

BỘ CÔNG AN
CÔNG AN THÀNH PHỐ HÀ NỘI



BÀI DỰ THI

Cuộc Thi

TÌM HIỂU LUẬT DỮ LIỆU TRONG CÔNG AN NHÂN DÂN
“DỮ LIỆU - NỀN TẢNG KIẾN TẠO TƯƠNG LAI SỐ VIỆT NAM”

Quyển 1
NỀN TẢNG



DATA



Hà Nội, năm 2025

BỘ CÔNG AN
CÔNG AN THÀNH PHỐ HÀ NỘI



BÀI DỰ THI

TÌM HIỂU LUẬT DỮ LIỆU TRONG CÔNG AN NHÂN DÂN
“DỮ LIỆU - NỀN TẢNG KIẾN TẠO TƯƠNG LAI SỐ VIỆT NAM”

Quyển 1
Nền Tảng

Họ tên : Đỗ Tất Thắng Ngày sinh : 13/10/1998 (27 tuổi)

Giới tính : Nam Dân tộc : Kinh

Cấp bậc : Thượng úy

Chức vụ, đơn vị : Cán bộ Đội An ninh thông tin và truyền thông,

Phòng An ninh chính trị nội bộ, Công an thành phố Hà Nội;

Ủy viên Ban chấp hành Chi đoàn Thanh niên Cơ sở

Phòng An ninh Chính trị nội bộ.

Số điện thoại : 0337.222.828

HÀ NỘI - 2025



GIỚI THIỆU

Bài dự thi tìm hiểu Luật Dữ liệu năm 2024 được triển khai theo kết cấu gồm 04 quyển, nhằm bảo đảm tính hệ thống, logic và chiều sâu khoa học. Toàn bộ nội dung tập trung phân tích các vấn đề lý luận và thực tiễn về dữ liệu, gắn liền với công tác xây dựng, hoàn thiện pháp luật, quản lý nhà nước cũng như nhiệm vụ bảo vệ an ninh quốc gia trong bối cảnh chuyển đổi số.

Quyển thứ nhất – “Nền tảng” tập trung lý giải chính sách pháp luật về dữ liệu của các quốc gia trên thế giới, từ đó rút ra sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng pháp luật dữ liệu ở Việt Nam. Bên cạnh đó, quyển này còn làm rõ quyền, nghĩa vụ, trách nhiệm của các chủ thể dữ liệu, chủ sở hữu và chủ quản dữ liệu, đồng thời phân tích cơ chế bảo đảm thực hiện quyền và nghĩa vụ này trong khu vực ngoài nhà nước.

...

Với bô cục chặt chẽ và nội dung phong phú, bài dự thi không chỉ mang tính nghiên cứu, học thuật mà còn gắn với thực tiễn công tác, góp phần khẳng định vai trò quan trọng của dữ liệu trong kỷ nguyên số và trong sự nghiệp xây dựng, bảo vệ Tổ quốc!

TÁC GIẢ



06 QUYỀN, 04 NGHĨA VỤ 04 NGUYÊN TẮC CỦA CHỦ THỂ DỮ LIỆU

1. Quyền của chủ thể dữ liệu cá nhân bao gồm:

- a) Được biết về hoạt động xử lý dữ liệu cá nhân;
- b) Đồng ý hoặc không đồng ý, yêu cầu rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân;
- c) Xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân;
- d) Yêu cầu cung cấp, xóa, hạn chế xử lý dữ liệu cá nhân; gửi yêu cầu phản đối xử lý dữ liệu cá nhân;
- đ) Khiếu nại, tố cáo, khởi kiện, yêu cầu bồi thường thiệt hại theo quy định của pháp luật;
- e) Yêu cầu cơ quan có thẩm quyền hoặc cơ quan, tổ chức, cá nhân liên quan đến xử lý dữ liệu cá nhân thực hiện các biện pháp, giải pháp bảo vệ dữ liệu cá nhân của mình theo quy định của pháp luật.

2. Nghĩa vụ của chủ thể dữ liệu cá nhân bao gồm:

- a) Tự bảo vệ dữ liệu cá nhân của mình;
- b) Tôn trọng, bảo vệ dữ liệu cá nhân của người khác;
- c) Cung cấp đầy đủ, chính xác dữ liệu cá nhân của mình theo quy định của pháp luật, theo hợp đồng hoặc khi đồng ý cho phép xử lý dữ liệu cá nhân của mình;
- d) Chấp hành pháp luật về bảo vệ dữ liệu cá nhân và tham gia phòng, chống hoạt động xâm phạm dữ liệu cá nhân.

3. Chủ thể dữ liệu cá nhân khi thực hiện quyền và nghĩa vụ của mình phải tuân thủ đầy đủ các nguyên tắc sau đây:

- a) Thực hiện theo quy định của pháp luật; tuân thủ nghĩa vụ của chủ thể dữ liệu cá nhân theo hợp đồng. Việc thực hiện quyền và nghĩa vụ của chủ thể dữ liệu cá nhân phải nhằm mục đích bảo vệ quyền, lợi ích hợp pháp của chính chủ thể dữ liệu cá nhân đó;
- b) Không được gây khó khăn, cản trở việc thực hiện quyền, nghĩa vụ pháp lý của bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân;
- c) Không được xâm phạm đến quyền, lợi ích hợp pháp của Nhà nước, cơ quan, tổ chức, cá nhân khác.



MỤC LỤC

Câu 1: Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam? 1

1.1. Chính sách pháp luật về dữ liệu của các nước trên thế giới 2

 1.1.1. Xu hướng chung toàn cầu 2

 1.1.2. Các mô hình pháp luật dữ liệu tiêu biểu trên thế giới 4

 1.1.3. Kết luận 26

1.2. Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam 26

 1.2.1. Sự cần thiết 26

 1.2.2. Quan điểm và nguyên tắc chỉ đạo về dữ liệu 31

 1.2.3. Mục tiêu phát triển và quản trị dữ liệu quốc gia 35

 1.2.4. Chính sách pháp luật về dữ liệu trong Luật Dữ liệu 2024 và Nghị định 165/2025/NĐ-CP 37

 1.2.5. Kiến nghị chính sách và kết luận 59

PHỤ LỤC 62

 PL1. So sánh và bài học kinh nghiệm quốc tế cho Việt Nam 62

 PL2. Đấu tranh, phản bác các quan điểm sai trái, thù địch 77

TÀI LIỆU THAM KHẢO 89

Câu 2: Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước? 91

2.1. Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu 91

 2.1.1. Chủ thể dữ liệu 91

 2.1.2. Chủ sở hữu dữ liệu 96

 2.1.3. Chủ quản dữ liệu 105

 2.1.4. Mối quan hệ giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và chủ quản dữ liệu 122

2.2. Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước 127



2.2.1. Nghĩa vụ bắt buộc của tổ chức, cá nhân trong xử lý dữ liệu....	127
2.2.2. Cơ chế kiểm tra, giám sát và xử lý vi phạm.....	134
2.3.3. Cơ chế khuyến khích và hỗ trợ thực hiện	140
KIẾN NGHỊ, ĐỀ XUẤT	145
PHỤ LỤC	148
Đáu tranh, phản bác các quan điểm sai trái, thù địch	148
TÀI LIỆU THAM KHẢO	162



Câu 1: Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam?





Câu 1: Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam?

Trả lời

1.1. Chính sách pháp luật về dữ liệu của các nước trên thế giới

1.1.1. Xu hướng chung toàn cầu

Từ sớm, dữ liệu đã được các quốc gia coi là tài nguyên chiến lược, “dầu mỏ mới” của nền kinh tế số và là nền tảng cho chuyển đổi số quốc gia. Các quốc gia đều nhận thức rằng việc thu thập và khai thác dữ liệu lớn mang lại lợi thế cạnh tranh cho nền kinh tế, đồng thời hỗ trợ cải thiện hiệu quả quản lý nhà nước. Do đó, xây dựng khung pháp luật về dữ liệu sớm và toàn diện trở thành ưu tiên ở nhiều nước nhằm bảo vệ tài sản dữ liệu quốc gia và thúc đẩy nền kinh tế số phát triển bền vững.



Các quốc gia với xu hướng bảo vệ dữ liệu quốc gia, thúc đẩy phát triển kinh tế số. Ảnh: Internet

Xu hướng chung là nhiều nước sớm ban hành luật dữ liệu quốc gia mang tính toàn diện, thiết lập nền tảng pháp lý cho quản trị và khai thác dữ liệu. Chẳng hạn, từ năm 2016, Liên minh Châu Âu thông qua Quy định chung về Bảo vệ Dữ liệu của Liên minh Châu Âu (*General Data Protection Regulation - có hiệu lực từ tháng*



5/2018), xây dựng một bộ khung pháp luật bao quát về bảo vệ dữ liệu cá nhân áp dụng trên toàn Châu Âu. Tương tự, Trung Quốc ban hành Luật An ninh Dữ liệu (2021) và Luật Bảo vệ Thông tin Cá nhân (2021), Mỹ cũng có Đạo luật Dữ liệu Chính phủ Mở (*OPEN Government Data Act - 2018*)... Các đạo luật này thường có tầm nhìn dài hạn, tạo nền móng cho việc quản lý dữ liệu trong kỷ nguyên số.

Các chính sách của mỗi quốc gia, khu vực có những điểm khác biệt theo tình hình thực tế địa chính trị, tuy nhiên đều hướng tới mục tiêu chung nhất cân bằng giữa bảo vệ quyền riêng tư cá nhân và thúc đẩy đổi mới sáng tạo dựa trên dữ liệu. Khẩu hiệu quốc tế như "***Data Free Flow with Trust***" dữ liệu lưu chuyển tự do kèm niềm tin, phản ánh mục tiêu thúc đẩy chia sẻ dữ liệu xuyên biên giới phục vụ phát triển kinh tế, đồng thời đảm bảo niềm tin về quyền riêng tư và an ninh.



Hình ảnh: Thủ tướng Nhật Bản Shinzo Abe đề xướng xây dựng "Khu vực lưu thông dữ liệu" và nhắc tới cụm từ *Data Free Flow with Trust* tại G20 năm 2019.

Ảnh: TTXVN

Nói cách khác, nhiều quốc gia xây dựng pháp luật để vừa bảo vệ dữ liệu cá nhân chặt chẽ, vừa mở đường cho sử dụng dữ liệu thứ cấp (ví dụ: dữ liệu đã ẩn



danh, dữ liệu vì lợi ích cộng đồng) nhằm phục vụ nghiên cứu, đổi mới sáng tạo và chuyển đổi số. Trong đó, Chính phủ đóng vai trò kiến tạo hạ tầng pháp lý lẩn kĩ thuật để các chủ thể có thể chia sẻ và sử dụng dữ liệu một cách an toàn. Chẳng hạn, Châu Âu ban hành Đạo luật Quản trị Dữ liệu (*Data Governance Act - DGA*) nhằm tăng cường lòng tin và thiết lập các cấu trúc, quy trình chia sẻ dữ liệu an toàn giữa khu vực công và tư. Tương tự, Australia xây dựng Ủy ban Dữ liệu Quốc gia và cơ chế công nhận, kiểm soát các bên dùng dữ liệu công; Singapore triển khai các sandbox (*bãi thử nghiệm*) về dữ liệu và Trung tâm dữ liệu quốc gia để thử nghiệm các mô hình chia sẻ dữ liệu mới một cách có giám sát. Tất cả nhằm tạo môi trường thuận lợi để dữ liệu được lưu thông, khai thác hiệu quả nhưng vẫn trong tầm kiểm soát.

Nhìn chung, chính sách pháp luật dữ liệu trên thế giới đang tiến hóa nhanh chóng theo hướng toàn diện hơn, linh hoạt hơn để vừa bảo vệ quyền lợi cá nhân, vừa phát huy tối đa giá trị của dữ liệu trong phát triển kinh tế, xã hội.

1.1.2. Các mô hình pháp luật dữ liệu tiêu biểu trên thế giới

Mỗi quốc gia, khu vực có thể chế chính trị, tình hình kinh tế, văn hóa, xã hội khác nhau, vì vậy pháp luật tiếp cận đối với việc quản trị và khai thác dữ liệu của các quốc gia, khu vực đều có đặc điểm riêng biệt, tuy nhiên cơ bản có thể kể đến một số mô hình tiêu biểu về chính sách pháp luật dữ liệu tại các quốc gia, khu vực lớn: Châu Âu, Mỹ, Australia, Singapore, Nhật Bản, Trung Quốc, Hàn Quốc...

1.1.2.1. Liên minh Châu Âu

Liên minh Châu Âu là khu vực tiên phong với khung pháp luật dữ liệu toàn diện và chặt chẽ; đặc biệt là rất coi trọng quyền của cá nhân đối với dữ liệu và đồng thời thúc đẩy chia sẻ dữ liệu an toàn để phát triển kinh tế số.

Từ 2016, Liên minh Châu Âu đã có Quy định Bảo vệ Dữ liệu Chung (*GDPR*) có hiệu lực từ năm 2018, đặt ra tiêu chuẩn cao về bảo vệ dữ liệu cá nhân trên toàn Liên minh Châu Âu. Gần đây, Liên minh Châu Âu tiếp tục thông qua Đạo luật Quản trị Dữ liệu (*Data Governance Act - DGA*) năm 2022 (áp dụng từ tháng 9/2023) và Đạo luật Dữ liệu (*Data Act*) năm 2023 (áp dụng từ 11/01/2024).



Bộ khung này tạo nên hệ sinh thái pháp lý toàn diện về dữ liệu từ bảo vệ quyền riêng tư cá nhân cho tới thúc đẩy chia sẻ dữ liệu công, từ một cách an toàn.



Quy định Bảo vệ Dữ liệu chung (General Data Protection Regulation - GDPR) của Liên minh châu Âu (EU) đã chính thức có hiệu lực kể từ ngày 25/5/2018.

Các quy định của Liên minh Châu Âu xác lập nguyên tắc dữ liệu cá nhân thuộc quyền kiểm soát của cá nhân (*data subject*). GDPR trao cho công dân Liên minh Châu Âu nhiều quyền đối với dữ liệu của mình, như quyền được thông báo, quyền truy cập, cải chính, xóa bỏ, quyền hạn chế và phản đối xử lý, quyền di chuyển dữ liệu, nhằm đảm bảo cá nhân kiểm soát cách dữ liệu của họ được thu thập và sử dụng. Mọi tổ chức khi xử lý dữ liệu tại Liên minh Châu Âu phải tuân thủ nguyên tắc minh bạch, hợp pháp và chỉ được xử lý trong phạm vi mục đích chính đáng mà cá nhân đã biết. Cách tiếp cận này thể hiện rõ quan điểm “người dùng làm chủ dữ liệu” trong hệ thống pháp luật Liên minh Châu Âu.

Ngoài ra, thay vì để dữ liệu bị phân mảnh, Liên minh Châu Âu xây dựng hạ tầng pháp lý để khuyến khích chia sẻ và tái sử dụng dữ liệu một cách an toàn, có kiểm soát. Đạo luật Quản trị Dữ liệu (*DGA*) năm 2022 và Quy định Bảo vệ Dữ liệu Chung (*GDPR*) đưa ra các cơ chế như:



- **Tái sử dụng dữ liệu khu vực công:** Cho phép sử dụng lại những dữ liệu do cơ quan nhà nước nắm giữ (đặc biệt là dữ liệu được bảo hộ; ví dụ: dữ liệu có tính bảo mật, dữ liệu cá nhân đã ẩn danh hoặc có bản quyền) cho mục đích khác mục đích ban đầu, miễn tuân thủ điều kiện nghiêm ngặt đảm bảo không xâm phạm quyền và lợi ích ban đầu. Mỗi quốc gia Liên minh Châu Âu sẽ có điểm truy cập duy nhất (*single information point*) để tiếp nhận yêu cầu tái sử dụng dữ liệu công, giúp quy trình này minh bạch, thuận tiện.

- **Dịch vụ trung gian về dữ liệu (data intermediation services):** DGA thiết lập khung pháp lý cho các bên trung gian kết nối dữ liệu, ví dụ: các nền tảng hoặc tổ chức đóng vai trò cầu nối giữa bên cung cấp dữ liệu và bên muốn sử dụng dữ liệu. Những dịch vụ trung gian dữ liệu này phải đăng ký và tuân thủ các yêu cầu nghiêm ngặt (đảm bảo nguyên tắc minh bạch, không sử dụng dữ liệu cho mục đích riêng, đảm bảo quyền lợi các bên). Mục tiêu là tăng cường lòng tin để các doanh nghiệp, cá nhân sẵn sàng chia sẻ dữ liệu thông qua bên trung gian mà không lo bị lạm dụng.

- **Chia sẻ dữ liệu vì lợi ích cộng đồng (Data altruism):** DGA đưa ra khái niệm “data altruism”, tức các tổ chức/tổ chức phi lợi nhuận thu thập dữ liệu do cá nhân tình nguyện cung cấp nhằm phục vụ lợi ích công cộng. Những tổ chức này phải đăng ký và đáp ứng tiêu chí chặt chẽ (*phi lợi nhuận, độc lập, minh bạch...*). Đây là cách Liên minh Châu Âu khuyến khích khai thác dữ liệu cho nghiên cứu khoa học, y tế, môi trường... đồng thời bảo đảm sự đồng ý và quyền rút lại của người cung cấp.

- **Bảo vệ dữ liệu nhạy cảm và hạn chế chuyển dữ liệu ra nước ngoài:** DGA yêu cầu các bên trung gian và tổ chức altruism phải bảo đảm an ninh cho dữ liệu nhạy cảm mà họ xử lý. Đồng thời, việc chuyển dữ liệu cho bên thứ ba ngoài Liên minh Châu Âu chỉ được phép nếu nước đó đảm bảo mức bảo vệ tương đương Liên minh Châu Âu. Ví dụ: GDPR quy định bên trung gian hoặc tổ chức altruism chỉ được truyền dữ liệu cho nước thứ ba nếu nơi đó có các bảo đảm thích hợp tương đương mức bảo vệ của Liên minh Châu Âu. Quy định này nhằm ngăn



chặn việc truy cập dữ liệu Liên minh Châu Âu bởi các chính phủ nước ngoài nếu không có thỏa thuận hoặc mức bảo vệ tương xứng, qua đó tăng cường “chủ quyền dữ liệu” của Liên minh Châu Âu.

Nhìn chung, mô hình Liên minh Châu Âu đề cao việc xây dựng thị trường dữ liệu chung an toàn. Dữ liệu được xem là tài sản thuộc về cá nhân, nhà nước tạo “đường ray pháp lý” để dữ liệu có thể lưu thông phục vụ phát triển kinh tế - xã hội, nhưng không đánh đổi quyền riêng tư của công dân. Cách tiếp cận này đã biến Liên minh Châu Âu thành hình mẫu về quản trị dữ liệu cân bằng giữa bảo vệ và khai thác.

1.1.2.2. Mỹ

Khác với Liên minh Châu Âu, Mỹ không có Luật Dữ liệu liên bang độc lập; các quy định về dữ liệu được quy định trong các luật chuyên ngành (ví dụ: *Đạo luật Đạo luật về khả năng chuyển giao và trách nhiệm giải trình bảo hiểm y tế năm 1996*, *Đạo luật về Quyền hạn giáo dục và bảo mật riêng tư gia đình*, *Đạo luật Hiện đại hóa Dịch vụ Tài chính năm 1999*, *Luật bảo vệ người tiêu dùng của từng bang...*). Cách tiếp cận này phản ánh triết lý Mỹ về quy định theo từng lĩnh vực rủi ro cao, tránh một luật chung có thể kìm hãm đổi mới. Khu vực tư nhân ở Mỹ do đó có tương đối nhiều tự do trong thu thập và sử dụng dữ liệu miễn tuân thủ các luật hiện hành về chống gian lận, cạnh tranh, các luật chuyên ngành nêu trên.

Tuy không có luật chung về dữ liệu cá nhân, Mỹ chú trọng mở dữ liệu khu vực công để phục vụ minh bạch và đổi mới. *Đạo luật OPEN Government Data Act 2018* (*Đạo Luật Dữ liệu Chính phủ mở, một phần của Đạo luật Foundations for Evidence-Based Policymaking - Đạo luật Nền tảng cho việc hoạch định chính sách dựa trên bằng chứng*) của Mỹ yêu cầu toàn bộ các cơ quan liên bang phải coi dữ liệu là “mở mặc định” (*open by default*). Cụ thể, mỗi cơ quan phải công bố dữ liệu của mình ở định dạng mở (*machine-readable*), xây dựng danh mục dữ liệu toàn diện và tích cực tương tác với cộng đồng sử dụng dữ liệu. Luật này cũng chế định rằng trừ khi có lý do bảo mật/quyền riêng tư chính đáng, dữ liệu liên bang nên được công khai. Trang web Data.gov được thiết lập làm cổng dữ liệu tập trung



(đến cuối 2021 đã có trên 190 ngàn tập dữ liệu mở từ các cơ quan liên bang đăng tải). Chính sách “mở mặc định” giúp Mỹ đứng đầu thế giới về cung cấp dữ liệu mở chính phủ, thúc đẩy việc doanh nghiệp và người dân tái sử dụng dữ liệu công để tạo ra ứng dụng, dịch vụ mới, đồng thời tăng tính minh bạch của chính phủ.



Hình ảnh: Tổng thống Mỹ Donald Trump ký ban hành Đạo luật Dữ liệu Chính phủ Mở, Công khai, Điện tử và Cân thiết (OPEN). Ảnh: Meritalk

Cùng với đó, Chính phủ Liên bang Mỹ đóng vai trò tương đối hạn chế trong điều tiết việc sử dụng dữ liệu của khu vực tư nhân (*ngoài các lĩnh vực nhạy cảm nêu trên*). Tinh thần chung trong quy định là tránh can thiệp quá mức để không cản trở sáng tạo. Thay vào đó, Mỹ khuyến khích các sáng kiến tự nguyện và thị trường điều tiết. Ví dụ: nhiều công ty công nghệ Mỹ tuân thủ các tiêu chuẩn/quy tắc đạo đức nội bộ hoặc chứng nhận tư nguyên về bảo mật dữ liệu. Ủy ban Thương mại Liên bang (FTC) sử dụng quyền hạn chung về chống hành vi thương mại không lành mạnh để xử lý các vụ vi phạm nghiêm trọng về quyền riêng tư (*nhiều vụ phạt Facebook, Google vì vi phạm cam kết bảo mật với người dùng*). Năm 2022, chính quyền Mỹ cũng ban hành Khuôn khổ Quyền riêng tư Dữ liệu Liên minh Châu Âu-Mỹ (EU-U.S. Data Privacy Framework) về truyền dữ liệu xuyên Đại Tây Dương nhằm tạo thuận lợi cho doanh nghiệp chuyển dữ liệu cá nhân từ



Liên minh Châu Âu sang Mỹ, cho thấy nỗ lực đáp ứng tiêu chuẩn quốc tế nhưng vẫn dựa trên cơ chế linh hoạt, không luật hóa cứng nhắc.

Nhìn chung, mô hình Mỹ thể hiện cách tiếp cận linh hoạt, phân tán: mở tối đa dữ liệu chính phủ để phục vụ lợi ích công cộng và thúc đẩy sáng tạo (*mở mặc định - open by default*), trong khi hạn chế điều tiết cứng nhắc khu vực tư nhân ở cấp liên bang, thay vào đó dựa vào luật chuyên ngành và cơ chế thị trường. Cách tiếp cận này phản ánh hệ giá trị đề cao sáng kiến tư nhân và tự do kinh doanh của Mỹ, tuy nhiên cũng gây tranh luận về mức độ bảo vệ quyền riêng tư khi không có một luật chung toàn liên bang.

1.1.2.3. Australia

Australia là quốc gia đi tiên phong trong việc mở rộng chia sẻ dữ liệu khu vực công một cách an toàn và có kiểm soát, thông qua một đạo luật khung hiện đại và cơ chế giám sát chuyên trách. Điểm nhấn trong chính sách dữ liệu của Australia là Đạo luật Khả dụng và Minh bạch Dữ liệu 2022 (*Data Availability and Transparency Act 2022*), cùng với việc thành lập Ủy viên Dữ liệu Quốc gia (*National Data Commissioner*) để điều phối việc chia sẻ dữ liệu công.

Đạo luật Đạo luật Khả dụng và Minh bạch Dữ liệu 2022 được Quốc hội Australia thông qua tháng 3/2022, tạo lập một cơ chế pháp lý mới cho việc chia sẻ dữ liệu khu vực công liên bang. Trong đó, các cơ quan Chính phủ Liên bang (*data custodians*) được phép cung cấp dữ liệu mà họ nắm giữ cho những người dùng dữ liệu được công nhận (*accredited users*) thuộc các cơ quan chính quyền khác và các trường đại học của Australia.

Điều kiện là việc chia sẻ phải nhằm các mục đích đã được luật cho phép và tuân thủ nghiêm ngặt các nguyên tắc chia sẻ an toàn trong luật. Đạo luật quy định rõ 03 mục đích hợp lệ để chia sẻ dữ liệu công: ⁽¹⁾cung cấp dịch vụ chính phủ; ⁽²⁾xây dựng chính sách và chương trình; ⁽³⁾nghiên cứu và phát triển. Mọi trường hợp chia sẻ phải được ghi trong thỏa thuận chia sẻ dữ liệu bằng văn bản giữa bên cung cấp và bên sử dụng; đồng thời không được phép chia sẻ dữ liệu được giữ bởi, hoặc có nguồn gốc từ, hoặc được nhận từ việc thực thi pháp luật hoặc an ninh quốc gia.



Việc chia sẻ dữ liệu của Australia tuân thủ nguyên tắc “Five-Safes” (5 yếu tố an toàn), đánh giá rủi ro và cho phép chia sẻ dữ liệu. Cụ thể, Đạo luật DAT yêu cầu việc chia sẻ phải nhất quán với các nguyên tắc chia sẻ dữ liệu (*data sharing principles*), vốn được phát triển dựa trên mô hình Five Safes quốc tế.



Hình ảnh: Mô hình Five Safes quốc tế. Nguồn ResearchGate

Năm yếu tố “an toàn” gồm:

- **Dự án an toàn (Project):** Mục đích sử dụng dữ liệu phải hợp lệ, vì lợi ích công hoặc nghiên cứu, được phê duyệt cụ thể.



- **Con người an toàn (People)**: Chỉ chia sẻ cho những cá nhân/tổ chức được công nhận có đủ năng lực và tin cậy (*accredited users*).
- **Môi trường an toàn (Setting)**: Dữ liệu phải được truy cập trong môi trường CNTT an toàn do chính phủ quy định (ví dụ qua dịch vụ trung gian hoặc nền tảng bảo mật).
- **Dữ liệu an toàn (Data)**: Chỉ những dữ liệu phù hợp, đã được xử lý ẩn danh hoặc bảo mật thích đáng mới được chia sẻ; không chia sẻ dữ liệu nhạy cảm nếu rủi ro cao.
- **Đầu ra an toàn (Outputs)**: Kết quả đầu ra từ việc sử dụng dữ liệu (*báo cáo, nghiên cứu*) phải được kiểm soát để không làm lộ thông tin cá nhân hay thông tin mật.

Những nguyên tắc này được quy định chi tiết trong Bộ quy tắc DAT 2022 và được Ủy viên Dữ liệu Quốc gia giám sát thực thi. Nhờ cách tiếp cận “5 Safes”, Australia đảm bảo rằng mỗi dự án chia sẻ dữ liệu đều được cân nhắc kỹ lưỡng về mục đích, đối tượng, nội dung và môi trường, giảm thiểu nguy cơ lọt hoặc lạm dụng dữ liệu.

Australia có cơ chế công nhận và giám sát chặt chẽ, để tham gia vào cơ chế chia sẻ, các bên phải qua quy trình công nhận (*accreditation*) nghiêm ngặt. Cơ quan cung cấp dữ liệu (*Data custodian*) đương nhiên là các cơ quan chính phủ liên bang, tự động thuộc phạm vi điều chỉnh. Còn người dùng dữ liệu hoặc đơn vị cung cấp dịch vụ dữ liệu (*Accredited users/Accredited data service providers*) phải nộp đơn xin chứng nhận với Ủy viên Dữ liệu Quốc gia và đáp ứng các tiêu chí về *năng lực quản lý dữ liệu an toàn*. Đáng chú ý, các thực thể nước ngoài, tư nhân hoặc cá nhân đều không đủ điều kiện trực tiếp tham gia, nghĩa là chỉ có cơ quan chính phủ Australia và đại học Australia mới được trở thành bên nhận dữ liệu. Đây là điểm khác biệt: Australia tạm thời chưa mở dữ liệu công cho khu vực tư nhân trong nước hay quốc tế.



Sau khi được chứng nhận, nếu vi phạm, Ủy viên Dữ liệu có quyền đình chỉ hoặc hủy chứng nhận. Ngoài ra, đạo luật quy định chế tài nghiêm khắc từ phạt tiền đến xử lý hình sự; đảm bảo tính răn đe và tuân thủ cao của các bên tham gia.

Đạo luật DAT 2022 cũng lập ra chức danh Ủy viên Dữ liệu Quốc gia với vai trò một cơ quan độc lập chịu trách nhiệm quản lý, giám sát việc thực thi cơ chế chia sẻ dữ liệu. Ủy viên có nhiệm vụ ban hành hướng dẫn, giáo dục các cơ quan về cách chia sẻ an toàn, đánh giá các đề xuất chia sẻ và giữ các bên có trách nhiệm giải trình. Đồng thời có Hội đồng Cố vấn Dữ liệu Quốc gia hỗ trợ về chính sách, đạo đức và cân bằng lợi ích. Có thể thấy Australia chú trọng việc xây dựng đầu mối chịu trách nhiệm để thúc đẩy văn hóa chia sẻ dữ liệu trong chính phủ nhưng vẫn đảm bảo tính minh bạch và an toàn.

Mô hình của Australia cũng cho thấy một hướng đi thực dụng, bắt đầu từ khu vực công, mở khóa giá trị từ dữ liệu chính phủ bằng cách chia sẻ cho nghiên cứu và cải tiến dịch vụ công, trên cơ sở kiểm soát chặt chẽ. Cách làm này vừa tạo ra những thắng lợi nhanh trong việc sử dụng dữ liệu (*vì dữ liệu công thường phong phú và ít vướng quyền riêng tư hơn dữ liệu tư nhân*), vừa xây dựng được niềm tin và năng lực trước khi mở rộng ra phạm vi rộng hơn. Australia là một trong các hình mẫu về “Chính phủ dữ liệu mở có kiểm soát”, cân bằng giữa minh bạch, chia sẻ và an ninh dữ liệu.

1.1.2.4. Nhật Bản

Nhật Bản có khung pháp luật dữ liệu được xây dựng khá toàn diện, gồm hai trụ cột chính: bảo vệ dữ liệu cá nhân và thúc đẩy sử dụng dữ liệu công, tư cho phát triển xã hội số. Hai văn bản tiêu biểu là Luật Bảo vệ Thông tin Cá nhân (APPI) và Luật Cơ bản về Thúc đẩy Sử dụng Dữ liệu khu vực công và tư. Cụ thể:

- **Luật Bảo vệ Thông tin Cá nhân (APPI):** Ban hành lần đầu năm 2003, APPI là đạo luật khung về bảo vệ dữ liệu cá nhân tại Nhật. Luật đã được sửa đổi nhiều lần, gần nhất là vào năm 2020 (*hiệu lực 2022*), nhằm nâng cao tiêu chuẩn bảo vệ tiệm cận GDPR. Một số nội dung chính của APPI:



+ *Đối tượng điều chỉnh rộng:* APPI áp dụng cho mọi tổ chức, cá nhân (bao gồm cả cơ quan nhà nước, doanh nghiệp, NPO) xử lý thông tin cá nhân trong hoạt động kinh doanh. Sau sửa đổi 2020, phạm vi này bao trùm cả khu vực công (*trước đây Nhật có luật riêng cho cơ quan nhà nước, nay đã hợp nhất vào APPI*).

+ *Quy định chi tiết về thu thập, sử dụng, cung cấp dữ liệu:* APPI yêu cầu minh bạch và mục đích cụ thể khi thu thập thông tin cá nhân; hạn chế sử dụng trong phạm vi mục đích đã thông báo (*trừ một số ngoại lệ theo luật định*); nếu thay đổi mục đích phải thông báo người dữ liệu. Việc cung cấp dữ liệu cá nhân cho bên thứ ba phải được sự đồng ý của đương sự, trừ các ngoại lệ rất hạn chế (*như phục vụ điều tra tội phạm, bảo vệ tính mạng, hoặc đã án danh*). Đối với thông tin nhạy cảm (*về chủng tộc, tín ngưỡng, sức khỏe, tiền án... tương tự “dữ liệu đặc biệt” theo GDPR*), APPI cấm thu thập nếu không có sự đồng ý rõ ràng và cấm chia sẻ cho bên thứ ba theo cơ chế opt-out (*phải luôn opt-in*).

+ *Quyền của cá nhân:* Luật trao cho cá nhân (*data subject*) các quyền quan trọng: quyền yêu cầu thông báo mục đích sử dụng dữ liệu, quyền truy cập (*được biết nội dung dữ liệu về mình mà doanh nghiệp nắm giữ*), quyền yêu cầu chỉnh sửa, bổ sung hoặc xóa dữ liệu nếu sai hoặc không cần thiết, quyền yêu cầu ngừng sử dụng hoặc xóa bỏ dữ liệu nếu vi phạm luật hoặc không còn cần thiết. Đáng lưu ý, nếu doanh nghiệp không đáp ứng yêu cầu chỉnh sửa trong vòng 02 tuần, cá nhân có thể khởi kiện dân sự để buộc thực hiện. Những quyền này đảm bảo cá nhân Nhật Bản có công cụ pháp lý để kiểm soát dữ liệu của mình.

+ *Nghĩa vụ của doanh nghiệp và cơ quan nhà nước:* Các tổ chức phải triển khai biện pháp bảo mật phù hợp để bảo vệ dữ liệu cá nhân (*từ biện pháp kỹ thuật đến đào tạo nhân viên*). APPI khuyến khích bổ nhiệm quản lý bảo vệ dữ liệu (*dù không bắt buộc với tất cả, nhưng được khuyến làm để tuân thủ nguyên tắc bảo mật*). Khi xảy ra sự cố rò rỉ dữ liệu, phải thông báo cho Ủy ban Bảo vệ Thông tin Cá nhân và người ảnh hưởng nếu rò rỉ nghiêm trọng (*trên 1.000 người, hoặc dữ liệu nhạy cảm, tài chính...*), quy định này mới được thêm năm 2020, giống yêu cầu 72 giờ của GDPR nhưng linh hoạt hơn. APPI cũng hạn chế chuyển dữ liệu cá



nhân ra nước ngoài: chỉ cho phép nếu nước nhận có mức bảo vệ tương đương hoặc có biện pháp bảo đảm hoặc đã được đương sự đồng ý sau khi biết rõ rủi ro.

+ *Ché tài và thực thi*: Sau sửa đổi, mức phạt vi phạm APPI đã tăng đáng kể lên mức tối đa 100 triệu Yên (*khoảng 18 tỷ VND*) với công ty. Ủy ban Bảo vệ Thông tin Cá nhân Nhật Bản là cơ quan giám sát độc lập, có quyền điều tra, ra lệnh hành chính và phối hợp quốc tế (*được thành lập năm 2005 và hiện nay có vai trò tương đương cơ quan bảo vệ dữ liệu ở các nước Liên minh Châu Âu*).

- **Luật Cơ bản về Thúc đẩy Sử dụng Dữ liệu Công - Tư (2016)**: Bên cạnh việc bảo vệ dữ liệu cá nhân, Nhật Bản cũng ban hành Đạo luật Cơ bản số 103/2016 nhằm thúc đẩy việc khai thác dữ liệu từ cả khu vực công và tư cho phát triển kinh tế, xã hội. Luật này đặt ra các nguyên tắc và trách nhiệm để xây dựng xã hội dữ liệu ở Nhật, có thể kể đến một số nội dung chính:

+ *Định hướng chiến lược*: Luật xác định cần sử dụng hiệu quả khối lượng lớn thông tin đa dạng trong xã hội (*đặc biệt qua Internet, IoT*) nhằm giải quyết các thách thức quốc gia (*nhiều già hóa dân số, năng suất lao động thấp*). Dữ liệu công và tư được coi là nguồn lực để tạo ra các dịch vụ mới, thúc đẩy tăng trưởng và nâng cao đời sống nhân dân. Luật yêu cầu chính phủ xây dựng “Kế hoạch cơ bản thúc đẩy sử dụng dữ liệu” toàn quốc, các tỉnh thành cũng xây kế hoạch địa phương phù hợp.

+ *Hài hòa giữa sử dụng dữ liệu và bảo vệ lợi ích công dân*: Luật đề ra các nguyên tắc cơ bản như: ⁽¹⁾đảm bảo luân chuyển thông tin thông suốt; ⁽²⁾đóng góp vào xã hội năng động (*qua tạo doanh nghiệp mới, nâng cao cạnh tranh*); ⁽³⁾nâng cao hiệu quả quản trị công dựa trên dữ liệu; ⁽⁴⁾đồng thời đảm bảo an toàn, bảo mật và không xâm hại quyền lợi người dân khi thúc đẩy sử dụng dữ liệu. Cụ thể, yêu cầu phải có nền tảng bảo vệ quyền và lợi ích công dân khi sử dụng dữ liệu, cũng như tiêu chuẩn kỹ thuật chung, tính tương thích hệ thống để các bên cùng khai thác hiệu quả.

+ *Hạ tầng và công nghệ*: Nhật Bản nhấn mạnh việc phát triển cơ sở hạ tầng thông tin phục vụ ICT, IoT, AI, điện toán đám mây... cũng như chuẩn hóa hệ



thống thông tin để chia sẻ dữ liệu dễ dàng giữa các bộ ngành và doanh nghiệp. Đồng thời, chú trọng đào tạo và thu hút nguồn nhân lực dữ liệu (*data scientists, kỹ sư AI*) để tận dụng được dữ liệu.

+ *Cơ chế phối hợp và thực thi:* Luật thành lập Hội nghị Chiến lược xúc tiến sử dụng dữ liệu công, tư do Thủ tướng làm chủ tịch, quy tụ bộ trưởng và chuyên gia, có nhiệm vụ đề xuất lĩnh vực ưu tiên, điều phối các bộ ngành thực hiện kế hoạch. Ngoài ra, luật khuyến khích tích hợp hạ tầng dữ liệu như sử dụng thẻ số cá nhân trong dịch vụ công, bắt buộc các thủ tục hành chính phải ưu tiên trực tuyến để tạo dữ liệu và tiện ích cho dân.

Với hai đạo luật trên, Nhật Bản thể hiện cách tiếp cận “hai mũi nhọn”, một mặt bảo vệ chặt chẽ quyền riêng tư cá nhân (*APPI*), mặt khác tích cực thúc đẩy chia sẻ dữ liệu liên thông trong chính phủ và với tư nhân để tạo giá trị kinh tế, xã hội (*Luật cơ bản 2016*). Nhật Bản cũng là nước khởi xướng ý tưởng “***Data Free Flow with Trust***” trên trường quốc tế, phù hợp với chính sách nội địa của họ là cân bằng giữa sử dụng dữ liệu và niềm tin của công chúng. Mô hình Nhật Bản cho thấy tầm quan trọng của khuôn khổ pháp lý đồng bộ: vừa có luật chuyên sâu về quyền riêng tư, vừa có luật tầm nhìn chiến lược về kinh tế dữ liệu.

1.1.2.5. Trung Quốc

Trung Quốc trong những năm gần đây đã xây dựng hệ thống pháp luật dữ liệu nghiêm ngặt và mang màu sắc “chủ quyền dữ liệu” rất rõ nét. Chính quyền Trung Quốc coi dữ liệu là tài sản quan trọng cần quản lý chặt để bảo vệ an ninh quốc gia và lợi ích công cộng, đồng thời muốn khai thác sức mạnh dữ liệu cho phát triển kinh tế. Hai đạo luật trụ cột là Luật An ninh Dữ liệu (*Data Security Law*) và Luật Bảo vệ Thông tin Cá nhân (*Personal Information Protection Law - PIPL*) đều ban hành năm 2021, với các nội dung chính:

- *Quản lý chặt và phân loại dữ liệu theo mức độ quan trọng:* Luật An ninh Dữ liệu của Trung Quốc có hiệu lực từ 9/2021, thiết lập khuôn khổ quản lý dữ liệu toàn diện trong lãnh thổ Trung Quốc. Luật An ninh Dữ liệu yêu cầu phân



loại dữ liệu thành các nhóm dựa trên tầm quan trọng đối với an ninh quốc gia, kinh tế và lợi ích công cộng. Cụ thể:

+ “*Dữ liệu lõi quốc gia*” (*National Core Data*): Là những dữ liệu liên quan an ninh quốc gia, kinh tế quốc dân, sinh kế dân chúng và lợi ích công cộng trọng yếu, được bảo vệ ở mức cao nhất. Đây có thể là dữ liệu về quốc phòng, tài nguyên quan trọng, kinh tế vĩ mô...

+ “*Dữ liệu quan trọng*” (*Important Data*): Là cấp tiếp theo, bao gồm dữ liệu mà nếu rò rỉ có thể ảnh hưởng trực tiếp tới an ninh quốc gia, kinh tế, trật tự xã hội, sức khỏe công cộng.... Luật chưa liệt kê cụ thể dữ liệu nào là “quan trọng”, giao Chính phủ định nghĩa qua các danh mục dữ liệu quan trọng theo ngành. Tuy nhiên, hướng dẫn năm 2019 gợi ý ví dụ: dữ liệu về năng lượng, giao thông, tài chính, y tế ở quy mô lớn có thể thuộc loại này.

+ “*Dữ liệu thông thường*”: Các dữ liệu khác không thuộc hai loại trên sẽ được quản lý lỏng hơn. Cách phân loại này cho thấy Trung Quốc muốn tập trung bảo vệ nghiêm ngặt dữ liệu nhạy cảm chiến lược, trong khi vẫn cho phép luân chuyển các dữ liệu ít nhạy cảm hơn để phát triển kinh tế.

- ***Nghĩa vụ bảo đảm an ninh dữ liệu toàn diện***: Luật An ninh Dữ liệu đặt ra hàng loạt yêu cầu về quản lý an ninh dữ liệu đối với mọi tổ chức, cá nhân xử lý dữ liệu tại Trung Quốc, bao gồm:

+ *Các tổ chức phải xây dựng chế độ quản lý an ninh dữ liệu nội bộ, định kỳ đào tạo nhân viên và chỉ định đơn vị/cá nhân phụ trách an ninh dữ liệu*. Phải thực hiện biện pháp kỹ thuật và tổ chức để bảo vệ dữ liệu khỏi truy cập trái phép, tấn công mạng, rò rỉ.

+ *Đánh giá rủi ro định kỳ*: Nếu xử lý dữ liệu quan trọng, tổ chức phải định kỳ đánh giá rủi ro an ninh dữ liệu và nộp báo cáo cho cơ quan quản lý. Báo cáo phải nêu loại dữ liệu quan trọng, khối lượng, cách xử lý và nguy cơ tiềm ẩn. Điều này tạo cơ chế giám sát thường xuyên từ phía nhà nước.

+ *Kiểm tra an ninh và ứng phó sự cố*: Doanh nghiệp phải giám sát lỗ hổng, rủi ro và có biện pháp xử lý, khắc phục kịp thời. Khi xảy ra sự cố an ninh dữ liệu,



phải thực hiện kế hoạch ứng phó khẩn cấp và thông báo cơ quan chức năng (*nếu nghiêm trọng*). Luật An ninh Dữ liệu cũng lồng ghép yêu cầu tuân thủ Chế độ bảo vệ an ninh mạng nhiều cấp đã có từ Luật An ninh mạng 2017 (ví dụ các hệ thống CNTT phải được phân loại cấp độ an ninh từ 1 đến 5 và áp dụng biện pháp bảo vệ tương ứng).

- Trách nhiệm của các nền tảng và trung gian giao dịch dữ liệu: Luật An ninh Dữ liệu không chỉ quản lý người thu thập dữ liệu mà còn các bên trung gian mua bán dữ liệu. Các tổ chức cung cấp dịch vụ giao dịch dữ liệu (*tương tự chợ dữ liệu, sàn dữ liệu*) phải yêu cầu bên cung cấp dữ liệu giải trình nguồn gốc dữ liệu, xác minh danh tính các bên giao dịch và lưu nhật ký giao dịch. Quy định này đặt nền móng cho việc xây dựng thị trường giao dịch dữ liệu hợp pháp, khuyến khích việc mua bán dữ liệu có kiểm soát, minh bạch, thay vì ngầm trao đổi chui. Trung Quốc thực tế đã mở các “sàn giao dịch dữ liệu” thử nghiệm tại Quảng Châu, Quý Châu... và Luật An ninh Dữ liệu hợp pháp hóa mô hình này.

- Hạn chế nghiêm ngặt chuyển dữ liệu ra nước ngoài: Đây là điểm đặc biệt quan trọng trong Luật An ninh Dữ liệu:

+ *Đối với hạ tầng thông tin quan trọng (Critical Information Infrastructure - CII)*: Các đơn vị vận hành CII (*ngành viễn thông, tài chính, năng lượng, hạ tầng...*) phải lưu trữ dữ liệu quan trọng trong lãnh thổ Trung Quốc. Muốn chuyển ra ngoài, phải có nhu cầu thực sự, qua đánh giá an ninh bởi Cục Quản lý Không gian mạng Trung Quốc (*Cyberspace Administration of China - CAC*) và được sự đồng ý của cá nhân nếu dữ liệu chứa thông tin cá nhân.

+ *Đối với các đơn vị không thuộc CII*: Nếu họ thu thập “dữ liệu quan trọng”, việc xuất ra nước ngoài sẽ tuân thủ quy định do CAC ban hành (*CAC đã ra Quy định về đánh giá an ninh chuyển dữ liệu ra nước ngoài năm 2022*). Nói chung, một khi dữ liệu bị xác định là “quan trọng”, doanh nghiệp phải nộp đơn đánh giá an ninh trước khi chuyển và chỉ được chuyển nếu được chấp thuận. Mọi trường hợp cung cấp dữ liệu cho cơ quan tư pháp hoặc thực thi pháp luật nước ngoài đều bị cấm nếu chưa được cơ quan Trung Quốc phê chuẩn. Điều khoản này rõ ràng



nhằm ngăn chặn yêu cầu từ tòa án hoặc chính phủ nước khác tiếp cận dữ liệu tại Trung Quốc.

+ *Ché tài nặng cho vi phạm xuất khẩu dữ liệu*: Nếu chuyển “dữ liệu lõi” ra ngoài trái phép, công ty có thể bị phạt tới 10 triệu Nhân dân tệ (*khoảng 36 tỷ VND*) thu hồi giấy phép hoặc đóng cửa. Vi phạm với dữ liệu quan trọng phạt tới 5 triệu Nhân dân tệ (*khoảng 18 tỷ VND*). Cá nhân quản lý trực tiếp có thể bị xử lý hình sự nếu nghiêm trọng. Những mức phạt này rất cao, tạo sức ép tuân thủ lớn.

- *Xây dựng thị trường và năng lực dữ liệu quốc gia*: Song song với kiểm soát, Trung Quốc cũng đề ra mục tiêu phát triển kinh tế dữ liệu nội địa. Chính phủ khuyến khích các doanh nghiệp khai thác “dữ liệu thông thường” để đổi mới dịch vụ và lập các khu thí điểm giao dịch dữ liệu. Luật An ninh Dữ liệu và các văn bản liên quan (*nhiều Chiến lược quốc gia về dữ liệu*) đề cập việc xây dựng hệ thống tiêu chuẩn dữ liệu, đào tạo nhân tài, đầu tư hạ tầng dữ liệu (*trung tâm dữ liệu, mạng 5G*) để tận dụng “mỏ dầu dữ liệu” trong nước. Trung Quốc đã có hàng chục sàn giao dịch dữ liệu cấp địa phương, dữ liệu được mua bán dưới dạng sản phẩm (*dưới sự giám sát của nhà nước*). Đây là nỗ lực nhằm hình thành thị trường giao dịch dữ liệu có trật tự, biến dữ liệu thành hàng hóa luân chuyển trong nền kinh tế, nhưng trong vòng kiểm soát chặt của chính phủ.

Tóm lại, trong bối cảnh phần lớn dữ liệu được lưu trữ tại Mỹ và Châu Âu, mô hình Trung Quốc mang tính đề cao tính an ninh, an toàn, dữ liệu được coi như yếu tố chủ quyền, phải quản lý tập trung, phân cấp độ. Trung Quốc điều chỉnh mức độ mở về dữ liệu xuyên biên giới để đảm bảo toàn quyền kiểm soát dữ liệu trong nước. Đồng thời, họ xây dựng thị trường dữ liệu nội địa và thúc đẩy các doanh nghiệp khai thác dữ liệu trong khuôn khổ cho phép. Cách tiếp cận này phù hợp với bối cảnh Trung Quốc muốn bảo vệ an ninh quốc gia và thúc đẩy các công ty nội địa trong cuộc đua dữ liệu toàn cầu.



1.1.2.6. Hàn Quốc và Singapore

Cuối cùng, hai mô hình từ châu Á là Hàn Quốc và Singapore cũng rất đáng chú ý, thể hiện nỗ lực cân bằng giữa quản lý dữ liệu cá nhân nghiêm ngặt và thúc đẩy đổi mới sáng tạo thông qua dữ liệu.

- *Hàn Quốc:*

Hàn Quốc có hệ thống pháp luật đầy đủ về dữ liệu cá nhân và dữ liệu công. Được biết đến với Luật Bảo vệ Thông tin Cá nhân (*PIPA*) ban hành 2011, một trong những luật bảo vệ dữ liệu cá nhân sớm và mạnh mẽ ở châu Á. *PIPA* áp dụng rộng, yêu cầu mọi tổ chức phải được sự đồng ý của chủ thể dữ liệu để xử lý thông tin cá nhân, với chế tài nghiêm (*phạt đến 3% doanh thu vi phạm*). Hàn Quốc còn có Đạo luật về Cung cấp và Sử dụng Dữ liệu Công (2013) quy định các cơ quan chính phủ phải mở dữ liệu công khai trừ trường hợp hạn chế, thiết lập cổng dữ liệu mở data.go.kr.

The screenshot shows the main homepage of data.go.kr. At the top, there's a search bar asking " 어떤 공공데이터를 찾으시나요? " (What public data are you looking for?). Below it are dropdown menus for filtering data by category (분류체계), service type (서비스유형), and location (회장자). The bottom navigation bar includes links for Thematic (테마별), Category (카테고리별), National Data Center (국가중점데이터별), and Provider Type (제공기관유형별). On the right side, a modal window titled "기업 공공데이터 문제해결 지원센터 개소" (Opening of the Business Public Data Problem Solving Center) is displayed. This window contains information about the center's purpose, its main tasks, and a process flow diagram showing steps from application submission to final report. It also features logos for the Ministry of Government Legislation and the National Information Agency.

Hình ảnh: Giao diện trang web data.go.kr của Hàn Quốc. Ảnh: Data.go.kr



+ *Thúc đẩy dữ liệu mở và dịch vụ công dữ liệu*: Chính phủ Hàn Quốc triển khai chương trình “Chính phủ 3.0” từ 2013 nhằm mạnh dữ liệu mở và chia sẻ giữa các cơ quan để cung cấp dịch vụ tốt hơn. Hàn Quốc xây Cổng dữ liệu mở quốc gia với hàng nghìn bộ dữ liệu được công bố, khuyến khích doanh nghiệp tái sử dụng để tạo ứng dụng. Ví dụ: dữ liệu giao thông, khí tượng, y tế được cung cấp miễn phí cho startup phát triển sản phẩm. Nhờ đó, hệ sinh thái khởi nghiệp dữ liệu ở Hàn phát triển năng động.

+ *Phát triển thị trường trung gian dữ liệu*: Nhận thấy tiềm năng từ dữ liệu lớn, năm 2020 Hàn Quốc sửa đổi 3 luật dữ liệu (*PIPA*, *Luật Mạng thông tin*, *Luật Tín dụng*) để tạo thuận lợi cho kinh tế dữ liệu. Bản sửa đổi giới thiệu khái niệm “dữ liệu được định danh (*pseudonymised data*)” cho phép các công ty sử dụng dữ liệu cá nhân đã khử danh tính mà không cần xin thêm đồng ý miễn là cho mục đích thống kê, nghiên cứu hoặc đổi mới kỹ thuật. Đồng thời, luật thiết lập cơ chế để kết hợp tập dữ liệu từ nhiều nguồn khác nhau thông qua các cơ quan chuyên môn (*specialised data combination agencies*). Những cơ quan trung gian này có phòng lab an toàn, nơi các doanh nghiệp gửi dữ liệu tới để kết hợp và phân tích mà không lộ danh tính người dùng. Đây chính là cách Hàn Quốc phát triển thị trường trung gian dữ liệu: cho phép chia sẻ và ghép nối dữ liệu liên ngành một cách an toàn để tạo ra giá trị mới (ví dụ *kết hợp dữ liệu viễn thông với dữ liệu tài chính để phát hiện gian lận*). Sau sửa đổi, Hàn Quốc cũng củng cố vai trò của Ủy ban Bảo vệ Thông tin Cá nhân (*PIPC*), nâng PIPC thành cơ quan độc lập giám sát tất cả vấn đề dữ liệu, tập trung quyền hạn trước đây phân tán ở nhiều bộ. Nhờ đó, Hàn Quốc có môi trường pháp lý linh hoạt, dữ liệu cá nhân được bảo vệ chặt, nhưng dữ liệu ẩn danh và gắn danh thì có thể tự do lưu chuyển hơn để phục vụ đổi mới sáng tạo.

Tóm lại, mô hình Hàn Quốc tương đồng Liên minh Châu Âu ở chỗ có luật bảo vệ dữ liệu cá nhân mạnh, nhưng cũng học hỏi Australia ở việc mở dữ liệu chính phủ và cho phép chia sẻ dữ liệu ẩn danh để phát triển kinh tế. Hàn Quốc



xây dựng thị trường dữ liệu sôi động với sự tham gia của cả khu vực công và tư, trên nền tảng pháp luật vững chắc và giám sát chặt.

- Singapore:

Singapore có chiến lược Smart Nation và khung pháp luật PDPA với mục tiêu trở thành “Quốc gia Thông minh” (*Smart Nation*), tận dụng dữ liệu và công nghệ để nâng cao chất lượng cuộc sống và năng lực chính phủ. Về pháp luật, Singapore ban hành Đạo luật Bảo vệ Dữ liệu Cá nhân (*PDPA*) năm 2012 (*hiệu lực 2014*), yêu cầu các công ty phải xin đồng ý khi thu thập, sử dụng dữ liệu cá nhân, bảo đảm an ninh dữ liệu và cho phép người dân rút lại sự đồng ý. PDPA do Ủy ban Bảo vệ Dữ liệu Cá nhân (*PDPC*) quản lý. Năm 2020, Singapore sửa PDPA, tăng mức phạt tối đa lên 10% doanh thu doanh nghiệp hoặc 1 triệu SGD (*khoảng 20 tỷ VNĐ, nếu cao hơn*) trong trường hợp vi phạm nghiêm trọng. Song song, Singapore triển khai các sáng kiến như Chứng nhận Tin cậy về Bảo vệ Dữ liệu (*Data Protection Trustmark*) để khuyến khích doanh nghiệp tuân thủ và được công nhận.

+ *Sandbox dữ liệu và chia sẻ dữ liệu giữa các cơ quan*: Để thúc đẩy đổi mới mà vẫn đảm bảo tuân thủ pháp luật, PDPC Singapore khởi xướng Regulatory Sandbox về chia sẻ dữ liệu. Sandbox này cho phép các công ty/thử nghiệm mô hình chia sẻ dữ liệu mới trong phạm vi giới hạn và dưới sự giám sát của PDPC, nhằm đánh giá tính khả thi trước khi điều chỉnh quy định. Ví dụ: năm 2022 Singapore ra mắt Sandbox công nghệ tăng cường quyền riêng tư (*PET Sandbox*) để doanh nghiệp thử nghiệm công nghệ bảo mật tiên tiến (*nhiều mã hóa đồng homomorphic, tính toán an toàn*) khi chia sẻ dữ liệu nhạy cảm. Kết quả sandbox giúp PDPC cập nhật hướng dẫn và doanh nghiệp sớm ứng dụng công nghệ mới mà không vi phạm luật.

+ *Hệ tầng dữ liệu quốc gia*: Singapore xây dựng Hệ tầng dữ liệu chính phủ rất mạnh, gồm:

National Government Data Centre (Trung tâm dữ liệu Chính phủ): tập trung lưu trữ và quản lý các dữ liệu do chính phủ thu thập. Bên trong có các “Data



Hubs” chuyên biệt như People Hub (*hồ dữ liệu công dân*), Business Hub (*dữ liệu doanh nghiệp*)..., tạo kho dữ liệu liên thông phục vụ dịch vụ công. Ví dụ: dịch vụ MyInfo cho phép người dân điền tự động thông tin cá nhân (*đã xác thực qua People Hub*) khi làm thủ tục hành chính hoặc mở tài khoản ngân hàng, nhờ kết nối API giữa các cơ quan. Điều này vừa tiện lợi cho dân, vừa giúp doanh nghiệp giảm chi phí xác minh. Hiện mỗi ngày có ~200.000 giao dịch sử dụng MyInfo.



