiểu số. **Đối với doanh nghiệp nhỏ và vừa (SMEs), vốn chiếm gần 98% trong cơ cấu thành phần kinh tế** nước ta[2], **các chi phí này trở thành gánh nặng**. Một số đơn vị chia sẻ rằng họ buộc phải lựa chọn "làm tối thiểu để tránh rủi ro, chứ chưa thể đầu tư toàn diện vào bảo vệ dữ liệu cá nhân. Tình trạng này có khả năng dẫn đến hiện tượng chuyển đổi số cầm chừng, chiếu lệ ở một bộ phận không nhỏ doanh nghiệp, gây rủi ro cao hơn đối với công tác quản trị, bảo vệ dữ liệu cá nhân.

Bên cạnh chi phí trực tiếp, doanh nghiệp còn chịu áp lực từ việc thay đổi quy trình nội bộ, tái cấu trúc luồng xử lý dữ liệu, và điều chỉnh hệ thống công nghệ thông tin. Trong một số trường hợp, việc áp dụng quy định mới dẫn đến chậm trễ trong cung cấp dịch vụ hoặc gián đoạn tạm thời trong hoạt động kinh doanh.

2.3. Hỗ trợ và hướng dẫn thực thi

[2] https://baodautu.vn/chiem-gan-98-tong-so-doanh-nghiep-doanh-nghiep-nho-va-vua-dang-o-dau-trong-nen-kinh-te-d249574.html

Ngay sau khi Nghị định 13 có hiệu lực, nhiều đơn vị đã chủ động triển khai các bước cần thiết để tuân thủ quy định. Một số doanh nghiệp lớn đã thành lập bộ phận chuyên trách về bảo vệ dữ liệu cá nhân, xây dựng quy trình nội bộ, ban hành chính sách bảo mật, tổ chức tập huấn và phân công rõ ràng trách nhiệm quản lý dữ liệu trong từng đơn vị. Một số doanh nghiệp, tổ chức phi lợi nhuận khác đã thuê tư vấn bên ngoài để rà soát và cập nhật hợp đồng, điều khoản sử dụng dịch vụ, biểu mẫu thu thập thông tin và hệ thống công nghệ. Bên cạnh đó, nhiều công ty luật và nhân sự phụ trách các công ty liên quan đến dữ liệu cũng đã chủ động xây dựng chương trình giao lưu, tập huấn, phổ biến kiến thức cho cộng đồng doanh nghiệp.

Tuy nhiên, quá trình thực hiện cho thấy còn **thiếu cơ chế tương tác hiệu quả giữa chủ thể thực thi với cơ quan quản lý nhà nước có thẩm quyền trong lĩnh vực bảo vệ dữ liệu cá nhân**. Nhiều tổ chức, doanh nghiệp phản ánh rằng họ đã gửi hồ sơ đánh giá tác động, báo cáo xử lý dữ liệu cá nhân hoặc yêu cầu hướng dẫn cụ thể nhưng không nhận được phản hồi. Một số đơn vị còn bày tỏ lo ngại rằng, dù đã nỗ lực triển khai quy định, nhưng vì thiếu xác nhận hoặc văn bản hướng dẫn chi tiết, buộc doanh nghiệp phải tự diễn giải và áp dụng theo cách riêng, thiếu sự thống nhất, làm gia tăng nguy cơ vi phạm không chủ ý.

Thực trạng này dẫn đến sự bị động trong việc áp dụng các mô hình sử dụng dữ liệu mới, đặc biệt là đối với các doanh nghiệp cung cấp nền tảng số, dịch vụ trực tuyến hoặc có nhu cầu xử lý khối lượng dữ liệu lớn trong các lĩnh vực như y tế, tài chính. Thời gian qua, **một số doanh nghiệp chọn cách trì hoãn hoặc thu hẹp quy mô hoạt động xử lý dữ liệu để tránh rủi ro, dù điều đó có thể ảnh hưởng đến năng lực cạnh tranh của doanh nghiệp trong bối cảnh chuyển đổi số**.

