

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 3  
TƯƠNG LAI SỐ VIỆT NAM



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 3  
TƯƠNG LAI SỐ VIỆT NAM

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 ba – “Tương lai số Việt Nam” tập trung phân tích định hướng xây dựng, phát triển Trung tâm dữ liệu quốc gia; quy định về sản phẩm, dịch vụ dữ liệu và giải pháp bảo đảm an ninh, an toàn dữ liệu; nội dung quản lý nhà nước về dữ liệu, trong đó nhấn mạnh vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương đến năm 2030.

...

Với bố 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



## 08 TRÁCH NHIỆM CỦA TRUNG TÂM DỮ LIỆU QUỐC GIA

1. Tích hợp, đồng bộ, lưu trữ, phân tích, khai thác dữ liệu của các cơ quan nhà nước theo quy định của pháp luật nhằm tạo lập, quản trị Cơ sở dữ liệu tổng hợp quốc gia.
2. Quản trị, vận hành hạ tầng kỹ thuật, hạ tầng công nghệ thông tin và sàn dữ liệu tại Trung tâm dữ liệu quốc gia; cung cấp hạ tầng kỹ thuật, hạ tầng công nghệ thông tin cho các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội khi có nhu cầu sử dụng.
3. Tổ chức vận hành, quản trị, lưu trữ, quản lý, khai thác, điều phối dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia cho cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội để thực hiện chức năng, nhiệm vụ được giao hoặc theo yêu cầu của chủ sở hữu dữ liệu, chủ quản dữ liệu, chủ thể dữ liệu phù hợp với quy định của pháp luật.
4. Giám sát việc bảo đảm chất lượng dữ liệu, hoạt động điều phối dữ liệu; xây dựng các hệ thống chỉ số đo lường và đánh giá hiệu suất cho hoạt động quản trị dữ liệu.
5. Thực hiện biện pháp bảo vệ dữ liệu.
6. Nghiên cứu khoa học về dữ liệu, ứng dụng công nghệ trong xử lý dữ liệu, cung cấp hạ tầng công nghệ, sản phẩm, dịch vụ về dữ liệu; hỗ trợ tổ chức, cá nhân trong xử lý dữ liệu; xây dựng trung tâm đổi mới sáng tạo, hỗ trợ đổi mới sáng tạo về khoa học dữ liệu; phát triển hoạt động đổi mới sáng tạo về khoa học dữ liệu; phát triển hệ sinh thái khởi nghiệp đổi mới sáng tạo về khoa học và công nghệ trên nền tảng dữ liệu của Cơ sở dữ liệu tổng hợp quốc gia.
7. Tổ chức thực hiện các nội dung hợp tác quốc tế về dữ liệu.
8. Chính phủ quy định chi tiết Điều này.

Điều 31, Luật Dữ liệu 2024  
ngày 30/11/2024, (Luật số 60/2024/QH15)



## 05 QUY ĐỊNH SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU

1. Sản phẩm, dịch vụ về dữ liệu trong hoạt động trung gian dữ liệu, phân tích, tổng hợp dữ liệu, xác thực điện tử, sàn dữ liệu thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.
2. Dịch vụ xác thực điện tử thực hiện việc xác thực dữ liệu trong các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống định danh và xác thực điện tử do đơn vị sự nghiệp công lập, doanh nghiệp nhà nước đáp ứng điều kiện cung cấp dịch vụ.
3. Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu được hưởng ưu đãi như các doanh nghiệp hoạt động trong lĩnh vực công nghệ cao, đổi mới sáng tạo, khởi nghiệp sáng tạo, công nghiệp công nghệ số.
4. Các sản phẩm, dịch vụ khác về dữ liệu trong hoạt động giao dịch điện tử, viễn thông, an ninh mạng, an toàn thông tin mạng, công nghiệp công nghệ số, cơ yếu, công nghiệp quốc phòng, an ninh và động viên công nghiệp thực hiện theo quy định của pháp luật có liên quan.
5. Chính phủ quy định chi tiết Điều này.

Điều 39, Luật Dữ liệu 2024  
ngày 30/11/2024, (Luật số 60/2024/QH15)



## 06 NỘI DUNG QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU

- a) Xây dựng, ban hành, tổ chức thực hiện Chiến lược dữ liệu quốc gia; văn bản quy phạm pháp luật về dữ liệu; tiêu chuẩn, quy chuẩn kỹ thuật, định mức kinh tế - kỹ thuật, chất lượng dữ liệu;
- b) Tuyên truyền, phổ biến chính sách, pháp luật về dữ liệu; hướng dẫn cơ quan quản lý cơ sở dữ liệu, hệ thống thông tin trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu;
- c) Quản lý, giám sát các hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu, bảo đảm an ninh, an toàn dữ liệu;
- d) Báo cáo, thống kê về dữ liệu; nghiên cứu, ứng dụng khoa học và công nghệ về dữ liệu; sản phẩm, dịch vụ về dữ liệu; quản lý, giám sát, phát triển thị trường dữ liệu;
- đ) Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về dữ liệu;
- e) Đào tạo, bồi dưỡng, phát triển nguồn nhân lực và hợp tác quốc tế về dữ liệu.

Khoản 1, Điều 8, Luật Dữ liệu 2024  
ngày 30/11/2024, (Luật số 60/2024/QH15)



## MỤC LỤC

Câu 6: Định hướng về xây dựng, phát triển Trung tâm dữ liệu quốc gia? Trách nhiệm của Trung tâm dữ liệu quốc gia trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu số? .....	1
6.1. Định hướng về xây dựng, phát triển Trung tâm dữ liệu quốc gia ..	2
6.1.1. Cơ sở pháp lý .....	3
6.1.2. Quan điểm và định hướng phát triển .....	6
6.1.3. Vai trò chiến lược của Trung tâm dữ liệu quốc gia.....	9
6.2. Trách nhiệm của Trung tâm dữ liệu quốc gia trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu số .....	15
6.2.1. Tích hợp, đồng bộ, lưu trữ, phân tích, khai thác dữ liệu của các cơ quan nhà nước nhằm tạo lập, quản trị Cơ sở dữ liệu tổng hợp Quốc gia.....	17
6.2.2. Quản trị, vận hành hạ tầng kỹ thuật, hạ tầng công nghệ thông tin và sàn dữ liệu tại Trung tâm dữ liệu quốc gia; cung cấp hạ tầng kỹ thuật, hạ tầng Công nghệ thông tin cho các cơ quan Đảng, Nhà nước, MTTQVN và các tổ chức chính trị - xã hội khi có nhu cầu sử dụng.....	20
6.2.3. Tổ chức vận hành, quản trị, lưu trữ, quản lý, khai thác, điều phối dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia cho các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội để thực hiện chức năng, nhiệm vụ hoặc theo yêu cầu của chủ sở hữu dữ liệu, chủ quản dữ liệu, chủ thể dữ liệu phù hợp với quy định của pháp luật .....	23
6.2.4. Giám sát việc bảo đảm chất lượng dữ liệu, hoạt động điều phối dữ liệu; xây dựng các hệ thống chỉ số đo lường và đánh giá hiệu suất cho hoạt động quản trị dữ liệu.....	27
6.2.5. Thực hiện biện pháp bảo vệ dữ liệu.....	30
6.2.6. Nghiên cứu khoa học về dữ liệu, ứng dụng công nghệ trong xử lý dữ liệu, cung cấp hạ tầng công nghệ, sản phẩm, dịch vụ về dữ liệu; hỗ trợ tổ chức, cá nhân trong xử lý dữ liệu; xây dựng trung tâm đổi mới sáng tạo, hỗ trợ đổi mới sáng tạo về khoa học dữ liệu; phát triển hoạt động đổi mới sáng tạo về khoa học và công nghệ trên nền tảng dữ liệu của Cơ sở dữ liệu tổng hợp Quốc gia.....	34
6.2.7. Tổ chức thực hiện các nội dung hợp tác quốc tế về dữ liệu .....	37
6.2.8. Các trách nhiệm khác do Chính phủ quy định .....	40



KẾT LUẬN.....	41
PHỤ LỤC .....	46
<i>Phản bác thông tin sai sự thật về Trung tâm Dữ liệu quốc gia - Bộ Công an.....</i>	46
TÀI LIỆU THAM KHẢO.....	50
Câu 7: Quy định về sản phẩm, dịch vụ về dữ liệu? Các giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu? .....	51
7.1. Quy định về sản phẩm, dịch vụ dữ liệu theo Luật Dữ liệu 2024.....52	
7.1.1. Phạm vi sản phẩm, dịch vụ về dữ liệu .....	54
7.1.2. Dịch vụ trung gian dữ liệu, điều kiện đăng ký, nguyên tắc hoạt động .....	57
7.1.3. Phân tích, tổng hợp dữ liệu, yêu cầu bảo vệ dữ liệu cá nhân và điều kiện khai thác dữ liệu quốc gia .....	60
7.1.4. Sàn dữ liệu, chủ thể vận hành và dữ liệu bị cấm giao dịch.....64	
7.1.5. Trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ dữ liệu ..	69
7.2. Các giải pháp bảo đảm an ninh, an toàn dữ liệu trong ứng dụng sản phẩm, dịch vụ dữ liệu.....75	
7.2.1. Các quy định đảm bảo an ninh, an toàn dữ liệu.....75	
7.2.2. Các giải pháp kỹ thuật - công nghệ bảo đảm an toàn dữ liệu....	81
7.2.3. Cơ chế vận hành tổ chức bảo đảm an toàn dữ liệu tại Trung tâm dữ liệu quốc gia.....86	
7.2.4. Quản lý rủi ro dữ liệu và bảo vệ dữ liệu cốt lõi, cá nhân nhạy cảm .....	90
7.2.5. Mô hình và kinh nghiệm quốc tế tiêu biểu về bảo đảm an toàn dữ liệu và phát triển thị trường dữ liệu .....	94
7.2.6. Giải pháp hợp tác quốc tế và nâng cao năng lực nhân lực.....98	
7.2.7. Tổng hợp rủi ro an toàn dữ liệu và biện pháp bảo vệ tương ứng; Sơ đồ quy trình bảo mật .....	105
KẾT LUẬN.....	110
PHỤ LỤC .....	114
<i>Phản bác các quan điểm sai sự thật về sản phẩm, dịch vụ về dữ liệu</i>	114



<b>TÀI LIỆU THAM KHẢO .....</b>	<b>122</b>
<b>Câu 8: Nội dung quản lý nhà nước về dữ liệu? Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu? Nhiệm vụ trọng tâm cần tập trung trong gian đoạn từ nay đến năm 2030? .....</b>	<b>123</b>
<b>8.1. Nội dung quản lý nhà nước về dữ liệu .....</b>	<b>124</b>
<b>8.2. Vai trò, trách nhiệm của Bộ Công an và Công an các cấp trong quản lý dữ liệu .....</b>	<b>125</b>
<b>8.2.1. Bộ Công an là cơ quan đầu mối quản lý nhà nước về dữ liệu .</b>	<b>125</b>
<b>8.2.2. Công an các đơn vị, địa phương.....</b>	<b>128</b>
<b>8.3. Nhiệm vụ trọng tâm giai đoạn 2025-2030: Chuyển đổi số, phát triển NDC và hệ sinh thái dữ liệu an toàn .....</b>	<b>130</b>
<b>8.3.1. Hoàn thiện thể chế pháp luật về dữ liệu .....</b>	<b>130</b>
<b>8.3.2. Xây dựng và phát triển hạ tầng Trung tâm dữ liệu quốc gia ...</b>	<b>131</b>
<b>8.3.3. Tích hợp và hoàn thiện các cơ sở dữ liệu quốc gia, chuyên ngành .....</b>	<b>132</b>
<b>8.3.4. Phát triển các ứng dụng và dịch vụ dữ liệu, thúc đẩy kinh tế dữ liệu.....</b>	<b>133</b>
<b>8.3.5. Bảo đảm an ninh, an toàn dữ liệu trong quá trình chuyển đổi.</b>	<b>134</b>
<b>8.3.3. Kết luận và kiến nghị .....</b>	<b>137</b>
<b>PHỤ LỤC .....</b>	<b>141</b>
<i>Phản bác thông tin sai sự thật liên quan đến việc QLNN về dữ liệu..</i>	<b>141</b>
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>145</b>



**Câu 6: Định hướng về xây dựng, phát triển Trung tâm dữ liệu quốc gia? Trách nhiệm của Trung tâm dữ liệu quốc gia trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu số?**





**Câu 6: Định hướng về xây dựng, phát triển Trung tâm dữ liệu quốc gia? Trách nhiệm của Trung tâm dữ liệu quốc gia trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu số?**

### Trả lời

#### 6.1. Định hướng về xây dựng, phát triển Trung tâm dữ liệu quốc gia

Dữ liệu số hiện nay được coi là tài nguyên chiến lược và “tư liệu sản xuất” quan trọng của quốc gia trong thời đại số. Thật vậy, dữ liệu là nền tảng cho phát triển Chính phủ số, kinh tế số, xã hội số. Việc khai thác hiệu quả dữ liệu giúp đổi mới phương thức quản trị, thúc đẩy tăng trưởng kinh tế, nâng cao chất lượng cuộc sống người dân. Luật Dữ liệu 2024 đã xác lập việc thành lập Trung tâm dữ liệu quốc gia với vai trò là thiết chế trung tâm, đầu mối quan trọng nhất để quản lý, vận hành kho dữ liệu quốc gia thống nhất. Trung tâm dữ liệu quốc gia gắn liền với Cơ sở Dữ liệu Tổng hợp Quốc gia trở thành nền tảng kết nối, tích hợp, chia sẻ, phân tích, khai thác, điều phối dữ liệu trên phạm vi toàn quốc.



Hình ảnh: Đồng chí Đại tá TS Vũ Văn Tấn, Phó Cục trưởng Cục Cảnh sát QLHC về TTXH phát biểu khai mạc Hội thảo khoa học đóng góp ý kiến cho Chiến lược Dữ liệu Quốc gia và dự thảo Luật Dữ liệu năm 2024. Ảnh: Bộ Công an



Việc xây dựng Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia đánh dấu bước chuyển đổi quan trọng trong hạ tầng số của Việt Nam, từ mô hình dữ liệu phân tán sang môi trường dữ liệu tập trung, được quản trị thống nhất. Trong bối cảnh Chính phủ đẩy mạnh chương trình chuyển đổi số quốc gia, Trung tâm dữ liệu quốc gia được kỳ vọng sẽ là nền tảng chiến lược giúp phát huy cao độ giá trị của dữ liệu, nguồn tài nguyên quý giá, tạo động lực cho đổi mới sáng tạo và nâng cao năng lực cạnh tranh quốc gia trong kỷ nguyên số.

### 6.1.1. Cơ sở pháp lý

Luật Dữ liệu năm 2024 là cơ sở pháp lý quan trọng nhất cho việc hình thành và phát triển Trung tâm dữ liệu quốc gia. Luật này có hiệu lực từ 1/7/2025, gồm một mục riêng (*Mục I, Chương III*) quy định về “Xây dựng, phát triển Trung tâm dữ liệu quốc gia” với 03 điều (*từ Điều 30 đến Điều 32*). Các điều khoản này đề ra khung pháp lý cho toàn bộ vòng đời của Trung tâm dữ liệu quốc gia, bao gồm:

- **Điều 30,** Cơ sở hạ tầng của Trung tâm dữ liệu quốc gia quy định Trung tâm dữ liệu quốc gia phải được thiết kế, xây dựng với hạ tầng kỹ thuật hiện đại, đáp ứng tiêu chuẩn kỹ thuật, an toàn, an ninh và có khả năng mở rộng linh hoạt; ưu tiên sử dụng công nghệ tiên tiến, năng lượng xanh...

- **Điều 31,** Trách nhiệm của Trung tâm dữ liệu quốc gia xác định nhiệm vụ của Trung tâm dữ liệu quốc gia là tích hợp, đồng bộ, lưu trữ, phân tích, khai thác và điều phối dữ liệu của các cơ quan nhà nước theo quy định pháp luật. Đồng thời, Trung tâm dữ liệu quốc gia cung cấp hạ tầng công nghệ thông tin cho các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và đoàn thể khi có nhu cầu. Luật cũng giao Trung tâm dữ liệu quốc gia giám sát chất lượng dữ liệu và điều phối dòng dữ liệu; thực hiện các biện pháp bảo vệ dữ liệu; nghiên cứu, ứng dụng công nghệ dữ liệu, phát triển hệ sinh thái đổi mới sáng tạo về dữ liệu; tổ chức hợp tác quốc tế về dữ liệu. Những nhiệm vụ chiến lược này cho thấy Trung tâm dữ liệu quốc gia không chỉ là nơi lưu trữ dữ liệu, mà còn là “bộ não” về dữ liệu, thúc đẩy khoa học dữ liệu và sáng tạo trong lĩnh vực dữ liệu của quốc gia.



- **Điều 32**, Bảo đảm nguồn lực cho Trung tâm dữ liệu quốc gia: nhấn mạnh sự ưu tiên đầu tư của Nhà nước về hạ tầng, kinh phí, nhân lực cho Trung tâm dữ liệu quốc gia. Ngân sách nhà nước đảm bảo hoạt động của Trung tâm dữ liệu quốc gia, cùng với việc huy động các nguồn hợp pháp khác. Nhà nước cũng có cơ chế thu hút nhân tài, nhân lực chất lượng cao vận hành Trung tâm dữ liệu quốc gia. Quy định này thể hiện quyết tâm của Chính phủ trong việc xây dựng Trung tâm dữ liệu quốc gia vững mạnh, ổn định và bền vững.

Ngoài Luật Dữ liệu 2024, việc phát triển Trung tâm dữ liệu quốc gia còn dựa trên các chính sách và chiến lược về chuyển đổi số quốc gia. Chiến lược phát triển Chính phủ số giai đoạn 2021-2025, định hướng đến 2030 (*Quyết định 942/QĐ-TTg ngày 15/06/2021*) đặt mục tiêu đến 2030 Việt Nam thuộc nhóm 50 nước dẫn đầu thế giới và đứng thứ 3 ASEAN về Chính phủ điện tử, kinh tế số. Để đạt được mục tiêu đó, Chiến lược nhấn mạnh phải phát triển hạ tầng dữ liệu quốc gia vững chắc, kết nối, chia sẻ và an toàn nhằm phục vụ phát triển kinh tế - xã hội toàn diện. Bên cạnh đó, Chương trình Chuyển đổi số quốc gia đến 2025, định hướng 2030 (*Quyết định 749/QĐ-TTg ngày 03/06/2020*) của Thủ tướng Chính phủ cũng coi dữ liệu là trụ cột của chuyển đổi số, yêu cầu xây dựng các cơ sở dữ liệu quốc gia lớn và nền tảng dữ liệu mở để người dân, doanh nghiệp cùng tham gia khai thác. Gần đây, Chiến lược Dữ liệu Quốc gia đến năm 2030 (*phê duyệt tháng 2/2024*) cũng khẳng định dữ liệu là “nguồn tài nguyên mới” và đề ra mục tiêu kết nối toàn diện các trung tâm dữ liệu trên cả nước thành một mạng lưới chia sẻ, xử lý dữ liệu lớn phục vụ phát triển. Như vậy, định hướng xây dựng Trung tâm dữ liệu quốc gia hoàn toàn phù hợp và là yêu cầu triển khai cụ thể của các chiến lược quốc gia về chính phủ số và chuyển đổi số.

Song song với khuôn khổ pháp lý trong nước, Việt Nam cũng tham khảo kinh nghiệm quốc tế trong quá trình xây dựng Trung tâm dữ liệu quốc gia. Trên thế giới, nhiều quốc gia đã thiết lập các trung tâm dữ liệu chính phủ tập trung nhằm tối ưu quản lý dữ liệu. Hàn Quốc là một ví dụ điển hình: năm 2005, Hàn Quốc thành lập Trung tâm Tích hợp Dữ liệu Chính phủ (*Government Integrated*



Data Center - GIDC) đầu tiên trên thế giới dành riêng cho cơ quan nhà nước. GIDC Hàn Quốc đã tích hợp, vận hành tập trung hơn 1.400 hệ thống chính phủ điện tử vốn trước đây rải rác tại 44 cơ quan trung ương. Toàn bộ máy chủ, thiết bị phần cứng của các bộ ngành được di dời về hai trung tâm dữ liệu (*tại Daejeon năm 2005 và Gwangju năm 2007*). Sau đó, Hàn Quốc dần hợp nhất các phần mềm, dịch vụ và triển khai hệ thống quản trị tập trung thời gian thực (*n-TOPS*) do nước này tự phát triển để giám sát tình trạng của hàng chục nghìn thiết bị, ứng dụng từ các bộ ngành. Nhờ mô hình tập trung, Chính phủ Hàn Quốc giảm đầu tư trùng lắp, nâng cao hiệu suất vận hành và đặc biệt là tăng cường an ninh mạng cho toàn bộ hệ thống dữ liệu quốc gia. GIDC áp dụng hệ thống bảo mật tích hợp “e-ANSI Sung” để ngăn chặn hiệu quả các cuộc tấn công mạng như hack, virus, DDoS... vào hệ thống chính phủ. Kinh nghiệm Hàn Quốc cho thấy tầm quan trọng của việc hiện đại hóa, tập trung hóa hạ tầng dữ liệu nhằm đảm bảo “hiện đại, đồng bộ, an ninh, an toàn, hiệu quả”. Việt Nam khi xây dựng Trung tâm dữ liệu quốc gia cũng hướng tới một mô hình tương tự: kết nối liên thông các kho dữ liệu rời rạc, đồng thời ứng dụng công nghệ điện toán đám mây, trí tuệ nhân tạo để nâng cao hiệu quả khai thác và bảo mật dữ liệu quốc gia.



Hình ảnh: Lễ ra mắt Trung tâm Dữ liệu quốc gia. Ảnh: Báo Nhân dân



Tóm lại, Trung tâm dữ liệu quốc gia được xây dựng trên nền tảng pháp lý vững chắc của Luật Dữ liệu 2024 và các chiến lược quốc gia, đồng thời kế thừa bài học từ các nước đi trước. Đây chính là tiền đề để triển khai Trung tâm dữ liệu quốc gia theo định hướng hiện đại, an toàn, linh hoạt và tích hợp cao, đáp ứng mục tiêu quản trị quốc gia bằng dữ liệu.



Hình ảnh: Đồng chí Thiếu tướng Nguyễn Ngọc Cường - Giám đốc Trung tâm  
Dữ liệu quốc gia, Bộ Công an. Ảnh: Báo CAND

#### **6.1.2. Quan điểm và định hướng phát triển**

Trong quá trình xây dựng và phát triển, Trung tâm dữ liệu quốc gia được định nghĩa là nền tảng hạ tầng số trọng yếu phục vụ quản trị quốc gia dựa trên dữ liệu. Theo định hướng chỉ đạo, phát triển Trung tâm dữ liệu quốc gia phải gắn liền với việc đổi mới phương thức quản lý nhà nước, từ ra quyết định, hoạch định chính sách cho đến cung cấp dịch vụ công đều dựa trên cơ sở dữ liệu tin cậy và



phân tích dữ liệu khoa học. Trung tâm dữ liệu quốc gia được Chính phủ xác định là hạ tầng nền tảng cốt lõi để cung cấp các dịch vụ dữ liệu cho Chính phủ, người dân và doanh nghiệp, hỗ trợ hoạch định chính sách, kiến tạo phát triển, thúc đẩy xây dựng Chính phủ số, kinh tế số, xã hội số, đồng thời bảo đảm các yêu cầu về quốc phòng, an ninh trong kỷ nguyên số. Quan điểm này thể hiện rõ trong phát biểu của lãnh đạo Bộ Công an: “Trung tâm dữ liệu quốc gia... phát huy cao độ giá trị của dữ liệu (*nguồn tài nguyên quý giá, tư liệu sản xuất mới*) nhằm tạo động lực thúc đẩy đổi mới sáng tạo, nâng cao hiệu suất lao động, năng lực cạnh tranh quốc gia, nâng tầm vị thế đất nước”. Như vậy, mục tiêu tối thượng khi phát triển Trung tâm dữ liệu quốc gia là biến dữ liệu thành tài sản, thành sức mạnh để quản trị và phát triển đất nước trong thời đại mới.

Về định hướng phát triển cụ thể, Trung tâm dữ liệu quốc gia cần được xây dựng theo hướng hiện đại hóa, bảo đảm an toàn - an ninh, linh hoạt và tích hợp cao:

- **Thứ nhất**, hiện đại hóa và tích hợp cao: Hạ tầng của Trung tâm dữ liệu quốc gia phải áp dụng các công nghệ tiên tiến nhất (*điện toán đám mây, big data, AI, IoT...*) nhằm đáp ứng tiêu chuẩn quốc tế về trung tâm dữ liệu, sẵn sàng cho các ứng dụng phân tích dữ liệu thời gian thực, trí tuệ nhân tạo phục vụ chính phủ và kinh tế số. Dữ liệu từ khắp các bộ, ngành, địa phương sẽ được tích hợp toàn diện tại Trung tâm dữ liệu quốc gia, tạo thành một kho dữ liệu tổng hợp tập trung có khả năng kết nối, chia sẻ mọi lúc mọi nơi. Nguyên tắc “một cửa” về dữ liệu được quán triệt, thay vì dữ liệu nằm rải rác, không tương thích, Trung tâm dữ liệu quốc gia bảo đảm một nền tảng tích hợp chung để các hệ thống khác chỉ cần kết nối một lần duy nhất. Hướng phát triển này phù hợp với tinh thần chỉ đạo của Đảng, phát triển hạ tầng số phải “hiện đại, đồng bộ, an ninh, an toàn, hiệu quả, tránh lãng phí”, làm chủ các công nghệ chiến lược, tận dụng tối đa tiềm năng của dữ liệu.

- **Thứ hai**, bảo đảm an toàn - an ninh: Trung tâm dữ liệu quốc gia được coi là trọng điểm về an ninh dữ liệu quốc gia, do đó việc đảm bảo an toàn thông tin và an ninh mạng là yêu cầu xuyên suốt trong quá trình xây dựng và vận hành.



Trung tâm sẽ được trang bị các hệ thống bảo mật nhiều lớp, cơ chế giám sát 24/7 và tuân thủ các chuẩn an ninh cao nhất để bảo vệ kho dữ liệu quốc gia khỏi các mối đe dọa. Bên cạnh đó, Trung tâm dữ liệu quốc gia cũng phải tuân thủ nghiêm ngặt Luật Bảo vệ dữ liệu cá nhân 2025 nhằm bảo vệ quyền riêng tư của người dân. Quan điểm phát triển là “an ninh dữ liệu gắn liền với an ninh quốc gia”, đảm bảo chủ quyền số của Việt Nam, dữ liệu quan trọng phải được lưu trữ, quản trị bởi hệ thống trong nước, hạn chế phụ thuộc nước ngoài. Điều này liên quan mật thiết đến việc Trung tâm dữ liệu quốc gia xây dựng các trung tâm dữ liệu vùng (*khu vực*) để dự phòng và nâng cao khả năng phục hồi hệ thống khi gặp sự cố, tấn công mạng.

- **Thứ ba**, linh hoạt, mở rộng: Hệ thống Trung tâm dữ liệu quốc gia phải có tính linh hoạt cao để thích ứng với sự phát triển nhanh chóng của công nghệ và khối lượng dữ liệu. Cho phép các cơ sở dữ liệu đặc thù (*nhiều quốc phòng, an ninh, cơ yếu*) không bắt buộc phải chuyển về hạ tầng Trung tâm dữ liệu quốc gia nếu chưa sẵn sàng, nhưng khuyến khích kết nối khai thác trên cơ sở tự nguyện và lộ trình thống nhất. Điều này tạo dư địa để Trung tâm dữ liệu quốc gia dần dần mở rộng phạm vi bao phủ, phục vụ đa mục tiêu, đa ngành mà không gây xáo trộn đột ngột.

Bên cạnh định hướng về kỹ thuật, một quan điểm quan trọng là Trung tâm dữ liệu quốc gia phải phục vụ “đa cơ quan, đa cấp, đa ngành”. Nghĩa là trung tâm được thiết kế cho nhiều đối tượng sử dụng, từ cơ quan Trung ương đến địa phương, từ khối Chính phủ, Đảng, đoàn thể đến khối doanh nghiệp và người dân. Chỉ khi đó, Trung tâm dữ liệu quốc gia mới thực sự trở thành hạ tầng dùng chung liên ngành, tối ưu hóa nguồn lực dữ liệu quốc gia. Luật Dữ liệu đã quán triệt tinh thần này khi trao quyền khai thác dữ liệu cho nhiều nhóm đối tượng (*cơ quan nhà nước, người dân, doanh nghiệp*) với cách thức phù hợp. Đồng thời, Trung tâm dữ liệu quốc gia đặt dưới sự quản lý tập trung của Chính phủ (*giao Bộ Công an vận hành*) để đảm bảo tính thống nhất, tránh trùng lặp đầu tư và thuận tiện cho tích hợp dữ liệu. Quan điểm “phục vụ đa ngành, đa cấp” còn thể hiện qua việc Trung tâm dữ liệu quốc gia cung cấp hạ tầng cho các cơ quan Đảng, Nhà nước, Mặt trận và đoàn thể khi có nhu cầu.



Điều này giúp tất cả các cấp, các ngành đều có cơ hội tiếp cận và khai thác tài nguyên dữ liệu chung, hướng tới một “Chính phủ dữ liệu” toàn diện.

Mục tiêu cuối cùng là hỗ trợ chuyển đổi số toàn diện mọi lĩnh vực: từ chính quyền, kinh tế đến xã hội, văn hóa, giáo dục, y tế, tư pháp, an ninh... Trung tâm dữ liệu quốc gia và kho Cơ sở dữ liệu tổng hợp Quốc gia sẽ đóng vai trò như hệ thần kinh dữ liệu kết nối các lĩnh vực này lại với nhau. Ví dụ: dữ liệu dân cư (*do Bộ Công an quản lý*) khi tích hợp vào Cơ sở dữ liệu tổng hợp Quốc gia có thể hỗ trợ ngành y tế xác thực thông tin bệnh nhân, hỗ trợ ngành giáo dục theo dõi tình hình học sinh, hỗ trợ tòa án tra cứu lý lịch tư pháp... Việc liên thông dữ liệu giữa các ngành thông qua Trung tâm dữ liệu quốc gia sẽ tạo nên bức tranh dữ liệu tổng thể về xã hội, giúp Chính phủ giám sát, điều hành ở tầm vĩ mô chính xác hơn. Định hướng này phù hợp với quan điểm của Bộ Chính trị tại Nghị quyết 57-NQ/TW (2024) rằng chuyển đổi số là cuộc cách mạng “**sâu sắc, toàn diện trên tất cả các lĩnh vực**”, trong đó dữ liệu và hạ tầng số là trọng tâm cốt lõi cần được ưu tiên phát triển. Thực tế, Bộ Công an cũng đã nhấn mạnh dữ liệu dân cư là dữ liệu lõi trong chuyển đổi số quốc gia, làm nền tảng hình thành các dữ liệu chuyên ngành khác. Vì vậy, phát triển Trung tâm dữ liệu quốc gia gắn liền với mục tiêu xây dựng các cơ sở dữ liệu quốc gia cốt lõi (*nhiều dân cư, đất đai, doanh nghiệp, tài chính công...*) và thúc đẩy các ngành sử dụng dữ liệu này để chuyển đổi phương thức hoạt động. Đến năm 2030, Việt Nam kỳ vọng hình thành một xã hội số, trong đó mọi quyết sách, dịch vụ đều dựa trên dữ liệu chung, người dân không phải khai báo lặp lại và hưởng tiện ích từ việc các ngành chia sẻ dữ liệu với nhau. Trung tâm dữ liệu quốc gia chính là bệ đỡ hạ tầng để hiện thực hóa viễn cảnh đó.