Hình ảnh: Singapore tăng thêm 35% công suất của các trung tâm dữ liệu, nhằm duy trì vị thế của nền kinh tế số hàng đầu thế giới. Ảnh: Keppel

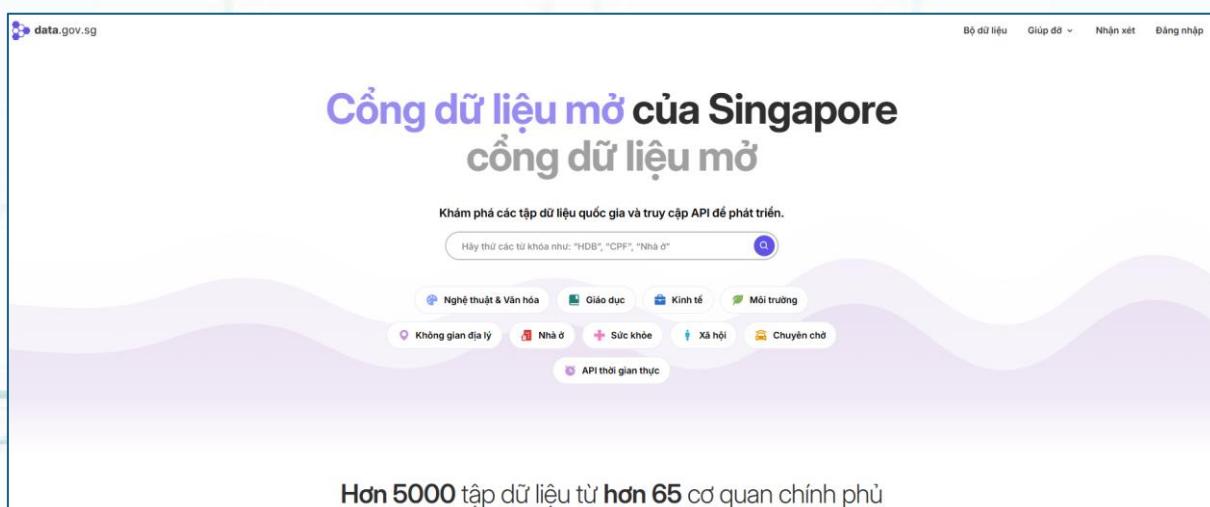
Nền tảng chia sẻ dữ liệu APEX (API Exchange): Đây là cổng API quốc gia do GovTech phát triển, cho phép các cơ quan chia sẻ dữ liệu qua API một cách an toàn, kiểm soát truy cập. APEX đóng vai trò “xương sống” kết nối các hệ thống, ví dụ hỗ trợ SingPass (*hệ thống định danh số quốc gia*) xác thực thông tin với các cơ sở dữ liệu khác. Đến 2021, APEX đã hỗ trợ hơn 2.000 API, với lưu lượng trên 100 triệu giao dịch API mỗi tháng. Singapore đang thí điểm mở APEX cho khu vực tư, cho thấy hướng đến chia sẻ dữ liệu công-tư có chọn lọc.

National Data Sandbox: Ngoài sandbox về quy định, Singapore còn thiết lập các sandbox kỹ thuật, môi trường điện toán nơi các cơ quan và doanh nghiệp có thể dùng dữ liệu giả lập hoặc ẩn danh để thử nghiệm giải pháp trước khi triển khai thực



té. Ví dụ: trong lĩnh vực giao thông, chính phủ cung cấp bộ dữ liệu giao thông ẩn danh để startup thử mô hình AI tối ưu lịch trình xe buýt. Những sandbox này là thành phần của sáng kiến Smart Nation, nhằm giảm rào cản khởi nghiệp về dữ liệu.

Nhờ những nỗ lực trên, Singapore duy trì được cân bằng giữa quản trị dữ liệu chặt chẽ và thúc đẩy sáng tạo. PDPA bảo vệ người dân khỏi lạm dụng dữ liệu, trong khi chính phủ lại chủ động mở dữ liệu (*qua data.gov.sg*) và tạo điều kiện sandbox để doanh nghiệp có không gian đổi mới. Singapore cũng tích cực tham gia các khuôn khổ quốc tế về luân chuyển dữ liệu (*nhiều hệ thống CBPR của APEC*) để hài hòa giữa phát triển kinh tế số và tuân thủ tiêu chuẩn bảo mật.



Hình ảnh: Giao diện trang web data.gov.sg của Singapore tập hợp hơn 5000 tập dữ liệu từ hơn 65 cơ quan chính phủ. Ánh: Data.gov.sg

Để tóm tắt và so sánh một cách trực quan các đặc điểm chính của các mô hình trên, bảng dưới đây tổng hợp một số tiêu chí nổi bật:

Quốc gia/Khu vực	Khung pháp luật dữ liệu chính	Đặc điểm nổi bật
Liên minh Châu Âu	GDPR (2016/2018); DGA (2022); Data Act (đang thảo)	- Bảo vệ dữ liệu cá nhân nghiêm ngặt, trao nhiều quyền cho cá nhân (GDPR). - Nhà nước tạo cơ chế chia sẻ dữ liệu an toàn: dịch vụ trung gian, data altruism, điểm truy cập một cửa.

BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU TRONG CÔNG AN NHÂN DÂN



		<ul style="list-style-type: none"> - Hạn chế chuyển dữ liệu ra ngoài Liên minh Châu Âu nếu nước nhận không đảm bảo tương đương (<i>chủ quyền dữ liệu</i>).
Mỹ	<p>Không có luật liên bang chung; luật theo ngành + Open Government Data Act (2018)</p>	<ul style="list-style-type: none"> - Cách tiếp cận phân tán, ít can thiệp: bảo vệ dữ liệu dựa trên luật chuyên ngành (<i>y tế, tài chính, trẻ em, tiêu dùng...</i>). - Chính phủ mở dữ liệu mặc định: các cơ quan liên bang phải công khai dữ liệu ở Data.gov; coi dữ liệu công là tài sản công cộng để thúc đẩy sáng tạo. - Ưu tiên khu vực tư: ít rào cản pháp lý cho doanh nghiệp khai thác dữ liệu (<i>ngoại trừ các quy định FTC về hành vi gian dối hoặc luật bang như CCPA</i>).
Australia	<p>Data Availability and Transparency Act (2022); Privacy Act (1988, sửa đổi)</p>	<ul style="list-style-type: none"> - Tập trung vào chia sẻ dữ liệu khu vực công an toàn: chỉ cho phép chia sẻ cho cơ quan nhà nước khác và đại học, phục vụ dịch vụ công, chính sách, R&D. - Áp dụng nguyên tắc Five Safes (<i>dự án, con người, môi trường, dữ liệu, đầu ra đều phải an toàn</i>) để quản lý rủi ro chia sẻ. - Lập Ủy viên Dữ liệu Quốc gia giám sát, có quyền chứng nhận/cấm các đơn vị tham gia. Chế tài nghiêm nếu lạm dụng dữ liệu chia sẻ.
Nhật Bản	<p>APPI (2003, sửa 2020); Basic Act on Public/Private Data Utilization (2016)</p>	<ul style="list-style-type: none"> - Bảo vệ dữ liệu cá nhân kỹ lưỡng (APPI): yêu cầu minh bạch, giới hạn mục đích; quyền truy cập, chỉnh sửa, xóa dữ liệu cho cá nhân; cấm chia sẻ thông tin nhạy cảm nếu không có đồng ý. - Thúc đẩy dùng dữ liệu cho xã hội số: Luật 2016 đề ra chiến lược dùng dữ liệu giải quyết vấn đề xã hội; phát triển ICT, AI, IoT; tiêu chuẩn hóa và chia sẻ dữ liệu công-tư. - Chính phủ Nhật cân bằng qua nguyên tắc “phát huy dữ liệu đi đôi với bảo vệ quyền và an ninh”. Khởi xướng khẩu hiệu DFIT quốc tế.



Trung Quốc	Data Security Law (2021); Personal Information Protection Law (2021)	<ul style="list-style-type: none"> - Quản lý tập trung, phân cấp dữ liệu: phân loại dữ liệu lõi, quan trọng, thường; bảo vệ nghiêm ngặt dữ liệu lõi và quan trọng (<i>yêu cầu đánh giá an ninh, lưu trữ nội địa</i>). - Hạn chế tối đa xuất khẩu dữ liệu: cấm cung cấp cho cơ quan nước ngoài nếu chưa duyệt; đánh giá an ninh bắt buộc trước khi chuyển dữ liệu quan trọng ra ngoài. - Phát triển thị trường dữ liệu nội địa: quy định trách nhiệm nền tảng giao dịch dữ liệu, khuyến khích giao dịch dữ liệu dưới sự giám sát; thúc đẩy kinh tế dữ liệu trong nước nhưng屏障lửa với bên ngoài.
Hàn Quốc	Personal Information Protection Act - PIPA (2011, sửa 2020); Open Data Law (2013)	<ul style="list-style-type: none"> - Luật PIPA chặt chẽ: yêu cầu đồng ý cá nhân cho mọi xử lý; phân biệt dữ liệu cá nhân, dữ liệu ẩn danh và định danh (2020) dữ liệu định danh được dùng không cần xin phép lại cho mục đích nghiên cứu, thống kê. - Mở dữ liệu chính phủ mạnh mẽ: hàng chục ngàn bộ dữ liệu trên data.go.kr; chính phủ điện tử 3.0 tận dụng dữ liệu để minh bạch và tiện ích cho dân. - Thị trường trung gian dữ liệu: cho phép tổ chức chuyên trách kết hợp dữ liệu từ nhiều nguồn một cách an toàn (<i>mô hình data sandbox tương tự</i>). PIPC tập trung quyền hạn quản lý dữ liệu, đảm bảo thực thi nhất quán.
Singapore	Personal Data Protection Act - PDPA (2012, sửa 2020)	<ul style="list-style-type: none"> - Khung PDPA cân bằng: bảo vệ thông tin cá nhân (<i>quy định xin consent, giới hạn mục đích, báo vi phạm</i>); phạt nặng nếu vi phạm (<i>tăng 10% doanh thu</i>). - Smart Nation - dữ liệu cho đổi mới: chính phủ xây nền tảng SingPass/MyInfo tích hợp dữ liệu công dân, chia sẻ cho dịch vụ công lẫn nhau (<i>với sự đồng ý</i>); công API APEC cho phép các cơ quan trao đổi dữ liệu real-time. - Sandbox và hợp tác quốc tế: PDPC mở regulatory sandbox cho các dự án chia sẻ dữ liệu mới; Singapore tham gia APEC CBPR, G7 DFFT... để vừa thúc đẩy luân chuyển dữ liệu vừa đảm bảo tiêu chuẩn bảo vệ.



1.1.3. Kết luận

Chính sách pháp luật dữ liệu trên thế giới đang có những điểm chung như xem dữ liệu là tài nguyên chiến lược, cần luật hóa sớm và toàn diện; xu hướng cân bằng bảo vệ và khai thác để vừa bảo đảm quyền riêng tư, vừa thúc đẩy đổi mới sáng tạo và hiệu quả quản trị. Tuy vậy, cách tiếp cận cụ thể có khác biệt: Liên minh Châu Âu tiên phong bảo vệ quyền cá nhân và thiết lập các chuẩn mực chia sẻ có kiểm soát toàn khái quát, Mỹ đề cao mở dữ liệu chính phủ và vai trò thị trường tư nhân, Australia và Singapore chú trọng khung chia sẻ an toàn trong chính phủ, Nhật Bản và Hàn Quốc kết hợp luật bảo vệ mạnh với chiến lược quốc gia về dữ liệu, còn Trung Quốc ưu tiên chủ quyền và an ninh dữ liệu quốc gia. Những mô hình này cung cấp bài học đa dạng cho các nước khác (*trong đó có Việt Nam*) trong việc thiết kế chính sách pháp luật nhằm quản trị và khai thác hiệu quả “tài nguyên dữ liệu” trong kỷ nguyên số hiện nay.

1.2. Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam

1.2.1. Sự cần thiết

Trong kỷ nguyên số hiện nay và bối cảnh cách mạng công nghiệp 4.0, dữ liệu đã và đang trở thành một nguồn tài nguyên quý giá và được ví như “mỏ vàng”, “nhiên liệu” của nền kinh tế số và xã hội hiện đại. Khối lượng dữ liệu số tăng trưởng bùng nổ cùng với sự phát triển của Internet, các hệ thống thông tin và dịch vụ số. Ở Việt Nam, chuyển đổi số được xác định là động lực quan trọng để phát triển kinh tế - xã hội, với mục tiêu xây dựng chính phủ số, kinh tế số và xã hội số. Dữ liệu được coi là tài nguyên mới giúp tối ưu hóa quản trị nhà nước, nâng cao hiệu quả sản xuất, kinh doanh và chất lượng cuộc sống; đồng thời mở ra thị trường dữ liệu, thúc đẩy sáng tạo và cạnh tranh trong kỷ nguyên số.

Trên thực tế, Nhà nước ta coi dữ liệu là một tài sản quốc gia, có chính sách huy động mọi nguồn lực để làm giàu dữ liệu, coi dữ liệu là yếu tố đột phá cho phát triển. Dữ liệu giữ vai trò trung tâm trong quản trị hiện đại: các quyết sách của Chính phủ ngày càng dựa vào phân tích dữ liệu lớn; dịch vụ công trực tuyến sử



dụng dữ liệu để cá nhân hóa và nâng cao hiệu quả phục vụ người dân; doanh nghiệp dùng dữ liệu để tối ưu vận hành, thấu hiểu khách hàng và tạo ra mô hình kinh doanh mới. Việc chia sẻ và mở dữ liệu công khai còn giúp nâng cao tính minh bạch, hỗ trợ người dân tiếp cận thông tin và thực hiện quyền giám sát, qua đó bảo đảm quyền con người, quyền công dân.

Tuy nhiên, cùng với giá trị kinh tế - xã hội, dữ liệu cũng đặt ra thách thức lớn về bảo vệ quyền riêng tư và dữ liệu cá nhân. Nếu quản lý, khai thác dữ liệu không được kiểm soát tốt, quyền riêng tư, an ninh thông tin của cá nhân có thể bị xâm phạm. Do đó, cân bằng giữa thúc đẩy sử dụng dữ liệu và bảo vệ quyền con người là bài toán khó đối với mọi quốc gia.



Hình ảnh: Kết quả biểu quyết thông qua Luật Dữ liệu. Ánh: Báo Nhân dân

Trước năm 2024, hệ thống pháp luật Việt Nam liên quan đến dữ liệu còn phân tán ở nhiều văn bản (*Luật An toàn thông tin mạng 2015*, *Luật An ninh mạng 2018*, *Luật Giao dịch điện tử*, *Luật Công nghệ thông tin*, các nghị định về chia sẻ dữ liệu...). Các quy định này chưa đầy đủ và thiếu tính thống nhất về thu thập, số hóa, đảm bảo chất lượng, lưu trữ, chia sẻ và kết nối dữ liệu; chưa đề cập rõ đến nền tảng công nghệ cao trong xử lý dữ liệu, cơ chế tích hợp dữ liệu từ các cơ sở dữ liệu quốc gia, hay quy định về các sản phẩm, dịch vụ mới dựa trên dữ liệu như



sàn giao dịch dữ liệu, dịch vụ trung gian dữ liệu, phân tích dữ liệu. Sự thiếu vắng một đạo luật khung tổng thể đã tạo ra khoảng trống pháp lý, gây khó khăn cho phát triển thị trường dữ liệu và bảo vệ các bên liên quan. Thực tiễn còn xuất hiện hiện tượng “data silo” dữ liệu bị phân mảnh, không liên thông cản trở cung cấp dịch vụ công số và ra quyết định dựa trên dữ liệu.



Hình ảnh: Bộ TT&TT quán triệt việc thực hiện Nghị quyết 35/NQ-TW của Bộ Chính trị 2014. Ảnh: Báo Cao Bằng

Trên thế giới, nhiều quốc gia đã xây dựng chiến lược dữ liệu và luật về dữ liệu như bước đi chiến lược để phát triển bền vững. Ở Việt Nam, chủ trương của Đảng và Nhà nước nhấn mạnh tầm quan trọng của Công nghệ thông tin và dữ liệu từ sớm. Nghị quyết 36-NQ/TW năm 2014 của Bộ Chính trị (*khóa XI*) khẳng định Công nghệ thông tin là động lực phát triển kinh tế tri thức, cần “đi trước một bước”. Chính phủ cũng đã ban hành Chương trình Chuyển đổi số quốc gia đến 2025, tầm nhìn 2030 (*Quyết định 749/QĐ-TTg* của Thủ tướng Chính phủ năm 2020), trong đó dữ liệu là một trụ cột quan trọng; xây dựng nhiều cơ sở dữ liệu



quốc gia trọng điểm (*dân cư, đất đai, bảo hiểm...*) nhưng việc kết nối, chia sẻ còn hạn chế do thiếu khung pháp lý thống nhất.

Nhận thức được nhu cầu cấp thiết này, tháng 2/2024, Chính phủ phê duyệt Chiến lược Dữ liệu quốc gia đến 2030 (*Quyết định 142/QĐ-TTg của Thủ tướng Chính phủ ngày 02/02/2024*), xác định rõ: xây dựng Luật Dữ liệu là bước đi nền tảng để hiện thực hóa mục tiêu chuyển đổi số. Cuối tháng 11/2024, Quốc hội thông qua Luật Dữ liệu 2024 (*Luật số 60/2024/QH15*) đạo luật chuyên ngành đầu tiên về dữ liệu số tại Việt Nam, có hiệu lực từ 01/7/2025. Luật này điều chỉnh toàn diện các vấn đề về dữ liệu số: xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; phát triển hạ tầng dữ liệu (*Trung tâm dữ liệu quốc gia, Cơ sở dữ liệu tổng hợp quốc gia*); quản lý sản phẩm, dịch vụ dữ liệu; quản lý nhà nước về dữ liệu; quy định quyền, nghĩa vụ, trách nhiệm của các chủ thể liên quan. Lần đầu tiên, pháp luật xác định rõ khái niệm và chế định pháp lý về chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu, đặt ra khung trách nhiệm cho mỗi bên trong vòng đời dữ liệu.

Song song, Việt Nam xây dựng Luật Bảo vệ Dữ liệu Cá nhân 2025, tập trung vào quyền của chủ thể dữ liệu cá nhân và trách nhiệm của bên xử lý dữ liệu cá nhân, bổ sung cho Luật Dữ liệu để bảo đảm tốt hơn quyền riêng tư. Như vậy, một hệ sinh thái pháp lý về dữ liệu đang hình thành, vừa bao quát quản trị dữ liệu chung, vừa chuyên sâu về dữ liệu cá nhân, phù hợp xu hướng quốc tế (*nhiều GDPR của Liên minh Châu Âu*).

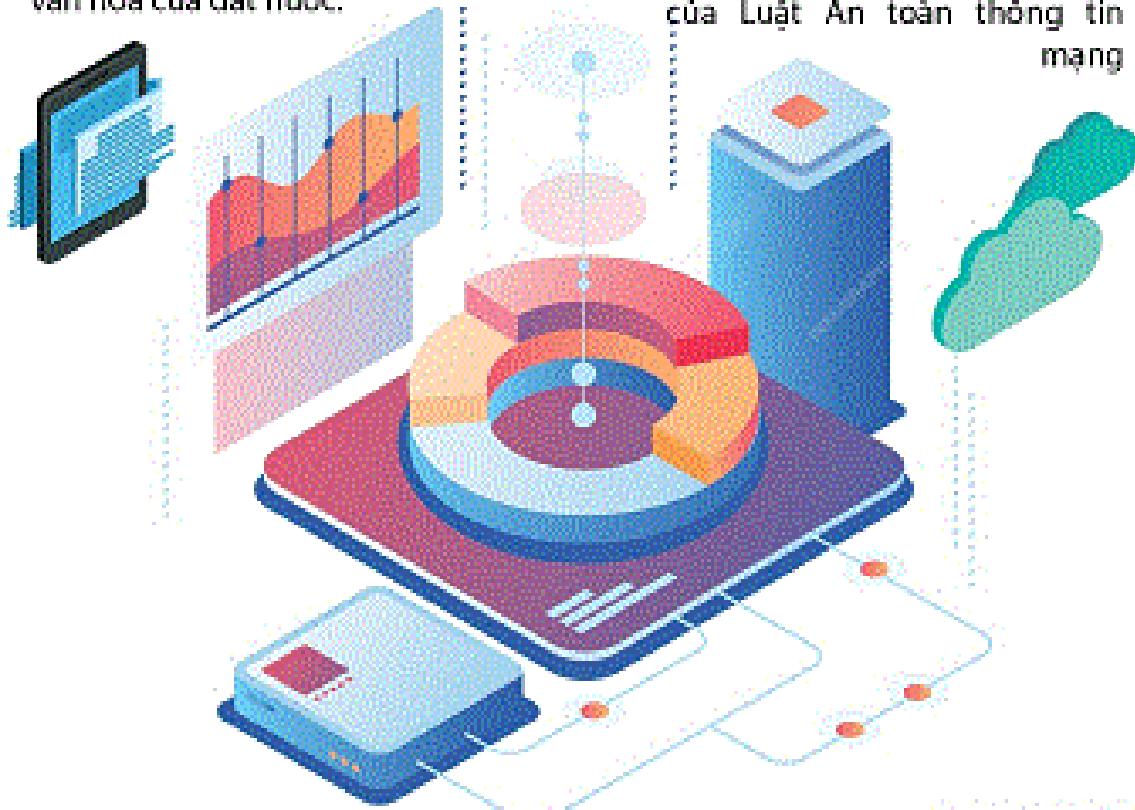


CHIẾN LƯỢC DỮ LIỆU QUỐC GIA ĐẾN NĂM 2030

PHÁT TRIỂN HẠ TẦNG DỮ LIỆU

(Quyết định số 142/QĐ-TTg ngày 2/2/2024 của Thủ tướng Chính phủ)

100% các Trung tâm dữ liệu quốc gia, Trung tâm dữ liệu vùng, khu vực, Trung tâm cấp quốc gia về lưu trữ dữ liệu lớn và tính toán hiệu năng cao trên cả nước được bảo đảm kết nối thành công, tạo thành một mạng lưới chia sẻ năng lực tính toán, xử lý dữ liệu lớn phục vụ cho phát triển kinh tế - xã hội, văn hóa của đất nước.



<http://infographic.vn>

© TTXVN
TTXVN

Hình ảnh: Infographic Chiến lược Dữ liệu quốc gia đến năm 2030.

Ảnh: TTXVN



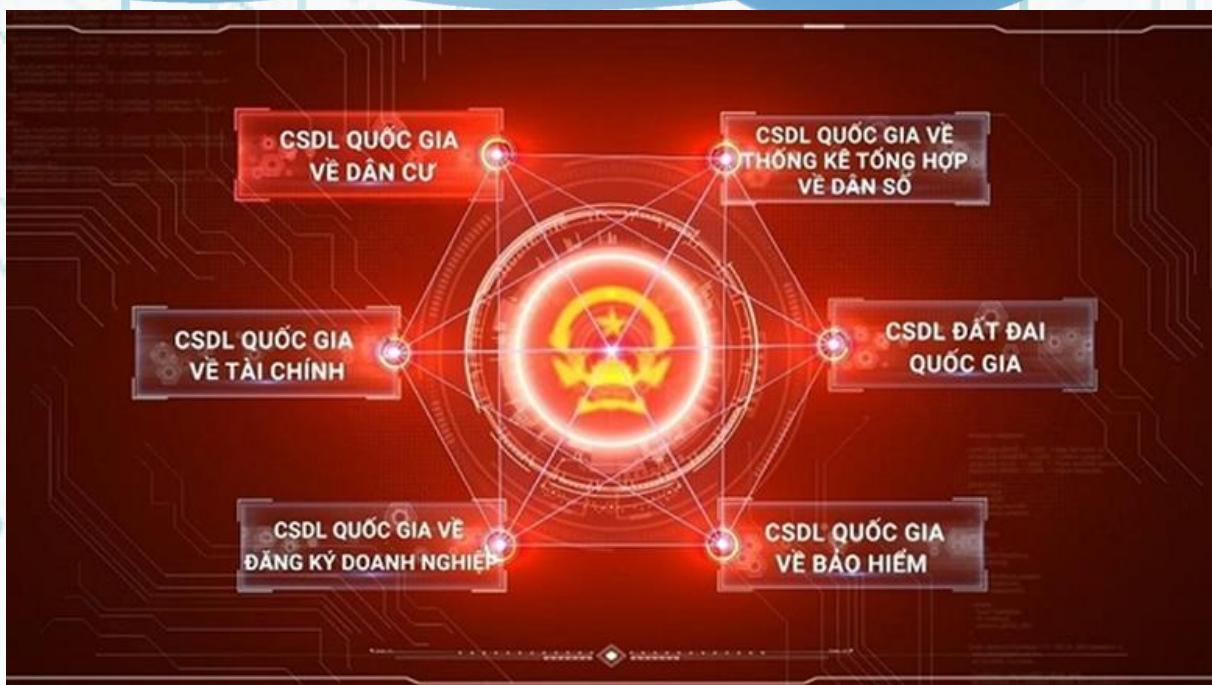
Để bảo đảm thực thi, Luật Dữ liệu 2024 và các văn bản dưới luật đã đưa ra các cơ chế: ⁽¹⁾đưa hoạt động liên quan đến dữ liệu quan trọng vào danh mục ngành nghề kinh doanh có điều kiện; ⁽²⁾yêu cầu doanh nghiệp đáp ứng tiêu chuẩn an ninh, ký quỹ tài chính; ⁽³⁾phân loại dữ liệu theo mức độ quan trọng; giao Bộ Công an giám sát hoạt động dữ liệu (*trữ dữ liệu quốc phòng*); ⁽⁴⁾quy định quyền khiếu nại, khởi kiện, yêu cầu bồi thường; và ⁽⁵⁾chế tài xử phạt nghiêm khắc với vi phạm.

Tóm lại, việc ban hành Luật Dữ liệu 2024 và Nghị định 165/2025/NĐ-CP hướng dẫn thi hành là yêu cầu bức thiết để giải quyết “điểm nghẽn” chia sẻ, kết nối dữ liệu; nâng cao bảo vệ dữ liệu quan trọng và dữ liệu cá nhân; hình thành thị trường dữ liệu; thúc đẩy đổi mới sáng tạo, khai thác “mỏ vàng dữ liệu” phục vụ phát triển kinh tế - xã hội, nâng cao năng lực cạnh tranh quốc gia và bảo đảm quyền con người trong môi trường số.

1.2.2. Quan điểm và nguyên tắc chỉ đạo về dữ liệu

Chiến lược Dữ liệu Quốc gia 2030 đã đề ra những quan điểm nền tảng cho chính sách dữ liệu của Việt Nam đến năm 2030. Cụ thể:

Thứ nhất, dữ liệu là tài nguyên cốt lõi cho chuyển đổi số: “Dữ liệu là nguồn tài nguyên mới, là yếu tố then chốt cho chuyển đổi số quốc gia, tạo ra giá trị mới thúc đẩy phát triển kinh tế - xã hội, nâng cao năng lực cạnh tranh quốc gia và phục vụ lợi ích người dân”. Quan điểm này nhấn mạnh dữ liệu tương tự như một loại tài sản, tài nguyên quý, cần được quản lý và khai thác hiệu quả. Thực tế, Luật Dữ liệu 2024 cũng khẳng định chính sách coi dữ liệu là tài sản: “Dữ liệu là tài nguyên, Nhà nước có chính sách huy động mọi nguồn lực để làm giàu dữ liệu, phát triển dữ liệu trở thành tài sản” (*Khoản 1, Điều 6 Luật Dữ liệu 2024*). Đồng thời, quyền của chủ thể dữ liệu đối với dữ liệu lần đầu tiên được luật định như một quyền tài sản theo pháp luật dân sự (*Khoản 15, Điều 3 Luật Dữ liệu 2024*).



Dữ liệu là nguồn tài nguyên mới, là yếu tố then chốt cho chuyển đổi số quốc gia, tạo ra giá trị mới thúc đẩy phát triển kinh tế - xã hội.

- **Thứ hai, nhà nước đóng vai trò dẫn dắt, thúc đẩy chia sẻ dữ liệu:** Chính phủ xác định sẽ tiên phong trong kết nối, chia sẻ dữ liệu, đồng thời huy động sự tham gia của toàn xã hội. Quan điểm chiến lược nêu rõ: Nhà nước lấy người dân, doanh nghiệp làm trung tâm; khuyến khích mọi thành phần tham gia thu thập, xây dựng, khai thác và “làm giàu dữ liệu”. Điều này phù hợp với yêu cầu chuyển đổi nhận thức từ tư duy “sở hữu dữ liệu” sang “chia sẻ dữ liệu dùng chung”. Dữ liệu do cơ quan nhà nước nắm giữ cần được mở rộng truy cập có kiểm soát để phục vụ lợi ích chung. Nguyên tắc công khai, minh bạch, bình đẳng trong tiếp cận dữ liệu được luật hóa tại Điều 5: “Bảo đảm công khai, minh bạch, bình đẳng trong tiếp cận, khai thác và sử dụng dữ liệu theo quy định của pháp luật” (Khoản 2, Điều 5 Luật Dữ liệu 2024). Đây là nguyên tắc quan trọng nhằm tránh độc quyền dữ liệu, tạo điều kiện cho mọi tổ chức, cá nhân có nhu cầu hợp pháp đều có thể tiếp cận nguồn dữ liệu mở hoặc dữ liệu được chia sẻ.

- **Thứ ba, đổi mới phương thức quản trị dựa trên dữ liệu:** Chiến lược quốc gia nhấn mạnh việc các cơ quan nhà nước phải chủ động chuyển đổi cách thức chỉ đạo, điều hành dựa trên dữ liệu, tương tác thời gian thực với người dân và doanh



nghiệp trên nền tảng số. Văn hóa ra quyết định dựa trên dữ liệu (*data-driven*) cần được thúc đẩy ở mọi cấp. Quan điểm này cũng bao hàm việc phát triển các hệ thống phân tích dữ liệu lớn, ứng dụng trí tuệ nhân tạo để hỗ trợ hoạch định chính sách chính xác và kịp thời.

- **Thứ tư, thúc đẩy thị trường dữ liệu và dữ liệu mở:** Một điểm nhấn trong quan điểm chỉ đạo là xác định phát triển thị trường dữ liệu là yếu tố đột phá. Nhà nước khuyến khích việc mở dữ liệu, tạo lập thị trường mua bán, trao đổi dữ liệu minh bạch. Thị trường dữ liệu sẽ là động lực để các tổ chức, doanh nghiệp tích cực thu thập, lưu trữ, xử lý và phân tích dữ liệu, qua đó thúc đẩy đổi mới sáng tạo và chuyển đổi số trong mọi ngành lĩnh vực. Cùng với đó, dữ liệu mở được xem như tài nguyên dùng chung phục vụ cộng đồng. Theo Luật Dữ liệu, cơ quan nhà nước có trách nhiệm công bố danh mục dữ liệu mở và tổ chức công khai dữ liệu đó để mọi tổ chức, cá nhân có thể khai thác, sử dụng. Đây là bước tiến quan trọng để tăng tính minh bạch của chính quyền và khuyến khích sáng tạo dựa trên dữ liệu mở (*open data*).

- **Thứ năm, an toàn, an ninh dữ liệu và bảo vệ quyền riêng tư:** Quan điểm xuyên suốt là phát triển đi đôi với bảo đảm an toàn, an ninh. Chiến lược quốc gia khẳng định việc khai thác, sử dụng dữ liệu phải đi kèm với bảo vệ dữ liệu cá nhân, an toàn thông tin mạng; đảm bảo quyền và lợi ích chính đáng của người dân, doanh nghiệp. Đây cũng là nguyên tắc nguyên tắc pháp lý quan trọng. Luật Dữ liệu 2024 yêu cầu thu thập, xử lý dữ liệu phải đảm bảo tính toàn vẹn, tin cậy, an ninh, an toàn (*Khoản 3, Điều 5 Luật Dữ liệu 2024*). Việc bảo vệ dữ liệu được đặt ngang hàng với phát triển dữ liệu: “*Bảo vệ dữ liệu được thực hiện đồng bộ, chặt chẽ với xây dựng, phát triển dữ liệu*” (*Khoản 4, Điều 5 Luật Dữ liệu 2024*). Nhà nước cũng nghiêm cấm các hành vi lợi dụng dữ liệu xâm phạm lợi ích quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân, hoặc tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu (*Điều 10 Luật Dữ liệu 2024*). Những nguyên tắc này đặt nền móng để vừa khai thác dữ liệu phục vụ phát triển, vừa bảo đảm chủ quyền số quốc gia và quyền riêng tư cá nhân.



- **Thứ sáu, đảm bảo chủ quyền dữ liệu quốc gia:** Trong bối cảnh dữ liệu xuyên biên giới luân chuyển, Chính phủ đề cao yêu cầu đảm bảo chủ quyền số quốc gia đối với dữ liệu. Quan điểm chiến lược nêu rõ: phải “đảm bảo tối đa lợi ích quốc gia - dân tộc” trong các vấn đề dữ liệu xuyên biên giới, phù hợp với luật pháp quốc tế; đồng thời bảo đảm dữ liệu của người Việt Nam, phát sinh tại Việt Nam chịu sự quản lý chủ quyền của Việt Nam. Tinh thần này được phản ánh trong Luật Dữ liệu qua quy định về hợp tác quốc tế và cung cấp dữ liệu ra nước ngoài. Mọi hợp tác, chuyển giao dữ liệu phải tôn trọng chủ quyền, tuân thủ pháp luật Việt Nam và các điều ước quốc tế (*Điều 7 Luật Dữ liệu 2024*). Đặc biệt, việc cơ quan nước ngoài yêu cầu cung cấp dữ liệu thuộc thẩm quyền của Việt Nam phải do cơ quan có thẩm quyền của Việt Nam xem xét, quyết định (*Khoản 3, Điều 7 Luật Dữ liệu 2024*) nhằm đảm bảo không một dữ liệu quan trọng nào ra nước ngoài trái phép, ảnh hưởng đến lợi ích quốc gia.



- **Thứ bảy, phát triển nguồn nhân lực dữ liệu:** Yếu tố con người được xem là quyết định sự thành công của chiến lược dữ liệu. Quan điểm chỉ đạo nhấn mạnh



việc ưu tiên phát triển đội ngũ chuyên gia, nhà khoa học về dữ liệu và xử lý dữ liệu số, làm chủ các công nghệ mới (*AI, big data, IoT...*). Luật Dữ liệu 2024 cũng có chính sách “*tập trung đào tạo, bồi dưỡng nâng cao năng lực... có cơ chế thu hút nhân lực trình độ cao để xây dựng và phát triển dữ liệu quốc gia*” (*Khoản 4, Điều 6 Luật Dữ liệu 2024*). Đây là cơ sở để các bộ, ngành đầu tư nhiều hơn cho đào tạo, tuyển dụng nhân sự chuyên trách về quản trị dữ liệu, bảo đảm có đủ năng lực thực thi các chính sách dữ liệu đề ra.

Như vậy, quan điểm và nguyên tắc của Việt Nam về dữ liệu thể hiện cái nhìn toàn diện, coi dữ liệu là tài sản chiến lược của quốc gia, vừa phải được khai thác tối ưu cho phát triển, vừa phải được bảo vệ chặt chẽ để đảm bảo chủ quyền và an ninh. Các nguyên tắc này được thể chế hóa cụ thể trong Luật Dữ liệu 2024, tạo thành kim chỉ nam cho việc xây dựng và thực thi các chính sách, pháp luật về dữ liệu trong giai đoạn tới.

1.2.3. Mục tiêu phát triển và quản trị dữ liệu quốc gia

Dựa trên những quan điểm nêu trên, Việt Nam đã đề ra các mục tiêu cụ thể về phát triển hạ tầng dữ liệu và kinh tế dữ liệu trong giai đoạn đến 2025 và 2030. Những mục tiêu này được thể hiện trong các chiến lược, chương trình quốc gia liên quan, tiêu biểu như Chiến lược Dữ liệu quốc gia 2030, Chiến lược phát triển Chính phủ số 2021-2025, định hướng 2030 và Chương trình Chuyển đổi số quốc gia.

- Thứ nhất, mục tiêu đến năm 2025:

Trước mắt, đến năm 2025, Việt Nam đặt mục tiêu cơ bản hình thành Chính phủ số và hạ tầng dữ liệu quốc gia đồng bộ. Theo Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số 2021-2025 (*Quyết định số 942/QĐ-TTg năm 2021*), đến 2025 Việt Nam phấn đấu nằm trong nhóm 70 nước dẫn đầu về Chính phủ điện tử (*EGDI*). Một số chỉ tiêu quan trọng bao gồm: 100% bộ, ngành, địa phương có nền tảng dữ liệu mở kết nối với Công dữ liệu quốc gia; hầu hết dịch vụ công thiết yếu được cung cấp trực tuyến ở mức độ cao, tối thiểu 80% hồ sơ thủ tục hành chính được xử lý hoàn toàn trên môi trường mạng. Mỗi người dân có danh tính số và hồ sơ số cơ bản (*y tế, giáo dục...*), các cơ sở dữ liệu quốc gia cốt



lõi (*nhiều dân cư, đất đai, doanh nghiệp, tài chính...*) được hoàn thành và kết nối chia sẻ giữa các cơ quan. Những mục tiêu này tạo tiền đề dữ liệu quan trọng cho giai đoạn tiếp theo.

Đặc biệt, Chiến lược Dữ liệu Quốc gia 2030 đặt mục tiêu đến 2025 phải xây dựng được hạ tầng dữ liệu mạnh mẽ, kết nối, chia sẻ an toàn phục vụ chuyển đổi số. Cụ thể, chiến lược hướng tới 100% các trung tâm dữ liệu (*của bộ, ngành, địa phương*) được kết nối đồng bộ, hình thành mạng lưới chia sẻ năng lực tính toán và lưu trữ dữ liệu lớn trên phạm vi toàn quốc. Đồng thời, hoàn thành cơ bản Chính phủ số với 100% cơ sở dữ liệu quốc gia được số hóa, kết nối, chia sẻ trên phạm vi toàn quốc. Tất cả các cơ sở dữ liệu quan trọng phải được bảo vệ theo mô hình nhiều lớp (*4 lớp*) và tuân thủ Luật An ninh mạng. Những mục tiêu này phản ánh quyết tâm xây dựng nền tảng dữ liệu vững chắc vào năm 2025, làm nền móng cho giai đoạn phát triển cao hơn.

- Mục tiêu đến năm 2030:

Tầm nhìn 2030, Việt Nam đặt ra những mục tiêu lớn nhằm vươn lên nhóm các quốc gia dẫn đầu trong khu vực về Chính phủ số, kinh tế số. Theo Nghị quyết 03/NQ-CP ngày 09/01/2025 của Chính phủ (*Chương trình hành động thực hiện Nghị quyết 57-NQ/TW về chuyển đổi số quốc gia*), phấn đấu đến năm 2030 Việt Nam thuộc top 3 ASEAN và top 50 thế giới về xếp hạng Chính phủ điện tử/Chính phủ số cũng như về năng lực cạnh tranh số. Mục tiêu này đồng bộ với định hướng đưa Việt Nam trở thành quốc gia số an toàn, thịnh vượng. Cụ thể, đến 2030, 100% dịch vụ công được cung cấp trực tuyến mức độ cao; 100% hoạt động quản lý nhà nước từ Trung ương đến địa phương vận hành trên môi trường số, kết nối xuyên suốt. Quy mô kinh tế số phấn đấu đạt khoảng 30% GDP vào năm 2030.

Về hạ tầng dữ liệu, Chiến lược Dữ liệu quốc gia 2030 đặt mục tiêu xây dựng một mạng lưới kết nối toàn diện các trung tâm dữ liệu trên cả nước, tạo thành nền tảng điện toán đám mây và phân tích dữ liệu lớn phục vụ mọi ngành, mọi cấp. Cơ sở Dữ liệu tổng hợp quốc gia sẽ đóng vai trò “trung tâm kết nối”, tích hợp dữ liệu từ các Cơ sở dữ liệu Quốc gia và chuyên ngành, phục vụ khai thác



liên thông. Chiến lược đề ra đích đến: dữ liệu sẽ cơ bản phản ánh đầy đủ mọi mặt của đời sống kinh tế - xã hội trên môi trường số, trở thành nhân tố thúc đẩy năng lực cạnh tranh quốc gia và đảm bảo quá trình chuyển đổi số thành công. Đồng thời, dữ liệu dân cư được xác định là dữ liệu lõi, gốc hình thành nên các dữ liệu chuyên ngành khác, phục vụ toàn dân. Việc hoàn thiện các bộ dữ liệu lớn trong các ngành (*nông nghiệp, công nghiệp, du lịch, giáo dục, y tế, lao động...*) cũng là mục tiêu để bảo đảm mọi quyết sách phát triển đều dựa trên dữ liệu tin cậy.



Hình ảnh: Trung tâm Dữ liệu lớn của Tập đoàn VNPT tại Hòa Lạc. Ảnh: VOV

Tóm lại, các mục tiêu đặt ra cho giai đoạn đến 2025 và 2030 hướng tới xây dựng hạ tầng dữ liệu quốc gia hiện đại, kết nối thông suốt và an toàn, đồng thời tận dụng dữ liệu để cải thiện dịch vụ công, nâng cao năng suất và năng lực cạnh tranh. Những mục tiêu này là cơ sở để triển khai các nhiệm vụ trong Luật Dữ liệu 2024 và các chính sách đi kèm, đảm bảo rằng đến năm 2030, Việt Nam có thể bước vào hàng ngũ các quốc gia mạnh về dữ liệu, sử dụng dữ liệu như một tài sản chiến lược để phát triển bền vững.

1.2.4. Chính sách pháp luật về dữ liệu trong Luật Dữ liệu 2024 và Nghị định 165/2025/NĐ-CP

Luật Dữ liệu 2024 là văn bản pháp luật đầu tiên ở Việt Nam quy định một cách tổng thể về dữ liệu số, từ khâu xây dựng, phát triển đến quản trị, khai thác



và bảo vệ dữ liệu. Để luật được triển khai hiệu quả, Chính phủ đã ban hành Nghị định 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu (có hiệu lực từ 01/7/2025).

Trong đó, chính sách pháp luật về dữ liệu được chia thành các nội dung: ⁽¹⁾phân loại dữ liệu và quyền sở hữu dữ liệu; ⁽²⁾xây dựng hạ tầng và Trung tâm dữ liệu quốc gia; quản trị, chia sẻ dữ liệu; ⁽³⁾bảo vệ và quản lý an toàn dữ liệu (*đặc biệt là dữ liệu quan trọng, dữ liệu cốt lõi*); ⁽⁴⁾cũng như vai trò, trách nhiệm của các chủ thể liên quan.

1.2.4.1 Phạm vi điều chỉnh và các khái niệm mới quan trọng

- **Phạm vi điều chỉnh:** Luật Dữ liệu 2024 điều chỉnh hầu hết các hoạt động liên quan đến dữ liệu số tại Việt Nam. Điều 1 của luật quy định luật bao gồm mọi vấn đề về “*dữ liệu số; xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu số; Trung tâm dữ liệu quốc gia; Cơ sở dữ liệu tổng hợp quốc gia; sản phẩm, dịch vụ về dữ liệu số; quản lý nhà nước về dữ liệu số; quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân liên quan*”. Như vậy, phạm vi rất rộng, bao quát cả dữ liệu khu vực công và khu vực tư, dữ liệu trong nước và dữ liệu xuyên biên giới liên quan đến Việt Nam. Luật áp dụng cho mọi cơ quan, tổ chức, cá nhân Việt Nam, cũng như tổ chức, cá nhân nước ngoài tại Việt Nam hoặc tham gia vào hoạt động dữ liệu số tại Việt Nam (Điều 2). Điều này đảm bảo bất kỳ ai xử lý dữ liệu trên lãnh thổ Việt Nam đều phải tuân thủ luật, tạo sân chơi pháp lý bình đẳng.

- **Khái niệm dữ liệu số và phân loại:** Luật đưa ra định nghĩa chính thức: “*Dữ liệu số là dữ liệu về sự vật, hiện tượng, sự kiện, bao gồm một hoặc kết hợp các dạng âm thanh, hình ảnh, chữ số, chữ viết, ký hiệu được thể hiện dưới dạng kỹ thuật số (gọi chung là dữ liệu)*” (Khoản 1, Điều 3). Một loạt khái niệm mới lần đầu xuất hiện trong pháp luật Việt Nam, phản ánh cách tiếp cận hiện đại về quản trị dữ liệu, gồm: dữ liệu dùng chung, dữ liệu dùng riêng, dữ liệu mở, dữ liệu gốc, dữ liệu quan trọng, dữ liệu cốt lõi, chủ thể dữ liệu, chủ quản dữ liệu, chủ sở hữu dữ liệu,... Chẳng hạn: “*Dữ liệu mở*” là dữ liệu mà mọi cơ quan, tổ chức, cá nhân có nhu cầu đều được tiếp cận, chia sẻ, khai thác, sử dụng; “*Dữ liệu quan trọng*”



là dữ liệu có thể tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng, thuộc danh mục do Thủ tướng ban hành; “*Dữ liệu cốt lõi*” là dữ liệu quan trọng trực tiếp tác động đến các lĩnh vực trọng yếu kể trên, thuộc danh mục do Thủ tướng ban hành. Việc phân biệt dữ liệu quan trọng (*important data*) và dữ liệu cốt lõi (*core data*) có ý nghĩa trong việc áp dụng các biện pháp quản lý, bảo vệ nghiêm ngặt hơn đối với nhóm dữ liệu cốt lõi. Tương tự, khái niệm chủ sở hữu dữ liệu và chủ quản dữ liệu được thiết lập để phân định ai có quyền quyết định đối với dữ liệu và ai được giao quản lý, vận hành dữ liệu theo yêu cầu của chủ sở hữu (*Khoản 13, 14, Điều 3*). Đặc biệt, luật khẳng định “*Quyền của chủ sở hữu dữ liệu đối với dữ liệu là quyền tài sản theo quy định của pháp luật về dân sự*”. Đây là điểm rất mới, lần đầu tiên ghi nhận dữ liệu có thể được xác lập quyền sở hữu và được coi như một loại tài sản.

- **Phân loại dữ liệu:** Trên cơ sở các khái niệm trên, Điều 13 Luật Dữ liệu quy định về phân loại dữ liệu. Các cơ quan nhà nước bắt buộc phải phân loại dữ liệu theo ít nhất hai tiêu chí chính: theo tính chất chia sẻ (*gồm dữ liệu dùng chung, dữ liệu dùng riêng, dữ liệu mở*) và theo mức độ quan trọng (*gồm dữ liệu cốt lõi, dữ liệu quan trọng, dữ liệu khác*). Chủ sở hữu, chủ quản dữ liệu ngoài khu vực nhà nước cũng phải phân loại dữ liệu theo mức độ quan trọng và có thể phân loại thêm theo các tiêu chí khác phù hợp nhu cầu quản trị. Việc phân loại này nhằm giúp áp dụng các chính sách quản lý, bảo vệ phù hợp với từng loại. Ví dụ: dữ liệu cốt lõi và quan trọng sẽ chịu các yêu cầu bảo mật cao hơn so với dữ liệu thông thường; dữ liệu mở thì phải được công khai sẵn sàng cho mọi người.

Luật giao Chính phủ quy định tiêu chí cụ thể để xác định dữ liệu nào thuộc loại cốt lõi, quan trọng (*Khoản 3, Điều 13*). Thực hiện nhiệm vụ này, Nghị định 165/2025/NĐ-CP đã dành các Điều 3 và 4 để đề ra tiêu chí phân định dữ liệu quan trọng và dữ liệu cốt lõi, cụ thể:

+ Dữ liệu quan trọng được xác định dựa trên mức độ có thể tác động nguy hiểm của dữ liệu nếu bị thu thập, sử dụng trái phép, đối với các lĩnh vực quốc phòng, an ninh, cơ yếu, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an



toàn cộng đồng (*không bao gồm bí mật nhà nước*). Nghị định liệt kê 4 nhóm tiêu chí, ví dụ: dữ liệu mà nếu lộ lọt có thể gây nguy hại đến an ninh quốc gia, chủ quyền, toàn vẹn lãnh thổ; gây nguy hại đến lợi ích quốc gia trong đối ngoại hoặc các dự án đầu tư nước ngoài; gây nguy hại đến vận hành kinh tế vĩ mô (*tổng cung cầu, thị trường tài chính, tỷ giá...*); hoặc đe dọa tính mạng, sức khỏe, tài sản của người dân trên diện rộng.

+ Dữ liệu cốt lõi là phần lõi quan trọng nhất trong dữ liệu quan trọng, được xác định dựa trên tác động trực tiếp, tức thời và nguy hiểm nếu bị xâm phạm trái phép. Tiêu chí dữ liệu cốt lõi cũng chia thành 04 nhóm tương tự, nhưng nhán mạnh mức độ trực tiếp gây nguy hại đến an ninh quốc gia, lợi ích quốc gia, kinh tế vĩ mô hoặc tính mạng, quyền lợi người dân. Nói cách khác, dữ liệu cốt lõi là tập con của dữ liệu quan trọng, có tính nhạy cảm cao nhất và đòi hỏi bảo vệ nghiêm ngặt nhất.

Để dễ hình dung sự khác biệt, có thể so sánh: dữ liệu quan trọng là dữ liệu có khả năng gây ảnh hưởng nghiêm trọng nếu lộ lọt, còn dữ liệu cốt lõi là dữ liệu mà chắc chắn, trực tiếp gây tổn hại nghiêm trọng nếu bị xâm phạm. Ví dụ: dữ liệu về an ninh quốc phòng nhìn chung là dữ liệu quan trọng; trong đó, các kế hoạch tác chiến cụ thể, thông tin tình báo tối mật sẽ là dữ liệu cốt lõi. Bảng dưới đây tóm tắt tiêu chí chính phân biệt hai loại dữ liệu này:

Dữ liệu quan trọng (Important Data)	Dữ liệu cốt lõi (Core Data)
Có thể gây tác động nguy hiểm đến an ninh quốc gia, lợi ích quốc gia, kinh tế vĩ mô, ổn định xã hội, sức khỏe cộng đồng... nếu bị thu thập, sử dụng trái phép.	Trực tiếp gây tác động nguy hiểm đến các lĩnh vực trên nếu bị thu thập, sử dụng trái phép (<i>mức độ ảnh hưởng nghiêm trọng hơn, tức thời hơn</i>).
Ví dụ: Dữ liệu về kinh tế vĩ mô, tài chính quốc gia, dữ liệu về hạ tầng năng lượng, dự án đầu tư chiến lược, dữ liệu cá nhân diện rộng... nếu lộ lọt có thể gây bất ổn kinh tế-xã hội hoặc phương hại đối ngoại.	Ví dụ: Dữ liệu tình báo quốc phòng tuyệt mật; dữ liệu định danh số toàn dân (<i>dân cư</i>) nền tảng của mọi giao dịch số; dữ liệu thời gian thực về điều hành kinh tế vĩ mô... nếu mất an toàn sẽ trực tiếp gây nguy hại lớn ngay lập tức.



Dữ liệu quan trọng (Important Data)	Dữ liệu cốt lõi (Core Data)
Yêu cầu quản lý, bảo vệ cao: cần đánh giá tác động, có biện pháp bảo vệ nhiều lớp, nhưng thủ tục xử lý linh hoạt hơn so với dữ liệu cốt lõi.	Yêu cầu quản lý, bảo vệ đặc biệt cao: chịu sự giám sát chặt của cơ quan an ninh (Bộ Công an/Bộ Quốc phòng); nhiều hoạt động (như chuyển ra nước ngoài) phải được thẩm định, chấp thuận trước.

Việc xác định chính xác danh mục dữ liệu nào là quan trọng, cốt lõi sẽ do Thủ tướng Chính phủ ban hành dựa trên tiêu chí nêu trên. Điều này đòi hỏi các bộ, ngành rà soát dữ liệu thuộc phạm vi quản lý để đề xuất. Danh mục này có thể bao gồm: dữ liệu dân cư (*có thể được coi là cốt lõi vì ảnh hưởng mọi lĩnh vực*), dữ liệu tài chính - ngân hàng quốc gia, dữ liệu về tài nguyên chiến lược, dữ liệu an ninh trật tự (*hồ sơ tội phạm, an ninh mạng,...*). Trong thực tiễn, việc phân loại đúng sẽ quyết định chế độ quản lý: dữ liệu cốt lõi và quan trọng sẽ được ưu tiên bảo vệ với ngân sách, nhân lực đặc biệt, đồng thời bị hạn chế trong chia sẻ, lưu trữ ở hạ tầng ngoài công lập.

1.2.4.2 Xây dựng hạ tầng dữ liệu: Trung tâm dữ liệu quốc gia và Cơ sở Dữ liệu tổng hợp quốc gia

Một trong những nội dung trọng tâm của Luật Dữ liệu 2024 là quy hoạch hạ tầng dữ liệu quốc gia, với hai cấu phần chính: Trung tâm dữ liệu quốc gia (TTDLQG) và Cơ sở Dữ liệu Tổng hợp Quốc gia (CSDLTQG). Đây được xem là nền tảng xương sống cho Chính phủ số và kinh tế số Việt Nam.

- Trung tâm dữ liệu quốc gia (National Data Center):** Luật Dữ liệu đã dành nguyên Mục 1, Chương III (*từ Điều 30 đến 32*) quy định về xây dựng, phát triển Trung tâm dữ liệu quốc gia. Theo luật, Trung tâm dữ liệu quốc gia sẽ là hạ tầng trọng điểm, đảm trách tích hợp, lưu trữ, quản trị và khai thác dữ liệu của các cơ quan nhà nước. Trung tâm dữ liệu quốc gia cũng cung cấp hạ tầng kỹ thuật và dịch vụ dữ liệu cho các cơ quan Đảng, Nhà nước khi có nhu cầu. Nhà nước ưu tiên đầu tư nguồn lực để xây dựng Trung tâm dữ liệu quốc gia: “Nhà nước ưu tiên đầu tư cơ sở hạ tầng, cơ sở vật chất, đất đai, trụ sở, công nghệ, bảo đảm ngân



sách cho xây dựng... và vận hành Trung tâm dữ liệu quốc gia” (Khoản 1, Điều 32). Hoạt động của Trung tâm sẽ được đảm bảo bằng ngân sách và các nguồn hợp pháp khác, đồng thời có cơ chế đai ngộ thu hút nhân lực chất lượng cao.



Hình ảnh: Lễ ra mắt Trung tâm dữ liệu quốc gia ngày 25/2/2025.

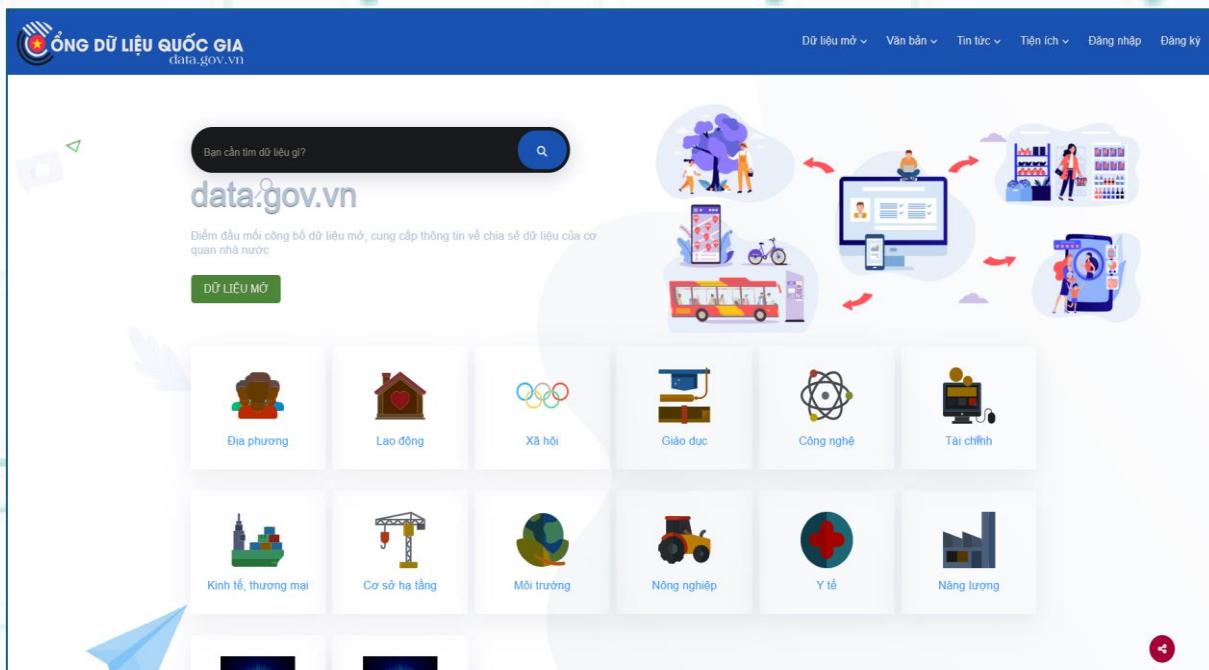
Ảnh: Bộ Công an

Luật quy định nguyên tắc cơ bản, còn chi tiết kỹ thuật giao cho Chính phủ hướng dẫn. Nghị định 165/2025/NĐ-CP tại Chương IV đã cụ thể hóa mô hình hạ tầng của Trung tâm dữ liệu quốc gia. Theo đó, Trung tâm dữ liệu quốc gia sẽ xây dựng, phát triển hạ tầng điện toán đám mây (*cloud*) và triển khai thành các vùng chức năng phục vụ nhu cầu của cơ quan nhà nước, bảo đảm khả năng phát triển các phân hệ tích hợp, đồng bộ, khai thác dữ liệu với yêu cầu bảo mật cao. Nói cách khác, Trung tâm dữ liệu quốc gia không chỉ là một trung tâm lưu trữ tập trung, mà là một hạ tầng đám mây liên vùng, linh hoạt phân bổ tài nguyên (*tính toán, lưu trữ*) cho các bộ ngành, địa phương theo nhu cầu.