Nhiều đơn vị cũng phản ánh rằng khi gặp vướng mắc trong thực tế, họ **không biết liên hệ cơ quan nào để được hướng dẫn kịp thời**. Chẳng hạn, một số doanh nghiệp cho biết họ đã xây dựng hồ sơ đánh giá tác động theo yêu cầu của Nghị định 13 (cụ thể là các bộ hồ sơ theo quy định tại Điều 24, Điều 25 của Nghị định 13) nhưng chưa nhận được phản hồi chính thức từ cơ quan chức năng về việc hồ sơ hợp lệ hay chưa. Điều 24, Điều 25 quy định Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân lập và lưu giữ Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của mình kể từ thời điểm bắt đầu xử lý dữ liệu cá nhân. Việc chậm phản hồi về tính hợp lệ của hồ sơ tạo ra tâm lý thiếu chắc chắn, khiến doanh nghiệp không dám xử lý dữ liệu cá nhân hoặc không dám chủ động áp dụng thêm các mô hình sử dụng dữ liệu mới, ảnh hưởng đến khả năng đổi mới và cạnh tranh.

Bên cạnh đó, các khóa đào tạo liên quan đến bảo vệ dữ liệu cá nhân hiện nay cũng chủ yếu do các đơn vị tư nhân tổ chức, với chi phí cao, chưa phổ cập được cho đa số doanh nghiệp nhỏ và vừa. Trong khi đó, các cơ sở dữ liệu hướng dẫn, các bộ câu hỏi thường gặp (FAQs), hoặc tài liệu hướng dẫn mẫu phục vụ việc triển khai nội bộ tại doanh nghiệp gần như chưa được xây dựng đầy đủ và công bố rộng rãi.

Ngoài ra, mặc dù đã có sự ra đời của một số tổ chức như Hiệp hội An ninh mạng quốc gia, Hiệp hội Dữ liệu quốc gia, nhưng vai trò hỗ trợ tổ chức, doanh nghiệp trong việc hướng dẫn tuân thủ bảo vệ dữ liệu cá nhân còn rất hạn chế. Các hiệp hội này chủ yếu hoạt động dựa trên mô hình thành viên, yêu cầu tham gia phức tạp, chi phí cao và chưa có quy trình rõ ràng cho việc chia sẻ kinh nghiệm, tư vấn hay hỗ trợ pháp lý kịp thời cho các bên quan tâm.

2.4. Cách hiểu và áp dụng khái niệm *"Dữ liệu cá nhân"* và *các khái niệm liên quan*

Một trong những khó khăn lớn nhất mà tổ chức, doanh nghiệp gặp phải trong quá trình triển khai Nghị định 13 là sự không thống nhất về cách hiểu đối với các khái niệm quan trọng như "dữ liệu cá nhân", "dữ liệu cá nhân nhạy cảm", hoặc xử lý dữ liệu cá nhân. Dù các khái niệm này đã được nêu trong Nghị định, nhưng phần lớn hoặc mang tính định danh liệt kê, hoặc còn quá chung chung, khiến chủ thể thực thi lúng túng trong việc xác định phạm vi áp dụng.

"Dữ liệu cá nhân" là thuật ngữ có nhiều cách hiểu, vì nó gắn liền với một số khái niệm liên quan trong pháp luật về quyền con người, pháp luật dân sự, và quản trị công nghệ thông tin. Theo quy định tại khoản 1 Điều 2, khoản 2 Điều 2, khoản 3 Điều 2 Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân, có bốn tiêu chí để xác định xem một đối tượng nào đó có phải là "dữ liệu cá nhân" hay không:

(1) đối tượng đó là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự;

(2) đối tượng đó tồn tại trên môi trường điện tử;

(3) nội dung của thông tin mà đối tượng đó phản ánh phải gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể;

(4) đối tượng đó phải thuộc một trong hai nhóm: (a) dữ liệu cá nhân cơ bản hoặc (b) dữ liệu cá nhân nhạy cảm.