#### **6.1.3. Vai trò chiến lược của Trung tâm dữ liệu quốc gia**

Với những định hướng trên, Trung tâm dữ liệu quốc gia được kỳ vọng đảm nhận nhiều vai trò chiến lược trong hệ sinh thái chính phủ số Việt Nam:

- **Thứ nhất**, Trung tâm dữ liệu quốc gia là “Trục kết nối” các cơ sở dữ liệu quốc gia, bộ ngành và địa phương: Trung tâm dữ liệu quốc gia đóng vai trò như nút trung tâm kết nối tất cả các cơ sở dữ liệu từ trung ương đến địa phương, từ dữ



liệu ngành y tế, giáo dục, tư pháp cho đến dữ liệu doanh nghiệp, dân cư, đất đai... Thông qua Cơ sở dữ liệu tổng hợp Quốc gia, dữ liệu từ các nguồn khác nhau được liên thông, tích hợp trên một nền tảng thống nhất. Điều này giúp phá vỡ tình trạng dữ liệu rời rạc trước đây, tạo nên một mạng lưới dữ liệu thống nhất trên phạm vi quốc gia. Mỗi bộ, ngành, địa phương chỉ cần kết nối hệ thống của mình với Trung tâm dữ liệu quốc gia là có thể chia sẻ và khai thác dữ liệu với các bên khác. Như vậy, Trung tâm dữ liệu quốc gia thực sự trở thành “hạ tầng liên thông dữ liệu” quốc gia. Vai trò này đặc biệt quan trọng trong việc giảm trùng lặp thu thập dữ liệu, tiết kiệm chi phí vận hành công nghệ thông tin cho toàn bộ khu vực công. Thay vì mỗi đơn vị phải đầu tư trung tâm dữ liệu riêng lẻ, Trung tâm dữ liệu quốc gia cung cấp dịch vụ tập trung cho nhiều đơn vị cùng sử dụng. Đây là mô hình quản trị dữ liệu tập trung mà nhiều quốc gia đã triển khai để tăng hiệu quả: ví dụ: Hàn Quốc đã tích hợp 47.000 thiết bị và ứng dụng CNTT của 44 cơ quan chính phủ về chung một đầu mối GIDC và vận hành tập trung 24/7. Kết quả là hạ tầng CNTT chính phủ Hàn Quốc trở nên tinh gọn, đồng bộ và an toàn hơn rất nhiều. Việt Nam kỳ vọng Trung tâm dữ liệu quốc gia cũng tạo ra hiệu ứng tương tự, giúp liên thông dữ liệu 3 cấp (*trung ương - tỉnh - xã*) và giữa các ngành, chia sẻ dữ liệu xuyên suốt từ trung ương tới cơ sở.

**- Thứ hai,** Trung tâm dữ liệu quốc gia là nền tảng xử lý, phân tích dữ liệu lớn phục vụ ra quyết định: Một vai trò cốt lõi của Trung tâm dữ liệu quốc gia là trở thành trung tâm phân tích dữ liệu chiến lược của Chính phủ. Với việc tập hợp lượng dữ liệu khổng lồ từ mọi lĩnh vực, Trung tâm dữ liệu quốc gia có điều kiện triển khai các hệ thống phân tích dữ liệu lớn (*Big Data Analytics*), trí tuệ nhân tạo để xử lý, khai thác dữ liệu này. Cơ sở Dữ liệu Tổng hợp Quốc gia chính là kho dữ liệu lớn cho phép thực hiện các phân tích chuyên sâu phục vụ công tác thống kê, dự báo, hoạch định chính sách ở tầm vĩ mô. Ví dụ: từ dữ liệu tổng hợp, Chính phủ có thể phân tích xu hướng kinh tế - xã hội, phát hiện sớm những vấn đề như dịch bệnh, thiên tai, tội phạm, từ đó ra quyết định kịp thời. Trung tâm dữ liệu quốc gia cũng hỗ trợ xây dựng các báo cáo thông minh, bảng điều khiển dữ liệu



(dashboard) cho lãnh đạo các cấp, giúp việc chỉ đạo, điều hành dựa trên bằng chứng dữ liệu thay vì cảm tính. Theo Bộ Công an, Trung tâm dữ liệu quốc gia sẽ hình thành một “kho dữ liệu về con người” và kho dữ liệu tổng hợp từ các nguồn, đóng vai trò trụ cột để phát triển các hệ thống dữ liệu tin cậy của Nhà nước phục vụ kết nối, chia sẻ và tạo ra nhiều giá trị mới. Nói cách khác, Trung tâm dữ liệu quốc gia sẽ là “bộ não số” hỗ trợ Chính phủ trong quản trị quốc gia bằng dữ liệu. Vai trò này càng quan trọng khi Việt Nam hướng đến Chính phủ số ra quyết định theo dữ liệu. Ngoài khu vực công, nền tảng dữ liệu tập trung còn phục vụ khu vực tư: doanh nghiệp, viện nghiên cứu có thể khai thác (*theo quy định*) dữ liệu mở, dữ liệu tổng hợp để tạo ra các sản phẩm, dịch vụ mới hoặc phân tích thị trường. Thực tế ở các nước phát triển cho thấy khi Chính phủ mở kho dữ liệu, khu vực tư nhân đã tận dụng để phát triển nhiều ứng dụng hữu ích, thúc đẩy đổi mới sáng tạo dựa trên dữ liệu. Do đó, Trung tâm dữ liệu quốc gia sẽ không chỉ hỗ trợ ra quyết định công, mà còn thúc đẩy nền kinh tế dữ liệu trong xã hội.



Hình ảnh: Lễ ra mắt Trung tâm Sáng tạo, khai thác dữ liệu và Phòng An ninh, an toàn hệ thống thuộc Trung tâm Dữ liệu quốc gia. Ảnh: Báo Chính phủ



- **Thứ ba**, Trung tâm dữ liệu quốc gia là hạ tầng kỹ thuật cho khởi nghiệp đổi mới sáng tạo về dữ liệu: Một nhiệm vụ chiến lược được Luật Dữ liệu giao cho Trung tâm dữ liệu quốc gia là phát triển hệ sinh thái khởi nghiệp đổi mới sáng tạo về dữ liệu. Trung tâm sẽ xây dựng Trung tâm Đổi mới sáng tạo về khoa học dữ liệu trực thuộc, cung cấp môi trường để các chuyên gia, doanh nghiệp khởi nghiệp có thể tiếp cận hạ tầng tính toán mạnh, dữ liệu lớn và công cụ phân tích phục vụ nghiên cứu, sáng tạo. Đây có thể hiểu là việc hình thành các phòng thí nghiệm dữ liệu (*data lab*), sandbox về dữ liệu dưới sự bảo trợ của Trung tâm dữ liệu quốc gia. Các doanh nghiệp khởi nghiệp có thể thử nghiệm các ý tưởng ứng dụng dữ liệu (ví dụ phân tích dữ liệu giao thông để tối ưu vận tải, dùng AI xử lý dữ liệu y tế để hỗ trợ chẩn đoán...) trên nền tảng dữ liệu và công nghệ của Trung tâm dữ liệu quốc gia. Bộ Công an cũng định hướng nghiên cứu phát triển Quỹ đổi mới sáng tạo về khoa học dữ liệu để hỗ trợ tài chính cho cá nhân, doanh nghiệp khởi nghiệp dữ liệu. Điều này cho thấy Trung tâm dữ liệu quốc gia sẽ là bệ phóng cho cộng đồng khởi nghiệp, giúp họ tiết kiệm chi phí đầu tư hạ tầng ban đầu (vì có thể dùng hạ tầng của Trung tâm dữ liệu quốc gia) và dễ dàng tiếp cận nguồn dữ liệu công chất lượng. Vai trò cung cấp hạ tầng này rất quan trọng để hình thành thị trường dữ liệu ở Việt Nam. Như Nghị quyết 57-NQ/TW đề ra, Việt Nam cần phát triển kinh tế dữ liệu và các sàn giao dịch dữ liệu, xây dựng ngành công nghiệp dữ liệu lớn của riêng mình. Trung tâm dữ liệu quốc gia chính là nơi có thể thiết lập sàn dữ liệu quốc gia, nơi gặp gỡ giữa bên cung (các cơ quan sở hữu dữ liệu, doanh nghiệp) và bên cầu (các startup, nhà phát triển) để giao dịch, trao đổi dữ liệu một cách an toàn, hợp pháp. Mặt khác, trung tâm cũng sẽ phát triển nền tảng dữ liệu mở quốc gia cho phép công bố các tập dữ liệu mở và API cho cộng đồng khai thác dễ dàng. Khi hệ sinh thái dữ liệu đã hình thành, Trung tâm dữ liệu quốc gia vừa là “nhà cung cấp hạ tầng”, vừa đóng vai trò điều phối, giám sát để đảm bảo mọi hoạt động khai thác dữ liệu tuân thủ pháp luật và bảo vệ được dữ liệu nhạy cảm.

- **Thứ tư**, Trung tâm dữ liệu quốc gia bảo đảm an ninh dữ liệu quốc gia và hỗ trợ quốc phòng, an ninh: Trong bối cảnh an ninh phi truyền thống và chiến



tranh mạng gia tăng, Trung tâm dữ liệu quốc gia có vai trò như “thành trì dữ liệu” bảo vệ chủ quyền số của đất nước. Trung tâm sẽ triển khai các giải pháp an ninh mạng thông nhất cho hệ thống dữ liệu chính phủ, qua đó phát hiện sớm và ngăn chặn các cuộc tấn công mạng nhắm vào kho dữ liệu quốc gia. Khi tất cả các dòng dữ liệu đều chảy qua Trung tâm dữ liệu quốc gia, việc giám sát và phản ứng sự cố bảo mật sẽ tập trung, nhanh chóng hơn so với trước kia (*mỗi nơi một kiểu*). Đồng thời, Trung tâm dữ liệu quốc gia hỗ trợ các cơ quan an ninh, quốc phòng phân tích dữ liệu lớn để phục vụ nhiệm vụ bảo vệ Tổ quốc (*Ví dụ: phân tích dữ liệu xuất nhập cảnh, dữ liệu di biến động dân cư giúp cơ quan công an theo dõi tốt hơn tình hình an ninh trật tự. Phân tích dữ liệu kinh tế, tài chính giúp phát hiện những nguy cơ đe dọa an ninh kinh tế*). Trung tâm dữ liệu quốc gia cũng có thể cung cấp năng lực tính toán cao phục vụ mô phỏng, thử nghiệm vũ khí công nghệ cao hoặc các ứng dụng AI trong quốc phòng.Thêm nữa, Trung tâm dữ liệu quốc gia tạo nền tảng để xây dựng các hệ thống chỉ huy và kiểm soát dựa trên dữ liệu thời gian thực trong lĩnh vực an ninh, quốc phòng. Có thể nói, việc Việt Nam xây dựng Trung tâm dữ liệu quốc gia cũng nhằm mục tiêu bảo vệ lợi ích, an ninh quốc gia trong không gian số, tương tự như việc củng cố một căn cứ hạ tầng chiến lược. Quan điểm “giữ dữ liệu như giữ đát đai” đang dần hình thành, dữ liệu được xem là tài sản quốc gia cần được quản lý tập trung để tránh rơi vào tay thế lực xấu hoặc bị khai thác bất hợp pháp ra nước ngoài.

- **Thứ năm**, Trung tâm dữ liệu quốc gia thúc đẩy cải cách hành chính và dịch vụ công thông minh: Trung tâm dữ liệu quốc gia khi đi vào vận hành đầy đủ sẽ tạo thuận lợi lớn cho người dân và doanh nghiệp trong giao dịch với chính quyền. Nhờ Cơ sở dữ liệu tổng hợp Quốc gia, các thủ tục hành chính có thể tự động điền thông tin (*auto-fill*) từ dữ liệu đã có, người dân không phải nộp lại giấy tờ mà cơ quan nhà nước đã nắm giữ. Ví dụ: làm thủ tục xin trợ cấp xã hội, nếu trước đây công dân phải nộp bản photo sổ hộ khẩu, CMND... thì với kết nối dữ liệu, cán bộ chỉ cần tra cứu Cơ sở dữ liệu tổng hợp Quốc gia để lấy thông tin, người dân không cần xuất trình giấy tờ nữa. Điều này giảm gánh nặng giấy tờ,



giảm chi phí tuân thủ cho người dân, đúng với mục tiêu cải cách hành chính. Bên cạnh đó, Trung tâm dữ liệu quốc gia còn cho phép dịch vụ công trực tuyến toàn trình hoạt động hiệu quả. Nhờ dữ liệu được chia sẻ, người dân có thể ngồi nhà làm thủ tục trên cổng dịch vụ công mà không cần qua nhiều bước xác minh thủ công giữa các cơ quan. Quy trình giải quyết thủ tục sẽ nhanh chóng, minh bạch hơn, vì dữ liệu được luân chuyển tự động và có thể theo dõi trạng thái xử lý theo thời gian thực. Đây chính là nền tảng để hướng tới một Chính phủ không giấy tờ, nơi mọi giao dịch với dân đều qua môi trường số. Trung tâm dữ liệu quốc gia cũng sẽ cung cấp dữ liệu tin cậy cho việc định danh điện tử công dân (*Usage of VN eID*), giúp xác thực thông tin nhanh trong các dịch vụ công và dịch vụ số. Như vậy, vai trò của Trung tâm dữ liệu quốc gia gắn chặt với việc xây dựng Chính phủ số phục vụ, lấy người dân, doanh nghiệp làm trung tâm thụ hưởng. Khi dữ liệu thông suốt, người dân sẽ cảm nhận rõ hiệu quả: thủ tục gọn nhẹ hơn, dịch vụ công cá nhân hóa hơn (*vì cơ quan nhà nước hiểu rõ dữ liệu của từng người để phục vụ phù hợp*). Đây là bước tiến quan trọng để nâng cao chất lượng quản trị công, củng cố niềm tin và sự hài lòng của xã hội đối với bộ máy nhà nước.

*Bảng Nhiệm vụ chính của Trung tâm dữ liệu quốc gia theo Luật Dữ liệu*

Nhiệm vụ trọng tâm	Mô tả cụ thể
Tích hợp, điều phối dữ liệu quốc gia	Tích hợp, đồng bộ, lưu trữ dữ liệu của các cơ quan nhà nước; điều phối, giám sát luồng dữ liệu giữa các hệ thống để bảo đảm chất lượng và tính thống nhất của dữ liệu. Xây dựng hệ thống chỉ số đo lường, đánh giá hiệu suất quản trị dữ liệu trên toàn quốc.
Bảo vệ và đảm bảo an ninh dữ liệu	Thực hiện các biện pháp bảo vệ an toàn dữ liệu, an ninh mạng cho các hệ thống thông tin và cơ sở dữ liệu kết nối với Trung tâm dữ liệu quốc gia. Phòng ngừa, phát hiện, ngăn chặn các rủi ro, sự cố xâm phạm dữ liệu; tuân thủ luật pháp về an toàn thông tin, an ninh mạng.
Phát triển hạ tầng, thúc đẩy đổi mới dữ liệu	Nghiên cứu ứng dụng công nghệ mới ( <i>AI, Big Data...</i> ) trong xử lý dữ liệu; cung cấp hạ tầng kỹ thuật, sản phẩm, dịch vụ về dữ liệu cho các cơ quan, tổ chức. Xây dựng Trung tâm Đổi mới sáng



Nhiệm vụ trọng tâm	Mô tả cụ thể
	tạo về khoa học dữ liệu; hỗ trợ tổ chức, cá nhân trong xử lý dữ liệu; phát triển hệ sinh thái khởi nghiệp đổi mới sáng tạo về dữ liệu trên nền tảng Cơ sở dữ liệu tổng hợp Quốc gia.
Hợp tác quốc tế về dữ liệu	Tổ chức thực hiện các hoạt động hợp tác với quốc tế trong lĩnh vực dữ liệu nhằm trao đổi kinh nghiệm, thu hút nguồn lực và nâng cao vị thế của Việt Nam về quản trị dữ liệu.

Nhìn chung, sự ra đời của Trung tâm dữ liệu quốc gia mang ý nghĩa chiến lược to lớn. Từ góc độ quản trị, Trung tâm dữ liệu quốc gia sẽ thay đổi phương thức quản lý nhà nước sang hướng hiện đại, dựa trên dữ liệu và bằng chứng. Từ góc độ công nghệ, Trung tâm dữ liệu quốc gia là bước đột phá về hạ tầng số, tạo nền tảng cho mọi hoạt động chính phủ điện tử, chính phủ số sau này. Từ góc độ kinh tế - xã hội, Trung tâm dữ liệu quốc gia mở ra kỷ nguyên khai thác tài nguyên dữ liệu để tạo ra của cải, giá trị mới, đồng thời nâng cao chất lượng dịch vụ công, hướng tới sự hài lòng của người dân, doanh nghiệp.

Có thể nói, trong bối cảnh cuộc Cách mạng công nghiệp 4.0 và chuyển đổi số diễn ra mạnh mẽ, dữ liệu thực sự trở thành quyền lực mới của quốc gia. Việc Quốc hội thông qua Luật Dữ liệu 2024 và Chính phủ xúc tiến thành lập Trung tâm dữ liệu quốc gia cho thấy Việt Nam đã sẵn sàng nắm lấy “quyền lực dữ liệu” này. Trung tâm dữ liệu quốc gia không chỉ là một cơ sở hạ tầng, nó là hệ điều hành của một quốc gia số. Với tầm nhìn chiến lược, sự đầu tư nghiêm túc và học hỏi kinh nghiệm thế giới, Trung tâm dữ liệu quốc gia Việt Nam hứa hẹn sẽ trở thành bệ phóng cho Chính phủ số và nền kinh tế số Việt Nam phát triển bứt phá trong thập kỷ tới.

## **6.2. Trách nhiệm của Trung tâm dữ liệu quốc gia trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu số**

Luật Dữ liệu năm 2024 xác định Trung tâm dữ liệu quốc gia là hạ tầng và đầu mối quan trọng nhằm tích hợp, quản lý tập trung dữ liệu của các cơ quan nhà nước, phục vụ cho chuyển đổi số và phát triển kinh tế - xã hội. Điều 31 của Luật



Dữ liệu 2024 quy định chi tiết các trách nhiệm của Trung tâm dữ liệu quốc gia, từ việc thu thập, lưu trữ dữ liệu cho đến đảm bảo chất lượng, an toàn dữ liệu, hỗ trợ nghiên cứu đổi mới sáng tạo và hợp tác quốc tế từ <sup>(1)</sup>Trách nhiệm về tích hợp - lưu trữ - khai thác dữ liệu; <sup>(2)</sup>Vận hành hạ tầng kỹ thuật; <sup>(3)</sup>Điều phối và chia sẻ dữ liệu; <sup>(4)</sup>Giám sát chất lượng dữ liệu; <sup>(5)</sup>Bảo vệ dữ liệu; <sup>(6)</sup>Nghiên cứu khoa học và đổi mới sáng tạo đến <sup>(7)</sup>Hợp tác quốc tế.

Theo luật, Trung tâm dữ liệu quốc gia do Chính phủ xây dựng, quản lý, khai thác và vận hành một cách tập trung, thống nhất, ổn định, bền vững. Trung tâm dữ liệu quốc gia được coi là “trái tim” của hạ tầng dữ liệu quốc gia, nơi tích hợp, đồng bộ, lưu trữ, chia sẻ, phân tích, khai thác, điều phối dữ liệu của các cơ quan nhà nước; đồng thời cung cấp hạ tầng công nghệ thông tin cho các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và đoàn thể khi có nhu cầu. Trên tinh thần đó, Điều 31 liệt kê 07 nhóm trách nhiệm cụ thể của Trung tâm dữ liệu quốc gia, phản ánh các vai trò đa dạng mà trung tâm này phải đảm nhiệm.



*Hình ảnh: Hệ thống Dữ liệu quốc gia về dân cư. Ảnh: Báo Nhân dân*



### 6.2.1. *Tích hợp, đồng bộ, lưu trữ, phân tích, khai thác dữ liệu của các cơ quan nhà nước nhằm tạo lập, quản trị Cơ sở dữ liệu tổng hợp Quốc gia*

Khoản 1 Điều 31 quy định trách nhiệm đầu tiên và cốt lõi nhất của Trung tâm dữ liệu quốc gia: “*Tích hợp, đồng bộ, lưu trữ, phân tích, khai thác dữ liệu của các cơ quan nhà nước theo quy định của pháp luật nhằm tạo lập, quản trị Cơ sở dữ liệu tổng hợp quốc gia.*”

Nội dung này giao cho Trung tâm dữ liệu quốc gia nhiệm vụ thu thập và quản lý tập trung dữ liệu từ các cơ quan nhà nước, tiến hành tích hợp (*gộp các nguồn dữ liệu rời rạc*), đồng bộ (*cập nhật nhất quán, thống nhất*), lưu trữ lâu dài, đồng thời phân tích và khai thác các dữ liệu đó. Mục đích cuối cùng là xây dựng và vận hành Cơ sở Dữ liệu Tổng hợp Quốc gia, tạo thành kho dữ liệu hợp nhất quy mô quốc gia, được quản trị tập trung tại Trung tâm dữ liệu quốc gia.

Cơ sở dữ liệu tổng hợp Quốc gia 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. Điều 33 Luật Dữ liệu cũng nêu rõ Cơ sở dữ liệu tổng hợp Quốc gia phải được Chính phủ xây dựng, quản lý tập trung, thống nhất tại Trung tâm dữ liệu quốc gia. Như vậy, vai trò của Trung tâm dữ liệu quốc gia theo khoản 1 là đầu mối tập hợp tất cả các dữ liệu quan trọng của quốc gia về một hệ thống chung. Các loại dữ liệu đưa vào Cơ sở dữ liệu tổng hợp Quốc gia được luật liệt kê bao gồm: dữ liệu mở, dữ liệu dùng chung của cơ quan nhà nước, dữ liệu dùng riêng (*theo quyết định của Thủ tướng*), dữ liệu của các cơ quan Đảng và đoàn thể (*nếu chủ sở hữu dữ liệu đồng ý*) và các dữ liệu khác do tổ chức, cá nhân cung cấp. Có thể thấy phạm vi dữ liệu rất rộng, bao trùm từ dữ liệu hành chính công, dữ liệu chuyên ngành cho đến dữ liệu do tư nhân đóng góp.

“Tích hợp, đồng bộ” dữ liệu hàm ý rằng Trung tâm dữ liệu quốc gia phải thiết lập các kết nối kỹ thuật (*API, nền tảng tích hợp*) với các cơ sở dữ liệu bộ, ngành, địa phương để tự động nhận và hợp nhất dữ liệu. Khi cơ quan nguồn có cập nhật hay điều chỉnh dữ liệu, Trung tâm dữ liệu quốc gia cần tiếp nhận để đồng bộ hóa vào Cơ sở dữ liệu tổng hợp Quốc gia, đảm bảo dữ liệu trung tâm luôn



thống nhất và mới nhất. Điều này sẽ giúp một thay đổi dữ liệu tại nguồn sẽ được truyền đến mọi nơi thông qua Cơ sở dữ liệu tổng hợp Quốc gia, giảm việc cập nhật thủ công rác rưởi ở từng cơ sở dữ liệu riêng lẻ. Việc đồng bộ qua Trung tâm dữ liệu quốc gia sẽ cắt giảm các thủ tục hành chính liên quan đến cập nhật, bổ sung thông tin (*ví dụ: khi một dữ liệu được thay đổi bởi cơ quan chủ quản, nó sẽ được cập nhật vào Cơ sở dữ liệu tổng hợp Quốc gia và đồng bộ tự động đến các cơ sở dữ liệu khác, từ đó người dân không phải làm thủ tục điều chỉnh thông tin lặp lại ở từng ngành*). Đây là lợi ích trực tiếp của việc tích hợp, đồng bộ dữ liệu tập trung, bảo đảm “một nguồn dữ liệu, sử dụng cho nhiều mục đích”, hạn chế tình trạng cát cứ dữ liệu và giảm gánh nặng giấy tờ cho người dân.

Bên cạnh việc tích hợp và lưu trữ, Trung tâm dữ liệu quốc gia còn có chức năng phân tích, khai thác dữ liệu. Điều này nghĩa là trung tâm sẽ ứng dụng các công nghệ dữ liệu lớn, trí tuệ nhân tạo, công cụ phân tích để xử lý, tổng hợp, phân tích chuyên sâu các dữ liệu đa ngành được tập hợp. Mục đích là tạo ra thông tin, tri thức hỗ trợ công tác quản lý, điều hành và hoạch định chính sách. Thực tế, luật yêu cầu Cơ sở dữ liệu tổng hợp Quốc gia phải thực hiện được việc phân tích chuyên sâu các dữ liệu, hỗ trợ xây dựng cơ chế chính sách và phát triển kinh tế - xã hội. Như vậy, Trung tâm dữ liệu quốc gia không chỉ thu động lưu trữ dữ liệu thô, mà còn trực tiếp xử lý dữ liệu để tạo giá trị gia tăng, phục vụ ra quyết định dựa trên dữ liệu (*data-driven decision making*) trong Chính phủ.

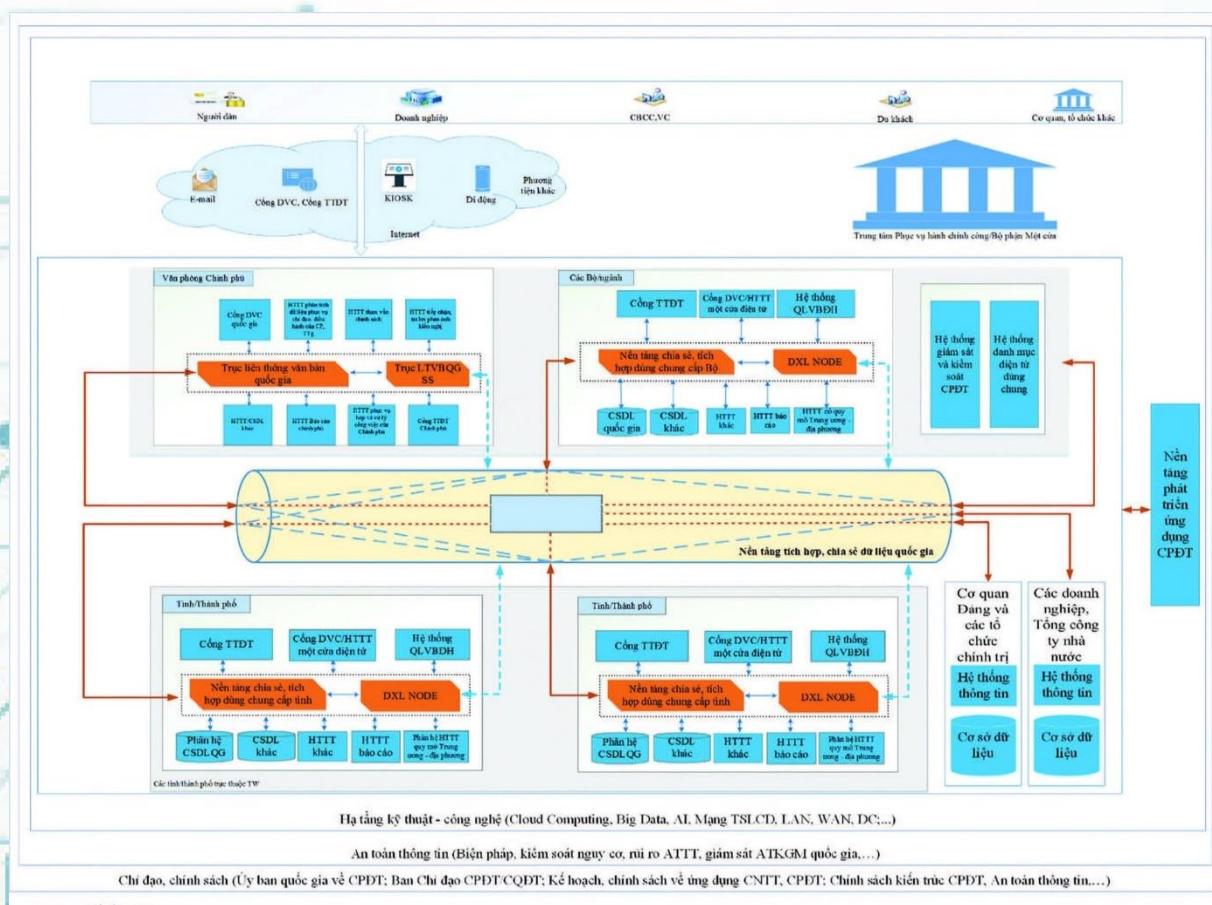
Trong giai đoạn xây dựng ban đầu, Trung tâm dữ liệu quốc gia sẽ phải tập trung vào việc thu thập và làm giàu dữ liệu. Dữ liệu số được luật coi là một tài nguyên, tài sản quý, cần huy động mọi nguồn lực để phát triển. Có thể hình dung Trung tâm dữ liệu quốc gia như một “kho dữ liệu tổng quốc gia” gom dữ liệu từ các lĩnh vực (*dân cư, đất đai, doanh nghiệp, tài chính, y tế, giáo dục...*) về. Điều này đặt ra yêu cầu về tiêu chuẩn và chất lượng dữ liệu khi tích hợp, để các dữ liệu khác nguồn có thể kết hợp hiệu quả. Luật đã giao Trung tâm dữ liệu quốc gia hướng dẫn các cơ quan trong việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu khi đồng bộ vào trung tâm. Nhờ đó, dữ liệu từ các bộ ngành khi đưa vào Cơ

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



sở dữ liệu tổng hợp Quốc gia sẽ có cấu trúc thống nhất, các định danh chung (*nhiều mã định danh cá nhân, mã đơn vị...*) nhằm đảm bảo khả năng liên thông, kết nối.