Nghị định cũng nêu rõ Trung tâm dữ liệu quốc gia sẽ thiết lập hệ thống tính toán hiệu suất cao và hệ thống phân tích dữ liệu phục vụ công tác quản lý, với các mô hình phân tích dự báo khai thác từ Cơ sở dữ liệu tổng hợp Quốc gia. Điều này



phù hợp xu hướng tận dụng dữ liệu lớn (*big data*) cho phân tích chiến lược. Đặc biệt, Trung tâm dữ liệu quốc gia sẽ thiết lập Cổng dữ liệu quốc gia làm đầu mối để các cơ quan công bố thông tin về các loại dữ liệu mình quản lý; qua đó công bố dữ liệu mở, cung cấp dữ liệu mở nhằm tăng cường minh bạch của Chính phủ và thúc đẩy sáng tạo, phát triển kinh tế - xã hội. Hiện nay Việt Nam đã có Cổng dữ liệu quốc gia (*data.gov.vn*) nhưng hoạt động còn hạn chế; với vai trò của Trung tâm dữ liệu quốc gia, Cổng dữ liệu sẽ được nâng tầm thành “chợ dữ liệu” trung ương, nơi cả cơ quan nhà nước và tư nhân có thể cung cấp dữ liệu vì lợi ích chung.



Hình ảnh: Giao diện Cổng dữ liệu quốc gia *data.gov.vn*

Về vị trí tổ chức, Trung tâm dữ liệu quốc gia dự kiến đặt dưới sự quản lý của Bộ Công an (*theo chức năng đầu mối quản lý nhà nước về dữ liệu mà luật giao Bộ Công an, điểm b, Khoản 2, Điều 8*). Trên thực tế, Bộ Công an đã có sẵn hạ tầng Trung tâm dữ liệu dân cư quốc gia hiện đại (*quản lý Cơ sở dữ liệu Quốc gia về dân cư*). Trung tâm dữ liệu quốc gia về dân cư sẽ là trung tâm để kết nối thêm các trung tâm dữ liệu của các bộ ngành khác (*Tài chính, TNMT, GTVT, Y tế, Giáo dục...*). Những trung tâm vùng hoặc chuyên ngành có thể trở thành “node” trong mạng lưới Trung tâm dữ liệu quốc gia.



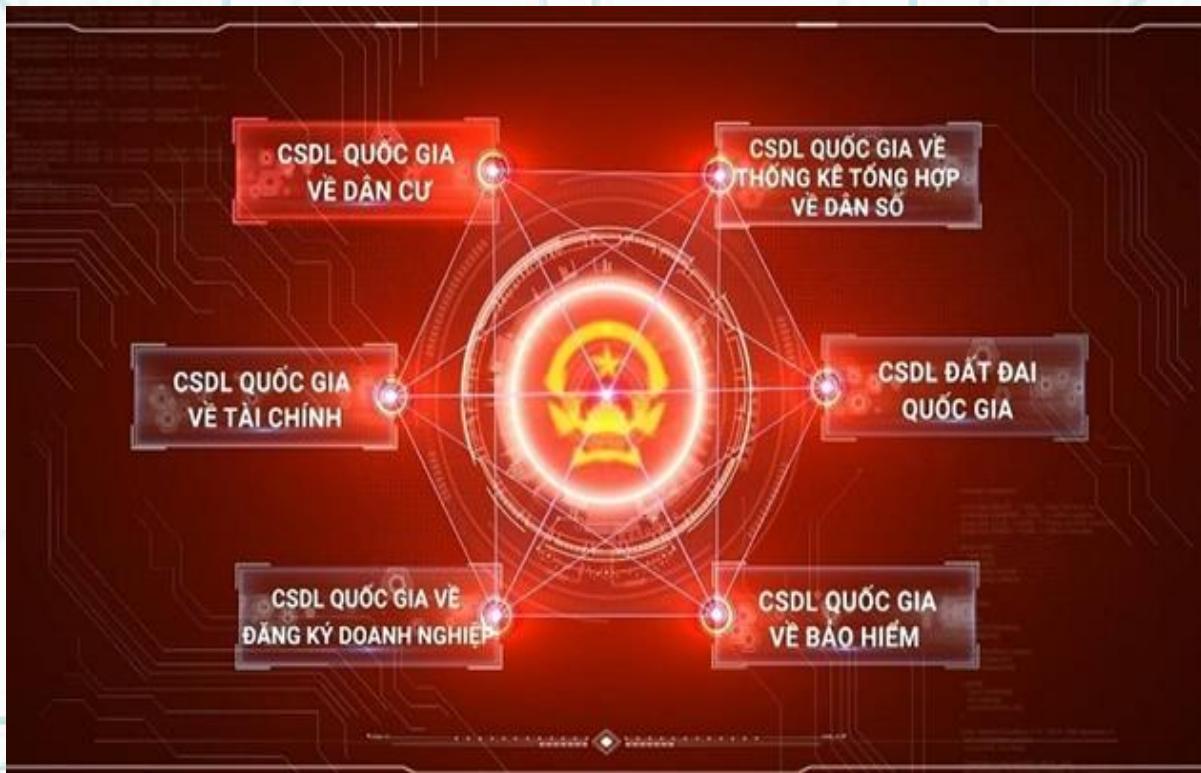
Hình ảnh: Trung tâm dữ liệu quốc gia về dân cư - Bộ Công an. Ảnh: Báo VNN

Cơ sở Dữ liệu Tổng hợp Quốc gia (Integrated National Database): Đây là khái niệm mới, lần đầu được luật hóa. Cơ sở dữ liệu tổng hợp QG được định nghĩa là cơ sở dữ liệu được tổng hợp từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và các cơ sở dữ liệu khác. Hiểu đơn giản, đó là một hệ thống tích hợp dữ liệu tập trung cấp quốc gia, đóng vai trò “kho dữ liệu chung” phục vụ khai thác trên quy mô toàn quốc. Mục 2, Chương III của Luật Dữ liệu 2024 (Điều 33-36) quy định về xây dựng, kết nối Cơ sở dữ liệu tổng hợp Quốc gia.

- Luật yêu cầu Cơ sở dữ liệu tổng hợp Quốc gia phải được xây dựng thống nhất tại Trung tâm dữ liệu quốc gia và đáp ứng các yêu cầu: ⁽¹⁾tuân thủ tiêu chuẩn kỹ thuật về dữ liệu; đảm bảo an ninh, an toàn thông tin, bảo vệ dữ liệu cá nhân; ⁽²⁾thuận lợi cho chia sẻ; và ⁽³⁾phải kiểm tra đối soát đảm bảo tính chính xác, thống nhất giữa dữ liệu trong các nguồn khác nhau. Nếu có sự không thống nhất giữa dữ liệu các bộ, ngành với dữ liệu trong Cơ sở dữ liệu tổng hợp, Trung tâm dữ liệu quốc gia sẽ phối hợp kiểm tra, đối chiếu và cập nhật đồng bộ. Điều này nhằm giải quyết tình trạng cùng một thông tin nhưng các cơ sở dữ liệu khác nhau lưu trữ



khác nhau (ví dụ: một công dân thay đổi địa chỉ nhưng Cơ sở dữ liệu dân cư, Cơ sở dữ liệu thuế, Cơ sở dữ liệu bảo hiểm xã hội có thể chưa đồng bộ). Cơ sở dữ liệu tổng hợp sẽ đóng vai trò “trọng tài”, đảm bảo dữ liệu được chuẩn hóa, thống nhất trên toàn quốc.



Hình ảnh minh họa Hệ thống thông tin cơ sở dữ liệu quốc gia được quản lý, xây dựng, duy trì tập trung. Ảnh: Báo Chính phủ

Luật cũng giao Thủ tướng quyết định lộ trình xây dựng, phát triển các Cơ sở dữ liệu Quốc gia, chuyên ngành và lộ trình thu thập, cập nhật dữ liệu vào Cơ sở dữ liệu tổng hợp. Điều này rất quan trọng, vì việc tích hợp dữ liệu đòi hỏi thời gian và kế hoạch chi tiết. Các bộ, ngành cần có thời gian hoàn thiện Cơ sở dữ liệu ngành mình, trước khi đồng bộ vào kho chung.

Một khi Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia hình thành, vấn đề kết nối, chia sẻ trở nên then chốt. Luật Dữ liệu quy định nguyên tắc: các Cơ sở dữ liệu Quốc gia, Cơ sở dữ liệu chuyên ngành, hệ thống thông tin khác phải kết nối, chia sẻ với Cơ sở dữ liệu tổng hợp Quốc gia thông qua nền tảng tích hợp, chia sẻ dữ liệu quốc gia và các hạ tầng kết nối dữ liệu cấp bộ, cấp tỉnh.



Thực tế, Việt Nam đã có Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (*NGSP* và *LGSP*). Luật Dữ liệu tiếp tục kế thừa và nâng cấp nền tảng này dưới sự phối hợp của Trung tâm dữ liệu quốc gia. Các phương thức khai thác, sử dụng dữ liệu cũng được luật liệt kê, bao gồm: kết nối chia sẻ trực tiếp qua hệ thống; thông qua cổng dữ liệu; thông qua API; thông qua thiết bị, phần mềm Trung tâm dữ liệu quốc gia cung cấp; hoặc phương thức khác. Chính phủ sẽ quy định chi tiết việc kết nối, chia sẻ (*Khoản 5, Điều 35*). Nghị định 165/2025/NĐ-CP dự kiến sẽ đồng bộ quy định này với các quy định trước đây (*nhiều Nghị định 47/2020/NĐ-CP về quản lý, kết nối, chia sẻ dữ liệu số của cơ quan nhà nước*). Mục tiêu cuối cùng là tạo nên một hệ sinh thái dữ liệu thông suốt: dữ liệu được lưu trữ tập trung hoặc phân tán nhưng liên thông với nhau, người dùng dữ liệu có thể truy xuất thông tin cần thiết mà không phải đi “gõ cửa” từng cơ quan như trước.



Hình ảnh minh họa hoạt nền tảng LGSP. Ảnh: VINA SA



Hình ảnh minh họa nền tảng LGSP và NGSP. Ảnh: Bytesoft

Từ góc độ thực tiễn, việc triển khai Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia là một bước ngoặt lớn. Ví dụ: khi hoàn thành, một cổng dữ liệu tập trung cho phép cán bộ Nhà nước (*hoặc người dân với dữ liệu mở*) truy vấn được nhiều loại thông tin khác nhau (*dân cư, doanh nghiệp, đất đai, tài chính, giáo dục, y tế...*) phục vụ giải quyết thủ tục hành chính hoặc nghiên cứu, thống kê... Điều này giảm tối đa việc cục bộ thông tin, giúp chia sẻ dữ liệu dùng chung thuận lợi. Một ví dụ thực tế: thay vì công dân phải nộp nhiều loại giấy tờ từ các nguồn khác nhau, cơ quan giải quyết thủ tục có thể tự khai thác dữ liệu được chia sẻ từ Cơ sở dữ liệu tổng hợp (*như tự tra cứu thông tin hộ tịch, bảo hiểm, thuế của công dân đó nếu đã có sổ định danh cá nhân*). Đó chính là tiền đề để thực hiện dịch vụ công “một cửa liên thông” thực sự.

Tuy nhiên, thách thức cũng rất lớn, việc di chuyển dữ liệu của các bộ ngành về lưu trữ tại Trung tâm dữ liệu quốc gia (*theo luật, “Cơ sở dữ liệu Quốc gia phải được lưu trữ trên hạ tầng của Trung tâm dữ liệu quốc gia”*) đòi hỏi đầu tư hạ tầng khổng lồ và sự đồng thuận của các bên. Hiện một số bộ có trung tâm dữ liệu



riêng và e ngại về an ninh khi đưa dữ liệu về một môi. Luật cũng cho phép “CSDL chuyên ngành và Cơ sở dữ liệu khác của cơ quan nhà nước được lưu trữ trên hạ tầng của Trung tâm dữ liệu quốc gia hoặc hạ tầng của cơ quan, tổ chức khác đáp ứng tiêu chuẩn”. Điều này nghĩa là chưa bắt buộc 100% mọi Cơ sở dữ liệu phải đặt vật lý tại Trung tâm dữ liệu quốc gia, miễn là hạ tầng bên ngoài đạt tiêu chuẩn (ví dụ một số bộ có *data center* hiện đại, đạt chuẩn thì có thể được tiếp tục sử dụng). Song về lâu dài, xu hướng tập trung hóa sẽ mạnh hơn để đảm bảo tính đồng bộ và tiết kiệm chi phí vận hành.

1.2.4.3 Quản trị, khai thác và chia sẻ dữ liệu; phát triển dữ liệu mở

Luật Dữ liệu 2024 đặt nền tảng cho một loạt chính sách nhằm khai thác tối đa giá trị dữ liệu, đồng thời tạo hành lang pháp lý cho việc chia sẻ dữ liệu một cách thông suốt giữa chính quyền, người dân, doanh nghiệp. Một số nội dung chính bao gồm:

- **Chính sách phát triển dữ liệu và dữ liệu mở:** Nhà nước khuyến khích mọi nguồn lực tham gia làm giàu dữ liệu và phát triển thị trường dữ liệu. Điều 6 Luật Dữ liệu đề ra các chính sách: ⁽¹⁾ưu tiên phát triển dữ liệu trong các lĩnh vực kinh tế-xã hội phục vụ chuyển đổi số; ⁽²⁾đầu tư xây dựng các Cơ sở dữ liệu Quốc gia trọng điểm và Trung tâm dữ liệu quốc gia; ⁽³⁾khuyến khích tổ chức, cá nhân trong và ngoài nước đầu tư nghiên cứu công nghệ dữ liệu, xây dựng trung tâm lưu trữ, xử lý dữ liệu tại Việt Nam; và ⁽⁴⁾phát triển thị trường dữ liệu. Có thể thấy định hướng rất rõ: dữ liệu không chỉ để quản lý nhà nước mà còn để tạo ra giá trị kinh tế. Các doanh nghiệp công nghệ số được tạo điều kiện tham gia cung cấp dịch vụ dữ liệu, khai thác dữ liệu (*theo mô hình data services, data analytics*). Việc khuyến khích xây dựng trung tâm dữ liệu tại Việt Nam cũng phù hợp với mục tiêu thu hút đầu tư của các “đại gia” trung tâm dữ liệu thế giới vào Việt Nam, biến Việt Nam thành một hub dữ liệu khu vực trong tương lai.

- **Về dữ liệu mở (open data):** Luật quy định nguyên tắc công khai dữ liệu (Điều 21 Luật Dữ liệu 2024) và nghĩa vụ của cơ quan nhà nước trong việc công bố danh mục dữ liệu mở, tổ chức công khai dữ liệu mở để mọi tổ chức, cá nhân



có thể khai thác, sử dụng. Đây là bước tiến lớn, đưa yêu cầu mở dữ liệu thành luật (*trước đây mới quy định trong một số nghị định, thông tư*). Mỗi cơ quan sẽ phải xác định dữ liệu nào có thể mở và công bố rộng rãi (*trừ các dữ liệu không được phép công khai theo Luật Tiếp cận thông tin hoặc luật chuyên ngành*). Thời điểm công khai dữ liệu từng lĩnh vực sẽ theo quy định pháp luật chuyên ngành. Song về nguyên tắc, dữ liệu thuần túy phục vụ lợi ích công cộng nên được mở tối đa. Ví dụ: dữ liệu thống kê kinh tế, dữ liệu thời tiết khí tượng, dữ liệu bản đồ nền,... khi được mở, sẽ tạo điều kiện cho doanh nghiệp, người dân sáng tạo dịch vụ mới (*ứng dụng thời tiết, bản đồ, phân tích thị trường...*). Luật cũng nhấn mạnh việc công khai dữ liệu phải đảm bảo “*phản ánh đúng dữ liệu từ nguồn gốc, thuận lợi cho khai thác*”, nghĩa là dữ liệu mở phải có chất lượng, đáng tin cậy.

Nghị định 165/2025/NĐ-CP dự kiến sẽ hướng dẫn cụ thể quy trình công bố dữ liệu mở, định dạng, tiêu chuẩn kỹ thuật cho dữ liệu mở (*theo hướng thống nhất với các tiêu chuẩn open data quốc tế như JSON, CSV, API mở...*). Công dữ liệu quốc gia sẽ đóng vai trò là nơi tập trung các dữ liệu mở được công bố từ các bộ ngành. Thực tế thời gian qua, các bộ như Bộ Tài chính, Bộ KH&CN, Bộ NN&MT đã bước đầu mở một số dữ liệu qua Công dữ liệu quốc gia, nhưng số lượng còn ít. Khi luật có hiệu lực, hy vọng sẽ có chuyển biến mạnh: dữ liệu mở sẽ trở thành “mặc định” đối với những dữ liệu không mật và không nhạy cảm.

- Quản trị và quản lý dữ liệu: Luật lần đầu tiên định nghĩa rõ hai khái niệm này (*Điều 15 Luật Dữ liệu 2024*). Quản trị dữ liệu bao gồm việc xây dựng chính sách, quy trình, tiêu chuẩn về dữ liệu của chủ sở hữu/chủ quản để quản lý dữ liệu một cách liên tục, hiệu quả, bảo đảm đầy đủ, chính xác, toàn vẹn, nhất quán, an toàn. Còn quản lý dữ liệu là tổ chức thực hiện các nội dung quản trị dữ liệu đó. Điều này có nghĩa là các tổ chức phải thiết lập chức năng quản trị dữ liệu (*data governance*) bài bản, từ khâu đặt ra quy định nội bộ về dữ liệu, đến vận hành chúng. Với cơ quan nhà nước, luật yêu cầu phải phối hợp với Trung tâm dữ liệu quốc gia trong quản trị, quản lý dữ liệu. Với tổ chức cá nhân bên ngoài, họ tự quản trị dữ liệu của mình, nhưng nếu dữ liệu thuộc diện cốt lõi/quan trọng thì phải tuân



thủ các quy định bảo vệ đặc thù (*Khoản 2, Điều 14 dẫn chiếu Khoản 3, Điều 27 Luật Dữ liệu 2024*).

- Kết nối, chia sẻ, điều phối dữ liệu: Đây là nội dung rất quan trọng để phá vỡ các “silo” dữ liệu giữa các cơ quan. Luật quy định (*Điều 17 Luật Dữ liệu 2024*) chủ sở hữu, chủ quản dữ liệu có trách nhiệm kết nối, chia sẻ dữ liệu cho người dùng dữ liệu được phép, có thể trực tiếp hoặc thông qua bên trung gian. Với dữ liệu của cơ quan nhà nước, luật yêu cầu các cơ quan thực hiện điều phối dữ liệu thuộc phạm vi mình quản lý, bảo đảm dữ liệu được chia sẻ an toàn, đồng bộ, hiệu quả phục vụ phát triển kinh tế-xã hội, quốc phòng an ninh. Đặc biệt, luật trao quyền cho Thủ tướng Chính phủ quyết định việc chia sẻ dữ liệu dùng riêng (*tức dữ liệu nội bộ của một cơ quan*) trong trường hợp đột xuất, cấp bách như phòng chống thiên tai, dịch bệnh, hoặc trường hợp cần thiết khác để giải quyết vấn đề phát sinh. Quy định này nhằm xử lý những tình huống mà một bộ ngành có dữ liệu nhưng không muốn chia sẻ, trong khi dữ liệu đó lại cần thiết để ứng phó sự cố quốc gia, Thủ tướng có thể ra quyết định bắt buộc chia sẻ.

Luật cũng giao Chính phủ quy định việc hỗ trợ chủ sở hữu dữ liệu (*ngoài nhà nước*) khi họ kết nối, chia sẻ dữ liệu cho cơ quan nhà nước. Thực hiện điều này, tại Điều 7 Nghị định 165/2025/NĐ-CP quy định cụ thể: các cơ quan nhà nước phải có các biện pháp hỗ trợ tổ chức, cá nhân chia sẻ dữ liệu cho Nhà nước, như “*xây dựng hệ thống bảo đảm kết nối, chia sẻ; cung cấp công cụ, hạ tầng kỹ thuật, an ninh an toàn; xây dựng quy trình, phần mềm để chủ sở hữu dữ liệu thực hiện các quyền của mình đối với dữ liệu đã cung cấp*”. Ngoài ra, người đứng đầu bộ, ngành, địa phương có thể quyết định hỗ trợ các nội dung cụ thể như hỗ trợ đường truyền, công cụ kết nối, hạ tầng bảo mật.... Quy định này rất nhân văn: nhiều doanh nghiệp sẵn sàng chia sẻ dữ liệu của họ (ví dụ dữ liệu từ nền tảng gọi xe, dữ liệu từ mạng xã hội,...) để giúp Chính phủ quản lý tốt hơn, nhưng họ ngại về chi phí và rủi ro. Nay Nhà nước sẵn sàng hỗ trợ về kỹ thuật, an ninh thì sẽ thúc đẩy sự hợp tác công-tư trong chia sẻ dữ liệu.



- Cung cấp dữ liệu cho cơ quan nhà nước: Điều 18 luật quy định: khuyến khích mọi tổ chức, cá nhân cung cấp dữ liệu thuộc quyền sở hữu cho cơ quan nhà nước (*điểm này phù hợp với xu hướng trên, doanh nghiệp chia sẻ dữ liệu với Chính phủ*). Đồng thời, bắt buộc tổ chức, cá nhân phải cung cấp dữ liệu cho cơ quan nhà nước có thẩm quyền mà không cần sự đồng ý của chủ thể dữ liệu trong một số trường hợp vì lợi ích công như: ứng phó tình trạng khẩn cấp, ngăn ngừa nguy cơ đe dọa an ninh quốc gia, thảm họa. Quy định này về bản chất là ngoại lệ của nguyên tắc bảo vệ dữ liệu cá nhân (*thông thường, cung cấp dữ liệu cá nhân phải có sự đồng ý của chính cá nhân đó theo Luật bảo vệ dữ liệu cá nhân 2025, trừ trường hợp luật khác cho phép*). Tình huống như dịch bệnh, thiên tai... đòi hỏi cơ quan chức năng có thể thu thập dữ liệu (*ví dụ: thông tin vị trí điện thoại người dân trong vùng dịch*) mà không kịp xin phép từng cá nhân thì được luật cho phép làm điều đó trên cơ sở vì lợi ích cộng đồng.

- Xác thực và xác nhận dữ liệu: Một điểm mới khác là luật đề cập đến xác nhận, xác thực dữ liệu (Điều 20 Luật Dữ liệu 2024). Đây là quy trình đảm bảo tính tin cậy của dữ liệu khi luân chuyển trên không gian mạng, đặc biệt trong các giao dịch điện tử. Dữ liệu có thể được xác nhận bởi cơ quan có thẩm quyền hoặc bởi tổ chức cung cấp dịch vụ xác thực điện tử và dữ liệu đã được xác thực sẽ có giá trị tương đương dữ liệu gốc lưu trong các Cơ sở dữ liệu chính thức. Quy định này tạo cơ sở pháp lý cho các dịch vụ như chứng thực số (*digital notarization*), đóng dấu thời gian (*timestamp*) để chống chối bỏ giao dịch. Chính phủ sẽ có hướng dẫn chi tiết (*ví dụ: Nghị định có thể quy định về dịch vụ chứng thực tài liệu số, chữ ký số từ xa...*). Điều này hỗ trợ đắc lực cho việc số hóa và lưu thông dữ liệu điện tử có giá trị pháp lý, giảm phụ thuộc vào giấy tờ.

Tựu trung, các quy định trên cho thấy một tư duy cởi mở, thực dụng trong quản trị và khai thác dữ liệu, tạo mọi điều kiện để dữ liệu chảy tự do có kiểm soát, phá bỏ tình trạng cát cứ dữ liệu. Đồng thời, tôn trọng quyền của chủ sở hữu dữ liệu (*cá nhà nước lẫn tư nhân*) nhưng luôn đặt lợi ích quốc gia, cộng đồng lên cao để trong trường hợp cần thiết có thể huy động dữ liệu phục vụ mục tiêu chung.



1.2.4.4. Bảo vệ dữ liệu và quản lý rủi ro, đặc biệt đối với dữ liệu quan trọng, cốt lõi

Song song với việc thúc đẩy khai thác dữ liệu, Luật Dữ liệu 2024 và Nghị định 165/2025/NĐ-CP đặt trọng tâm vào bảo vệ dữ liệu. Điều này bao gồm ⁽¹⁾bảo đảm an toàn kỹ thuật, an ninh mạng cho dữ liệu; ⁽²⁾ngăn ngừa các rủi ro trong quá trình xử lý dữ liệu; và ⁽³⁾kiểm soát chặt chẽ việc chuyển dữ liệu ra nước ngoài. Có thể coi đây là “mặt trận” phòng thủ để bảo vệ tài sản dữ liệu quốc gia trước các nguy cơ mất mát, lạm dụng.

^{(1)Đảm bảo chất lượng và an toàn dữ liệu:}

Điều 12 Luật Dữ liệu 2024 quy định về bảo đảm chất lượng dữ liệu, yêu cầu dữ liệu phải chính xác, hợp lệ, đầy đủ, cập nhật kịp thời và thống nhất. Các cơ quan quản lý Cơ sở dữ liệu phải thường xuyên kiểm tra, giám sát, khắc phục sai sót, cập nhật dữ liệu đồng bộ. Điều này nhấn mạnh một thực tế: dữ liệu chỉ có giá trị nếu chất lượng tốt; dữ liệu sai lệch có thể dẫn đến quyết định sai. Do đó, văn hóa quản lý dữ liệu phải chuyển từ “nhập cho có” sang “nhập liệu sạch”, duy trì dữ liệu “sạch” liên tục.

Luật cũng cấm các hành vi như: ⁽¹⁾lợi dụng dữ liệu để xâm phạm lợi ích quốc gia, quyền hợp pháp của ai đó; ⁽²⁾cản trở trái phép quá trình xử lý dữ liệu; ⁽³⁾tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu; làm giả, sửa sai hoặc cố ý làm hỏng dữ liệu; ⁽⁴⁾mua bán dữ liệu trái phép; và ⁽⁵⁾các hành vi vi phạm khác (Điều 10 Luật Dữ liệu 2024). Đặc biệt, hành vi mua bán dữ liệu cá nhân dưới mọi hình thức đã được Quốc hội xác định là hành vi bị nghiêm cấm (*quy định tại Luật Bảo vệ dữ liệu cá nhân 2025*). Các quy định cấm này tạo cơ sở để xử phạt, truy cứu trách nhiệm những cá nhân, tổ chức vi phạm an toàn dữ liệu.

^{(2)Quản lý rủi ro trong xử lý dữ liệu:}

Điều 25 Luật Dữ liệu nhận diện các loại rủi ro phát sinh trong xử lý dữ liệu, gồm: rủi ro về quyền riêng tư, rủi ro an ninh mạng, rủi ro nhận dạng và quản lý truy cập và các rủi ro khác. Cơ quan nhà nước phải thiết lập cơ chế cảnh báo sớm về rủi ro và có biện pháp bảo vệ dữ liệu tương ứng. Các chủ quản dữ liệu ngoài nhà nước cũng phải tự đánh giá, xác định rủi ro và thực hiện biện pháp bảo vệ, khắc phục kịp thời, thông báo cho các bên



liên quan khi xảy ra sự cố. Đặc biệt, chủ quản dữ liệu cốt lõi, quan trọng phải định kỳ đánh giá rủi ro đối với hoạt động xử lý các dữ liệu này và thông báo kết quả đánh giá tới cơ quan chuyên trách về an ninh mạng (Bộ Công an, Bộ Quốc phòng) để phối hợp bảo vệ. Đây là yêu cầu bắt buộc để đảm bảo các dữ liệu “nhạy cảm” luôn được giám sát ở mức cao nhất. Nghị định 165/2025/NĐ-CP đã cụ thể hóa nội dung này: Chủ quản dữ liệu cốt lõi, quan trọng hàng năm phải đánh giá rủi ro đối với xử lý dữ liệu đó, lập báo cáo theo mẫu kèm nghị định và luôn sẵn sàng để phục vụ kiểm tra của cơ quan thẩm quyền. Báo cáo rủi ro gồm thông tin về loại dữ liệu, phương pháp xử lý, biện pháp bảo vệ, các sự cố đã xảy ra và cách khắc phục. Đây là quy định rất chi tiết, thể hiện mức độ quản lý chủ động và phòng ngừa đối với dữ liệu quan trọng.

Nghị định cũng yêu cầu chủ quản dữ liệu cốt lõi, quan trọng phải ghi nhật ký toàn bộ quá trình xử lý, lưu giữ ít nhất 6 tháng. Đồng thời phải chỉ định người chịu trách nhiệm bảo vệ dữ liệu và bộ phận bảo vệ an toàn dữ liệu, với chức năng xây dựng kế hoạch bảo vệ, đánh giá rủi ro, báo cáo định kỳ về tình hình bảo vệ dữ liệu. Điều này tương tự mô hình Data Protection Officer (DPO) ở châu Âu, nâng cao trách nhiệm giải trình của tổ chức có dữ liệu nhạy cảm.

Chương III, Nghị định 165/2025/NĐ-CP (*từ Điều 15 đến 18*) quy định rất chi tiết về các biện pháp bảo vệ dữ liệu trong từng khâu: từ thu thập, tạo lập; lưu trữ; đến khai thác, sử dụng; và khi xóa/hủy dữ liệu. Ví dụ: khi thu thập dữ liệu cốt lõi, quan trọng, chủ quản phải xây dựng quy trình, đánh giá biện pháp bảo vệ trước; kiểm tra tính xác thực, giám sát chất lượng và khả năng truy xuất nguồn gốc dữ liệu. Khi lưu trữ dữ liệu, phải có quy trình lưu trữ, sao lưu, phục hồi, nhật ký; áp dụng công cụ kỹ thuật để bảo vệ dữ liệu lưu trữ; xóa, hủy dữ liệu khi hết hạn lưu trữ hoặc không còn cần thiết. Khi sử dụng dữ liệu cốt lõi, quan trọng, phải có quy chế truy cập tuân thủ nguyên tắc “quyền tối thiểu” (*least privilege*); xây dựng hệ thống kiểm soát truy cập với nhận dạng thống nhất; áp dụng biện pháp kỹ thuật kiểm soát truy cập, truy xuất dữ liệu. Chủ sở hữu dữ liệu cũng phải phân tích, đánh giá tác động đến quốc phòng, an ninh, xã hội trước khi công khai dữ



liệu của mình. Đặc biệt, đối với xóa, hủy dữ liệu quan trọng, cốt lõi, phải có tài liệu chứng minh rằng dữ liệu đã được hủy không thể khôi phục được - ngăn ngừa nguy cơ dữ liệu nhạy cảm bị khôi phục trái phép.

Các tổ chức cũng phải chú ý quản lý tình huống tổ chức lại, giải thể: nếu có chuyển dữ liệu do sáp nhập, giải thể, phải lập kế hoạch chuyển dữ liệu và thông báo cho các bên bị ảnh hưởng; nếu dữ liệu thuộc loại cốt lõi, quan trọng thì phải báo cáo phương án cho cơ quan thẩm quyền và đảm bảo an toàn dữ liệu khi chuyển giao. Ngoài ra, nếu ủy thác xử lý dữ liệu cho bên khác, phải quy định rõ nghĩa vụ bảo mật qua hợp đồng; nếu ủy thác dữ liệu quan trọng, cốt lõi thì bên ủy thác phải thẩm định năng lực bảo vệ dữ liệu của bên nhận trước.

Những quy định rất chi tiết này cho thấy định hướng quản lý dữ liệu ở mức vi mô, đòi hỏi các tổ chức phải xây dựng quy trình nội bộ và áp dụng công nghệ bảo mật phù hợp. Nó đặt ra thách thức nhưng cũng tạo khuôn khổ để dữ liệu quan trọng được xử lý an toàn.

Tiếp tục Điều 22 Luật Dữ liệu 2024 quy định về mã hóa, giải mã dữ liệu, trong đó dữ liệu thuộc danh mục bí mật nhà nước bắt buộc phải mã hóa bằng mật mã của cơ yếu khi lưu trữ, truyền, nhận trên mạng. Các cơ quan, tổ chức khác được tự sử dụng giải pháp mã hóa phù hợp hoạt động của mình; chủ sở hữu dữ liệu quyết định việc mã hóa hay không dữ liệu của họ. Đồng thời, luật cho phép cơ quan nhà nước có thẩm quyền được quyền giải mã dữ liệu không cần sự đồng ý của chủ sở hữu trong các trường hợp khẩn cấp, an ninh quốc gia bị đe dọa, thảm họa, chống bạo loạn khủng bố (*tương tự các trường hợp ở Luật An ninh mạng*). Quy định này cân bằng giữa việc khuyến khích sử dụng mã hóa để bảo vệ dữ liệu và quyền của Nhà nước can thiệp khi thật cần thiết vì lý do an ninh.

(3) Chuyển dữ liệu xuyên biên giới (data transfer): Đây là nội dung được quan tâm nhất, vì liên quan đến chủ quyền dữ liệu và hoạt động của doanh nghiệp quốc tế. Điều 23 Luật Dữ liệu quy định khá khái quát: “*Cơ quan, tổ chức, cá nhân được tự do chuyển dữ liệu từ nước ngoài về Việt Nam, xử lý dữ liệu của nước ngoài tại Việt Nam*” (tức Việt Nam ngăn cản dòng dữ liệu vào); còn việc



chuyển dữ liệu cốt lõi, dữ liệu quan trọng ra nước ngoài phải đảm bảo quốc phòng, an ninh, lợi ích quốc gia, quyền lợi hợp pháp của chủ thể dữ liệu... theo luật Việt Nam và các điều ước quốc tế liên quan. Đồng thời luật giao Chính phủ quy định chi tiết việc này.

Nghị định 165/2025/NĐ-CP đã đưa ra cơ chế chặt chẽ về chuyển dữ liệu ra nước ngoài (*Điều 12*). Theo đó, khi cần chuyển hoặc xử lý dữ liệu cốt lõi, quan trọng ra bên ngoài biên giới, chủ sở hữu/chủ quản phải tiến hành đánh giá tác động trước. Việc đánh giá tập trung xem xét: tính hợp pháp, sự cần thiết, phạm vi, phương thức truyền và xử lý dữ liệu bên nhận; những rủi ro có thể gây ra cho quốc phòng, an ninh, lợi ích công cộng hoặc quyền lợi cá nhân; trách nhiệm và biện pháp của bên nhận dữ liệu; và các vấn đề liên quan khác. Nói cách khác, doanh nghiệp/tổ chức muôn đưa dữ liệu quan trọng ra nước ngoài phải tự phân tích kỹ lưỡng nguy cơ và biện pháp quản trị.

Sau đó, tùy loại dữ liệu, nếu là dữ liệu cốt lõi, tổ chức chuyển dữ liệu phải lập hồ sơ đánh giá tác động (*theo mẫu*) gửi Bộ Công an (*hoặc Bộ Quốc phòng nếu thuộc lĩnh vực quốc phòng, cơ yếu*) để thẩm định trước khi chuyển. Cơ quan thẩm định sẽ kiểm tra hồ sơ và phải hoàn thành đánh giá trong 10 ngày (*phức tạp thì 15 ngày*) kể từ khi nhận đủ hồ sơ. Kết quả đánh giá nếu đạt yêu cầu, chủ quản dữ liệu mới được quyết định chuyển dữ liệu cốt lõi ra nước ngoài. Còn nếu là dữ liệu quan trọng, thì không cần chờ chấp thuận nhưng vẫn phải lập hồ sơ đánh giá tác động, gửi 01 bản chính cho Bộ Công an hoặc Bộ Quốc phòng trước 15 ngày khi tiến hành chuyển dữ liệu. Cơ quan quản lý sẽ kiểm tra giám sát trong trường hợp cần thiết.

Quy định này tạo ra một cơ chế “giấy phép” linh hoạt: Dữ liệu cốt lõi, quan trọng nhất thì phải có sự đồng ý trước khi chuyển; Dữ liệu quan trọng, ít nhạy hơn thì chỉ cần thông báo hồ sơ trước (*có thể coi như đăng ký*), không phải xin phép, nhưng cơ quan an ninh có thể kiểm tra bất kỳ lúc nào. Điều này nhằm tránh cản trở không cần thiết đến hoạt động kinh doanh, nhưng vẫn giúp Nhà nước nắm được dữ liệu gì sắp chuyển ra ngoài, có rủi ro gì.



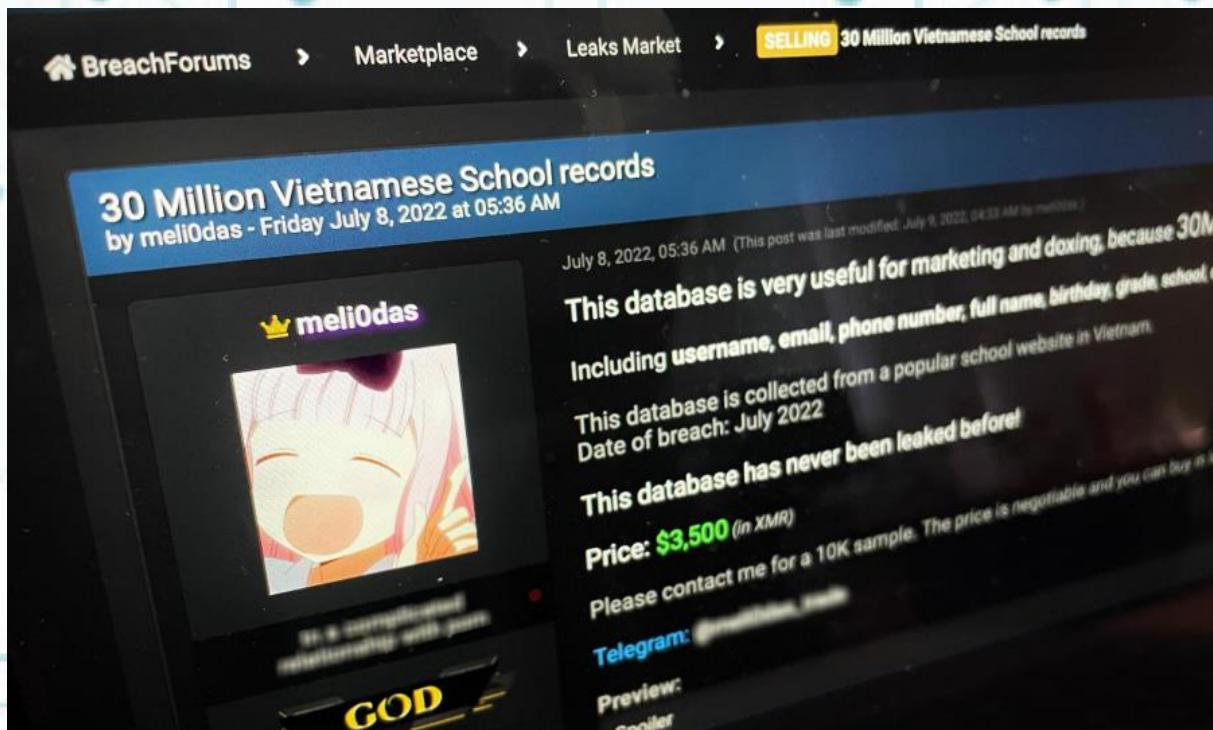
Nghị định cũng nêu rõ khi đánh giá, cơ quan có thẩm quyền tập trung đánh giá các rủi ro đối với an ninh quốc gia, lợi ích công cộng hoặc quyền lợi hợp pháp (*liệt kê 5 nhóm tương tự như đánh giá của doanh nghiệp nhưng ở tầm quốc gia, bao gồm: tính hợp pháp và cần thiết của việc chuyển; tác động của chính sách bảo vệ dữ liệu nước nhận; quy mô, phạm vi, loại dữ liệu và nguy cơ bị xâm phạm sau chuyển; trách nhiệm các bên; và các vấn đề khác ảnh hưởng quốc phòng, lợi ích quốc gia*). Nếu có thay đổi lớn sau khi đã chuyển (*như thay đổi mục đích, kéo dài lưu trữ, thay đổi chính sách nước nhận, ...*) thì bên chuyển phải sửa đổi, bổ sung hồ sơ đánh giá. Đặc biệt, Bộ Công an/Bộ Quốc phòng có quyền yêu cầu ngừng chuyển, xử lý dữ liệu cốt lõi, quan trọng ra nước ngoài trong trường hợp dữ liệu đó bị sử dụng cho hoạt động xâm phạm an ninh quốc gia, lợi ích công cộng hoặc quyền lợi hợp pháp của cá nhân, tổ chức. Đây là biện pháp mạnh nhằm bảo vệ chủ quyền dữ liệu, nếu phát hiện dữ liệu chuyển ra bị lạm dụng, Việt Nam có thể buộc dừng ngay việc chuyển tiếp hoặc xử lý thêm.

Có thể thấy, quy định về đưa dữ liệu ra nước ngoài trong Luật Dữ liệu của Việt Nam khá tương đồng với một số quốc gia như Trung Quốc với Đánh giá an ninh mạng cho chuyển dữ liệu quan trọng, hay Liên minh Châu Âu với quy định về chuyển dữ liệu cá nhân ra ngoài EEA đòi hỏi đánh giá và điều kiện bảo vệ tương đương. Việt Nam chọn cách không cấm đoán hoàn toàn nhưng tạo thủ tục kiểm soát kỹ lưỡng. Điều này phù hợp bối cảnh nhiều nền tảng công nghệ lớn đang thu thập dữ liệu Việt Nam, những dữ liệu cốt lõi, quan trọng (*ví dụ dữ liệu sinh trắc học, dữ liệu tài chính quan trọng*) khó có thể được chuyển ra khỏi Việt Nam một cách tùy tiện nữa. Doanh nghiệp nước ngoài phải cân nhắc lưu trữ và xử lý các dữ liệu nhạy cảm ngay tại Việt Nam (*đầu tư máy chủ ở Việt Nam*), hoặc nếu chuyển thì phải thông báo và chấp nhận sự giám sát.

Cuối cùng, Nghị định 165/2025/NĐ-CP cũng đề cập việc giám sát bảo mật dữ liệu, cảnh báo sớm và quản lý khẩn cấp (*Điều 19, 20*). Đây là việc các cơ quan chuyên trách (*như Cục An ninh mạng, Trung tâm ứng cứu sự cố an toàn thông tin*) sẽ giám sát lưu lượng, phát hiện sớm các sự cố rò rỉ dữ liệu lớn, từ đó cảnh



báo các đơn vị liên quan kịp thời. Quy định cụ thể của các điều này chưa trích trong các phần trên, nhưng có thể hình dung nó tương tự cơ chế giám sát an toàn thông tin hiện nay, chỉ bổ sung thêm đối tượng giám sát là dữ liệu. Khi xảy ra sự cố nghiêm trọng (ví dụ lỗ lọt Cơ sở dữ liệu lớn), Nhà nước có thể ra lệnh “khẩn cấp” đình chỉ kết nối, cô lập hệ thống để điều tra khắc phục.



Hình ảnh: Bài rao bán dữ liệu người Việt xuất hiện trên một diễn đàn hacker.

Ảnh: Báo VNexpress

Nhìn chung, chính sách bảo vệ dữ liệu của Việt Nam được thiết kế rất toàn diện: từ khâu phòng ngừa (*đánh giá rủi ro, quy trình bảo vệ*), bảo vệ trong vận hành thường nhật (*mã hóa, kiểm soát truy cập, giám sát nhật ký*), đến xử lý tình huống đặc biệt (*khẩn cấp, chuyển ra nước ngoài*). Điều này phản ánh sự thận trọng và coi trọng của Chính phủ với việc giữ an toàn cho “tài sản dữ liệu” quốc gia. Bài học từ nhiều vụ lỗ lọt dữ liệu thời gian qua cho thấy nếu không có khung pháp lý và chế tài đủ mạnh, các tổ chức sẽ chưa thực sự chú tâm đầu tư cho bảo mật dữ liệu. Nay với các quy định chi tiết và chắc chắn sẽ có chế tài xử phạt nặng (*Nghị định xử phạt vi phạm hành chính dự kiến sẽ ban hành*), các đơn vị buộc phải nâng cao năng lực bảo vệ dữ liệu. Điều này không chỉ bảo vệ người dân, mà còn tạo dựng niềm tin số - yếu tố then chốt để chuyển đổi số thành công.



1.2.4.5 Trách nhiệm quản lý nhà nước và phối hợp thực thi

Luật Dữ liệu 2024 cũng xác định rõ cơ chế quản lý nhà nước về dữ liệu. Điều 8 phân công: Chính phủ thống nhất quản lý; Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ về quản lý nhà nước lĩnh vực dữ liệu (*trừ phạm vi cơ yếu do Bộ Quốc phòng quản lý*). Các bộ, ngành trong phạm vi nhiệm vụ của mình có trách nhiệm xây dựng, phát triển các cơ sở dữ liệu và phối hợp với Bộ Công an trong quản lý nhà nước về dữ liệu. UBND cấp tỉnh quản lý nhà nước về dữ liệu tại địa phương. Như vậy, mô hình quản lý sẽ tập trung về một mối (Bộ Công an), tương tự mô hình một số nước giao cho Bộ Công nghệ thông tin hoặc cơ quan an ninh mạng chủ trì. Điều này đòi hỏi Bộ Công an phải xây dựng được bộ máy và năng lực tương xứng.

Ngoài ra, Điều 9 Luật Dữ liệu 2024 đề cập việc xây dựng, phát triển dữ liệu trong các cơ quan Đảng, Mặt trận, đoàn thể do cơ quan có thẩm quyền của các tổ chức đó quyết định và Tỉnh ủy, Thành ủy cũng thực hiện việc này trong phạm vi địa phương mình. Điều này tôn trọng tính độc lập của khối Đảng, đoàn thể, nhưng cũng đặt ra yêu cầu họ phải tham gia vào lộ trình chuyển đổi số chung, xây dựng các cơ sở dữ liệu của mình.

Về tổ chức thực hiện, luật quy định Quỹ Phát triển dữ liệu quốc gia (Điều 29). Quỹ phát triển dữ liệu quốc gia là quỹ tài chính nhà nước ngoài ngân sách, được hình thành ở trung ương để thúc đẩy phát triển, khai thác, ứng dụng, quản trị dữ liệu quốc gia. Việc thành lập và vận hành Quỹ sẽ do Chính phủ hướng dẫn, đảm bảo có kinh phí bền vững cho các chương trình dữ liệu trọng điểm.

Trong quá trình thực thi, sự phối hợp giữa Bộ Công an với Bộ Khoa học và Công nghệ, Bộ Văn hóa, Du lịch và Thể thao, Bộ Tài chính... là rất quan trọng. Bộ Khoa học và Công nghệ có vai trò lớn về hạ tầng ICT, an toàn thông tin, chính phủ điện tử - cần phối hợp chuyển giao một số nhiệm vụ về dữ liệu cho Bộ Công an hoặc cùng thực hiện (*chẳng hạn vận hành Nền tảng tích hợp chia sẻ dữ liệu quốc gia, Công dữ liệu quốc gia*). Bộ Khoa học và Công nghệ, Bộ Tài chính giữ



nhiều dữ liệu kinh tế, cũng như quản lý đầu tư cho CNTT, nên cũng phải phối hợp nhịp nhàng tránh trùng lặp nguồn lực.

1.2.5. Kiến nghị chính sách và kết luận

Thứ nhất, Luật Dữ liệu 2024 và Nghị định 165/2025/NĐ-CP đã tạo nền tảng pháp lý quan trọng, nhưng để phát huy hiệu lực, cần ban hành kịp thời các văn bản hướng dẫn chi tiết và chế tài xử lý vi phạm. Kiến nghị Chính phủ sớm ban hành nghị định xử phạt vi phạm trong lĩnh vực dữ liệu. Ví dụ: cần quy định rõ mức phạt hành chính cao đối với hành vi không tuân thủ bảo vệ dữ liệu (*để xảy ra lộ lọt dữ liệu cốt lõi, quan trọng*) nhằm răn đe, tương tự mức phạt lên tới 5% doanh thu toàn cầu theo GDPR của Liên minh Châu Âu.

- **Thứ hai,** đẩy nhanh triển khai hạ tầng Trung tâm dữ liệu quốc gia, đây là “xương sống” của mọi chính sách dữ liệu. Hiện nay Bộ Công an đang được giao xây dựng Trung tâm dữ liệu quốc gia (*dự kiến sẽ hoạt động trong tháng 8/2025*.

Vì vậy cần đầu tư trọng điểm từ ngân sách và huy động đối tác công nghệ lớn để xây dựng trung tâm theo tiêu chuẩn hiện đại (*tier 4, xanh, an toàn*). Đồng thời, tiến hành kết nối thí điểm một số cơ sở dữ liệu quan trọng vào Cơ sở dữ liệu tổng hợp Quốc gia (ví dụ: kết nối Cơ sở dữ liệu dân cư với Cơ sở dữ liệu đất đai, doanh nghiệp) để sớm cho kết quả. Việc vận hành Trung tâm dữ liệu quốc gia cũng nên có sự tham gia của khối tư nhân theo mô hình dịch vụ thuê hạ tầng (*cloud services*) để tối ưu chi phí.

- **Thứ ba,** đảm bảo an ninh, chủ quyền số nhưng không cản trở dòng chảy dữ liệu cho phát triển kinh tế. Các quy định về chuyển dữ liệu xuyên biên giới cần được thực thi linh hoạt, tránh trở thành rào cản thương mại. Kiến nghị cơ quan quản lý xây dựng hướng dẫn minh bạch về quy trình đánh giá tác động, tiêu chí đạt hay không đạt, thời hạn xử lý hồ sơ... để doanh nghiệp (*nhất là doanh nghiệp nước ngoài*) có thể tuân thủ dễ dàng. Song song, cần phát triển các dịch vụ trung gian đảm bảo dữ liệu xuyên biên giới (*chẳng hạn dịch vụ mã hóa dữ liệu trước khi ra nước ngoài, dịch vụ lưu trữ đám mây tại Việt Nam*) để hỗ trợ doanh nghiệp vừa đáp ứng luật vừa kinh doanh thông suốt.



- **Thứ tư**, thúc đẩy mạnh dữ liệu mở và thị trường dữ liệu, kiến nghị các bộ, ngành, địa phương xây dựng kế hoạch dữ liệu mở ngay sau khi luật có hiệu lực. Mỗi đơn vị cần xác định danh mục dữ liệu sẽ mở trong 1-2 năm tới và công bố lộ trình. Bộ KH&CN (*hoặc Trung tâm dữ liệu quốc gia*) cần nâng cấp Cổng dữ liệu quốc gia cả về dung lượng và tính năng (*cung cấp API, công cụ tìm kiếm dữ liệu*). Ngoài ra, để kích thích thị trường dữ liệu, Chính phủ có thể thí điểm cơ chế *sandbox* về kinh doanh dữ liệu, cho phép doanh nghiệp khai thác các *tập dữ liệu* ẩn danh của Nhà nước theo mô hình thu phí hoặc hợp tác công tư. Những dữ liệu có giá trị cao (*nhiều dữ liệu giao thông đô thị, dữ liệu tiêu dùng...*) nếu được chia sẻ cho doanh nghiệp đổi mới sáng tạo sẽ tạo ra nhiều ứng dụng hữu ích (*giao thông thông minh, dịch vụ tài chính số,...*).

- **Thứ năm**, nâng cao nhận thức và năng lực thực thi ở các cấp. Cuối cùng, yếu tố con người vẫn quyết định sự thành bại. Cần đẩy mạnh công tác tuyên truyền, đào tạo về Luật Dữ liệu cho đội ngũ cán bộ từ trung ương đến địa phương, cũng như cho khối doanh nghiệp. Kiến nghị thiết lập chương trình đào tạo “*quản trị dữ liệu cho lãnh đạo*”, “*an toàn dữ liệu cho cán bộ kỹ thuật*” để mọi người hiểu rõ trách nhiệm của mình. Bên cạnh đó, cần sớm hình thành đội ngũ chuyên gia dữ liệu (*Data Scientist, Data Engineer, Chuyên gia pháp lý về dữ liệu*) đủ mạnh. Bộ Giáo dục và Đào tạo nên phối hợp đưa các nội dung về quản trị dữ liệu, pháp luật dữ liệu vào chương trình đào tạo đại học và sau đại học (*ví dụ ngành Hệ thống thông tin, Khoa học dữ liệu, Luật công nghệ*).

■ Chính sách và pháp luật về dữ liệu tại Việt Nam đang có bước chuyển biến lịch sử với việc ban hành Luật Dữ liệu 2024 và các văn bản liên quan. Khung pháp lý mới này kỳ vọng sẽ tạo nền tảng vững chắc để Việt Nam khai thác hiệu quả “mỏ vàng dữ liệu”, phục vụ phát triển Chính phủ số, kinh tế số và xã hội số bền vững. Đồng thời, các quy định chặt chẽ sẽ giúp chuẩn hóa hoạt động quản trị dữ liệu, bảo vệ an ninh dữ liệu quốc gia và quyền lợi của người dân trong kỷ nguyên số. Chặng đường phía trước còn nhiều thách thức về triển khai, nhưng với quyết tâm chính trị cao và lộ trình chiến lược rõ ràng, Việt Nam có cơ sở để tin tưởng rằng mục tiêu



trở thành quốc gia số an toàn, thịnh vượng, nằm trong nhóm dẫn đầu khu vực về chính phủ số và dữ liệu số vào năm 2030 sẽ đạt được. Luật Dữ liệu 2024 chính là một dấu mốc quan trọng trên hành trình đó, đưa ra nguyên tắc, mục tiêu và công cụ pháp lý để biến dữ liệu thành động lực phát triển mới của đất nước.



PHỤ LỤC

PL1. So sánh và bài học kinh nghiệm quốc tế cho Việt Nam

1. Điểm tương đồng nổi bật

Luật Dữ liệu 2024 của Việt Nam phù hợp với xu thế chung của quốc tế và hấp thu những tinh hoa trong quy định pháp luật về Dữ liệu của các quốc gia và khu vực, phù hợp với tình hình kinh tế, chính trị, xã hội trong nước, có thể thấy một số điểm tương đồng nổi bật:

Thứ nhất, coi dữ liệu là tài nguyên chiến lược, thúc đẩy song song khai thác và bảo vệ:

Tất cả các nước/luật đều nhìn nhận dữ liệu có vai trò nền tảng cho phát triển kinh tế - xã hội trong thời đại số. Chính phủ các nước đều đặt mục tiêu kép: một mặt tạo điều kiện khai thác dữ liệu để thúc đẩy đổi mới sáng tạo, tăng trưởng (ví dụ APPI của Nhật nêu rõ việc ứng dụng hiệu quả thông tin cá nhân góp phần tạo ra ngành công nghiệp mới, mang lại xã hội kinh tế sôi động; Liên minh Châu Âu thì nhấn mạnh tiềm năng kinh tế và xã hội to lớn của dữ liệu để tạo sản phẩm dịch vụ mới, giải quyết các thách thức như chăm sóc sức khỏe, môi trường); mặt khác, các luật cũng đề ra các biện pháp bảo vệ chặt chẽ an ninh, quyền riêng tư và lợi ích hợp pháp của cá nhân, tổ chức. Nói cách khác, bài toán cân bằng giữa khai thác dữ liệu và bảo vệ dữ liệu được đặt ra tương tự ở mọi quốc gia. Ví dụ: Nhật Bản trong Luật Cơ bản 2016 đã viết rõ nguyên tắc: thúc đẩy sử dụng dữ liệu đi đôi với “đảm bảo an toàn, độ tin cậy, không tổn hại quyền lợi công dân và an ninh quốc gia”. Liên minh Châu Âu thì thông qua các bộ luật kép: một mặt GDPR bảo vệ dữ liệu cá nhân nghiêm ngặt, mặt khác DGA tạo khung chia sẻ dữ liệu an toàn. Trung Quốc nhấn mạnh “phát triển dữ liệu phải gắn liền với bảo đảm an ninh” ngay từ tên chỉ Luật An ninh Dữ liệu. Việt Nam cũng quy định nguyên tắc tương tự trong Luật Dữ liệu: bảo vệ dữ liệu phải được thực hiện đồng bộ, chặt chẽ cùng với phát triển dữ liệu và khai thác sử dụng dữ liệu phải hiệu quả, thuận tiện nhưng tuân thủ pháp luật, bảo đảm quyền con người và an ninh.