Tuy nhiên, thực tiễn thi hành trong thời gian vừa qua cho thấy, giữa cơ quan xây dựng luật, cơ quan kiểm tra, cơ quan thi hành và doanh nghiệp chưa thống nhất cách hiểu khái niệm "dữ liệu cá nhân". Nội dung mâu thuẫn chủ yếu xoay quanh tiêu chí (2), tiêu chí (3) và tiêu chí (4).

Đối với cơ quan soạn thảo, xây dựng luật, dựa trên các tài liệu nghiên cứu, báo cáo, tổng hợp, dự thảo của cơ quan, có thể thấy cơ quan đang hiểu "dữ liệu cá nhân" theo nghĩa rộng. Theo đó, "dữ liệu cá nhân" có xu hướng được cơ quan hiểu là toàn bộ thông tin trong môi trường điện tử, "gắn liền vớimột con người sinh học cụ thể" hoặc "giúp xác định một con người cụ thể".

Nói cách khác, khi xác định một đối tượng dữ liệu/thông tin có phải là "dữ liệu cá nhân" hay không, cơ quan soạn thảo có xu hướng tập trung nhất vào tiêu chí (2) và tiêu chí (3): thông tin đó có "gắn liền với một con ngườicụ thể" hoặc "có thể từ đó suy diễn ra một con người cụ thể" hay không.

Đối với cơ quan kiểm tra, thi hành, tiếp xúc và làm việc trực tiếp với doanh nghiệp, dựa trên khảo sát, phỏng vấn với đại diện các doanh nghiệp, nhận thấy cơ quan kiểm tra, thực thi quan tâm nhiều đến tính chất "nhạy cảm" hay "không đến mức nhạy cảm" của dữ liệu cá nhân được doanh nghiệp, tổ chức thu thập, lưu trữ, xử lý.

Tuy nhiên, hiện nay định nghĩa tại khoản 3 Điều 2, khoản 4 Điều 2 Nghị định 13/2023/NĐ-CP được quy định theo dạng liệt kê, các loại dữ liệu được xác định sẵn theo dạng danh sách chi tiết chứ không có tiêu chí giúp phân biệt rõ. Chỉ có tiêu chí giúp xác định "dữ liệu cá nhân nhạy cảm" tại khoản 4 Điều 2 là "Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân". Tuy nhiên, định nghĩa trên quá rộng, có nguy cơ dẫn đến cách giải thích chủ quan, dẫn đến nhiều cách hiểu không thống nhất.

Ngoài ra, một yếu tố phát sinh trên thực tế nhưng chưa được dự liệu khi soạn thảo luật, đó là trong công nghiệp công nghệ số, dữ liệu luôn tồn tại dưới hình thức tổ chức chứ không phải dưới hình thức đơn lẻ. Nói cách khác, dữ liệu cá nhân thường tồn tại lẫn trong các "trường" dữ liệu và các "khối" dữ liệu số khác. Việc xác định dữ liệu nào là "dữ liệu cá nhân nhạy cảm" và "dữ liệu cá nhân cơ bản" đòi hỏi doanh nghiệp phải can thiệp sâu hơn vào các khối dữ liệu thô, phải chiết tách các dữ liệu ra và phân loại, sắp xếp. Việc này rất khó đối với các hình thức dữ liệu khó chuyển thành dạng văn bản. Ví dụ: dữ liệu cuộc gọi của người dùng mạng viễn thông, dữ liệu lịch sử truy cập và sử dụng dịch vụ, v.v.

Cuối cùng, việc liệt kê các loại dữ liệu theo hướng danh sách chi tiết sẽ tiềm ẩn nguy cơ bỏ qua một số loại dữ liệu nhạy cảm khác, có thể phát sinh trên thực tiễn mà chưa thể dự liệu trước. Ví dụ: dữ liệu về hình ảnh cá nhân (công nghệ nhận diện khuôn mặt, nhận diện một số chi tiết giải phẫu học trên mặt), dữ liệu sinh trắc học, v.v.

Điều này gây lúng túng cho công tác kiểm tra, giám sát, đánh giá thực thi của cơ quan kiểm tra, thực thi, cũng như cho việc hiểu và tuân thủ quy định của doanh nghiệp.