Một ví dụ thực tiễn cho thấy nỗ lực thực hiện chức năng tích hợp dữ liệu này là Nền tảng tích hợp, chia sẻ, điều phối dữ liệu quốc gia mà Bộ Công an ra mắt tháng 7/2025. Nền tảng này được thiết kế như một hạ tầng số chuyên dụng để thu thập, xử lý, kiểm tra và phân phối dữ liệu, với các quy trình được tự động hóa tối đa. Đây chính là công cụ giúp Trung tâm dữ liệu quốc gia thực hiện hiệu quả nhiệm vụ tích hợp, đồng bộ và luân chuyển dữ liệu giữa các hệ thống. Nhờ nền tảng này, việc kết nối, chia sẻ dữ liệu trở nên trơn tru: các hệ thống của bộ, ngành, địa phương chỉ cần kết nối với Trung tâm dữ liệu quốc gia thay vì phải kết nối từng hệ thống với nhau, từ đó giảm đáng kể số lượng kết nối phải thực hiện cũng như khôi lượng công việc tích hợp kỹ thuật.



Hình ảnh: Sơ đồ kết nối cấp quốc gia - Khung kiến trúc CPĐT Việt Nam phiên bản 2.0. Ảnh: Tạp chí TT&TT



Tóm lại, Khoản 1 xác lập vai trò “nhạc trưởng” về dữ liệu cho Trung tâm dữ liệu quốc gia, thu thập mọi dữ liệu then chốt từ các cơ quan, hợp nhất thành một nguồn dữ liệu quốc gia duy nhất, đảm bảo dữ liệu luôn cập nhật, nhất quán; đồng thời khai thác, phân tích kho dữ liệu đó để phục vụ quản lý nhà nước và các nhu cầu phát triển. Đây là tiền đề cho các nhiệm vụ khác, bởi nếu không có dữ liệu đầy đủ và được quản trị tập trung thì các chức năng như điều phối, chia sẻ, phân tích, đổi mới sáng tạo sẽ không thể triển khai hiệu quả.

#### **6.2.2. Quản trị, vận hành hạ tầng kỹ thuật, hạ tầng công nghệ thông tin và sàn dữ liệu tại Trung tâm dữ liệu quốc gia; cung cấp hạ tầng kỹ thuật, hạ tầng Công nghệ thông tin cho các cơ quan Đảng, Nhà nước, MTTQVN và các tổ chức chính trị - xã hội khi có nhu cầu sử dụng**

Khoản 2 Điều 31 quy định Trung tâm dữ liệu quốc gia có nhiệm vụ “Quản trị, vận hành hạ tầng kỹ thuật, hạ tầng công nghệ thông tin và sàn dữ liệu tại Trung tâm dữ liệu quốc gia; cung cấp hạ tầng kỹ thuật, hạ tầng công nghệ thông tin cho các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội khi có nhu cầu sử dụng.”

Cụ thể bao gồm <sup>(1)</sup>Quản trị, vận hành hạ tầng kỹ thuật/CNTT và “sàn dữ liệu” tại Trung tâm dữ liệu quốc gia - nghĩa là Trung tâm dữ liệu quốc gia phải xây dựng, quản lý bộ máy hạ tầng công nghệ của chính mình, đảm bảo nó hoạt động ổn định, thông suốt. <sup>(2)</sup>Cung cấp hạ tầng kỹ thuật/CNTT cho các cơ quan khác khi có nhu cầu, Trung tâm dữ liệu quốc gia đóng vai trò như một nhà cung cấp dịch vụ hạ tầng (*infrastructure provider*) cho các cơ quan Đảng, Nhà nước, đoàn thể.

- **Trước hết**, hạ tầng kỹ thuật và hạ tầng Công nghệ thông tin của Trung tâm dữ liệu quốc gia cần hiểu là toàn bộ hệ thống trung tâm dữ liệu vật lý và nền tảng công nghệ do Trung tâm dữ liệu quốc gia vận hành. Điều 30 Luật Dữ liệu có quy định các yêu cầu đối với hạ tầng này, chẳng hạn phải đáp ứng tiêu chuẩn trung tâm dữ liệu, đảm bảo an ninh bảo mật theo cấp độ, tách biệt môi trường phát triển/kiểm thử... Trong Nghị định 165/2025/NĐ-CP hướng dẫn Luật Dữ liệu, Chính phủ nêu



rõ Trung tâm dữ liệu quốc gia sẽ xây dựng, phát triển hạ tầng điện toán đám mây và triển khai thành các vùng chức năng để phục vụ nhu cầu các cơ quan, đáp ứng việc phát triển các phân hệ tích hợp, đồng bộ, khai thác dữ liệu đòi hỏi bảo mật cao. Đồng thời, Trung tâm dữ liệu quốc gia thiết lập hệ thống tính toán hiệu suất cao và hệ thống phân tích dữ liệu phục vụ quản lý, với các mô hình phân tích dự báo để khai thác dữ liệu từ Cơ sở dữ liệu tổng hợp Quốc gia. Những định hướng này cho thấy hạ tầng của Trung tâm dữ liệu quốc gia sẽ rất hiện đại, bao gồm các trung tâm dữ liệu lớn, nền tảng điện toán đám mây chính phủ, các cụm máy chủ tính toán mạnh, nền tảng phân tích dữ liệu lớn, đảm bảo đủ năng lực lưu trữ, xử lý khối lượng dữ liệu khổng lồ tập trung.

Khái niệm “sàn dữ liệu” tại Trung tâm dữ liệu quốc gia cũng được đề cập. Thuật ngữ này ám chỉ một nền tảng dữ liệu tập trung (*data platform*) đặt tại Trung tâm dữ liệu quốc gia, có thể hiểu như “chợ dữ liệu” hoặc hạ tầng chia sẻ dữ liệu. Thực tế, Trung tâm dữ liệu quốc gia được giao thiết lập Công dữ liệu quốc gia làm đầu mối để cơ quan nhà nước công bố thông tin về dữ liệu họ quản lý, công bố và cung cấp dữ liệu mở, qua đó tăng cường minh bạch và thúc đẩy sáng tạo. Bên cạnh đó, Trung tâm dữ liệu quốc gia còn xây dựng “sàn giao dịch dữ liệu quốc gia” với vai trò là hạ tầng số chuyên biệt để thực hiện giao dịch, chia sẻ và khai thác dữ liệu, góp phần hình thành thị trường dữ liệu minh bạch, hiệu quả và an toàn tại Việt Nam. Những hệ thống này (*công dữ liệu, sàn dữ liệu*) chính là các “sàn dữ liệu” mà luật đề cập, về bản chất là nền tảng kỹ thuật cho phép kết nối cung-cầu dữ liệu, quản lý danh mục dữ liệu, API truy cập, thanh toán hoặc chia sẻ dữ liệu giữa các bên. Trung tâm dữ liệu quốc gia chịu trách nhiệm vận hành các nền tảng đó.

- **Thứ hai**, phần thứ hai của Khoản 2 cho thấy Trung tâm dữ liệu quốc gia cung cấp dịch vụ hạ tầng cho các cơ quan khác. Điều này phù hợp với chiến lược tối ưu hóa hạ tầng CNTT của Chính phủ, thay vì mỗi bộ, ngành tự đầu tư trung tâm dữ liệu riêng, họ có thể sử dụng hạ tầng của Trung tâm dữ liệu quốc gia. Theo luật, các Cơ sở dữ liệu Quốc gia bắt buộc phải sử dụng hạ tầng của Trung tâm dữ



liệu quốc gia theo lộ trình do Chính phủ quy định. Các Cơ sở dữ liệu thuộc lĩnh vực quốc phòng, an ninh, đối ngoại, cơ yếu, chuyên ngành... thì không bắt buộc nhưng nếu có nhu cầu sử dụng để nâng cao hiệu quả, bảo đảm an ninh an toàn thì có thể thỏa thuận với Trung tâm dữ liệu quốc gia. Quy định này cho thấy lộ trình chuyển dịch hạ tầng, dần dần các cơ sở dữ liệu trọng yếu sẽ được đưa về lưu trữ, vận hành trên hệ thống Trung tâm dữ liệu quốc gia, tạo sự tập trung thay vì phân tán. Chính phủ sẽ có văn bản quy định trình tự, thủ tục để các đơn vị chuyển đổi sang dùng hạ tầng Trung tâm dữ liệu quốc gia.

Theo Nghị định 165/2025/NĐ-CP, Trung tâm dữ liệu quốc gia cung cấp nhiều loại dịch vụ hạ tầng:

- Dịch vụ đặt máy chủ: Trung tâm dữ liệu quốc gia cho phép các cơ quan đưa máy chủ, thiết bị của mình tới đặt tại Trung tâm dữ liệu quốc gia, cung cấp không gian, nguồn điện, điều hòa, bảo đảm môi trường vật lý. Các cơ quan có thể lựa chọn dùng chung không gian hoặc khu riêng và vẫn tự kiểm soát hệ thống của mình trên hạ tầng đó.

- Dịch vụ hạ tầng ảo/máy chủ dùng chung: Trung tâm dữ liệu quốc gia cung cấp máy chủ, thiết bị mạng, thiết bị an ninh an toàn mạng, thiết bị lưu trữ... với cấu hình đa dạng tại trung tâm, đáp ứng nhu cầu của các cơ quan. Điều này tương tự dịch vụ cloud computing (*điện toán đám mây*) nội bộ cho Chính phủ các cơ quan có thể thuê máy chủ ảo, dung lượng lưu trữ từ Trung tâm dữ liệu quốc gia thay vì phải mua sắm; đồng thời đảm bảo vấn đề bảo mật dữ liệu.

- Dịch vụ triển khai, vận hành hạ tầng cho cơ sở dữ liệu: Trung tâm dữ liệu quốc gia hỗ trợ triển khai và vận hành hạ tầng kỹ thuật phục vụ các Cơ sở dữ liệu Quốc gia, các hệ thống thông tin cơ sở dữ liệu khác. Nói cách khác, Trung tâm dữ liệu quốc gia có thể đảm nhận luôn việc quản trị kỹ thuật cho hạ tầng Cơ sở dữ liệu của bộ, ngành nếu được đề nghị, giúp các đơn vị đỡ gánh nặng về nhân sự kỹ thuật.

Với những dịch vụ trên, Trung tâm dữ liệu quốc gia đóng vai trò như “nhà cung cấp hạ tầng dùng chung của Chính phủ”. Đây là mô hình tương tự một số quốc gia xây dựng chính phủ điện tử tập trung, ví dụ GovCloud cung cấp bởi



Chính phủ Singapore cho các bộ ngành, hoặc các trung tâm dữ liệu dùng chung cấp nhà nước ở một số nước châu Âu. Mục tiêu là tiết kiệm chi phí đầu tư, vận hành, bảo đảm tiêu chuẩn an toàn, bảo mật thông nhất và dễ dàng kết nối liên thông qua một hạ tầng chung.

Về phương diện này, việc Bộ Công an chủ trì xây dựng Trung tâm dữ liệu quốc gia đã được khẳng định. Bộ Công an phối hợp cùng các cơ quan liên quan để bảo đảm Trung tâm dữ liệu quốc gia đáp ứng các tiêu chuẩn kỹ thuật về trung tâm dữ liệu. Đồng thời, chính sách đã có cơ chế hỗ trợ tài chính: cán bộ, chiến sĩ làm việc tại Trung tâm dữ liệu quốc gia được hưởng phụ cấp 500.000 đồng/ngày từ nguồn thu phí khai thác dữ liệu và có cơ chế thu hút nhân lực chất lượng cao. Đây là những điều kiện quan trọng để vận hành một hạ tầng lớn.

Tóm lại, Khoản 2 giao cho Trung tâm dữ liệu quốc gia trách nhiệm vận hành tốt “phần cứng” và “phần mềm nền tảng” của trung tâm, bao gồm đảm bảo Trung tâm dữ liệu quốc gia hoạt động 24/7 ổn định, an toàn, cũng như xây dựng các nền tảng tích hợp, cổng dữ liệu phục vụ chia sẻ. Đồng thời, trung tâm phải mở dịch vụ hạ tầng hỗ trợ các cơ quan khác, hướng tới một môi trường CNTT tập trung hóa. Nhiệm vụ này bổ trợ chặt chẽ cho Khoản 1: có hạ tầng mạnh thì mới tích hợp được nhiều dữ liệu, phân tích dữ liệu hiệu quả.

#### ***6.2.3. Tổ chức vận hành, quản trị, lưu trữ, quản lý, khai thác, điều phối dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia cho các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội để thực hiện chức năng, nhiệm vụ hoặc theo yêu cầu của chủ sở hữu dữ liệu, chủ quản dữ liệu, chủ thể dữ liệu phù hợp với quy định của pháp luật***

Khoản 3 Điều 31 quy định Trung tâm dữ liệu quốc gia có vai trò như đơn vị điều phối và phục vụ khai thác dữ liệu quốc gia: “*Tổ chức vận hành, quản trị, lưu trữ, quản lý, khai thác, điều phối dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia cho các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội để thực hiện chức năng, nhiệm vụ được giao hoặc theo yêu*



cầu của chủ sở hữu dữ liệu, chủ quản dữ liệu, chủ thẻ dữ liệu phù hợp với quy định của pháp luật.”

Nội dung có thể tóm lược là Trung tâm dữ liệu quốc gia có trách nhiệm vận hành và điều phối việc sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia để phục vụ các cơ quan nhà nước, đoàn thể thực hiện nhiệm vụ; đồng thời cung ứng dữ liệu theo yêu cầu của các bên có quyền liên quan (*chủ sở hữu, chủ quản, chủ thẻ dữ liệu*).

Nói cách khác, sau khi đã tích hợp và quản trị được kho dữ liệu tập trung (*khoản 1*), Trung tâm dữ liệu quốc gia phải đảm bảo dữ liệu đó được khai thác, chia sẻ thông suốt đến những người cần dùng, theo đúng thẩm quyền và quy định pháp luật, cụ thể:

- **Một là**, điều phối và cung cấp dữ liệu cho cơ quan nhà nước thực hiện chức năng, nhiệm vụ: Trung tâm dữ liệu quốc gia đóng vai trò đầu mối cung ứng dữ liệu liên ngành. Các cơ quan Đảng, Chính phủ, đoàn thể muốn khai thác dữ liệu dùng chung cho công việc của mình sẽ thông qua Trung tâm dữ liệu quốc gia. Thay vì mỗi cơ quan phải kết nối riêng rẽ tới từng cơ sở dữ liệu của cơ quan khác, giờ đây họ chỉ cần kết nối đến Trung tâm dữ liệu quốc gia - trung tâm sẽ điều phối dữ liệu từ kho tổng hợp đến cho cơ quan yêu cầu. Điều này như phân tích ở trên, giúp giảm rất nhiều kết nối và tăng hiệu quả chia sẻ dữ liệu. Ví dụ: một tỉnh muốn tra cứu thông tin dân cư, doanh nghiệp, đất đai... để giải quyết thủ tục hành chính, thay vì gọi đến từng bộ quản lý dữ liệu tương ứng, thì qua Trung tâm dữ liệu quốc gia có thể nhận thông tin tổng hợp nhanh chóng.

Trung tâm dữ liệu quốc gia được giao quản trị và lưu trữ dữ liệu trong quá trình phục vụ khai thác, nghĩa là trung tâm phải có các hệ thống quản lý truy cập, cấp quyền, theo dõi log để đảm bảo đúng đối tượng, đúng mục đích. Các cơ quan khai thác dữ liệu qua Trung tâm dữ liệu quốc gia sẽ được cấp tài khoản truy cập để tra cứu thông tin trong Cơ sở dữ liệu tổng hợp Quốc gia. Dữ liệu lấy ra có giá trị pháp lý như dữ liệu gốc và có thể được sử dụng trực tiếp trong xử lý công việc hành chính. Điều này đã được quy định chi tiết tại Nghị định 165/2025/NĐ-CP:



Trung tâm dữ liệu quốc gia cấp tài khoản cho cơ quan, tổ chức; cơ quan sử dụng có trách nhiệm quản lý tài khoản và phân quyền cho cá nhân trực thuộc; cá nhân được phân quyền có thể tra cứu thông tin công dân trong Cơ sở dữ liệu tổng hợp Quốc gia qua hệ thống của cơ quan mình; kết quả khai thác được lưu trữ tại hệ thống của cơ quan và Trung tâm dữ liệu quốc gia kiểm tra, xác thực thông tin tài khoản, trả kết quả theo đúng quyền hạn của tài khoản đó. Quy trình này cho thấy Trung tâm dữ liệu quốc gia như một “công dịch vụ dữ liệu” phục vụ các cơ quan hành chính một cách có kiểm soát.

Lợi ích rõ rệt của việc điều phối tập trung được chính sách nêu ra “Thay vì hệ thống của một bộ, ngành, địa phương phải kết nối với các hệ thống của các bộ, ngành khác và các địa phương thì chỉ cần kết nối với Trung tâm dữ liệu quốc gia... xử lý dữ liệu khi giải quyết thủ tục hành chính sẽ nhanh hơn”. Không chỉ vậy, dữ liệu đồng bộ qua Trung tâm dữ liệu quốc gia còn giúp “cắt giảm giấy tờ, tài liệu trong thủ tục hành chính”, bởi nếu thông tin đã có trong Cơ sở dữ liệu tổng hợp Quốc gia thì công dân không phải xuất trình giấy tờ mà cán bộ có thể tra cứu trên hệ thống, quy trình giải quyết TTHC được đơn giản hóa (*không phải khai nhiều thông tin như trước*). Đây chính là hiệu quả mà Khoản 3 hướng đến: phục vụ tốt hơn người dân, doanh nghiệp nhờ chia sẻ dữ liệu liên thông.

- **Hai là**, cung cấp dữ liệu theo yêu cầu của chủ sở hữu, chủ quản, chủ thẻ dữ liệu: Đây là điểm rất mới và tiến bộ. Các khái niệm này được luật giải thích "*Chủ thẻ dữ liệu là cơ quan, tổ chức, cá nhân được dữ liệu phản ánh; Chủ quản dữ liệu là đơn vị thực hiện xây dựng, quản lý, vận hành dữ liệu theo yêu cầu của chủ sở hữu; Chủ sở hữu dữ liệu là đơn vị/cá nhân có quyền quyết định việc xây dựng, phát triển, sử dụng dữ liệu*". Hiểu đơn giản, chủ sở hữu dữ liệu thường là cơ quan, cá nhân tạo ra dữ liệu (ví dụ Bộ GD&ĐT sở hữu dữ liệu văn bằng, một doanh nghiệp sở hữu dữ liệu do mình thu thập, cá nhân sở hữu dữ liệu cá nhân của họ theo luật dân sự); chủ quản dữ liệu là nơi được giao vận hành dữ liệu (ví dụ Cục CNTT của Bộ GD&ĐT là chủ quản dữ liệu văn bằng); chủ thẻ dữ liệu là người mà dữ liệu nói về (ví dụ sinh viên là chủ thẻ của dữ liệu văn bằng về họ).



Khoản 3 cho phép các chủ sở hữu, chủ quản, chủ thẻ dữ liệu có thể yêu cầu Trung tâm dữ liệu quốc gia cung cấp dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia liên quan đến họ, miễn là phù hợp quy định pháp luật. Điều này rất quan trọng trong thực thi quyền dữ liệu cá nhân và quyền tài sản dữ liệu. Ví dụ: một công dân (*chủ thẻ dữ liệu*) có quyền yêu cầu Trung tâm dữ liệu quốc gia cung cấp cho mình các dữ liệu về bản thân trong Cơ sở dữ liệu tổng hợp Quốc gia (*trong phạm vi được phép*) đây là cách thức để cá nhân tiếp cận dữ liệu cá nhân của họ, góp phần minh bạch dữ liệu. Hoặc một bộ/ngành (*chủ sở hữu dữ liệu*) có thể yêu cầu Trung tâm dữ liệu quốc gia khai thác tập dữ liệu do mình sở hữu cho một mục đích nào đó. Trung tâm dữ liệu quốc gia sẽ phải đáp ứng các yêu cầu chính đáng này. Quy định này có nghĩa Trung tâm dữ liệu quốc gia là một cổng truy cập tập trung không chỉ cho cơ quan nhà nước mà cho toàn xã hội (*trong chừng mực luật cho phép*), hướng tới tương lai có thể người dân, doanh nghiệp cũng khai thác được dữ liệu qua các dịch vụ do Trung tâm dữ liệu quốc gia cung cấp (ví dụ *Cổng dữ liệu mở quốc gia do Trung tâm dữ liệu quốc gia quản lý*).

Hiện nay, Nghị định 165/2025/NĐ-CP đã cụ thể hóa một phần: các cơ quan, tổ chức, cá nhân có thể yêu cầu khai thác dữ liệu bằng văn bản gửi Trung tâm dữ liệu quốc gia; trong 3 ngày làm việc người có thẩm quyền sẽ xét duyệt và trả kết quả hoặc từ chối nếu rõ lý do. Quy trình này tạo điều kiện cho những trường hợp khai thác đơn lẻ hoặc không có kết nối điện tử, ví dụ một người dân có thể gửi văn bản yêu cầu trích xuất dữ liệu của mình trong Cơ sở dữ liệu tổng hợp Quốc gia.

Bên cạnh đó, Trung tâm dữ liệu quốc gia cũng được giao nhiệm vụ điều phối dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia. “Điều phối dữ liệu” được định nghĩa là hoạt động tổ chức điều động, phân phối dữ liệu, quản lý, giám sát, tối ưu luồng dữ liệu chia sẻ giữa các hệ thống. Như vậy Trung tâm dữ liệu quốc gia phải đảm bảo dòng chảy dữ liệu từ Cơ sở dữ liệu tổng hợp Quốc gia đến các nơi được thông suốt, hiệu quả. Điều này đòi hỏi xây dựng các thỏa thuận kết nối, chia sẻ dữ liệu giữa Trung tâm dữ liệu quốc gia với các cơ quan quản lý cơ sở dữ liệu khác, quy định rõ mục đích chia sẻ, phạm vi dữ liệu, phương thức kết nối,...



Đồng thời, Trung tâm dữ liệu quốc gia hướng dẫn các đơn vị tuân thủ chuẩn kĩ thuật khi kết nối chia sẻ và điều phối dung lượng, băng thông, lịch trình đồng bộ để tránh tắc nghẽn hay xung đột khi nhiều dữ liệu luân chuyển.

Có thể thấy Khoản 3 nhấn mạnh vai trò “dịch vụ dữ liệu công” của Trung tâm dữ liệu quốc gia. Trung tâm không chỉ giữ dữ liệu mà còn phục vụ tích cực cho các đối tượng thụ hưởng dữ liệu (*cơ quan nhà nước làm dịch vụ công và cả người dân, tổ chức có liên quan*). Điều này đặt Trung tâm dữ liệu quốc gia ở vị trí rất trung tâm trong hệ sinh thái dữ liệu quốc gia, mọi luồng trao đổi dữ liệu quan trọng đều đi qua Trung tâm dữ liệu quốc gia.

Thực tế trong việc giải quyết thủ tục hành chính liên thông, giả sử công dân nộp hồ sơ xin trợ cấp xã hội. Cán bộ một cửa có thể thông qua hệ thống kết nối với Trung tâm dữ liệu quốc gia để tra cứu ngay thông tin dân cư (*đối tượng bảo trợ*), thông tin hộ nghèo (*Bộ Nội vụ*), thông tin nhân thân (*Bộ Công an*) tất cả tại một điểm thay vì yêu cầu người dân cung cấp giấy tờ tương ứng. Điều này khả thi khi Trung tâm dữ liệu quốc gia đã điều phối cho các Cơ sở dữ liệu dân cư, an sinh xã hội,... tích hợp và cùng chia sẻ qua nền tảng dữ liệu quốc gia. Kết quả là tiết kiệm thời gian, công sức cho cả người dân và chính quyền, nâng cao hiệu quả quản lý.

Tóm lại, Khoản 3 trao cho Trung tâm dữ liệu quốc gia vai trò của “bà đỡ dữ liệu” tổ chức và vận hành việc chia sẻ, khai thác dữ liệu liên thông cho bộ máy nhà nước cũng như cung cấp dữ liệu cho các chủ thể có quyền. Nhiệm vụ này hiện thực hóa mục tiêu “kết nối, liên thông dữ liệu quốc gia”, giúp một dữ liệu được nhiều nơi dùng chung, đúng với nguyên tắc “once-only” (*mỗi thông tin chỉ cung cấp một lần*) trong chính phủ điện tử hiện đại.

#### **6.2.4. Giám sát việc bảo đảm chất lượng dữ liệu, hoạt động điều phối dữ liệu; xây dựng các hệ thống chỉ số đo lường và đánh giá hiệu suất cho hoạt động quản trị dữ liệu**

Khoản 4 yêu cầu Trung tâm dữ liệu quốc gia thực hiện các trách nhiệm về đảm bảo chất lượng và đánh giá hiệu quả trong quản trị dữ liệu: “*Giám sát việc*



bảo đảm chất lượng dữ liệu, hoạt động điều phối dữ liệu; xây dựng các hệ thống chỉ số đo lường và đánh giá hiệu suất cho hoạt động quản trị dữ liệu.”

Nội dung này có hai ý chính là <sup>(1)</sup>Giám sát bảo đảm chất lượng dữ liệu và hoạt động điều phối dữ liệu và <sup>(2)</sup>xây dựng hệ thống chỉ số (*metrics*) để đo lường, đánh giá hiệu suất quản trị dữ liệu.

- **Trước hết**, chất lượng dữ liệu là yếu tố sống còn đối với mọi hệ thống dữ liệu. Dữ liệu kém chất lượng (*thiếu chính xác, không cập nhật, không đầy đủ*) sẽ dẫn đến quyết định sai lầm và làm mất niềm tin của người dùng. Luật đã đề cập nguyên tắc bảo đảm tính chính xác, toàn vẹn, tin cậy của dữ liệu. Trung tâm dữ liệu quốc gia, với vai trò quản trị kho dữ liệu tập trung, phải chịu trách nhiệm giám sát việc tuân thủ các tiêu chí chất lượng đối với dữ liệu được đồng bộ về trung tâm. Điều này bao gồm theo dõi việc các cơ quan nguồn có thường xuyên cập nhật dữ liệu hay không, dữ liệu gửi sang có đầy đủ các trường thông tin bắt buộc, có đúng định dạng, tiêu chuẩn kỹ thuật đã quy định hay không,...

Nghị định 165/2025/NĐ-CP đã giao Trung tâm dữ liệu quốc gia thực hiện các biện pháp giám sát, đánh giá chất lượng dữ liệu được chia sẻ, đồng bộ về trung tâm. Trung tâm có quyền (*và trách nhiệm*) kiểm tra, giám sát chất lượng dữ liệu mà các nơi cung cấp. Thực tế, Điều 34 khoản 3 Luật Dữ liệu cũng quy định Trung tâm dữ liệu quốc gia phối hợp với các cơ quan kiểm tra dữ liệu khi thu thập, cập nhật, đồng bộ để bảo đảm tính chính xác, thống nhất; nếu phát hiện dữ liệu trong Cơ sở dữ liệu bộ ngành không thống nhất với dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia, Trung tâm dữ liệu quốc gia sẽ phối hợp kiểm tra, đối soát và cập nhật, đồng bộ lại ở các bên. Như vậy, Trung tâm dữ liệu quốc gia đóng vai trò như một “trọng tài chất lượng”: phát hiện chênh lệch, lỗi dữ liệu giữa các nguồn và yêu cầu chỉnh sửa/đối soát. Ví dụ: nếu dữ liệu dân cư trong Cơ sở dữ liệu tổng hợp Quốc gia (*tổng hợp từ Bộ Công an*) phát hiện khác với dữ liệu dân số mà một tỉnh báo cáo, Trung tâm dữ liệu quốc gia sẽ báo về Bộ Công an và tỉnh đó để kiểm tra, làm rõ, thống nhất số liệu.



Bên cạnh chất lượng dữ liệu, hoạt động điều phối dữ liệu (*tức chia sẻ qua lại*) cũng cần giám sát. Trung tâm dữ liệu quốc gia phải bảo đảm quá trình chia sẻ diễn ra suôn sẻ, an toàn, tránh việc cơ quan A yêu cầu dữ liệu nhưng cơ quan B không cung cấp kịp, hoặc nghẽn đường truyền, hay chia sẻ tràn lan vượt phạm vi. Trung tâm có thể giám sát thông qua các công cụ kỹ thuật (*nhật ký hệ thống, dashboard giám sát lưu lượng, tần suất chia sẻ*) và cả cơ chế báo cáo định kỳ từ các đơn vị.

- *Cùng với đó*, phần thứ hai của khoản 4 quy định hệ thống chỉ số đo lường và đánh giá hiệu suất (*performance metrics*) cho hoạt động quản trị dữ liệu. Đây là một điểm tiến bộ, thể hiện tư duy quản trị bằng kết quả thực hiện. Trung tâm dữ liệu quốc gia được giao xây dựng các bộ chỉ số để định lượng hóa chất lượng và hiệu quả công tác dữ liệu. Những chỉ số này có thể bao gồm: <sup>(1)</sup>Chỉ số về chất lượng dữ liệu: % dữ liệu có đầy đủ thuộc tính, % bản ghi lỗi, độ chính xác qua đối soát, mức độ trùng lặp,... <sup>(2)</sup>Chỉ số về cập nhật: độ trễ của việc đồng bộ dữ liệu từ nguồn đến Cơ sở dữ liệu tổng hợp Quốc gia, tần suất cập nhật (*theo ngày/tuần*), số lượng bản ghi mới cập nhật,... <sup>(3)</sup>Chỉ số về chia sẻ/khai thác: số lượng yêu cầu khai thác được xử lý, thời gian phản hồi trung bình, số cơ quan kết nối liên thông, dung lượng dữ liệu chia sẻ,... <sup>(4)</sup>Chỉ số về an toàn dữ liệu: số sự cố dữ liệu xảy ra, số lần vi phạm chất lượng phát hiện,... <sup>(5)</sup>Chỉ số về hiệu quả kinh tế - xã hội: tỷ lệ thủ tục hành chính liên thông dữ liệu, thời gian tiết kiệm được do dùng Cơ sở dữ liệu tổng hợp Quốc gia, mức độ hài lòng của người dân khi không phải nộp giấy tờ...

Luật không liệt kê cụ thể các chỉ số, nhưng nhiệm vụ “xây dựng hệ thống chỉ số” cho thấy Trung tâm dữ liệu quốc gia phải nghiên cứu và đề xuất. Những chỉ số này giúp đánh giá hiệu suất hoạt động quản trị dữ liệu, hiểu là đánh giá xem công tác quản trị dữ liệu quốc gia (*bao gồm xây dựng, vận hành Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia*) đạt kết quả thế nào. Kết quả đo lường sẽ hỗ trợ cơ quan quản lý (*nhiều Bộ Công an - cơ quan chủ trì, hoặc Chính phủ*) có cơ sở định lượng để đánh giá (ví dụ: nếu tỷ lệ dữ liệu lỗi giảm dần, số cơ sở dữ liệu kết nối tăng, thời gian cung cấp dữ liệu rút ngắn, thì hoạt động quản



trị dữ liệu tiến triển tốt; ngược lại, nếu nhiều chỉ số kém có thể cản chấn chỉnh, đầu tư thêm).