- **Thứ hai**, vai trò trung tâm của Chính phủ trong quản lý và thúc đẩy dữ liệu. Các quốc gia đều xác định Chính phủ đóng vai trò dẫn dắt trong xây dựng hạ tầng, khuôn khổ pháp lý và giám sát việc sử dụng dữ liệu:

- Ở Nhật Bản, Chính phủ xây dựng Chiến lược quốc gia về dữ liệu (*thông qua các Kế hoạch cơ bản về sử dụng dữ liệu công-tư*), thành lập Hội nghị Chiến lược về dữ liệu do Thủ tướng làm chủ tịch để điều phối thực hiện chiến lược. Đồng thời Ủy ban PPC độc lập giám sát việc bảo vệ dữ liệu cá nhân trên phạm vi cả nước.

- EU thông qua DGA yêu cầu các nước thành viên chỉ định cơ quan có thẩm quyền giám sát các dịch vụ trung gian dữ liệu và hoạt động data altruism. Ủy ban Châu Âu cũng lập ra Ban Đổi mới Dữ liệu châu Âu (*European Data Innovation Board*) để phối hợp ban hành hướng dẫn, tiêu chuẩn chung.

- Australia thành lập Ủy viên Dữ liệu Quốc gia làm cơ quan điều phối duy nhất cho chương trình chia sẻ dữ liệu liên bang; đồng thời có Hội đồng cố vấn với sự tham gia của các chuyên gia độc lập nhằm đảm bảo khách quan trong việc tư vấn chính sách.

- Trung Quốc có cách tiếp cận tập trung hơn: Ủy ban An ninh Quốc gia trung ương nắm quyền chỉ đạo cao nhất về dữ liệu. Bên dưới, nhiều bộ ngành cùng tham gia, Chính phủ đóng vai trò chính trong ban hành chính sách và thực thi.

Việt Nam trao cho Chính phủ thẩm quyền thống nhất quản lý nhà nước về dữ liệu, giao Bộ Công an làm đầu mối và thành lập Trung tâm dữ liệu quốc gia trực thuộc Bộ Công an. Điều này tương tự mô hình Trung Quốc ở sự tập trung, nhưng khác ở chỗ Việt Nam chưa có một cơ quan độc lập tương tự PPC hay các Data Protection Authority của phương Tây.

- **Thứ ba**, quy định về luân chuyển dữ liệu xuyên biên giới:

Mặc dù mức độ cởi mở khác nhau, tất cả các khuôn khổ pháp lý đều có điều khoản điều chỉnh việc đưa dữ liệu ra/vào biên giới quốc gia, thể hiện sự thừa nhận rằng dòng chảy dữ liệu toàn cầu là tất yếu trong thời đại số:



- Nhật Bản (*APPI*): Muốn truyền dữ liệu cá nhân ra nước ngoài thì doanh nghiệp phải được sự đồng ý riêng biệt của cá nhân sau khi đã cung cấp thông tin về hệ thống bảo vệ dữ liệu của nước tiếp nhận, trừ khi dữ liệu gửi đến một quốc gia đã được PPC công nhận có mức độ bảo vệ tương đương Nhật Bản (*whitelist*) hoặc bên nhận cam kết các biện pháp bảo vệ tương đương. Quy định này tương đồng với cơ chế “quyết định phù hợp” (*adequacy*) của Liên minh Châu Âu. Nhật Bản cũng có riêng khuôn khổ APEC CBPR để hỗ trợ chuyển dữ liệu trong khối APEC.

- EU (*GDPR* và *DGA*): GDPR cấm chuyển dữ liệu cá nhân ra ngoài EEA trừ khi đáp ứng một trong các điều kiện: quốc gia nhận có quyết định công nhận từ Liên minh Châu Âu, hoặc tổ chức nhận áp dụng biện pháp bảo vệ thích hợp (*ví dụ hợp đồng mẫu, chứng nhận*), hoặc thuộc trường hợp ngoại lệ (*đồng ý của cá nhân,...*). DGA thì chủ yếu nhắc tới dữ liệu phi cá nhân nhạy cảm: nếu chia sẻ ra ngoài Liên minh Châu Âu phải có biện pháp ngăn không để nước thứ ba truy cập trái phép dữ liệu (*ví dụ mã hóa hoặc xử lý trong môi trường an toàn trên lãnh thổ Liên minh Châu Âu*). Liên minh Châu Âu cũng đang xây dựng khuôn khổ liên kết dữ liệu quốc tế thông qua các hiệp định song phương.

- Australia (*DATA Act*): Chương trình chia sẻ dữ liệu công của Australia hiện không cho phép thực thể nước ngoài truy cập. Tuy nhiên, Australia có thể ký các thỏa thuận quốc tế để trao đổi dữ liệu trong những lĩnh vực nhất định. Luật cũng có hiệu lực ngoài lãnh thổ đối với hành vi vi phạm của công dân/ tổ chức Australia ở nước ngoài. Điểm đáng chú ý: Australia cấm sử dụng dữ liệu chia sẻ cho mục đích an ninh, thực thi pháp luật - ngược hẳn với quan điểm Trung Quốc, cho thấy sự khác biệt về ưu tiên quốc gia.

- Trung Quốc (*DSL* và *PIPL*): Kiểm soát chặt chẽ luồng dữ liệu ra ngoài. Dữ liệu quan trọng muốn đưa ra nước ngoài phải qua đánh giá an ninh. Mọi yêu cầu của cơ quan nước ngoài đòi dữ liệu trên đất Trung Quốc đều bị chặn nếu chưa được phép. Ngoài ra, Trung Quốc áp dụng quy định đối đẳng: nếu nước khác đối xử doanh nghiệp Trung Quốc bất lợi về dữ liệu thì Trung Quốc sẽ có biện pháp



tương ứng. Với dữ liệu cá nhân, Luật Bảo vệ Thông tin Cá nhân (*PIPL*) của Trung Quốc cũng yêu cầu các công ty phải xin phép cơ quan quản lý nếu chuyển nhiều dữ liệu cá nhân ra ngoài, trừ khi có chứng nhận bảo vệ (ví dụ tham gia Cơ chế bảo vệ chuẩn).

- Việt Nam (*Luật Dữ liệu 2024*): Cho phép chuyển dữ liệu qua biên giới nhưng dữ liệu quan trọng/cốt lõi muốn đưa ra ngoài phải đảm bảo an ninh và được kiểm soát. Việt Nam cũng quy định cơ quan thực thi pháp luật hoặc tư pháp nước ngoài muốn yêu cầu dữ liệu phải thông qua cơ quan có thẩm quyền Việt Nam quyết định (*điểm tương đồng Trung Quốc*). Có thể thấy Việt Nam có chế độ hài hòa: vừa tạo điều kiện cho luồng dữ liệu phục vụ đầu tư, hợp tác quốc tế, vừa giữ quyền kiểm soát ở những dữ liệu nhạy cảm.

- **Thứ tư**, phân loại dữ liệu và biện pháp bảo vệ theo mức độ nhạy cảm:

Hầu hết các quy định đều có khái niệm phân loại dữ liệu:

- Nhật Bản phân chia dữ liệu cá nhân thường, dữ liệu cá nhân nhạy cảm (*đòi hỏi xử lý cẩn trọng hơn; có cơ chế khuyến khích sử dụng dữ liệu đã được khử danh tính để vừa khai thác được vừa giảm rủi ro vi phạm quyền riêng tư*).

- Trung Quốc có “dữ liệu thông thường - quan trọng - cốt lõi” và yêu cầu Nhà nước lập danh mục dữ liệu quan trọng làm căn cứ quản lý.

- Việt Nam cũng thiết lập phân cấp tương tự (*thông thường - quan trọng - cốt lõi*). Liên minh Châu Âu thì không định nghĩa “dữ liệu quan trọng” chung, nhưng có các khái niệm như dữ liệu nhạy cảm trong các lĩnh vực cụ thể hoặc dữ liệu liên quan lợi ích công cộng (ví dụ *DGA* nói đến dữ liệu do cơ quan công nham nắm giữ nhưng được bảo vệ bởi luật khác như bí mật công nghiệp, IP, dữ liệu cá nhân...).

- Australia phân loại dữ liệu theo mục đích sử dụng (*chỉ chia sẻ được nếu phục vụ 3 mục đích công đã định*) và loại trừ các dữ liệu nhạy cảm như dữ liệu an ninh, thực thi pháp luật.

Nhìn chung, các nước đều có cách xác định dữ liệu nào cần bảo vệ đặc biệt (*cá nhân, nhạy cảm, quan trọng...*) và đưa ra quy chế chặt chẽ hơn cho nhóm đó.



- **Thứ năm**, khuyến khích đổi mới sáng tạo và phát triển công nghệ dữ liệu:

Các quốc gia đều nhận ra giá trị của dữ liệu trong việc thúc đẩy công nghệ mới như AI, IoT, điện toán đám mây. Do đó, luật và chính sách đi kèm thường khuyến khích nghiên cứu, phát triển và sáng tạo dựa trên dữ liệu:

- Nhật Bản trong Luật Cơ bản nêu rõ phải tận dụng công nghệ tiên tiến (AI, IoT, cloud) để gia tăng giá trị dữ liệu; chính phủ Nhật cũng hỗ trợ các Information Bank (ngân hàng dữ liệu) để doanh nghiệp chia sẻ dữ liệu với nhau.

- Liên minh Châu Âu có chiến lược Không gian dữ liệu chung Châu Âu trong nhiều lĩnh vực (y tế, nông nghiệp, công nghiệp...) nhằm tạo kho dữ liệu dùng chung cho doanh nghiệp khởi nghiệp, nghiên cứu AI. DGA có cơ chế data altruism như đã nói, một dạng đóng góp dữ liệu phục vụ nghiên cứu khoa học, cải tiến dịch vụ công.

- Australia kỳ vọng chương trình DATA sẽ giúp cải tiến dịch vụ công và hỗ trợ nghiên cứu đẳng cấp thế giới. Australia cũng đầu tư nhiều vào mở dữ liệu (data.gov.au) để doanh nghiệp khai thác.

- Trung Quốc thúc đẩy mạnh mẽ việc phát triển kinh tế số dựa trên dữ liệu, thể hiện qua chiến lược quốc gia “Internet+” và hàng loạt chính sách AI. Luật An ninh Dữ liệu đặt mục tiêu “thúc đẩy phát triển và sử dụng dữ liệu” bên cạnh việc bảo vệ, nghĩa là Trung Quốc muốn tận dụng dữ liệu trong nước để cạnh tranh công nghệ.

Việt Nam với Luật Dữ liệu cũng nhấn mạnh ưu tiên phát triển dữ liệu trong các lĩnh vực kinh tế - xã hội trọng điểm để phục vụ chuyển đổi số quốc gia, phát triển kinh tế số. Nhà nước khuyến khích đầu tư, nghiên cứu, phát triển công nghệ dữ liệu, sản phẩm dịch vụ dữ liệu, đổi mới sáng tạo và xây dựng các trung tâm dữ liệu, thị trường dữ liệu. Điều này cho thấy Việt Nam rất coi trọng việc tạo hệ sinh thái đổi mới quanh dữ liệu.

2. Điểm khác biệt nổi bật

Như đã nói, Luật Dữ liệu 2024 của Việt Nam phù hợp với xu thế chung của quốc tế và hấp thu những tinh hoa trong quy định pháp luật về Dữ liệu của các



quốc gia. Nhưng mỗi quốc gia có một đặc điểm riêng biệt về chính trị, kinh tế, văn hóa, vì vậy Luật Dữ liệu của Việt Nam cũng có những khác biệt so với các luật trên thế giới, cụ thể:

Thứ nhất, về phạm vi điều chỉnh và trọng tâm chính của luật:

- Nhật Bản (*APPI*): Tập trung chuyên sâu vào bảo vệ thông tin cá nhân. Luật APPI chủ yếu đặt ra các nghĩa vụ đối với việc thu thập, xử lý dữ liệu cá nhân, áp dụng cho mọi thực thể (*doanh nghiệp tư nhân lẫn cơ quan nhà nước*). APPI định nghĩa rõ các khái niệm “thông tin cá nhân”, “thông tin cá nhân nhạy cảm”, “thông tin được định danh giả/ẩn danh” và đặt ra quy tắc xử lý tương ứng. Có thể coi APPI tương đương “GDPR phiên bản Nhật” ở phạm vi và mục đích bảo vệ quyền riêng tư cá nhân trong bối cảnh dữ liệu số bùng nổ, đồng thời cho phép sử dụng dữ liệu cá nhân đã ẩn danh/ngụy danh cho đổi mới sáng tạo. APPI cũng có các điều khoản về chuyển dữ liệu ra nước ngoài tương tự GDPR như đã nêu.

- Nhật Bản (*Luật Cơ bản 2016*): Phạm vi rộng hơn nhiều, không giới hạn ở dữ liệu cá nhân mà hướng tới tất cả dữ liệu khu vực công và tư nhân. Trọng tâm luật này là thúc đẩy chia sẻ, mở dữ liệu giữa các cơ quan chính phủ với doanh nghiệp và xã hội để giải quyết vấn đề (*dân số già, thiên tai, giao thông...*) và phát triển kinh tế. Nó đặt ra các nguyên tắc, kế hoạch để chính quyền các cấp chủ động công bố dữ liệu và hỗ trợ khu vực tư khai thác. Tuy nhiên, luật này mang tính định hướng chiến lược, ít có chế tài cưỡng chế cụ thể như APPI. Có thể hiểu Luật Cơ bản là tuyên ngôn chính sách dữ liệu mở của Nhật, bổ sung cho APPI về mặt khai thác dữ liệu phi cá nhân.

- EU (*DGA*): Khác với các luật khác là luật tổng quát, DGA có phạm vi hẹp hơn theo chiều dọc: tập trung vào thiết lập cơ chế quản trị cho việc chia sẻ dữ liệu. DGA không điều chỉnh mọi khía cạnh dữ liệu số, mà chỉ nhắm vào ba trụ cột:

⁽¹⁾Tái sử dụng dữ liệu khu vực công được bảo vệ (*nhiều dữ liệu chứa thông tin cá nhân, bí mật thương mại...*); ⁽²⁾Quy định hoạt động của các dịch vụ trung gian dữ liệu (*data sharing service providers*); ⁽³⁾Khuyến khích hoạt động lòng vị tha dữ liệu. DGA hỗ trợ cho các đạo luật khác (*nhiều GDPR, luật Cảnh tranh...*). Một điểm



khác là DGA mang tính thị trường nội khôi: tạo tiền đề hình thành thị trường dữ liệu chung châu Âu, phá bỏ các rào cản quốc gia trong chia sẻ dữ liệu. Trong khi đó, các nước khác (*Nhật, Australia, TQ, VN*) luật dữ liệu chủ yếu tác động trong phạm vi quốc gia.

- Mỹ: Mỹ có cách tiếp cận khác biệt, mở dữ liệu chính phủ theo mặc định (*Open Government Data Act 2019 yêu cầu dữ liệu cơ quan liên bang phải công khai ở định dạng mở, trừ khi có lý do bảo mật*) và ưu tiên khu vực tư dân dắt đổi mới. Mỹ coi khu vực tư nhân là động lực chính khai thác dữ liệu, còn chính phủ tạo môi trường pháp lý thuận lợi. Cách tiếp cận này trái ngược với Trung Quốc nơi nhà nước kiểm soát dữ liệu chặt chẽ.

- Australia (*DATA Act*): Phạm vi giới hạn ở dữ liệu khu vực công liên bang. Khác với các quốc gia khác có tham vọng điều chỉnh mọi loại dữ liệu, luật Australia chỉ tập trung tạo ra cơ chế chia sẻ dữ liệu giữa các cơ quan chính phủ với nhau và với một số tổ chức được chỉ định (*các trường đại học*). Nó không áp dụng cho dữ liệu do doanh nghiệp tư nhân nắm giữ, cũng không điều chỉnh dữ liệu của tiểu bang (*trừ khi tiểu bang tham gia tình nguyện*). Vì giới hạn này, DATA Act có tính chuyên biệt cao: đi thẳng vào việc xử lý trở ngại khi cơ quan chính phủ muốn dùng dữ liệu của nhau (*vấn đề mà nhiều nước cũng gặp*). Mục đích của Australia là cung cấp dịch vụ công tốt hơn, hoạch định chính sách dựa trên bằng chứng và hỗ trợ nghiên cứu học thuật - tất cả đều trong phạm vi lợi ích công.

- Trung Quốc (*DSL*): Phạm vi bao trùm gần như mọi hoạt động dữ liệu. Khác với GDPR (*chỉ dữ liệu cá nhân*) hay DGA (*một mảng hẹp*), Luật An ninh Dữ liệu áp dụng cho tất cả các loại dữ liệu (*kể cả dữ liệu cá nhân lẫn phi cá nhân, dữ liệu công lẫn tư*). Trọng tâm của Luật An ninh Dữ liệu là an ninh quốc gia và trật tự quản lý nhà nước trong không gian dữ liệu. Nếu GDPR đặt quyền cá nhân là trung tâm, Luật An ninh Dữ liệu đặt lợi ích công lên trên hết. Có thể thấy, Luật An ninh Dữ liệu được thiết kế trong bối cảnh cạnh tranh địa chính trị về công nghệ: Trung Quốc muốn kiểm soát chặt dữ liệu trong nước trước nguy cơ từ bên ngoài. Bởi vậy, Luật An ninh Dữ liệu chứa nhiều điều khoản cấm, hạn chế (*cấm*



cung cấp dữ liệu cho nước ngoài nếu chưa duyệt, kiểm soát xuất khẩu dữ liệu, xử phạt nặng vi phạm...). Mặc dù Luật An ninh Dữ liệu cũng nói đến “thúc đẩy phát triển sử dụng dữ liệu”, nhưng có thể thấy tính kiểm soát vẫn lấn át.

Việt Nam (Luật Dữ liệu 2024): Có phạm vi rất rộng và bao quát, gần như là sự kết hợp của nhiều khía cạnh mà các luật nước ngoài tách riêng. Luật Dữ liệu VN điều chỉnh từ xây dựng hạ tầng dữ liệu quốc gia (*Trung tâm, Cơ sở dữ liệu Quốc gia*) đến quản trị dữ liệu, phân loại dữ liệu, bảo vệ dữ liệu cá nhân, chia sẻ dữ liệu công, thị trường dữ liệu. Trọng tâm nổi bật của Việt Nam là coi dữ liệu là tài sản công dân và quốc gia, cần vừa khai thác cho phát triển kinh tế số, vừa quản lý để bảo vệ chủ quyền, an ninh. So với Trung Quốc, Việt Nam cởi mở hơn trong việc hợp tác quốc tế (*VN khuyến khích tham gia xây dựng tiêu chuẩn, quy tắc quốc tế về dữ liệu; còn Trung Quốc thường tự đặt tiêu chuẩn riêng*).

- **Thứ hai,** cơ chế quản lý trung gian dữ liệu và thị trường dữ liệu:

- **Liên minh Châu Âu (DGA):** Liên minh Châu Âu thận trọng với các dịch vụ trung gian dữ liệu, đóng vai trò như môi giới, sàn giao dịch giúp kết nối người có dữ liệu với người muốn sử dụng dữ liệu. DGA yêu cầu các nhà cung cấp dịch vụ này phải đăng ký và chịu sự giám sát của cơ quan nhà nước, đồng thời phải tuân thủ nguyên tắc trung lập (*nghĩa là không được dùng dữ liệu cho lợi ích riêng hoặc có hành vi cạnh tranh không lành mạnh*). Đặc biệt, nhà cung cấp dịch vụ trung gian phải tách biệt pháp nhân với các hoạt động kinh doanh dữ liệu khác của mình. Ví dụ một công ty công nghệ muốn mở nền tảng chia sẻ dữ liệu thì nền tảng đó phải độc lập, không được trộn lẫn với mảng kinh doanh dùng dữ liệu của chính công ty, nhằm tránh xung đột lợi ích. Đây là yêu cầu khắt khe để tạo niềm tin cho các bên tham gia chia sẻ dữ liệu qua trung gian. Liên minh Châu Âu cũng khuyến khích mô hình kho dữ liệu chung phi lợi nhuận và các hợp tác xã dữ liệu.

- **Mỹ:** thị trường dữ liệu tại Mỹ phát triển khá tự do, có nhiều sàn dữ liệu tư nhân (*data marketplace*) mua bán dữ liệu thương mại mà chính phủ không can thiệp nhiều (*ngoại trừ luật cạnh tranh và một số quy định bảo mật*



(ngành). Sự khác biệt này xuất phát từ triết lý quản trị: Mỹ coi dữ liệu (*trù dữ liệu cá nhân nhạy cảm*) là tài sản thương mại bình thường, nhà nước không nhất thiết quản lý chặt việc ai làm trung gian. Trái lại, Liên minh Châu Âu và VN muốn có giám sát nhà nước để đảm bảo dữ liệu được chia sẻ minh bạch, đúng mục đích.

- Trung Quốc: Thị trường giao dịch dữ liệu ở Trung Quốc cũng chịu kiểm soát mạnh của nhà nước. Luật An ninh Dữ liệu như đã nêu yêu cầu các nền tảng giao dịch dữ liệu phải xác minh danh tính, nguồn gốc và lưu trữ nhật ký giao dịch, nếu vi phạm sẽ bị phạt nặng. Trung Quốc có lập một số sàn giao dịch dữ liệu ở các thành phố lớn (*Bắc Kinh, Thượng Hải*) nhưng các sàn này đều hoạt động dưới sự hướng dẫn của chính phủ và tập trung giao dịch dữ liệu doanh nghiệp nhà nước, dữ liệu chính phủ mở.

Úc: Luật Australia không đề cập “sàn dữ liệu” thương mại, vì như đã nói nó chỉ chia sẻ giữa các cơ quan và một số tổ chức nghiên cứu. Tuy nhiên, trong khuôn khổ đó, Australia có khái niệm “Nhà cung cấp dịch vụ dữ liệu được chứng nhận” (*ADSP*) đóng vai trò trung gian kỹ thuật (*ví dụ giúp gộp dữ liệu từ nhiều cơ quan, ẩn danh dữ liệu trước khi cung cấp cho người dùng cuối*). Các ADSP này cũng phải là cơ quan chính phủ hoặc trường đại học và cần xin chứng nhận. Về cơ bản, Australia xây dựng một hệ sinh thái khép kín, chưa có thị trường dữ liệu mở cho doanh nghiệp tư nhân.

Việt Nam với Luật Dữ liệu 2024 cũng đề cập mô hình sàn dữ liệu nhưng cách tiếp cận khác Liên minh Châu Âu. Sàn dữ liệu tại Việt Nam được hiểu là một nền tảng do Nhà nước lập ra hoặc quản lý để cung cấp dữ liệu cho các mục đích nghiên cứu, đổi mới và giao dịch dữ liệu. Việc giới hạn chủ thể vận hành sàn dữ liệu chỉ là đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước cho thấy Việt Nam chọn mô hình nhà nước dẫn dắt thị trường dữ liệu giai đoạn đầu. Các dịch vụ trung gian dữ liệu khác (*nhiều dịch vụ phân tích, xác thực dữ liệu*) được phép hoạt động nhưng phải ký hợp đồng và tuân thủ quy định của luật.



- **Thứ ba**, về mô hình tổ chức cơ quan quản lý/giám sát dữ liệu:

- Nhật Bản: Điểm đáng học hỏi là Ủy ban Bảo vệ Thông tin Cá nhân (*PPC*) cơ quan độc lập trực thuộc Văn phòng Nội các. PPC có quyền giám sát cả khu vực tư và nhà nước về việc tuân thủ APPI, ban hành hướng dẫn và xử phạt vi phạm. PPC Nhật tương tự các cơ quan bảo vệ dữ liệu (*DPA*) ở châu Âu. Tính độc lập và chuyên môn hóa cao của PPC giúp tạo lòng tin cho công chúng rằng việc bảo vệ dữ liệu không bị chi phối bởi lợi ích chính trị hay kinh tế.

- EU: Trước hết là mạng lưới Cơ quan bảo vệ dữ liệu quốc gia (*DPA*) ở mỗi nước thành viên để thực thi GDPR - các DPA này đều đòi hỏi phải độc lập (*về pháp lý và chức năng*) với chính phủ. Đối với DGA, Liên minh Châu Âu yêu cầu các nước lập cơ quan có thẩm quyền giám sát dịch vụ trung gian và tổ chức altruism và cơ quan này cũng phải độc lập tương tự (*không nằm trong doanh nghiệp hay cơ quan nào có xung đột lợi ích*). Ngoài ra, Liên minh Châu Âu lập Ban Đổi mới Dữ liệu ở cấp Liên minh Châu Âu để phối hợp, nhưng đây là cơ chế tư vấn chứ không phải cơ quan quản lý tập trung.

- Australia: Ủy viên Dữ liệu Quốc gia (*NDC*) là một chức danh mới, đặt trong bộ máy chính phủ (*trực thuộc Bộ Thủ tướng và Nội các*). NDC có quyền hạn như một regulator: cấp phép, thanh tra, xử phạt việc chia sẻ dữ liệu theo DATA Act. Điểm khác là NDC còn có nhiệm vụ hướng dẫn, giáo dục các cơ quan và công chúng về chia sẻ dữ liệu an toàn. Bên cạnh đó, Hội đồng Cố vấn Dữ liệu (*bao gồm đại diện chính phủ, chuyên gia và đại diện cộng đồng*) giúp đảm bảo tiếng nói đa dạng trong việc hoàn thiện chính sách. Mô hình này kết hợp giữa cơ quan nhà nước (*NDC*) với tham vấn bên ngoài (*Advisory Council*), phản ánh văn hóa quản trị cầu thị của Australia.

- Trung Quốc: Trung Quốc không lập một “ủy ban dữ liệu” riêng biệt nào; thay vào đó, họ sử dụng các cơ quan sẵn có: Ủy ban An ninh Quốc gia TW nắm quyền chỉ đạo vĩ mô, còn thực thi thì giao cho CAC (*thuộc Quốc vụ viện*) chủ trì về dữ liệu mạng, phối hợp với Bộ Công an và các bộ chuyên ngành. Tức là cách quản lý đa trung tâm: mỗi mảng có một cơ quan chính, nhưng tất cả dưới sự điều



phối của Ủy ban An ninh. Mô hình này phù hợp hệ thống chính trị Trung Quốc, nhưng có thể dẫn tới chồng chéo trong thực thi (*vì nhiều cơ quan cùng quản*). Trung Quốc cũng xây dựng các ủy ban/nhóm công tác về dữ liệu ở cấp địa phương để triển khai chính sách Luật An ninh Dữ liệu.

Tại Việt Nam, hiện tại giao cho Bộ Công an là cơ quan chủ trì quản lý nhà nước về dữ liệu (*trù quốc phòng, cơ yếu*). Trung tâm dữ liệu quốc gia cũng thuộc Bộ Công an. Ưu điểm là tập trung, thống nhất; nhược điểm là có thể khiến khôi tư nhân, đối tác quốc tế ngại khi cơ quan công an nắm dữ liệu dân sự. Ngoài ra, Việt Nam có Quỹ phát triển dữ liệu do Bộ Tài chính quản lý, có thể xem như công cụ hỗ trợ tài chính hơn là cơ quan quản lý.

3. Bài học kinh nghiệm quốc tế cho Việt Nam

Từ những so sánh trên, có thể rút ra một số bài học cho Việt Nam trong quản trị và phát triển tài nguyên dữ liệu:

- **Thứ nhất**, nâng cao năng lực bảo vệ dữ liệu cá nhân và dữ liệu quan trọng:

Đảm bảo thực thi nghiêm Luật Bảo vệ dữ liệu cá nhân 2025, Nghị định bảo vệ dữ liệu cá nhân (2023) và các quy định về an toàn hệ thống thông tin. Bài học từ các vụ rò rỉ dữ liệu lớn ở Trung Quốc (*dịch vụ cảnh sát, ứng dụng chat*) hay ở các công ty công nghệ toàn cầu: nếu không đầu tư đúng mức cho an ninh mạng, hậu quả rất nghiêm trọng. Việt Nam cần thúc đẩy việc tuân thủ tiêu chuẩn an ninh dữ liệu trong cả khu vực công và tư (*ví dụ áp dụng tiêu chuẩn ISO 27001, đào tạo nhân sự an ninh mạng...*).

- **Thứ hai**, minh bạch và cân bằng lợi ích:

Một điểm tinh tế là phải minh bạch với người dân về việc dữ liệu của họ được sử dụng cho mục đích gì, đồng thời cho họ thấy lợi ích từ việc chia sẻ dữ liệu. Liên minh Châu Âu triển khai data altruism dựa trên sự tin tưởng rằng dữ liệu cá nhân sẽ được dùng vì lợi ích chung (*nghiên cứu bệnh hiểm, cải thiện dịch vụ công...*). Việt Nam có thể học theo: truyền thông cho công chúng về lợi ích của



việc chia sẻ dữ liệu (*ví dụ đóng góp dữ liệu y tế ẩn danh để nghiên cứu dịch bệnh*), từ đó xây dựng văn hóa dữ liệu cởi mở nhưng có trách nhiệm.

- **Thứ ba**, phát triển nguồn nhân lực chuyên môn:

Các nước đều chú trọng đào tạo chuyên gia về quản trị dữ liệu, luật và công nghệ. Việt Nam cần đầu tư mạnh vào đào tạo đội ngũ cán bộ hiểu biết sâu về dữ liệu (*cả khía cạnh pháp lý lẫn kỹ thuật*) cho các cơ quan nhà nước. Đồng thời, cần có chế độ đãi ngộ thu hút chuyên gia giỏi từ khu vực tư nhân, nước ngoài tham gia vào xây dựng chính sách dữ liệu (*điều mà Điều 6 Luật Dữ liệu cũng đề cập: cơ chế thu hút nhân lực trình độ cao phát triển dữ liệu quốc gia*). Nếu không có nhân lực đủ tầm, rất khó quản lý một lĩnh vực mới phức tạp như dữ liệu.

- **Thứ tư**, hướng dẫn về ẩn danh hóa và chia sẻ dữ liệu an toàn: Để thúc đẩy tái sử dụng dữ liệu công mà không vi phạm riêng tư, cần có hướng dẫn kỹ thuật cụ thể: dữ liệu cá nhân công bố cần được ẩn danh ở mức nào; có thể dùng phương pháp pseudonymization (*thay định danh bằng mã*) để cho phép nghiên cứu mà vẫn bảo vệ danh tính không. Liên minh Châu Âu DGA gợi ý sử dụng môi trường xử lý an toàn, nghĩa là dữ liệu nhạy cảm không đưa cho bên ngoài trực tiếp mà cho phép nhà nghiên cứu chạy phân tích trong môi trường do cơ quan công cung cấp, không được tải dữ liệu gốc ra. Việt Nam có thể thiết lập cơ chế tương tự khi chia sẻ dữ liệu y tế, dân cư...: bên ngoài chỉ được kết quả đã tổng hợp, không thấy dữ liệu thô.

- **Thứ năm**, quy trình xin phép chia sẻ dữ liệu quan trọng/cốt lõi: Luật Dữ liệu cấm tùy tiện chuyển dữ liệu quan trọng ra nước ngoài, nhưng chưa nêu rõ quy trình thẩm định. Cần sớm ban hành văn bản hướng dẫn: ví dụ nếu doanh nghiệp muốn đưa dữ liệu khách hàng (*được coi là quan trọng*) cho công ty mẹ ở nước ngoài xử lý thì xin phép ai? Bao lâu có kết quả? Tiêu chí xét duyệt là gì? Sự rõ ràng này rất cần thiết để doanh nghiệp có thể tuân thủ mà không bị đình trệ hoạt động.

- **Thứ sáu**, Xây dựng khung pháp lý về chuyển giao dữ liệu xuyên biên giới linh hoạt và phù hợp thông lệ quốc tế:



Để hội nhập kinh tế số, Việt Nam phải tạo điều kiện cho dòng chảy dữ liệu hợp pháp đồng thời bảo vệ chủ quyền. Cơ chế “đánh giá mức độ bảo vệ tương đương” (*Adequacy*) Liên minh Châu Âu sử dụng công cụ công nhận quốc gia khác có luật bảo vệ dữ liệu đủ mạnh để cho phép dữ liệu cá nhân lưu chuyển tự do sang nước đó. Việt Nam có thể nghiên cứu áp dụng tương tự: Ví dụ: nếu một công ty Việt Nam muốn đưa dữ liệu sang Liên minh Châu Âu thì Liên minh Châu Âu đã có GDPR - ta có thể coi Liên minh Châu Âu là “đạt chuẩn” nên duyệt nhanh hơn. Ngược lại, Việt Nam cũng nên chủ động đánh giá một số đối tác lớn (*EU, Nhật, Hàn*) xem luật họ có tương đồng không, từ đó ký kết thỏa thuận công nhận lẫn nhau về bảo vệ dữ liệu. Điều này sẽ giảm thủ tục cho doanh nghiệp hai bên, tăng độ tin cậy khi trao đổi dữ liệu.

- **Thứ bảy**, xây dựng sẵn các điều khoản hợp đồng mẫu cho chuyển dữ liệu quốc tế:

Không phải lúc nào Chính phủ cũng ra quyết định ngay được, nên cách linh hoạt là ban hành bộ hợp đồng mẫu về bảo vệ dữ liệu khi chuyển ra nước ngoài (*tương tự bộ Standard Contractual Clauses của Liên minh Châu Âu*). Doanh nghiệp nếu áp dụng đúng hợp đồng mẫu này khi ký với đối tác nước ngoài thì coi như đáp ứng yêu cầu pháp lý, không cần xin phép từng trường hợp. Cách làm này giảm gánh nặng cho cả nhà nước lẫn doanh nghiệp, đồng thời đảm bảo doanh nghiệp nước ngoài cam kết tuân thủ chuẩn bảo vệ dữ liệu Việt Nam.

- **Thứ tám**, Gia nhập các thỏa thuận quốc tế về dữ liệu: Như tham gia Khung CBPR của APEC, nghiên cứu tham gia Công ước 108+ của Hội đồng Châu Âu về bảo vệ dữ liệu cá nhân... Những điều này thể hiện thiện chí của Việt Nam trong việc hài hòa với chuẩn mực quốc tế, giúp nâng uy tín và thu hút đầu tư.

- **Thứ chín**, phát triển thị trường dữ liệu gắn liền với bảo vệ quyền cá nhân: Cuối cùng, bài học cốt lõi là lòng tin của người dân và doanh nghiệp quyết định sự thành công của mọi chính sách dữ liệu. Do đó cần:



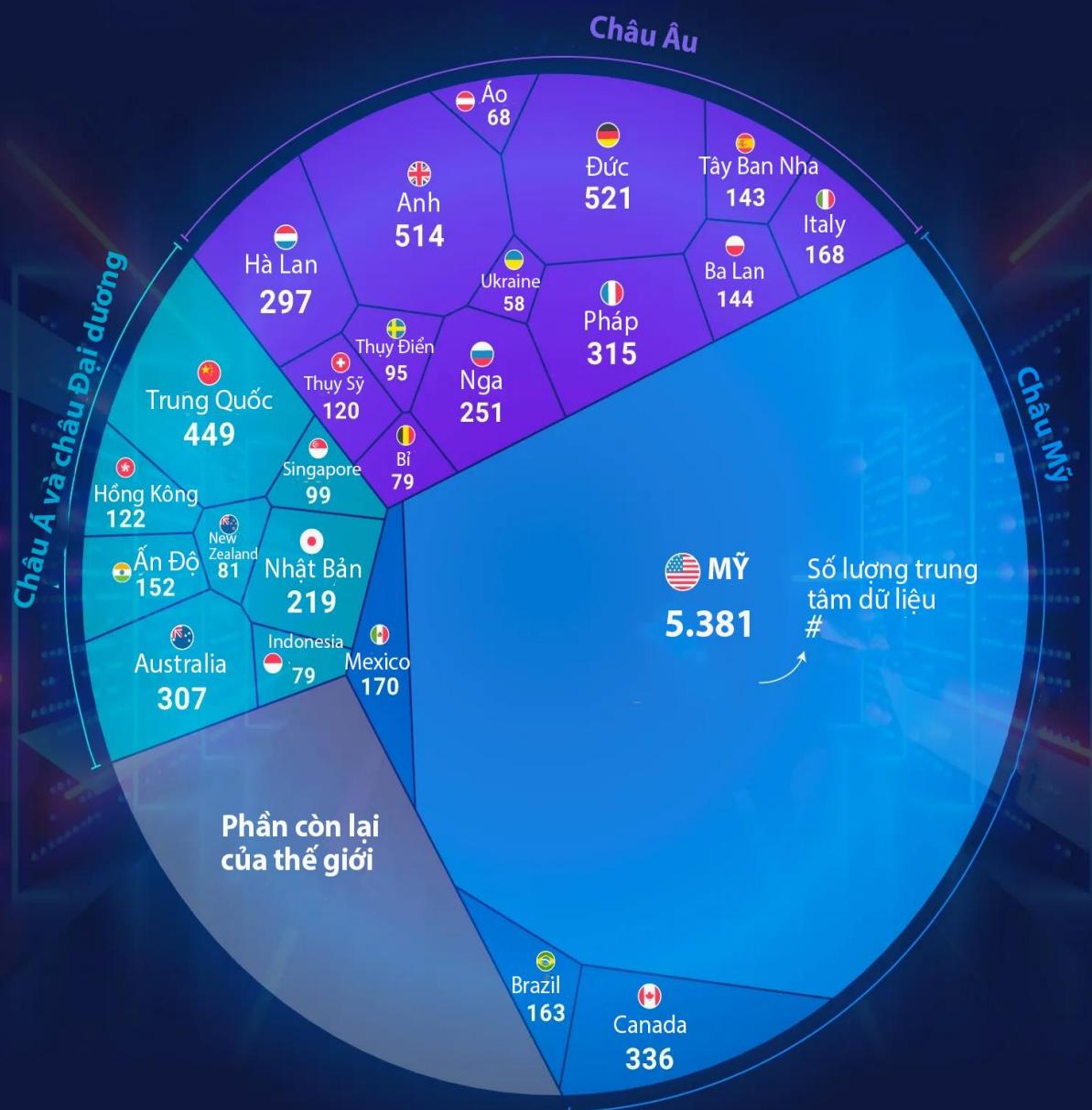
- + Tăng cường minh bạch, trách nhiệm giải trình: Mọi hoạt động thu thập, chia sẻ dữ liệu (*đặc biệt dữ liệu cá nhân*) cần được công khai về mục đích, phạm vi. Các cá nhân phải có quyền truy cập, hiệu đính, xóa dữ liệu của mình ở mức tối đa có thể (*theo tinh thần quyền chủ thể dữ liệu*). Cần thiết lập cơ chế để người dân khiếu nại hoặc khởi kiện nếu thấy quyền dữ liệu bị xâm phạm và cơ quan chức năng phải xử lý nhanh chóng, công bằng.
- + Nâng cao nhận thức và kỹ năng số cho cộng đồng: Một bài học từ các chiến dịch an ninh mạng phương Tây là giáo dục người dùng rất quan trọng. Việt Nam nên đưa nội dung về bảo vệ dữ liệu cá nhân vào chương trình giáo dục, tổ chức chiến dịch truyền thông giúp người dân hiểu giá trị dữ liệu và cách tự bảo vệ (*ví dụ cẩn trọng khi chia sẻ thông tin trên mạng, quyền từ chối cung cấp dữ liệu không cần thiết...*). Khi người dân hiểu biết, họ sẽ ủng hộ hơn các chính sách dữ liệu của nhà nước và hợp tác trong việc chia sẻ dữ liệu lợi ích chung.

- + Phát huy vai trò của Quỹ Phát triển Dữ liệu Quốc gia: Quỹ này có thể hỗ trợ tài chính cho các dự án số hóa dữ liệu, nghiên cứu giải pháp công nghệ bảo vệ dữ liệu (*VD: mã hóa đồng bộ, chia sẻ dữ liệu đảm bảo riêng tư - PETs*), hoặc tài trợ các sáng kiến data altruism trong nước (*nhiều xây dựng kho dữ liệu mở cho nghiên cứu khoa học*). Việc sử dụng quỹ phải công khai, minh bạch để đạt hiệu quả cao nhất.

Tóm lại, Việt Nam đang ở giai đoạn đầu xây dựng nền móng pháp lý cho nền kinh tế dữ liệu. Kinh nghiệm quốc tế từ những mô hình cân bằng bảo vệ và khai thác dữ liệu của Liên minh Châu Âu, Nhật Bản cho đến cách tiếp cận mạnh tay vì an ninh của Trung Quốc, hay sự thận trọng trong chia sẻ dữ liệu công của Australia đều cung cấp những bài học quý. Bằng cách chọn lọc áp dụng phù hợp với bối cảnh trong nước, Việt Nam có thể thiết kế được hệ thống quản trị dữ liệu hiệu quả, thúc đẩy chuyển đổi số và đổi mới sáng tạo, đồng thời bảo vệ vững chắc chủ quyền, an ninh và quyền lợi của người dân trong kỷ nguyên số.



THẾ GIỚI HIỆN CÓ 11.800 TRUNG TÂM DỮ LIỆU



Hình ảnh: Bản đồ phân tích, thống kê các trung tâm dữ liệu trên thế giới. Ảnh: Cloudscene, Stalista



PL2. Đấu tranh, phản bác các quan điểm sai trái, thù địch

1. Phản bác thông tin sai sự thật: “Việt Nam bắt chước Trung Quốc”

Trong thời gian qua, một số ý kiến cho rằng chính sách pháp luật về dữ liệu của Việt Nam đang “bắt chước Trung Quốc”, đi ngược lại các tiêu chuẩn quốc tế, xâm phạm quyền riêng tư và tự do ngôn luận của công dân, đồng thời thiếu minh bạch về pháp lý.

The screenshot shows a news article from NIKKEI Asia. The title is "Vietnam weighs new tech law that risks irking U.S. under Trump". Below the title, a sub-headline reads "Rules echoing China's may stymie tech giants and add to trade deficit". To the left of the main content area, there is a vertical column of social media sharing icons (X, f, s, e-mail, etc.). To the right of the main content area, there is a large image of the Vietnamese flag overlaid with a binary code pattern.

Hình ảnh: Tờ Nikkei Asia cho rằng Việt Nam ban hành Luật Dữ liệu là “học theo” Trung Quốc. Ảnh: Tác giả

Trái với lo ngại rằng Việt Nam đang mô phỏng cách tiếp cận “đóng cửa” Internet như Trung Quốc, thực tế pháp luật Việt Nam không hề cấm người dân truy cập các mạng xã hội toàn cầu như Facebook, Google, YouTube. Từ Luật An ninh mạng năm 2018 (*bị các thế lực thù địch công kích nhiều nhất*) đến Luật Dữ liệu 2024 mới đây, Việt Nam không đặt ra bất kỳ điều khoản nào nhằm chặn hay cấm đoán việc sử dụng dịch vụ Internet nước ngoài. Có thể nói rõ, quyền tự do ngôn luận của công dân luôn được đảm bảo... Các hoạt động liên lạc, trao đổi,



đăng tải, chia sẻ thông tin, mua bán, kinh doanh, thương mại vẫn diễn ra bình thường... miễn là những hoạt động đó không vi phạm pháp luật Việt Nam. Công dân Việt Nam được tự do làm những gì pháp luật không cấm trên không gian mạng, kể cả truy cập các trang mạng xã hội nước ngoài. Thực tế, chưa hề có chuyện Việt Nam chặn Facebook hay Google, ngược lại, Việt Nam yêu cầu các nhà mạng, nhà cung cấp dịch vụ phải có biện pháp để bảo vệ người dùng trên những nền tảng đó trước nguy cơ tội phạm mạng. Rõ ràng, Việt Nam không “đi theo” mô hình cực đoan như Trung Quốc; ngược lại chính sách Internet của Việt Nam khá cởi mở khi nằm trong nhóm 20 quốc gia có số lượng người dùng mạng xã hội đông đảo nhất thế giới. Điều này cho thấy pháp luật Việt Nam lựa chọn hướng quản lý cân bằng, vừa đảm bảo môi trường mạng tự do cho người dân, vừa đặt ra giới hạn với những hành vi vi phạm pháp luật hoặc lợi dụng không gian mạng để xâm hại lợi ích công cộng.

2. Vấn đề bản địa hóa dữ liệu

Một thông tin khác bị các đối tượng thường xuyên đưa lên công kích, việc Luật An ninh mạng, Luật Dữ liệu yêu cầu lưu trữ dữ liệu người dùng trong lãnh thổ Việt Nam (*data localization*) và đặt văn phòng đại diện đối với doanh nghiệp nước ngoài cung cấp dịch vụ tại Việt Nam. Một số ý kiến xem đây là bước đi “bắt chước Trung Quốc” và vi phạm cam kết hội nhập. Tuy nhiên, điều này không hề xa lạ trên thế giới. Nhiều quốc gia từ Hoa Kỳ, Đức, Pháp, Nga, Ấn Độ, cho tới Indonesia, Trung Quốc... đều có quy định về lưu trữ dữ liệu trong nước hoặc định danh dữ liệu tương tự. Thậm chí Nga đã ban hành Luật số 242-FZ từ năm 2006 yêu cầu dữ liệu cá nhân của công dân Nga phải được lưu trữ tại máy chủ trong nước. Liên minh châu Âu tuy không bắt buộc lưu trữ dữ liệu nội địa một cách rộng rãi, nhưng cũng có những hạn chế chuyển dữ liệu cá nhân ra ngoài EU nếu quốc gia nhận dữ liệu không đáp ứng tiêu chuẩn bảo mật (*theo chế độ “Adequacy” của GDPR*).



BBC NEWS TIẾNG VIỆT

Tin chính Việt Nam Thế giới Kinh tế Thể thao Video

Luật Dữ liệu: Bộ Công an thúc đẩy, doanh nghiệp lo ngại



GETTYIMAGES/VGP

Tin chính

Không ngừng bắn, không thỏa thuận: Thượng đỉnh Alaska có ý nghĩa gì với Trump, Putin và Ukraine?

4 giờ trước

Vụ thảm sát trước Thế chiến II vẫn ám ảnh quan hệ Trung – Nhật

5 giờ trước

Việt Nam và Hàn Quốc 'chốt đơn' 20 pháo tự hành K9 Thunder 250 triệu USD

15 tháng 8 năm 2025

BBC xuyên tạc các quy định của Luật Dữ liệu. Ảnh: Tác giả

Về mặt cam kết thương mại quốc tế, các chuyên gia pháp lý đã phân tích rằng quy định dữ liệu của Việt Nam không vi phạm các điều ước như Liên Hợp quốc (WTO) hay Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP). Điều khoản ngoại lệ về an ninh quốc gia trong CPTPP cho phép các nước có quyền áp dụng biện pháp cần thiết để bảo vệ lợi ích an ninh thiết yếu. Ngoài ra, trong chính CPTPP, Việt Nam còn được tạm hoãn thực thi một số nghĩa vụ về dòng chảy thông tin xuyên biên giới trong 2 năm sau khi Hiệp định có hiệu lực.

Nói cách khác, yêu cầu đặt máy chủ tại Việt Nam là phù hợp quyền bảo vệ an ninh quốc gia và đã được cân nhắc kỹ trong khuôn khổ ngoại lệ cho phép của các hiệp định quốc tế. Nếu những quy định như vậy “trái luật chơi” toàn cầu, hẳn các cường quốc như Mỹ hay Đức đã không thể ban hành các chính sách tương tự. Thực tiễn cho thấy, ngày nay khái niệm “chủ quyền dữ liệu” được nhiều nước coi trọng, đặc biệt trong bối cảnh bảo vệ thông tin cá nhân và an ninh mạng.

Chính sách bảo vệ dữ liệu của Việt Nam không những không đi ngược tiêu chuẩn quốc tế, mà thực tế chịu ảnh hưởng tích cực từ các mô hình tiến bộ như GDPR của EU. Xác định Việt Nam và EU “đã đặt ra các tiêu chuẩn tương tự để



bảo vệ dữ liệu cá nhân bên cạnh một số khác biệt cụ thể”. Chẳng hạn, cả GDPR và Nghị định 13/2023/NĐ-CP của Việt Nam (*văn bản tiền thân Luật Bảo vệ dữ liệu cá nhân*) đều dựa trên các nguyên tắc chung: tôn trọng quyền của chủ thẻ dữ liệu, yêu cầu minh bạch và sự đồng ý rõ ràng khi thu thập, xử lý dữ liệu cá nhân. Cả hai hệ thống đều đảm bảo các quyền cơ bản của người dùng: quyền được biết, quyền truy cập, quyền chỉnh sửa, quyền yêu cầu xóa, quyền rút lại sự đồng ý, v.v. – như GDPR quy định tại Điều 15–20 và Nghị định 13/2023/NĐ-CP của Việt Nam cũng có các điều khoản tương ứng. Chưa dừng ở đó, yêu cầu thông báo vi phạm dữ liệu cũng tương tự: GDPR bắt buộc thông báo sự cố cho cơ quan giám sát trong 72 giờ, Việt Nam theo Nghị định 13 cũng yêu cầu thông báo cho Bộ Công an và cá nhân bị ảnh hưởng khi xảy ra lộ lọt dữ liệu. Những điểm tương đồng này cho thấy Việt Nam tiếp thu tinh thần của GDPR trong việc đề cao quyền riêng tư và trách nhiệm giải trình.

Tuy nhiên, Việt Nam có đặc thù riêng trong cách tiếp cận quản lý dữ liệu, xuất phát từ bối cảnh chính trị, kinh tế và năng lực thực thi. Chẳng hạn, Hoa Kỳ hiện chưa có đạo luật bảo vệ dữ liệu cá nhân chung cấp liên bang, mà điều chỉnh thông qua nhiều đạo luật ngành (y tế, tài chính) và cơ chế tự điều tiết của doanh nghiệp. Điều này khác với Việt Nam ở chỗ Việt Nam muốn ban hành một đạo luật thống nhất về dữ liệu cá nhân. Còn tại Trung Quốc, chính quyền áp dụng các biện pháp mạnh tay hơn như xây dựng “tường lửa” kín, kiểm soát chặt chẽ nội dung thông tin và cấm nhiều nền tảng nước ngoài. So sánh để thấy, Việt Nam không áp dụng mô hình cực đoan của Trung Quốc; thay vào đó Việt Nam lựa chọn xây dựng khung pháp luật tiệm cận các chuẩn mực quốc tế (như quyền cá nhân kiểu GDPR) nhưng đồng thời phù hợp với điều kiện trong nước. Ví dụ, Luật Bảo vệ dữ liệu cá nhân của Việt Nam phân loại dữ liệu cá nhân thành cơ bản và nhạy cảm nhằm ưu tiên bảo vệ dữ liệu nhạy cảm (Điều 2 Dự thảo Luật). Về phạm vi áp dụng, GDPR có hiệu lực toàn cầu đối với bất kỳ ai xử lý dữ liệu công dân EU, còn quy định Việt Nam chủ yếu tập trung đối tượng trong nước và nhấn mạnh yêu cầu lưu trữ dữ liệu tại chỗ vì mục đích an ninh. Những khác biệt này phản ánh



bối cảnh và ưu tiên riêng, EU chú trọng thương mại tự do và quyền riêng tư cá nhân tuyệt đối (*ngoài ra cần phải làm rõ, trên thế giới hiện có hơn 11.000 trung tâm lưu trữ, trong đó 50% đặt tại Mỹ, khoảng 25% đặt tại Châu Âu*), trong khi Việt Nam ưu tiên hài hòa giữa bảo vệ quyền cá nhân với bảo vệ an ninh quốc gia, trật tự xã hội. Mặc dù cách thức có thể khác nhau, song mục tiêu chung của Việt Nam không nằm ngoài xu hướng thế giới, xây dựng môi trường số an toàn, đáng tin cậy cho người dân và doanh nghiệp.

3. Phản bác luận điệu xuyên tạc: “Vi phạm nhân quyền quốc tế”

Một số tổ chức và cá nhân chỉ trích luật dữ liệu của Việt Nam “vi phạm quyền con người” như quyền riêng tư, tự do ngôn luận. Cần khẳng định rằng Việt Nam luôn đề cao các giá trị quyền con người và tuân thủ các điều ước quốc tế về nhân quyền mà mình tham gia. Hiến pháp 2013 của Việt Nam ghi nhận rõ quyền tự do ngôn luận, tiếp cận thông tin, bảo vệ đời sống riêng tư của công dân (Điều 25 và Điều 21 Hiến pháp). Các đạo luật chuyên ngành như Bộ luật Dân sự 2015, Luật An toàn thông tin mạng 2015, Luật Tiếp cận thông tin 2016... đều cụ thể hóa những quyền này. Trong lĩnh vực an ninh mạng và dữ liệu, pháp luật Việt Nam luôn quán triệt nguyên tắc: bảo vệ an ninh quốc gia đi đôi với bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân. Ngay trong Điều 5 Luật Dữ liệu về Nguyên tắc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu, nêu rõ phải “tuân thủ Hiến pháp và pháp luật; bảo đảm... quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân”. Như đã phân tích, luật không cấm đoán hoạt động ngôn luận hay trao đổi thông tin bình thường của công dân. Những hành vi duy nhất bị ngăn chặn là lợi dụng việc xử lý dữ liệu để phạm tội, như tuyên truyền chống Nhà nước, tấn công mạng, lừa đảo... Đây là cách tiếp cận hợp lý và phù hợp Công ước quốc tế về các quyền dân sự, chính trị (ICCPR). Điều 19 ICCPR về tự do ngôn luận cho phép hạn chế quyền này để bảo vệ an ninh quốc gia, trật tự công cộng, sức khỏe hoặc đạo đức xã hội. Pháp luật Việt Nam chỉ giới hạn tự do ngôn luận ở những trường hợp cần thiết tương tự, chứ không “bóp nghẹt” tiếng nói của người dân như luận điệu xuyên tạc. Bằng chứng là Việt Nam có hơn 78 triệu người dùng



Internet, gần 73% dân số dùng mạng xã hội một cách sôi động, với hàng triệu ý kiến phản biện xã hội được nêu ra hàng ngày mà không hề bị ngăn cản. Nhà nước cũng khuyến khích người dân tham gia phản biện, góp ý chính sách trên môi trường mạng một cách xây dựng. Do đó, cáo buộc Việt Nam vi phạm tự do ngôn luận là thiếu cơ sở.



Submission to the United Nations Human Rights Committee During its Periodic Review of Vietnam under the ICCPR at its 144th Session

Between 2018 and April 2025, Vietnamese courts convicted and sentenced at least 128 people to harsh prison terms under article 331, including prominent lawyer [Tran Dinh Trien](#), influential blogger [Truong Huy San](#), and internet commentator [Nguyen Thai Hung](#). This is a significant increase over the previous six-year period (2011-2017), when 28 people were reportedly convicted and sentenced to prison for violating the predecessor to article 331.

Laws Restricting Internet Access

In November 2024, the Vietnamese government issued [Decree 147](#) to regulate the use and provision of internet services and online information. The decree expands government control over access to information on the internet for vaguely defined reasons of “national security” and “social order,” and to prevent transgressions of Vietnam’s “morals, beautiful customs, and traditions.” The authorities have extensively misused such legislation to repress political dissent. The decree requires social media platforms providing services to users in Vietnam to store user data, provide it to the authorities on demand, and take down anything the authorities consider “illegal content” within 24 hours.

Decree 147 includes other [problematic provisions](#). It requires owners of public internet access points, such as at hotels, restaurants, airports, and other public spaces, to prevent internet users from carrying out “propaganda against the state” or face unstated consequences. As a prerequisite for registering all .vn domain names, the decree requires the “exclusion of any phrases that violate national interests” and “phrases that can be easily mistaken for a press agency or press product if the registered users is not a press agency” and that they be “in accordance with social morality.”