Đối với doanh nghiệp, khi doanh nghiệp sử dụng các dữ liệu đặc thù trong lĩnh vực hoạt động sản xuất, dịch vụ, kinh doanh, có một vấn đề được đặt ra là các quy định bảo vệ dữ liệu cá nhân hiện hành có được áp dụng với các doanh nghiệp này không và liệu có cần quy định các biện pháp mang tính chặt chẽ hơn đối với doanh nghiệp thu thập và sử dụng các dữ liệu sức khỏe, hội thoại, tài chính, v.v, của người tiêu dùng không? Lý do là, nếu như "địa chỉ", "số điện thoại" của một người cũng được xếp vào dữ liệu cá nhân thì rõ ràng, các dữ liệu về hội thoại, ví dụ về cảm xúc, suy nghĩ của người gọi, cũng như tình hình tài chính, hộ tịch, v.v được tiết lộ trong quá trình nói chuyện, tuy cũng có thể coi là "dữ liệu" nhưng độ "nhạy cảm" của các dữ liệu này lớn hơn nhiều so với thông tin về "số điện thoại" hoặc "tên", "tuổi", v.v. Khó khăn này cũng tương đồng với khó khăn trong việc phân loại thành "dữ liệu cơ bản" và "dữ liệu nhạy cảm" như đối với cơ quan kiểm tra, thực thi.

Trong quá trình khảo sát, nhiều doanh nghiệp chia sẻ rằng khi thực hiện đánh giá dữ liệu nội bộ, họ không thể xác định rõ đâu là dữ liệu cá nhân nhạy cảm nếu thông tin đó nằm trong các khối dữ liệu hỗn hợp (ví dụ: dữ liệu cuộc gọi, dữ liệu lịch sử truy cập dịch vụ). Một số doanh nghiệp đã gửi văn bản xin hướng dẫn hoặc xác nhận về việc phân loại dữ liệu, nhưng không nhận được phản hồi từ cơ quan nhà nước.

Đặc biệt, tiêu chí "gắn liền với một con người cụ thể" hoặc "có thể dùng để xác định con người cụ thể" được hiểu theo nhiều cách khác nhau giữa doanh nghiệp và cơ quan quản lý. Điều này dẫn đến rủi ro bị áp dụng chế tài ngay cả khi doanh nghiệp không cố ý vi phạm.

Ví dụ, khi các trường dữ liệu đơn lẻ, không chứa thông tin về cá nhân hoặc gắn liền với một cá nhân cụ thể được gửi từ chủ thể A sang chủ thể B (đúng mục đích xử lý đã thông báo với chủ thể dữ liệu cá nhân và đã được sự đồng ý), dữ liệu đó có thể là một chuỗi kí tự ngẫu nhiên hoặc chuỗi mã số ngẫu nhiên, không có ý

nghĩa. Tuy nhiên, khi chủ thể B nhận được dữ liệu đó, chủ thể B tự kết hợp với bể dữ liệu mà chủ thể B đang xử lý, từ đó tái nhận diện lại được cá nhân. Việc này phụ thuộc vào lượng dữ liệu mà B đang lưu trữ, xử lý, cũng như thuật toán mà chủ thể B sử dụng, chứ chủ thể A không biết được. Như vậy, khi gửi dữ liệu cho chủ thể B, chủ thể A có phải đang "xử lý dữ liệu cá nhân" hay không? Trường hợp này là một trong những trường hợp mà doanh nghiệp gặp phải. Khi doanh nghiệp trao đổi với cơ quan thực thi, cũng nhận lại được sự lúng túng của cơ quan thực thi.

Việc thiếu tiêu chuẩn kỹ thuật, thiếu ví dụ áp dụng và không có văn bản hướng dẫn thực thi rõ ràng đã khiến không ít doanh nghiệp bị động, tự diễn giải và dẫn đến áp dụng thiếu nhất quán. Thực tế này cũng khiến cơ quan kiểm tra gặp khó trong việc giám sát đồng bộ, và dẫn đến cách xử lý chưa thống nhất giữa các địa phương.