Việc giám sát chất lượng và lượng hóa hiệu quả cũng thúc đẩy tính minh bạch và trách nhiệm giải trình trong quản lý dữ liệu. Các bộ, ngành địa phương biết rằng chất lượng dữ liệu họ cung cấp sẽ bị giám sát và so sánh, từ đó có động lực cải thiện. Chính phủ cũng có căn cứ để tuyên dương hoặc phê bình các đơn vị trong thực hiện chuyển đổi số dữ liệu.

Để thực hiện Khoản 4, Trung tâm dữ liệu quốc gia cần thiết lập một hệ thống giám sát dữ liệu tập trung (*Data Governance Monitoring System*). Nghị định 165/2025/NĐ-CP đã hỗ trợ phần nào khi yêu cầu Trung tâm dữ liệu quốc gia hướng dẫn việc áp dụng tiêu chuẩn dữ liệu và theo dõi chất lượng dữ liệu được đồng bộ. Đây là nền tảng để xây dựng chỉ số. Ngoài ra, trung tâm có thể phối hợp Tổng cục Thống kê hoặc các cơ quan đánh giá để xây dựng những chỉ số phù hợp thông lệ quốc tế.

Tóm lại, Khoản 4 đảm bảo rằng Trung tâm dữ liệu quốc gia không chỉ làm mà còn phải đo đếm, đánh giá được công việc liên quan đến dữ liệu. Chỉ khi đo lường được, chúng ta mới quản lý và cải thiện được (*theo nguyên tắc quản lý hiệu suất*). Điều này đặc biệt quan trọng vì quản trị dữ liệu quốc gia là một lĩnh vực mới, cần liên tục đánh giá rút kinh nghiệm để hoàn thiện. Trách nhiệm này bỗ trợ trực tiếp cho Khoản 1-3, trung tâm vừa triển khai các nghiệp vụ dữ liệu, vừa giám sát chất lượng các nghiệp vụ đó, đảm bảo dữ liệu luôn “sạch” và hệ thống vận hành hiệu quả.

#### **6.2.5. Thực hiện biện pháp bảo vệ dữ liệu**

Khoản 5 quy định nhiệm vụ "*Thực hiện biện pháp bảo vệ dữ liệu*" yêu cầu Trung tâm dữ liệu quốc gia phải thực thi các biện pháp cần thiết để bảo vệ dữ liệu, hiểu bao hàm cả an ninh, an toàn, bảo mật dữ liệu. Trong bối cảnh Trung tâm dữ liệu quốc gia lưu trữ và điều phối một khối lượng dữ liệu khổng lồ, bao gồm dữ liệu cá nhân, dữ liệu quan trọng, cốt lõi của quốc gia, nhiệm vụ bảo vệ dữ liệu là tối quan trọng nhằm ngăn chặn mất mát, rò rỉ, truy cập trái phép hoặc lạm dụng dữ liệu.



Bảo vệ dữ liệu theo Luật Dữ liệu không chỉ giới hạn ở dữ liệu cá nhân, mà là bảo vệ mọi dữ liệu trước các rủi ro. Nguyên tắc của luật là bảo vệ dữ liệu phải được thực hiện đồng bộ, chặt chẽ cùng với xây dựng, phát triển dữ liệu quy định ngay từ khi tạo lập dữ liệu đã phải nghĩ đến bảo vệ. Do đó, Trung tâm dữ liệu quốc gia phải tích hợp các biện pháp bảo mật vào toàn bộ vòng đời xử lý dữ liệu.

Nghị định 165/2025/NĐ-CP đã cụ thể hóa yêu cầu này tại khoản 4, Điều 21 Trung tâm dữ liệu quốc gia phải thực hiện các biện pháp bảo vệ dữ liệu được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu. Cụm từ này nhấn mạnh nguyên lý “Security by Design và by Default” bảo mật dữ liệu được thiết kế sẵn và mặc định ở mọi giai đoạn.

**VGP** Người ký: CÔNG THÔNG TIN ĐIỆN TỬ CHÍNH PHỦ  
Email: thongtinchinhphu@chinhphu.vn  
Cơ quan: VĂN PHÒNG CHÍNH PHỦ  
CHINHPHU.VN Thời gian ký: 03.07.2025 16:52:14 +07:00 *TĐĐT*

**CHÍNH PHỦ** **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  
**Độc lập - Tự do - Hạnh phúc**

Số: 165/2025/NĐ-CP *Hà Nội, ngày 30 tháng 6 năm 2025*

CÔNG THÔNG TIN ĐIỆN TỬ CHÍNH PHỦ
DEN Giờ: C Ngày: 03/07/2025
<b>NGHỊ ĐỊNH</b> <b>Quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu</b>

**Điều 21. Trách nhiệm của Trung tâm dữ liệu quốc gia**

1. Hướng dẫn cơ quan, tổ chức, cá nhân trong việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu thuộc phạm vi đồng bộ về Trung tâm dữ liệu quốc gia.
2. Thực hiện các biện pháp giám sát, đánh giá chất lượng dữ liệu được chia sẻ, đồng bộ về Trung tâm dữ liệu quốc gia.
3. Điều phối dữ liệu của Cơ sở dữ liệu tổng hợp quốc gia.
4. Thực hiện các biện pháp bảo vệ dữ liệu được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu theo quy định tại khoản 6 Điều 16 Nghị định này.

*Điều 16, Nghị định 165/2025/NĐ-CP chỉ có 4 khoản, không có khoản sáu*

**Điều 16. Bảo vệ dữ liệu**

4. Các biện pháp bảo vệ dữ liệu bao gồm:
  - a) Quản lý có liên quan đến xử lý dữ liệu gồm: xây dựng chính sách, quy chế, tiêu chí đánh giá an toàn, an ninh dữ liệu để bảo đảm tuân thủ các tiêu

*Hình ảnh: Văn bản Nghị định 165/2025/NĐ-CP quy định mẫu thuẫn giữa điều 16 và điều 21. Ảnh: Tác giả*



Nội dung quy định tại Khoản 4, Điều 21 Nghị định 165/2025/NĐ-CP hướng dẫn thực hiện theo khoản 6 Điều 16, tuy nhiên thực tế tại Điều 16 không có khoản 6, trong khi khoản 4 quy định các biện pháp bảo vệ dữ liệu, vì vậy có thể hiểu theo khoản 4, điều 16: <sup>(1)</sup>Quản lý có liên quan đến xử lý dữ liệu gồm: xây dựng chính sách, quy chế, tiêu chí đánh giá an toàn, an ninh dữ liệu để bảo đảm tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật, quy định về bảo vệ dữ liệu và các biện pháp quản lý khác theo quy định của pháp luật; <sup>(2)</sup>Biện pháp kỹ thuật có liên quan đến xử lý dữ liệu: bảo đảm an ninh vật lý, kiểm soát truy cập, kiểm tra an ninh mạng và các biện pháp kỹ thuật khác theo quy định của pháp luật; <sup>(3)</sup>Quản lý nhân lực bảo vệ dữ liệu: xây dựng quy chế quản lý con người, đào tạo nhân lực bảo vệ dữ liệu; và các quy định khác.

Ngoài ra, việc thực hiện các biện pháp bảo vệ dữ liệu được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu có thể hiểu là: <sup>(1)</sup>Khi thu thập, tạo lập dữ liệu: xây dựng quy trình thu thập an toàn, đánh giá và áp dụng biện pháp bảo vệ trước khi thu thập; kiểm tra tính xác thực và giám sát chất lượng dữ liệu; <sup>(2)</sup>Khi lưu trữ dữ liệu: xây dựng quy trình lưu trữ (*bao gồm quy trình sao lưu, phục hồi, ghi nhật ký*); thiết lập hệ thống quản lý lưu trữ an toàn, áp dụng công cụ mã hóa, sao lưu tự động; xóa, hủy dữ liệu khi hết hạn hoặc không cần thiết; <sup>(3)</sup>Khi sử dụng, xử lý dữ liệu: xây dựng, triển khai quy chế truy cập, truy xuất dữ liệu tuân thủ nguyên tắc quyền tối thiểu; thiết lập hệ thống kiểm soát truy cập với nhận dạng thống nhất; áp dụng biện pháp kỹ thuật bảo vệ dữ liệu và giám sát truy xuất trong quá trình sử dụng; <sup>(4)</sup>Khi chia sẻ, cung cấp dữ liệu ra bên ngoài: làm rõ phạm vi, mục đích; quy định trách nhiệm bảo mật trong hợp đồng thỏa thuận; đặc biệt nếu ủy thác xử lý dữ liệu cho bên thứ ba thì ràng buộc chặt nghĩa vụ và xác minh năng lực bảo vệ của bên nhận; <sup>(5)</sup>Khi xóa, hủy dữ liệu: xây dựng phương án xóa, hủy, đảm bảo dữ liệu quan trọng, cốt lõi khi hủy không thể khôi phục (*có chứng minh*); <sup>(6)</sup>Quản lý nhân sự bảo vệ dữ liệu: xác định người chịu trách nhiệm bảo vệ dữ liệu, lập bộ phận an toàn dữ liệu; đào tạo, bồi dưỡng nhân sự này.



Mặc dù các nội dung trên chủ yếu áp cho chủ quản dữ liệu (*các bộ ngành quản lý dữ liệu nguồn*), nhưng Trung tâm dữ liệu quốc gia chính là chủ quản Cơ sở dữ liệu tổng hợp Quốc gia, do đó trung tâm cũng phải tuân thủ những yêu cầu tương tự. Nghĩa là, Trung tâm dữ liệu quốc gia phải có quy trình và công cụ bảo vệ dữ liệu đầy đủ ở mọi khâu: từ khi nhận dữ liệu vào (*kiểm soát đầu vào, chống giả mạo*), trong khi lưu trữ (*mã hóa, backup, kiểm soát truy cập nội bộ*), khi chia sẻ ra (*xác thực người nhận, phân quyền chính xác, mã hóa kênh truyền, theo dõi nhật ký*) và khi hủy dữ liệu (*có tiêu chuẩn hủy an toàn*).

Các biện pháp bảo vệ dữ liệu có thể phân thành biện pháp kỹ thuật và biện pháp quản lý. Về kỹ thuật, Trung tâm dữ liệu quốc gia triển khai những công nghệ bảo mật hiện đại bằng hệ thống tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập (*IDS/IPS*), mã hóa dữ liệu khi lưu trữ và truyền tải, quản lý khóa mật mã, sao lưu dự phòng nhiều lớp, kiểm soát truy cập dựa trên vai trò và nguyên tắc bảo mật đặc quyền tối thiểu,... Về quản lý, trung tâm cần có chế nội bộ nghiêm ngặt về ai được quyền truy cập dữ liệu gì, quy trình phê duyệt khi cung cấp dữ liệu cho đơn vị khác, trách nhiệm cá nhân khi vi phạm bảo mật, đồng thời tổ chức kiểm tra đánh giá an ninh thường xuyên (*ví dụ diễn tập an ninh, đánh giá rủi ro hàng năm cho dữ liệu quan trọng*).

Luật Dữ liệu bổ sung rằng dữ liệu cốt lõi, dữ liệu quan trọng cần bảo vệ đặc biệt. Trung tâm dữ liệu quốc gia phải tuân theo các quy định hạn chế chuyển dữ liệu ra nước ngoài đối với loại dữ liệu này, chỉ được chuyển nếu đáp ứng điều kiện và qua đánh giá tác động của Bộ Công an/Bộ Quốc phòng nhằm bảo đảm an ninh quốc gia.

Nhận thức rõ tầm quan trọng, ngay khi luật có hiệu lực, Bộ Công an đã cho ra mắt Phòng An ninh, an toàn hệ thống trực thuộc Trung tâm dữ liệu quốc gia (*tháng 7/2025*). Phòng này có nhiệm vụ xây dựng, tham mưu các văn bản hướng dẫn đảm bảo an ninh, an toàn, bảo mật dữ liệu; xây dựng hành lang pháp lý, cơ chế chính sách thúc đẩy đổi mới sáng tạo nhưng đồng thời bảo đảm an ninh mạng, an toàn dữ liệu trong lĩnh vực dữ liệu. Việc thành lập đơn vị chuyên trách an ninh thuộc Trung tâm



dữ liệu quốc gia là một bước đi cụ thể để thực hiện khoản 5 - tức là có bộ máy tổ chức và con người phụ trách công tác bảo vệ dữ liệu trong trung tâm.

Tóm lại, Khoản 5 cho thấy an toàn dữ liệu là ưu tiên hàng đầu tại Trung tâm dữ liệu quốc gia. Mọi thành quả tích hợp, khai thác dữ liệu có thể tiêu tan nếu xảy ra sự cố rò rỉ hay tấn công mạng nghiêm trọng. Do vậy, trung tâm phải thiết lập hệ thống bảo vệ dữ liệu toàn diện. Thành công của Trung tâm dữ liệu quốc gia không chỉ đo bằng lượng dữ liệu xử lý, mà còn ở việc giữ dữ liệu an toàn, bảo mật, tạo niềm tin cho các cơ quan khi gửi dữ liệu vào và cho người dân khi dữ liệu của họ được quản lý ở đó.

**6.2.6. Nghiên cứu khoa học về dữ liệu, ứng dụng công nghệ trong xử lý dữ liệu, cung cấp hạ tầng công nghệ, sản phẩm, dịch vụ về dữ liệu; hỗ trợ tổ chức, cá nhân trong xử lý dữ liệu; xây dựng trung tâm đổi mới sáng tạo, hỗ trợ đổi mới sáng tạo về khoa học dữ liệu; phát triển hoạt động đổi mới sáng tạo về khoa học dữ liệu; phát triển hệ sinh thái khởi nghiệp đổi mới sáng tạo về khoa học và công nghệ trên nền tảng dữ liệu của Cơ sở dữ liệu tổng hợp Quốc gia.**

Khoản 6 của Điều 31 trao cho Trung tâm dữ liệu quốc gia một loạt trách nhiệm liên quan đến nghiên cứu, ứng dụng công nghệ và thúc đẩy đổi mới sáng tạo dựa trên dữ liệu, cụ thể: “*Nghiên cứu khoa học về dữ liệu, ứng dụng công nghệ trong xử lý dữ liệu, cung cấp hạ tầng công nghệ, sản phẩm, dịch vụ về dữ liệu; hỗ trợ tổ chức, cá nhân trong xử lý dữ liệu; xây dựng trung tâm đổi mới sáng tạo, hỗ trợ đổi mới sáng tạo về khoa học dữ liệu; phát triển hoạt động đổi mới sáng tạo về khoa học dữ liệu; phát triển hệ sinh thái khởi nghiệp đổi mới sáng tạo về khoa học và công nghệ trên nền tảng dữ liệu của Cơ sở dữ liệu tổng hợp Quốc gia.*”

Quy định này có thể nhóm lại thành các nhiệm vụ chính sau:

- **Một là**, nghiên cứu khoa học về dữ liệu, ứng dụng công nghệ trong xử lý dữ liệu: Trung tâm dữ liệu quốc gia phải tiến hành hoặc hỗ trợ các nghiên cứu khoa học nhằm nâng cao khả năng quản trị và khai thác dữ liệu. Đồng thời, trung tâm cần ứng dụng các công nghệ mới (*AI, machine learning, big data analytics*,



*cloud computing, blockchain,...)* vào quy trình xử lý dữ liệu. Điều này đảm bảo Trung tâm dữ liệu quốc gia luôn tiên phong về công nghệ dữ liệu, không lạc hậu.

- **Hai là**, cung cấp hạ tầng công nghệ, sản phẩm, dịch vụ về dữ liệu: Bên cạnh việc cung cấp hạ tầng, Trung tâm dữ liệu quốc gia còn có thể phát triển các sản phẩm, dịch vụ dữ liệu để phục vụ cơ quan nhà nước và xã hội. Ví dụ: dịch vụ phân tích dữ liệu theo yêu cầu, các bộ dữ liệu mẫu (*data set*) cho nghiên cứu, các API dữ liệu mở cho doanh nghiệp khởi nghiệp... Trung tâm có thể trở thành nhà cung cấp dịch vụ dữ liệu công.

- **Ba là**, hỗ trợ tổ chức, cá nhân trong xử lý dữ liệu: Nhiệm vụ này mang tính phục vụ: Trung tâm dữ liệu quốc gia không chỉ làm cho các cơ quan nhà nước, mà còn hỗ trợ các tổ chức, cá nhân bên ngoài (*trong khả năng cho phép*) về kỹ thuật xử lý dữ liệu. Ví dụ: hỗ trợ doanh nghiệp nhỏ về hạ tầng tính toán dữ liệu, tư vấn địa phương trong việc làm sạch dữ liệu,...

- **Bốn là**, xây dựng trung tâm đổi mới sáng tạo về khoa học dữ liệu, hỗ trợ đổi mới sáng tạo về khoa học dữ liệu: Trung tâm dữ liệu quốc gia được giao lập ra các trung tâm đổi mới sáng tạo chuyên về dữ liệu. Đây có thể là đơn vị con hoặc vườn ươm trực thuộc Trung tâm dữ liệu quốc gia, với nhiệm vụ nghiên cứu phát triển các giải pháp, công nghệ dữ liệu lõi, cũng như ươm tạo các sáng kiến công nghệ. Thực tế, Bộ Công an đã ra mắt Trung tâm Sáng tạo, khai thác dữ liệu thuộc Trung tâm dữ liệu quốc gia. Trung tâm này được định vị là đơn vị dẫn dắt đổi mới sáng tạo trong lĩnh vực dữ liệu, thúc đẩy khai thác, ứng dụng và chuyển hóa dữ liệu thành giá trị phục vụ quản trị và phát triển kinh tế-xã hội. Đồng thời, nó còn có vai trò thúc đẩy nghiên cứu, phát triển và ứng dụng các sản phẩm công nghệ dữ liệu lõi, ươm tạo các sáng kiến công nghệ chiến lược.

- **Năm là**, phát triển hoạt động đổi mới sáng tạo về khoa học dữ liệu; phát triển hệ sinh thái khởi nghiệp đổi mới sáng tạo về Khoa học và Công nghệ trên nền tảng dữ liệu của Cơ sở dữ liệu tổng hợp Quốc gia: Hai yếu tố này nhấn mạnh đến việc nuôi dưỡng một hệ sinh thái đổi mới sáng tạo, khởi nghiệp dựa trên dữ liệu. Trung tâm dữ liệu quốc gia cần tạo môi trường và điều kiện để các hoạt động đổi



mới sáng tạo về dữ liệu nở rộ, có thể thông qua các cuộc thi, hackathon về dữ liệu, chương trình tăng tốc khởi nghiệp sử dụng dữ liệu mở, hoặc thiết lập quỹ hỗ trợ khởi nghiệp dữ liệu. Luật Dữ liệu thậm chí còn quy định thành lập Quỹ Phát triển Dữ liệu Quốc gia nhằm huy động nguồn lực xã hội hỗ trợ xây dựng, phát triển dữ liệu và nghiên cứu ứng dụng công nghệ cao liên quan đến dữ liệu. Điều này hỗ trợ trực tiếp cho nhiệm vụ của Trung tâm dữ liệu quốc gia ở khoản 6, vì quỹ có thể tài trợ cho các dự án đổi mới sáng tạo do Trung tâm dữ liệu quốc gia ươm tạo hoặc đề xuất.



Hình ảnh: Cuộc thi Hackathon Data For Life 2025 do Bộ Công an tổ chức.

Ảnh: Trung tâm Dữ liệu quốc gia về dân cư

Tóm lại, Khoản 6 định vị Trung tâm dữ liệu quốc gia như một trung tâm đổi mới sáng tạo dữ liệu quốc gia. Đây là bước tiến mang tính chiến lược: tận dụng kho dữ liệu tập trung và năng lực hạ tầng của Trung tâm dữ liệu quốc gia để phát triển khoa học dữ liệu trong nước, xây dựng các giải pháp Make in Vietnam phục vụ chuyển đổi số. Đồng thời, nó cho thấy quyết tâm của Việt Nam trong việc tạo dựng một hệ sinh thái dữ liệu sôi động, kết nối khu vực công - tư - viện trường, biến dữ liệu thành động lực tăng trưởng kinh tế.



### 6.2.7. Tổ chức thực hiện các nội dung hợp tác quốc tế về dữ liệu

Khoản 7 Điều 31 quy định “*Tổ chức thực hiện các nội dung hợp tác quốc tế về dữ liệu*” đặt ra vai trò đối ngoại cho Trung tâm dữ liệu quốc gia trong lĩnh vực dữ liệu. Cụ thể, Trung tâm dữ liệu quốc gia được giao tổ chức thực hiện các hoạt động hợp tác quốc tế liên quan đến dữ liệu. Trong bối cảnh hiện nay, hợp tác quốc tế về dữ liệu có thể bao gồm nhiều nội dung:

- Trao đổi, học tập kinh nghiệm về xây dựng trung tâm dữ liệu, quản trị dữ liệu số từ các quốc gia tiên tiến. Ví dụ: hợp tác với Singapore về chính phủ số, với Liên minh Châu Âu về khung pháp lý dữ liệu, với Estonia về mô hình chia sẻ dữ liệu X-Road,...
- Tham gia các diễn đàn, sáng kiến quốc tế: như Diễn đàn Quản trị Dữ liệu Toàn cầu, các chương trình của ASEAN về dữ liệu (*ASEAN Data Management Framework*), Diễn đàn chuyển đổi số,... Trung tâm dữ liệu quốc gia có thể được cử làm đại diện Việt Nam hoặc hỗ trợ Bộ Công an (*cơ quan quản lý nhà nước về dữ liệu*) tham dự các diễn đàn này, đóng góp tiếng nói và tiếp thu kiến thức.
- Hợp tác nghiên cứu khoa học: Có thể phối hợp với các tổ chức quốc tế, viện nghiên cứu nước ngoài để thực hiện các dự án nghiên cứu về dữ liệu (ví dụ ứng dụng AI trong quản trị dữ liệu, tiêu chuẩn dữ liệu mở...).
- Hợp tác về chuyển giao công nghệ dữ liệu: Trung tâm dữ liệu quốc gia có thể ký kết với các tập đoàn công nghệ lớn (*Google, Microsoft, Oracle...*) để nhận chuyển giao hoặc dùng thử các công nghệ quản trị dữ liệu mới, hoặc hợp tác phát triển giải pháp phù hợp cho Việt Nam.
- Đào tạo, nâng cao năng lực: Gửi cán bộ đi đào tạo ở nước ngoài về khoa học dữ liệu, an ninh dữ liệu; hoặc mời chuyên gia quốc tế sang tập huấn. Khoản 7 cho phép Trung tâm dữ liệu quốc gia thực hiện các thỏa thuận này.

Nghị định 165/2025/NĐ-CP đã cụ thể hóa khá rõ trong Điều 21 khoản 5: Trung tâm dữ liệu quốc gia thực hiện ký kết các thỏa thuận, biên bản ghi nhớ với các cơ quan, tổ chức quốc tế nhằm thúc đẩy hợp tác quốc tế trong quản lý, bảo vệ dữ liệu, nghiên cứu khoa học, chuyển giao dữ liệu xuyên biên giới, đào tạo, nâng



cao năng lực,..., hướng đến thúc đẩy hoạt động đổi mới sáng tạo, chuyển giao công nghệ phục vụ phát triển kinh tế xã hội. Như vậy, trung tâm có thể chủ động thiết lập các mối quan hệ hợp tác với đối tác quốc tế trong các lĩnh vực:

- Quản lý, bảo vệ dữ liệu: hợp tác trao đổi chính sách, luật pháp về bảo vệ dữ liệu (*ví dụ học hỏi GDPR của Liên minh Châu Âu, Đạo luật dữ liệu của nước khác*), hoặc hợp tác xây dựng cơ chế bảo vệ dữ liệu khi chia sẻ xuyên biên giới.

- Chuyển giao dữ liệu xuyên biên giới: Thế giới đang rất quan tâm việc chuyển dữ liệu qua biên giới (*cross-border data transfer*), do liên quan chủ quyền dữ liệu và bảo mật. Việc hợp tác giúp Việt Nam đảm bảo dữ liệu cốt lõi không bị chuyển giao bừa bãi nhưng vẫn tham gia được luồng dữ liệu toàn cầu. Có thể thông qua đàm phán các thỏa thuận song phương hoặc đa phương về trao đổi dữ liệu có bảo hộ.

- Đào tạo, nâng cao năng lực: ví dụ hợp tác với Nhật, Hàn để đào tạo chuyên gia phân tích dữ liệu; tham gia các khóa của Ngân hàng Thế giới, Liên Hợp Quốc về quản trị dữ liệu.

- Đổi mới sáng tạo và chuyển giao công nghệ: tìm kiếm các cơ hội nhận chuyển giao công nghệ dữ liệu tiên tiến. Ví dụ: hợp tác với doanh nghiệp Israel về công nghệ big data cho nông nghiệp, với Mỹ về công nghệ cloud bảo mật cao,...

Có thể nói, khoản 7 giúp gắn kết nỗ lực của Trung tâm dữ liệu quốc gia với cộng đồng quốc tế, đảm bảo Việt Nam đi cùng nhịp với xu hướng toàn cầu về quản trị dữ liệu. Dữ liệu là phạm vi mới, nhiều nước cũng đang thử nghiệm chính sách; hợp tác quốc tế sẽ giúp tránh được sai lầm, học được cách làm hay. Đồng thời, việc này cũng có ý nghĩa ngoại giao số: Việt Nam thể hiện trách nhiệm trong dòng chảy dữ liệu toàn cầu, nhất là đối với dữ liệu xuyên biên giới. Như luật đã nêu, nhiều nước (*Trung Quốc, Mỹ, Nga*) có quy định kiểm soát dữ liệu quan trọng ra nước ngoài, Việt Nam cũng đang xây dựng chính sách tương tự. Hợp tác quốc tế sẽ giúp tránh xung đột giữa các quy định, tìm điểm chung để dữ liệu được chia sẻ phục vụ kinh tế nhưng vẫn bảo đảm chủ quyền.



Trung tâm dữ liệu quốc gia có thể phối hợp chặt với Bộ Khoa học và Công nghệ trong mảng này, vì Bộ Khoa học và Công nghệ cũng làm nhiều việc về hợp tác chính phủ điện tử quốc tế, dữ liệu mở,... Vai trò của trung tâm có thể thiên về kỹ thuật và triển khai. Ví dụ: nếu Việt Nam tham gia sáng kiến Data Free Flow with Trust (DFFT) của G20, Trung tâm dữ liệu quốc gia có thể là đầu mối kỹ thuật thực hiện cam kết.



Hình ảnh: Hội thảo khu vực Đông Á về Trung tâm dữ liệu quốc gia ngày 14/8/2025. Ảnh: Bộ KH&CN

Nhìn chung, hợp tác quốc tế là một phần không thể thiếu để Trung tâm dữ liệu quốc gia phát triển bền vững. Những lĩnh vực chuyên môn cao như an toàn dữ liệu, phân tích dữ liệu lớn sẽ được nâng tầm qua hợp tác. Và ngược lại, Việt Nam cũng có thể chia sẻ kinh nghiệm triển khai Trung tâm dữ liệu quốc gia (*mô hình tập trung dữ liệu*) cho các nước quan tâm. Khoản 7 tuy ngắn gọn nhưng mở ra cánh cửa hội nhập cho hoạt động của Trung tâm dữ liệu quốc gia.



### 6.2.8. Các trách nhiệm khác do Chính phủ quy định

Khoản 8 xác định rằng “Chính phủ quy định chi tiết Điều này”. Đây là điều khoản giao quyền hướng dẫn chi tiết cho Chính phủ, thường thấy ở cuối các điều luật quan trọng. Nó có nghĩa là các nội dung từ khoản 1 đến 7 Điều 31 sẽ được Chính phủ cụ thể hóa thêm qua các văn bản dưới luật (*Nghị định, Quyết định*).

Thực tế, sau khi Luật Dữ liệu được thông qua, Chính phủ đã ban hành Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 để quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu. Nghị định 165/2025/NĐ-CP dành một chương (*Chương IV*) quy định cụ thể về Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia. Từ việc giao Bộ Công an chủ trì Trung tâm dữ liệu quốc gia, quy định Trung tâm dữ liệu quốc gia cung cấp những dịch vụ gì, đến các trách nhiệm hướng dẫn tiêu chuẩn, giám sát chất lượng, bảo vệ dữ liệu, hợp tác quốc tế... Tất cả đều nhằm chi tiết hóa các khoản 1-7.

Như vậy, Khoản 8 tạo cơ sở pháp lý để nội luật hóa đầy đủ vai trò của Trung tâm dữ liệu quốc gia. Điều 31 trong luật là khung định hướng, còn chi tiết thực hiện (*ai làm, làm thế nào, bao giờ làm...*) do Chính phủ hướng dẫn. Với cơ chế này, khi cần thiết, Chính phủ có thể sửa đổi, bổ sung hướng dẫn một cách linh hoạt mà không phải chờ sửa luật, nhằm đáp ứng thực tiễn triển khai.

Tóm lại, Khoản 8 mang tính thủ tục, nhưng rất quan trọng, bảo đảm tính khả thi của Điều 31 thông qua văn bản dưới luật. Đến nay, Nghị định 165/2025/NĐ-CP đã được ban hành kịp thời đúng khi Luật có hiệu lực (1/7/2025), là cơ sở để Trung tâm dữ liệu quốc gia chính thức đi vào hoạt động. Trong tương lai, có thể sẽ có thêm Thông tư hướng dẫn của Bộ Công an hoặc văn bản liên tịch để làm rõ hơn một số nghiệp vụ (ví dụ tiêu chuẩn kỹ thuật, quy trình kết nối cơ sở dữ liệu). Nhờ Khoản 8, hệ thống văn bản pháp quy về Trung tâm dữ liệu quốc gia sẽ đầy đủ, đồng bộ.



## KẾT LUẬN

Điều 31 Luật Dữ liệu 2024 đã xác lập một cách toàn diện vai trò, chức năng của Trung tâm dữ liệu quốc gia là một thiết chế mới, trọng yếu trong chiến lược chuyển đổi số và quản trị dữ liệu tại Việt Nam. Qua phân tích chi tiết từng khoản, chúng ta thấy Trung tâm dữ liệu quốc gia được giao thực hiện một sứ mệnh kép: <sup>(1)</sup>Vận hành hạ tầng và kho dữ liệu tập trung phục vụ hiệu quả cho Chính phủ, người dân, doanh nghiệp; <sup>(2)</sup>Đồng thời thúc đẩy hệ sinh thái dữ liệu phát triển sáng tạo, an toàn và hội nhập.

Cụ thể, Trung tâm dữ liệu quốc gia vừa là “người quản kho” dữ liệu quốc gia (*tích hợp, lưu trữ, quản trị dữ liệu cho cả nước*), vừa là “người phân phối” (*điều phối chia sẻ dữ liệu liên thông phục vụ mọi ngành*), vừa đóng vai “người gác cổng” (*giám sát chất lượng, bảo vệ dữ liệu khỏi rủi ro*), kiêm “nhà công nghệ” (*nghiên cứu, áp dụng công nghệ mới về dữ liệu*), “nhà ươm tạo” (*hỗ trợ đổi mới sáng tạo, khởi nghiệp dữ liệu*) và “đại sứ” về dữ liệu trên trường quốc tế. Tất cả các vai trò ấy gộp lại làm nên hình ảnh một Trung tâm dữ liệu quốc gia đa năng, giữ vị trí trung tâm trong kiến trúc dữ liệu quốc gia.