HRW đưa thông tin sai sự thật về Nghị định 147/2024/NĐ-CP. Ảnh: Tác giả

- Về quyền riêng tư, Việt Nam coi trọng bảo vệ dữ liệu cá nhân không kém gì các nước dân chủ. Thời gian qua có những ý kiến hiểu lầm rằng cơ quan công an chủ trì xây dựng Luật Dữ liệu, Luật Bảo vệ Dữ liệu cá nhân là để “siết chặt kiểm soát” thông tin của dân. Thực tế hoàn toàn ngược lại, lần đầu tiên, Việt Nam ban hành một đạo luật đầy đủ về quyền dữ liệu cá nhân nhằm bảo vệ đời tư người dân trong kỷ nguyên số. Luật Bảo vệ dữ liệu cá nhân xác lập rõ các quyền của chủ thể dữ liệu, tức quyền của mỗi cá nhân đối với thông tin của mình. Theo Điều 4 của luật này, cá nhân có hàng loạt quyền cụ thể: “(a) Được biết về hoạt động xử lý dữ



liệu cá nhân; (b) Đồng ý hoặc không đồng ý, yêu cầu rút lại sự đồng ý cho phép xử lý dữ liệu của mình; (c) Xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân; (d) Yêu cầu cung cấp, xóa, hạn chế xử lý dữ liệu; phản đối việc xử lý dữ liệu cá nhân; (đ) Khiếu nại, tố cáo, khởi kiện, yêu cầu bồi thường thiệt hại...; (e) Yêu cầu cơ quan, tổ chức, cá nhân có liên quan thực hiện các biện pháp bảo vệ dữ liệu của mình theo quy định pháp luật". Những quyền này tương đồng với quyền của công dân EU dưới GDPR, bao gồm cả quyền được xóa dữ liệu ("quyền được lãng quên") và quyền phản đối xử lý dữ liệu. Việc luật Việt Nam công nhận các quyền trên cho thấy chính sách dữ liệu hoàn toàn không vi phạm quyền riêng tư, mà ngược lại nhằm tăng cường bảo vệ quyền riêng tư cho người dân. Tới đây, có thể khẳng định quan điểm "pháp luật dữ liệu Việt Nam xâm phạm nhân quyền" là không có cơ sở, bởi các đạo luật liên quan đều có điều khoản bảo đảm quyền con người, quyền công dân phù hợp Hiến pháp. Nhà nước Việt Nam luôn nhất quán nguyên tắc phát triển công nghệ gắn liền với tôn trọng quyền con người, như Nghị quyết 27-NQ/TW năm 2022 của Đảng đã nêu rõ: "lấy con người làm trung tâm... gắn bảo vệ dữ liệu cá nhân với bảo vệ quyền con người trong kỷ nguyên số"

4. Tính minh bạch trong chính sách và pháp luật dữ liệu

Các ý kiến tiêu cực thường cho rằng quá trình xây dựng chính sách dữ liệu ở Việt Nam thiếu minh bạch, văn bản pháp luật khó tiếp cận. Tuy nhiên, thực tế lại cho thấy sự minh bạch được chú trọng trên cả hai phương diện: (1) Minh bạch nội dung pháp luật, và (2) Minh bạch trong quá trình xây dựng chính sách.

Về nội dung, các luật và nghị định liên quan đến dữ liệu đều được công bố công khai, đăng tải rộng rãi trên cổng thông tin điện tử và các phương tiện thông tin đại chúng để người dân, doanh nghiệp biết và thực thi. Nguyên tắc minh bạch cũng được thể hiện ngay trong các quy định. Chẳng hạn, Luật An ninh mạng yêu cầu doanh nghiệp phải thông báo cho người dùng khi xảy ra sự cố lộ lọt dữ liệu người dùng. Luật Dữ liệu 2024 nêu rõ nguyên tắc số 2 là "bảo đảm công khai, minh bạch, bình đẳng trong tiếp cận, khai thác và sử dụng dữ liệu". Điều này có nghĩa là việc quản lý và chia sẻ dữ liệu ở Việt Nam phải được thực hiện minh



bạch, không được tùy tiện hay bí mật xâm phạm dữ liệu mà không có căn cứ pháp luật. Luật Bảo vệ dữ liệu cá nhân 2025 cũng yêu cầu cơ quan chuyên trách phải tiếp nhận và giải quyết các yêu cầu của công dân liên quan đến dữ liệu cá nhân một cách công khai, đúng hạn định. Như vậy, xuyên suốt các văn bản, tính minh bạch pháp lý luôn được đề cao, bác bỏ luận điệu cho rằng chính sách dữ liệu của Việt Nam mập mờ hay khuất tất.

Về quy trình chính sách, Việt Nam đã có nhiều hoạt động tham vấn, lấy ý kiến công khai trước khi ban hành các quy định quan trọng về dữ liệu. Điển hình, trong quá trình soạn thảo Luật Dữ liệu vừa qua, Bộ Công an và cơ quan liên quan đã tổ chức tọa đàm, hội thảo góp ý với sự tham gia của hiệp hội doanh nghiệp, chuyên gia, người dân.



Ngày 4 tháng 9 năm 2024

GÓP Ý CỦA BSA VỀ DỰ THẢO LUẬT DỮ LIỆU

Kính gửi: Bộ Công an

BSA | Liên minh Phần mềm (BSA)¹ xin cảm ơn Bộ Công an (Bộ CA) đã cho chúng tôi cơ hội được đóng góp ý kiến đối với dự thảo Luật Dữ Liệu. BSA là tổ chức vận động hàng đầu cho ngành công nghiệp phần mềm doanh nghiệp toàn cầu trước các chính phủ và trên thị trường quốc tế. Các thành viên của BSA là một trong những công ty sáng tạo nhất thế giới, tạo ra các giải pháp phần mềm có thể châm ngòi phát triển cho nền kinh tế.

Tại Việt Nam, BSA đã tích cực tham gia vào các hoạt động liên quan đến các quy định bảo vệ dữ liệu cá nhân và chuyển dữ liệu ra nước ngoài. Gần đây nhất, BSA đã trình bày quan điểm về việc xây dựng Luật Bảo Vệ Dữ Liệu Cá Nhân (Luật BVDLCN) tại Hội thảo của Bộ CA về Chính Sách Bảo Vệ Dữ Liệu Cá Nhân ngày 5 tháng 6 năm 2024 và đóng góp ý kiến về việc xây dựng Luật BVDLCN ngày 29 tháng 3 năm 2024.² BSA đã cho ý kiến về dự thảo Nghị định về Bảo Vệ Dữ Liệu Cá Nhân (Nghị định BVDLCN) trong tháng 4 năm 2021³ và tháng 6 năm 2023.⁴ Bên cạnh đó, BSA đã tham dự Hội thảo về Nghị Định Xử Phạt Hành Chính Trong Lĩnh Vực An Ninh Mạng do Bộ CA tổ chức vào tháng 11 năm 2022, đồng thời tích cực tham gia các hoạt động liên quan đến Luật An Ninh Mạng và các nghị định hướng dẫn thi hành. Chẳng hạn như góp ý của BSA về Nghị Định 53 vào tháng 9 năm 2022⁵ và ý

Góp ý Dự thảo Luật Dữ liệu của Liên minh phần mềm BSA.Ảnh:Tác giả



Trên thực tế, dự thảo Luật đã được chỉnh sửa nhiều điểm sau khi tiếp thu phản hồi. Những động thái này cho thấy tính minh bạch và cầu thị trong quá trình hoàn thiện chính sách pháp luật về dữ liệu tại Việt Nam. Các văn bản như Nghị định 53/2022/NĐ-CP hay Nghị định 13/2023/NĐ-CP trước khi ban hành đều đã trải qua bước đăng công khai dự thảo trên Công thông tin Chính phủ để lấy ý kiến nhân dân. Do đó, không thể nói rằng chính sách được ban hành một cách thiếu minh bạch hay không có sự tham gia của xã hội. Trái lại, Nhà nước đang nỗ lực hướng dẫn dư luận hiểu đúng và đóng góp vào quá trình xây dựng pháp luật dữ liệu, tránh những hiểu lầm và đồn đoán không đáng có.

Tóm lại, những luận điểm cho rằng chính sách dữ liệu của Việt Nam “sao chép Trung Quốc, đi ngược quốc tế, vi phạm nhân quyền, thiếu minh bạch” đều không phù hợp với thực tiễn lập pháp và thực thi. Việt Nam có cách tiếp cận riêng biệt nhưng hợp lý, vừa tham khảo kinh nghiệm quốc tế (như GDPR), vừa đảm bảo chủ quyền và lợi ích quốc gia. Các quy định đặt ra nhằm bảo vệ người dân và an ninh quốc gia trên không gian mạng, chứ không phải để hạn chế các quyền tự do chính đáng.

5. Phản bác luận điệu “Luật Dữ liệu - tập trung quyền lực, ảnh hưởng kinh tế, tự do cá nhân”

Một số ý kiến cho rằng việc giao nhiều thẩm quyền về dữ liệu cho Bộ Công an sẽ dẫn đến tập trung quyền lực, thiếu cơ chế kiểm soát độc lập, gây lo ngại lạm quyền. Tuy nhiên, nếu xem xét kỹ các quy định, có thể thấy phân công quản lý dữ liệu tại Việt Nam rất rõ ràng và có sự phân quyền hợp lý. Theo Luật Dữ liệu 2024, Chính phủ thống nhất quản lý nhà nước về dữ liệu, Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ về quản lý nhà nước lĩnh vực này (*trừ dữ liệu thuộc quốc phòng do Bộ Quốc phòng phụ trách*). Các bộ, cơ quan ngang bộ khác phối hợp với Bộ Công an trong phạm vi ngành mình quản lý và chịu trách nhiệm xây dựng cơ sở dữ liệu chuyên ngành. Ủy ban nhân dân cấp tỉnh cũng thực hiện quản lý nhà nước về dữ liệu tại địa phương. Như vậy, không có chuyện Bộ Công an “ôm hết” quyền lực dữ liệu.



Thay vào đó, luật định rõ đầu mối để tránh chồng chéo, nhưng đồng thời các bộ ngành và chính quyền địa phương đều có vai trò, trách nhiệm cụ thể. Bản thân Bộ Công an khi thực hiện nhiệm vụ cũng bị ràng buộc bởi luật. Ví dụ, cơ quan chuyên trách bảo vệ dữ liệu cá nhân (*thuộc Bộ Công an*) có trách nhiệm tiếp nhận, giải quyết khiếu nại của người dân về dữ liệu; phải tuân thủ thời hạn luật định khi người dân yêu cầu thực hiện quyền dữ liệu của họ. Điều này tạo ra cơ chế buộc cơ quan quản lý phải công khai, minh bạch và chịu sự giám sát của xã hội. Bên cạnh đó, Quốc hội với vai trò lập pháp và giám sát tối cao hoàn toàn có thể chất vấn, yêu cầu báo cáo về việc thực thi luật dữ liệu, đảm bảo không có lạm quyền. Mô hình Việt Nam chọn (*cơ quan bảo vệ dữ liệu trực thuộc Chính phủ*) thực ra không hiếm trên thế giới: ví dụ Singapore, Hàn Quốc cũng giao việc bảo vệ dữ liệu cá nhân cho cơ quan thuộc Chính phủ (*Ủy ban PDPC ở Singapore thuộc Bộ Truyền thông, Ủy ban PIPC ở Hàn Quốc trực thuộc Thủ tướng*). Điểm chung là dù trực thuộc hành pháp, các cơ quan này hoạt động theo luật định và phải chịu trách nhiệm trước người dân. Vì vậy, lo ngại “tập trung quyền lực” là thiếu căn cứ nếu hiểu đúng cơ chế phân công và giám sát đã được luật hóa.

Về tác động đối với nền kinh tế, một số doanh nghiệp lo ngại chi phí tuân thủ luật dữ liệu mới có thể gia tăng, ảnh hưởng đến hoạt động kinh doanh. Nhưng cần nhìn dài hạn, bảo vệ dữ liệu tốt sẽ tạo niềm tin số, từ đó thúc đẩy kinh tế số phát triển bền vững. Bài học từ châu Âu cho thấy sau khi GDPR có hiệu lực, dù doanh nghiệp ban đầu gặp khó khăn tuân thủ, nhưng về lâu dài môi trường thị trường trở nên lành mạnh, người dùng tin tưởng dịch vụ số hơn, giúp kinh tế số tăng trưởng mạnh mẽ. Việt Nam cũng kỳ vọng tương tự, Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân đánh dấu bước tiến lớn trong việc hoàn thiện cơ chế thực thi quyền dữ liệu, áp dụng chế tài nghiêm khắc để “nâng cao niềm tin của người dân và doanh nghiệp vào môi trường số”. Mục tiêu cuối cùng là tạo nền móng pháp lý vững chắc để nền kinh tế số Việt Nam tiếp tục tăng trưởng nhanh nhưng an toàn. Trên thực tế, nhiều doanh nghiệp công nghệ trong nước đã ủng hộ việc sớm có luật dữ liệu và luật dữ liệu cá nhân, vì họ hiểu rằng luật sẽ giúp chống nạn cạnh



tranh không lành mạnh qua việc mua bán dữ liệu, đồng thời nâng cao uy tín của doanh nghiệp trong mắt khách hàng.

Còn về tự do cá nhân, như nội dung phân tích ở trên, pháp luật dữ liệu nhằm tới bảo vệ người dân, chỉ hạn chế những hành vi lạm dụng tự do để xâm phạm người khác. Luật không tước đi quyền tự do ngôn luận hay riêng tư, mà trao cho cá nhân công cụ pháp lý để tự bảo vệ mình (*quyền biệt, quyền yêu cầu xóa dữ liệu...*). Đa số người dân và doanh nghiệp chân chính đều đồng tình và phản khởi trước các chính sách này, bởi họ nhận thấy lợi ích thiết thực: ít bị lừa đảo hơn, dữ liệu được an toàn hơn, môi trường mạng văn minh hơn.

Những ai phản đối gay gắt thường rơi vào hai nhóm: ⁽¹⁾nhóm lợi dụng kẽ hở ẩn danh để làm điều sai trái, nên sợ bị luật mới “lôi ra ánh sáng”; ⁽²⁾nhóm chưa hiểu đúng tinh thần luật, lo sợ thái quá do ảnh hưởng thông tin sai lệch. Do đó, nhiệm vụ của chúng ta là tiếp tục tuyên truyền, giải thích để người dân hiểu rằng quyền lợi hợp pháp của họ luôn được pháp luật tôn trọng và bảo vệ, còn luật dữ liệu sinh ra để chống lại những hành vi vi phạm quyền lợi đó.

Từ những phân tích trên, có thể kết luận rằng các thông tin cho rằng chính sách pháp luật về dữ liệu của Việt Nam “mô phỏng Trung Quốc, đi ngược tiêu chuẩn quốc tế, vi phạm quyền riêng tư, tự do ngôn luận, thiếu minh bạch, tập trung quyền lực, gây hại cho kinh tế và tự do cá nhân” đều là nhận định thiếu khách quan và không đúng với thực tế. Trái lại, Việt Nam đang dần định hình một khung pháp luật về dữ liệu phù hợp với xu hướng toàn cầu nhưng vẫn phản ánh bản sắc và nhu cầu trong nước. Chúng ta tiếp thu những nguyên tắc tiên bộ như trong GDPR để bảo vệ quyền của người dân, đồng thời đề cao yếu tố chủ quyền và an ninh dữ liệu quốc gia như nhiều nước đang làm. Pháp luật dữ liệu của Việt Nam không nhằm hạn chế quyền con người, mà để tạo môi trường an toàn hơn cho việc thực thi các quyền đó trong không gian mạng. Quá trình xây dựng luật được tiến hành thận trọng, minh bạch, có sự đóng góp của nhiều bên. Những điều chỉnh chính sách linh hoạt cho thấy Nhà nước luôn lắng nghe ý kiến xã hội, bảo đảm luật khi ban hành vừa nghiêm minh vừa khai thi, đem lại lợi ích chung.



Ngày 4 tháng 9 năm 2024

GÓP Ý CỦA LIÊN MINH DỮ LIỆU TOÀN CẦU VỀ DỰ THẢO LUẬT DỮ LIỆU

Liên minh Dữ liệu Toàn cầu (GDA) xin cảm ơn Bộ Công an (BCA) đã cho chúng tôi cơ hội được đóng góp ý kiến đối với dự thảo Luật Dữ Liệu.

GDA là một liên minh liên ngành của các công ty, có trụ sở tại các khu vực khác nhau trên thế giới, cam kết các tiêu chuẩn cao về quyền riêng tư và bảo mật dữ liệu. GDA hỗ trợ các chính sách giúp thấm nhuần niềm tin vào nền kinh tế kỹ thuật số mà không áp đặt các hạn chế dữ liệu xuyên biên giới quá mức hoặc các yêu cầu bản địa hóa làm suy yếu an ninh dữ liệu, an ninh mạng, đổi mới, phát triển kinh tế và thương mại quốc tế. Với sự tập trung của GDA vào dữ liệu xuyên biên giới, chúng tôi bình luận cụ thể về các khía cạnh dữ liệu xuyên biên giới trong dự thảo Luật Dữ Liệu.

Chúng tôi hy vọng rằng những đề xuất này sẽ giúp BCA hoàn thiện dự thảo Luật Dữ Liệu.¹ Chúng tôi hy vọng sẽ đóng vai trò như một nguồn lực của BCA khi Quý Bộ xây dựng một khuôn khổ quản trị dữ liệu toàn diện và mạnh mẽ tại Việt Nam, có khả năng tương thích với các thông lệ quốc tế tốt nhất, đặc biệt là liên quan đến chuyển dữ liệu xuyên biên giới và hỗ trợ sự phát triển của nền kinh tế kỹ thuật số sôi động và sáng tạo.

Góp ý của Liên minh Dữ liệu toàn cầu (GDA). Ánh: Tác giả

Trong kỷ nguyên số, dữ liệu thực sự đã trở thành tài sản quý giá. Việc quản trị dữ liệu hiệu quả, công bằng và an toàn là bài toán mà mọi quốc gia phải giải. Việt Nam không phải ngoại lệ, và chúng ta đang chọn cách tiếp cận chủ động bằng việc hoàn thiện hệ thống pháp luật. Đây là nền tảng để Việt Nam vươn lên trong kinh tế số, đồng thời bảo vệ vững chắc an ninh quốc gia và quyền lợi của người dân trên không gian mạng. Bất cứ chính sách nào cũng có thể gặp phải hiểu lầm ban đầu, nhưng bằng lập luận logic, bằng chứng pháp lý và thực tiễn như đã trình bày, có thể tin rằng dư luận sẽ dần nhận thức đúng đắn hơn về bản chất tích cực của chính sách pháp luật dữ liệu ở nước ta. Việt Nam không “đi ngược” dòng chảy, mà đang nỗ lực sánh bước cùng thế giới trong việc xây dựng một tương lai số an toàn, nhân văn và thịnh vượng.



TÀI LIỆU THAM KHẢO

* Tài liệu trong nước:

1. Luật Dữ liệu (*Luật số 60/2024/QH15*);
2. Luật Bảo vệ dữ liệu cá nhân (*Luật số 91/2025/QH15*);
3. Nghị quyết 36-NQ/TW ngày 01/7/2014 của Bộ Chính trị (*Khóa XI*) về đẩy mạnh ứng dụng, phát triển CNTT phục vụ phát triển bền vững và hội nhập quốc tế;
4. Nghị quyết số 03/NQ-CP ngày 09/01/2025 của Chính phủ về Chương trình hành động thực hiện NQ 57-NQ/TW về chuyển đổi số quốc gia;
5. Nghị định 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều của Luật Dữ liệu;
6. Quyết định 942/QĐ-TTg ngày 15/6/2021 của Thủ tướng Chính phủ phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số 2021-2025, định hướng 2030.
7. Nghị định 47/2024/NĐ-CP ngày 09/5/2024 về danh mục Cơ sở dữ liệu Quốc gia; xây dựng, cập nhật, duy trì, khai thác, sử dụng Cơ sở dữ liệu Quốc gia

* Tài liệu nước ngoài:

1. Australia, Đạo luật Khả dụng và Minh bạch Dữ liệu 2022 (*DAT*);
2. Hàn Quốc, Luật Bảo vệ Thông tin Cá nhân 2011 (*PIPA*);
3. Liên minh Châu Âu, Đạo luật Quản trị Dữ liệu 2022 (*DGA*);
4. Liên minh Châu Âu, Quy định Bảo vệ Dữ liệu Chung 2016 (*GDPR*);
5. Mỹ, Đạo Luật Dữ liệu Chính phủ mở 2018 (*OGDA*);
6. Nhật Bản, Luật Bảo vệ Thông tin Cá nhân 2003 (*APPI*) SĐBS 2020;
7. Nhật Bản, Luật Cơ bản về Thúc đẩy Sử dụng Dữ liệu Công - Tư 2016;
8. Singapore, Đạo luật Bảo vệ Dữ liệu Cá nhân 2012 (*PDPA*);
9. Trung Quốc, Luật An ninh Dữ liệu 2021 (*DSL*);
10. Trung Quốc, Luật Bảo vệ Thông tin Cá nhân 2021 (*PIPL*).



Câu 2: Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước?





Câu 2: Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước?

Trả lời

2.1. Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu

2.1.1. Chủ thể dữ liệu

2.1.1.1. Khái niệm Chủ thể dữ liệu

Chủ thể dữ liệu được định nghĩa tại Khoản 12 Điều 3 Luật Dữ liệu 2024 là “cơ quan, tổ chức, cá nhân được dữ liệu phản ánh”. Nói cách khác, đây là đối tượng mà thông tin dữ liệu mô tả hoặc phản ánh, ví dụ như cá nhân mà dữ liệu cá nhân đề cập, hay một tổ chức mà dữ liệu về tổ chức đó thể hiện. Về đặc điểm pháp lý, chủ thể dữ liệu có thể bao gồm cả chủ thể dữ liệu cá nhân (*một cá nhân cụ thể có dữ liệu liên quan đến mình*) và chủ thể dữ liệu không phải cá nhân (*cơ quan, tổ chức được dữ liệu đề cập*). Chủ thể dữ liệu nằm ở trung tâm của hệ sinh thái dữ liệu vì dữ liệu được thu thập, xử lý chính là về họ hoặc gắn liền với họ.

Với vai trò là đối tượng được dữ liệu phản ánh, chủ thể dữ liệu đặc biệt (*nhất là cá nhân*) được pháp luật bảo vệ quyền lợi. Trong hệ sinh thái dữ liệu, họ là bên cung cấp thông tin đầu vào (*dữ liệu được tạo ra từ hoạt động của họ hoặc từ thông tin về họ*) và cũng là bên chịu tác động từ việc dữ liệu đó được thu thập, sử dụng. Pháp luật hiện hành (*đặc biệt trong lĩnh vực bảo vệ dữ liệu cá nhân*) coi trọng việc trao cho chủ thể dữ liệu các quyền nhằm kiểm soát dữ liệu của mình, đồng thời đặt ra các nghĩa vụ cho họ để đảm bảo môi trường dữ liệu an toàn, trung thực. Chủ thể dữ liệu cá nhân có vị trí trung tâm về quyền riêng tư: họ được trao nhiều quyền nhân thân liên quan đến dữ liệu (*quyền được biết, đồng ý, yêu cầu xóa dữ liệu,...*). Chủ thể dữ liệu doanh nghiệp hoặc cơ quan nhà nước tuy không thuộc phạm vi luật bảo vệ dữ liệu cá nhân, nhưng vẫn là đối tượng mà dữ liệu đề cập và cũng có lợi ích cần được bảo vệ (*như bí mật kinh doanh, dữ liệu nội bộ...*). Tóm lại, chủ thể dữ liệu là khái niệm rộng, bao gồm mọi cá nhân/tổ chức mà dữ liệu nói về, đóng vai



trò là đối tượng cuối cùng mà các hoạt động xử lý dữ liệu hướng tới và cần cân bằng giữa khai thác dữ liệu với quyền và lợi ích hợp pháp của họ.

2.1.1.2. Quyền, nghĩa vụ của chủ thể dữ liệu

Chủ thể dữ liệu, đặc biệt là chủ thể dữ liệu cá nhân được pháp luật Việt Nam trao cho nhiều quyền quan trọng nhằm bảo vệ thông tin của mình, đồng thời họ cũng có những nghĩa vụ nhất định khi cung cấp dữ liệu. Luật Bảo vệ dữ liệu cá nhân 2025 (*Luật số 91/2025/QH15*) và Nghị định 13/2023/NĐ-CP đã quy định cụ thể các quyền và nghĩa vụ của chủ thể dữ liệu cá nhân.

** Quyền của chủ thể dữ liệu:*

Điều 9 Nghị định 13/2023/NĐ-CP, chủ thể dữ liệu có 11 quyền cơ bản liên quan đến dữ liệu cá nhân của mình và Khoản 1 Điều 4 Luật Bảo vệ dữ liệu cá nhân 2025 sau đó cũng xác định các quyền tương tự (*gồm 06 điểm, được liệt kê từ điểm a đến điểm e*). Các quyền chính bao gồm:

- **Thứ nhất**, quyền được biết về hoạt động xử lý dữ liệu cá nhân: Chủ thể dữ liệu có quyền được thông báo và biết về hoạt động xử lý dữ liệu cá nhân của mình. Ví dụ: họ phải được biết ai thu thập dữ liệu của họ, mục đích gì.
- **Thứ hai**, quyền đồng ý hoặc không đồng ý, yêu cầu rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân: Chủ thể dữ liệu có quyền đồng ý hoặc không đồng ý cho phép xử lý dữ liệu cá nhân của mình và có thể rút lại sự đồng ý bất kỳ lúc nào (*trừ một số trường hợp luật định ngoại lệ, như xử lý không cần sự đồng ý của chủ thể dữ liệu theo Điều 17 Nghị định 13/2023/NĐ-CP*).
- **Thứ ba**, quyền xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân: Chủ thể dữ liệu có quyền truy cập để xem dữ liệu cá nhân về mình và yêu cầu chỉnh sửa nếu dữ liệu không chính xác hoặc không cập nhật. Điều này đảm bảo dữ liệu cá nhân được duy trì chính xác, đầy đủ.
- **Thứ tư**, quyền yêu cầu cung cấp, xóa, hạn chế xử lý dữ liệu cá nhân; gửi yêu cầu phản đối xử lý dữ liệu cá nhân



+ Quyền xóa dữ liệu: Chủ thể dữ liệu có quyền xóa hoặc yêu cầu xóa dữ liệu cá nhân của mình khi mục đích xử lý đã hoàn thành hoặc khi họ rút lại sự đồng ý, trừ trường hợp pháp luật có quy định khác.

+ Quyền hạn chế xử lý: Chủ thể dữ liệu có quyền yêu cầu hạn chế việc xử lý dữ liệu cá nhân của mình trong những trường hợp nhất định (*ví dụ tạm ngừng xử lý cho đến khi dữ liệu được chỉnh sửa xong, hoặc khi đang giải quyết khiếu nại về việc xử lý sai*). Khi nhận yêu cầu, bên xử lý phải thực hiện trong 72 giờ trừ trường hợp luật khác có quy định.

+ Quyền cung cấp dữ liệu (*data portability*): Chủ thể dữ liệu được quyền yêu cầu bên kiểm soát dữ liệu cung cấp cho mình một bản sao dữ liệu cá nhân của họ. Quyền này cho phép cá nhân chuyển dữ liệu của mình sang đơn vị khác hoặc tự lưu giữ.

+ Quyền phản đối việc xử lý dữ liệu: Chủ thể dữ liệu có quyền phản đối việc một bên kiểm soát dữ liệu xử lý dữ liệu cá nhân của mình trong một số mục đích nhất định - chẳng hạn họ có thể phản đối việc sử dụng dữ liệu cho mục đích quảng cáo, tiếp thị hoặc để ngăn chặn việc tiết lộ dữ liệu. Bên kiểm soát phải ngừng hoặc hạn chế xử lý trong 72 giờ nếu nhận được phản đối hợp lệ.

- **Thứ năm**, quyền khiếu nại, tố cáo, khởi kiện, yêu cầu bồi thường thiệt hại theo quy định của pháp luật:

+ Quyền khiếu nại, tố cáo và khởi kiện: Nếu cho rằng quyền lợi của mình bị xâm phạm, chủ thể dữ liệu có quyền khiếu nại đến cơ quan có thẩm quyền, tố cáo hành vi vi phạm, hoặc khởi kiện ra tòa án để bảo vệ quyền lợi. Đây là các quyền pháp lý nhằm đảm bảo việc thực thi các quy định bảo vệ dữ liệu.

+ Quyền yêu cầu bồi thường thiệt hại: Cùng với quyền khởi kiện, chủ thể dữ liệu có thể yêu cầu bồi thường thiệt hại nếu có tổn thất do việc vi phạm quy định bảo vệ dữ liệu cá nhân gây ra. Quyền này tuân theo quy định chung của pháp luật dân sự về bồi thường ngoài hợp đồng.

- **Thứ sáu**, quyền yêu cầu cơ quan có thẩm quyền hoặc cơ quan, tổ chức, cá nhân liên quan đến xử lý dữ liệu cá nhân thực hiện các biện pháp, giải pháp



bảo vệ dữ liệu cá nhân của mình theo quy định của pháp luật: Chủ thể dữ liệu có quyền tự mình thực hiện các biện pháp bảo vệ dữ liệu cá nhân của mình, cũng như yêu cầu cơ quan có thẩm quyền bảo vệ quyền dân sự cho mình. Ví dụ: họ có thể sử dụng các biện pháp kỹ thuật để bảo vệ dữ liệu, hoặc nhờ đến cơ quan quản lý (Cục An ninh mạng và PCTP sử dụng công nghệ cao - Bộ Công an) để can thiệp khi cần thiết.

So với Nghị định 13/2023/NĐ-CP, Luật Bảo vệ dữ liệu cá nhân 2025 gộp quyền “được cung cấp, xóa, hạn chế, phản đối” vào cùng nhóm và bổ sung quyền yêu cầu cơ quan, tổ chức có thẩm quyền áp dụng biện pháp bảo vệ dữ liệu cho mình. Nhìn chung, các quyền này tương đồng với 11 quyền trong Nghị định 13/2023/NĐ-CP, chỉ khác về cách phân nhóm.



Hình ảnh: hội nghị phổ biến, hướng dẫn Nghị định số 13/2003/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân. Ảnh: Báo Nhân dân

* Nghĩa vụ của chủ thể dữ liệu:

Bên cạnh các quyền trên, chủ thể dữ liệu cũng phải thực hiện một số nghĩa vụ do pháp luật quy định nhằm đảm bảo tính trung thực và an toàn của hệ sinh thái dữ liệu. Điều 10 Nghị định 13/2023/NĐ-CP và Khoản 2 Điều 4 Luật Bảo vệ dữ liệu cá nhân 2025 liệt kê các nghĩa vụ chính như sau:



Thứ nhất, tự bảo vệ dữ liệu cá nhân của mình: Chủ thể dữ liệu có trách nhiệm chủ động bảo vệ thông tin của bản thân - ví dụ: giữ bí mật thông tin cá nhân nhạy cảm, thận trọng khi cung cấp dữ liệu cho người khác, sử dụng các công cụ bảo mật (*mật khẩu, mã hóa cá nhân...*) nếu có thể.

- **Thứ hai**, tôn trọng, bảo vệ dữ liệu cá nhân của người khác: Chủ thể dữ liệu phải tôn trọng và bảo vệ dữ liệu cá nhân của người khác. Điều này nghĩa là cá nhân không được xâm phạm quyền riêng tư dữ liệu của người khác, không thu thập hay sử dụng dữ liệu người khác một cách trái phép.

- **Thứ ba**, cung cấp thông tin chính xác, trung thực: Khi đồng ý cung cấp dữ liệu cá nhân của mình cho bên xử lý, chủ thể dữ liệu phải cung cấp đầy đủ và chính xác dữ liệu đó. Đây là nghĩa vụ trung thực, không giả mạo, không cung cấp sai thông tin về bản thân. Ví dụ: khi đăng ký tài khoản hay thực hiện giao dịch, cá nhân phải dùng thông tin đúng của mình; việc sử dụng thông tin giả mạo có thể vừa vi phạm nghĩa vụ, vừa gây rủi ro pháp lý.

- **Thứ tư**, chấp hành pháp luật về bảo vệ dữ liệu cá nhân: Chủ thể dữ liệu cần tuân thủ các quy định pháp luật hiện hành về bảo vệ dữ liệu, đồng thời tham gia vào việc phòng chống các hành vi vi phạm (ví dụ: *kịp thời tố giác nếu phát hiện vụ việc rò rỉ dữ liệu cá nhân, hợp tác với cơ quan chức năng điều tra vi phạm...*). Luật Bảo vệ dữ liệu cá nhân 2025 yêu cầu chủ thể dữ liệu không được lạm dụng quyền của mình để cản trở bát hợp lý hoạt động hợp pháp của bên kiểm soát dữ liệu và không xâm phạm quyền, lợi ích hợp pháp của người khác khi thực hiện quyền dữ liệu.

Nhìn chung, chủ thể dữ liệu có bộ quyền năng mạnh mẽ để kiểm soát dữ liệu cá nhân, nhưng cũng phải có ý thức trách nhiệm bảo vệ dữ liệu cho mình và tôn trọng dữ liệu của người khác. Điều này nhằm tạo ra một môi trường an toàn, dữ liệu cá nhân được xử lý minh bạch, có sự đồng ý, cá nhân có công cụ pháp lý để tự vệ hoặc đòi hỏi sự công bằng. Ngược lại, cá nhân cũng cần hành động trung thực, tuân thủ pháp luật để hỗ trợ các bên kiểm soát dữ liệu vận hành đúng đắn, cũng như góp phần ngăn chặn hành vi vi phạm (ví dụ: *không tiếp tay cho mua bán*



dữ liệu cá nhân của người khác, không cần trở doanh nghiệp thực hiện nghĩa vụ pháp lý về dữ liệu).

2.1.2. Chủ sở hữu dữ liệu

2.1.2.1. Khái niệm chủ sở hữu dữ liệu

Chủ sở hữu dữ liệu được Luật Dữ liệu 2024 lần đầu tiên công nhận như một chủ thể pháp lý có quyền tài sản đối với dữ liệu. Theo Khoản 14 Điều 3 Luật Dữ liệu 2024, chủ sở hữu dữ liệu là “*cơ quan, tổ chức, cá nhân có quyền quyết định việc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng và trao đổi giá trị của dữ liệu do mình sở hữu*”. Như vậy, chủ sở hữu dữ liệu có toàn quyền định đoạt đối với dữ liệu thuộc sở hữu của mình; từ việc tạo lập, thu thập dữ liệu, tổ chức quản trị dữ liệu, cho đến khai thác, sử dụng dữ liệu đó và trao đổi giá trị (ví dụ: *mua bán, chuyển giao, chia sẻ dữ liệu vì lợi ích kinh tế*). Luật cũng khẳng định tại Khoản 15 Điều 3 rằng quyền của chủ sở hữu dữ liệu đối với dữ liệu là một loại quyền tài sản theo quy định pháp luật dân sự. Điều này có nghĩa dữ liệu được nhìn nhận như một loại tài sản vô hình và chủ sở hữu dữ liệu có các quyền tài sản như chiếm hữu, sử dụng, định đoạt dữ liệu tương tự như đối với các tài sản khác theo Bộ luật Dân sự.

Về đặc điểm pháp lý, quyền sở hữu dữ liệu là một khái niệm mới và có phần nhạy cảm. Trước đây, pháp luật Việt Nam (ví dụ Nghị định 13/2023/NĐ-CP và các luật về bảo vệ dữ liệu cá nhân) không thừa nhận “quyền sở hữu” của cá nhân đối với dữ liệu cá nhân của chính họ. Thay vào đó, cá nhân chỉ có các quyền nhân thân liên quan đến dữ liệu, còn doanh nghiệp/đơn vị thu thập dữ liệu thường được coi là bên kiểm soát dữ liệu chứ chưa được gọi là “chủ sở hữu”. Sự xuất hiện của khái niệm chủ sở hữu dữ liệu trong Luật Dữ liệu 2024 cho phép một tổ chức, cá nhân sở hữu tập hợp dữ liệu (*bao gồm cả dữ liệu phi cá nhân và dữ liệu cá nhân đã được hợp pháp thu thập*) và có quyền tài sản đầy đủ đối với tập dữ liệu đó. Tuy nhiên, khái niệm này cũng đặt ra câu hỏi: trong trường hợp dữ liệu cá nhân, công ty thu thập dữ liệu có thể là chủ sở hữu dữ liệu theo Luật Dữ liệu, nhưng vẫn phải tôn trọng các quyền của chủ thể dữ liệu cá nhân theo Luật Bảo vệ dữ liệu cá nhân.



Chủ sở hữu dữ liệu là người có quyền kiểm soát cao nhất đối với dữ liệu. Họ quyết định mục đích và phương thức xử lý dữ liệu, quyết định ai được truy cập, chia sẻ dữ liệu và có thể định giá, khai thác dữ liệu về mặt kinh tế. Đây có thể là chủ thể công (*cơ quan nhà nước sở hữu các cơ sở dữ liệu quốc gia*) hoặc tư (*doanh nghiệp sở hữu dữ liệu khách hàng, dữ liệu giao dịch...*). Chủ sở hữu dữ liệu cung cấp định hướng và nguồn lực cho việc quản lý dữ liệu và thường sẽ giao cho chủ quản dữ liệu thực hiện việc vận hành kỹ thuật. Dữ liệu trở thành tài sản của chủ sở hữu, do đó họ có động lực bảo vệ dữ liệu khỏi mất mát, lạm dụng, đồng thời có trách nhiệm trước pháp luật về việc tuân thủ các quy định khi khai thác dữ liệu đó (*đặc biệt là dữ liệu cá nhân, dữ liệu nhạy cảm*).

2.1.2.2. Quyền, nghĩa vụ và trách nhiệm của chủ sở hữu dữ liệu

Chủ sở hữu dữ liệu có vị thế là chủ thể có quyền tài sản đối với dữ liệu, do đó pháp luật trao cho họ nhiều quyền để khai thác giá trị của dữ liệu, đồng thời yêu cầu họ thực hiện nghĩa vụ nhằm sử dụng dữ liệu một cách có trách nhiệm, tuân thủ pháp luật.



Facebook là chủ sở hữu dữ liệu người sử dụng cực lớn. Ảnh: fourthwall

*** Quyền của chủ sở hữu dữ liệu:**

Như đã nêu, Luật Dữ liệu 2024 khẳng định quyền của chủ sở hữu dữ liệu là quyền tài sản dân sự. Cụ thể, chủ sở hữu dữ liệu có đầy đủ các quyền định đoạt đối với dữ liệu thuộc sở hữu mình, bao gồm:

- **Thứ nhất**, quyền quyết định lưu trữ dữ liệu: Luật Dữ liệu 2024 quy định tổ chức, cá nhân không phải cơ quan nhà nước (*tức chủ sở hữu dữ liệu*) được quyền quyết định việc lưu trữ dữ liệu do mình thu thập, tạo lập, sở hữu. Điều này có nghĩa là chỉ chủ sở hữu dữ liệu (*không tính cơ quan nhà nước*) mới được tự chọn nơi và cách lưu trữ dữ liệu của mình, trừ trường hợp dữ liệu đó là dữ liệu cốt lõi hoặc quan trọng thuộc lĩnh vực nhạy cảm phải tuân thủ quy định riêng.

- **Thứ hai**, quyền thỏa thuận lưu trữ tại Trung tâm dữ liệu quốc gia: Chủ sở hữu dữ liệu có thể thỏa thuận lưu trữ dữ liệu của mình trên hạ tầng của Trung tâm dữ liệu quốc gia thông qua hợp đồng dịch vụ. Luật quy định rõ chủ sở hữu dữ liệu “được quyền thỏa thuận lưu trữ dữ liệu trên cơ sở hạ tầng của Trung tâm dữ liệu quốc gia bằng hợp đồng cung cấp dịch vụ”, tạo điều kiện để doanh nghiệp và cá nhân sử dụng dịch vụ lưu trữ tập trung do Nhà nước đầu tư.

- **Thứ ba**, quyền quản trị, quản lý dữ liệu: Chủ sở hữu dữ liệu được quyền tự thiết lập chính sách, kế hoạch, quy trình quản trị và quản lý dữ liệu của mình căn cứ vào điều kiện thực tế. Theo Luật Dữ liệu (Khoản 4, Điều 15), chủ sở hữu dữ liệu và chủ quản dữ liệu không phải cơ quan nhà nước “căn cứ vào điều kiện thực tế” để thực hiện quản trị, quản lý dữ liệu do mình thu thập, tạo lập, sở hữu. Như vậy, họ có quyền tự định ra cách thức quản lý, tiêu chuẩn chất lượng, phân quyền truy cập... cho dữ liệu thuộc sở hữu của mình.

- **Thứ tư**, quyền cung cấp công cụ truy cập, truy xuất: Nhà nước khuyến khích chủ sở hữu dữ liệu và chủ quản dữ liệu khác tự cung cấp công cụ giúp người dùng truy cập, truy xuất dữ liệu. Cụ thể, khoản 2, Điều 16, Luật Dữ liệu quy định: “Cơ quan nhà nước phải cung cấp công cụ... Khuyến khích chủ sở hữu dữ liệu, chủ quản dữ liệu khác thực hiện cung cấp công cụ truy cập, truy xuất dữ liệu”. Như vậy, ngoài việc Nhà nước trang bị công cụ truy cập, chủ sở hữu dữ liệu có



quyền và được khuyến khích xây dựng hoặc cung cấp các công cụ kỹ thuật giúp người khác đọc, xuất dữ liệu do mình sở hữu.

- **Thứ năm**, quyền kết nối, chia sẻ dữ liệu: Chủ sở hữu dữ liệu được phép kết nối và chia sẻ dữ liệu cho người dùng dữ liệu (*các cơ quan, tổ chức, cá nhân*) theo quy định pháp luật hoặc theo thỏa thuận, có thể thực hiện trực tiếp hoặc qua bên trung gian. Luật Dữ liệu (*Khoản 1 Điều 17*) ghi rõ: “Chủ sở hữu dữ liệu... kết nối, chia sẻ dữ liệu cho người dùng dữ liệu theo quy định của pháp luật hoặc theo thỏa thuận, bằng cách trực tiếp hoặc thông qua một bên trung gian”. Điều này trao quyền cho chủ sở hữu dữ liệu chủ động chia sẻ dữ liệu, song vẫn phải tuân thủ các quy định về bảo mật và quyền riêng tư.

- **Thứ sáu**, quyền quyết định mã hóa/giải mã dữ liệu: Luật Dữ liệu giao cho chủ sở hữu dữ liệu quyền quyết định việc mã hóa và giải mã dữ liệu của mình. Cụ thể Khoản 3 Điều 22 của Luật quy định: “Chủ sở hữu dữ liệu, chủ quản dữ liệu quyết định việc mã hóa, giải mã dữ liệu”. Như vậy, họ có toàn quyền lựa chọn phương pháp và mức độ mã hóa các dữ liệu do mình sở hữu (*trừ dữ liệu bí mật Nhà nước đã có quy định riêng*) để bảo vệ thông tin của mình.

- **Thứ bảy**, quyền tham gia xử lý các dữ liệu thuộc sở hữu: Chủ sở hữu dữ liệu có nhiệm vụ thực hiện việc kết hợp, điều chỉnh, cập nhật, sao chép, truyền, chuyển giao các dữ liệu của mình theo quy định của luật. Luật Dữ liệu (*Khoản 3 Điều 26*) quy định: “Chủ sở hữu dữ liệu... thực hiện kết hợp, điều chỉnh, cập nhật, sao chép, truyền đưa, chuyển giao dữ liệu theo quy định của Luật này và các quy định khác của pháp luật có liên quan”. Điều này có nghĩa là chủ sở hữu dữ liệu được phép và có trách nhiệm chủ động xử lý dữ liệu của mình trong khuôn khổ pháp luật (*ví dụ khi phối hợp với đối tác hoặc cơ quan Nhà nước*), miễn là tuân thủ các quy định liên quan.

- **Thứ tám**, quyền đồng ý chia sẻ dữ liệu vào Cơ sở dữ liệu tổng hợp Quốc gia: Dữ liệu của các cơ quan Đảng, Mặt trận Tổ quốc và tổ chức chính trị - xã hội chỉ được đưa vào Cơ sở dữ liệu tổng hợp Quốc gia khi có sự đồng ý của chủ sở hữu dữ liệu. Luật Dữ liệu (*khoản 1 Điều 34*) nêu rõ danh mục dữ liệu thu thập vào



Cơ sở dữ liệu tổng hợp Quốc gia, trong đó có điểm d: “Dữ liệu của cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội khi được chủ sở hữu dữ liệu đồng ý”. Do vậy, chủ sở hữu dữ liệu (*cơ quan Đảng, tổ chức chính trị - xã hội*) có quyền từ chối hoặc cho phép đưa dữ liệu của mình vào Cơ sở dữ liệu tổng hợp Quốc gia.

- **Thứ chín**, quyền sử dụng giải pháp và quy trình mã hóa: Nghị định 165/2025/NĐ-CP (*hướng dẫn Luật Dữ liệu*) quy định cơ quan, tổ chức, cá nhân (*bao gồm cả chủ sở hữu dữ liệu*) có thể sử dụng một hoặc nhiều giải pháp mã hóa và quy trình mã hóa, giải mã phù hợp với hoạt động quản trị, quản lý dữ liệu của mình. Cụ thể Điều 11 của Nghị định nêu các biện pháp mã hóa khi truyền tải, lưu trữ, trên thiết bị số, quy trình yêu cầu xác thực định danh khi giải mã... để bảo vệ dữ liệu. Như vậy, chủ sở hữu dữ liệu được quyền áp dụng công nghệ mã hóa phù hợp để bảo vệ dữ liệu của mình.

- **Thứ mười**, quyền yêu cầu sửa đổi hoặc rút lại yêu cầu cung cấp dữ liệu từ cơ quan nhà nước: Nghị định 165/2025/NĐ-CP quy định trước thời hạn giao dữ liệu, chủ sở hữu hoặc chủ quản dữ liệu có thể yêu cầu cơ quan có thẩm quyền sửa đổi hoặc hủy bỏ yêu cầu cung cấp dữ liệu nếu yêu cầu đó vi phạm pháp luật, không thuộc phạm vi quản lý dữ liệu của họ, hoặc dữ liệu đã không còn tồn tại vì lý do khách quan. Cụ thể, Khoản 5 Điều 8 của Nghị định nêu: trong các trường hợp yêu cầu cung cấp dữ liệu “trái với quy định của Luật Dữ liệu và các luật khác..., phạm vi quản lý... không nằm trong yêu cầu, hoặc... dữ liệu không còn tồn tại”, chủ sở hữu/chủ quản dữ liệu “có thể yêu cầu sửa đổi, rút lại yêu cầu cung cấp dữ liệu”. Điều này bảo vệ chủ sở hữu dữ liệu khỏi các yêu cầu không hợp lệ.

- **Thứ mười một**, quyền được hỗ trợ khi kết nối/chia sẻ dữ liệu cho cơ quan nhà nước: Nghị định 165/2025/NĐ-CP (*Điều 7*) quy định cơ quan nhà nước phải áp dụng các biện pháp hỗ trợ chủ sở hữu dữ liệu trong quá trình kết nối, chia sẻ dữ liệu. Các biện pháp bao gồm xây dựng hạ tầng và công cụ kết nối, hỗ trợ đường truyền, công cụ kỹ thuật, an ninh bảo mật, hỗ trợ hạ tầng vật lý, kinh phí kết nối/chia sẻ và nguồn nhân lực tập huấn cho chủ sở hữu dữ liệu. Điều này có nghĩa



khi tổ chức, cá nhân chia sẻ dữ liệu với Nhà nước, Nhà nước sẽ giúp đỡ về mặt kỹ thuật, tài chính, nhân sự... để quá trình kết nối, chia sẻ dữ liệu diễn ra hiệu quả và an toàn.

- **Thứ mười hai**, quyền yêu cầu khai thác thông tin từ Cơ sở dữ liệu tổng hợp Quốc gia: Theo Nghị định 165/2025/NĐ-CP (*Khoản 4 Điều 23*), cơ quan, tổ chức, cá nhân có thể gửi văn bản yêu cầu Trung tâm dữ liệu quốc gia cung cấp thông tin, khai thác dữ liệu từ Cơ sở dữ liệu tổng hợp Quốc gia. Cụ thể, điểm a khoản 4 Điều 23 quy định: “Cơ quan, tổ chức, cá nhân có văn bản yêu cầu khai thác, cung cấp thông tin trong Cơ sở dữ liệu tổng hợp quốc gia và gửi về Trung tâm dữ liệu quốc gia”. Như vậy, ngoài việc kết nối trực tiếp qua hệ thống, các thực thể cũng được phép gửi yêu cầu chính thức để lấy thông tin từ Cơ sở dữ liệu tổng hợp.

- **Thứ mười ba**, quyền được thông báo về sự cố an toàn dữ liệu: Chủ sở hữu dữ liệu có quyền được thông báo kịp thời về các sự cố an toàn dữ liệu có thể gây hại đến quyền và lợi ích hợp pháp của mình, cũng như về các biện pháp khắc phục, giảm thiểu thiệt hại. Nghị định 165/2025/NĐ-CP (*Điều 19, khoản 4*) quy định: “Chủ quản dữ liệu có trách nhiệm: a) Thông báo kịp thời cho chủ sở hữu dữ liệu về các sự cố an toàn dữ liệu có thể gây tổn hại đến quyền và lợi ích hợp pháp... và đưa ra các biện pháp giảm thiểu thiệt hại”.

Bên cạnh các quyền trên, chủ sở hữu dữ liệu cũng được pháp luật khuyến khích sử dụng dữ liệu vào các mục đích có lợi cho xã hội. Luật Dữ liệu 2024 có chính sách khuyến khích tổ chức, cá nhân chia sẻ dữ liệu của mình cho cơ quan nhà nước vì mục tiêu lợi ích chung (*nhiều chăm sóc sức khỏe, cải thiện giao thông, nghiên cứu khoa học...*). Việc chia sẻ này trên cơ sở tự nguyện và phải được sự đồng ý của chủ thể dữ liệu đối với dữ liệu cá nhân hoặc sự cho phép của chủ sở hữu đối với dữ liệu phi cá nhân. Như vậy, chủ sở hữu dữ liệu có quyền (và được khuyến khích) đóng góp dữ liệu phục vụ lợi ích cộng đồng, đồng thời vẫn phải tôn trọng quyền của chủ thể dữ liệu cá nhân khi làm điều đó.

*** Trách nhiệm của chủ sở hữu dữ liệu:**

- **Thứ nhất**, quy định thời hạn lưu trữ dữ liệu: Khoản 1, Điều 5 Nghị định 165/2025/NĐ-CP quy định chủ sở hữu dữ liệu phải quy định thời hạn lưu trữ cụ thể cho dữ liệu do mình thu thập, tạo lập. Câu chử của Nghị định nêu rõ: “Chủ sở hữu dữ liệu quy định thời hạn lưu trữ cụ thể đối với dữ liệu do mình thu thập, tạo lập”. Điều này có nghĩa chủ sở hữu dữ liệu không được để dữ liệu tồn đọng vô thời hạn, mà phải xác định khoảng thời gian tối thiểu cần lưu trữ sao cho phù hợp với mục đích sử dụng và quy định của pháp luật liên quan.

- **Thứ hai**, phối hợp xây dựng kế hoạch lưu trữ: Chủ sở hữu dữ liệu phải phối hợp với Trung tâm dữ liệu quốc gia xây dựng kế hoạch, lộ trình thực hiện dịch vụ lưu trữ dữ liệu cụ thể. Khoản 1, Điều 6 Nghị định 165/2025/NĐ-CP nêu: “Chủ sở hữu dữ liệu, chủ quản dữ liệu phối hợp với Trung tâm dữ liệu quốc gia xây dựng kế hoạch, lộ trình thực hiện theo dịch vụ lưu trữ dữ liệu cụ thể”. Tức là sau khi TTDL Quốc gia cung cấp các dịch vụ lưu trữ, chủ sở hữu dữ liệu có trách nhiệm cùng phối hợp hoạch định việc sử dụng các dịch vụ đó theo một lộ trình rõ ràng.

- **Thứ ba**, xây dựng quy trình và tổ chức xác nhận dữ liệu: Chủ sở hữu dữ liệu phải tự xây dựng quy trình, hình thức và tổ chức hoạt động xác nhận dữ liệu trong phạm vi mình sở hữu, quản lý. Nghị định 165/2025/NĐ-CP quy định: “Chủ sở hữu dữ liệu... chịu trách nhiệm về chất lượng... của dữ liệu do mình cung cấp, xác nhận; xây dựng quy trình, hình thức và tổ chức hoạt động xác nhận dữ liệu”. Điều này có nghĩa chủ sở hữu dữ liệu phải có quy định và công cụ kiểm chứng (ví dụ đối chiếu với nguồn gốc hoặc dữ liệu gốc) để xác thực tính đúng đắn của dữ liệu do họ tạo ra hoặc thu thập.

- **Thứ tư**, công khai dữ liệu mở: Nếu dữ liệu do chủ sở hữu tạo lập được phân loại là “dữ liệu mở”, họ phải công khai ngay lập tức dữ liệu đó qua Cổng dữ liệu quốc gia hoặc các cổng dữ liệu mở khác. Nghị định 165/2025/NĐ-CP (Điều 10) nêu rõ: “Việc công khai dữ liệu mở được thực hiện ngay sau khi dữ liệu được phân loại là dữ liệu mở. Chủ sở hữu dữ liệu... thực hiện công khai dữ liệu mở



dưới hình thức: a) Công dữ liệu quốc gia; b) Các công dữ liệu mở...; c) Các hệ thống trung gian phục vụ kết nối, chia sẻ dữ liệu...”. Như vậy, khi dữ liệu trở thành dữ liệu mở, chủ sở hữu không được giữ lại hay chậm trễ công bố, mà cần đăng tải trên các nền tảng quy định.

- **Thứ năm**, đánh giá tác động trước khi công khai: Trước khi công khai dữ liệu (*dù là mở hay dùng chung*), chủ sở hữu dữ liệu phải phân tích, đánh giá tác động của việc công bố đối với an ninh quốc gia, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe cộng đồng.... Cụ thể, Nghị định 165/2025/NĐ-CP (*Khoản 6, Điều 17*) quy định: “Chủ sở hữu dữ liệu phải phân tích, đánh giá tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng trước khi công khai dữ liệu”. Đây là yêu cầu đảm bảo chủ sở hữu cân nhắc kỹ càng những tác động tiềm ẩn (*ví dụ lộ thông tin nhạy cảm*) trước khi cho phép dữ liệu được truy cập rộng rãi.

- **Thứ sáu**, xây dựng phương án xóa, hủy dữ liệu: Chủ sở hữu và chủ quản dữ liệu phải xây dựng phương án xóa, hủy dữ liệu rõ ràng. Nghị định 165/2025/NĐ-CP (*Khoản 7, Điều 17*) nêu: “Chủ sở hữu dữ liệu, chủ quản dữ liệu xây dựng phương án xóa, hủy dữ liệu, làm rõ mục tiêu, quy tắc, quy trình, kỹ thuật xóa, hủy, ghi nhận và lưu giữ hoạt động xóa, hủy”. Đặc biệt, nếu dữ liệu là quan trọng hoặc cốt lõi thì phải có tài liệu chứng minh dữ liệu đã được xóa/hủy không thể khôi phục. Điều này yêu cầu chủ sở hữu phải xác định cách thức và tiêu chí xóa bỏ dữ liệu (*ví dụ sau khi hết hạn lưu trữ*), đồng thời ghi lại quá trình xóa để chứng minh tuân thủ quy định.

- **Thứ bảy**, tham gia bàn giao, tiếp nhận dữ liệu theo yêu cầu: Khi có yêu cầu cung cấp dữ liệu từ cơ quan Nhà nước, chủ sở hữu dữ liệu (*hoặc người đại diện hợp pháp của họ*) phải tham gia vào quá trình bàn giao, tiếp nhận dữ liệu. Nghị định 165/2025/NĐ-CP (*Khoản 3, Điều 8*) quy định về bàn giao dữ liệu: “Thành phần tham gia bàn giao, tiếp nhận dữ liệu gồm có: Chủ sở hữu dữ liệu, người đại diện hợp pháp hoặc người đang quản lý, sử dụng hợp pháp dữ liệu...”. Điều này có nghĩa là chủ sở hữu không được ủy quyền toàn bộ cho người khác



mà cần trực tiếp tham gia (*hoặc cử người hợp pháp*) vào quá trình giao nhận dữ liệu nếu cơ quan nhà nước yêu cầu.

- **Thứ tám**, thu hồi, xóa hoặc hủy dữ liệu của chủ thẻ: Luật Dữ liệu (Điều 26) quy định chủ thẻ dữ liệu có quyền yêu cầu chủ sở hữu dữ liệu thu hồi, xóa hoặc hủy dữ liệu cá nhân đã cung cấp. Theo đó, trong hợp tác cung cấp dữ liệu, nếu dữ liệu liên quan cá nhân đã được cung cấp cho ai đó (*ví dụ cho cơ quan nhà nước*), cá nhân đó có quyền yêu cầu thu hồi dữ liệu của mình trừ khi có quy định khác của luật. Mặc dù đây là quyền của chủ thẻ dữ liệu (*cá nhân/tổ chức mà dữ liệu phản ánh*), nó cũng đặt ra yêu cầu cho chủ sở hữu dữ liệu phải chấp hành các yêu cầu hợp pháp về thu hồi hoặc hủy dữ liệu do chính chủ thẻ cung cấp.

* **Trách nhiệm của Chủ sở hữu dữ liệu:**

- **Thứ nhất**, chịu trách nhiệm về chất lượng dữ liệu: Chủ sở hữu dữ liệu phải chịu trách nhiệm đảm bảo dữ liệu do mình cung cấp có chất lượng cao, tin cậy và hợp pháp. Nghị định 165/2025/NĐ-CP (*Điểm d, Khoản 1, Điều 9*) quy định rõ: “Chủ sở hữu dữ liệu... chịu trách nhiệm về chất lượng dữ liệu, mức độ tin cậy, hợp pháp của dữ liệu do mình cung cấp, xác nhận”. Điều này nghĩa là chủ sở hữu dữ liệu phải có trách nhiệm pháp lý với dữ liệu của mình: nếu dữ liệu sai sót, không đầy đủ hay vi phạm pháp luật, họ là người chịu trách nhiệm chỉnh sửa hoặc bồi thường.