2.5. Phạm vi áp dụng và mối quan hệ với các văn bản pháp luật khác

Một bất cập lớn khác trong thực tiễn thi hành Nghị định số 13/2023/NĐ-CP là sự chưa rõ ràng về phạm vi áp dụng và mối quan hệ giữa các quy định bảo vệ dữ liệu cá nhân với các văn bản pháp luật liên quan.

Trước hết, dữ liệu cá nhân vừa được nhìn nhận là đối tượng bảo vệ quyền nhân thân, vừa được coi là tài sản có giá trị kinh tế trong bối cảnh phát triển kinh tế số. Tuy nhiên, Nghị định 13 chưa làm rõ nguyên tắc phân định khi nào quyền nhân thân được ưu tiên, khi nào quyền tài sản đối với dữ liệu có thể được công nhận và bảo vệ. Điều này gây lúng túng cho doanh nghiệp trong việc xác định căn cứ pháp lý áp dụng, đặc biệt trong các hoạt động khai thác, phân tích và kinh doanh dữ liệu.

Thứ hai, song song với Nghị định 13, các quy định tại Luật Dữ liệu, Luật An toàn thông tin mạng, Luật Giao dịch điện tử, Bộ luật Dân sự và các văn bản chuyên ngành như Luật Viễn thông, Luật Bưu chính, Luật Bảo vệ quyền lợi người tiêu dùng cũng điều chỉnh vấn đề thông tin cá nhân hoặc dữ liệu cá nhân. Tuy nhiên, giữa các văn bản này còn tồn tại sự giao thoa, chồng lấn, và trong nhiều trường hợp không có nguyên tắc giải quyết xung đột rõ ràng. Đặc biệt, giữa Luật Dữ liệu và Nghị định 13/2023/NĐ-CP tồn tại rất nhiều điểm giao thoa, nhưng không có điều khoản nào giúp xác định khi nào thì áp dụng quy định tại văn bản nào. Điều này khiến doanh nghiệp không biết nên ưu tiên áp dụng quy định nào trong trường hợp xảy ra mâu thuẫn.

Ngoài ra, việc Nghị định 13/2023/NĐ-CP chưa có cơ chế liên thông hoặc phân định rõ phạm vi điều chỉnh so với Luật An ninh mạng cũng khiến các tổ chức phải đồng thời tuân thủ nhiều tầng quy định về bảo vệ thông tin, dữ liệu, gây tăng chi phí và rủi ro tuân thủ.

Lấy ví dụ, cho một trường dữ liệu về hoạt động của doanh nghiệp C, bao gồm thông tin về nhân sự, thông tin về người đại diện theo pháp luật của doanh nghiệp mình (ông D), thông tin về sản phẩm do C sản xuất và thông tin về kết quả hoạt động sản xuất, kinh doanh của C. Giả sử C có nhu cầu chuyển giao trường dữ liệu này cho E, một chủ quản dữ liệu để họ xử lý. Trường hợp này, C có phải xin sự đồng ý từ D - là chủ thể dữ liệu cá nhân, có dữ liệu phản ánh về mình trong trường dữ liệu nói trên hay không?

Rõ ràng, trong ví dụ nêu trên, D hoàn toàn có quyền áp dụng pháp luật về bảo vệ dữ liệu cá nhân để từ chối không cho C chuyển giao dữ liệu liên quan đến mình cho E. Tuy nhiên, doanh nghiệp C cũng có thể áp dụng Luật Dữ liệu, lập luận rằng: trường dữ liệu nói trên là những thông tin phản ánh về doanh nghiệp C, trong đó gồm có dữ liệu do hoạt động lao động/sản xuất của doanh nghiệp C tạo ra, vì thế C là chủ thể dữ liệu/chủ sở hữu dữ liệu theo Luật Dữ liệu và có quyền định đoạt đối với trường dữ liệu này.

Vậy ở góc độ thi hành, diễn giải luật, cần ưu tiên việc thực hiện quyền của C hay của D? Vấn đề này khó có thể được giải quyết chỉ bằng việc "tách" giữa dữ liệu cá nhân và dữ liệu phi cá nhân, vì trong nhiều trường hợp, dữ liệu sẽ tồn tại thành một khối.