So sánh với thế giới, mô hình Trung tâm dữ liệu quốc gia của Việt Nam mang tính tích hợp cao, không chỉ lo kỹ thuật mà còn có chức năng thúc đẩy đổi mới và phối hợp quốc tế. Điều này nếu triển khai tốt sẽ đưa Việt Nam tiệm cận các nước tiên tiến trong quản trị dữ liệu, tạo nền tảng vững chắc cho chính phủ số và kinh tế số. Những bước đi đầu tiên (*ban hành Nghị định 165/2025/NĐ-CP, thành lập các đơn vị chuyên trách thuộc Trung tâm dữ liệu quốc gia, ra mắt một số nền tảng dữ liệu*) cho thấy triển vọng tích cực.

Tuy nhiên, để Trung tâm dữ liệu quốc gia thực sự phát huy hết tiềm năng và hoàn thành tốt các trọng trách được giao, cần lưu ý một số vấn đề và giải pháp sau:

- **Thứ nhất**, hoàn thiện khung pháp lý chi tiết và đồng bộ: Mặc dù đã có Nghị định 165/2025, song cần tiếp tục rà soát, ban hành các văn bản hướng dẫn dưới nghị định (*Thông tư liên tịch, quy chế vận hành*) để làm rõ quy trình phối



hợp giữa Trung tâm dữ liệu quốc gia với các bộ, ngành, địa phương. Ví dụ: quy trình chuẩn để một bộ chuyển dữ liệu lên Trung tâm dữ liệu quốc gia; quy định về phí khai thác dữ liệu (*luật có đे cập phí khai thác Cơ sở dữ liệu tổng hợp Quốc gia, cần có Thông tư Bộ Tài chính hướng dẫn*). Sự rõ ràng về pháp lý giúp tránh lúng túng và thúc đẩy các đơn vị tích cực tham gia kết nối dữ liệu.

- **Thứ hai**, bảo đảm nguồn lực đầu tư bền vững: Điều 32 Luật Dữ liệu đã nêu Nhà nước ưu tiên ngân sách, đất đai, cơ sở vật chất cho Trung tâm dữ liệu quốc gia. Kiến nghị cụ thể hóa bằng đề án đầu tư công trung hạn cho Trung tâm dữ liệu quốc gia (*giai đoạn 2025-2030*), với danh mục dự án xây dựng mở rộng trung tâm dữ liệu, mua sắm thiết bị bảo mật,... Đồng thời, triển khai nhanh cơ chế đổi ngô nhân lực (*luật cho phép thu hút nhân tài, trả lương cao*) - có thể học hỏi mô hình Singapore tuyển chuyên gia an ninh mạng quốc tế cho GovTech. Nhân lực chất lượng cao đảm bảo vận hành an toàn một hạ tầng quan trọng như Trung tâm dữ liệu quốc gia.

- **Thứ ba**, đẩy mạnh phối hợp liên ngành, xóa bỏ rào cản cát cứ dữ liệu: Sự thành công của Trung tâm dữ liệu quốc gia phụ thuộc nhiều vào việc các bộ, ngành, địa phương chủ động đồng bộ dữ liệu về. Do tâm lý “sở hữu dữ liệu”, có nơi có thể chưa sẵn sàng chia sẻ. Cần có chỉ đạo quyết liệt từ Chính phủ, Thủ tướng (*qua các Nghị quyết chuyển đổi số, qua việc đưa tiêu chí chia sẻ dữ liệu vào đánh giá thi đua bộ ngành*). Văn phòng Chính phủ và Bộ Công an nên phối hợp tổ chức các cuộc họp liên ngành định kỳ tháo gỡ khó khăn trong kết nối dữ liệu, đảm bảo lộ trình thu thập, đồng bộ dữ liệu vào Cơ sở dữ liệu tổng hợp Quốc gia mà Thủ tướng sẽ ban hành được thực hiện đúng tiến độ.

- **Thứ tư**, nâng cao nhận thức và kỹ năng về quản trị dữ liệu trong cơ quan nhà nước: Trung tâm dữ liệu quốc gia tuy vận hành tập trung nhưng thành bại cũng do cách các đơn vị nguồn và đơn vị khai thác sử dụng dữ liệu. Cần tổ chức các chương trình đào tạo ngắn hạn cho cán bộ tại các bộ, tỉnh về tiêu chuẩn dữ liệu, về an ninh dữ liệu khi kết nối với Trung tâm dữ liệu quốc gia. Bộ Công an có thể phối hợp Bộ Khoa học và Công nghệ phát hành cảm nang hướng dẫn kết



nối, chia sẻ dữ liệu cho các cơ quan, đơn vị cơ sở. Khi mọi người cùng hiểu và có kỹ năng, dữ liệu đưa vào sẽ sạch hơn (*giảm gánh nặng cho Trung tâm dữ liệu quốc gia*) và việc khai thác cũng hiệu quả hơn.

- **Thứ năm**, phát triển các công cụ hỗ trợ giám sát chất lượng, an ninh một cách tự động: Với khối lượng dữ liệu và giao dịch lớn, Trung tâm dữ liệu quốc gia cần ứng dụng công nghệ AI/ML để giám sát thông minh. Kiến nghị đầu tư phát triển hoặc mua sắm các hệ thống như: Data Quality Management System - tự động kiểm tra phát hiện dữ liệu bất thường, Security Information and Event Management (*SIEM*) tập trung log và phát hiện sớm sự cố an ninh. Những hệ thống này sẽ trở thành “tai mắt” giúp đội ngũ Trung tâm dữ liệu quốc gia quản lý chất lượng (*khoản 4*) và bảo mật (*khoản 5*) liên tục, thay vì thủ công. Cần ưu tiên thực hiện trong 1-2 năm tới, vì ngay khi mới vận hành, trung tâm đã phải xử lý khối dữ liệu khổng lồ (*ví dụ: hàng trăm triệu bản ghi dân cư, hàng tỷ giao dịch thủ tục hành chính*).

- **Thứ sáu**, triển khai hiệu quả Quỹ Phát triển dữ liệu quốc gia: Quỹ này khi thành lập (*theo Luật*) sẽ là nguồn hỗ trợ tài chính cho các dự án đổi mới sáng tạo về dữ liệu. Kiến nghị sớm trình Chính phủ ban hành nghị định riêng về Quỹ (*theo gợi ý tại Điều 44 Luật Dữ liệu*), quy định nguồn vốn (*ngân sách cấp, đóng góp doanh nghiệp dữ liệu*), cơ chế tài trợ. Trung tâm dữ liệu quốc gia nên đóng vai trò đầu mối vận hành Quỹ hoặc tư vấn cho Hội đồng quản lý Quỹ về lĩnh vực ưu tiên đầu tư. Có như vậy, nguồn lực xã hội mới được huy động vào các hoạt động khoa học dữ liệu (*khoản 6*) một cách đúng hướng và gắn kết với định hướng phát triển của Trung tâm dữ liệu quốc gia.

- **Thứ bảy**, thúc đẩy mở dữ liệu và phát triển thị trường dữ liệu: Để tận dụng tối đa giá trị của Cơ sở dữ liệu tổng hợp Quốc gia, Trung tâm dữ liệu quốc gia cần phối hợp các cơ quan để phân loại dữ liệu nào có thể mở công khai hoặc cung cấp theo dịch vụ thương mại. Đề xuất xây dựng Chiến lược dữ liệu mở quốc gia, trong đó giao Trung tâm dữ liệu quốc gia vận hành Công dữ liệu mở tập trung (*như data.gov.vn*). Cung cấp dữ liệu mở sẽ kích thích doanh nghiệp sáng tạo dịch vụ



(khoản 6) và cũng tăng tính minh bạch của Chính phủ (*mục tiêu của Luật*). Song song, cần cơ chế cho phép Trung tâm dữ liệu quốc gia thu phí với dữ liệu giá trị cao cung cấp cho doanh nghiệp (*nhiều dữ liệu phân tích đã xử lý*), nguồn thu này vừa khuyến khích hình thành thị trường dữ liệu vừa tạo thu nhập nuôi chính trung tâm (*theo Luật, Trung tâm dữ liệu quốc gia được dùng nguồn thu phí khai thác dữ liệu để tái đầu tư*). Một thị trường dữ liệu sôi động sẽ chứng minh hiệu quả hoạt động của Trung tâm dữ liệu quốc gia và đóng góp cho GDP kỹ thuật số.

- **Thứ tam**, tăng cường hợp tác quốc tế thực chất: Kiến nghị Bộ Công an/ Trung tâm dữ liệu quốc gia chủ động đề xuất ký kết hợp tác cụ thể, ví dụ với Cơ quan phát triển quốc tế Nhật (*JICA*) về dự án nâng cấp Trung tâm dữ liệu quốc gia an toàn, với Chính phủ Singapore về chia sẻ kinh nghiệm quản lý GovTech. Tham gia tích cực các diễn đàn như ASEAN về Dữ liệu, APEC Digital Economy Steering Group... để vừa học hỏi vừa quảng bá năng lực. Đồng thời, sẵn sàng trao đổi hỗ trợ các nước bạn về kỹ thuật nếu cần (*ví dụ giúp Lào xây dựng trung tâm dữ liệu tương tự quy mô nhỏ hơn*). Qua hợp tác, xây dựng hình ảnh Việt Nam như một quốc gia tiên bộ về quản trị dữ liệu, từ đó thu hút đầu tư công nghệ dữ liệu nước ngoài vào Việt Nam.

- **Thứ chín**, giám sát, đánh giá việc thực thi nhiệm vụ của Trung tâm dữ liệu quốc gia theo hiệu quả: Cuối cùng, cần có cơ chế giám sát độc lập việc thực thi các chức năng Điều 31. Có thể thành lập Ban chỉ đạo về phát triển Trung tâm dữ liệu quốc gia do Phó Thủ tướng đứng đầu, họp mỗi năm để nghe báo cáo kết quả từng nhiệm vụ (*số lượng Cơ sở dữ liệu đã tích hợp, số kết nối liên thông, % dữ liệu sạch, số sự cố an ninh, số dự án nghiên cứu triển khai...*). Áp dụng các chỉ số hiệu suất (khoản 4) đã xây dựng để đánh giá khách quan. Từ đó, Chính phủ kịp thời chỉ đạo điều chỉnh, thưởng phạt phân minh (*ví dụ khen thưởng bộ, tỉnh làm tốt kết nối dữ liệu, phê bình đơn vị trì trệ*). Việc này nhằm đảm bảo mọi nhiệm vụ giao cho Trung tâm dữ liệu quốc gia đều được thực hiện hiệu quả, không hình thức và tạo động lực cải thiện liên tục.



Luật Dữ liệu 2024 với Điều 31 đã vạch ra một tầm nhìn lớn, dữ liệu sẽ trở thành tài sản quốc gia chung, được quản trị tập trung, khai thác an toàn, thúc đẩy đổi mới sáng tạo vì lợi ích chung. Trung tâm dữ liệu quốc gia là công cụ then chốt để biến tầm nhìn đó thành hiện thực. Với quyết tâm chính trị cao, sự phối hợp đồng bộ của các bộ ngành và việc áp dụng các kiến nghị nêu trên, chúng ta tin tưởng rằng Trung tâm dữ liệu quốc gia sẽ hoàn thành xuất sắc sứ mệnh, đưa Việt Nam bước vào kỷ nguyên mới, kỷ nguyên của chính phủ số và kinh tế dữ liệu thịnh vượng.



## PHỤ LỤC

### *Phản bác thông tin sai sự thật về Trung tâm Dữ liệu quốc gia - Bộ Công an*

Trong bối cảnh cách mạng công nghiệp lần thứ tư và chuyển đổi số quốc gia, dữ liệu được xác định là “tư liệu sản xuất chính” và là nguồn lực chiến lược để thúc đẩy phát triển kinh tế - xã hội. Bộ Chính trị đã ban hành nhiều chủ trương quan trọng, như Nghị quyết 57/NQ-TW (22/12/2024), nhấn mạnh “làm giàu, khai thác tối đa tiềm năng của dữ liệu, đưa dữ liệu thành tư liệu sản xuất chính” và yêu cầu “sớm hoàn thành và phát huy hiệu quả Trung tâm Dữ liệu quốc gia”. Tuy nhiên, thời gian qua đã xuất hiện nhiều thông tin sai lệch cho rằng việc xây dựng Trung tâm Dữ liệu quốc gia chỉ nhằm “tập trung hóa dữ liệu”, xâm phạm quyền riêng tư người dân và thiếu minh bạch, thậm chí cho rằng tập trung dữ liệu để bán cho được giá.

*Trang của tổ chức phản động việt tân xuyên tạc tình hình bán dữ liệu ở Việt Nam.Ảnh: Tác giả*

Trung tâm Dữ liệu quốc gia ra đời theo Nghị quyết 175/NQ-CP (30/10/2023) của Chính phủ, giao Bộ Công an thành lập và chịu trách nhiệm xây dựng, quản lý, khai thác. Là đơn vị tương đương cấp Cục thuộc Bộ Công an, hoạt động theo quy định pháp luật chung. Nhiệm vụ chính của Trung tâm Dữ liệu quốc



gia là tích hợp, đồng bộ, lưu trữ, chia sẻ, phân tích và điều phối dữ liệu từ các cơ sở dữ liệu quốc gia của các cơ quan Nhà nước. Đặc biệt, trung tâm hình thành kho dữ liệu quốc gia về con người và kho dữ liệu tổng hợp từ nhiều lĩnh vực, làm nền tảng cốt lõi hỗ trợ hoạch định chính sách, kiến tạo phát triển Chính phủ số, kinh tế số, xã hội số, đồng thời bảo đảm quốc phòng - an ninh.

Trên thực tế, mục tiêu xây dựng Trung tâm Dữ liệu quốc gia là phục vụ phát triển chung, không phải để giám sát cá nhân. Bộ trưởng Công an Lương Tam Quang khẳng định mục tiêu của trung tâm là “*phát huy cao độ giá trị của dữ liệu, nguồn tài nguyên quý giá, tư liệu sản xuất mới nhằm tạo động lực thúc đẩy đổi mới sáng tạo, nâng cao hiệu suất lao động, năng lực cạnh tranh quốc gia*”. Trung tâm này cũng cung cấp hạ tầng CNTT dùng chung cho các bộ, ngành, địa phương và các tổ chức chính trị - xã hội có nhu cầu, giúp phát triển các sản phẩm số, hệ thống dữ liệu tin cậy, kết nối chia sẻ tạo nhiều giá trị mới cho phát triển kinh tế - xã hội. Nghị quyết 57/NQ-TW của Bộ Chính trị xác định Trung tâm Dữ liệu quốc gia là “lõi”, trụ cột của quá trình chuyển đổi số quốc gia, đồng thời đề ra đầu tư xây dựng hạ tầng lưu trữ, trung tâm dữ liệu vùng, cơ sở dữ liệu quốc gia bảo đảm liên thông, tích hợp, chia sẻ.

Luật Dữ liệu (số 60/2024/QH15, hiệu lực từ 1/7/2025) và dự thảo luật liên quan quy định rõ: Nhà nước thống nhất quản lý dữ liệu quốc gia, Chính phủ quyết định định hướng chính sách, Bộ Công an giữ vai trò đầu mối chủ trì quản lý nhà nước về dữ liệu. Theo trình bày trước Quốc hội, Bộ trưởng Công an cho biết “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 trong việc chủ trì, phối hợp với các bộ, ngành, địa phương thực hiện quản lý nhà nước về dữ liệu”. Trong khuôn khổ này, việc thành lập Trung tâm Dữ liệu quốc gia đã được quy định là đơn vị mới thuộc Bộ Công an, do Chính phủ quyết định về tổ chức, và Bộ trưởng Công an sẽ ban hành chức năng, nhiệm vụ, cơ cấu tổ chức.

Vai trò của Bộ Công an trong quản lý dữ liệu phục vụ cho lợi ích chung, không phải “đơn độc” chuyên quyền. Trái lại, theo quy định, mọi hoạt động dữ



liệu đều phải tuân thủ luật pháp, bảo đảm minh bạch và phối hợp liên ngành. Chẳng hạn, Nghị định 165/2025/NĐ-CP (*hướng dẫn Luật Dữ liệu*) yêu cầu các bộ, ngành, địa phương xác định rõ nhu cầu sử dụng dịch vụ của Trung tâm Dữ liệu quốc gia và gửi văn bản đề nghị cung cấp dịch vụ, thể hiện nguyên tắc phối hợp chặt chẽ và công khai với các tổ chức chính trị - xã hội. Trung tâm Dữ liệu quốc gia cũng chịu trách nhiệm hướng dẫn áp dụng tiêu chuẩn, giám sát chất lượng và điều phối dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia, đồng thời “thực hiện các biện pháp bảo vệ dữ liệu được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu” theo quy định hiện hành. Điều này cho thấy Trung tâm Dữ liệu quốc gia không phải là “vùng đất không luật lệ” mà nằm trong hệ thống pháp luật chặt chẽ về dữ liệu.

Một trong những thông tin bị xuyên tạc là Trung tâm Dữ liệu quốc gia sẽ xâm phạm quyền riêng tư cá nhân. Thực tế, cả hệ thống pháp luật Việt Nam hiện hành đều nhấn mạnh bảo vệ dữ liệu cá nhân và an toàn thông tin. Điển hình, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (*có hiệu lực từ 1/7/2023*) là văn bản đầu tiên sử dụng khái niệm dữ liệu cá nhân và quy định rất chặt chẽ về nghĩa vụ bảo vệ dữ liệu. Nghị định này đã tạo hành lang pháp lý bảo vệ dữ liệu cá nhân hiệu quả, giảm thiểu tối đa nguy cơ xâm phạm thông tin cá nhân của người dân. Theo Nghị định, các hành vi thu thập, lưu trữ, chia sẻ dữ liệu cá nhân trái pháp luật đều bị nghiêm cấm và xử lý nghiêm minh. Cũng cần nhấn mạnh rằng Luật Bảo vệ dữ liệu cá nhân (*đã được Quốc hội thông qua tháng 6/2025, có hiệu lực 1/1/2026*) quy định cấm hoàn toàn mua bán dữ liệu cá nhân và nghiêm cấm mạng xã hội yêu cầu người dùng cung cấp hình ảnh hoặc video về giấy tờ tùy thân để xác thực. Luật này còn buộc các nền tảng mạng xã hội công khai chính sách bảo mật, cho phép người dùng truy cập, chỉnh sửa, xóa dữ liệu cá nhân của mình. Như vậy, công dân được bảo hộ quyền riêng tư mạnh mẽ ngay trong Luật Căn cước (*quy định nguyên tắc bảo vệ dữ liệu cá nhân trong cơ sở dữ liệu quốc gia*) và trong các văn bản quy phạm pháp luật mới về bảo vệ dữ liệu cá nhân.



Đồng thời, trong quá trình xây dựng và vận hành Trung tâm Dữ liệu quốc gia, Nhà nước cam kết công khai, minh bạch để giám sát xã hội. Theo Nghị định 165/2025/NĐ-CP, Trung tâm Dữ liệu quốc gia sẽ thiết lập Cổng dữ liệu quốc gia làm đầu mối để các cơ quan Nhà nước công bố thông tin về dữ liệu đang quản lý, cũng như cung cấp dữ liệu mở nhằm “tăng cường tính minh bạch trong hoạt động của Chính phủ và thúc đẩy sáng tạo, phát triển kinh tế, xã hội”. Thông tin về tiến độ xây dựng Trung tâm Dữ liệu quốc gia cũng đã được công bố rõ ràng: trung tâm sẽ đi vào hoạt động chính thức từ ngày 19/8/2025, với hạ tầng hiện đại đảm bảo an ninh, an toàn và hiệu quả. Bộ Công an cam kết tuân thủ các quy chuẩn kỹ thuật và phối hợp với các bộ, ngành để hoàn thiện khung pháp lý, chính sách kèm theo (như quy chế chia sẻ dữ liệu, tiêu chuẩn an ninh thông tin...) sao cho hoạt động của Trung tâm Dữ liệu quốc gia luôn đúng quy định và chịu sự giám sát của nhân dân.

Qua đó có thể thấy, định hướng xây dựng Trung tâm Dữ liệu quốc gia và vai trò của Bộ Công an trong lĩnh vực dữ liệu đã được quy định rõ ràng trong các nghị quyết và văn bản pháp luật của Đảng và Nhà nước. Mục tiêu chính là tích hợp, chia sẻ dữ liệu công nhằm phục vụ lợi ích chung cho sự phát triển của đất nước trong kỷ nguyên số, đồng thời bảo đảm tuyệt đối an toàn thông tin và quyền riêng tư của người dân. Những thông tin xuyên tạc về việc “tập trung hóa dữ liệu” hay “vi phạm quyền riêng tư” đều trái với quy định pháp luật và tầm nhìn chiến lược của Đảng, Nhà nước. Báo chí chính thống và các chuyên gia khẳng định mọi hoạt động liên quan đến dữ liệu cá nhân phải tuân thủ pháp luật, người dân có quyền giám sát, truy cập và quản lý thông tin cá nhân của mình. Trong tiến trình chuyển đổi số, mỗi cá nhân, doanh nghiệp cần hiểu đúng chủ trương của Đảng, hợp tác cung cấp dữ liệu phục vụ mục tiêu chung (như cải thiện dịch vụ công, hoạch định chính sách) trong giới hạn pháp luật cho phép. Việc tuyên truyền, nâng cao nhận thức đúng đắn về chính sách dữ liệu là góp phần bảo vệ quyền lợi của người dân và cung cấp nền tảng só của quốc gia.



## TÀI LIỆU THAM KHẢO

1. Luật Dữ liệu (*Luật số 60/2024/QH15*)
2. Luật An ninh mạng (*Luật số 24/2018/QH14*)
3. Luật An toàn thông tin mạng (*Luật số 86/2015/QH13*)
4. Luật Bảo vệ dữ liệu cá nhân (*Luật số 91/2025/QH15*)
5. Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết thi hành Luật Dữ liệu.
6. Nghị quyết số 57-NQ/TW ngày 22/12/2024 về phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.
7. Công TTĐT Chính phủ, Nội dung cơ bản của Luật Dữ liệu, 2025



**Câu 7: Quy định về sản phẩm, dịch vụ về dữ liệu? Các giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu?**





**Câu 7: Quy định về sản phẩm, dịch vụ về dữ liệu? Các giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu?**

### Trả lời

#### 7.1. Quy định về sản phẩm, dịch vụ dữ liệu theo Luật Dữ liệu 2024

Trong kỷ nguyên số, dữ liệu được xem như tài nguyên chiến lược, là “năng lượng mới”, thậm chí được ví như “máu” của nền kinh tế số. Nhiều quốc gia trên thế giới coi dữ liệu là trụ cột phát triển kinh tế số, ví như dầu mỏ trong nền kinh tế công nghiệp. Tại Việt Nam, các định hướng chiến lược đều nhấn mạnh vai trò của dữ liệu, Nghị quyết 57-NQ/TW (2024) của Bộ Chính trị chỉ rõ cần “làm giàu, khai thác tối đa tiềm năng của dữ liệu, đưa dữ liệu thành tư liệu sản xuất chính, thúc đẩy phát triển... kinh tế dữ liệu”. Dữ liệu không chỉ mang giá trị kinh tế to lớn mà còn là yếu tố cốt lõi để chuyển đổi số thành công, nâng cao năng lực quản trị và năng suất lao động.

Trong bối cảnh đó, việc xây dựng khung pháp lý cho quản trị và khai thác dữ liệu trở thành yêu cầu cấp thiết. Ngày 30/11/2024, Quốc hội Việt Nam thông qua Luật Dữ liệu 2024 dấu mốc quan trọng thể hiện quyết tâm tạo nền tảng pháp lý vững chắc để quản lý, bảo vệ và phát huy hiệu quả dữ liệu, thúc đẩy sản xuất chiến lược quốc gia trong thời đại số. Luật Dữ liệu 2024 gồm 5 chương, 46 điều, điều chỉnh toàn diện vòng đời dữ liệu số, từ thu thập, phát triển, chia sẻ, xử lý đến bảo vệ dữ liệu; thiết lập Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia; đồng thời lần đầu tiên mở rộng phạm vi điều chỉnh tới các sản phẩm, dịch vụ liên quan đến dữ liệu số. Đáng chú ý, luật thừa nhận quyền tài sản đối với dữ liệu, trao cho chủ sở hữu dữ liệu quyền định đoạt và trao đổi giá trị dữ liệu do mình sở hữu, qua đó khuyến khích việc thương mại hóa và lưu thông dữ liệu một cách có trật tự, an toàn.

Các điều từ 39 đến 43 của Luật Dữ liệu nằm trong Chương IV (*Sản phẩm, dịch vụ về dữ liệu*), thiết lập khung pháp lý để quản lý những loại hình dịch vụ dữ liệu hoàn toàn mới tại Việt Nam. Cụ thể, luật định nghĩa và điều chỉnh các dịch



vụ trung gian dữ liệu, dịch vụ phân tích, tổng hợp dữ liệu, dịch vụ xác thực điện tử và sàn giao dịch dữ liệu. Đây là những thành phần thiết yếu của “thị trường dữ liệu” - nơi dữ liệu được trao đổi, mua bán và tạo ra giá trị mới. Luật quy định điều kiện kinh doanh, giới hạn chủ thể cung cấp cũng như trách nhiệm pháp lý đối với từng loại dịch vụ này, nhằm vừa thúc đẩy phát triển ngành công nghiệp dữ liệu, vừa đảm bảo an toàn, bảo mật trong hoạt động giao dịch dữ liệu. Các quy định tại điều 39-43 cũng mang tính chất khung, giao Chính phủ hướng dẫn chi tiết thêm (*theo khoản cuối cùng của các điều 39-43*), thể hiện sự thận trọng của Bộ Công an đối với lĩnh vực còn rất mới mẻ.

Có thể thấy, Việt Nam đang từng bước hình thành hệ sinh thái quản trị dữ liệu quốc gia tương đồng với xu hướng quốc tế. Ví dụ: Liên minh châu Âu ban hành Đạo luật Quản trị Dữ liệu (*Data Governance Act - DGA*) năm 2022 (*có hiệu lực 9/2023*) nhằm thiết lập môi trường chia sẻ và lưu thông dữ liệu an toàn. Đạo luật này đề ra mô hình dịch vụ trung gian dữ liệu, các tổ chức trung gian độc lập làm bên thứ ba kết nối bên cung dữ liệu với bên sử dụng dữ liệu, hoạt động trong “không gian dữ liệu” chung để tạo thuận lợi cho chia sẻ thông tin và hình thành thị trường dữ liệu châu Âu. Những tổ chức trung gian phải đảm bảo tính trung lập, không xung đột lợi ích và không được kinh doanh trực lợi tiếp từ dữ liệu (*không bán dữ liệu hay sử dụng dữ liệu được chia sẻ để phát triển sản phẩm riêng*) qua đó xây dựng lòng tin cho các bên tham gia. Tương tự, Singapore từ năm 2003 đã triển khai nền tảng định danh số quốc gia Singpass cho phép người dân truy cập mọi dịch vụ công trực tuyến qua một tài khoản duy nhất, tích hợp hơn 200 dịch vụ của chính phủ và tư nhân. Singpass đóng vai trò như dịch vụ xác thực điện tử đáng tin cậy, giúp xác minh danh tính và thông tin của cá nhân khi tham gia giao dịch số, qua đó nâng cao trải nghiệm và niềm tin số. Những kinh nghiệm quốc tế này cho thấy việc luật hóa các mô hình trung gian dữ liệu, sàn giao dịch dữ liệu hay dịch vụ xác thực điện tử là xu hướng cần thiết để thúc đẩy kinh tế dữ liệu phát triển minh bạch, bền vững.



### 7.1.1. Phạm vi sản phẩm, dịch vụ về dữ liệu

Điều 39 xác định phạm vi các sản phẩm, dịch vụ về dữ liệu thuộc đối tượng điều chỉnh của Luật Dữ liệu 2024. Khoản 1 liệt kê các nhóm chính: trung gian dữ liệu, phân tích, tổng hợp dữ liệu, xác thực điện tử, sàn dữ liệu. Đây đều là những loại hình dịch vụ gắn liền với quá trình khai thác, trao đổi dữ liệu trong nền kinh tế số. Quy định này mang ý nghĩa định danh các loại hình kinh doanh dữ liệu mới để đưa vào khuôn khổ quản lý nhà nước. Trước đây, pháp luật Việt Nam chưa có khái niệm rõ ràng về những dịch vụ như “trung gian dữ liệu” hay “sàn giao dịch dữ liệu”; do đó, Điều 39 tạo nền tảng pháp lý ban đầu cho thị trường dữ liệu.

Khoản 1 cũng nhấn mạnh việc cung cấp sản phẩm, dịch vụ dữ liệu trong các lĩnh vực này phải tuân thủ cả Luật Dữ liệu và các quy định pháp luật liên quan khác. Nghĩa là, ngoài Luật Dữ liệu, các dịch vụ dữ liệu vẫn chịu sự điều chỉnh của những luật chuyên ngành tương ứng. Ví dụ: dịch vụ phân tích dữ liệu nếu liên quan đến dữ liệu cá nhân thì phải tuân thủ quy định về bảo vệ dữ liệu cá nhân; hay hoạt động của sàn giao dịch dữ liệu phải phù hợp với pháp luật về thương mại điện tử, giao dịch điện tử,... Đây là cách tiếp cận “khung khổ chung + chuyên ngành” nhằm tránh mâu thuẫn với luật hiện hành, đồng thời đảm bảo mọi khía cạnh đều có hành lang pháp lý.