- **Thứ hai**, trách nhiệm xây dựng quy trình xác thực dữ liệu: Chủ sở hữu dữ liệu có trách nhiệm tự xây dựng quy trình, hình thức và tổ chức thực hiện xác thực dữ liệu trong phạm vi mình sở hữu, quản lý. Cũng tại Nghị định 165/2025/NĐ-CP (*Khoản 2, Điều 9*) quy định: “Chủ sở hữu dữ liệu, chủ quản dữ liệu có trách nhiệm tự xây dựng quy trình, hình thức và tổ chức hoạt động xác thực dữ liệu trong phạm vi mình sở hữu, quản lý”. Nói cách khác, chủ sở hữu phải đảm bảo rằng dữ liệu của họ đã được kiểm chứng chính xác (*xác thực*) theo một quy trình rõ ràng, trước khi sử dụng hoặc cung cấp cho người khác.

Tóm lại, chủ sở hữu dữ liệu có quyền rộng rãi đối với tài sản dữ liệu nhưng đồng thời chịu trách nhiệm lớn. Họ được tự do khai thác giá trị kinh tế của dữ



liệu, song phải tuân thủ pháp luật, đảm bảo an ninh dữ liệu và không xâm phạm quyền riêng tư. Các quy định mới buộc chủ sở hữu dữ liệu nâng cao năng lực quản trị dữ liệu: ví dụ thiết lập quy trình xác thực dữ liệu, phân loại và bảo vệ dữ liệu theo mức độ quan trọng, hợp tác với Nhà nước khi cần. Nếu vi phạm nghĩa vụ (*như làm lộ dữ liệu cá nhân, không cung cấp dữ liệu khi có lệnh hợp pháp*), chủ sở hữu dữ liệu có thể chịu chế tài hành chính hoặc hình sự tùy mức độ. Do vậy, việc hiểu rõ và tuân thủ các nghĩa vụ trên là rất quan trọng đối với mọi tổ chức, cá nhân giữ vai trò chủ sở hữu dữ liệu trong nền kinh tế số.

2.1.3. Chủ quản dữ liệu

2.1.3.1. Khái niệm Chủ quản dữ liệu

Chủ quản dữ liệu được định nghĩa tại Khoản 13 Điều 3 Luật Dữ liệu 2024 là “*cơ quan, tổ chức, cá nhân thực hiện hoạt động xây dựng, quản lý, vận hành, khai thác dữ liệu theo yêu cầu của chủ sở hữu dữ liệu*”. Nói cách khác, đây là chủ thể được chủ sở hữu dữ liệu ủy nhiệm hoặc phân công để trực tiếp thực thi các công việc liên quan đến dữ liệu: tạo lập hệ thống thu thập, lưu trữ dữ liệu; quản lý, vận hành kho dữ liệu hoặc cơ sở dữ liệu; triển khai các hoạt động khai thác, phân tích dữ liệu phục vụ nhu cầu của chủ sở hữu. Chủ quản dữ liệu có thể chính là chủ sở hữu (*nếu tự mình vận hành dữ liệu của mình*), hoặc có thể là một bên thứ ba được thuê/giao nhiệm vụ (*ví dụ: một đơn vị cung cấp dịch vụ xử lý dữ liệu được doanh nghiệp thuê ngoài*). Luật Dữ liệu 2024 lần đầu giới thiệu rõ vai trò chủ quản dữ liệu nhằm phân định với chủ sở hữu: chủ quản là bên trực tiếp xử lý, vận hành trên dữ liệu, nhưng làm theo yêu cầu và vì lợi ích của chủ sở hữu.

Về vai trò pháp lý, chủ quản dữ liệu là bên phải đảm bảo các yêu cầu kỹ thuật và bảo mật trong quá trình xử lý dữ liệu. Họ đóng vai trò tương tự “bên kiểm soát và xử lý dữ liệu” trong khái niệm bảo vệ dữ liệu cá nhân (*data controller/processor*) ở chỗ chịu trách nhiệm vận hành hệ thống quản trị dữ liệu. Chủ quản dữ liệu thường có hiểu biết chuyên môn về công nghệ và quản lý dữ liệu, chịu trách nhiệm duy trì tính toàn vẹn, an ninh, an toàn của dữ liệu trong suốt vòng đời của nó. Trong hệ sinh thái dữ liệu, nếu ví dữ liệu là tài sản thì chủ sở



hữu là người quyết định sử dụng tài sản đó vào việc gì, còn chủ quản dữ liệu là người quản lý, kỹ thuật viên đảm bảo tài sản dữ liệu được vận hành trôi chảy, an toàn. Luật Dữ liệu cũng đặt ra một số nghĩa vụ cụ thể cho chủ quản dữ liệu nhằm bảo đảm họ thực hiện tốt vai trò này - chẳng hạn phải phân loại dữ liệu, quản lý rủi ro, bảo vệ dữ liệu... Nhìn chung, chủ quản dữ liệu là mắt xích quan trọng, quyết định hiệu quả quản trị và bảo vệ dữ liệu trên thực tế, giúp chủ sở hữu hiện thực hóa quyền sở hữu của mình thông qua các hoạt động thu thập, lưu trữ, xử lý dữ liệu một cách chuyên nghiệp và tuân thủ pháp luật.



Hình ảnh: Bên trong Trung tâm dữ liệu Internet của Tập đoàn Bưu chính Viễn thông Việt Nam tại Khu công nghệ cao Hòa Lạc, Hà Nội. Ảnh: TTXVN

2.1.3.2. Quyền, nghĩa vụ và trách nhiệm của chủ quản dữ liệu

** Quyền của chủ quản dữ liệu:*

- **Thứ nhất**, Luật Dữ liệu 2024 trao quyền cho chủ quản dữ liệu được tự quyết định biện pháp mã hóa và giải mã dữ liệu do mình quản lý. Cụ thể, Khoản 3 Điều 22 Luật Dữ liệu nêu rõ: “Chủ sở hữu dữ liệu, chủ quản dữ liệu quyết định việc mã hóa, giải mã dữ liệu”. Điều này có nghĩa là bên nắm quyền dữ liệu có



toàn quyền lựa chọn phương thức bảo vệ thông tin (*ví dụ chọn chuẩn mã hóa, quản lý khóa*) và xử lý ngược lại (*giải mã*) khi cần, trừ các trường hợp pháp luật chuyên biệt (*ví dụ dữ liệu tối mật*) có quy định khác.

- **Thứ hai**, về công cụ truy cập, truy xuất dữ liệu, nhà nước khuyến khích chủ sở hữu và chủ quản dữ liệu cung cấp các công cụ hỗ trợ bên thứ ba trong việc truy cập, lấy dữ liệu. Khoản 2 Điều 16 Luật Dữ liệu 2024 quy định: “Nhà nước khuyến khích chủ sở hữu dữ liệu, chủ quản dữ liệu khác thực hiện cung cấp công cụ truy cập, truy xuất dữ liệu”. Điều này có nghĩa các bên nắm dữ liệu có thể (*mà không bắt buộc*) phát triển và cung cấp các giao diện, API hoặc công cụ kỹ thuật cho phép người dùng hoặc tổ chức khác truy cập và truy xuất dữ liệu, nhằm thúc đẩy tính liên kết và chia sẻ dữ liệu nhưng vẫn đảm bảo an toàn.

- **Thứ ba**, chủ quản dữ liệu cũng được quyền quy định loại hình truy cập và truy xuất dữ liệu. Theo Khoản 1, Điều 6 Nghị định 165/2025/NĐ-CP quy định chủ quản dữ liệu phải quy định rõ các loại hình truy cập: bao gồm truy cập đọc, truy cập ghi, truy cập sửa, truy cập xóa, truy cập thực thi và có thể thêm các loại khác phù hợp mục đích tổ chức. Tương tự, Khoản 2 của cùng Điều này quy định các hình thức “truy xuất dữ liệu” như truy xuất thủ công, tự động, truy xuất theo thời gian thực. Như vậy, chủ quản dữ liệu có quyền thiết lập chính sách phân quyền chi tiết (*ai được đọc/ghi/sửa dữ liệu*) và quyết định công nghệ hoặc quy trình truy xuất, trích xuất dữ liệu (*ví dụ cho phép tải trực tiếp, qua API tự động hay chỉ thông qua báo cáo mẫu lập thủ công*).

- **Thứ tư**, về kết sử dụng kinh phí, tại Khoản 3 Điều 14 Nghị định 194/2025/NĐ-CP (*hướng dẫn Luật Giao dịch điện tử về cơ sở dữ liệu quốc gia*) quy định: “Chủ quản cơ sở dữ liệu quốc gia sử dụng kinh phí cấp từ ngân sách nhà nước, từ nguồn thu phí và lệ phí, kinh phí khác theo quy định để phục vụ xây dựng, cập nhật, quản lý và duy trì cơ sở dữ liệu”. Điều này cho thấy ngân sách vận hành và phát triển cơ sở dữ liệu quốc gia do chính phủ cấp, cộng với nguồn thu phí/le phí và nguồn kinh phí hợp pháp khác. Chủ quản dữ liệu quốc gia (*ví dụ các bộ, ngành*) có quyền phân bổ và sử dụng các nguồn kinh phí này để đầu tư về



cơ sở hạ tầng, phần mềm, nhân lực cho việc quản lý cơ sở dữ liệu, cập nhật dữ liệu mới và duy trì hệ thống.

- **Thứ năm**, chủ quản dữ liệu có quyền nhận dữ liệu được chia sẻ từ các cơ quan nhà nước khác. Điều 16 Nghị định 194/2025/NĐ-CP quy định hai nhóm nội dung quan trọng. Thứ nhất, các cơ quan nhà nước quản lý ngành, lĩnh vực ở địa phương “được chia sẻ dữ liệu từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu của bộ, ngành theo phạm vi quản lý”. Thứ hai, “dữ liệu sử dụng chung, dữ liệu mở trong cơ quan nhà nước” có mặc định phải chia sẻ cho các cơ quan nhà nước khi có đề nghị và hợp pháp yêu cầu quản lý nhà nước. Nói cách khác, chủ quản dữ liệu quốc gia được quyền tiếp cận và yêu cầu chia sẻ nguồn dữ liệu chung do cơ quan khác nắm giữ, phục vụ công tác quản lý theo ngành, lĩnh vực. Các dữ liệu công cộng, mở được chia sẻ mặc định mà không cần trở bởi quy định nội bộ.

- **Thứ sáu**, Luật An toàn thông tin mạng 2015 trao quyền và trách nhiệm cho chủ sở hữu dữ liệu cá nhân tiếp cận và tự quản lý thông tin cá nhân của mình. Cụ thể, Điều 18 ghi rõ: khi chủ sở hữu dữ liệu (*chủ thẻ cá nhân*) có yêu cầu, phải được “cung cấp quyền tiếp cận để tự cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình”. Nói cách khác, chủ quản dữ liệu (*hay noi lưu giữ thông tin cá nhân*) phải tạo điều kiện để người dùng cá nhân có thể kiểm tra, hiệu chỉnh hoặc xóa thông tin về mình đang lưu trữ. Nếu không trực tiếp cho phép chỉnh sửa thông tin, họ cũng phải xử lý yêu cầu của cá nhân, thông báo kết quả. Điều này đảm bảo quyền cá nhân kiểm soát dữ liệu của chính mình.

- **Thứ bảy**, chủ quản dữ liệu còn được miễn trừ trách nhiệm pháp lý đối với các thiệt hại phát sinh, nếu đã có thỏa thuận trước. Nghị định 165/2025/NĐ-CP tại Điều 18 Khoản 6 quy định: “*Người chịu trách nhiệm về bảo vệ dữ liệu* được thỏa thuận với chủ sở hữu, chủ quản dữ liệu về các trường hợp miễn trừ trách nhiệm khi xảy ra thiệt hại đối với dữ liệu được bảo vệ”. Điều này có nghĩa trong hợp đồng hoặc thỏa thuận giữa chủ quản dữ liệu với bên phụ trách bảo vệ dữ liệu (*chẳng hạn nhà cung cấp dịch vụ bảo mật*), nếu có các điều khoản miễn trừ trách nhiệm khi dữ liệu bị mất mát hoặc rủi ro, thì các bên phải tuân thủ thỏa thuận đó.



Nói khác, chủ quản dữ liệu có thể ký kết về việc họ sẽ không truy cứu trách nhiệm bên bảo vệ nếu thiệt hại nằm trong điều kiện đã thỏa thuận (*ví dụ lỗi của chủ quản hoặc sự kiện bất khả kháng*).

- **Cuối cùng**, về hình thức lưu trữ văn bản hay dữ liệu, Luật Giao dịch điện tử 2023 cho phép các tổ chức và cá nhân (*bao gồm cả chủ quản dữ liệu*) lựa chọn lưu trữ thông tin dưới dạng văn bản giấy hoặc “dưới dạng thông điệp dữ liệu” (*dữ liệu điện tử*) khi đáp ứng các tiêu chí truy cập, định dạng và xác định nguồn gốc. Khoản 2, Điều 13 Luật này nêu rõ: trừ khi pháp luật có quy định khác, người lưu trữ được tự quyết định hình thức văn bản hay thông điệp dữ liệu nếu đảm bảo có thể truy cập, định dạng chính xác và xác nhận được nguồn gốc. Như vậy, chủ quản dữ liệu có quyền lựa chọn lưu trữ hồ sơ, chứng từ dưới dạng điện tử hay giấy miễn sao dữ liệu điện tử đó được quản lý an toàn, có chữ ký số hoặc chứng thực thích hợp để đảm bảo tính pháp lý.

* Nghĩa vụ và Trách nhiệm của Chủ quản dữ liệu:

- Nghĩa vụ và trách nhiệm chung về quản lý và xử lý dữ liệu:

+ Quản lý, vận hành, khai thác dữ liệu: Chủ quản dữ liệu có nghĩa vụ thực hiện các hoạt động xây dựng, quản lý, vận hành và khai thác dữ liệu dựa trên yêu cầu của chủ sở hữu dữ liệu. Luật Dữ liệu 2024 định nghĩa “Chủ quản dữ liệu” là cơ quan, tổ chức, cá nhân thực hiện các hoạt động xây dựng, quản lý, vận hành, khai thác dữ liệu theo yêu cầu của chủ sở hữu. Điều này nghĩa là chủ quản dữ liệu chịu trách nhiệm thu thập, lưu trữ và xử lý dữ liệu một cách có hệ thống, đáp ứng mục tiêu công tác quản lý hoặc kinh doanh dữ liệu mà chủ sở hữu đưa ra.

+ Quản trị dữ liệu: Chủ quản dữ liệu phải xây dựng hệ thống quản trị dữ liệu toàn diện. Theo Điều 15 Luật Dữ liệu 2024, quản trị dữ liệu bao gồm việc xây dựng chính sách, kế hoạch, chương trình, quy trình, tiêu chuẩn về dữ liệu nhằm quản lý liên tục và hiệu quả, đảm bảo dữ liệu “đầy đủ, chính xác, toàn vẹn, nhất quán, thống nhất, được chuẩn hóa, an toàn, bảo mật, kịp thời”.

+ Đảm bảo chất lượng dữ liệu: Chủ quản dữ liệu phải chịu trách nhiệm về chất lượng và tính pháp lý của dữ liệu do mình cung cấp, xác nhận. Nghị định



165/2025/NĐ-CP quy định rõ: “Chủ sở hữu dữ liệu, chủ quản dữ liệu chịu trách nhiệm về chất lượng dữ liệu, mức độ tin cậy, hợp pháp của dữ liệu do mình cung cấp, xác nhận”. Đồng thời, chủ quản phải xây dựng quy trình và tổ chức hoạt động xác nhận, xác thực dữ liệu trong phạm vi quản lý. Nói cách khác, chủ quản dữ liệu phải có quy trình đối chiếu, kiểm tra, bổ sung khi phát hiện lỗi; dữ liệu cần được thu thập đầy đủ, cập nhật kịp thời và đảm bảo đúng yêu cầu của bên khai thác. Tiêu chí “đầy đủ, chính xác, kịp thời” cũng được nhấn mạnh trong Luật Dữ liệu về chất lượng dữ liệu.

+ Công khai dữ liệu: Nếu dữ liệu được xác định là “mở” hoặc không thuộc diện cấm, chủ quản dữ liệu phải công khai thông tin này lên cổng dữ liệu quốc gia hoặc nền tảng dữ liệu mở. Nghị định 165/2025/NĐ-CP nêu: “Việc công khai dữ liệu mở được thực hiện ngay sau khi dữ liệu được phân loại là dữ liệu mở” và “Dữ liệu của cơ quan nhà nước không thuộc diện bị cấm công khai, phải được công khai như dữ liệu mở”. Nghĩa vụ này yêu cầu chủ quản dữ liệu phải đăng tải, chia sẻ dữ liệu sau khi phân loại, đồng thời đảm bảo tuân thủ nguyên tắc an toàn thông tin (*phải đánh giá các tác động đến quốc phòng, an ninh, đối ngoại, ổn định xã hội, sức khỏe cộng đồng trước khi công khai dữ liệu mới*).

+ Xử lý và lưu trữ dữ liệu: Chủ quản dữ liệu phải thực hiện các quy trình xử lý (kết hợp, điều chỉnh, cập nhật, sao chép, truyền, chuyển giao) theo đúng quy định pháp luật. Với dữ liệu “cốt lõi” và “quan trọng” (theo định nghĩa của Luật Dữ liệu), phải ghi nhật ký đầy đủ quá trình xử lý và lưu giữ nhật ký ít nhất sáu tháng. Đồng thời, chủ quản phải xây dựng phương án xóa, hủy dữ liệu (bao gồm mục tiêu, kỹ thuật, quy trình, ghi nhận việc xóa) và đảm bảo tài liệu chứng minh dữ liệu quan trọng, cốt lõi đã bị hủy không thể khôi phục. Luật Dữ liệu và Nghị định 165/2025/NĐ-CP cũng quy định phải xóa dữ liệu khi hết hạn lưu trữ hoặc không còn cần thiết và lưu trữ theo phương pháp, thời hạn do pháp luật quy định. Đối với dữ liệu quan trọng, chủ quản phải xây dựng quy trình lưu trữ (bao gồm sao lưu, phục hồi) và áp dụng biện pháp kỹ thuật bảo vệ, đảm bảo sao lưu tự động, phục hồi được dữ liệu.



+ Truy cập, truy xuất dữ liệu: Chủ quản chỉ được truy cập hoặc cho phép truy cập dữ liệu trong phạm vi quyền hạn được giao và mục đích cụ thể. Khi xử lý dữ liệu cốt lõi, quan trọng, phải xây dựng và triển khai quy chế truy cập dữ liệu tuân thủ nguyên tắc tối thiểu đặc quyền. Cơ chế bảo mật như hệ thống quản lý truy cập, định danh tập trung, biện pháp kỹ thuật để kiểm soát truy cập/truy xuất dữ liệu đều phải được áp dụng. Nghị định 165/2025/NĐ-CP quy định rõ các biện pháp này nhằm đảm bảo rằng chỉ những người có thẩm quyền và đúng mục đích mới được phép xem hoặc sử dụng dữ liệu. Ví dụ, hệ thống giám sát và kiểm soát quyền truy cập phải được xây dựng để ngăn chặn truy cập trái phép.

- Nghĩa vụ và Trách nhiệm về Bảo vệ Dữ liệu Cá nhân:

+ Tuân thủ pháp luật: Chủ quản dữ liệu cá nhân (*cả bên kiểm soát và bên xử lý*) phải tuân thủ đầy đủ quy định Luật Bảo vệ dữ liệu cá nhân 2025 và các văn bản có liên quan. Luật này quy định trách nhiệm rõ: mọi hoạt động thu thập, lưu trữ, xử lý dữ liệu cá nhân đều phải phù hợp với quy định của Luật và các quy định khác của pháp luật liên quan. Như vậy, chủ quản dữ liệu không chỉ tuân thủ các quy định mới của Luật Bảo vệ dữ liệu cá nhân mà còn phải tuân thủ những quy định khác như Luật An toàn thông tin mạng, Luật Giao dịch điện tử, Luật Tiếp cận thông tin... khi xử lý dữ liệu cá nhân.

+ Đảm bảo sự đồng ý của chủ thể dữ liệu: Mọi việc thu thập và sử dụng dữ liệu cá nhân phải dựa trên sự đồng ý trước của chủ thể. Cụ thể: ⁽¹⁾ Trước khi thu thập, chủ thể dữ liệu cá nhân phải đồng ý cho phạm vi và mục đích sử dụng dữ liệu. (*Luật Bảo vệ dữ liệu cá nhân 2025 quy định rõ: "Dữ liệu cá nhân được thu thập phải được sự đồng ý của chủ thể... trước khi thu thập, trừ trường hợp pháp luật khác quy định."*); ⁽²⁾ Không được sử dụng thông tin tín dụng của cá nhân để chấm điểm, xếp hạng hoặc đánh giá tín dụng nếu chưa có sự đồng ý của người đó. Điều này được nêu trong quy định về thông tin tín dụng; ⁽³⁾ Nếu sử dụng dữ liệu cá nhân vào mục đích khác so với mục đích ban đầu, phải xin phép và được đồng ý thêm từ chủ thể dữ liệu. Nói cách khác, thỏa thuận ban đầu chỉ có hiệu lực cho mục đích đã nêu; nếu thay đổi mục đích, chủ quản phải thông báo và lấy ý kiến



đồng ý mới; ⁽⁴⁾Sự đồng ý phải là tự nguyện, được thông báo đầy đủ (*chủ thể biết rõ loại dữ liệu, mục đích xử lý, tổ chức xử lý, quyền và nghĩa vụ của mình*). Điều 9 Luật Bảo vệ dữ liệu cá nhân quy định “sự đồng ý chỉ có hiệu lực khi dựa trên sự tự nguyện và biết rõ các thông tin: loại dữ liệu, mục đích xử lý...”.

Khi có nhiều mục đích xử lý, người được thu thập phải được liệt kê riêng từng mục đích để họ chọn đồng ý với một hoặc nhiều mục đích. Luật quy định sự đồng ý phải rõ ràng cho từng mục đích và không được gán điều kiện bắt buộc phải đồng ý với mục đích khác.

Đặc biệt, nếu xử lý dữ liệu cá nhân nhạy cảm (*y tế, sinh trắc học...*), chủ thể phải được thông báo rõ ràng đây là dữ liệu nhạy cảm và ý nghĩa của việc thu thập.

Chủ quản phải tôn trọng quyền rút lại sự đồng ý của chủ thể. Khi người dùng yêu cầu rút lại hoặc hạn chế xử lý, phải đáp ứng kịp thời trong thời hạn luật định. Ví dụ, Điều 10 Luật Bảo vệ dữ liệu cá nhân quy định chủ thể được quyền rút đồng ý và yêu cầu hạn chế xử lý; yêu cầu này phải được thể hiện bằng văn bản (*ké cả điện tử*) và gửi đến bên kiểm soát dữ liệu. Sau khi nhận yêu cầu, chủ quản phải thực thi (*ngưng xử lý dữ liệu*) hoặc phối hợp bên xử lý dữ liệu thực hiện yêu cầu. Trường hợp này cũng bao gồm dữ liệu nhạy cảm của trẻ em, người khuyết tật, khi cha mẹ/người giám hộ rút ý đồng ý thì phải ngừng xử lý và xóa (*không phục hồi*).

+ Thông báo hoạt động xử lý: Chủ quản dữ liệu phải thông báo (*một lần*) cho chủ thể dữ liệu về các hoạt động xử lý sắp thực hiện. Nội dung thông báo phải nêu rõ mục đích xử lý, loại dữ liệu, cách thức xử lý, các bên liên quan (*ví dụ đối tác cung cấp dịch vụ*), hệ quả/thiệt hại tiềm ẩn (*nếu có*), thời điểm bắt đầu và dự kiến kết thúc xử lý. Phương thức thông báo phải rõ ràng, có thể in sao được, cho dù ở dạng văn bản giấy hay điện tử có chứng thực. Ngoài ra, chủ quản có trách nhiệm thông báo cho chủ thể nếu xảy ra sự cố lộ, mất thông tin cá nhân (*ví dụ lộ thông tin tài khoản ngân hàng, tín dụng*) để người đó kịp thời phòng ngừa hậu quả.



+ Đáp ứng quyền của chủ thẻ dữ liệu cá nhân: Khi nhận được yêu cầu thực hiện quyền (*theo Điều 4 Luật Bảo vệ dữ liệu cá nhân*), chủ quản phải xử lý kịp thời. Ví dụ: nếu chủ thẻ yêu cầu cung cấp sao bản dữ liệu, sửa chữa, thu hồi đồng ý, hạn chế xử lý, phải thực hiện theo quy định về thời gian (*Điều 10 Luật Bảo vệ dữ liệu cá nhân quy định xử lý rút đồng ý trong vài ngày*). Chủ quản không được cung cấp, chia sẻ hoặc phát tán thông tin cá nhân cho bên thứ ba trừ khi có sự đồng ý hoặc theo yêu cầu của cơ quan thẩm quyền (*ví dụ thanh tra, tòa án*). Khi kết thúc mục đích xử lý hoặc hết thời hạn lưu trữ, hoặc khi chủ thẻ rút lại đồng ý/không còn đồng ý, hoặc phát hiện xử lý không đúng mục đích/vi phạm pháp luật, chủ quản phải xóa (*hủy*) dữ liệu cá nhân. Nếu không thể xóa vì lý do chính đáng (*ví dụ pháp luật chuyên ngành yêu cầu lưu trữ*), phải thông báo cho chủ thẻ về lý do. Luật Bảo vệ dữ liệu cá nhân còn quy định riêng trường hợp dữ liệu trẻ em: nếu xử lý không đúng mục đích, hoàn thành mục đích, cha mẹ/giám hộ rút ý đồng ý, hoặc theo yêu cầu cơ quan có thẩm quyền (*khi có dấu hiệu xâm hại quyền trẻ em*), phải ngừng xử lý và xóa không khôi phục được. Đối với dữ liệu người lao động, hết hợp đồng thì phải xóa, trừ khi thỏa thuận khác hoặc luật chuyên ngành có quy định khác.

+ Bảo vệ dữ liệu cá nhân: Chủ quản dữ liệu phải áp dụng các biện pháp quản lý và kỹ thuật thích hợp để bảo vệ dữ liệu cá nhân. Cụ thể: ⁽¹⁾Triển khai các biện pháp phòng, chống truy cập, sử dụng, tiết lộ, chỉnh sửa trái phép dữ liệu cá nhân. Ví dụ, xây dựng tường lửa, mã hóa dữ liệu, kiểm soát truy cập và theo dõi nhật ký truy cập; ⁽²⁾Định kỳ rà soát, cập nhật biện pháp bảo vệ. Luật ghi rõ bên kiểm soát phải “thực hiện biện pháp quản lý, kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân... rà soát và cập nhật các biện pháp này khi cần thiết”; ⁽³⁾Có phương án khôi phục dữ liệu khi bị mất mát. Chủ quản phải lưu trữ và sao lưu dữ phòng để có thể khôi phục khi có sự cố; ⁽⁴⁾Bảo mật quy trình thu thập, cung cấp dữ liệu cá nhân trong hoạt động tín dụng, đảm bảo bí mật và tuân thủ quy định chuyên ngành về bảo mật (*Luật Bảo vệ Dữ liệu 2025 quy định khắt khe về tín dụng cá nhân*); ⁽⁵⁾Không để lộ dữ liệu cho bên không có thẩm quyền (*trừ khi có lý do pháp lý, ví*



du cung cấp thông tin thuê bao theo yêu cầu thanh tra). Nếu chưa thực hiện được yêu cầu của chủ thẻ (ví dụ chưa xóa do khó khăn kỹ thuật), phải thông báo ngay cho chủ thẻ biết và giải trình lý do; ⁽⁶⁾ Ngăn chặn thu thập dữ liệu cá nhân trái phép từ hệ thống hay thiết bị của mình. Luật Bảo vệ dữ liệu quy định rõ bên kiểm soát “ngăn chặn hoạt động thu thập dữ liệu cá nhân trái phép từ hệ thống, trang thiết bị, dịch vụ của mình”; ⁽⁷⁾ Với dữ liệu sinh trắc học, ngoài các biện pháp kỹ thuật mã hóa, lưu trữ an toàn, phải có bảo mật vật lý đối với thiết bị lưu trữ/transmission dữ liệu sinh trắc học, hạn chế số người truy cập và có hệ thống giám sát xâm phạm. Nếu xảy ra thiệt hại do xử lý dữ liệu sinh trắc học, phải thông báo cho chủ thẻ dữ liệu.

Dữ liệu thu qua ghi âm, ghi hình ở nơi công cộng phải dùng đúng mục đích ghi âm đã nêu, không sử dụng sai phạm; lưu trữ chỉ trong thời gian cần thiết, sau đó phải xóa hủy.

Với các công nghệ mới (*big data, AI, blockchain, metaverse, điện toán đám mây*): hệ thống phải được tích hợp biện pháp bảo mật tương ứng. Phải áp dụng xác thực, định danh, phân quyền truy cập phù hợp. Khi xử lý dữ liệu cá nhân bằng AI, cần phân loại mức độ rủi ro (*phải có quy định trong luật*) để có biện pháp bảo vệ phù hợp. Tuyệt đối không sử dụng hệ thống AI hay các công nghệ kề trên nhằm gây hại cho quốc phòng, an ninh, trật tự, nhân phẩm, tính mạng, sức khỏe của người khác.

Với ứng dụng di động, bên cung cấp phải thông báo rõ khi sử dụng dữ liệu vị trí của người dùng. Phải có biện pháp ngăn tổ chức, cá nhân không liên quan thu thập trái phép dữ liệu vị trí. Cung cấp cho người dùng tùy chọn bật/tắt theo dõi vị trí.

+ Quản lý hồ sơ và báo cáo vi phạm: Khi xử lý dữ liệu cá nhân, chủ quản phải lưu trữ đầy đủ hồ sơ liên quan. Luật buộc phải lập Hồ sơ đánh giá tác động (*ĐGTD*) nếu xử lý dữ liệu cá nhân có rủi ro cao, ghi chi tiết các nội dung đánh giá. Nếu phát hiện vi phạm quyền riêng tư, phải lập biên bản xác nhận vi phạm và phối hợp với Bộ Công an/cơ quan chức năng xử lý vi phạm. Mọi hành vi vi phạm



(xử lý sai mục đích, lô/hỗng dữ liệu, chủ thẻ bị xâm hại quyền) phải được thông báo kịp thời cho cơ quan bảo vệ dữ liệu cá nhân và cơ quan chuyên trách. Chủ quản có trách nhiệm phối hợp điều tra, xử lý vi phạm, ngăn chặn hậu quả phát tán dữ liệu cá nhân.

+ Trách nhiệm khi chuyển giao dữ liệu cá nhân: Trong hợp đồng hoặc thỏa thuận ủy thác xử lý dữ liệu cá nhân, chủ quản phải nêu rõ trách nhiệm, quyền, nghĩa vụ bảo mật của các bên. Đặc biệt, khi ủy thác xử lý dữ liệu quan trọng/cốt lõi, chủ quản phải kiểm tra năng lực, quy trình bảo vệ dữ liệu của bên nhận ủy thác trước khi ký hợp đồng.

+ Trong hoạt động tài chính - ngân hàng - tín dụng: Chủ quản hoạt động trong lĩnh vực này phải tuân thủ các tiêu chuẩn bảo mật, an toàn dữ liệu cá nhân nhạy cảm theo luật chuyên ngành. Họ chỉ được thu thập các thông tin cá nhân thật sự cần thiết cho nghiệp vụ tín dụng từ nguồn hợp pháp.

+ Trong hoạt động quảng cáo: Mọi việc chuyển giao và sử dụng dữ liệu cá nhân để mục đích quảng cáo phải tuân thủ Điều 28 Luật Bảo vệ dữ liệu cá nhân:

- (¹) Chỉ được sử dụng dữ liệu khách hàng do chính doanh nghiệp thu thập hoặc chuyển giao hợp pháp; (²) Chỉ được chuyển dữ liệu cá nhân cho doanh nghiệp quảng cáo khi pháp luật cho phép; (³) Việc xử lý dữ liệu cá nhân để quảng cáo phải có sự đồng ý rõ ràng của khách hàng và khách hàng phải được thông tin rõ nội dung, hình thức, tần suất quảng cáo; đồng thời phải được cung cấp cơ chế từ chối nhận quảng cáo; (⁴) Tuân thủ các quy định về chống tin nhắn, thư, cuộc gọi rác;
- (⁵) Chủ thẻ dữ liệu có quyền yêu cầu ngừng nhận quảng cáo và doanh nghiệp quảng cáo phải thiết lập cơ chế xử lý yêu cầu này; (⁶) Không được thuê lại toàn bộ dịch vụ quảng cáo có sử dụng dữ liệu cá nhân cho bên thứ ba; (⁷) Doanh nghiệp quảng cáo có trách nhiệm chứng minh việc sử dụng dữ liệu cá nhân đúng mục đích;
- (⁸) Đối với quảng cáo hành vi/mục tiêu cụ thể (*cá nhân hóa*), nếu thu thập dữ liệu qua việc theo dõi web/app chỉ được thực hiện khi có sự đồng ý trước; phải cho phép chủ thẻ từ chối chia sẻ dữ liệu, xác định thời hạn lưu trữ và xóa hủy khi hết cần thiết.



+ Trong quản lý thông tin thuê bao di động: Chủ quản thông tin thuê bao di động phải tuân thủ quy định chặt chẽ: ⁽¹⁾Phải có đầy đủ các cách thức để thuê bao từ chối nhận thông tin quảng cáo, tin nhắn rác; ⁽²⁾Không được xây dựng hoặc liên kết một cơ sở dữ liệu tập trung thu thập, lưu giữ thông tin thuê bao vượt quy định. Cơ sở dữ liệu phải đầy đủ các trường tối thiểu hoặc không thu thập không đầy đủ; ⁽³⁾Không được lưu giữ thông tin thuê bao sau 2 năm kể từ khi thuê bao chấm dứt dịch vụ; ⁽⁴⁾Phải cho phép thuê bao trả trước tự kiểm tra thông tin thuê bao của mình, cung cấp đủ thông tin cần thiết; ⁽⁵⁾Phải phối hợp cung cấp thông tin thuê bao cho cơ quan quản lý khi có yêu cầu đúng quy định; ⁽⁶⁾Phải công bố danh sách điểm cung cấp dịch vụ viễn thông đầy đủ trên trang điện tử doanh nghiệp và có thông tin liên hệ rõ ràng.

- Nghĩa vụ và Trách nhiệm khi chuyển, xử lý dữ liệu xuyên biên giới (Bên chuyển dữ liệu)

+ Lập và gửi hồ sơ đánh giá tác động: Khi cần chuyển xử lý dữ liệu xuyên biên giới, bên chuyển (chủ sở hữu/chủ quản dữ liệu) phải lập báo cáo đánh giá tác động. Với dữ liệu cốt lõi (như bí mật quốc gia) và dữ liệu quan trọng, Luật Dữ liệu quy định phải thực hiện đánh giá tác động an ninh quốc gia. Cụ thể theo NĐ 165/2025/NĐ-CP: ⁽¹⁾Với dữ liệu cốt lõi: Sau khi lập hồ sơ ĐGTD, phải gửi cho Bộ Công an (nếu không thuộc lĩnh vực quân sự, quốc phòng) hoặc Bộ Quốc phòng (nếu dữ liệu liên quan quân sự) để đánh giá. Đơn vị này có trách nhiệm kiểm tra, phê duyệt hồ sơ trong 10-15 ngày; ⁽²⁾Với dữ liệu quan trọng: Phải lập ĐGTD trước khi chuyển và gửi 1 bản chính cho Bộ Công an (hoặc Bộ Quốc phòng) trước ít nhất 15 ngày khi triển khai. Dù một số trường hợp đặc biệt (cấp bách, nhân sự xuyên biên giới, hợp đồng quốc tế) được miễn đồng ý chủ thể, nhưng vẫn phải gửi hồ sơ ĐGTD trong vòng 15 ngày sau khi thực hiện; ⁽³⁾Nếu có thay đổi (mục đích, phạm vi, bên nhận, chính sách bảo vệ của bên nhận, quyền kiểm soát...) sau khi đã gửi hồ sơ, bên chuyển phải bổ sung, cập nhật hồ sơ (phải tiếp tục gửi cho các bộ chức năng để xem xét).



+ Tuân thủ yêu cầu ngừng chuyển giao: Bộ Quốc phòng, Bộ Công an có thể yêu cầu bên chuyển ngừng ngay việc chuyển hoặc xử lý dữ liệu cốt lõi, quan trọng nếu phát hiện dữ liệu đó được sử dụng vào hoạt động xâm phạm quốc phòng, an ninh hoặc lợi ích quốc gia, quyền lợi hợp pháp của cá nhân, tổ chức. Bên chuyển có nghĩa vụ tuân thủ mọi quyết định của các bộ này về việc dừng chuyển dữ liệu.

• + Trách nhiệm của bên chuyển và bên nhận trong văn bản giao kết: Tất cả các điều khoản giao kết phải xác định rõ mục đích, phương pháp, phạm vi xuất/xử lý, địa điểm, thời gian lưu trữ dữ liệu, biện pháp xử lý khi hết hạn sử dụng, yêu cầu về bảo vệ dữ liệu và cung cấp bên thứ ba, cũng như các biện pháp khắc phục hậu quả và bồi thường khi có sự cố. Chẳng hạn, hợp đồng phải nêu rõ nếu dữ liệu bị xâm phạm do lỗi bên nhận thì bồi thường thế nào và ai chịu trách nhiệm pháp lý. Các điểm a-e tại Điều 12 Nghị định 165/2025/NĐ-CP quy định chi tiết các nội dung này. Ngoài ra, văn bản phải ghi rõ trách nhiệm xử lý dữ liệu đối với từng bên khi xung đột hoặc tranh chấp phát sinh.

+ Đối với dữ liệu cốt lõi, quan trọng: Bên nhận dữ liệu phải thực hiện đầy đủ nghĩa vụ bảo vệ dữ liệu, xử lý đúng mục đích, phương thức và phạm vi đã thỏa thuận. Điều này được cam kết ngay trong hợp đồng hoặc thoả thuận chuyển giao: bên nhận chỉ được sử dụng dữ liệu cho mục đích đã ghi, áp dụng các biện pháp bảo vệ cần thiết (*mã hóa, truy cập hạn chế, giám sát...*).

- *Nghĩa vụ và Trách nhiệm đối với Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu quốc gia*

+ Chủ quản cơ sở dữ liệu quốc gia: Các bộ, ngành, địa phương, tổ chức chủ quản Cơ sở Dữ liệu quốc gia phải phối hợp chặt chẽ với Trung tâm dữ liệu quốc gia. Cụ thể phải lập kế hoạch, lộ trình cụ thể chuyển dữ liệu về Trung tâm dữ liệu quốc gia. Bộ trưởng, Chủ tịch Ủy ban phải xây dựng và phê duyệt phương án chuyển hệ thống về Trung tâm dữ liệu quốc gia, trong đó xác định lộ trình và kinh phí. Nghị định 194/2025/NĐ-CP quy định chủ trì phối hợp xây dựng kế hoạch, lộ



trình và đề xuất kinh phí chuyển hệ thống Cơ sở Dữ liệu quốc gia về Trung tâm dữ liệu quốc gia.

Trong quá trình đồng bộ dữ liệu vào Trung tâm dữ liệu quốc gia, chủ quản vẫn quản lý vận hành cơ sở dữ liệu của mình. Cơ quan này phải đảm bảo an ninh, an toàn thông tin cho hệ thống của mình ngay khi dữ liệu được đồng bộ lên Trung tâm dữ liệu quốc gia. Nếu cơ quan sử dụng hạ tầng của Trung tâm dữ liệu quốc gia để triển khai hệ thống thông tin (*nhiều thuê chỗ đặt máy chủ, sử dụng cloud của Trung tâm dữ liệu quốc gia*), thì các cơ quan đó vẫn tự quản trị, vận hành lớp ứng dụng, dữ liệu và hệ điều hành. Trung tâm dữ liệu quốc gia chỉ cung cấp tầng hạ tầng dùng chung. Bên cạnh đó, chủ quản phải tiếp tục cập nhật và bảo trì dữ liệu thuộc phạm vi quản lý vào cơ sở dữ liệu quốc gia (*CSDLQG*). Không được yêu cầu thu thập lại dữ liệu mà đã có sẵn trong Cơ sở Dữ liệu quốc gia hoặc đã do cơ quan khác chia sẻ (*trừ trường hợp có lý do đặc biệt*). Mọi sai sót trong quản lý, lưu trữ, chia sẻ dữ liệu do mình đàm nhận thì chủ quản chịu trách nhiệm sửa chữa.

Chủ quản phải ban hành quy trình cập nhật dữ liệu chủ (*master data*), dữ liệu tham chiếu và các loại dữ liệu liên quan vào Cơ sở Dữ liệu quốc gia, cũng như quy chế khai thác, sử dụng Cơ sở Dữ liệu quốc gia. Quyền truy cập dữ liệu, kiến trúc dữ liệu, mô hình dữ liệu, tích hợp và lưu trữ đều phải tuân thủ các tiêu chuẩn được ban hành.

Chủ quản phải phân công đơn vị chịu trách nhiệm quản lý, duy trì dữ liệu; đảm bảo bộ máy và nhân sự (*tuyển dụng, đào tạo*) phù hợp để vận hành Cơ sở Dữ liệu quốc gia.

Cuối cùng, chủ quản phải đảm bảo hạ tầng kỹ thuật cho kết nối, chia sẻ dữ liệu (*bao gồm chuẩn giao tiếp, bảo mật*), thực hiện kết nối Cơ sở Dữ liệu quốc gia với các hệ thống khác thông qua nền tảng trung gian. Cơ sở Dữ liệu quốc gia cũng phải cung cấp dữ liệu lên Công dữ liệu quốc gia (*giống như các Cơ sở dữ liệu khác*) cho công khai dữ liệu.

+ Cung cấp dữ liệu cho Cơ sở dữ liệu tổng hợp quốc gia: Luật Giao dịch điện tử và Nghị định 194/2025/NĐ-CP quy định bắt buộc các cơ quan chủ quản



Cơ sở Dữ liệu quốc gia (*các bộ, ngành, địa phương, tổ chức chính trị - xã hội*) phải cung cấp dữ liệu cho Cơ sở Dữ liệu tổng hợp quốc gia. Theo quy định của pháp luật, sau khi đồng bộ, “các cơ sở dữ liệu quốc gia thực hiện đồng bộ, cập nhật dữ liệu về Cơ sở dữ liệu tổng hợp quốc gia. Dữ liệu sau khi được đồng bộ sẽ được cung cấp dưới dạng dữ liệu dùng chung, dữ liệu mở để các cơ quan, tổ chức, cá nhân khai thác, sử dụng”. Tóm lại, tất cả dữ liệu từ các Cơ sở Dữ liệu quốc gia, Cơ sở dữ liệu ngành đều phải được tập trung, đồng bộ vào Cơ sở Dữ liệu tổng hợp quốc gia để lưu trữ và khai thác tập trung; dữ liệu được cập nhật liên tục và được cung cấp ở dạng dùng chung/mở theo quy định.

+ Quản lý Cơ sở dữ liệu quốc gia: Các nhiệm vụ sau đây được giao cho đơn vị quản lý Cơ sở Dữ liệu quốc gia thuộc cơ quan chủ quản: ⁽¹⁾Xây dựng, duy trì và cập nhật dữ liệu trong Cơ sở Dữ liệu quốc gia theo phạm vi quản lý, đảm bảo hệ thống Cơ sở Dữ liệu quốc gia hoạt động ổn định, sẵn sàng 24/7; ⁽²⁾Không thu thập dữ liệu đã có trong Cơ sở Dữ liệu quốc gia hoặc đã được cơ quan khác chia sẻ (*trừ trường hợp đặc biệt*); ⁽³⁾Chịu trách nhiệm về mọi sai sót, thay đổi phát sinh trong quá trình quản lý, lưu trữ, chia sẻ dữ liệu; ⁽⁴⁾Ban hành quy trình cập nhật dữ liệu chủ, dữ liệu tham chiếu và các dữ liệu khác vào Cơ sở Dữ liệu quốc gia; tổ chức giám sát việc thực hiện; ⁽⁵⁾Xây dựng và thực hiện Quy chế khai thác, sử dụng Cơ sở Dữ liệu quốc gia (*cấp quyền truy cập, giới hạn đối tượng sử dụng, giám sát luồng dữ liệu...*); ⁽⁶⁾Quản lý kiến trúc dữ liệu: thiết kế, duy trì hạ tầng (*phần cứng, phần mềm*) đảm bảo tích hợp, chất lượng và khả năng truy cập; ⁽⁷⁾Quản lý mô hình dữ liệu: xác định cấu trúc, quan hệ dữ liệu trong Cơ sở Dữ liệu quốc gia để dữ liệu nhất quán và logic; ⁽⁸⁾Bảo đảm lưu trữ an toàn dữ liệu và vận hành hệ thống Cơ sở Dữ liệu quốc gia: lưu trữ dự phòng, duy trì khả năng truy xuất dữ liệu; ⁽⁹⁾Quản lý tích hợp dữ liệu: kết nối và đồng bộ dữ liệu từ các nguồn khác nhau (*các Cơ sở dữ liệu khác nhau*) vào Cơ sở Dữ liệu quốc gia; ⁽¹⁰⁾Quản lý dữ liệu chủ: lựa chọn công nghệ, công cụ và quy trình đảm bảo dữ liệu chủ trong Cơ sở Dữ liệu quốc gia được thu thập, cập nhật, khai thác chính xác và đầy đủ; ⁽¹¹⁾Phân công rõ đơn vị quản lý, duy trì dữ liệu; đảm bảo tổ chức nhân sự (*thu hút, tuyển dụng, đào tạo,*



thuê chuyên gia) phục vụ Cơ sở Dữ liệu quốc gia; ⁽¹²⁾Bảo đảm hạ tầng kỹ thuật cho kết nối, chia sẻ dữ liệu: thực hiện kết nối giữa Cơ sở Dữ liệu quốc gia và hệ thống thông tin khác qua nền tảng trung gian; cung cấp dữ liệu từ Cơ sở Dữ liệu quốc gia lên Cổng dữ liệu quốc gia; ⁽¹³⁾Ban hành quy định kỹ thuật về cấu trúc dữ liệu trao đổi, kết nối, chia sẻ giữa Cơ sở Dữ liệu quốc gia và Cơ sở dữ liệu các bộ, ngành, địa phương; ban hành quy chế khai thác, sử dụng dữ liệu Cơ sở Dữ liệu quốc gia.

- *Nghĩa vụ và Trách nhiệm về An ninh, An toàn Hệ thống và Dữ liệu*

+ Bảo vệ an ninh mạng và an toàn thông tin: Chủ quản hệ thống thông tin (*tức tổ chức quản lý hệ thống mạng, dữ liệu*) phải triển khai đồng bộ các biện pháp kỹ thuật và quản lý nhằm ngăn chặn, phát hiện và xử lý các mối đe dọa an ninh mạng. Cụ thể: ⁽¹⁾Áp dụng các biện pháp phòng chống mã độc, giám sát an ninh (*quét virus, dọn mã độc, vá lỗ hổng bảo mật*) để ngăn chặn xâm nhập và loại bỏ phần mềm độc hại; ⁽²⁾Phòng ngừa và gỡ bỏ kịp thời thông tin trái pháp luật hoặc sai sự thật trên hệ thống khi có yêu cầu; ⁽³⁾Ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật (*bí mật nhà nước, kinh doanh, đời tư*) bằng các giải pháp giám sát và xử lý thông tin; ⁽⁴⁾Hợp tác với lực lượng chuyên trách an ninh mạng (*Bộ Công an*) về phòng chống gián điệp mạng và bảo vệ thông tin bí mật; ⁽⁵⁾Triển khai phương án ứng phó với tấn công mạng (*DDOS, tấn công ứng dụng...*) cho hệ thống thông tin dưới quyền quản lý; ⁽⁶⁾Kịp thời thông báo cho cơ quan chuyên trách về an ninh mạng khi phát hiện vi phạm pháp luật liên quan (*ví dụ có người tấn công mạng hoặc bị xâm nhập trái phép*); ⁽⁷⁾Tuân thủ mọi quy định về bảo vệ an toàn thông tin mạng theo cấp độ hệ thống thông tin (*Luật An toàn thông tin 2015 quy định các cấp độ bảo mật, kiểm định an toàn thông tin*). Đặc biệt, hệ thống cơ sở dữ liệu quốc gia là hệ thống quan trọng quốc gia nên phải kiểm định an toàn thông tin trước khi vận hành và chịu trách nhiệm chung về an toàn mạng; ⁽⁸⁾Giám sát an toàn hệ thống (*thiết lập tường lửa, kiểm soát truy nhập, giám sát các tuyến kết nối chính, máy chủ quan trọng, thiết bị lỗi*); ⁽⁹⁾Đảm bảo hạ tầng kỹ thuật mạng (*máy chủ, lưu trữ, kết nối*) đáp ứng yêu cầu về an toàn theo quy định;



(¹⁰) Tạo điều kiện cần thiết (*mở cổng, cung cấp thông tin kỹ thuật*) để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng; (¹¹) Sau khi có yêu cầu từ cơ quan có thẩm quyền, phải chặn chia sẻ hoặc xóa thông tin trái pháp luật (*tin xấu, tin lừa đảo*) trên hệ thống trong thời gian tối đa 24 giờ và lưu giữ log thao tác; (¹²) Xây dựng và thường xuyên luyện tập phương án ứng phó sự cố an ninh mạng; báo cáo nhanh cho lực lượng chuyên trách khi xảy ra sự cố (*theo quy định của pháp luật về an toàn thông tin mạng, mức độ cấp báo tùy theo mức độ nghiêm trọng*).

+ Thông báo sự cố an toàn dữ liệu: Khi có sự cố an toàn dữ liệu (*ví dụ mất, lộ dữ liệu quan trọng*), chủ quản dữ liệu có nghĩa vụ thông báo kịp thời cho chủ sở hữu dữ liệu và có biện pháp giảm thiểu thiệt hại. Sau khi sự cố xảy ra, phải khẩn cấp thực hiện kế hoạch ứng phó đã lập và báo cáo với Bộ Công an/Bộ Quốc phòng (*tùy loại dữ liệu*) càng sớm càng tốt. Ví dụ, ngay khi phát hiện lộ dữ liệu quan trọng, dữ liệu cốt lõi, phải báo cáo Bộ Công an quản lý dữ liệu đó. Báo cáo phải mô tả sự cố, phạm vi ảnh hưởng, biện pháp khắc phục đã và sẽ thực hiện.

+ Quản lý nhân lực bảo vệ dữ liệu: Chủ quản dữ liệu phải quản lý chặt chẽ về mặt nhân sự: (¹) Đặt ra tiêu chí an ninh trong tuyển dụng, sử dụng, luân chuyển, đánh giá nhân viên IT và bảo mật dữ liệu; (²) Không bố trí người có tiền án về CNTT, viễn thông làm phụ trách an toàn dữ liệu; (³) Tất cả nhân viên liên quan đến xử lý dữ liệu nhạy cảm hoặc quan trọng phải ký cam kết, thỏa thuận về bảo mật thông tin; (⁴) Xây dựng kế hoạch đào tạo, nâng cao nhận thức an toàn thông tin, bảo vệ dữ liệu định kỳ (*ít nhất hàng năm*) cho nhân viên.

- Các Trách nhiệm khác:

+ Khi tổ chức lại, giải thể, phá sản: Chủ quản dữ liệu phải lập kế hoạch chuyển giao dữ liệu và thông báo cho các bên liên quan (*chủ sở hữu dữ liệu, đối tác, người sử dụng*) biết trước. Với dữ liệu cốt lõi, dữ liệu quan trọng, phải áp dụng biện pháp bảo đảm an toàn (*mã hóa, lưu trữ tách biệt, tự hủy...*) khi chuyển giao, đồng thời báo cáo phương án xử lý dữ liệu và thông tin bên nhận cho cơ quan chức năng liên quan (Bộ Công an, Bộ Quốc phòng) để giám sát.



+ Khi ủy thác xử lý dữ liệu: Chủ quản dữ liệu phải quy định trách nhiệm bảo mật của bên ủy thác và bên được ủy thác trong hợp đồng hoặc thỏa thuận. Đối với dữ liệu quan trọng, cốt lõi, bắt buộc bên ủy thác phải đánh giá năng lực và khả năng bảo vệ dữ liệu của bên nhận ủy thác trước khi ký hợp đồng.

Nhìn chung, tất cả quy định nêu trên nhằm đảm bảo hoạt động quản lý, khai thác, lưu trữ và chia sẻ dữ liệu của các cơ quan, tổ chức được thực hiện một cách nghiêm ngặt, an toàn và đúng luật. Đặc biệt trong bối cảnh kinh tế số và chuyển đổi số phát triển mạnh, mỗi chủ quản dữ liệu phải nhận thức rõ trách nhiệm pháp lý cao khi đảm bảo quyền lợi của cá nhân, tổ chức và lợi ích quốc gia.

2.1.4. Mối quan hệ giữa chủ thẻ dữ liệu, chủ sở hữu dữ liệu và chủ quản dữ liệu

2.1.4.1. Quan hệ giữa chủ thẻ dữ liệu và chủ sở hữu dữ liệu

Quan hệ giữa chủ thẻ dữ liệu và chủ sở hữu dữ liệu là mối quan hệ giữa người cung cấp dữ liệu (*hoặc bị thu thập dữ liệu*) và người thu thập, kiểm soát dữ liệu. Thường thể hiện dưới dạng quan hệ hợp đồng hoặc mặc nhiên: ví dụ, khi một cá nhân đăng ký sử dụng dịch vụ của doanh nghiệp, họ cung cấp dữ liệu cá nhân (*tên, tuổi, địa chỉ...*) lúc này cá nhân đồng ý cho doanh nghiệp thu thập và sử dụng dữ liệu đó cho mục đích cung cấp dịch vụ, hình thành một thỏa thuận (*có thể trong điều khoản người dùng*). Cá nhân trở thành chủ thẻ dữ liệu, doanh nghiệp là chủ sở hữu dữ liệu tương ứng.

Giữa hai bên có quyền và nghĩa vụ tương hỗ, chủ thẻ dữ liệu có quyền được tôn trọng quyền riêng tư, còn chủ sở hữu có quyền khai thác dữ liệu trong phạm vi được cho phép. Chủ sở hữu phải bảo đảm dữ liệu được sử dụng đúng mục đích, không xâm phạm lợi ích của chủ thẻ; ngược lại, chủ thẻ dữ liệu có trách nhiệm cung cấp thông tin chính xác và tuân thủ thỏa thuận. Pháp luật đóng vai trò “trọng tài” quy định giới hạn cho mối quan hệ này, đặc biệt nghiêng về bảo vệ bên yếu thế hơn là chủ thẻ dữ liệu. Ví dụ, luật quy định dữ liệu cá nhân của một người không được giao dịch mua bán nếu không có sự đồng ý của chính người đó. Điều này bảo vệ chủ thẻ dữ liệu khỏi việc bị biến thông tin cá nhân thành hàng hóa trao



tay khi họ chưa cho phép. Ngay cả khi họ đồng ý, nhà nước vẫn có thể giới hạn (như Nghị định 13/2023/NĐ-CP cấm triệt để việc mua bán dữ liệu cá nhân, nhằm bảo vệ quyền riêng tư tuyệt đối).

Thêm vào đó, chủ sở hữu dữ liệu phải thiết lập cơ chế để chủ thẻ thực hiện quyền của mình. Ví dụ: một mạng xã hội (*chủ sở hữu dữ liệu*) phải có tính năng cho người dùng (*chủ thẻ dữ liệu*) tải về bản sao dữ liệu của họ, hoặc xóa tài khoản (*tương ứng xóa dữ liệu*) nếu người dùng yêu cầu. Khi có yêu cầu chính đáng từ chủ thẻ, chủ sở hữu không được gây khó khăn, cản trở. Mọi quan hệ này mang tính bất đối xứng (vì bên nắm dữ liệu thường có lợi thế hơn), nên luật phải điều chỉnh để cân bằng, trao công cụ cho chủ thẻ dữ liệu đòi quyền lợi (như khiếu nại, khởi kiện). Nếu chủ sở hữu vi phạm (ví dụ dùng dữ liệu sai mục đích, để lộ dữ liệu), chủ thẻ dữ liệu có thể kiện đòi bồi thường và cơ quan quản lý có thể phạt chủ sở hữu. Trách nhiệm pháp lý của chủ sở hữu do đó cũng là một cơ chế bảo vệ lợi ích cho chủ thẻ dữ liệu.

Trong một số trường hợp, chủ sở hữu dữ liệu có thể chính là Nhà nước, còn chủ thẻ dữ liệu là công dân. Luật Dữ liệu cũng áp dụng cho cơ quan nhà nước, đòi hỏi cơ quan nhà nước khi thu thập thông tin người dân phải tôn trọng quyền riêng tư và chỉ sử dụng dữ liệu vào mục đích quản lý đã định. Công dân có quyền tiếp cận dữ liệu về mình trong các cơ sở dữ liệu quốc gia (ví dụ: tra cứu thông tin cư trú, hộ tịch) thể hiện quyền dữ liệu cá nhân trong quan hệ với Nhà nước.