Về phía tổ chức, doanh nghiệp, nhiều đơn vị phản ánh rằng họ phải đối mặt với tình trạng "mỗi cơ quan hiểu một cách", khiến quá trình vận hành và xử lý dữ liệu cá nhân gặp khó khăn. Thậm chí, một số doanh nghiệp phải xin ý kiến riêng biệt cho từng tình huống cụ thể, thay vì có thể tham khảo một hệ thống nguyên tắc chung, rõ ràng, hoặc từ các ví dụ mẫu.

2.6. Một số tồn tại khác

Quá trình triển khai Nghị định số 13/2023/NĐ-CP đã cho thấy, ngoài các khó khăn về kỹ thuật và pháp lý, vẫn còn tồn tại nhiều khoảng trống thể chế khiến các chủ thể không thể tiếp cận đầy đủ các công cụ cần thiết để tuân thủ pháp luật về bảo vệ dữ liệu cá nhân.

Thứ nhất, hiện chưa có một cơ quan chuyên trách độc lập đóng vai trò làm đầu mối hỗ trợ doanh nghiệp và hướng dẫn thực thi các quy định bảo vệ dữ liệu cá

nhân. Trong khi Bộ Công an là cơ quan chủ trì ban hành và kiểm tra thực hiện Nghị định, Cục An ninh mạng và phòng, chống tội phạm công nghệ cao (A05) là cơ quan diễn giải, thực thi, kiểm tra, xử lý vi phạm hành chính, thì vai trò tư vấn, hướng dẫn, đối thoại với doanh nghiệp vẫn chưa được phân công rõ ràng. Điều này khiến việc xây dựng các hướng dẫn kỹ thuật, tài liệu mẫu, công cụ đánh giá tuân thủ và giải đáp vướng mắc chậm được triển khai, hoặc không thống nhất giữa các địa phương.

Thứ hai, vai trò của các tổ chức trung gian như hiệp hội nghề nghiệp, đơn vị tư vấn, cơ quan nghiên cứu vẫn còn hạn chế. Hiệp hội An ninh mạng và Hiệp hội Dữ liệu quốc gia tuy đã tồn tại, nhưng chưa xây dựng được hệ sinh thái hỗ trợ doanh nghiệp tuân thủ quy định một cách thực chất và phổ cập. Các tài liệu, công cụ được cung cấp hiện nay chủ yếu do các tổ chức quốc tế hoặc doanh nghiệp lớn tự phát triển, không đồng đều và khó tiếp cận đối với khối doanh nghiệp nhỏ.

Thứ ba, thiếu các nền tảng công khai phục vụ quản trị tri thức chung. Hiện chưa có hệ thống cơ sở dữ liệu mở về tiền lệ áp dụng, giải thích tình huống, hoặc danh mục mẫu hồ sơ đánh giá tác động và hợp đồng mẫu bảo vệ dữ liệu cá nhân. Doanh nghiệp không có kênh để học hỏi lẫn nhau, trao đổi thông tin với chuyên gia hoặc kết nối với cơ quan quản lý theo cách hiệu quả.

Trên cơ sở đó, cần thiết lập một hệ sinh thái hỗ trợ thực thi với các thành tố sau:

- Cơ quan chuyên trách đóng vai trò định hướng, xây dựng hướng dẫn và tổ chức phản hồi cho doanh nghiệp;
- Diễn đàn đa ngành (với sự tham gia của doanh nghiệp, chuyên gia, hội/hiệp hội/tổ chức xã hội, cơ quan nhà nước) để chia sẻ kinh nghiệm áp dụng;
- Cổng dữ liệu mở hoặc thư viện hướng dẫn kỹ thuật, biểu mẫu thực hành, công cụ tự đánh giá tuân thủ;
- Chính sách khuyến khích đào tạo, phổ cập kiến thức và nâng cao ý thức về bảo vệ dữ liệu cá nhân, giảm chi phí tiếp cận thông tin và kỹ năng tuân thủ cho doanh nghiệp vừa và nhỏ, tổ chức phi lợi nhuận quy mô vừa và nhỏ.