Dịch vụ xác thực điện tử là một điểm mới đáng chú ý tại khoản 2 Điều 39. Quy định này nêu: “*Dịch vụ xác thực điện tử thực hiện việc xác thực dữ liệu trong các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống định danh và xác thực điện tử...*” và đặc biệt giới hạn chủ thể cung cấp dịch vụ này là đơn vị sự nghiệp công lập, doanh nghiệp nhà nước đáp ứng điều kiện. Như vậy, không phải tổ chức, doanh nghiệp nào cũng được kinh doanh dịch vụ xác thực điện tử, nhà nước bước đầu kiểm soát chặt loại hình dịch vụ liên quan đến xác thực dữ liệu chính thức. Việc này xuất phát từ tính chất nhạy cảm và yêu cầu độ tin cậy cao của dịch vụ xác thực về tính chính xác, hợp lệ của dữ liệu (ví dụ xác thực thông tin công dân trong Cơ sở dữ liệu Quốc gia về dân cư, xác thực văn bản điện tử so với bản gốc...). Chỉ những chủ thể nhà nước hoặc do nhà nước nắm giữ mới được trao quyền cung cấp dịch vụ



này, nhằm đảm bảo uy tín và an ninh. Điều 20 Luật Dữ liệu 2024 cũng quy định dữ liệu sau khi được xác thực bằng dịch vụ xác thực điện tử sẽ có giá trị pháp lý tương đương dữ liệu gốc trong phạm vi, thời gian nhất định. Do đó, dịch vụ xác thực điện tử giống như “công chứng số” xác nhận tính xác thực của dữ liệu, tạo niềm tin cho việc sử dụng dữ liệu điện tử thay cho bản giấy. Hiện nay, Việt Nam đã xây dựng Hệ thống định danh và xác thực điện tử quốc gia (*theo Nghị định 59/2022/NĐ-CP*), do Bộ Công an quản lý, cấp tài khoản định danh điện tử (*VNeID*) cho công dân. Các dịch vụ xác thực điện tử trong Luật Dữ liệu có thể sẽ gắn với hệ thống này, ví dụ dịch vụ xác thực thông tin công dân, xác thực giấy tờ từ Cơ sở dữ liệu Quốc gia... Kinh nghiệm quốc tế cho thấy dịch vụ xác thực dữ liệu thường do nhà nước chủ trì: Singapore sử dụng Singpass làm nền tảng xác thực danh tính và chữ ký điện tử cho cả khu vực công lẫn tư; đầu năm 2025, Hàn Quốc cũng hoàn tất triển khai thẻ căn cước công dân kỹ thuật số trên ứng dụng di động, cho phép người dân dùng ID điện tử trên smartphone thay thế bản giấy một cách hợp pháp. Việc triển khai này cho thấy dịch vụ xác thực điện tử là xu hướng tất yếu, nhưng để bảo đảm an ninh, các nước đều giao cho cơ quan nhà nước hoặc doanh nghiệp được ủy quyền thực hiện.



Hình ảnh: Tích hợp căn cước vào điện thoại tại Hàn Quốc. Ảnh: Yonhap



Bên cạnh đó, khoản 3 Điều 39 xác định chính sách ưu đãi cho các tổ chức cung cấp dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu. Cụ thể, các doanh nghiệp này được hưởng ưu đãi như doanh nghiệp công nghệ cao, đổi mới sáng tạo, khởi nghiệp số. Đây là tín hiệu tích cực từ nhà nước nhằm khuyến khích hình thành và phát triển các doanh nghiệp hoạt động trong lĩnh vực dữ liệu mới mẻ, cần hỗ trợ về thuế, đất đai, vốn... tương tự các ngành công nghệ cao khác. Quy định này phù hợp với chủ trương thúc đẩy công nghiệp dữ liệu của Việt Nam, xem dữ liệu và các dịch vụ dữ liệu như một ngành kinh tế mũi nhọn trong tương lai.

Khoản 4 Điều 39 loại trừ một số sản phẩm, dịch vụ dữ liệu thuộc các lĩnh vực đặc thù khỏi phạm vi luật này. Cụ thể, các sản phẩm, dịch vụ dữ liệu trong hoạt động giao dịch điện tử, viễn thông, an ninh mạng, an toàn thông tin mạng, công nghiệp công nghệ thông tin, cơ yếu, công nghiệp quốc phòng, an ninh và động viên công nghiệp tiếp tục thực hiện theo pháp luật chuyên ngành tương ứng. Điều này hàm ý rằng Luật Dữ liệu không bao quát toàn bộ mọi dịch vụ liên quan đến dữ liệu, mà tôn trọng ranh giới với các luật hiện hành. Ví dụ: dịch vụ dữ liệu trong viễn thông (*nhiều cung cấp dữ liệu thuê bao*) vẫn do Luật Viễn thông điều chỉnh; dịch vụ về an toàn thông tin mạng (*nhiều chứng thực chữ ký số, dịch vụ mật mã dân sự*) vẫn theo Luật An toàn thông tin mạng 2015; dịch vụ trong lĩnh vực cơ yếu, quốc phòng (*liên quan đến dữ liệu mật, dữ liệu quân sự*) theo luật chuyên ngành. Sự phân định này nhằm tránh chồng lấn pháp lý và khăng định Luật Dữ liệu 2024 chủ yếu tập trung vào các dịch vụ dữ, chưa điều chỉnh mảng dữ liệu đã có luật riêng.

Cuối cùng, khoản 5 Điều 39 giao Chính phủ quy định chi tiết thêm về sản phẩm, dịch vụ dữ liệu. Có thể dự kiến Chính phủ sẽ ban hành nghị định hướng dẫn, làm rõ điều kiện kinh doanh, quy trình cấp phép, tiêu chuẩn kỹ thuật... cho từng loại hình dịch vụ dữ liệu. Trên thực tế, trước khi Luật Dữ liệu được ban hành danh mục ngành nghề kinh doanh có điều kiện trong Luật Đầu tư đã được bổ sung thêm các ngành nghề mới gồm “*Kinh doanh sản phẩm, dịch vụ trung gian dữ liệu*”, “*Kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu*” và “*Kinh doanh*



dịch vụ sàn dữ liệu”. Điều này cho thấy Nhà nước chính thức coi các dịch vụ dữ liệu là ngành nghề kinh doanh có điều kiện, phải được quản lý chặt chẽ. Việc đăng ký hoạt động và đáp ứng điều kiện theo Luật Đầu tư (*nhiều quy định tại điều 40, 41, 42*) vì thế mang tính bắt buộc để được phép kinh doanh các dịch vụ này. Tóm lại, Điều 39 mang tính chất mở đầu chương, xác định rõ phạm vi và nguyên tắc chung khi quản lý sản phẩm, dịch vụ dữ liệu, tạo sự minh bạch cho các chủ thể tham gia lĩnh vực dữ liệu mới.

### **7.1.2. Dịch vụ trung gian dữ liệu, điều kiện đăng ký, nguyên tắc hoạt động**

Điều 40 của Luật Dữ liệu tập trung quy định về sản phẩm, dịch vụ trung gian dữ liệu, qua đó chính thức định nghĩa và đặt ra khung pháp lý cho loại hình dịch vụ môi giới, kết nối dữ liệu. Theo khoản 1, sản phẩm, dịch vụ trung gian dữ liệu là sản phẩm, dịch vụ nhằm thiết lập mối quan hệ thương mại giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng sản phẩm, dịch vụ, thông qua thỏa thuận, nhằm mục đích trao đổi, chia sẻ, truy cập dữ liệu, thực hiện các quyền của chủ thể dữ liệu, chủ sở hữu dữ liệu, người dùng dữ liệu. Nói cách khác, dịch vụ trung gian dữ liệu đóng vai trò cầu nối giữa bên cung cấp dữ liệu và bên khai thác dữ liệu. Thông qua trung gian, các bên có thể gặp gỡ, thỏa thuận với nhau về việc mua bán, chia sẻ hoặc cho phép truy cập dữ liệu theo các điều khoản thương mại nhất định.

Ở đây cần hiểu “chủ thể dữ liệu” là cá nhân mà dữ liệu phản ánh (*data subject - thường chỉ cá nhân có dữ liệu cá nhân*), “chủ sở hữu dữ liệu” là tổ chức, cá nhân nắm quyền sở hữu dữ liệu (*data owner*), còn “người dùng dữ liệu” là bên muốn tiếp cận, sử dụng dữ liệu. Dịch vụ trung gian có thể dưới nhiều hình thức: một nền tảng trực tuyến kết nối bên cung cấp dữ liệu và bên cần dữ liệu; hoặc một công ty môi giới dữ liệu đứng ra thu thập dữ liệu từ nhiều nguồn rồi cung ứng cho khách hàng theo yêu cầu; hay các data marketplace (*chợ dữ liệu*) nơi dữ liệu được niêm yết và giao dịch. Điểm chung là trung gian không trực tiếp tạo ra dữ liệu mà tạo môi trường giao dịch dữ liệu.

Luật yêu cầu hoạt động trung gian dữ liệu phải dựa trên thỏa thuận bằng hợp đồng giữa các bên. Điều này nhấn mạnh tính pháp lý rõ ràng của giao dịch:



các quyền và nghĩa vụ về dữ liệu (*phạm vi sử dụng, giá cả, trách nhiệm nếu vi phạm,...*) cần được cụ thể hóa thành hợp đồng. Yêu cầu này phù hợp với nguyên tắc chung về giao kết dân sự, thương mại và giúp bảo vệ quyền lợi các bên trong trường hợp tranh chấp.

Khoản 2 Điều 40 đặt ra điều kiện chủ yếu: “*Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu phải được đăng ký hoạt động và quản lý theo quy định của pháp luật về đầu tư*”, ngoại trừ trường hợp cung cấp dịch vụ trung gian dữ liệu nội bộ trong tổ chức. Quy định này có hai ý chính: <sup>(1)</sup>Doanh nghiệp muốn kinh doanh dịch vụ trung gian dữ liệu phải đăng ký ngành nghề kinh doanh và chịu sự quản lý như một ngành nghề đầu tư kinh doanh có điều kiện; <sup>(2)</sup>Nếu một tổ chức chỉ làm trung gian dữ liệu phục vụ cho nội bộ mình (ví dụ một tập đoàn chia sẻ dữ liệu giữa các công ty con) thì không bắt buộc đăng ký.

Trên thực tế, Luật Đầu tư 2020 (*Phụ lục IV*) chưa từng liệt kê “kinh doanh trung gian dữ liệu” trước đây. Nhưng trước khi Luật Dữ liệu được ban hành, Luật Đầu tư đã đã bổ sung “Kinh doanh sản phẩm, dịch vụ trung gian dữ liệu” vào danh mục ngành nghề kinh doanh có điều kiện. Điều kiện cụ thể sẽ do cơ quan có thẩm quyền quy định (có thể về năng lực tài chính, nhân sự, kỹ thuật, bảo mật...). Bắt buộc đăng ký kinh doanh giúp nhà nước kiểm soát được các công ty môi giới dữ liệu, tránh tình trạng dữ liệu bị thu gom, mua bán tràn lan bởi các bên không phép, nhất là dữ liệu cá nhân. Đồng thời, việc này tạo sự công khai minh bạch, tổ chức nào kinh doanh dữ liệu hợp pháp sẽ nằm trong danh sách quản lý. Trường hợp trung gian dữ liệu nội bộ thì miễn đăng ký vì không phát sinh giao dịch thương mại ra bên ngoài, rủi ro thấp hơn.

Việc đưa trung gian dữ liệu vào quản lý có điều kiện tương đồng với xu hướng quốc tế. Đạo luật Quản trị Dữ liệu 2022 của Liên minh châu Âu yêu cầu các “nhà cung cấp dịch vụ trung gian chia sẻ dữ liệu” (*data intermediation services*) phải đăng ký với cơ quan có thẩm quyền và tuân thủ các tiêu chí nghiêm ngặt để đảm bảo tính trung lập, minh bạch. Họ phải thông báo mô hình hoạt động cho cơ quan quản lý và chịu sự giám sát liên tục. Luật An ninh dữ liệu của Trung



Quốc cũng nhấn mạnh nhà nước cần xây dựng hệ thống quản lý giao dịch dữ liệu lành mạnh, trong đó các tổ chức trung gian giao dịch dữ liệu phải thực hiện nghĩa vụ xác minh nguồn dữ liệu, xác thực danh tính các bên giao dịch và lưu trữ hồ sơ giao dịch. Điều này nhằm phòng ngừa dữ liệu bất hợp pháp lưu thông qua trung gian. Với Việt Nam, điều 40 mới dừng ở yêu cầu đăng ký, còn các nghĩa vụ chi tiết của bên trung gian (*nhiều phải bảo đảm an toàn giao dịch, kiểm soát nguồn dữ liệu, giải quyết tranh chấp...*) được quy định chung tại điều 43 và do nghị định hướng dẫn bổ sung.



*Hình ảnh: Đại tướng Lương Tam Quang - Bộ trưởng Bộ Công an phát biểu về sàn dữ liệu tại Việt Nam. Ảnh: Báo Tuổi trẻ*

Nhìn chung, Điều 40 đặt nền tảng pháp lý cho mô hình doanh nghiệp môi giới dữ liệu, một thành phần quan trọng để hình thành thị trường dữ liệu. Trung gian dữ liệu giúp kết nối cung cầu, thương mại hóa dữ liệu một cách chuyên nghiệp. Ví dụ: một công ty A sở hữu tập dữ liệu khách hàng có thể thông qua một nền tảng trung gian để cung cấp dữ liệu (*có kiểm soát*) cho công ty B muốn dùng dữ liệu đó nghiên cứu thị trường, thay vì tự giao dịch riêng lẻ. Mô hình này đã phổ biến tại châu Âu, Mỹ với các nền tảng như Dawex, Oracle Data Marketplace...



Tại châu Á, Nhật Bản và Hàn Quốc cũng phát triển các chợ dữ liệu số: Hàn Quốc hiện có 21 sàn giao dịch dữ liệu trong nhiều lĩnh vực (*vận tải, y tế, tài chính...*), do cả nhà nước và tư nhân phối hợp vận hành. Những sàn này đóng vai trò trung gian, tạo môi trường cho dữ liệu lưu thông. Vì vậy, việc Việt Nam luật hóa trung gian dữ liệu là bước đi phù hợp thông lệ, mở đường cho các doanh nghiệp Việt Nam tham gia vào lĩnh vực môi giới dữ liệu đầy tiềm năng.

Tuy nhiên, quản lý dịch vụ trung gian dữ liệu đòi hỏi phải cân bằng giữa khuyến khích đổi mới và kiểm soát rủi ro. Điều 40 mới chỉ nêu nguyên tắc, chưa có tiêu chí cụ thể cho điều kiện kinh doanh. Cần chờ các văn bản dưới luật hướng dẫn (ví dụ: *quy định về bảo vệ dữ liệu cá nhân trong hoạt động của trung gian, đảm bảo trung gian không lạm dụng dữ liệu của các bên*), quy định về an ninh mạng (*trung gian phải tuân thủ lưu trữ dữ liệu quan trọng trong nước theo Luật An ninh mạng 2018 nếu có*), hay trách nhiệm thông báo, báo cáo với cơ quan quản lý. Dù sao, việc đưa trung gian dữ liệu vào khuôn khổ cho thấy Việt Nam sẵn sàng “mở cửa thị trường dữ liệu” nhưng có kiểm soát, tương tự nhận định của giới chuyên gia rằng Luật Dữ liệu 2024 tạo nền móng pháp lý để thị trường dữ liệu phát triển minh bạch, trật tự.

### **7.1.3. Phân tích, tổng hợp dữ liệu, yêu cầu bảo vệ dữ liệu cá nhân và điều kiện khai thác dữ liệu quốc gia**

Điều 41 Luật Dữ liệu điều chỉnh về sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu, tức các hoạt động xử lý dữ liệu tạo ra thông tin giá trị gia tăng. Có thể hiểu đây là dịch vụ mà doanh nghiệp dùng kỹ thuật phân tích (*data analytics, data mining, AI...*) để biến dữ liệu thô thành thông tin hữu ích, rồi bán thông tin đó hoặc cung cấp kết quả phân tích cho khách hàng theo yêu cầu. Khoản 1 định nghĩa rõ: “*Sản phẩm phân tích, tổng hợp dữ liệu là kết quả của quá trình phân tích, tổng hợp dữ liệu thành thông tin chuyên sâu hữu ích ở các cấp độ khác nhau theo yêu cầu của bên sử dụng sản phẩm. Dịch vụ phân tích, tổng hợp dữ liệu là hoạt động phân tích, tổng hợp dữ liệu theo yêu cầu của bên sử dụng dịch vụ*”. Như vậy, sản



phẩm ở đây là đầu ra (*báo cáo, kết luận, dữ liệu đã qua xử lý*), còn dịch vụ là quá trình thực hiện để tạo ra sản phẩm đó theo đặt hàng.

Ví dụ: một công ty có thể cung cấp sản phẩm dữ liệu dạng báo cáo phân tích xu hướng thị trường dựa trên tổng hợp dữ liệu tiêu dùng từ nhiều nguồn. Hoặc một ngân hàng thuê một đơn vị phân tích dữ liệu để tổng hợp dữ liệu khách hàng, đưa ra mô hình dự báo rủi ro tín dụng, đó là dịch vụ phân tích dữ liệu theo yêu cầu. Điểm chung là có bên sử dụng dữ liệu thuê bên chuyên môn phân tích nhằm nhận được tri thức hoặc giá trị tăng từ dữ liệu gốc.

Vì hoạt động phân tích dữ liệu tiềm ẩn nhiều rủi ro (*đặc biệt khi phân tích dữ liệu lớn, dữ liệu cá nhân có thể ảnh hưởng đến quyền riêng tư hay an ninh*), khoản 2 Điều 41 đặt ra hai lớp điều kiện quản lý:

- **Thứ nhất**, “Tổ chức kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có thể gây nguy hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng phải đăng ký hoạt động, quản lý theo quy định của pháp luật về đầu tư”. Quy định này tương tự điều 40 yêu cầu đăng ký kinh doanh với cơ quan nhà nước nếu kinh doanh phân tích dữ liệu thuộc loại có rủi ro cao cho các lợi ích công cộng quan trọng. Các cụm từ liệt kê (*quốc phòng, an ninh, trật tự an toàn xã hội, đạo đức xã hội, sức khỏe cộng đồng*) cho thấy Nhà nước đặc biệt quan tâm nếu việc phân tích dữ liệu có thể tác động tiêu cực đến xã hội (ví dụ: *phân tích dữ liệu nhạy cảm về an ninh, phân tích dự báo gây hoang mang xã hội, phân tích dữ liệu y tế sai lệch ảnh hưởng sức khỏe cộng đồng,...*) Khi đó, doanh nghiệp phải đăng ký để được giám sát. Như đã đề cập, từ 15/01/2025, pháp luật đầu tư đã bổ sung ngành nghề “Kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu” vào danh mục kinh doanh có điều kiện. Do đó, hầu hết các công ty cung cấp dịch vụ phân tích dữ liệu (*trừ phi hoạt động của họ hoàn toàn vô hại*) đều sẽ phải đăng ký và đáp ứng điều kiện kinh doanh do Chính phủ quy định.

- **Thứ hai**, “Trường hợp có kết nối, chia sẻ với cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành để kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ



liệu phải được quản lý theo quy định của pháp luật". Điểm này nhằm kiểm soát việc khai thác dữ liệu từ các cơ sở dữ liệu do Nhà nước quản lý để kinh doanh phân tích. Nếu một doanh nghiệp muốn truy cập Cơ sở dữ liệu Quốc gia (ví dụ Cơ sở dữ liệu dân cư, Cơ sở dữ liệu doanh nghiệp, Cơ sở dữ liệu đất đai...) hoặc Cơ sở dữ liệu chuyên ngành của cơ quan nhà nước để phân tích và cung cấp dịch vụ, thì phải tuân theo quy định pháp luật hiện hành về khai thác dữ liệu công. Thực tế, tại Điều 35 và Điều 36 Luật Dữ liệu 2024 cũng quy định về việc khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu do nhà nước quản lý: cơ quan, tổ chức ngoài nhà nước muốn khai thác dữ liệu trong Cơ sở dữ liệu Quốc gia, Cơ sở dữ liệu khác phải được sự đồng ý và có thể phải trả phí. Như vậy, doanh nghiệp phân tích dữ liệu không được tự do kết nối vào kho dữ liệu quốc gia nếu chưa được phép. Điểm này để bảo vệ tài nguyên dữ liệu quốc gia và tránh lạm dụng dữ liệu công vào mục đích thương mại khi chưa có cơ chế rõ ràng.

Từ hai yêu cầu trên, có thể thấy trọng tâm quản lý của Điều 41 nằm ở việc đảm bảo an ninh dữ liệu và bảo vệ quyền lợi chung trong hoạt động phân tích dữ liệu. So với trung gian dữ liệu (*chỉ môi giới, không nhất thiết xử lý sâu dữ liệu*), các dịch vụ phân tích dữ liệu trực tiếp sử dụng và chuyển hóa dữ liệu, nên nguy cơ lộ lọt hoặc bị lạm dụng dữ liệu (*đặc biệt dữ liệu cá nhân*) cao hơn. Do đó, pháp luật đòi hỏi các đơn vị này phải “có danh có phận” (*đăng ký*) và tuân thủ các chuẩn mực an toàn.

Về bảo vệ dữ liệu cá nhân, mặc dù Điều 41 không nêu trực tiếp cụm từ này, nhưng rõ ràng bất kỳ dịch vụ phân tích nào liên quan đến dữ liệu cá nhân đều phải tuân thủ pháp luật về bảo vệ dữ liệu cá nhân. Hiện nay, Việt Nam đã ban hành Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân và Luật Bảo vệ Dữ liệu Cá nhân 2025, trong đó quy định nguyên tắc xử lý dữ liệu cá nhân phải có sự đồng ý của chủ thể dữ liệu (*trừ một số ngoại lệ pháp luật cho phép*) và phải đảm bảo an ninh, an toàn. Doanh nghiệp phân tích dữ liệu cá nhân cho khách hàng cần tuân thủ các yêu cầu như: xin phép chủ thể dữ liệu nếu dữ liệu không ẩn danh, chỉ sử dụng trong phạm vi mục đích được đồng ý, áp dụng biện pháp mã hóa, ẩn danh



khi có thể,... Luật Dữ liệu 2024 cũng không “miễn trừ” các quy định khác (ví dụ Điều 30 Luật An ninh mạng 2018 yêu cầu dữ liệu cá nhân quan trọng phải lưu trữ trong nước, Điều 17 Nghị định 13/2023 cấm tiết lộ dữ liệu nhạy cảm như tình trạng sức khỏe, tài chính nếu không có căn cứ). Vì vậy, doanh nghiệp phân tích dữ liệu phải xây dựng quy trình tuân thủ chặt chẽ.

Ví dụ: Công ty X phân tích dữ liệu hành vi người dùng từ mạng xã hội để dự đoán xu hướng tiêu dùng. Bộ dữ liệu này có thể chứa thông tin cá nhân, quan điểm riêng tư. Nếu công ty X không được sự chấp thuận của người dùng hoặc lén thu thập mà không công khai, thì việc phân tích đã vi phạm quyền cá nhân. Do đó, X phải đảm bảo dữ liệu đưa vào phân tích đã được thu thập hợp pháp, hoặc ít nhất phải ẩn danh (để không truy ngược lại cá nhân cụ thể). Đây chính là khía cạnh đạo đức và pháp lý trong phân tích dữ liệu mà Điều 41 bao trùm kiểm soát qua cụm từ “đạo đức xã hội” trong khoản 2.

Trên thế giới, dịch vụ phân tích dữ liệu ngày càng phổ biến nhưng cũng chịu sự giám sát gắt gao. Quy định Bảo vệ Dữ liệu Chung của Liên minh châu Âu quy định nếu phân tích dữ liệu cá nhân, đặc biệt dùng AI ra quyết định tự động, thì phải minh bạch thuật toán và có cơ chế để người dân phản đối quyết định dựa trên phân tích đó. Singapore cũng đã ban hành hướng dẫn về AI và quản trị dữ liệu, yêu cầu các công ty khi dùng dữ liệu khách hàng để phân tích (ví dụ trong bảo hiểm, ngân hàng) phải có biện pháp bảo vệ quyền riêng tư, đánh giá tác động. Những quy tắc này chắc chắn sẽ dần được nội luật hóa tại Việt Nam. Hiện tại, ít nhất Luật Dữ liệu đã khởi đầu bằng việc đưa ngành phân tích dữ liệu vào diện quản lý có điều kiện.

Tóm lại, Điều 41 tạo khung pháp lý cho ngành phân tích dữ liệu thương mại, vừa thừa nhận giá trị của việc khai thác dữ liệu để tạo thông tin chuyên sâu phục vụ phát triển kinh tế - xã hội, vừa đề cao nghĩa vụ quản lý rủi ro của các tổ chức tham gia. Doanh nghiệp phân tích dữ liệu phải cân nhắc tuân thủ cả Luật Dữ liệu lẫn các luật khác như Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước (nếu dữ liệu là mật), Luật Bảo vệ người tiêu dùng (nếu kết quả phân tích cung cấp cho



(người dùng phải trung thực). Việc kết nối với kho dữ liệu nhà nước để phân tích cũng cần có cơ chế rõ ràng (có thể là xin phép truy cập từng lần, hoặc thông qua thỏa thuận chia sẻ dữ liệu công do cơ quan quản lý quy định). Luật Dữ liệu giao Chính phủ quy định chi tiết Điều 41 (khoản 3), do đó trong tương lai có thể sẽ có hướng dẫn như tiêu chí xác định thế nào là “gây nguy hại” (để biết khi nào phải đăng ký), quy trình đăng ký kinh doanh dịch vụ phân tích dữ liệu, quy định về chứng chỉ, giấy phép nếu cần.

Ở khía cạnh thực tiễn, các dịch vụ phân tích dữ liệu tại Việt Nam hiện nay chủ yếu do các công ty công nghệ, marketing cung cấp (ví dụ phân tích dữ liệu khách hàng cho doanh nghiệp bán lẻ, phân tích dữ liệu giao thông cho đô thị thông minh...). Những dịch vụ này trước đây chưa chịu sự kiểm soát riêng. Từ khi luật có hiệu lực, các công ty sẽ phải rà soát xem mình có thuộc diện “gây nguy hại” không để đăng ký, đồng thời tăng cường biện pháp bảo vệ dữ liệu cá nhân trong quy trình phân tích. Nhà nước khuyến khích đổi mới sáng tạo trong dữ liệu, nhưng chắc chắn sẽ mạnh tay nếu dữ liệu bị lạm dụng, chẳng hạn việc phân tích dữ liệu cá nhân nhạy cảm mà không được phép có thể bị xử phạt theo Nghị định riêng. Tất cả nhằm hướng tới một thị trường dịch vụ phân tích dữ liệu phát triển lành mạnh, có trách nhiệm.

#### 7.1.4. Sàn dữ liệu, chủ thể vận hành và dữ liệu bị cấm giao dịch

Điều 42 Luật Dữ liệu quy định về sàn dữ liệu, có thể hiểu là nền tảng giao dịch dữ liệu phục vụ kết nối nhiều bên tham gia trao đổi dữ liệu và các sản phẩm, dịch vụ liên quan đến dữ liệu. Đây là bước tiến quan trọng trong việc hình thành thị trường dữ liệu công khai tại Việt Nam. Khoản 1 nêu khái quát: “Sàn dữ liệu là nền tảng cung cấp tài nguyên liên quan đến dữ liệu để phục vụ nghiên cứu, phát triển khởi nghiệp, đổi mới sáng tạo; cung cấp các sản phẩm, dịch vụ liên quan đến dữ liệu phục vụ phát triển kinh tế - xã hội; là môi trường để giao dịch, trao đổi dữ liệu và các sản phẩm, dịch vụ liên quan đến dữ liệu.”. Như vậy, sàn dữ liệu được thiết kế với ba mục tiêu chính:



- **Thứ nhất**, cung cấp tài nguyên dữ liệu cho nghiên cứu, đổi mới sáng tạo, khởi nghiệp: Tức là tạo ra một kho hoặc cổng dữ liệu tập trung, nơi các nhà nghiên cứu, doanh nghiệp khởi nghiệp có thể tìm kiếm, tiếp cận dữ liệu (*có thể miễn phí hoặc có phí*) để phát triển ứng dụng, dịch vụ mới. Điều này tương tự các cổng dữ liệu mở nhưng ở tầm rộng hơn, cho phép không chỉ dữ liệu công mà cả dữ liệu từ nhiều nguồn khác nhau.

- **Thứ hai**, cung cấp sản phẩm, dịch vụ dữ liệu phục vụ phát triển kinh tế - xã hội: Sàn dữ liệu không chỉ chứa dữ liệu thô mà còn có thể niêm yết các sản phẩm dữ liệu (*báo cáo, phân tích*) và dịch vụ (*như dịch vụ phân tích theo yêu cầu, dịch vụ xác thực...*) liên quan, nhằm đáp ứng nhu cầu đa dạng của xã hội. Nói cách khác, sàn như một chợ trực tuyến không chỉ bán dữ liệu mà bán cả dịch vụ dữ liệu.

- **Thứ ba**, là môi trường giao dịch, trao đổi dữ liệu và các sản phẩm, dịch vụ dữ liệu: Đây là chức năng cốt lõi, sàn dữ liệu đóng vai trò trung gian tao lập thị trường, nơi người có dữ liệu cần bán/chia sẻ gặp người cần mua/sử dụng dữ liệu, cùng giao kết giao dịch trên sàn. Sàn có thể hỗ trợ các chức năng: đăng tin chào bán dữ liệu, tìm kiếm dữ liệu, thực hiện thanh toán, giao nhận dữ liệu, đánh giá uy tín, giải quyết tranh chấp,... tương tự một sàn thương mại điện tử nhưng mặt hàng ở đây là dữ liệu.

Qua định nghĩa trên, có thể hình dung sàn dữ liệu như sự kết hợp của nền tảng công nghệ (*để lưu trữ, tích hợp, phân phối dữ liệu*) và môi trường thương mại (*với quy tắc giao dịch, hợp đồng, thanh toán*). Đây chính là mô hình mà nhiều nước đang xây dựng để thúc đẩy nền kinh tế dữ liệu. Nhật Bản đã triển khai Data Exchange trong Chiến lược dữ liệu quốc gia; Liên minh Châu Âu thì đề xuất xây dựng các data marketplace theo ngành trong chiến lược dữ liệu 2020 (*chẳng hạn European Health Data Space làm sàn trao đổi dữ liệu y tế giữa các quốc gia Liên minh Châu Âu*).

Điểm đặc thù trong luật Việt Nam là quy định về chủ thể được cung cấp dịch vụ sàn dữ liệu (*khoản 2*): “*Tổ chức cung cấp dịch vụ sàn dữ liệu là đơn vị sự nghiệp công lập, doanh nghiệp nhà nước đáp ứng điều kiện cung cấp dịch vụ và*



được cấp phép thành lập theo quy định của pháp luật.”. Điều này có nghĩa nhà nước hạn chế quyền vận hành sàn dữ liệu chỉ cho các đơn vị nhà nước (*hoặc chịu sự kiểm soát của Nhà nước*). Cụ thể:

- Đơn vị sự nghiệp công lập, thường là các trung tâm, viện, tổ chức do Nhà nước thành lập để cung ứng dịch vụ công như Trung tâm dữ liệu quốc gia... Nếu đơn vị này được giao nhiệm vụ, họ có thể mở sàn dữ liệu phục vụ mục đích công cộng và thương mại.

- Doanh nghiệp nhà nước (*do Nhà nước nắm giữ trên 50% vốn điều lệ theo Luật Doanh nghiệp*). Các tập đoàn, tổng công ty lớn của nhà nước (*Viettel, VNPT, Vietnam Post,...*) có tiềm lực hạ tầng có thể được cho phép lập sàn dữ liệu. Trường hợp cụ thể: Tổng công ty Bưu điện Việt Nam (*Vietnam Post*) gần đây đã hợp tác với công ty DataStreams (*Hàn Quốc*) hướng tới xây dựng một sàn giao dịch dữ liệu thí điểm tại Việt Nam. Vietnam Post là doanh nghiệp nhà nước và có lợi thế mạng lưới, dữ liệu lớn, nếu được cấp phép, họ có thể là một trong những đơn vị tiên phong vận hành sàn dữ liệu đúng như yêu cầu luật định.