2.1.4.2. Quan hệ giữa chủ sở hữu dữ liệu và chủ quản dữ liệu

Quan hệ giữa chủ sở hữu dữ liệu và chủ quản dữ liệu thường là quan hệ hợp đồng dịch vụ (nếu khác tổ chức) hoặc quan hệ phân công nội bộ (nếu cùng một tổ chức). Chủ sở hữu đóng vai trò ủy quyền, giao cho chủ quản những nhiệm vụ nhất định liên quan tới dữ liệu. Chủ quản phải phối hợp chặt chẽ với chủ sở hữu, bởi mọi hành động của họ phải theo yêu cầu của chủ sở hữu. Chủ sở hữu cần cung cấp đầy đủ thông tin hướng dẫn, giám sát chủ quản; ngược lại chủ quản phải báo cáo, tham vấn chủ sở hữu khi có vấn đề vượt thẩm quyền. Sự phối hợp này được quy định ngay trong luật: ví dụ, chủ quản dữ liệu của cơ quan nhà nước phải phối



hợp với Trung tâm dữ liệu quốc gia trong quản trị dữ liệu; hay chủ quản và chủ sở hữu (*không phải cơ quan nhà nước*) cần cù điều kiện thực tế để thực hiện quản trị dữ liệu, hiểu là họ tự thỏa thuận, phối hợp trong nội bộ mình.

Một vấn đề quan trọng trong quan hệ này là phân chia trách nhiệm khi có sự cố. Luật quy định cả chủ sở hữu và chủ quản đều chịu trách nhiệm về chất lượng, tính hợp pháp của dữ liệu do mình cung cấp, xác nhận. Điều này hàm ý: nếu dữ liệu kém chất lượng hay vi phạm (*sai lệch, bất hợp pháp*), thì cả chủ sở hữu và chủ quản đều có lỗi. Trên thực tế, hợp đồng giữa họ sẽ cụ thể hóa: ví dụ, chủ quản chịu trách nhiệm về khía cạnh an ninh kỹ thuật, còn chủ sở hữu chịu về nội dung dữ liệu. Khi xảy ra sự cố (*ví dụ lộ thông tin khách hàng*), chủ sở hữu có thể phải xin lỗi và đền bù cho khách hàng, sau đó có quyền yêu cầu chủ quản bồi hoàn nếu lỗi thuộc về chủ quản (*theo hợp đồng*). Ngược lại, nếu lỗi do chỉ đạo từ chủ sở hữu (*ví dụ yêu cầu thiết lập an ninh lỏng lẻo để tiện khai thác, dẫn đến bị hack*), chủ quản có thể không chịu trách nhiệm. Tất cả đòi hỏi hợp đồng dịch vụ dữ liệu phải chặt chẽ, lường trước rủi ro và chia sẻ trách nhiệm rõ ràng.

2.1.4.3. Quan hệ giữa chủ thể dữ liệu và chủ quản dữ liệu

Quan hệ giữa chủ thể dữ liệu và chủ quản dữ liệu thông thường, chủ thể dữ liệu không tương tác trực tiếp nhiều với chủ quản, mà thông qua chủ sở hữu. Tuy nhiên, luật vẫn dự liệu một số tình huống tiếp xúc trực tiếp: Chẳng hạn, chủ thể dữ liệu có quyền yêu cầu trực tiếp chủ quản xóa dữ liệu của mình. Điều này có thể xảy ra khi chủ thể biết ai đang vận hành dữ liệu (*ví dụ biết công ty A đang quản lý hệ thống cho công ty B nơi mình dùng dịch vụ*). Khi nhận được yêu cầu, chủ quản phải xử lý như đã nói. Chủ thể dữ liệu cũng có quyền khai thác dữ liệu về mình từ hệ thống, đôi khi qua sự hỗ trợ kỹ thuật của chủ quản. Một ví dụ: cá nhân muốn biết thông tin dữ liệu định danh của mình trong Cơ sở dữ liệu Quốc gia, có thể liên hệ đơn vị quản trị hệ thống (*chủ quản*) để được cấp tài khoản tra cứu. Lúc này, chủ quản thực hiện theo quy trình do pháp luật và chủ sở hữu (*cơ quan nhà nước quản lý Cơ sở dữ liệu đó*) quy định.



Mỗi quan hệ này nhìn chung bị chi phối bởi chủ sở hữu: chủ thẻ dữ liệu thường sẽ liên hệ chủ sở hữu trước (*ví dụ gửi yêu cầu xóa dữ liệu đến công ty cung cấp dịch vụ*), công ty đó chuyển cho bộ phận kỹ thuật (*chủ quản*) thực hiện. Chủ thẻ dữ liệu ít khi làm việc trực tiếp với bên kỹ thuật trừ phi được hướng dẫn. Do đó, trách nhiệm của chủ sở hữu là thiết lập đầu mối tiếp nhận yêu cầu của chủ thẻ dữ liệu và phân luồng nội bộ tới chủ quản để giải quyết. Nếu chủ quản không thực hiện đúng (*ví dụ chậm trễ xóa dữ liệu*), chủ thẻ dữ liệu có thể vẫn quy trách nhiệm cho chủ sở hữu và chủ sở hữu sẽ yêu cầu chủ quản giải trình.

Trong một số trường hợp đặc thù, chủ thẻ dữ liệu có thể liên hệ chủ quản là cơ quan nhà nước. Chẳng hạn, Luật Dữ liệu cho phép cá nhân (*chủ thẻ dữ liệu*) khai thác và sử dụng dữ liệu cá nhân của mình nếu được sự đồng ý của Trung tâm dữ liệu quốc gia. Ở đây Trung tâm dữ liệu quốc gia (*Bộ Công an*) đóng vai trò chủ quản vận hành kho dữ liệu quốc gia, cho phép cá nhân truy cập dữ liệu về mình trong Cơ sở Dữ liệu tổng hợp. Như vậy, cá nhân vừa là người được phục vụ vừa giám sát cách chủ quản nhà nước quản lý dữ liệu về mình.

2.1.4.4. Nguyên tắc phân quyền, cơ chế phối hợp

Chủ sở hữu giữ quyền quyết định cao nhất với dữ liệu, chủ quản có quyền hành động trên dữ liệu theo ủy quyền, còn chủ thẻ dữ liệu có quyền giám sát việc sử dụng dữ liệu về mình và đòi hỏi lợi ích chính đáng.

Chủ sở hữu và chủ quản thường sẽ ký hợp đồng xử lý dữ liệu (*data processing agreement*) nếu là hai pháp nhân khác nhau, trong đó quy định: phạm vi xử lý, loại dữ liệu, mục đích, biện pháp bảo vệ, trách nhiệm khi vi phạm...

Chủ sở hữu có thể ban hành quy chế nội bộ hoặc chính sách cho thấy rõ vai trò của các bên. Ví dụ, doanh nghiệp ban hành chính sách bảo mật nêu rằng “công ty X là đơn vị lưu trữ dữ liệu cho tôi” để khách hàng biết. Sự minh bạch này giúp chủ thẻ dữ liệu hiểu ai đang giữ dữ liệu của mình, từ đó họ biết phải khiếu nại ai khi có sự cố.

Khi xảy ra xung đột (*ví dụ rò rỉ dữ liệu*), Chủ sở hữu, chủ quản phải hợp tác điều tra, không đổ lỗi vòng quanh. Pháp luật sẽ xem xét trách nhiệm từng bên:



nếu lỗi tại chủ quản (*lỗi hỏng bảo mật*), chủ sở hữu vẫn bị phạt (*vì dữ liệu của anh, anh phải chịu*) nhưng sau đó có quyền truy đòi chủ quản; nếu lỗi do chủ sở hữu (*cấu hình sai*), chủ quản có thể không bị phạt hành chính nhưng vẫn chịu tổn hại uy tín.

Cơ quan quản lý nhà nước (*Bộ Công an*) đóng vai trò giám sát, ban hành tiêu chuẩn, quy chuẩn kỹ thuật, thanh tra định kỳ việc bảo vệ dữ liệu. Nhờ đó, các bên có trách nhiệm luôn phải phối hợp tuân thủ theo hướng dẫn của cơ quan quản lý. Ví dụ, Bộ Công an có thể kiểm tra một doanh nghiệp về việc thực hiện xóa dữ liệu cá nhân khi có yêu cầu, nếu phát hiện doanh nghiệp (*chủ sở hữu*) chưa yêu cầu chủ quản làm hoặc chủ quản làm không triệt để, cả hai đều bị nhắc nhở/phạt.

Ngoài ra, trong xử lý xung đột, không tránh khỏi trường hợp lợi ích của các bên va chạm nhau, vì vậy được quy định:

- Mâu thuẫn giữa chủ sở hữu và chủ thẻ dữ liệu: Chủ sở hữu muốn khai thác dữ liệu tối đa để kinh doanh, còn chủ thẻ muốn giữ bí mật cá nhân. Xung đột này giải quyết bằng yêu cầu chủ sở hữu phải xin phép chủ thẻ (*đồng ý*) trước khi dùng dữ liệu cá nhân vào mục đích thương mại và chủ thẻ có quyền rút lại sự đồng ý. Nếu chủ thẻ không đồng ý bán dữ liệu, chủ sở hữu không được bán (*vì cấm giao dịch dữ liệu khi chưa có đồng ý*). Đây là sự ưu tiên rõ rệt cho quyền cá nhân.

- Mâu thuẫn giữa chủ quản và chủ thẻ dữ liệu: Chủ quản có thể muốn giữ dữ liệu lâu để dễ quản lý, nhưng chủ thẻ đòi xóa ngay khi không dùng nữa. Luật nghiêm về chủ thẻ: khi không còn cần thiết cho mục đích thì dữ liệu phải được hủy và thông báo cho chủ thẻ. Chủ quản không thể tự ý giữ lại chỉ vì “tiện việc”.

- Mâu thuẫn giữa chủ sở hữu và chủ quản: Chủ sở hữu muốn tiết kiệm chi phí nên không đầu tư bảo mật, chủ quản thấy không đủ an toàn. Nếu chủ quản chiêu theo để giảm chi phí, có thể vi phạm tiêu chuẩn bảo vệ. Luật yêu cầu tuân thủ chuẩn an toàn, nên trong trường hợp này chủ quản phải tuân theo chuẩn mực kỹ thuật, thuyết phục chủ sở hữu chi đủ cho bảo mật. Nếu chủ sở hữu không đồng ý, chủ quản có quyền từ chối vận hành trong điều kiện không an toàn (*hoặc ghi rõ miễn trừ trách nhiệm trong hợp đồng nếu buộc phải làm*).



Nhìn chung, khuôn khổ pháp lý càng rõ ràng thì xung đột càng dễ giải quyết vì “luật đã quy định sẵn phải làm gì”. Luật Dữ liệu 2024 và các văn bản liên quan đã tạo nền tảng để các bên biết giới hạn của mình; luật yêu cầu các bên lưu vết xử lý, đánh giá tác động, phân cấp phân quyền rõ (*minh chứng cho trách nhiệm*).

Một ví dụ minh họa quan hệ ba bên: Một công ty cung cấp dịch vụ gọi xe công nghệ. Người dùng A đăng ký tài khoản và đặt xe – A là chủ thể dữ liệu (*có thông tin cá nhân, vị trí chuyến đi...*). Công ty gọi xe là chủ sở hữu dữ liệu (*thu thập dữ liệu của A và tài xé để vận hành dịch vụ*). Công ty thuê một công ty cloud XYZ để lưu trữ cơ sở dữ liệu – XYZ là chủ quản dữ liệu (*vận hành server theo yêu cầu*). Khi A yêu cầu xóa tài khoản và dữ liệu, công ty gọi xe phải tiếp nhận yêu cầu, xác minh và sau đó yêu cầu tiếp công ty XYZ xóa dữ liệu của A trên hệ thống. XYZ thực hiện xóa và xác nhận lại với công ty gọi xe, đồng thời công ty gọi xe thông báo lại cho A biết dữ liệu đã được xóa. Nếu quy trình này trọn tru, quyền của A được đảm bảo, trách nhiệm các bên rõ ràng. Giả sử XYZ chậm xóa dẫn đến dữ liệu A vẫn bị giữ, A khiếu nại lên cơ quan chức năng. Lúc này, công ty gọi xe (*chủ sở hữu*) sẽ bị xử lý trước tiên do không đảm bảo kịp thời, sau đó họ có thể quy trách nhiệm XYZ theo hợp đồng. Cơ quan chức năng có thể phạt cả hai nếu xác định cả hai cùng lỗi. Tình huống này cho thấy tầm quan trọng của sự phối hợp nhịp nhàng cũng như việc đúc kết trách nhiệm rõ ràng từ đầu.

2.2. Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước

2.2.1. Nghĩa vụ bắt buộc của tổ chức, cá nhân trong xử lý dữ liệu

Các văn bản pháp luật chuyên ngành về dữ liệu số và bảo vệ dữ liệu cá nhân đã thiết lập những nghĩa vụ pháp lý bắt buộc nhằm đảm bảo mọi tổ chức, cá nhân (*không phải cơ quan nhà nước*) tuân thủ khi tham gia hoạt động dữ liệu. Luật Dữ liệu 2024, Luật Bảo vệ Dữ liệu Cá nhân 2025 và Nghị định 13/2023/NĐ-CP đều quy định rõ các nguyên tắc, yêu cầu trong việc thu thập, xử lý dữ liệu mà các chủ thể phi nhà nước phải tuân thủ. Những nghĩa vụ này tập trung vào các nguyên tắc



cơ bản như: tính hợp pháp, tính chính xác, minh bạch, giới hạn mục đích, bảo mật, an toàn dữ liệu, giới hạn lưu trữ và trách nhiệm giải trình.

Nguyên tắc/Nghĩa vụ	Luật Dữ liệu 2024	Luật Bảo vệ Dữ liệu cá nhân 2025
Tính hợp pháp (xử lý đúng quy định pháp luật)	Điều 5(1): Tuân thủ Hiến pháp, luật và bảo đảm quyền hợp pháp của các bên.	Điều 3(1): Tuân thủ Hiến pháp, luật này và pháp luật liên quan.
Minh bạch (chủ thể được biết về xử lý dữ liệu)	Điều 5(2): Bảo đảm công khai, minh bạch trong tiếp cận, khai thác dữ liệu.	Điều 4(1): Quyền được biết của chủ thể dữ liệu và quyền được thông báo về xử lý dữ liệu.
Giới hạn mục đích (chỉ xử lý trong phạm vi mục đích cụ thể)	<i>Cơ quan nhà nước nhận dữ liệu phải dùng đúng mục đích</i>	Điều 3(2): Chỉ được thu thập, xử lý đúng phạm vi, mục đích cụ thể, rõ ràng .
Hạn chế thu thập, không mua bán dữ liệu	<i>Khuyến khích chia sẻ hợp pháp</i>	Khoản 6, Điều 7: Hành vi bị nghiêm cấm: Mua, bán dữ liệu cá nhân, trừ trường hợp luật có quy định khác.
Tính chính xác, đầy đủ (cập nhật khi cần thiết)	Điều 12(1): Chất lượng dữ liệu chính xác, hợp lệ, toàn vẹn, đầy đủ, cập nhật kịp thời .	Điều 3(3): Bảo đảm dữ liệu cá nhân chính xác và được chỉnh sửa, bổ sung khi cần; lưu trữ trong thời gian phù hợp mục đích.
Bảo mật và an toàn dữ liệu (ngăn ngừa truy cập trái phép, rõ rệt)	Điều 5(3): Bảo đảm toàn vẹn, tin cậy, an ninh, an toàn trong thu thập, cập nhật dữ liệu.	Điều 3(4): Thực hiện đồng bộ các biện pháp kỹ thuật, tổ chức phù hợp để bảo vệ dữ liệu cá nhân.
Giới hạn lưu trữ (chỉ lưu giữ trong thời gian cần thiết)	Điều 14(2): Yêu cầu tuân thủ quy định lưu trữ với dữ liệu cốt lõi, quan trọng).	Điều 3(3): Dữ liệu cá nhân được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý, trừ luật khác quy định.

Bảng trên cho thấy sự tương đồng về các nguyên tắc xử lý dữ liệu cốt lõi trong các văn bản pháp luật. Về tính hợp pháp, mọi hoạt động xử lý dữ liệu phải



có cơ sở pháp lý rõ ràng và tuân thủ pháp luật hiện hành. Luật Bảo vệ Dữ liệu Cá nhân 2025 yêu cầu xử lý dữ liệu phải tuân thủ Hiến pháp, luật này và các luật liên quan. Điều này có nghĩa là doanh nghiệp, tổ chức tư nhân khi thu thập, sử dụng dữ liệu phải dựa trên sự đồng ý hợp lệ của chủ thẻ dữ liệu hoặc một căn cứ pháp lý phù hợp (ví dụ: *thực hiện hợp đồng, nghĩa vụ pháp luật, lợi ích công cộng... theo quy định của pháp luật về bảo vệ dữ liệu*).

Về tính minh bạch, pháp luật đòi hỏi chủ thẻ dữ liệu được thông tin về việc dữ liệu của họ được xử lý như thế nào. Luật Dữ liệu 2024 đề cao sự công khai, minh bạch trong tiếp cận và sử dụng dữ liệu. Do đó, các tổ chức, doanh nghiệp có nghĩa vụ công bố chính sách quyền riêng tư, thông báo cho cá nhân về mục đích, phạm vi thu thập dữ liệu và bên sẽ xử lý dữ liệu... Minh bạch cũng bao gồm việc cung cấp cơ chế để chủ thẻ thực hiện quyền của mình (*truy cập, chỉnh sửa, xóa dữ liệu...*). Ví dụ: Luật Bảo vệ Dữ liệu Cá nhân 2025 liệt kê quyền của chủ thẻ dữ liệu như được biết, đồng ý hoặc không đồng ý, truy cập, rút consent, xóa, hạn chế xử lý, phản đối, khiếu nại và yêu cầu bồi thường. Tổ chức, cá nhân kiểm soát dữ liệu phải tạo điều kiện để chủ thẻ thực thi các quyền này, nếu không sẽ bị coi là vi phạm nghĩa vụ minh bạch và tôn trọng quyền chủ thẻ.

Giới hạn mục đích sử dụng dữ liệu cũng là một nghĩa vụ quan trọng. Doanh nghiệp chỉ được phép thu thập và xử lý dữ liệu phù hợp với mục đích cụ thể đã xác định và thông báo. Luật Bảo vệ Dữ liệu Cá nhân 2025 quy định rõ dữ liệu cá nhân chỉ được xử lý đúng phạm vi, mục đích cụ thể, rõ ràng đã đề ra (*Khoản 2 Điều 3*). Dữ liệu phải được xử lý đúng với mục đích mà bên kiểm soát đã đăng ký, tuyên bố; không được xử lý cho mục đích khác khi chưa có sự đồng ý lại của chủ thẻ. Song song đó, việc thu thập và mua bán dữ liệu chỉ thu thập dữ liệu trong phạm vi cần thiết và nghiêm cấm mua bán dữ liệu cá nhân dưới mọi hình thức (*trừ trường hợp pháp luật cho phép*). Điều này buộc các công ty không được “thu thập thừa” dữ liệu so với nhu cầu công bố, đồng thời ngăn chặn tình trạng trao đổi, thương mại hóa dữ liệu cá nhân trái phép.



Bên cạnh đó, đảm bảo tính chính xác của dữ liệu là nghĩa vụ bắt buộc nhằm bảo vệ quyền lợi của chủ thể và chất lượng dữ liệu. Luật Dữ liệu 2024 coi đảm bảo chất lượng dữ liệu là yêu cầu bắt buộc, bao gồm tính chính xác, hợp lệ, đầy đủ và cập nhật kịp thời của dữ liệu. Luật Bảo vệ Dữ liệu Cá nhân 2025 cũng yêu cầu dữ liệu cá nhân phải được cập nhật, bổ sung khi cần thiết để bảo đảm chính xác và chỉ lưu trữ trong thời gian phù hợp với mục đích. Các doanh nghiệp do vậy có nghĩa vụ thiết lập quy trình để kiểm tra, cập nhật, hiệu chỉnh dữ liệu định kỳ, xóa bỏ dữ liệu sai hoặc lạc hậu, đảm bảo không sử dụng dữ liệu sai lệch ảnh hưởng đến quyền lợi cá nhân. Nếu chủ thể yêu cầu chỉnh sửa, xóa dữ liệu, bên kiểm soát phải thực hiện kịp thời theo luật định.

Bảo mật và an toàn dữ liệu là nhóm nghĩa vụ nhằm ngăn ngừa truy cập, tiết lộ, mót mát hoặc sử dụng dữ liệu trái phép. Pháp luật yêu cầu tổ chức, cá nhân xử lý dữ liệu phải áp dụng các biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ dữ liệu trong suốt vòng đời xử lý. Luật Bảo vệ Dữ liệu Cá nhân 2025 yêu cầu thực hiện đồng bộ, hiệu quả các giải pháp thể chế, kỹ thuật, con người để bảo vệ dữ liệu (*khoản 4 Điều 3*). Những biện pháp này bao gồm: mã hóa dữ liệu, ẩn danh/hạn chế truy cập, tường lửa, hệ thống quản lý quyền truy cập, đào tạo nhân sự,... Ví dụ: đối với dữ liệu thuộc danh mục bí mật nhà nước, Luật Dữ liệu quy định bắt buộc phải mã hóa bằng mật mã của cơ yếu khi lưu trữ, truyền, nhận trên mạng. Các tổ chức tư nhân cũng được khuyến khích tự quyết định việc mã hóa dữ liệu của mình và sử dụng các giải pháp mã hóa phù hợp để bảo vệ dữ liệu trong quản trị (*Điều 22 Luật Dữ liệu*). Nhìn chung, nghĩa vụ bảo mật đòi hỏi doanh nghiệp phải đảm bảo an ninh mạng và an toàn thông tin cho hệ thống CNTT có chứa dữ liệu cá nhân, tuân thủ các tiêu chuẩn kỹ thuật về an toàn thông tin do cơ quan có thẩm quyền ban hành.

Đi đôi với bảo mật là giới hạn thời gian lưu trữ dữ liệu. Để giảm rủi ro lọt và vi phạm quyền riêng tư, pháp luật quy định dữ liệu chỉ được lưu giữ trong thời hạn cần thiết cho mục đích đã định. Luật Bảo vệ Dữ liệu Cá nhân nhấn mạnh dữ liệu được lưu trữ trong khoảng thời gian phù hợp mục đích, trừ trường hợp luật



có quy định khác. Sau khi đạt được mục đích hoặc hết thời hạn, dữ liệu cá nhân phải được xóa hoặc hủy nếu không có cơ sở pháp lý nào khác để tiếp tục lưu giữ. Việc không hủy dữ liệu khi đã hết mục đích có thể bị chế tài.

Ngoài các nguyên tắc chung nêu trên, pháp luật còn đặt ra những nghĩa vụ cụ thể khác đối với tổ chức, cá nhân xử lý dữ liệu nhằm bảo đảm quyền của chủ thẻ dữ liệu:

- **Thứ nhất**, nghĩa vụ thu thập sự đồng ý hợp pháp: Đối với dữ liệu cá nhân thông thường, nguyên tắc chung là phải có sự đồng ý rõ ràng của chủ thẻ dữ liệu trước khi xử lý, trừ các trường hợp luật định (*nhiều để bảo vệ tính mạng, thực thi hợp đồng, nghĩa vụ pháp lý, lợi ích công cộng...*).

- **Thứ hai**, nghĩa vụ bảo vệ dữ liệu trẻ em và người yếu thế: Luật Bảo vệ Dữ liệu Cá nhân 2025 có quy định riêng bảo vệ dữ liệu của trẻ em, người mất năng lực hành vi, người khó khăn nhận thức (Điều 24). Theo đó, việc xử lý dữ liệu trẻ em dưới 7 tuổi phải có sự đồng ý của cha mẹ/người giám hộ; trẻ em từ đủ 7 tuổi trở lên thì cần cả sự đồng ý của trẻ và của người đại diện. Doanh nghiệp có nghĩa vụ kiểm tra độ tuổi, xin consent kép (*dual consent*) khi thu thập dữ liệu trẻ em và ngừng xử lý dữ liệu nếu người đại diện hợp pháp rút lại sự đồng ý hoặc cơ quan có thẩm quyền yêu cầu vì quyền lợi trẻ em (Điều 24(3)). Tương tự, dữ liệu người yếu thế phải được đại diện thực hiện quyền và được bảo vệ đặc biệt. Những yêu cầu này đòi hỏi tổ chức phải có cơ chế phân loại dữ liệu theo độ tuổi, xác minh tuổi và sự chấp thuận của phụ huynh, cũng như cẩn trọng khi công bố thông tin riêng tư của trẻ em (*vi phạm có thể bị xử lý nghiêm theo luật trẻ em*).

- **Thứ ba**, nghĩa vụ thực hiện Đánh giá tác động xử lý dữ liệu: Đây là một nghĩa vụ mới quan trọng được Luật Bảo vệ Dữ liệu Cá nhân 2025 đặt ra nhằm đánh giá rủi ro bảo mật, riêng tư trước và trong quá trình xử lý dữ liệu. Cụ thể, Điều 21 yêu cầu bên kiểm soát dữ liệu (*hoặc bên kiểm soát và xử lý*) phải lập và lưu trữ hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, đồng thời gửi một bản chính cho Cơ quan chuyên trách BV dữ liệu cá nhân trong vòng 60 ngày kể từ ngày bắt đầu xử lý dữ liệu cá nhân. Đánh giá này chỉ cần thực hiện một lần cho suốt quá



trình hoạt động, nhưng phải cập nhật định kỳ mỗi 6 tháng hoặc khi có thay đổi rủi ro (*Điều 22*). Nội dung Đánh giá tác động xử lý dữ liệu thường bao gồm mô tả hoạt động xử lý, đánh giá tính cần thiết và tỷ lệ, phân tích rủi ro xâm phạm quyền riêng tư, biện pháp giảm thiểu rủi ro.... Đây là nghĩa vụ khá nặng nề, đặc biệt đối với doanh nghiệp vừa và nhỏ, nhưng mục đích để bảo đảm các đơn vị chủ động nhận diện và khắc phục lỗ hổng bảo mật trước khi sự cố xảy ra. Nghị định 13/2023 trước đó (*dù không bắt buộc DPIA rộng rãi như Luật*) cũng khuyến khích việc đánh giá rủi ro xử lý dữ liệu, nhất là đối với chuyển dữ liệu xuyên biên giới và Luật đã luật hóa yêu cầu này. Lưu ý rằng Luật miễn trừ tạm thời cho doanh nghiệp nhỏ, siêu nhỏ trong 5 năm đầu, nhưng về lâu dài, Đánh giá tác động xử lý dữ liệu sẽ là nghĩa vụ chung để nâng cao mức tuân thủ.

- **Thứ tư**, nghĩa vụ đăng ký đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài: Liên quan đến dữ liệu xuyên biên giới, Luật Bảo vệ Dữ liệu Cá nhân 2025 quy định tại Điều 20 về việc nếu một tổ chức có hoạt động chuyển dữ liệu cá nhân ra khỏi lãnh thổ Việt Nam (*ví dụ lưu trữ trên máy chủ nước ngoài, hoặc cung cấp dữ liệu cho tổ chức nước ngoài*), thì phải lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới và gửi cho cơ quan chuyên trách trong vòng 60 ngày từ khi bắt đầu chuyển. Hồ sơ này đánh giá các rủi ro khi dữ liệu ra nước ngoài (*về an ninh, quyền riêng tư*) và đề xuất biện pháp quản lý. Việc chuyển dữ liệu cốt lõi, quan trọng xuyên biên giới càng bị kiểm soát chặt: Luật Dữ liệu 2024 yêu cầu phải đảm bảo lợi ích quốc gia, công cộng, quyền lợi hợp pháp của chủ thể dữ liệu khi chuyển dữ liệu quan trọng/cốt lõi ra khỏi Việt Nam. Chính phủ sẽ quy định tiêu chí dữ liệu cốt lõi, quan trọng và chi tiết thủ tục (*Điều 23 Luật Dữ liệu*). Do đó, doanh nghiệp Việt Nam nếu muốn đưa dữ liệu người dùng ra lưu trữ trên cloud nước ngoài hoặc chia sẻ cho đối tác ở nước ngoài cần thực hiện đánh giá tác động và tuân thủ các điều kiện do pháp luật đặt ra (*ví dụ có thể phải cam kết dữ liệu được bảo vệ tương đương, có sự chấp thuận của cơ quan quản lý...*). Nếu không tuân thủ, cơ quan chức năng có thể yêu cầu kiểm tra hoạt động chuyển dữ liệu và thậm chí đình chỉ hoặc cấm chuyển giao nếu vi phạm (*Điều*



20(4) Luật Bảo vệ Dữ liệu Cá nhân 2025 cho phép cơ quan Bảo vệ dữ liệu cá nhân quyết định kiểm tra hoạt động chuyển dữ liệu xuyên biên giới).

- **Thứ năm**, nghĩa vụ bổ nhiệm đầu mối bảo vệ dữ liệu: Để tuân thủ hiệu quả, các tổ chức, doanh nghiệp được yêu cầu thiết lập bộ máy quản trị dữ liệu nội bộ. Luật Bảo vệ Dữ liệu Cá nhân 2025 tại Điều 33 quy định lực lượng bảo vệ dữ liệu cá nhân bao gồm cơ quan chuyên trách thuộc Bộ Công an, bộ phận bảo vệ dữ liệu tại tổ chức, các dịch vụ bảo vệ dữ liệu và các tổ chức cá nhân được huy động. Khoản 2 Điều 33 luật yêu cầu cơ quan, tổ chức phải chỉ định bộ phận hoặc nhân sự đủ năng lực để bảo vệ dữ liệu cá nhân, hoặc thuê dịch vụ bảo vệ dữ liệu bên ngoài. Điều này tương tự khái niệm Data Protection Officer (*DPO*) trong thông lệ quốc tế. Nhiệm vụ của nhân sự/bộ phận này là giám sát việc tuân thủ pháp luật bảo vệ dữ liệu trong tổ chức, tư vấn cho lãnh đạo và làm đầu mối với cơ quan quản lý. Tuy nhiên, luật cũng hiểu khó khăn cho doanh nghiệp nhỏ nên cho phép doanh nghiệp nhỏ, khởi nghiệp có thể chưa thực hiện nghĩa vụ này ngay trong 5 năm đầu (vì Điều 33(2) thuộc diện được miễn 5 năm theo khoản 2 Điều 38). Dù vậy, về lâu dài, việc có bộ phận chuyên trách về dữ liệu sẽ là bắt buộc với tất cả tổ chức xử lý dữ liệu cá nhân ở mức độ đáng kể. Đây là bước chuẩn bị quan trọng để bảo đảm nghĩa vụ được thực thi trong thực tế, bởi có nhân sự phụ trách thì các quy trình như duyệt *DPIA*, trả lời yêu cầu chủ thể dữ liệu, xử lý sự cố rò rỉ... mới được tiến hành kịp thời, đúng pháp luật.

Tóm lại, nghĩa vụ bắt buộc đối với tổ chức, cá nhân (*không phải cơ quan nhà nước*) trong hoạt động dữ liệu trải rộng trên nhiều khía cạnh, nhưng đều hướng tới mục tiêu cuối cùng là bảo đảm tính hợp pháp, an toàn của dữ liệu và bảo vệ quyền, lợi ích hợp pháp của chủ thể dữ liệu. Các doanh nghiệp cần tuân thủ đầy đủ các nghĩa vụ về nguyên tắc xử lý (*hợp pháp, chính xác, minh bạch...*), tạo lập quy trình nội bộ để thực hiện các yêu cầu về bảo mật, đánh giá tác động, xử lý yêu cầu của người dùng, cũng như chuẩn bị cho việc kiểm tra, giám sát của cơ quan quản lý.



2.2.2. Cơ chế kiểm tra, giám sát và xử lý vi phạm

Bên cạnh việc đặt ra nghĩa vụ, pháp luật cũng thiết lập cơ chế kiểm tra, giám sát việc thực hiện các nghĩa vụ đó, đồng thời quy định các hình thức chế tài xử lý đối với tổ chức, cá nhân vi phạm. Cơ chế này bao gồm: phân định vai trò cơ quan quản lý, hoạt động thanh tra kiểm tra định kỳ và đột xuất, các hình thức xử phạt hành chính, trách nhiệm dân sự, hình sự và áp dụng các biện pháp kỹ thuật để ngăn chặn vi phạm. Cụ thể:

- **Thứ nhất**, vai trò của cơ quan quản lý nhà nước: Theo Luật Dữ liệu 2024 và Luật Bảo vệ Dữ liệu Cá nhân 2025, Bộ Công an được giao là cơ quan đầu mối chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về dữ liệu số và bảo vệ dữ liệu cá nhân trên phạm vi toàn quốc. Cụ thể, khoản 2 Điều 36 Luật Bảo vệ Dữ liệu Cá nhân 2025 quy định Bộ Công an là cơ quan đầu mối thống nhất quản lý nhà nước về bảo vệ dữ liệu cá nhân, trừ nội dung thuộc quốc phòng. Hiện tại Cục An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao là cơ quan chuyên trách bảo vệ dữ liệu cá nhân. Song song, Bộ Thông tin và Truyền thông (KH&CN) với vai trò quản lý lĩnh vực công nghệ thông tin, an toàn thông tin - cũng có trách nhiệm phối hợp giám sát việc bảo vệ dữ liệu trên không gian mạng. Thực tế, trước khi có Luật Bảo vệ Dữ liệu Cá nhân, Bộ KH&CN thông qua Thanh tra thông tin và truyền thông đã thực hiện xử phạt các vi phạm về thu thập, sử dụng thông tin cá nhân trực tuyến dựa trên Nghị định 15/2020/NĐ-CP. Trong hệ thống mới, Bộ, cơ quan ngang Bộ khác cũng thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân trong ngành/lĩnh vực của mình (*Khoản 4 Điều 36 Luật Bảo vệ Dữ liệu Cá nhân 2025*). Điều này có nghĩa là các bộ như Bộ Tài chính, Bộ Y tế, NHNN... sẽ giám sát việc bảo vệ dữ liệu cá nhân trong ngành mình (*tài chính, y tế, ngân hàng...*). UBND cấp tỉnh cũng có trách nhiệm quản lý tại địa phương (*Khoản 5 Điều 36*). Tuy nhiên, đầu mối tập trung vẫn là Bộ Công an, đảm bảo sự thống nhất.

Trong lĩnh vực dữ liệu số nói chung, Luật Dữ liệu 2024 cũng quy định Chính phủ thống nhất quản lý, Bộ Công an là đầu mối (*trừ lĩnh vực dữ liệu cơ yếu*



do Bộ Quốc phòng quản lý). Như vậy có thể thấy, Bộ Công an đóng vai trò “nhạc trưởng” trong giám sát thực thi pháp luật về dữ liệu và dữ liệu cá nhân, còn Bộ KH&CN cùng các cơ quan khác đóng vai trò phối hợp, thanh tra chuyên ngành trong phạm vi quản lý của họ. Ví dụ: Bộ KH&CN sẽ tiếp tục thanh tra các doanh nghiệp viễn thông, internet, mạng xã hội về việc tuân thủ bảo vệ dữ liệu người dùng; nếu phát hiện vi phạm nghiêm trọng có thể phối hợp chuyển Bộ Công an xử lý.

- **Thứ hai**, hoạt động thanh tra, kiểm tra định kỳ và đột xuất: Pháp luật đã trao quyền cho cơ quan quản lý tiến hành thanh tra, kiểm tra việc tuân thủ các quy định bảo vệ dữ liệu. Nghị định 13/2023 liệt kê một trong những nội dung quản lý nhà nước về bảo vệ dữ liệu cá nhân là thanh tra, kiểm tra việc thực hiện pháp luật về bảo vệ dữ liệu cá nhân; giải quyết khiếu nại, tố cáo; xử lý vi phạm. Điều 35 Luật Bảo vệ Dữ liệu Cá nhân 2025 khẳng định việc kiểm tra hoạt động bảo vệ dữ liệu cá nhân được thực hiện theo quy định của luật và của Chính phủ. Như vậy, cơ quan chuyên trách (Bộ Công an) và thanh tra các bộ ngành liên quan có thẩm quyền kiểm tra các tổ chức về: việc xin phép có đúng quy định không, hệ thống công nghệ thông tin có đáp ứng tiêu chuẩn an toàn không, doanh nghiệp đã thực hiện đánh giá tác động chưa, có vi phạm quyền chủ thể dữ liệu nào không... Việc kiểm tra có thể theo kế hoạch định kỳ hoặc đột xuất khi có dấu hiệu vi phạm hay khiếu nại từ công dân. Ví dụ: nếu nhiều người dùng khiếu nại một công ty công nghệ lạm dụng dữ liệu, cơ quan chức năng có thể mở cuộc thanh tra đột xuất với công ty đó. Các doanh nghiệp lớn xử lý lượng dữ liệu cá nhân “không lồ” sẽ nằm trong diện giám sát đặc biệt. Luật Bảo vệ Dữ liệu Cá nhân 2025 cũng yêu cầu các bên kiểm soát dữ liệu phải phối hợp với Bộ Công an khi cơ quan này tiến hành bảo vệ dữ liệu hoặc điều tra vi phạm.

Chủ thể dữ liệu (*người dân*) có thể gửi khiếu nại, tố cáo về vi phạm dữ liệu tới cơ quan chuyên trách (Bộ Công an). Bộ Công an phối hợp với Thanh tra Bộ KH&CN và các đơn vị liên quan tiến hành kiểm tra, điều tra đối với tổ chức, cá nhân bị tố cáo. Trong quá trình đó, doanh nghiệp có nghĩa vụ cung cấp thông tin,



cho phép kiểm tra hệ thống và thực thi các yêu cầu kỹ thuật (*như tạm dừng xử lý dữ liệu vi phạm*). Nếu phát hiện vi phạm, cơ quan chức năng sẽ xử phạt và yêu cầu khắc phục. Đồng thời, doanh nghiệp phải phản hồi, giải quyết yêu cầu của chủ thẻ dữ liệu (*như cung cấp dữ liệu, chỉnh sửa, xóa...*) trong thời hạn luật định. Cơ quan quản lý cũng có thể chủ động thanh tra định kỳ mà không cần có khiếu nại, nhất là với các ngành nhạy cảm (*viễn thông, tài chính, y tế...*).

- Thứ ba, xử phạt vi phạm hành chính: Đối với các hành vi vi phạm nghĩa vụ bảo vệ dữ liệu, chế tài chủ yếu hiện nay là xử phạt hành chính (*phạt tiền, kèm biện pháp khắc phục hậu quả*). Trước khi có Luật Bảo vệ Dữ liệu Cá nhân, các hành vi vi phạm về thông tin cá nhân trên mạng bị xử phạt theo Nghị định 15/2020/NĐ-CP (*sửa đổi bởi Nghị định 14/2022/NĐ-CP và sắp tới là Nghị định 211/NĐ-CP*). Ví dụ: Điều 84 Nghị định 15/2020/NĐ-CP quy định phạt 10-20 triệu đồng nếu thu thập thông tin cá nhân khi chưa được chủ thẻ đồng ý, 40-60 triệu đồng với hành vi cung cấp thông tin cá nhân cho bên thứ ba khi chủ thẻ đã yêu cầu ngừng. Mức phạt tăng lên 40-60 triệu đồng nếu vi phạm nghiêm trọng hơn như sử dụng thông tin cá nhân sai mục đích đã thông báo, hoặc mua bán, phát tán thông tin cá nhân của người khác mà chưa được phép. Ngoài ra, Điều 85, 86 Nghị định 15/2020/NĐ-CP cũng xử phạt việc không đáp ứng yêu cầu bảo đảm an toàn thông tin cá nhân (*ví dụ: không cập nhật, chỉnh sửa hoặc xóa thông tin cá nhân theo yêu cầu của chủ thẻ; không có biện pháp bảo vệ bí mật thông tin cá nhân của người dùng*). Các hình phạt bổ sung và biện pháp khắc phục hậu quả cũng được áp dụng, như buộc hủy bỏ dữ liệu cá nhân đã thu thập trái phép, tước quyền sử dụng giấy phép, hoặc kiến nghị thu hồi giấy phép kinh doanh nếu vi phạm nghiêm trọng nhiều lần.

Với sự ra đời của Nghị định 13/2023 và Luật Bảo vệ Dữ liệu Cá nhân 2025, dự kiến sẽ có văn bản thay thế Nghị định 15/2020/NĐ-CP cho mảng bảo vệ dữ liệu cá nhân, với mức phạt có thể cao hơn để đủ sức răn đe. Mặc dù Luật Bảo vệ Dữ liệu Cá nhân 2025 chưa quy định mức phạt cụ thể, nhưng tham khảo quốc tế (*ví dụ GDPR của Liên minh Châu Âu có mức phạt tối 4% doanh thu toàn cầu của*



(doanh nghiệp), khả năng trong tương lai gần Việt Nam cũng tăng nặng chế tài tài chính đối với vi phạm dữ liệu nghiêm trọng (nhất là vi phạm liên quan dữ liệu nhạy cảm, ảnh hưởng nhiều người). Hiện tại, theo Nghị định 13/2023/NĐ-CP, người vi phạm quy định bảo vệ dữ liệu cá nhân có thể bị kỷ luật, phạt hành chính hoặc truy cứu hình sự tùy mức độ. Doanh nghiệp vi phạm lần đầu có thể bị cảnh cáo hoặc phạt tiền; tái phạm nhiều lần có thể bị tước giấy phép hoạt động có thời hạn (như đã quy định trong Nghị định 15/2020/NĐ-CP đối với vi phạm ATTT mạng). Cơ quan quản lý còn có thể công khai danh tính tổ chức vi phạm trên phương tiện thông tin đại chúng để tăng sức ép tuân thủ.

- **Thứ tư**, trách nhiệm dân sự và bồi thường: Chủ thẻ dữ liệu có quyền yêu cầu bồi thường thiệt hại nếu việc xử lý dữ liệu của tổ chức gây tổn thất cho họ. Quyền yêu cầu bồi thường thiệt hại được luật ghi nhận rõ (ví dụ: Khoản 10 Điều 9 Nghị định 13/2023/NĐ-CP quy định chủ thẻ có quyền đòi bồi thường khi xảy ra vi phạm dữ liệu cá nhân). Theo nguyên tắc chung của Bộ luật Dân sự, bên xâm phạm dữ liệu phải bồi thường toàn bộ thiệt hại vật chất và một phần thiệt hại tinh thần cho nạn nhân. Ví dụ: nếu một công ty bị lộ dữ liệu khách hàng khiến khách bị lừa đảo tiền bạc, công ty đó có thể phải bồi hoàn khoản tiền thiệt hại. Luật cũng quy định bên kiểm soát dữ liệu phải chịu trách nhiệm trước chủ thẻ về thiệt hại xảy ra do quá trình xử lý dữ liệu gây ra. Điều này xác lập nguyên tắc trách nhiệm bồi thường của bên kiểm soát, trừ khi họ chứng minh được mình không có lỗi gây ra vi phạm. Cơ chế thực thi trách nhiệm dân sự là thông qua tòa án: cá nhân có thể khởi kiện dân sự đòi bồi thường. Hiện nay, chưa có nhiều án lệ ở Việt Nam về bồi thường do vi phạm dữ liệu cá nhân, nhưng luật đã mở đường cho khả năng này và trong tương lai khi nhận thức người dân tăng lên, có thể sẽ xuất hiện các vụ kiện dân sự đòi bồi thường, tạo thêm áp lực để doanh nghiệp tuân thủ tốt hơn.

- **Thứ năm**, chế tài hình sự: Đối với các hành vi vi phạm nghiêm trọng (ví dụ: mua bán dữ liệu cá nhân số lượng lớn để trực lợi, hoặc thu thập, truyền đưa thông tin nhằm xâm hại an ninh quốc gia), pháp luật hình sự có thể được áp dụng. Bộ luật Hình sự hiện hành của Việt Nam có một số tội danh liên quan, như Điều



288 Bộ luật Hình sự 2015 về Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông - trong đó hành vi mua bán, trao đổi trái phép thông tin về tài khoản ngân hàng, thông tin cá nhân của người khác trên mạng có thể bị phạt tiền đến 200 triệu đồng hoặc phạt tù đến 7 năm. Ngoài ra, nếu việc xử lý dữ liệu bị lợi dụng nhằm chống phá Nhà nước hoặc phạm tội khác (*khủng bố, lừa đảo...*), người thực hiện sẽ bị truy cứu theo tội danh tương ứng. Tuy nhiên, việc xử lý hình sự các vi phạm dữ liệu cá nhân đơn thuần (*không gắn với tội phạm khác*) ở Việt Nam còn chưa phổ biến. Cơ chế chính vẫn là xử phạt hành chính nhanh chóng, kịp thời. Luật Bảo vệ Dữ liệu Cá nhân 2025 nhấn mạnh yêu cầu xử lý kịp thời, nghiêm minh mọi hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân - điều này bao hàm cả việc nếu đủ yếu tố cấu thành tội phạm thì phải chuyển sang điều tra hình sự để truy tố.

- **Thứ sáu**, biện pháp kỹ thuật bắt buộc và khắc phục hậu quả: Cơ quan có thẩm quyền có quyền áp dụng một số biện pháp kỹ thuật - nghiệp vụ nhằm ngăn chặn, chấm dứt vi phạm về dữ liệu. ⁽¹⁾Như đã đề cập, buộc tiêu hủy dữ liệu cá nhân vi phạm là một biện pháp khắc phục hậu quả thường được áp dụng (*Nghị định 15/2020/NĐ-CP đã liệt kê biện pháp “Buộc hủy bỏ thông tin cá nhân” đối với hành vi thu thập, phát tán trái phép*). ⁽²⁾Trong trường hợp vi phạm nghiêm trọng đe dọa an ninh dữ liệu quốc gia, cơ quan quản lý có thể đình chỉ tạm thời hoạt động xử lý dữ liệu của tổ chức vi phạm. Ví dụ: một ứng dụng mạng xã hội nếu liên tục vi phạm quy định bảo vệ dữ liệu người dùng, cơ quan chức năng có thể yêu cầu tạm dừng cung cấp dịch vụ một phần hoặc toàn bộ cho đến khi khắc phục xong. Thực tế trong lĩnh vực viễn thông, nếu nhà mạng vi phạm quản lý thông tin thuê bao, Bộ Thông tin và truyền thông trước kia đã từng yêu cầu dừng phát triển thuê bao mới để khắc phục vi phạm - tương tự, trong lĩnh vực dữ liệu, biện pháp “ngắt kết nối hệ thống” cũng có thể được xem xét. ⁽³⁾Cơ quan an ninh mạng có thể sử dụng biện pháp kỹ thuật để thu thập chứng cứ vi phạm (*nghiêm định hệ thống, truy vết giao dịch dữ liệu trái phép trên mạng*). Đối với dữ liệu số, các log truy cập, bản sao cơ sở dữ liệu sẽ được kiểm tra bởi chuyên gia kỹ thuật



trong quá trình thanh tra. Nếu cần, cơ quan chức năng có thể yêu cầu tổ chức cung cấp quyền truy cập vào hệ thống thông tin để kiểm tra tại chỗ.⁽⁴⁾ Các tiêu chuẩn kỹ thuật về bảo vệ dữ liệu sẽ dần mang tính bắt buộc - doanh nghiệp phải tuân thủ, nếu không sẽ bị coi là vi phạm. Ví dụ: Điều 34 Luật Bảo vệ Dữ liệu Cá nhân 2025 giao việc ban hành quy chuẩn kỹ thuật về bảo vệ dữ liệu cá nhân (*đối với hệ thống thông tin, phần cứng, phần mềm, quản lý vận hành dữ liệu*) và yêu cầu tuân thủ các tiêu chuẩn này. Nếu một doanh nghiệp không đáp ứng tiêu chuẩn tối thiểu (ví dụ *không mã hóa dữ liệu nhạy cảm, không có quy trình quản lý truy cập*), thì ngay cả khi chưa xảy ra sự cố, họ cũng có thể bị xử phạt vì vi phạm quy định kỹ thuật (Điều 86 Nghị định 15/2020/NĐ-CP quy định phạt 10-20 triệu nếu “Không kiểm tra, giám sát việc tuân thủ quy định về bảo đảm an toàn thông tin mạng”).

Như vậy, các biện pháp kỹ thuật bắt buộc đóng vai trò vừa phòng ngừa (yêu cầu tuân thủ tiêu chuẩn để giảm nguy cơ) vừa xử lý hậu quả (xóa dữ liệu vi phạm, đình chỉ hoạt động để ngăn ngừa lây lan thiệt hại).

- Cuối cùng, cơ chế giám sát không chỉ thuần túy mang tính cưỡng chế, mà còn có yếu tố tham gia của cộng đồng và hợp tác quốc tế. Người dân được khuyến khích tố giác, thông báo vi phạm tới cơ quan chức năng (Khoản 3 Điều 23 Luật Bảo vệ Dữ liệu Cá nhân 2025 cho phép bất kỳ cơ quan, tổ chức, cá nhân nào thông báo cho cơ quan chuyên trách nếu phát hiện vi phạm quy định bảo vệ dữ liệu cá nhân). Đây là kênh giám sát từ cộng đồng giúp phát hiện vi phạm nhanh hơn. Về hợp tác quốc tế, Nghị định 13/2023 yêu cầu xây dựng cơ chế hợp tác quốc tế nhằm thực thi hiệu quả pháp luật về bảo vệ dữ liệu. Cơ quan Việt Nam sẽ phối hợp với các nước trong việc tương trợ điều tra, trao đổi thông tin, khiếu nại liên quan đến bảo vệ dữ liệu. Điều này rất quan trọng trong bối cảnh nhiều vi phạm xuyên biên giới (ví dụ vụ lộ dữ liệu của một công ty nước ngoài ảnh hưởng người Việt, hoặc ngược lại). Hợp tác giúp đảm bảo các chế tài xử lý có thể thực hiện được ngay cả khi dữ liệu hay đối tượng vi phạm không nằm hoàn toàn trong lãnh thổ Việt Nam.



Tóm lại, cơ chế kiểm tra, giám sát thực thi bao gồm một mạng lưới các cơ quan với vai trò cụ thể (*trọng tâm là Bộ Công an*), sử dụng các công cụ thanh tra, xử phạt hành chính, dân sự, hình sự và kỹ thuật để đảm bảo các nghĩa vụ về dữ liệu được tuân thủ. Sự nghiêm minh và phối hợp chặt chẽ của cơ quan quản lý là yếu tố then chốt để quyền và lợi ích của chủ thể dữ liệu được bảo vệ hiệu quả trên thực tế.

2.3.3. Cơ chế khuyến khích và hỗ trợ thực hiện

Bên cạnh các biện pháp chế tài bắt buộc, pháp luật và chính sách hiện hành cũng đưa ra những cơ chế khuyến khích, hỗ trợ nhằm thúc đẩy tổ chức, cá nhân tự nguyện tuân thủ tốt các quy định về dữ liệu. Việc khuyến khích tuân thủ không chỉ tạo động lực tích cực cho doanh nghiệp, mà còn góp phần xây dựng văn hóa quản trị dữ liệu lành mạnh, nâng cao hiệu quả bảo vệ dữ liệu trong toàn xã hội.

- **Thứ nhất**, khuyến khích đầu tư hạ tầng, công nghệ bảo vệ dữ liệu: Nhà nước ta nhận thức rằng việc bảo vệ dữ liệu phải song hành với phát triển kinh tế số. Do đó, Luật Dữ liệu 2024 đưa ra chính sách khuyến khích, tạo điều kiện cho cơ quan, tổ chức, cá nhân trong và ngoài nước đầu tư, nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, đổi mới sáng tạo, ứng dụng trong lĩnh vực dữ liệu; xây dựng trung tâm lưu trữ, xử lý dữ liệu tại Việt Nam; phát triển thị trường dữ liệu (*Khoản 5 Điều 6*). Chính sách này mang lại lợi ích kép: vừa thúc đẩy kinh tế dữ liệu, vừa nâng cao năng lực bảo vệ dữ liệu (*vì có công nghệ tiên tiến hơn*). Các doanh nghiệp triển khai hệ thống quản trị dữ liệu hiện đại, đạt tiêu chuẩn an toàn cao có thể được hưởng lợi từ môi trường đầu tư thuận lợi, thậm chí có thể tiếp cận các ưu đãi về tín dụng, thuế theo các chương trình hỗ trợ chuyển đổi số. Bên cạnh đó, Nhà nước khuyến khích các tổ chức, cá nhân tài trợ, hỗ trợ việc xây dựng, quản trị, vận hành cơ sở dữ liệu (*Khoản 4 Điều 6*) - ví dụ doanh nghiệp công nghệ có thể tài trợ dự án cơ sở dữ liệu y tế, giáo dục... và đổi lại được ghi nhận, vinh danh, hoặc được quyền khai thác dữ liệu trong khuôn khổ pháp luật. Đây là những cách huy động nguồn lực xã hội để phát triển dữ liệu đồng thời bảo đảm dữ liệu được quản trị tốt.



- **Thứ hai**, khuyến khích thiết lập hệ thống quản trị dữ liệu tốt và chứng nhận bảo vệ dữ liệu: Mặc dù chưa có quy định cụ thể về chứng nhận bảo vệ dữ liệu (*nhiều kiểu chứng chỉ xếp hạng mức độ bảo vệ dữ liệu của doanh nghiệp*), nhưng pháp luật hướng tới việc yêu cầu và khuyến khích doanh nghiệp áp dụng tiêu chuẩn, quy chuẩn tốt trong quản trị dữ liệu. Luật Dữ liệu 2024 định nghĩa “quản trị dữ liệu” bao gồm xây dựng chính sách, quy trình, tiêu chuẩn về dữ liệu để quản lý dữ liệu liên tục, hiệu quả, bảo đảm tính đầy đủ, chính xác, toàn vẹn, an toàn, bảo mật.... Đối với các tổ chức, cá nhân (*không phải cơ quan nhà nước*), luật khuyến khích họ tự thực hiện quản trị, quản lý dữ liệu phù hợp điều kiện thực tế.Thêm vào đó, Nghị định 165/2025/NĐ-CP nêu rõ: “Khuyến khích các chủ quản dữ liệu không thuộc cơ quan nhà nước xây dựng các quy định riêng về bảo vệ dữ liệu do mình quản lý”. Điều này nghĩa là doanh nghiệp được khuyến khích ban hành quy chế nội bộ về bảo vệ dữ liệu phù hợp với tính chất hoạt động của mình, miễn là không trái luật. Những doanh nghiệp tiên phong xây dựng hệ thống quản trị dữ liệu tốt (*ví dụ đạt các chứng chỉ quốc tế như ISO/IEC 27701 về hệ thống quản lý thông tin riêng tư, hoặc chuẩn PCI-DSS trong lĩnh vực thanh toán*) có thể sẽ được công nhận uy tín, tạo niềm tin với khách hàng và cơ quan quản lý. Mặc dù pháp luật chưa trực tiếp quy định “ưu đãi” cho các doanh nghiệp này, nhưng trên thực tế, khi đánh giá mức độ tuân thủ, thanh tra có thể xem xét giảm tần suất kiểm tra đối với đơn vị có lịch sử tuân thủ tốt, tương tự như cách tiếp cận quản lý rủi ro. Trong tương lai, Việt Nam có thể thiết lập cơ chế chứng nhận mức độ bảo vệ dữ liệu (*ví dụ nhãn “Trusted Data” cấp bởi cơ quan chức năng*) cho những doanh nghiệp đáp ứng tiêu chí cao, từ đó khuyến khích các doanh nghiệp khác noi theo.

- **Thứ ba**, ưu đãi và hỗ trợ doanh nghiệp vừa và nhỏ (SME), startup: Nhận thấy việc tuân thủ toàn bộ nghĩa vụ bảo vệ dữ liệu có thể quá sức đối với các doanh nghiệp nhỏ, pháp luật đã có quy định miễn/giãn một số nghĩa vụ cho SME trong giai đoạn đầu. Cụ thể, Khoản 2 Điều 38 Luật Bảo vệ Dữ liệu Cá nhân 2025 cho phép doanh nghiệp nhỏ và doanh nghiệp khởi nghiệp được quyền lựa chọn thực



hiện hoặc không thực hiện các quy định về Đánh giá tác động xử lý dữ liệu cá nhân (*Điều 21*), Cập nhật hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới (*Điều 22*) và Cơ quan, tổ chức có trách nhiệm chỉ định bộ phận, nhân sự đủ điều kiện năng lực bảo vệ dữ liệu cá nhân hoặc thuê tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân (*khoản 2 Điều 33*) trong 5 năm kể từ khi luật có hiệu lực. Đây là giai đoạn quá độ 5 năm (2026-2030) để các doanh nghiệp nhỏ có thời gian thích nghi, chuẩn bị nguồn lực.Thêm nữa, Khoản 3 Điều 38 còn miễn hẳn cho hộ kinh doanh, doanh nghiệp siêu nhỏ các nghĩa vụ trên (*DPIA, DPO*) trừ trường hợp họ kinh doanh dịch vụ xử lý dữ liệu, xử lý dữ liệu nhạy cảm hoặc dữ liệu số lượng lớn. Như vậy, một startup công nghệ mới thành lập với vài nhân viên sẽ chưa bắt buộc phải lập DPIA hay cử cán bộ phụ trách dữ liệu ngay, miễn là họ không xử lý dữ liệu nhạy cảm hay hàng triệu người dùng. Đây là cơ chế hỗ trợ rất thiết thực, giúp giảm gánh nặng chi phí tuân thủ cho doanh nghiệp nhỏ trong bước đầu, tránh cản trở đổi mới sáng tạo. Tuy nhiên, luật cũng đặt tiêu chí loại trừ: nếu doanh nghiệp nhỏ trực tiếp xử lý dữ liệu nhạy cảm hoặc dữ liệu quy mô lớn thì vẫn phải tuân thủ ngay từ đầu (*vì rủi ro cao*). Song hành với miễn giảm nghĩa vụ, Nhà nước cũng cần hỗ trợ SME bằng cách xây dựng các hướng dẫn đơn giản, mẫu biểu, công cụ có sẵn để họ có thể thực thi bảo vệ dữ liệu với chi phí thấp. Ví dụ: cung cấp mẫu chính sách quyền riêng tư, mẫu hợp đồng xử lý dữ liệu, phần mềm mã hóa miễn phí... Việc này chưa được quy định chi tiết nhưng là hướng hỗ trợ cần thiết trong tương lai.