3. Khuyến nghị hoàn thiện dự thảo Luật Bảo vệ dữ liệu cá nhân

Trên cơ sở tổng hợp ý kiến từ doanh nghiệp, chuyên gia và kết quả khảo sát thực tiễn, Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS) đề xuất một số nhóm kiến nghị chính sách cụ thể để hoàn thiện Dự thảo Luật Bảo vệ dữ liệu cá nhân như sau:

3.1. Bổ sung tiêu chí phân biệt dữ liệu cá nhân và dữ liệu cá nhân nhạy cảm

Cần bổ sung xác định "dữ liệu cá nhân" và phân biệt "dữ liệu cá nhân" với "dữ liệu cá nhân nhạy cảm" trong Luật Bảo vệ dữ liệu cá nhân hoặc Nghị định hướng dẫn thi hành Luật Bảo vệ dữ liệu cá nhân:

(1) Chủ thể chính được phản ánh trong nội dung của dữ liệu cá nhân phải là chủ thể dữ liệu cá nhân;

(2) Chủ thể dữ liệu cá nhân phải là người tự nhiên;

(3) Nội dung mà dữ liệu cá nhân phản ánh phải gắn liền với chủ thể dữ liệu cá nhân hoặc từ nội dung mà dữ liệu phản ánh có thể xác định được ít nhất một chủ thể dữ liệu cá nhân đặc định;

(4) Dữ liệu cá nhân có thể bao gồm thông tin khách quan về cá nhân và thông tin chủ quan về cá nhân. Thông tin chủ quan về cá nhân bao gồm những thông tin phản ánh tình trạng ý thức hoặc xuất phát từ ý thức cá nhân, có thể bao gồm quan điểm, ý kiến, sự đánh giá, xu hướng, v.v. Dữ liệu chứa thông tin chủ quan về cá nhân là dữ liệu nhạy cảm.

(5) Nếu thông điệp chính được phản ánh trong dữ liệu là các yếu tố không gắn liền với một con người cụ thể, hoặc không liên quan đến việc xác định một con người cụ thể, hoặc không thể từ thông điệp này mà xác định được một con người cụ thể, thì dữ liệu này không phải là dữ liệu cá nhân. Dữ liệu không phải là dữ liệu cá nhân được gọi là dữ liệu phi-cá nhân. Dữ liệu phi-cá nhân là một loại dữ liệu số.

(6) Trường hợp không thể phân tách giữa dữ liệu cơ bản và dữ liệu nhạy cảm thì dữ liệu cá nhân được xử lý là dữ liệu nhạy cảm.

Bổ sung khái niệm mới phù hợp với thực tiễn, bao gồm:

(1) Khái niệm, điều kiện tiêu chuẩn đối với chức danh, vị trí chuyên gia bảo vệ dữ liệu; tiêu chuẩn thành lập, hoạt động của tổ chức cung cấp dịch vụ tuân thủ;

(2) Khái niệm liên quan đến hoạt động xử lý dữ liệu có yếu tố kinh doanh (ví dụ: dùng để tiếp thị, phân tích hành vi); khái niệm liên quan đến "giao dịch" hoặc "chia sẻ dữ liệu cá nhân" để hợp pháp hóa các hoạt động trao đổi, chia sẻ dữ liệu cá nhân giữa các doanh nghiệp có quan hệ gần gũi hoặc nằm trong cùng "hệ sinh thái".

3.2. Bổ sung điều khoản mới về cơ chế thực thi

Bổ sung các điều khoản quy định trách nhiệm của cơ quan quản lý nhà nước trong việc:

(1) Ban hành hướng dẫn thực thi, mẫu hồ sơ đánh giá tác động hợp lệ, cũng như biểu mẫu thu thập dữ liệu gợi ý để các doanh nghiệp có mẫu tuân thủ tốt để làm theo;

(2) Cung cấp cơ chế xác nhận, phản hồi, tư vấn chính thức cho doanh nghiệp;

(3) Công khai các án lệ, các tiền lệ thực tiễn, báo cáo hướng dẫn tự đánh giá tuân thủ định kì.