- Phải đáp ứng điều kiện dịch vụ, các tiêu chuẩn kỹ thuật, tài chính, nhân lực... mà Chính phủ sẽ ban hành cho việc vận hành sàn (*chắc chắn phải có nền tảng công nghệ đủ mạnh, an toàn bảo mật cao, quy trình quản lý giao dịch...*). Và được cấp phép thành lập, tức không tự do muốn lập là lập, mà cần xin phép cơ quan có thẩm quyền (*có thể Thủ tướng hoặc Bộ KH&CN tùy quy định cụ thể*). Việc cấp phép này tương tự như cấp phép sàn giao dịch chứng khoán hay sàn thương mại điện tử đặc thù, nhằm đảm bảo chỉ chủ thể có năng lực và đáng tin cậy mới tham gia.

Như vậy, ít nhất giai đoạn đầu, khu vực tư nhân thuận túy chưa được tự mở sàn dữ liệu. Đây là điểm khác so với một số nước phương Tây nơi các công ty công nghệ có thể tự xây dựng data marketplace. Song hoàn toàn hợp lý với điều kiện Việt Nam khi dữ liệu là lĩnh vực mới, nhà nước muốn chủ động kiểm soát để tránh các nguy cơ (*chẳng hạn sàn dữ liệu tư nhân có thể buôn bán dữ liệu nhạy cảm vượt kiểm soát*). Mặt khác, nhà nước cũng có lợi thế vì nắm giữ nhiều nguồn



dữ liệu công quý giá, việc tự tổ chức sàn giúp khai thác nguồn lực đó phục vụ phát triển kinh tế - xã hội, thay vì để tư nhân thao túng.

Một nội dung rất quan trọng tại khoản 3 Điều 42: quy định dữ liệu không được phép giao dịch trên sàn. Luật liệt kê các loại dữ liệu cấm giao dịch, gồm:

(<sup>1</sup>)Dữ liệu gây nguy hại đến quốc phòng, an ninh, đối ngoại, cơ yếu: chủ yếu là dữ liệu thuộc phạm trù bí mật nhà nước hoặc nhạy cảm an ninh (*cơ yếu, lĩnh vực mật mã nhà nước*). Rõ ràng những dữ liệu này bị cấm mua bán trao đổi dưới mọi hình thức. Ví dụ: dữ liệu về kế hoạch quốc phòng, tình báo, dữ liệu về hệ thống an ninh quốc gia... không được đưa lên sàn.

(<sup>2</sup>)Dữ liệu không được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác. Loại này chủ yếu ám chỉ dữ liệu cá nhân, nếu cá nhân chưa đồng ý cho giao dịch dữ liệu của họ thì sàn không được cho mua bán. Thậm chí ngay cả khi cá nhân đồng ý, sàn vẫn phải tuân thủ các luật liên quan (ví dụ Nghị định 13/2023/NĐ-CP yêu cầu đăng ký nếu xử lý dữ liệu cá nhân nhạy cảm). Quy định này nhằm bảo vệ quyền riêng tư, không ai có thể tự ý đưa dữ liệu cá nhân người khác lên sàn bán nếu chưa có sự chấp thuận. Tất nhiên có ngoại lệ “pháp luật có quy định khác”, chẳng hạn cơ quan nhà nước có thể chia sẻ dữ liệu cá nhân vì mục đích công vụ theo Luật (*không cần sự đồng ý*), nhưng đó không phải “giao dịch sàn dữ liệu” theo nghĩa thương mại.

(<sup>3</sup>)Dữ liệu khác bị cấm giao dịch theo quy định pháp luật. Đây là điều khoản mở, dẫn chiếu đến bất kỳ quy định nào khác cấm buôn bán dữ liệu loại cụ thể nào. Ví dụ: pháp luật về văn hóa cấm mua bán dữ liệu di sản văn hóa bất hợp pháp; pháp luật về y tế cấm mua bán dữ liệu hồ sơ bệnh án tràn lan; hay Luật An toàn thông tin mạng cấm mua bán trái phép thông tin riêng tư của tổ chức, cá nhân. Nếu luật chuyên ngành đã cấm, thì trên sàn cũng nghiêm cấm.

Quy định cấm giao dịch dữ liệu này rất quan trọng để định hướng phát triển sàn dữ liệu lành mạnh. Sàn chỉ được giao dịch những dữ liệu “sạch”, hợp pháp. Bất cứ dữ liệu nào nhạy cảm đều cấm hoặc phải lọc ra. Điều này tương tự cách quản lý sàn giao dịch các tài sản đặc biệt, ví dụ sàn chứng khoán cấm giao dịch



cô phiếu không đăng ký; sàn thương mại điện tử cấm bán hàng quốc cấm. Đối với dữ liệu vốn là một loại hàng hóa vô hình thì càng cần quy định để tránh vi phạm. Luật đã đưa ra khung, sau này Chính phủ có thể cụ thể hóa thêm danh mục dữ liệu cấm giao dịch. Ví dụ: có thể liệt kê dữ liệu chứa bí mật đòi tư, dữ liệu về trẻ em, dữ liệu ADN, dữ liệu vị trí cá nhân... (*những loại nhạy cảm cao*) là cấm.

Nhìn sang quốc tế, Đạo luật Data Governance Act của Liên minh Châu Âu cũng đề cập khái niệm “data altruism” khuyến khích chia sẻ dữ liệu vì mục đích lợi ích chung, đồng thời bảo vệ dữ liệu cá nhân nghiêm ngặt. Họ yêu cầu các dịch vụ trung gian dữ liệu phải tách bạch dữ liệu nhạy cảm, tuân thủ Quy định Bảo vệ Dữ liệu chung của Liên Minh Châu Âu khi có dữ liệu cá nhân. Trung Quốc khi xây dựng các sàn dữ liệu thí điểm tại Thâm Quyến, Thiên Tân cũng đặt ra danh mục dữ liệu cấm giao dịch (*thường trùng với bí mật nhà nước, dữ liệu cá nhân nhạy cảm*). Do đó, quy định của Điều 42 khoản 3 không khác biệt nhiều so với thông lệ.

Tổng thể, Điều 42 cho thấy Việt Nam hướng tới mô hình sàn giao dịch dữ liệu do nhà nước dẫn dắt. Các sàn này sẽ tạo hạ tầng thị trường để dữ liệu lưu thông có kiểm soát, giúp “mở cánh cửa” thị trường dữ liệu nhưng vẫn bảo đảm chủ quyền và an ninh dữ liệu. Ví dụ: sàn dữ liệu quốc gia có thể cho phép doanh nghiệp khởi nghiệp tiếp cận một phần dữ liệu công (*đã ẩn danh*) để phát triển sản phẩm AI, đổi lại doanh nghiệp đóng phí hoặc chia sẻ lại kết quả cho nhà nước. Đây là mô hình win-win từng được áp dụng ở một số nước như Singapore (*cổng dữ liệu Data.gov.sg và các chương trình sandbox dữ liệu cho startup*), Hàn Quốc trung tâm dữ liệu mở hỗ trợ doanh nghiệp vừa và nhỏ)...

Tuy nhiên, việc giới hạn chủ thể vận hành sàn dữ liệu cũng đặt ra bài toán, liệu khu vực tư nhân có thể tham gia không và nếu có thì dưới hình thức nào? Có thể tương lai nhà nước sẽ cho phép liên doanh công - tư vận hành sàn, hoặc cấp phép tư nhân khi thị trường “trưởng thành” hơn. Bởi lẽ, nguồn lực công có hạn, trong khi dữ liệu trong xã hội rất phong phú. Nếu quá hạn chế, sợ rằng thị trường ngầm trao đổi dữ liệu sẽ vẫn tồn tại ngoài luồng.



Tóm lại, Điều 42 xác lập khuôn khổ pháp lý nền tảng cho việc xây dựng các sàn giao dịch dữ liệu tại Việt Nam, bao gồm mục tiêu của sàn, ai được lập sàn và giới hạn những gì không được giao dịch. Đây là bước đầu cho một thị trường mà ở đó dữ liệu trở thành hàng hóa hợp pháp, có giá trị. Để triển khai, cần thêm nhiều hướng dẫn chi tiết về tiêu chuẩn kỹ thuật sàn (*đảm bảo tốc độ truy cập, an toàn mạng*), cơ chế giám sát giao dịch trên sàn, chính sách giá dữ liệu, chia sẻ doanh thu, giải quyết tranh chấp. Song, với quy định khá chặt chẽ của luật, có thể kỳ vọng những sàn dữ liệu đầu tiên sẽ ra mắt trong tương lai gần theo mô hình thí điểm có sự bảo trợ của Nhà nước, sau đó dần mở rộng.

#### **7.1.5. Trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ dữ liệu**

Điều 43 quy định các trách nhiệm chung của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu, sàn dữ liệu. Đây là các nghĩa vụ mà mọi doanh nghiệp kinh doanh các dịch vụ dữ liệu (*được nêu ở các điều 40-42*) đều phải tuân thủ khi hoạt động. Điều luật này rất quan trọng vì nó đặt ra chuẩn mực vận hành an toàn, tin cậy cho các nhà cung cấp dịch vụ dữ liệu, cũng là yếu tố then chốt để thị trường dữ liệu phát triển bền vững. Các trách nhiệm chính bao gồm:

(i) Cung cấp dịch vụ trên cơ sở hợp đồng: Tổ chức cung cấp dịch vụ dữ liệu phải ký kết hợp đồng với khách hàng (*tổ chức, cá nhân sử dụng dịch vụ*) theo thỏa thuận giữa các bên. Hợp đồng là cơ sở pháp lý ràng buộc quyền và nghĩa vụ, do đó yêu cầu này bảo vệ cả nhà cung cấp lẫn người dùng. Ví dụ: công ty trung gian dữ liệu cần có hợp đồng với bên cung cấp dữ liệu về việc môi giới dữ liệu, hoặc sàn dữ liệu cần có thỏa thuận người dùng về điều khoản giao dịch. Hợp đồng dịch vụ dữ liệu cũng có thể giúp xác định rõ phạm vi sử dụng dữ liệu, phí dịch vụ, trách nhiệm bồi thường nếu vi phạm... Trên thực tế, việc lập hợp đồng ở Việt Nam đôi khi bị xem nhẹ (*nhiều giao dịch bằng niềm tin miệng*), nhưng với lĩnh vực dữ liệu nhạy cảm, luật bắt buộc văn bản hóa hợp đồng. Điều này cũng tương tự yêu cầu tại châu Âu, khi các nhà cung cấp dịch vụ chia sẻ dữ liệu phải có thỏa thuận sử



dụng dữ liệu (*Data Sharing Agreement*) với các điều khoản tiêu chuẩn để bảo vệ bên cung cấp dữ liệu.

(2) Bảo đảm kênh tiếp nhận thông tin và dịch vụ thông suốt, liên tục: Nhà cung cấp phải duy trì hệ thống hạ tầng kỹ thuật để dịch vụ dữ liệu luôn sẵn sàng, ổn định, hạn chế tối đa gián đoạn. Dữ liệu thường được sử dụng theo thời gian thực hoặc phục vụ quyết định quan trọng, nên nếu kênh dịch vụ bị gián đoạn sẽ gây thiệt hại lớn. Trách nhiệm này tương tự cam kết SLA (*Service Level Agreement*) trong lĩnh vực CNTT, yêu cầu về độ sẵn sàng (*uptime*) của dịch vụ. Để tuân thủ, các doanh nghiệp dữ liệu phải đầu tư hệ thống máy chủ, đường truyền dự phòng, cơ chế giám sát 24/7, có trung tâm hỗ trợ khách hàng... Ví dụ: một sàn dữ liệu quốc gia phải hoạt động liên tục, nếu thời gian tải dữ liệu kéo dài có thể ảnh hưởng đến nhiều doanh nghiệp đang lấy dữ liệu từ sàn. Luật không quy định cụ thể mức độ thông suốt (*99% uptime hay khác*) nhưng chắc chắn Chính phủ sẽ có hướng dẫn hoặc tiêu chuẩn riêng.

(3) Quản lý, kiểm tra, giám sát an toàn dữ liệu, bảo mật dữ liệu thường xuyên; phòng ngừa, ngăn chặn và xử lý rủi ro dữ liệu; giám sát hành vi có thể ảnh hưởng đến bảo vệ dữ liệu. Đây là một trách nhiệm rất quan trọng, yêu cầu nhà cung cấp dịch vụ dữ liệu phải thực hiện đầy đủ các biện pháp bảo đảm an toàn thông tin và quản trị rủi ro dữ liệu. Cụ thể bao gồm:

- **Thứ nhất**, xây dựng hệ thống quản lý an toàn dữ liệu: ví dụ phân quyền truy cập dữ liệu hợp lý, mã hóa dữ liệu khi lưu trữ và truyền tải, sao lưu dữ liệu định kỳ, kiểm tra lỗ hổng bảo mật,...

- **Thứ hai**, kiểm tra, giám sát thường xuyên: liên tục theo dõi hệ thống phát hiện truy cập trái phép, rò rỉ dữ liệu; gắn thiết bị giám sát an ninh mạng (*IDS/IPS, firewall*) để kịp thời phát hiện cuộc tấn công; giám sát hành vi người dùng trên nền tảng (*phát hiện người tải lượng dữ liệu bất thường có thể là đánh cắp...*).

- **Thứ ba**, phòng ngừa rủi ro dữ liệu: rủi ro có thể là mất dữ liệu, lộ dữ liệu, dữ liệu bị sửa đổi. Nhà cung cấp cần có kế hoạch ứng phó như kế hoạch sao lưu và khôi phục dữ liệu sau thảm họa, kế hoạch ứng cứu sự cố an toàn thông tin.



- **Thứ tư**, xử lý rủi ro dữ liệu: khi xảy ra sự cố (*nếu bị hack, lộ thông tin người dùng*), phải có quy trình cô lập, vá lỗ hổng, thông báo cho cơ quan chức năng và khách hàng bị ảnh hưởng,... Hiện nay, Luật An toàn thông tin mạng 2015 và Luật An ninh mạng 2018 đều có yêu cầu chung về việc tổ chức vận hành hệ thống thông tin phải bảo đảm an toàn, thông báo sự cố cho cơ quan quản lý (Ví dụ: *Trung tâm dữ liệu quốc gia*). Điều 43 bổ sung nhấn mạnh riêng cho các công ty dịch vụ dữ liệu, do dữ liệu là hàng hóa chính của họ nên càng phải chú trọng bảo mật.

- **Thứ năm**, giám sát hành vi có thể ảnh hưởng bảo vệ dữ liệu: tức không chỉ chống tấn công từ bên ngoài, mà còn giám sát nội bộ, giám sát người dùng. Ví dụ: phát hiện một nhân viên nội bộ truy xuất và copy lượng lớn dữ liệu khách hàng ra ngoài, đó là hành vi bất thường cần ngăn chặn (*tránh trường hợp lộ dữ liệu khách hàng do nội gián*). Hoặc giám sát người dùng sàn dữ liệu xem họ có có vượt tường lửa để xem dữ liệu cấm không.

Tóm lại, điểm (3) đòi hỏi doanh nghiệp phải có năng lực đảm bảo an ninh, an toàn dữ liệu ở mức cao. Điều này phù hợp vì các dịch vụ dữ liệu nếu xảy ra sự cố lộ dữ liệu cá nhân hay dữ liệu nhạy cảm sẽ ảnh hưởng nhiều người, gây mất niềm tin. Thực tế, các quy định tương tự cũng có ở nước ngoài; Ví dụ: Điều 25 của Luật Dữ liệu 2024 yêu cầu chủ quản dữ liệu đánh giá rủi ro thường xuyên và báo cáo cơ quan an ninh mạng. Ở Liên minh Châu Âu, nhà cung cấp dịch vụ dữ liệu phải tuân thủ cả GDPR (*an ninh dữ liệu cá nhân*) lẫn NIS2 (*chỉ thị an ninh mạng cho dịch vụ số*). Luật An ninh mạng Việt Nam 2018 cũng quy định chế tài xử phạt nặng nếu tổ chức để lộ dữ liệu cá nhân số lượng lớn.

<sup>(4)</sup>Tuân thủ pháp luật về an toàn thông tin mạng, an ninh mạng, giao dịch điện tử và quy định liên quan. Đây là điều khoản dẫn chiếu, khẳng định rằng ngoài Luật Dữ liệu, các nhà cung cấp dịch vụ dữ liệu phải chấp hành đầy đủ các luật hiện hành trong lĩnh vực tương ứng:

Luật An toàn thông tin mạng 2015: quy định về bảo vệ thông tin không phân loại nhà nước, chẳng hạn khi thu thập, xử lý dữ liệu phải được sự đồng ý của



chủ thẻ (*Điều 17*); quản lý hệ thống thông tin theo cấp độ an toàn... Nếu doanh nghiệp dịch vụ dữ liệu vi phạm (*ví dụ mua bán trái phép dữ liệu cá nhân*) có thể bị xử phạt theo luật này.

Luật An ninh mạng 2018 có một số yêu cầu đặc thù như lưu trữ dữ liệu người dùng Việt Nam trên lãnh thổ Việt Nam đối với các dịch vụ quan trọng; phải gỡ bỏ thông tin vi phạm pháp luật khi có yêu cầu từ Bộ Công an; phối hợp cho phép kiểm tra an ninh mạng khi cần. Các công ty cung cấp nền tảng dữ liệu lớn có thể thuộc phạm vi điều chỉnh của luật này (*nếu được coi là hệ thống thông tin quan trọng về an ninh quốc gia*). Do đó, họ phải có nghĩa vụ tương ứng (*ví dụ tuân thủ yêu cầu kiểm tra an ninh định kỳ*).

Luật Giao dịch điện tử 2023 quy định phải tuân thủ quy định về thông điệp dữ liệu, chữ ký số, hợp đồng điện tử, chứng từ điện tử... Nếu sàn dữ liệu có triển khai hợp đồng điện tử, chứng thực điện tử thì phải theo luật này. Mặc dù Luật Dữ liệu đã sửa đổi quy định trong Luật Giao dịch điện tử liên quan đến kết nối dữ liệu, nhưng những nguyên tắc chung vẫn áp dụng. Ví dụ: tính pháp lý của thông tin, tài liệu ở dạng điện tử trên sàn dữ liệu phải được thừa nhận như bản giấy, hoặc quy trình ký kết hợp đồng dịch vụ qua mạng phải tuân thủ điều kiện có hiệu lực của hợp đồng điện tử.

Quy định pháp luật khác liên quan: bao gồm bảo vệ người tiêu dùng (*nếu khách hàng là cá nhân*), cạnh tranh (*tránh hành vi độc quyền dữ liệu*), sở hữu trí tuệ (*dữ liệu có bản quyền*)...

Như vậy, Khoản 4 Điều 43 mang tính nhắc nhở tuân thủ toàn diện. Một doanh nghiệp kinh doanh dữ liệu phải cùng lúc ở vai trò doanh nghiệp công nghệ (*tuân thủ luật công nghệ thông tin, luật an toàn mạng*), doanh nghiệp dịch vụ (*tuân thủ luật bảo vệ khách hàng, quảng cáo...*) và luật chuyên ngành dữ liệu họ xử lý (*ví dụ phân tích dữ liệu y tế phải tuân thủ Luật Khám chữa bệnh về bảo mật thông tin bệnh nhân*).

Cuối cùng, khoản 5 Điều 43 giao Chính phủ quy định chi tiết điều này. Có thể Chính phủ sẽ ban hành các quy định cụ thể hơn về tiêu chuẩn an toàn dữ liệu,



quy trình báo cáo sự cố, hoặc mẫu hợp đồng cung cấp dịch vụ dữ liệu tối thiểu. Tương tự lĩnh vực viễn thông có Nghị định hướng dẫn về chất lượng dịch vụ, an toàn mạng cho nhà mạng, thì lĩnh vực dữ liệu cũng cần hướng dẫn để các doanh nghiệp thực thi thống nhất.

*Bảng: hệ thống trách nhiệm của nhà cung cấp dịch vụ dữ liệu:*

Nhóm trách nhiệm	Nội dung cụ thể	Cơ sở pháp lý liên quan
Giao kết hợp đồng	Cung cấp dịch vụ trên cơ sở hợp đồng với khách hàng, thỏa thuận rõ quyền nghĩa vụ	Bộ Luật dân sự 2015 về hợp đồng dịch vụ; Luật Giao dịch điện tử 2023 ( <i>hợp đồng điện tử</i> )
Đảm bảo tính sẵn sàng của dịch vụ	Duy trì kênh tiếp nhận thông tin và cung cấp dịch vụ thông suốt, liên tục	Tiêu chuẩn dịch vụ CNTT ( <i>uptime, SLA</i> ); Luật BVNTD nếu gián đoạn gây hại người dùng
Bảo mật và an toàn dữ liệu	Quản lý, kiểm tra, giám sát an toàn dữ liệu thường xuyên; phòng ngừa, ngăn chặn rủi ro mất an toàn; phát hiện và xử lý kịp thời sự cố, hành vi xâm phạm	Luật An toàn thông tin mạng 2015 ( <i>quản lý an toàn hệ thống</i> ); Luật An ninh mạng 2018 ( <i>bảo vệ hệ thống QG</i> ); Nghị định 13/2023 ( <i>xử lý vi phạm bảo vệ dữ liệu cá nhân</i> )
Bảo vệ quyền và lợi ích hợp pháp	Giám sát và ngăn chặn hành vi có thể ảnh hưởng đến việc bảo vệ dữ liệu ( <i>ví dụ truy cập trái phép, lạm dụng dữ liệu cá nhân</i> )	Luật ATTTM 2015, Luật ANM 2018; Bộ luật Hình sự ( <i>tội xâm nhập trái phép mạng</i> )
Tuân thủ pháp luật liên quan	Tuân thủ các luật: an toàn thông tin mạng, an ninh mạng, giao dịch điện tử và các quy định chuyên ngành khác khi cung cấp dịch vụ dữ liệu	Luật ATTTM 2015; Luật ANM 2018; Luật GDĐT 2023; các luật khác ( <i>bảo vệ NTD, sở hữu trí tuệ, cạnh tranh...</i> )



Việc quán triệt các nghĩa vụ trên sẽ giúp các nhà cung cấp dịch vụ dữ liệu vận hành một cách chuyên nghiệp và đáng tin cậy. Trong thị trường dữ liệu, niềm tin là yếu tố then chốt - nếu doanh nghiệp, người dân không tin rằng dữ liệu của họ an toàn khi giao cho nhà cung cấp dịch vụ, họ sẽ không tham gia thị trường. Luật Dữ liệu 2024 bằng Điều 43 đã cố gắng thiết lập ngưỡng chuẩn về an toàn, trách nhiệm cho các chủ thể kinh doanh dữ liệu. Thời gian tới, cơ quan quản lý (Bộ Thông tin và Truyền thông, Bộ Công an) sẽ cần giám sát chặt chẽ việc tuân thủ. Những vụ vi phạm (ví dụ để lộ lọt dữ liệu khách hàng từ sàn dữ liệu) phải được xử lý nghiêm, có thể bằng chế tài hành chính hoặc hình sự tùy mức độ. Điều đó tạo tính răn đe và thúc đẩy các doanh nghiệp đầu tư nhiều hơn vào bảo mật.

Thực tế, 21/2/2025 mới đây, Công an thành phố Huế vừa triệt phá đường dây mua bán gần 56 triệu thông tin dữ liệu cá nhân của cán bộ, công chức viên chức, người lao động ở nhiều tỉnh, thành trên cả nước. Theo đó, nhóm đối tượng đã mua lượng lớn thông tin dữ liệu cá nhân để sử dụng và bán trao tay, thu lợi bất chính khoảng 1 tỷ đồng.



Hình ảnh: Cơ quan ANĐT đọc lệnh bắt tạm giam nhóm đối tượng. Ảnh: CAND

Nếu có các sàn dữ liệu hợp pháp tuân thủ trách nhiệm như Điều 43, những dữ liệu cá nhân như vậy sẽ không bị tuồn ra chợ đen mà được kiểm soát trên chợ hợp pháp, có sự đồng ý của chủ thể. Đây chính là mục tiêu mà luật hướng đến,



thiết lập một thị trường dữ liệu hợp pháp, an toàn và đáng tin cậy, thay thế dần thị trường ngầm và hành vi vi phạm.

Kết lại, từ Điều 39 đến 43 Chương IV của Luật Dữ liệu 2024 đã tạo hành lang pháp lý nền tảng cho việc quản lý và phát triển các sản phẩm, dịch vụ dữ liệu số tại Việt Nam. Mỗi điều tập trung vào một khía cạnh: phân loại và phạm vi (Điều 39), điều kiện kinh doanh trung gian dữ liệu (Điều 40), điều kiện kinh doanh phân tích dữ liệu (Điều 41), tổ chức vận hành sàn dữ liệu (Điều 42) và nghĩa vụ chung của nhà cung cấp (Điều 43). Sự ra đời của các quy định này thể hiện tầm nhìn của Nhà nước trong việc biến dữ liệu thành một thị trường có trật tự, đồng thời bảo vệ chủ quyền dữ liệu quốc gia và quyền lợi của từng cá nhân, tổ chức trong nền kinh tế số. Với cơ sở pháp lý này, Việt Nam đặt nền móng để thúc đẩy kinh tế dữ liệu tăng trưởng, tận dụng nguồn "dầu mỏ số" hiệu quả, phục vụ sự thịnh vượng kinh tế - xã hội, nhưng vẫn giữ vững các giá trị về an ninh, an toàn, quyền riêng tư. Các ví dụ quốc tế từ Liên minh Châu Âu, Singapore, Hàn Quốc minh chứng rằng nếu thực thi tốt, khung pháp lý về dữ liệu sẽ trở thành đòn bẩy cho chuyển đổi số quốc gia, giúp Việt Nam sớm bắt nhịp xu hướng toàn cầu và chủ động hội nhập trong lĩnh vực dữ liệu số đầy cạnh tranh.

## **7.2. Các giải pháp bảo đảm an ninh, an toàn dữ liệu trong ứng dụng sản phẩm, dịch vụ dữ liệu**

### **7.2.1. Các quy định đảm bảo an ninh, an toàn dữ liệu**

Luật Dữ liệu năm 2024 đặt ra khung pháp lý cho việc xây dựng, phát triển, bảo vệ, quản trị, xử lý và sử dụng dữ liệu số; đồng thời thiết lập Trung tâm dữ liệu quốc gia và Cơ sở Dữ liệu tổng hợp quốc gia để phục vụ chuyển đổi số và phát triển kinh tế số. Một mục tiêu quan trọng của Luật Dữ liệu là bảo vệ và bảo đảm an ninh, an toàn, bảo mật dữ liệu trước các nguy cơ tấn công, xâm nhập, phá hoại hệ thống thông tin. Luật Dữ liệu yêu cầu hạ tầng trung tâm dữ liệu phải có giải pháp kỹ thuật bảo mật nhằm kiểm soát, phát hiện, ngăn chặn mọi hành vi tấn công, đột nhập trái phép, bảo đảm hệ thống luôn sẵn sàng và dự phòng mở rộng khi cần thiết, cụ thể:



**- Thứ nhất**, phân loại dữ liệu và dữ liệu cốt lõi: Luật yêu cầu các cơ quan nhà nước phải phân loại dữ liệu theo mức độ chia sẻ (*dùng chung, dùng riêng, dữ liệu mở*) và theo mức độ quan trọng (*dữ liệu cốt lõi, dữ liệu quan trọng, dữ liệu khác*). Dữ liệu quan trọng là dữ liệu có thể tác động đến quốc phòng, an ninh quốc gia, đối ngoại, kinh tế vĩ mô, trật tự xã hội, sức khỏe cộng đồng... theo danh mục do Thủ tướng Chính phủ ban hành. Dữ liệu cốt lõi là tập hợp con của dữ liệu quan trọng, có ảnh hưởng trực tiếp đến các lĩnh vực trên, cũng do Thủ tướng quy định danh mục. Việc phân loại này giúp xác định dữ liệu nào cần cơ chế bảo vệ nghiêm ngặt nhất. Luật giao Chính phủ ban hành tiêu chí xác định dữ liệu cốt lõi, quan trọng. Đồng thời, Điều 14 Luật Dữ liệu quy định nếu tổ chức, cá nhân lưu trữ dữ liệu cốt lõi, dữ liệu quan trọng thì phải tuân thủ các yêu cầu bảo vệ dữ liệu chặt chẽ theo khoản 3 Điều 27 của Luật (*quy định chủ quản dữ liệu cốt lõi, quan trọng phải tuân thủ các biện pháp bảo vệ dữ*). Như vậy, pháp luật bắt buộc bảo vệ đặc biệt đối với dữ liệu cốt lõi và dữ liệu quan trọng vì đây là những tài sản số có giá trị cao đối với quốc gia và tổ chức.

**- Thứ hai**, Chương II Luật Dữ liệu quy định về bảo vệ, quản trị dữ liệu, bảo vệ dữ liệu và an toàn thông tin.

+ Điều 25 yêu cầu các chủ thể xác định và quản lý rủi ro phát sinh trong quá trình xử lý dữ liệu, bao gồm: rủi ro quyền riêng tư, rủi ro an ninh mạng, rủi ro về định danh 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 xây dựng biện pháp bảo vệ dữ liệu tương ứng. Chủ quản các dữ liệu cốt lõi, quan trọng được yêu cầu định kỳ đánh giá rủi ro đối với hoạt động xử lý dữ liệu và thông báo cho đơn vị chuyên trách về an ninh mạng, an toàn thông tin (*thuộc Bộ Công an, Bộ Quốc phòng*) để phối hợp bảo vệ an toàn dữ liệu. Quy định này nhấn mạnh việc phối hợp với cơ quan chuyên trách nhằm bảo vệ dữ liệu trọng yếu khỏi các mối đe dọa trên không gian mạng.

+ Điều 27 về bảo vệ dữ liệu liệt kê các biện pháp bảo vệ dữ liệu phải được áp dụng xuyên suốt quá trình xử lý dữ liệu. Bao gồm: <sup>(1)</sup>Xây dựng và thực thi chính sách, quy định nội bộ về bảo vệ dữ liệu; <sup>(2)</sup>Quản lý chặt chẽ hoạt động xử lý



dữ liệu (ví dụ phân quyền, kiểm soát truy cập); <sup>(3)</sup> Triển khai các giải pháp kỹ thuật bảo mật (mã hóa, sao lưu, tường lửa...); <sup>(4)</sup> Đào tạo, bồi dưỡng và quản lý nguồn nhân lực về an toàn dữ liệu; <sup>(5)</sup> Các biện pháp khác theo quy định pháp luật. Như vậy, Luật yêu cầu một hệ thống biện pháp toàn diện gồm cả kỹ thuật, tổ chức, con người để bảo vệ dữ liệu. Đối với cơ quan nhà nước, Luật bắt buộc thiết lập hệ thống bảo vệ dữ liệu thống nhất nhằm đánh giá rủi ro an ninh, giám sát và cảnh báo sớm các nguy cơ. Chủ sở hữu/chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải tuân thủ đầy đủ các quy định bảo vệ dữ liệu này. Quy định này đảm bảo các dữ liệu “nhạy cảm” nhất được bảo vệ nghiêm ngặt và yêu cầu các cơ quan nhà nước chủ động giám sát an ninh dữ liệu trong lĩnh vực mình quản lý.