- **Thứ tư**, ưu đãi tiếp cận dữ liệu dùng chung và dữ liệu mở: Một khía cạnh khuyến khích khác là tạo điều kiện cho doanh nghiệp tiếp cận các nguồn dữ liệu do Nhà nước quản lý để phục vụ hoạt động của mình một cách hợp pháp. Luật Dữ liệu 2024 đề cập khái niệm “dữ liệu dùng chung” (*dữ liệu được chia sẻ, khai thác chung trong các cơ quan Đảng, Nhà nước, tổ chức chính trị-xã hội*) và “dữ liệu mở” (*dữ liệu mọi tổ chức, cá nhân đều có thể tiếp cận*). Nhà nước có chủ trương công khai các dữ liệu mở, xây dựng cổng dữ liệu mở để doanh nghiệp, người dân sử dụng. Bên cạnh đó, khoản 1 Điều 17 Luật Dữ liệu khuyến khích chủ sở hữu dữ



liệu, chủ quản dữ liệu (*bao gồm doanh nghiệp tư nhân*) kết nối, chia sẻ dữ liệu cho người dùng dữ liệu theo quy định pháp luật hoặc thỏa thuận, có thể thông qua bên trung gian. Điều này mở ra triển vọng hình thành thị trường dữ liệu nơi các bên chia sẻ dữ liệu hợp pháp. Doanh nghiệp nào có hệ thống quản trị dữ liệu tốt, đảm bảo an ninh có thể được ưu tiên tham gia các dự án kết nối dữ liệu với cơ quan nhà nước, từ đó khai thác tài nguyên dữ liệu công phục vụ kinh doanh. Ví dụ: một doanh nghiệp khởi nghiệp về giao thông nếu tuân thủ tốt bảo vệ dữ liệu có thể được quyền tiếp cận dữ liệu giao thông đô thị (*dữ liệu dùng chung của cơ quan nhà nước*) để phát triển ứng dụng, qua đó vừa tạo giá trị kinh tế vừa giúp Nhà nước tận dụng dữ liệu hiệu quả. Nghị định 165/2025/NĐ-CP cũng khuyến khích cá nhân, tổ chức chia sẻ dữ liệu của mình cho cơ quan nhà nước vì các mục tiêu lợi ích chung (*y tế, giao thông, biến đổi khí hậu, cung cấp dịch vụ công...*). Khi các doanh nghiệp chủ động chia sẻ dữ liệu phục vụ lợi ích xã hội, họ có thể nhận lại ưu đãi như được truy cập các dữ liệu tổng hợp, thống kê chính thức mà cơ quan nhà nước nắm giữ để nghiên cứu thị trường, hoặc đơn giản là nâng cao hình ảnh trách nhiệm xã hội của doanh nghiệp.

- **Thứ năm**, hỗ trợ về hướng dẫn, đào tạo và hợp tác: Nhà nước cũng đóng vai trò hỗ trợ kỹ thuật thông qua việc ban hành hướng dẫn thực thi và tổ chức đào tạo. Nghị định 13/2023/NĐ-CP giao nhiệm vụ cho cơ quan quản lý phải hướng dẫn cơ quan, tổ chức, cá nhân về biện pháp, quy trình, tiêu chuẩn bảo vệ dữ liệu cá nhân. Hiện nay, Bộ Công an đã xây dựng một số tài liệu hướng dẫn cơ bản về 13/2023/NĐ-CP và thiết lập kênh thông tin (*website*) để giải đáp thắc mắc cho doanh nghiệp. Các hội thảo, tập huấn về Luật Bảo vệ Dữ liệu Cá nhân sẽ được tổ chức để cộng đồng doanh nghiệp hiểu rõ nghĩa vụ mới. Ngoài ra, như đã nói, Chính phủ sẽ sớm ban hành tiêu chuẩn, quy chuẩn kỹ thuật về bảo vệ dữ liệu và điều này thực chất là một hình thức hỗ trợ doanh nghiệp: khi có chuẩn mực rõ ràng, doanh nghiệp biết cần làm gì để đạt yêu cầu, tránh mơ hồ.Thêm vào đó, việc hợp tác quốc tế cũng mang lại lợi ích hỗ trợ cho doanh nghiệp trong nước. Tham gia các diễn đàn, cơ chế hợp tác giúp Việt Nam có thể tiếp nhận công nghệ



bảo vệ dữ liệu tiên tiến (*Khoản 5 Điều 7 Nghị định 13/2023/NĐ-CP khuyễn khích chuyển giao công nghệ phục vụ bảo vệ dữ liệu cá nhân*). Nhờ đó, doanh nghiệp Việt có thể được tiếp cận với các giải pháp bảo mật mới, nâng cao khả năng tuân thủ với chi phí hợp lý hơn.

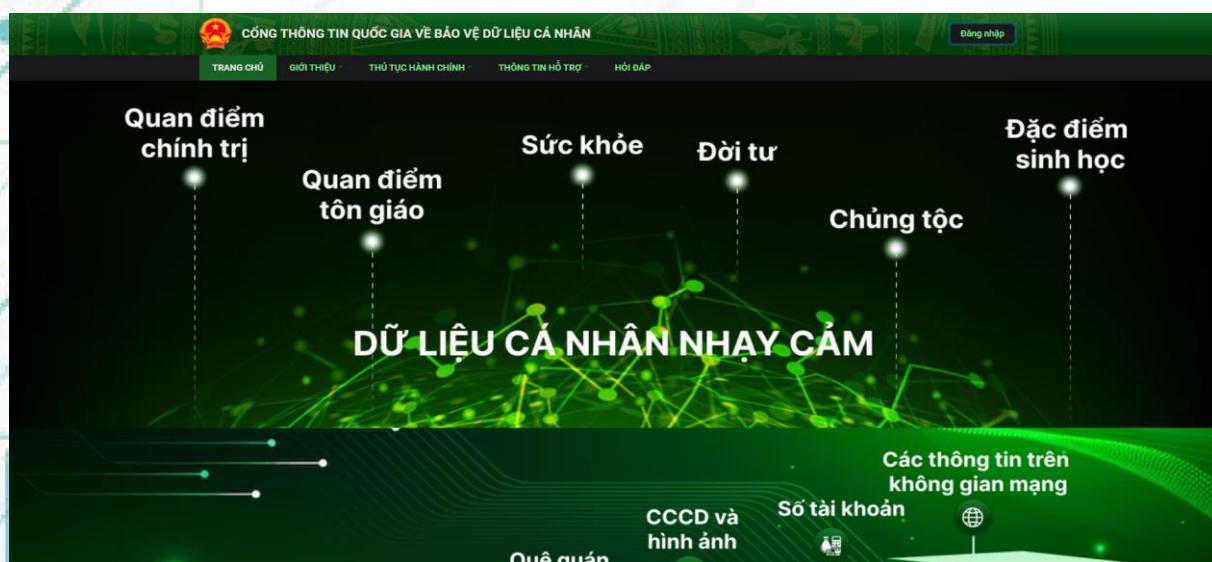
Tóm lại, cơ chế khuyến khích và hỗ trợ tập trung vào việc tạo môi trường thuận lợi và động lực tích cực để các tổ chức, cá nhân nâng cao ý thức và năng lực bảo vệ dữ liệu. Nhà nước không chỉ dùng “cây gậy” chế tài mà còn dùng “cù cà rốt” là các chính sách ưu đãi, miễn giảm, hỗ trợ kỹ thuật và công nhận thành tích. Về phần mình, doanh nghiệp nên tận dụng những hỗ trợ này để hoàn thiện hệ thống quản trị dữ liệu, vừa tuân thủ pháp luật vừa tạo lợi thế cạnh tranh trong nền kinh tế dữ liệu đang lên.



KIẾN NGHỊ, ĐỀ XUẤT

Để những quy định pháp luật đi vào cuộc sống hiệu quả, cần có các giải pháp triển khai cụ thể. Tác giả đề xuất một số nội dung nhằm tăng cường bảo đảm quyền và nghĩa vụ về dữ liệu đối với các tổ chức, cá nhân phi nhà nước:

- Thứ nhất,** xây dựng hệ thống tiếp nhận khiếu nại dữ liệu trực tuyến: Thiết lập một cổng thông tin điện tử quốc gia về bảo vệ dữ liệu cá nhân, cho phép người dân nộp khiếu nại, phản ánh vi phạm một cách thuận tiện. Hệ thống này hoạt động như “một cửa” tập trung, tích hợp với cơ quan chuyên trách (*Bộ Công an*) và có thể chuyển tiếp đến các cơ quan liên quan. Người dân có thể gửi các khiếu nại về việc lộ lọt thông tin, doanh nghiệp sử dụng dữ liệu sai mục đích... kèm chứng cứ. Cổng thông tin cần có chức năng theo dõi trạng thái xử lý và phản hồi kết quả cho người khiếu nại. Hiện nay, Luật Bảo vệ Dữ liệu Cá nhân 2025 đã đề cập tới Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân, có thể tận dụng cổng này vừa làm nơi doanh nghiệp nộp hồ sơ DPIA, vừa làm nơi công dân gửi khiếu nại. Một hệ thống trực tuyến minh bạch, dễ sử dụng sẽ khuyến khích người dân tham gia giám sát, giúp phát hiện vi phạm nhanh chóng hơn và giảm tải thủ tục hành chính (*so với nộp đơn giấy*). Đồng thời, dữ liệu tổng hợp từ cổng khiếu nại sẽ giúp cơ quan quản lý phân tích xu hướng vi phạm, từ đó có biện pháp phòng ngừa phù hợp.



Hình ảnh giao diện Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân

<https://baovedlcn.gov.vn/>



- Thứ hai, tăng cường kiểm tra hệ thống công nghệ xử lý dữ liệu người dùng: Cơ quan chức năng cần đẩy mạnh các đợt kiểm tra định kỳ về an ninh dữ liệu tại những doanh nghiệp thu thập lượng lớn dữ liệu người dùng (*ngân hàng, thương mại điện tử, viễn thông, mạng xã hội...*). Các cuộc kiểm tra nên tập trung vào hệ thống kỹ thuật: ví dụ kiểm tra việc mã hóa dữ liệu nhạy cảm, kiểm soát truy cập, lưu vết truy cập, biện pháp chống tấn công mạng, sao lưu và hủy dữ liệu... Nếu phát hiện lỗ hổng hay vi phạm, yêu cầu doanh nghiệp khắc phục trong thời hạn nhất định và có thể phạt cảnh cáo hoặc phạt tiền nếu thiếu sót nghiêm trọng (*như không tuân thủ tiêu chuẩn mã hóa bắt buộc, không có chính sách mật khẩu an toàn - vi phạm các quy chuẩn tối thiểu*). Bên cạnh kiểm tra trên giấy tờ, cần triển khai cả kiểm thử thực tế với sự phối hợp của chuyên gia an ninh mạng để đánh giá khả năng bảo vệ dữ liệu. Kết quả kiểm tra phải được thông báo cho doanh nghiệp cùng hướng dẫn khắc phục chi tiết. Về phía doanh nghiệp, nên chủ động thuê tư vấn độc lập đánh giá hệ thống của mình định kỳ, coi đó là việc làm thường xuyên thay vì đợi cơ quan nhà nước kiểm tra. Tăng cường kiểm tra kỹ thuật sẽ giúp kịp thời phát hiện rủi ro tiềm ẩn, ngăn chặn sự cố lớn và tạo sức ép để doanh nghiệp không lơ là trong bảo mật dữ liệu người dùng.

- Thứ ba, hỗ trợ doanh nghiệp SME triển khai chuẩn kỹ thuật về dữ liệu: Như đã phân tích, nhiều doanh nghiệp nhỏ thiếu nguồn lực để thiết lập hệ thống bảo vệ dữ liệu bài bản. Do đó, cơ quan quản lý nên có chương trình hỗ trợ tư vấn và đào tạo miễn phí cho nhóm doanh nghiệp này. Ví dụ: xây dựng các bộ tài liệu hướng dẫn đơn giản về tuân thủ Luật Bảo vệ Dữ liệu Cá nhân (*checklist những việc tối thiểu cần làm*), cung cấp các mẫu biểu (*mẫu chính sách quyền riêng tư, mẫu hợp đồng xử lý dữ liệu, mẫu thông báo vi phạm...*) để SME có thể áp dụng ngay. Ngoài ra, khi ban hành các tiêu chuẩn, quy chuẩn kỹ thuật, cần phổ biến rộng rãi và tổ chức hội thảo hướng dẫn cách đáp ứng tiêu chuẩn đó. Có thể thành lập một “vườn ươm tuân thủ” nơi các startup, SME được các chuyên gia về dữ liệu hướng dẫn trực tiếp cách thiết lập hạ tầng IT an toàn, cách thực hiện đánh giá tác động đơn giản. Nhà nước cũng có thể xem xét hỗ trợ tài chính dưới dạng



voucher dịch vụ: chẳng hạn trợ cấp một phần chi phí để SME thuê dịch vụ bảo mật, dịch vụ kiểm tra an ninh hệ thống. Một ý tưởng khác là công nhận những doanh nghiệp nhỏ làm tốt (*trao giải thưởng hoặc chứng nhận “Doanh nghiệp SME bảo vệ dữ liệu tốt”*) để họ có lợi thế quảng bá với khách hàng. Tổng thể, sự hỗ trợ này sẽ giúp nâng mặt bằng tuân thủ của khôi SME, tránh để khôi này trở thành “mắt xích yếu” trong chuỗi bảo vệ dữ liệu.

- **Thứ tư**, đề xuất cơ chế phối hợp quốc tế trong bảo vệ dữ liệu xuyên biên giới: Dữ liệu không biên giới, nên việc bảo vệ dữ liệu hiệu quả đòi hỏi hợp tác giữa các quốc gia. Việt Nam cần chủ động tham gia và đề xướng các cơ chế phối hợp quốc tế. Trước mắt, có thể thiết lập kênh liên lạc trực tiếp giữa Cơ quan chuyên trách bảo vệ dữ liệu cá nhân (Bộ Công an) với các cơ quan bảo vệ dữ liệu của các nước (ví dụ: Ủy ban Bảo vệ Dữ liệu cá nhân của Singapore, Cơ quan bảo vệ dữ liệu của Liên minh Châu Âu...). Thông qua đó, hai bên có thể trao đổi thông tin vi phạm, yêu cầu hỗ trợ điều tra các vụ việc liên quan đến công ty hoặc đối tượng nước ngoài. Ví dụ: nếu một công ty nước ngoài thu thập dữ liệu công dân Việt Nam trái phép, ta có thể nhờ nước sở tại xử lý và ngược lại. Việt Nam cũng có thể gia nhập các điều ước quốc tế đa phương về bảo vệ dữ liệu như Công ước 108+ của Hội đồng châu Âu, tạo cơ sở pháp lý cho tương trợ tư pháp về lĩnh vực này. Song song, tích cực tham gia các diễn đàn toàn cầu và khu vực (ASEAN, APEC) về quản trị dữ liệu để học hỏi kinh nghiệm và đóng góp tiếng nói. Việc tổ chức các hội nghị, hội thảo quốc tế tại Việt Nam về bảo vệ dữ liệu (như quy định tại Nghị định 13/2023/NĐ-CP, Luật Bảo vệ Dữ liệu cá nhân 2025) cũng rất hữu ích: doanh nghiệp Việt có dịp tiếp xúc với xu hướng và yêu cầu toàn cầu, từ đó chuẩn bị nâng cao tiêu chuẩn của mình cho tương thích. Tóm lại, tăng cường hợp tác quốc tế sẽ hỗ trợ thực thi pháp luật trong những vụ việc xuyên biên giới, đồng thời giúp Việt Nam nâng cao năng lực bảo vệ dữ liệu theo chuẩn mực tiên tiến, tạo môi trường thuận lợi thu hút đầu tư nước ngoài trong kỷ nguyên kinh tế số.



PHỤ LỤC

Đấu tranh, phản bác các quan điểm sai trái, thù địch

Trong kỷ nguyên số, dữ liệu đã trở thành tài nguyên cốt lõi của nền kinh tế và xã hội. Việc Việt Nam ban hành đạo luật đầu tiên chuyên sâu về dữ liệu thể hiện quyết tâm hoàn thiện chế độ quản lý, khai thác và bảo vệ dữ liệu một cách hiệu quả. Đây là bước ngoặt quan trọng nhằm tạo nền móng pháp lý vững chắc cho quốc gia số an toàn, hiệu quả, khẳng định chủ quyền dữ liệu của Việt Nam. Tuy nhiên, một số thế lực thù địch và truyền thông thiếu thiện chí đã có tình bóp méo nội dung luật, tung ra những luận điệu sai lệch nhằm gieo rắc hoài nghi. Họ xuyên tạc rằng Luật Dữ liệu 2024 mập mờ khái niệm “chủ sở hữu dữ liệu”, bỏ qua quyền riêng tư, cho phép tùy tiện thu thập dữ liệu cá nhân, tập trung kiểm soát dữ liệu tại Bộ Công an, vi phạm quyền ẩn danh, hạn chế tự do ngôn luận, thiếu minh bạch, không có giám sát tư pháp và gây cản trở đầu tư do quy định chuyển dữ liệu xuyên biên giới...

VIETNAM BUSINESS LAW

from Venture North Law

[VIETNAM BUSINESS LAW BLOG](#)
[LUẬT KINH DOANH](#)
[RECENT POSTS](#)
[PUBLICATIONS](#)
[ABOUT](#)
[VISIT VENTURE NORTH LAW](#)

Covid-19
Arbitration

Energy and Infrastructure
Employment

Technology and Telecom
Legal Environment

Securities Regulations
Real Estate

Contract Law

Key Highlights Of Vietnam New Data Law

4) Confusing concept of data owner

The Data Law introduces the concept of data owner, which is a person who has the rights to decide on the construction, development, protection, administration, processing, use, and exchange of the value of data such person owns (such rights, **Data Owner Rights**). It is unclear that to be a data owner whether (i) one will have to have both ownership of and also the Data Owner Rights over the data or (ii) simply having the Data Owner Rights makes one the owner of the data.

On March 2, 2025
In Technology and
Telecom, Commerce &
Trading

VBL nhận định “Khái niệm về chủ sở hữu dữ liệu gây nhầm lẫn”. Ảnh: Tác giả

Trước những luận điệu vô căn cứ này, cần khẳng định rõ: “Luật Dữ liệu 2024 cùng các văn bản liên quan đã thiết lập hệ thống quy định chặt chẽ, cân bằng giữa phát triển kinh tế dữ liệu với bảo vệ quyền và lợi ích hợp pháp của

Trang 148



người dân”. Các quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu và chủ quản dữ liệu được luật pháp quy định minh bạch. Đồng thời, cơ chế thực thi và giám sát được xây dựng đa tầng, đảm bảo mọi tổ chức, cá nhân (kể cả ngoài khu vực nhà nước) tuân thủ nghiêm túc pháp luật về dữ liệu. Những điểm tiến bộ này không chỉ bảo vệ quyền riêng tư và lợi ích người dân, mà còn thúc đẩy chuyển đổi số toàn diện, tạo niềm tin cho doanh nghiệp đầu tư, phát triển kinh tế số bền vững.

1. Quyền dữ liệu của người dân được bảo vệ vững chắc

Luật Dữ liệu 2024 đặt chủ thể dữ liệu (người mà dữ liệu phản ánh, chủ yếu là cá nhân) ở vị trí trung tâm và trao cho họ nhiều quyền quan trọng đối với thông tin của mình. Theo Khoản 12 Điều 3 Luật Dữ liệu 2024, chủ thể dữ liệu là “cơ quan, tổ chức, cá nhân được dữ liệu phản ánh” – hiểu đơn giản là cá nhân hoặc tổ chức mà dữ liệu đề cập tới. Với vai trò là người cung cấp dữ liệu ban đầu và chịu tác động trực tiếp từ việc dữ liệu được thu thập, sử dụng, chủ thể dữ liệu được pháp luật bảo vệ đặc biệt, nhất là về quyền riêng tư. Luật Dữ liệu 2024, Luật Bảo vệ Dữ liệu Cá nhân 2025 và Nghị định 13/2023/NĐ-CP và các văn bản pháp luật khác của Việt Nam xác định rõ các quyền và nghĩa vụ của chủ thể dữ liệu cá nhân. Theo đó, người dân có đầy đủ quyền được biết, quyền đồng ý hoặc từ chối, quyền truy cập, chỉnh sửa, xóa dữ liệu của mình, quyền yêu cầu hạn chế hoặc phản đối xử lý, quyền khiếu nại, tố cáo, khởi kiện và đòi bồi thường nếu thông tin cá nhân bị xâm phạm. Những quyền này bảo đảm mỗi cá nhân kiểm soát được dữ liệu cá nhân, biết dữ liệu của mình “được sử dụng ra sao, bởi ai và trong mục đích gì”. Thực tế, Luật Dữ liệu 2024 nhấn mạnh nguyên tắc minh bạch trong xử lý dữ liệu: mọi tổ chức, cá nhân khi thu thập dữ liệu đều phải thông báo rõ cho chủ thể về mục đích, phạm vi sử dụng và bên sẽ xử lý dữ liệu.

Quan trọng hơn, Luật Bảo vệ Dữ liệu Cá nhân 2025 quy định dữ liệu cá nhân chỉ được thu thập, xử lý khi có căn cứ pháp lý phù hợp, thông thường là sự đồng ý tự nguyện, rõ ràng của chủ thể dữ liệu. Mọi trường hợp xử lý vượt phạm vi mục đích ban đầu phải xin lại sự đồng ý. Như vậy, hoàn toàn bác bỏ luận điệu



cho rằng luật cho phép “*thu thập dữ liệu cá nhân không cần đồng ý*”. Sự đồng ý của người dân là nguyên tắc bắt buộc, trừ một số ngoại lệ đặc thù được luật định (ví dụ: *vì an ninh, quốc phòng, phòng chống dịch bệnh...*). Ngay cả trong các trường hợp đó, việc xử lý dữ liệu vẫn phải tuân thủ Hiến pháp và pháp luật liên quan, không được tùy tiện. Một ngoại lệ đáng lưu ý được Luật Dữ liệu 2024 đặt ra trong tình huống khẩn cấp như thiên tai, dịch bệnh, khủng bố, đe dọa an ninh quốc gia, cơ quan nhà nước có quyền yêu cầu tổ chức, cá nhân cung cấp dữ liệu cần thiết mà không cần sự đồng ý của chủ thể dữ liệu. Quy định này hoàn toàn phù hợp thông lệ quốc tế (*nhiều nước cho phép tạm thời giới hạn quyền riêng tư khi có tình trạng khẩn cấp*) và nhằm bảo vệ an toàn công cộng, tính mạng người dân trong tình huống nguy cấp. Ngay cả khi đó, luật vẫn đòi hỏi nhà nước chỉ được sử dụng dữ liệu trong khuôn khổ pháp luật cho mục tiêu ứng phó khẩn cấp, không phải lạm dụng tùy ý. Nói cách khác, Luật Dữ liệu 2024 không hề “thả lỏng” việc thu thập dữ liệu cá nhân, mà trái lại còn đặt ra các nguyên tắc chặt chẽ về sự đồng ý và mục đích xử lý, đồng thời tạo hành lang pháp lý để nhà nước bảo vệ người dân kịp thời trong trường hợp đặc biệt.

Bên cạnh nhóm quyền năng chủ động của chủ thể dữ liệu, pháp luật cũng yêu cầu người dân có ý thức trách nhiệm khi tham gia môi trường dữ liệu số. Chủ thể dữ liệu phải tự bảo vệ thông tin của mình, tôn trọng dữ liệu của người khác và cung cấp thông tin trung thực. Đây là những nghĩa vụ cơ bản nhằm xây dựng văn hóa dữ liệu lành mạnh. Ví dụ: mỗi cá nhân cần cẩn trọng khi chia sẻ thông tin cá nhân, không xâm phạm quyền riêng tư của người khác, không sử dụng thông tin giả mạo. Luật nghiêm cấm hành vi mua bán, trao đổi trái phép dữ liệu cá nhân dưới mọi hình thức. Như vậy, nếu có ai lo ngại Luật Dữ liệu “không bảo vệ quyền riêng tư” thì rõ ràng họ đã hiểu sai hoặc cố tình bóp méo sự thật. Ngược lại, luật cũng có vững chắc quyền riêng tư dữ liệu, coi an toàn dữ liệu cá nhân là yếu tố xuyên suốt không thể tách rời trong phát triển quốc gia số. Người dân được bảo vệ an toàn dữ liệu cá nhân như một phần của quyền con người, được pháp luật trao công cụ pháp lý mạnh mẽ để tự bảo vệ mình (*khiếu nại, tố cáo, khởi kiện đòi*



bồi thường...). Đồng thời, mọi cá nhân cũng có trách nhiệm tuân thủ luật chơi chung, chung tay phòng chống các vi phạm dữ liệu. Đây chính là sự cân bằng cần thiết giữa quyền và nghĩa vụ nhằm xây dựng một xã hội số an toàn, văn minh.

2. Quy định rõ “chủ sở hữu dữ liệu”, tài sản dữ liệu được quản lý và khai thác hợp pháp

Một điểm đột phá của Luật Dữ liệu 2024 là lần đầu tiên luật pháp Việt Nam xác định khái niệm “chủ sở hữu dữ liệu” và thừa nhận dữ liệu là một loại tài sản có giá trị. Theo Khoản 14 Điều 3 Luật Dữ liệu 2024, chủ sở hữu dữ liệu là “*cơ quan, tổ chức, cá nhân có quyền quyết định việc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng và trao đổi giá trị của dữ liệu do mình sở hữu*”. Đồng thời, Khoản 15 Điều 3 khẳng định quyền của chủ sở hữu dữ liệu đối với dữ liệu là một dạng quyền tài sản theo pháp luật dân sự. Điều này có nghĩa dữ liệu (*đặc biệt là dữ liệu phi cá nhân, dữ liệu do tổ chức, doanh nghiệp tạo ra*) được xem như một loại tài sản vô hình. Chủ sở hữu dữ liệu có đầy đủ quyền chiếm hữu, sử dụng và định đoạt đối với tài sản dữ liệu đó, tương tự như đối với các tài sản khác (*theo nguyên tắc Bộ luật Dân sự*).

Quy định trên không hề mập mờ hay tùy tiện, trái lại xuất phát từ định hướng chiến lược của Đảng và Nhà nước ta về phát triển kinh tế số. Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia đã nêu rõ: cần “*xác lập quyền sở hữu, kinh doanh dữ liệu và phân phối giá trị tạo ra từ dữ liệu. Phát triển kinh tế dữ liệu, thị trường dữ liệu và các sàn giao dịch dữ liệu*”. Đây chính là cơ sở chính trị vững chắc để Luật Dữ liệu 2024 công nhận quyền sở hữu dữ liệu, tạo hành lang pháp lý cho việc khai thác giá trị kinh tế của dữ liệu một cách minh bạch, hợp pháp. Trong thời đại cách mạng công nghiệp 4.0, dữ liệu được ví như “*năng lượng mới, thậm chí là ‘máu’ của nền kinh tế số*”. Việc thừa nhận dữ liệu là tài sản giúp khuyến khích tổ chức, cá nhân đầu tư xây dựng hạ tầng dữ liệu, phát triển sản phẩm dịch vụ dữ liệu và đổi mới sáng tạo. Luật Dữ liệu ra đời “đúng thời điểm khi Việt Nam đang đẩy mạnh chuyển đổi số”, tạo khung pháp lý quan



trọng để thu thập, chia sẻ và bảo vệ dữ liệu xuyên biên giới, hình thành niềm tin số giữa các chủ thể. Thực tế, nhiều doanh nghiệp công nghệ Việt Nam đã chủ động chuẩn bị hạ tầng kỹ thuật, quy trình bảo mật và nhân lực để sẵn sàng tuân thủ luật, coi đây là cơ hội phát triển sản phẩm dữ liệu số phục vụ chuyển đổi số và kinh tế số.

Từ góc độ kinh tế, chế định “chủ sở hữu dữ liệu” còn góp phần bảo đảm công bằng trong phân phối giá trị dữ liệu. Trước đây, do chưa có khung pháp lý rõ ràng, không ít trường hợp doanh nghiệp thu thập, khai thác dữ liệu nhưng trốn tránh trách nhiệm với người cung cấp dữ liệu. Giờ đây, khi đã trở thành chủ sở hữu tài sản dữ liệu, doanh nghiệp có quyền lợi kinh tế đi đôi với trách nhiệm pháp lý rõ ràng. Luật Dữ liệu yêu cầu chủ sở hữu dữ liệu phải tôn trọng quyền và lợi ích hợp pháp của chủ thể dữ liệu cá nhân theo Luật Bảo vệ Dữ liệu Cá nhân. Nói cách khác, dữ liệu cá nhân dù được doanh nghiệp thu thập hợp pháp thì doanh nghiệp cũng không “toute quyền” muốn làm gì thì làm. Họ phải tuân thủ các giới hạn về quyền riêng tư, bảo vệ dữ liệu cá nhân do luật chuyên ngành quy định. Đây chính là điểm mấu chốt cho thấy sự vô lý của luận điệu “*Luật Dữ liệu cho phép xâm phạm đời tư*”. Quyền sở hữu dữ liệu không đồng nghĩa với việc tước bỏ quyền của cá nhân đối với dữ liệu về mình, ngược lại, hai chế định này bổ sung cho nhau trong một hệ sinh thái pháp luật toàn diện. Cá nhân có quyền nhân thân (quyền riêng tư, quyền được bảo vệ dữ liệu cá nhân), còn doanh nghiệp có quyền tài sản đối với tập dữ liệu họ tạo lập; mọi hành vi khai thác dữ liệu cá nhân vẫn phải được sự đồng ý của người đó, trừ trường hợp luật định.

Mặt khác, Luật Dữ liệu 2024 không chỉ bảo vệ người dân, mà còn bảo vệ chính các doanh nghiệp sở hữu dữ liệu. Quyền của chủ sở hữu dữ liệu được luật quy định rất cụ thể, tạo điều kiện cho doanh nghiệp toàn quyền quyết định đối với tài sản dữ liệu của mình. Chẳng hạn, chủ sở hữu dữ liệu (*ngoài khỏi nhà nước*) có quyền tự do quyết định nơi và cách thức lưu trữ dữ liệu do mình thu thập, tạo lập, được tự chọn sử dụng hệ thống của mình hoặc thuê dịch vụ lưu trữ, kể cả lưu trên hạ tầng Trung tâm dữ liệu quốc gia theo thỏa thuận hợp đồng. Do đó, không có



chuyên Luật Dữ liệu buộc tất cả dữ liệu tập trung về một mối kiểm soát của nhà nước. Trái lại, luật tôn trọng quyền tự chủ của doanh nghiệp trong quản trị dữ liệu: từ việc đặt ra chính sách, quy trình quản lý dữ liệu phù hợp điều kiện thực tế, đến việc chủ động mã hóa, bảo vệ dữ liệu bằng giải pháp riêng. Nhà nước chỉ đóng vai trò định hướng, hỗ trợ hạ tầng (*nhiều xây dựng Trung tâm Dữ liệu quốc gia để cung cấp dịch vụ lưu trữ tập trung đạt chuẩn cao*) và can thiệp khi có vi phạm. Chính vì thế, có thể nói Luật Dữ liệu “được thiết kế theo hướng hậu kiểm thay vì tiền kiểm, Nhà nước chỉ can thiệp, xử lý khi phát hiện vi phạm” một điểm tiến bộ giảm gánh nặng thủ tục và khuyến khích đổi mới sáng tạo.



Hình ảnh: Ông Phan Đức Trung, Chủ tịch Hiệp hội Blockchain Việt Nam, nhận định: “Luật (Luật Dữ liệu) không đóng khung mà trao quyền cho doanh nghiệp chủ động xây dựng quy trình, áp dụng công nghệ, đồng thời chịu trách nhiệm hậu kiểm”. Ảnh: Vietnamplus

Như vậy, những lo ngại cho rằng luật tạo cơ chế “kiểm soát tập trung quan liêu” là hoàn toàn sai lệch. Thực tế, Luật Dữ liệu bảo đảm môi trường kinh doanh dữ liệu thông thoáng nhưng có trách nhiệm, nơi doanh nghiệp được quyền khai



thác tài sản dữ liệu của mình để làm giàu, nhưng phải tuân thủ luật và sẵn sàng chịu trách nhiệm nếu vi phạm.

Thêm vào đó, Luật Dữ liệu 2024 khuyến khích các tổ chức, cá nhân chia sẻ dữ liệu vì lợi ích chung, góp phần phát triển dữ liệu mở và dữ liệu dùng chung cho xã hội. Chủ sở hữu dữ liệu được quyền (*và được khuyến khích*) chia sẻ dữ liệu mà mình sở hữu cho cơ quan nhà nước hoặc cộng đồng nhằm phục vụ mục tiêu lợi ích công cộng, chẳng hạn trong lĩnh vực y tế, giáo dục, giao thông.... Đương nhiên, việc chia sẻ này phải trên cơ sở tự nguyện và tuân thủ quy định bảo mật (*ví dụ dữ liệu cá nhân chỉ chia sẻ khi có sự đồng ý của chủ thẻ dữ liệu*). Bằng cách đó, luật động viên các doanh nghiệp đóng góp vào hệ sinh thái dữ liệu quốc gia, trong khi vẫn bảo đảm quyền tài sản và bí mật kinh doanh của họ. Thật vậy, Nghị quyết 57-NQ/TW khẳng định cần “*có cơ chế, chính sách bảo đảm dữ liệu thành nguồn tài nguyên, tư liệu sản xuất quan trọng*” và “*phát triển mạnh mẽ công nghiệp dữ liệu, hình thành các cơ sở dữ liệu lớn có chủ quyền của Việt Nam*”. Luật Dữ liệu đã cụ thể hóa chủ trương này, khuyến khích đặt các trung tâm dữ liệu tại Việt Nam, xây dựng thị trường giao dịch dữ liệu, thu hút doanh nghiệp trong và ngoài nước đầu tư vào lĩnh vực dữ liệu. Điều này bác bỏ hoàn toàn luận điệu rằng luật sẽ “cản trở kinh tế, đầu tư”. Trái lại, một khung pháp lý rõ ràng về dữ liệu chính là điều kiện tiên quyết để doanh nghiệp số yên tâm đầu tư và hội nhập quốc tế.

Có thể nói, Luật Dữ liệu 2024 là hành lang pháp lý chặt chẽ cho thị trường dữ liệu, thúc đẩy phát triển kinh tế số và chuyển đổi số bền vững.

3. Vai trò của “chủ quản dữ liệu” và cơ chế giám sát thực thi nghiêm minh

Cùng với chủ thẻ và chủ sở hữu, Luật Dữ liệu 2024 định danh một chủ thể quan trọng khác: “chủ quản dữ liệu”. Nếu chủ sở hữu là “ông chủ” quyết định hướng khai thác tài sản dữ liệu, thì chủ quản dữ liệu chính là người “quản lý kỹ thuật”, đảm bảo dữ liệu được vận hành an toàn, trôi chảy theo yêu cầu của chủ sở hữu. Khoản 13 Điều 3 Luật Dữ liệu 2024 định nghĩa chủ quản dữ liệu là “*cơ quan, tổ chức, cá nhân thực hiện hoạt động xây dựng, quản lý, vận hành, khai thác dữ*



liệu theo yêu cầu của chủ sở hữu dữ liệu”. Chủ quản dữ liệu có thể chính là chủ sở hữu (nếu tự mình vận hành dữ liệu) hoặc là bên thứ ba được thuê/giao quản lý (ví dụ một công ty dịch vụ dữ liệu được doanh nghiệp thuê ngoài). Việc luật phân định rõ vai trò chủ sở hữu và chủ quản giúp mô hình hóa các quan hệ trong nền kinh tế dữ liệu: chủ sở hữu quyết định “sử dụng tài sản dữ liệu vào việc gì”, còn chủ quản là người triển khai kỹ thuật, vận hành dữ liệu để thực hiện mục tiêu đó.

Trong bối cảnh nhiều tổ chức, doanh nghiệp thuê ngoài dịch vụ dữ liệu, việc quy định cụ thể trách nhiệm của chủ quản dữ liệu là rất cần thiết. Chủ quản dữ liệu có nghĩa vụ áp dụng các biện pháp kỹ thuật và quản trị phù hợp để bảo đảm tính toàn vẹn, an ninh, an toàn của dữ liệu trong suốt vòng đời xử lý. Điều 15 Luật Dữ liệu 2024 yêu cầu chủ quản dữ liệu phải xây dựng hệ thống quản trị dữ liệu đáp ứng các tiêu chí: dữ liệu phải đầy đủ, chính xác, toàn vẹn, nhất quán, được chuẩn hóa, an toàn, bảo mật và kịp thời. Nói cách khác, chủ quản dữ liệu chịu trách nhiệm về chất lượng và bảo mật dữ liệu do mình vận hành. Nếu có sai sót, rủi ro (như lọt lọt, mất mát dữ liệu), chủ quản trước tiên phải chịu trách nhiệm khắc phục và có thể bị chế tài. Luật cũng quy định chủ quản dữ liệu phải phân loại dữ liệu theo mức độ nhạy cảm, xây dựng phương án bảo vệ, sao lưu, phục hồi dữ liệu quan trọng và xóa/hủy dữ liệu khi hết thời hạn. Các quy trình truy cập, truy xuất dữ liệu phải tuân thủ nguyên tắc “đúng người, đúng quyền, đúng mục đích”: chỉ những người được ủy quyền hợp pháp mới được tiếp cận dữ liệu, và chỉ trong phạm vi cần thiết cho công việc.

Những quy định này cho thấy Luật Dữ liệu đặt ra yêu cầu rất cao về trách nhiệm của chủ quản dữ liệu trong bảo vệ thông tin, đặc biệt là dữ liệu cá nhân. Luật Bảo vệ Dữ liệu Cá nhân 2025 dành hẳn một chương quy định nghĩa vụ của bên kiểm soát và bên xử lý dữ liệu (*tương ứng với chủ sở hữu và chủ quản*) trong việc bảo đảm an ninh dữ liệu cá nhân. Chẳng hạn, mọi hoạt động thu thập, lưu trữ, sử dụng thông tin cá nhân đều phải được thông báo trước cho người liên quan, kể cả nội dung như mục đích xử lý, loại dữ liệu, thời gian lưu trữ, các bên liên quan...; nếu xảy ra sự cố mất an toàn thì phải kịp thời thông báo cho chủ thể dữ



liệu. Chủ quản dữ liệu có trách nhiệm đáp ứng nhanh chóng các yêu cầu thực thi quyền của chủ thẻ dữ liệu (*nhiều cung cấp bản sao dữ liệu, chỉnh sửa, xóa dữ liệu, rút lại sự đồng ý...*) trong thời hạn luật định. Tuyệt đối không được cung cấp hay phát tán dữ liệu cá nhân cho bên thứ ba nếu không có sự đồng ý của chủ thẻ hoặc yêu cầu từ cơ quan có thẩm quyền. Khi mục đích xử lý kết thúc hoặc hết hạn lưu trữ, chủ quản phải xóa/hủy dữ liệu cá nhân, trừ khi có căn cứ pháp lý để tiếp tục lưu (ví dụ *nghĩa vụ lưu trữ giao dịch tài chính theo luật thuế*). Những yêu cầu này bác bỏ luận điệu cho rằng luật “vi phạm quyền ẩn danh hay tự do ngôn luận”: thực tế, luật không điều chỉnh nội dung phát ngôn hay danh tính trên mạng, mà tập trung vào việc bảo đảm dữ liệu cá nhân (ví dụ *thông tin định danh, lịch sử hoạt động trực tuyến của công dân*) được lưu trữ, sử dụng một cách an toàn, có sự cho phép của họ. Điều này góp phần bảo vệ người dùng khỏi các rủi ro như đánh cắp danh tính, lừa đảo trực tuyến ‘vốn là điều kiện tiên quyết để tự do ngôn luận trên mạng được thực hiện một cách lành mạnh, văn minh.

Để đảm bảo các quyền, nghĩa vụ trên không chỉ nằm trên giấy mà được thực thi nghiêm túc, pháp luật Việt Nam đã thiết lập một cơ chế kiểm tra, giám sát và chế tài toàn diện. Trước hết, vai trò của cơ quan quản lý nhà nước được phân định rõ, trong đó Bộ Công an được giao làm đầu mối thống nhất quản lý nhà nước về dữ liệu số và bảo vệ dữ liệu cá nhân trên phạm vi toàn quốc. Điều này không có nghĩa “tất cả tập trung về Bộ Công an” theo nghĩa tiêu cực, mà là nhằm bảo đảm sự chỉ huy thống nhất, tránh chồng chéo trong thực thi. Cục An ninh mạng và Phòng chống tội phạm công nghệ cao (Bộ Công an) hiện là cơ quan chuyên trách bảo vệ dữ liệu cá nhân. Đồng thời, các bộ, ngành khác cũng được phân công giám sát lĩnh vực dữ liệu trong phạm vi ngành mình (ví dụ *Bộ Y tế quản lý bảo vệ dữ liệu y tế, Ngân hàng Nhà nước giám sát bảo vệ dữ liệu khách hàng ngành ngân hàng...* Ủy ban nhân dân các tỉnh thành cũng chịu trách nhiệm trên địa bàn). Như vậy, một mạng lưới đa cơ quan cùng tham gia dưới sự điều phối của Bộ Công an nhằm đảm bảo thực thi luật về dữ liệu được đồng bộ, hiệu quả. Đây là mô hình phổ biến trên thế giới: tương tự như



Liên minh châu Âu có các Cơ quan bảo vệ dữ liệu độc lập phối hợp với Ủy ban châu Âu, thì Việt Nam chọn cách huy động các bộ ngành hiện có dưới sự chỉ đạo tập trung để phù hợp hệ thống hành chính. Cách làm này vừa tận dụng chuyên môn ngành, vừa bảo đảm thống nhất quốc gia, không hề là “bí mật” hay “mắt minh bạch” như kẻ xâu xuyên tạc.

Hoạt động thanh tra, kiểm tra việc tuân thủ luật về dữ liệu sẽ được tiến hành định kỳ và đột xuất. Cơ quan chuyên trách có quyền kiểm tra hệ thống của các tổ chức, doanh nghiệp: từ việc có xin phép người dùng đúng luật không, hệ thống bảo mật có đáp ứng tiêu chuẩn không, doanh nghiệp đã thực hiện đánh giá tác động dữ liệu (*DPIA*) chưa, có vi phạm quyền chủ thể nào không.... Khi có dấu hiệu vi phạm hoặc có khiếu nại từ người dân, cơ quan chức năng có thể thanh tra đột xuất. Ví dụ, nếu nhiều người dùng tố cáo một công ty công nghệ lạm dụng dữ liệu khách hàng, Bộ Công an phối hợp Thanh tra Chính phủ (*phụ trách*) có thể tiến hành thanh tra ngay công ty đó. Doanh nghiệp sẽ phải cung cấp đầy đủ thông tin, cho phép kiểm tra hệ thống và thực thi các yêu cầu kỹ thuật của đoàn thanh tra (*như tạm dừng một hoạt động xử lý dữ liệu vi phạm*). Nếu phát hiện sai phạm, cơ quan chức năng sẽ xử phạt nghiêm minh và yêu cầu khắc phục hậu quả. Song song đó, doanh nghiệp cũng phải nhanh chóng phản hồi, giải quyết các yêu cầu của cá nhân liên quan (*ví dụ cung cấp dữ liệu, chỉnh sửa hoặc xóa dữ liệu theo đúng thời hạn luật định*), nếu không sẽ bị coi là vi phạm và tiếp tục bị xử lý.

- Về chế tài, pháp luật quy định nhiều mức độ xử lý vi phạm tương ứng với tính chất, mức độ hành vi. Xử phạt vi phạm hành chính được áp dụng đối với phần lớn vi phạm về bảo vệ dữ liệu, với mức phạt tiền đáng kể kèm biện pháp khắc phục hậu quả. Chẳng hạn, theo Nghị định 15/2020/NĐ-CP (*sửa đổi 14/2022/NĐ-CP*), hành vi thu thập thông tin cá nhân khi chưa được chủ thể đồng ý có thể phạt từ 10–20 triệu đồng; nếu cung cấp thông tin cá nhân cho bên thứ ba dù chủ thể đã yêu cầu ngừng thì phạt 40–60 triệu đồng. Hành vi sử dụng thông tin cá nhân sai mục đích hoặc mua bán dữ liệu cá nhân có thể phạt tới 60 triệu đồng. Ngoài ra,



cơ quan chức năng có thể áp dụng biện pháp như buộc tiêu hủy dữ liệu cá nhân đã thu thập trái phép, đình chỉ dịch vụ có thời hạn hoặc kiến nghị rút giấy phép nếu vi phạm nghiêm trọng, tái phạm nhiều lần. Với việc Luật Bảo vệ Dữ liệu Cá nhân ban hành, dự kiến sẽ sớm có nghị định mới thay thế Nghị định 15/2020/NĐ-CP để tăng năng lực tài, đủ sức răn đe. Tham khảo quốc tế như GDPR của EU (*phạt đến 4% doanh thu toàn cầu*), Việt Nam cũng cân nhắc mức phạt cao hơn với vi phạm nghiêm trọng liên quan dữ liệu nhạy cảm, ảnh hưởng nhiều người. Đối với cá nhân vi phạm, tùy trường hợp có thể bị xử lý kỷ luật (*nếu là công chức*), xử phạt hành chính, hoặc truy cứu hình sự. Bộ luật Hình sự hiện hành đã có tội danh như Điều 288 “*Tôi đưa hoặc sử dụng trái phép thông tin mạng, theo đó hành vi mua bán, trao đổi trái phép thông tin cá nhân của người khác trên mạng*” có thể bị phạt tù đến 7 năm. Nếu việc lợi dụng dữ liệu nhằm xâm phạm an ninh quốc gia, tuyên truyền chống phá thì sẽ bị truy tố về tội tương ứng (*như tội xâm phạm ANQG*). Mặc dù đến nay chưa nhiều vụ án hình sự về vi phạm dữ liệu cá nhân đơn thuần, nhưng luật đã mở đường cho khả năng này và yêu cầu xử lý kịp thời, nghiêm minh mọi hành vi vi phạm. Điều đó thêm một lần nữa khẳng định tính pháp quyền và minh bạch của hệ thống: mọi vi phạm (*dù là cơ quan, doanh nghiệp hay cá nhân*) đều không có “vùng cấm”, đều bị xử lý theo pháp luật. Nếu người dân cho rằng quyền lợi mình bị xâm phạm, họ có quyền khởi kiện ra tòa đòi bồi thường, thông qua tòa án đảm bảo giám sát tư pháp đối với các tranh chấp dữ liệu.

- Cùng với chế tài, pháp luật cũng dự liệu các biện pháp kỹ thuật bắt buộc để ngăn chặn, khắc phục vi phạm về dữ liệu. Cơ quan chức năng có thể ra quyết định buộc xóa bỏ thông tin cá nhân vi phạm, ngắt kết nối hệ thống hoặc đình chỉ hoạt động xử lý dữ liệu tạm thời nếu phát hiện vi phạm nghiêm trọng (*ví dụ một mạng xã hội liên tục vi phạm bảo vệ dữ liệu người dùng có thể bị yêu cầu tạm dừng dịch vụ để khắc phục*). Các chuyên gia an ninh mạng cũng sẽ tham gia giám định hệ thống, truy vết giao dịch dữ liệu trái phép để thu thập chứng cứ xử lý. Về lâu dài, các tiêu chuẩn kỹ thuật về bảo vệ dữ liệu sẽ được ban hành và bắt buộc tuân thủ,



doanh nghiệp nếu không đáp ứng mức tối thiểu (*ví dụ không mã hóa dữ liệu nhạy cảm, không có quy trình quản lý truy cập*) thì dù chưa xảy ra sự cố vẫn có thể bị xử phạt. Đây chính là cách tiếp cận “phòng ngừa hơn chữa cháy”, buộc tuân thủ tiêu chuẩn để giảm nguy cơ sự cố, đồng thời có phương án ngăn chặn kịp thời nếu sự cố xảy ra, tránh thiệt hại lan rộng.

Nhìn một cách tổng quát, cơ chế thực thi Luật Dữ liệu bao gồm sự kết hợp đa dạng giữa các biện pháp hành chính, kinh tế, kỹ thuật, tư pháp và cả sự tham gia của cộng đồng. Người dân được khuyến khích tố giác các vi phạm tới cơ quan chức năng, bất kỳ ai phát hiện hành vi xâm phạm dữ liệu cá nhân đều có thể báo tin cho cơ quan chuyên trách để kịp thời xử lý. Sự giám sát từ cộng đồng này giúp phát hiện nhanh vi phạm tiềm ẩn mà cơ quan quản lý có thể chưa bao quát hết. Về hợp tác quốc tế, Việt Nam cũng chủ động phối hợp với các nước để điều tra, xử lý vi phạm xuyên biên giới. Đây là yếu tố rất quan trọng trong bối cảnh dữ liệu lưu chuyển qua biên giới ngày càng nhiều. Thực tế, Luật Dữ liệu 2024 và Luật Bảo vệ Dữ liệu Cá nhân 2025 đã đặt ra những yêu cầu chặt chẽ nhưng hợp lý đối với hoạt động chuyển dữ liệu ra nước ngoài, nhằm đảm bảo lợi ích quốc gia và quyền lợi người dùng. Cụ thể, doanh nghiệp muốn chuyển dữ liệu cá nhân ra khỏi lãnh thổ Việt Nam phải lập hồ sơ đánh giá tác động gửi cơ quan chuyên trách trong vòng 60 ngày từ khi bắt đầu chuyển. Đối với dữ liệu quan trọng, dữ liệu cốt lõi (*liên quan an ninh, lợi ích công cộng...*), luật yêu cầu phải đảm bảo yêu cầu nghiêm ngặt hơn: có thể cần sự chấp thuận của cơ quan quản lý, cam kết dữ liệu được bảo vệ tương đương ở nước ngoài... Nếu không tuân thủ, cơ quan chức năng có quyền kiểm tra và đình chỉ việc chuyển dữ liệu. Những biện pháp này là hoàn toàn cần thiết để bảo vệ chủ quyền số và an ninh dữ liệu quốc gia, yếu tố được Đảng và Nhà nước ta xác định là sống còn trong chuyển đổi số. Song song đó, luật cũng tạo thuận lợi cho hội nhập dữ liệu quốc tế, khi doanh nghiệp tuân thủ các điều kiện đặt ra, họ có thể tự tin kết nối, trao đổi dữ liệu xuyên biên giới, mở rộng thị trường và dịch vụ. Như ông Nguyễn Phú Dũng (*Hiệp hội Dữ liệu quốc gia*) đánh giá: “Luật



Dữ liệu giúp doanh nghiệp an tâm đầu tư vào công nghệ như blockchain, định danh số phi tập trung, xác thực dữ liệu xuyên biên giới... Đặc biệt, khung pháp lý rõ ràng là điều kiện tiên quyết để các doanh nghiệp số hội nhập với tiêu chuẩn quốc tế". Điều này đập tan luận điệu cho rằng luật "đóng cửa" với thế giới, trái lại, Việt Nam đang xây dựng môi trường pháp lý minh bạch, an toàn để hội nhập và thu hút dòng dữ liệu xuyên biên giới một cách có lợi nhất.

Quốc hội khóa XV biểu quyết thông qua Luật Dữ liệu năm 2024 với sự đồng thuận cao, cho thấy quyết tâm lập pháp nhằm hoàn thiện hành lang pháp lý cho chuyển đổi số quốc gia. Luật Dữ liệu đặt ra các nguyên tắc quản lý và bảo vệ dữ liệu trên cơ sở tôn trọng quyền và lợi ích hợp pháp của người dân, đồng thời thúc đẩy khai thác hiệu quả “nguồn tài nguyên dữ liệu” phục vụ phát triển kinh tế – xã hội

Luật Dữ liệu 2024 ra đời là minh chứng hùng hồn cho nỗ lực của Việt Nam trong việc vừa phát triển kinh tế số, vừa bảo vệ chủ quyền số và quyền lợi của Nhân dân. Luật đã quy định rõ ràng quyền, nghĩa vụ, trách nhiệm của các chủ thể trong hệ sinh thái dữ liệu, từ người dân (*chủ thể dữ liệu*) đến doanh nghiệp (*chủ sở hữu dữ liệu*) và các bên vận hành kỹ thuật (*chủ quản dữ liệu*). Hệ thống pháp luật dữ liệu mới mẻ này đảm bảo rằng tài sản dữ liệu được quản lý, khai thác một cách minh bạch, an toàn, có trách nhiệm, đặt quyền riêng tư và lợi ích hợp pháp của người dân làm trọng tâm. Đồng thời, luật cũng mở đường cho việc chuyển hóa dữ liệu thành nguồn lực sản xuất mới, thúc đẩy chuyển đổi số toàn diện và sáng tạo số trong mọi ngành nghề. Những luận điệu xuyên tạc về Luật Dữ liệu 2024 thực chất chỉ là sự bóp méo, cắt xén nhằm gây hoang mang dư luận, đi ngược lại lợi ích quốc gia và nguyện vọng chính đáng của người dân về một xã hội số văn minh, an toàn. Thực tế thi hành luật sẽ chứng minh rằng pháp luật Việt Nam luôn đề cao và bảo vệ quyền con người trong không gian mạng, đồng thời xử lý nghiêm những ai lợi dụng dữ liệu để xâm hại an ninh, trật tự. Với niềm tin số được xây dựng trên nền tảng Luật Dữ liệu, Việt Nam sẽ vững bước trên con đường chuyển đổi số, tận dụng tối đa



“mỏ vàng” dữ liệu phục vụ phát triển đất nước phồn vinh, mà vẫn giữ vững chủ quyền, an ninh quốc gia và các giá trị nhân văn của xã hội. Luật Dữ liệu 2024 chính là tuyên ngôn pháp lý khẳng định chủ quyền số của Việt Nam, bác bỏ mọi luận điệu sai trái, và thể hiện rõ ràng rằng trong Nhà nước pháp quyền Cộng hòa xã hội chủ nghĩa Việt Nam, không một ai được phép đứng ngoài hoặc đứng trên luật pháp, kể cả trong không gian số.



TÀI LIỆU THAM KHẢO

1. Luật Dữ liệu (*Luật số 60/2024/QH15*);
2. Luật Bảo vệ dữ liệu cá nhân (*Luật số 91/2025/QH15*);
3. Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân;
4. Nghị định 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều của Luật Dữ liệu;
5. Nghị định 194/2025/NĐ-CP ngày 18/7/2025 về kết nối, chia sẻ dữ liệu, dữ liệu mở;
6. Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân;
7. Nghị định số 15/2020/NĐ-CP (*sửa đổi bổ sung 2022 và 2025*) quy định xử phạt vi phạm hành chính lĩnh vực CNTT, các mức phạt liên quan đến thông tin giả, tấn công mạng.;
8. Đoàn Công Yên, "Nhiệm vụ của doanh nghiệp khi xử lý dữ liệu cá nhân của người lao động", Tạp chí Luật sư Việt Nam, 2025.
9. Hồng Minh, "Luật Dữ liệu xây dựng niềm tin số và thúc đẩy chuyển đổi số toàn diện", Báo Nhân dân, 2025;
10. Minh Hiếu, "Luật Dữ liệu có hiệu lực: nền móng pháp lý cho quốc gia số an toàn và hiệu quả", Thông tấn xã Việt Nam, 2025;
11. Nguyễn Hương, "Cần thiết xây dựng và ban hành Luật Dữ liệu", Báo Công an Nhân dân, 2024;
12. Nguyễn Hương, "Các quyền và nghĩa vụ của chủ thẻ dữ liệu tại dự thảo Luật Bảo vệ dữ liệu cá nhân", Báo Công an nhân dân, 2025;
13. Nguyễn Văn Phúc, "Khung pháp lý chuyển dữ liệu xuyên biên giới của Việt Nam: Góc nhìn từ Luật Dữ liệu 2024 và Luật Bảo vệ dữ liệu cá nhân 2025", Tạp chí Pháp lý, 2025.