3.3. Bổ sung cơ chế hỗ trợ tổ chức, doanh nghiệp tuân thủ

- Xây dựng hệ thống hỗ trợ thực thi toàn diện, gồm:

(1) Diễn đàn chính thức hỗ trợ thực thi quy định về bảo vệ dữ liệu cá nhân, trong đó có các chuyên gia về giới để đảm bảo tính hòa nhập, đa dạng và tôn trọng quyền của nhóm dễ tổn thương. Đánh giá tác động về giới trong quá trình xây dựng các Nghị định hướng dẫn, cũng như trong đánh giá thực thi Luật sau này;

(2) Hoàn thiện cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân. Cụ thể, phần thông tin hỗ trợ trên cổng nên bao gồm mẫu hợp đồng, mẫu khiếu nại, hướng dẫn bảo vệ dữ liệu cá nhân dành cho cá nhân và doanh nghiệp hướng dẫn tuân thủ dành cho bên kiểm soát/ bên xử lý dữ liệu/ bên kiểm soát và xử lý dữ liệu, kho ngân hàng tình huống điển hình trong bảo vệ dữ liệu cá nhân. Cơ quan nhà nước có thẩm quyền có thể tham khảo một thực hành tốt về xây dựng và vận hành cổng thông tin về bảo vệ dữ liệu cá nhân - cổng thông tin Văn phòng ủy viên

thông tin (Information Commissioner's Office) của Vương quốc Anh tại địa chỉ truy cập sau: https://ico.org.uk/.

(3) Công bố danh sách các đơn vị tư vấn được công nhận và các chuyên gia bảo vệ dữ liệu đã được chứng nhận.

- Chính sách khuyến khích:

(1) Có cơ chế đào tạo phổ cập miễn phí hoặc có hỗ trợ tài chính cho doanh nghiệp vừa và nhỏ, tổ chức phi lợi nhuận;

(2) Có cơ chế hỗ trợ kỹ thuật bước đầu (chuyển giao quy trình mẫu, danh mục kiểm tra - checklist, mô hình hệ thống đơn giản);

(3) Cơ chế hợp tác công – tư trong thực thi quy định mới.

Việc ban hành Nghị định số 13/2023/NĐ-CP là bước khởi đầu quan trọng trong việc thiết lập khung pháp lý về bảo vệ dữ liệu cá nhân tại Việt Nam. Tuy nhiên, quá trình triển khai trong thực tiễn cho thấy nhiều vướng mắc vẫn tồn tại, đặc biệt là từ góc độ doanh nghiệp – chủ thể trực tiếp chịu trách nhiệm tuân thủ.

Trên cơ sở tổng hợp ý kiến từ thực tiễn và kinh nghiệm quốc tế, Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS) cho rằng, Luật Bảo vệ dữ liệu cá nhân cần được hoàn thiện theo hướng:

- Rõ ràng về khái niệm và phạm vi áp dụng;
- Có hệ thống hướng dẫn thực thi, cơ chế phản hồi, và công cụ hỗ trợ cụ thể;
- Tạo điều kiện để doanh nghiệp tuân thủ hiệu quả, chi phí hợp lý, minh bạch và nhất quán.

Một đạo luật khả thi, dễ áp dụng, có sự đồng hành từ phía nhà nước sẽ không chỉ bảo vệ quyền cá nhân mà còn góp phần hình thành một môi trường kinh doanh minh bạch, nâng cao năng lực cạnh tranh, bảo đảm an toàn dữ liệu quốc gia và thúc đẩy kinh tế số phát triển bền vững.

IPS Viện Nghiên cứu Chính sách
và Phát triển Truyền thông

Tầng 18, Tòa nhà VTC Online,
18 Tam Trinh, Hai Bà Trưng, Hà Nội
Tel: (84) 373 643 601
Email: contact@ips.org.vn
ips.org.vn