- **Thứ ba**, quy định về Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia:

+ Điều 30 quy định hạ tầng của Trung tâm dữ liệu quốc gia phải đáp ứng tiêu chuẩn trung tâm dữ liệu quốc tế và có giải pháp an ninh, bảo mật để kiểm soát, phát hiện, ngăn chặn tấn công, đột nhập, phá hoại; đồng thời đảm bảo hệ thống dự phòng và mở rộng khi cần. Trung tâm dữ liệu quốc gia sẽ tích hợp các thành phần quan trọng như Cơ sở dữ liệu tổng hợp Quốc gia, nền tảng chia sẻ dữ liệu, cổng dữ liệu, hệ thống phân tích dữ liệu... trên một hạ tầng an toàn, chống chịu được các mối đe dọa (*khủng bố, thiên tai*).

+ Điều 31 quy định trách nhiệm của Trung tâm dữ liệu quốc gia trong vận hành và bảo vệ dữ liệu: lưu trữ, khai thác dữ liệu tập trung; cung cấp hạ tầng cho các cơ quan khi cần; giám sát bảo đảm chất lượng dữ liệu và thực hiện các biện pháp bảo vệ dữ liệu. Như vậy, Trung tâm dữ liệu quốc gia đóng vai trò hạt nhân trong bảo đảm an toàn cho hệ thống dữ liệu quốc gia, vừa là nơi lưu trữ tập trung, vừa có nhiệm vụ triển khai các biện pháp kỹ thuật và quy trình vận hành an toàn. Cùng với đó, Cơ sở Dữ liệu tổng hợp quốc gia (*đặt tại Trung tâm dữ liệu quốc gia*) phải được xây dựng đáp ứng các yêu cầu an ninh, an toàn thông tin và bảo vệ dữ liệu cá nhân; đảm bảo hoạt động ổn định, liên tục, kết nối thông suốt với các Cơ sở dữ liệu khác. Đây là yêu cầu pháp lý để



kiến trúc Cơ sở dữ liệu Quốc gia có tích hợp sẵn các lớp bảo mật và tuân thủ luật bảo vệ dữ liệu cá nhân.

- **Thứ tư**, Chương IV Luật Dữ liệu quy định về sản phẩm, dịch vụ dữ liệu điều chỉnh hoạt động cung cấp sản phẩm, dịch vụ trung gian dữ liệu, dịch vụ phân tích dữ liệu và sàn giao dịch dữ liệu. Các quy định này ràng buộc các doanh nghiệp kinh doanh dịch vụ dữ liệu phải tuân thủ chặt chẽ yêu cầu về an toàn, bảo mật. Cụ thể, Điều 43 quy định trách nhiệm của tổ chức cung cấp dịch vụ dữ liệu gồm: đảm bảo kênh dịch vụ thông suốt, liên tục; quản lý, kiểm tra, giám sát an toàn dữ liệu thường xuyên; phòng ngừa, ngăn chặn và xử lý rủi ro dữ liệu; giám sát các hành vi có thể ảnh hưởng đến bảo vệ dữ liệu. Đặc biệt, các tổ chức này phải tuân thủ pháp luật về an toàn thông tin mạng và an ninh mạng cùng các quy định liên quan. Như vậy, nhà cung cấp dịch vụ dữ liệu có nghĩa vụ thiết lập hệ thống bảo mật, giám sát 24/7, xử lý kịp thời sự cố và tuân thủ các luật chuyên ngành về an ninh mạng, an toàn thông tin. Ví dụ: doanh nghiệp sàn giao dịch dữ liệu không được phép cho giao dịch những dữ liệu bị cấm (*dữ liệu gây phương hại quốc phòng, an ninh; dữ liệu cá nhân chưa có sự đồng ý chủ thẻ...*). Những quy định này nhằm bảo đảm thị trường dữ liệu phát triển lành mạnh và an toàn, tránh việc lợi dụng mua bán dữ liệu nhạy cảm, trái phép.

- **Thứ năm**, Luật Giao dịch điện tử 2023, Luật Viễn thông 2024

Bên cạnh Luật Dữ liệu, các luật mới như Luật Giao dịch điện tử (*sửa đổi 2023*) và Luật Viễn thông (*sửa đổi 2024*) cũng có một số quy định liên quan đến bảo đảm an toàn thông tin và dữ liệu trong hoạt động giao dịch điện tử, viễn thông. Các luật này cùng với Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018 tạo thành khung khổ pháp lý tổng thể về an ninh, an toàn không gian mạng tại Việt Nam. Luật Dữ liệu 2024 dẫn chiếu: trường hợp luật khác (ví dụ *Luật An toàn thông tin mạng, Luật An ninh mạng*) có quy định về an toàn thông tin và bảo vệ dữ liệu thì tổ chức, cá nhân phải tuân thủ các quy định đó song song với Luật Dữ liệu.



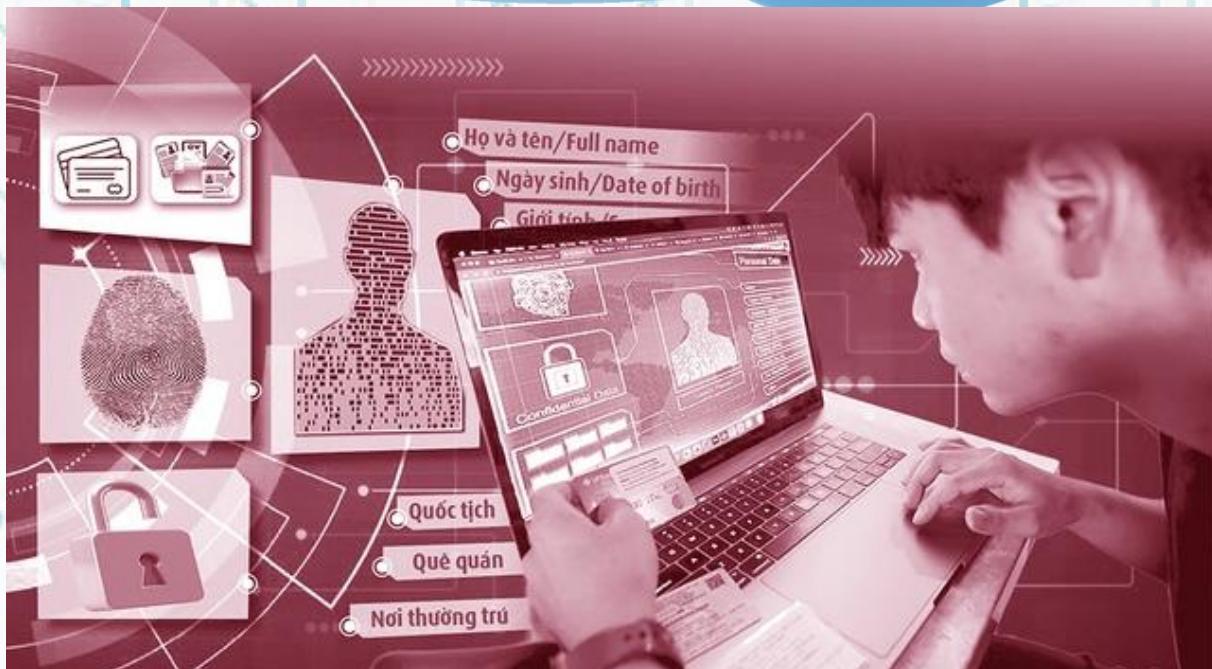
- **Thứ sáu,** Luật An toàn thông tin mạng 2015 và Luật An ninh mạng 2018
  - + Luật An toàn thông tin mạng năm 2015 quy định về bảo đảm an toàn thông tin trên mạng, bao gồm các yêu cầu kỹ thuật, tiêu chuẩn và việc phân loại hệ thống thông tin theo cấp độ để áp dụng biện pháp bảo vệ phù hợp. Theo luật và các nghị định hướng dẫn, hệ thống thông tin của các cơ quan, tổ chức Việt Nam được phân loại thành 5 cấp độ an toàn; hệ thống cấp độ càng cao (*đặc biệt cấp 4,5 - hệ thống quan trọng quốc gia*) càng phải tuân thủ tiêu chuẩn bảo mật nghiêm ngặt (*mã hóa, kiểm soát truy cập, sao lưu dự phòng, diễn tập an ninh mạng định kỳ...*). Việc bảo đảm an toàn hệ thống thông tin theo cấp độ là bắt buộc; nếu không thực hiện đánh giá, thẩm định và phê duyệt hồ sơ phân loại cấp độ sẽ bị xử phạt hành chính. Quy định này góp phần bảo vệ dữ liệu bên trong các hệ thống CNTT của cơ quan nhà nước và doanh nghiệp theo mức độ quan trọng của hệ thống đó.
  - + Luật An ninh mạng 2018 tập trung vào bảo vệ an ninh quốc gia trên không gian mạng. Luật An ninh mạng yêu cầu các cơ quan, doanh nghiệp vận hành hệ thống thông tin quan trọng về an ninh quốc gia phải tuân thủ các biện pháp bảo vệ đặc biệt và chịu sự kiểm tra về an ninh mạng của Bộ Công an. Luật An ninh mạng định nghĩa an ninh mạng là trạng thái đảm bảo hoạt động trên không gian mạng không gây phuơng hại đến an ninh quốc gia, trật tự an toàn xã hội, quyền lợi hợp pháp của cơ quan, tổ chức, cá nhân. Các hành vi như tấn công mạng, gián điệp mạng bị nghiêm cấm và sẽ bị xử lý hình sự nghiêm khắc. Luật An ninh mạng cũng đặt ra nghĩa vụ cho doanh nghiệp cung cấp dịch vụ mạng (*ví dụ Facebook, Google*) phải lưu trữ dữ liệu người dùng Việt Nam trong nước và tuân thủ yêu cầu bảo mật, cung cấp thông tin cho cơ quan chức năng khi cần (*điều này liên quan đến chủ quyền dữ liệu và phòng chống tội phạm mạng*). Luật An ninh mạng năm 2018 là cơ sở để cơ quan chức năng phòng ngừa, phát hiện, ngăn chặn, xử lý các hành vi xâm hại an ninh mạng, qua đó gián tiếp bảo vệ an toàn dữ liệu trọng yếu của quốc gia và tổ chức.



## - *Thứ bảy*, quy định về bảo vệ dữ liệu cá nhân:

Song song với Luật Dữ liệu, Việt Nam đã ban hành Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, có hiệu lực từ 7/2023. Nghị định 13/2023 định nghĩa rõ dữ liệu cá nhân gồm dữ liệu cơ bản và dữ liệu cá nhân nhạy cảm. Dữ liệu cá nhân nhạy cảm là dữ liệu gắn liền quyền riêng tư (*quan điểm chính trị, tình trạng sức khỏe, đời sống tình dục, thông tin sinh trắc học, thông tin tài chính, vị trí cá nhân,...*) mà khi bị xâm phạm có thể ảnh hưởng trực tiếp đến quyền, lợi ích hợp pháp của cá nhân. Ví dụ: thông tin về tôn giáo, tình trạng sức khỏe, dữ liệu về tội phạm, thông tin sinh học riêng... được xếp vào loại nhạy cảm cần bảo vệ đặc biệt. Nghị định yêu cầu tổ chức, cá nhân phải có biện pháp bảo mật cần thiết đối với dữ liệu nhạy cảm và chỉ được xử lý khi có sự đồng ý rõ ràng của chủ thẻ dữ liệu (*trừ trường hợp luật cho phép*). Bảo vệ dữ liệu cá nhân được định nghĩa là các hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân.

Đến tháng 6/2025, Quốc hội đã thông qua Luật Bảo vệ Dữ liệu Cá nhân 2025 (số 91/2025/QH15) nhằm luật hóa các quy định của Nghị định 13/2023/NĐ-CP và nâng tầm bảo vệ dữ liệu cá nhân. Luật này (*có hiệu lực từ 01/01/2026*) tái khẳng định nguyên tắc: chỉ được thu thập, xử lý dữ liệu cá nhân trong phạm vi mục đích rõ ràng và phải có căn cứ pháp lý, trong đó sự đồng ý tự nguyện, rõ ràng của chủ thẻ dữ liệu là căn cứ quan trọng hàng đầu. Mọi việc chia sẻ, mua bán dữ liệu cá nhân không có sự đồng ý đều bị coi là vi phạm nghiêm trọng. Luật Bảo vệ Dữ liệu Cá nhân 2025 yêu cầu bên kiểm soát dữ liệu phải thực hiện đánh giá tác động xử lý dữ liệu cá nhân và gửi báo cáo đến cơ quan chuyên trách trong vòng 60 ngày kể từ khi bắt đầu xử lý dữ liệu. Việc đánh giá này giúp xác định trước các rủi ro và biện pháp giảm thiểu đối với dữ liệu cá nhân sẽ xử lý. Ngoài ra, luật quy định thông báo vi phạm, nếu phát hiện vi phạm bảo vệ dữ liệu cá nhân gây ảnh hưởng nghiêm trọng, bên kiểm soát phải thông báo cho cơ quan chuyên trách trong vòng 72 giờ. Đây là cơ chế quan trọng để nhà chức trách giám sát, kịp thời can thiệp khi xảy ra lỗ hổng, sự cố rò rỉ dữ liệu cá nhân trên diện rộng.



*Việc mua bán dữ liệu được công khai trên mạng. Ảnh: Báo Thanh niên*

Tổng hợp lại, hệ thống pháp luật Việt Nam hiện hành đã và đang hình thành khung pháp lý khá đầy đủ cho việc bảo đảm an ninh, an toàn dữ liệu. Luật Dữ liệu 2024 tạo nền tảng chung về quản trị và bảo vệ dữ liệu số; Luật An toàn thông tin mạng 2015 và Luật An ninh mạng 2018 đảm bảo an ninh hệ thống và không gian mạng; Luật Bảo vệ dữ liệu cá nhân 2025, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân chuyên sâu vào quyền riêng tư và an toàn dữ liệu cá nhân. Các luật này có mối quan hệ bổ trợ cho nhau, Khoản 4, Điều 43 Luật Dữ liệu yêu cầu tổ chức cung cấp dịch vụ dữ liệu phải tuân thủ cả luật an toàn thông tin mạng và luật an ninh mạng; đồng thời bảo vệ dữ liệu cá nhân cũng được đề cập trong Luật Dữ liệu như một nguyên tắc cơ bản. Vì vậy, khi triển khai các giải pháp an toàn dữ liệu, các tổ chức cần đồng thời đáp ứng các yêu cầu của nhiều văn bản pháp luật liên quan.

### **7.2.2. Các giải pháp kỹ thuật - công nghệ bảo đảm an toàn dữ liệu**

Các giải pháp kỹ thuật - công nghệ đóng vai trò chủ chốt trong việc hiện thực hóa các yêu cầu pháp lý về an toàn dữ liệu. Cụ thể:

- **Mật mã**, mã hóa dữ liệu: Mã hóa là “chìa khóa” để bảo vệ tính bí mật của dữ liệu. Luật Dữ liệu định nghĩa mã hóa dữ liệu là việc chuyển đổi dữ liệu từ định



dạng nhận biết được sang định dạng không thể nhận biết, thông qua thuật toán hoặc giải pháp kỹ thuật. Triển khai mã hóa đảm bảo rằng dữ liệu nếu bị truy cập trái phép cũng không thể hiểu được nội dung. Có hai loại mã hóa chính: mã hóa khi lưu trữ (*encryption at rest*) áp dụng cho dữ liệu trong cơ sở dữ liệu, ổ đĩa và mã hóa khi truyền (*encryption in transit*) áp dụng cho dữ liệu khi trao đổi qua mạng. Ví dụ: một cơ quan có thể mã hóa toàn bộ trường dữ liệu nhạy cảm (số CMND/CCCD, *hồ sơ sức khỏe...*) trong cơ sở dữ liệu. Chỉ những người có khóa giải mã hợp lệ mới đọc được nội dung gốc. Tương tự, khi truyền dữ liệu qua Internet cần sử dụng giao thức HTTPS/TLS để mã hóa dòng thông tin. Mã hóa mạnh (*sử dụng thuật toán hiện đại như AES-256*) kết hợp quản lý khóa an toàn sẽ ngăn chặn hiệu quả nguy cơ rò rỉ dữ liệu kể cả khi hacker xâm nhập được hệ thống. Ngoài ra, giải pháp mã hóa đồng bộ, liên tục nên được tích hợp ở cấp ứng dụng, cơ sở dữ liệu lẫn thiết bị lưu trữ để tạo nhiều lớp bảo vệ. Luật cũng đề cập đến giải mã dữ liệu, chỉ những chủ thẻ được cấp phép mới thực hiện giải mã để truy cập dữ liệu gốc. Việc quản lý chặt chẽ khóa mã (*mã hóa khóa bí mật trong HSM, phân quyền truy cập khóa*) cũng là một phần quan trọng của giải pháp mã hóa toàn diện.

- **Hai là**, quản lý định danh và kiểm soát truy cập: Xác thực và phân quyền người dùng truy cập dữ liệu là lớp phòng thủ đầu tiên trước nguy cơ truy cập trái phép. Mỗi người dùng/hệ thống phải có một định danh duy nhất và được quản lý qua hệ thống định danh tin cậy (*hệ thống xác thực điện tử quốc gia*). Thực hiện xác thực đa yếu tố (*MFA*) giúp tăng cường độ tin cậy (*ví dụ yêu cầu cả mật khẩu và OTP hoặc sinh trắc học khi đăng nhập hệ thống quan trọng*). Sau khi xác thực, cần áp dụng nguyên tắc phân quyền tối thiểu (*least privilege*), mỗi người dùng chỉ được cấp quyền cần thiết tối thiểu trên những dữ liệu cần truy cập. Việc phân quyền chi tiết tới mức từng trường dữ liệu, từng chức năng (*CRUD: Create-Read-Update-Delete*) giúp giảm nguy cơ lạm dụng. Các hệ thống hiện đại thường triển khai mô hình Zero Trust, luôn xác thực và kiểm tra quyền mỗi khi truy cập tài nguyên, thay vì tin cậy mặc định bất kỳ ai. Luật Dữ liệu yêu cầu cơ quan nhà nước phải cung cấp công cụ và phân quyền truy cập, truy xuất dữ liệu một cách an toàn.



Điều này có nghĩa là các hệ thống dữ liệu phải tích hợp các giải pháp như quản lý truy cập dựa trên vai trò hoặc dựa trên thuộc tính, đồng thời ghi nhật ký mọi hoạt động truy cập. Nhật ký truy cập sẽ phục vụ truy vết khi có sự cố an ninh và đảm bảo tính tuân thủ. Ngoài ra, cơ chế Single Sign-On (SSO) kết hợp với quản lý phiên đăng nhập chặt chẽ sẽ giúp quản lý danh tính người dùng hiệu quả hơn, tránh tình trạng tài khoản “ma” hoặc phiên làm việc không hợp lệ.

- **Ba là**, giải pháp Sandbox (*khu vực cách ly*): Sandbox là môi trường tách biệt dùng để chạy thử nghiệm mã độc, ứng dụng mới hoặc cách ly các tiến trình có độ rủi ro, nhằm ngăn chặn ảnh hưởng tới hệ thống chính. Trong bối cảnh an toàn dữ liệu, sandbox có thể được sử dụng để kiểm tra các tập tin, phần mềm lạ trước khi đưa vào hệ thống; hoặc cài đặt các dịch vụ xử lý dữ liệu quan trọng khỏi phần còn lại của môi trường. Ví dụ: một ngân hàng khi nhận các tệp dữ liệu từ đối tác có thể cho tệp chạy trong sandbox để quan sát hành vi, nếu an toàn mới chuyển vào mạng chính. Sandbox thường được triển khai bằng công nghệ ảo hóa hoặc container hóa, có cơ chế giới hạn quyền hệ thống và tài nguyên. Nhờ đó, nếu mã độc ẩn trong dữ liệu kích hoạt, nó chỉ gây hại trong “hộp” và không ảnh hưởng tới dữ liệu thật. Một ứng dụng khác của sandbox là trong phát triển ứng dụng khi các nhà phát triển có thể truy cập một bản sao dữ liệu thật trong sandbox (*đã ẩn danh các thông tin nhạy cảm*) để thử nghiệm mà không sơ lộ dữ liệu thật. Sử dụng sandbox đảm bảo nguyên tắc phân tách môi trường, tách biệt môi trường sản xuất và môi trường kiểm thử, giảm nguy cơ dữ liệu sản xuất bị truy cập trái phép trong quá trình phát triển, vận hành.

- **Bốn là**, hệ thống giám sát an ninh và phát hiện xâm nhập: Để bảo đảm an toàn dữ liệu, cần có năng lực giám sát, phát hiện sớm các hành vi bất thường hoặc sự cố. Các tổ chức lớn hiện nay triển khai Trung tâm vận hành an ninh (SOC) với các công cụ quản lý Thông tin và Sự kiện Bảo mật (SIEM - *Security Information and Event Management*) để thu thập nhật ký từ hệ thống máy chủ, ứng dụng, thiết bị mạng... và phân tích cảnh báo theo thời gian thực. Hệ thống ngăn ngừa/ phát hiện xâm nhập (IDS/IPS - *Intrusion Detection/Prevention System*) được đặt tại



ranh giới mạng giúp phát hiện các mảnh tấn công mạng vào cơ sở dữ liệu hoặc máy chủ ứng dụng và tự động ngăn chặn. Bên cạnh đó, giải pháp Phân tích hành vi người dùng và thực thể (*UEBA - User and Entity Behavior Analytics*) sử dụng AI/ML phân tích hành vi người dùng, hệ thống, khi phát hiện hành vi bất thường (ví dụ nhân viên đột nhiên tải lượng lớn dữ liệu ngoài giờ làm, hoặc một server tự gửi dữ liệu ra ngoài trái phép) sẽ cảnh báo để kịp thời xử lý. Điều 43 Luật Dữ liệu đã nêu rõ các đơn vị cung cấp dịch vụ dữ liệu phải kiểm tra, giám sát an toàn dữ liệu thường xuyên và giám sát hành vi có thể ảnh hưởng đến bảo vệ dữ liệu. Điều này phù hợp với thực tiễn, hệ thống giám sát hoạt động 24/7 sẽ giúp phòng ngừa, ngăn chặn sớm các nguy cơ như rò rỉ dữ liệu, tấn công APT trước khi hậu quả nghiêm trọng xảy ra. Các tổ chức nên thiết lập quy trình giám sát và phản ứng sự cố rõ ràng: khi hệ thống cảnh báo, đội ứng cứu sẽ phân tích, cô lập sự cố và thông báo cho lãnh đạo cũng như cơ quan quản lý (*theo yêu cầu luật định trong vòng 72 giờ đối với vi phạm dữ liệu cá nhân nhạy cảm*).

- **Năm là**, sao lưu và phục hồi dữ liệu (*Backup và Recovery*): Để đảm bảo tính sẵn sàng và toàn vẹn của dữ liệu, không thể thiếu giải pháp sao lưu định kỳ. Một chiến lược sao lưu tốt (ví dụ quy tắc 3-2-1: 3 bản sao lưu, trên 2 phương tiện, 1 lưu offline) sẽ bảo vệ dữ liệu khỏi mất mát do sự cố kỹ thuật, thiên tai hoặc tấn công ransomware. Dữ liệu nên được sao lưu hàng ngày hoặc theo tần suất phù hợp mức độ cập nhật. Các bản sao lưu phải được mã hóa và lưu ở nơi an toàn (khác phân vùng mạng với hệ thống chính để tránh bị tấn công lan). Song song, cần xây dựng kế hoạch phục hồi thảm họa với các kịch bản giả định hệ thống bị sự cố lớn (ví dụ trung tâm dữ liệu chính gặp cháy nổ, mất điện kéo dài - thì chuyển đổi sang trung tâm dự phòng như thế nào). Luật Dữ liệu đòi hỏi hạ tầng Trung tâm dữ liệu quốc gia phải có mức dự phòng, sẵn sàng cao nhằm sẵn sàng mở rộng hoặc thay thế khi cần. Ở cấp độ doanh nghiệp, các trung tâm dữ liệu cũng nên áp dụng thiết kế dự phòng, lưu trữ dữ liệu theo công nghệ RAID, cụm máy chủ... để tránh gián đoạn dịch vụ. Việc diễn tập định kỳ phương án khôi phục từ backup sẽ giúp đảm bảo dữ liệu sao lưu thực sự sử dụng được khi cần. Ngoài ra, các giải



pháp chống xóa dữ liệu (*WORM storage*) có thể được cân nhắc cho dữ liệu cốt lõi, nhằm ngăn dữ liệu bị thay đổi hoặc xóa bởi tác nhân độc hại. Tóm lại, sao lưu và phục hồi là giải pháp kỹ thuật quan trọng để duy trì tính liên tục của hoạt động dữ liệu và giảm thiểu thiệt hại khi xảy ra sự cố an ninh.

- **Sáu là**, kiểm tra, đánh giá bảo mật thường xuyên: Các hệ thống dữ liệu cần được đánh giá bảo mật định kỳ nhằm phát hiện sớm lỗ hổng và điểm yếu. Giải pháp bao gồm quét lỗ hổng tự động (*bằng các công cụ như Nessus, OpenVAS...*) trên máy chủ, cơ sở dữ liệu, ứng dụng web; tiến hành kiểm thử xâm nhập (*penetration testing*) định kỳ (*giả lập tấn công có kiểm soát vào hệ thống*) để đánh giá khả năng bị tấn công thực tế. Thông qua đó, các lỗ hổng như cấu hình sai, lỗi SQL injection, lỗ hổng zero-day... sẽ được phát hiện và khắc phục trước khi tin tặc khai thác. Việc đánh giá bảo mật cũng nên bao gồm kiểm tra tuân thủ các chính sách (*ví dụ kiểm tra xem có tài khoản người dùng nào dư thừa, mật khẩu có tuân thủ độ phức tạp, dữ liệu nhạy cảm có được mã hóa hay không...*). Kết quả đánh giá cần được báo cáo cho lãnh đạo và lên kế hoạch vá lỗi kịp thời. Nhiều tiêu chuẩn quốc tế như ISO/IEC 27001 yêu cầu tổ chức phải thực hiện đánh giá rủi ro bảo mật thường xuyên và có quy trình xử lý cải thiện liên tục, đây cũng là thông lệ tốt để nâng cao an toàn dữ liệu.

- **Bảy là**, các giải pháp kỹ thuật khác: Bên cạnh các giải pháp chính nêu trên, tùy đặc thù mỗi tổ chức có thể triển khai thêm: Hệ thống ngăn ngừa thất thoát dữ liệu (*DLP*) để kiểm soát việc sao chép, gửi dữ liệu ra bên ngoài (*ví dụ chặn nhân viên gửi email chứa dữ liệu nhạy cảm hoặc copy file vào USB nếu chưa được phép*); Công cụ quản lý khóa và chứng thư số để đảm bảo tất cả kết nối đều được mã hóa và xác thực đúng nguồn; Nền tảng quản trị cấu hình và vá lỗi tự động giúp hệ thống luôn cập nhật bản vá bảo mật; Cơ chế hệ thống con mồi (*honeypot*) để phát hiện sớm hành vi dò quét của hacker;... Điều quan trọng là mọi giải pháp kỹ thuật cần được thiết kế thành một kiến trúc nhiều lớp (*defense-in-depth*), lớp sau bổ sung cho lớp trước, tạo nên một môi trường an toàn dữ liệu toàn diện. Ví dụ: lớp bảo vệ mạng (*tường lửa*) ngăn truy cập trái phép; lớp ứng

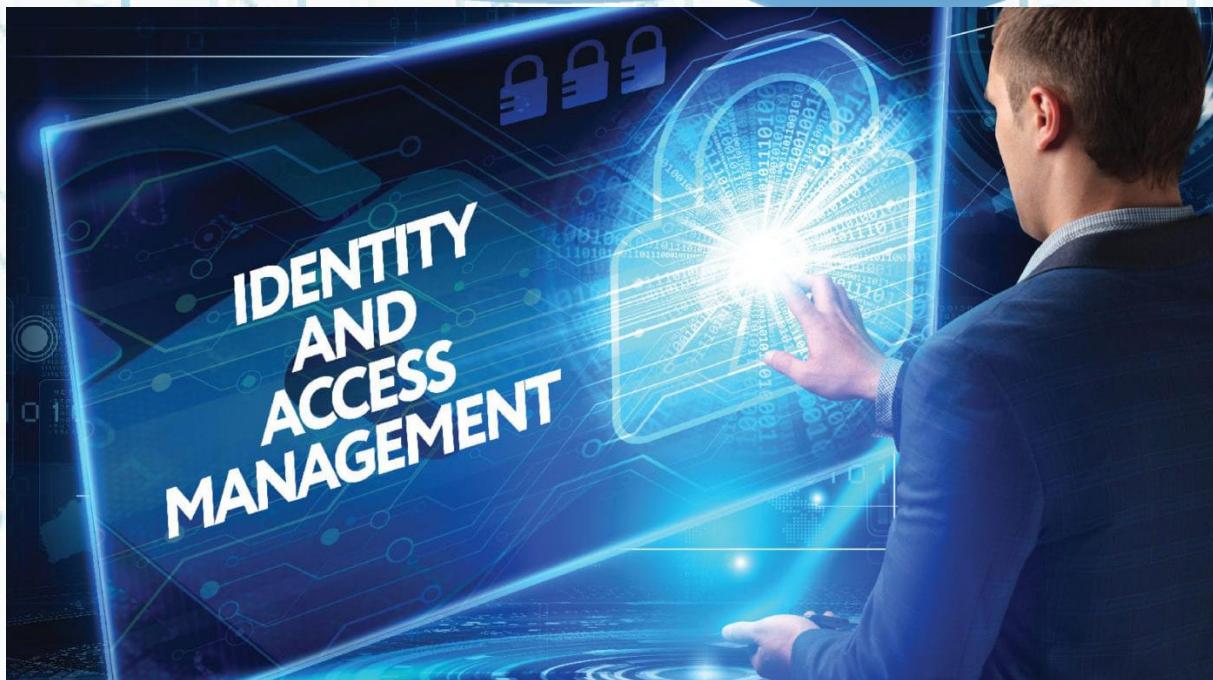


dụng kiểm soát quyền; lớp dữ liệu có mã hóa; lớp giám sát phát hiện xâm nhập; lớp sao lưu đảm bảo khôi phục... Tất cả phối hợp nhịp nhàng để giảm thiểu tối đa xác suất mất an toàn dữ liệu.

### 7.2.3. Cơ chế vận hành tổ chức bảo đảm an toàn dữ liệu tại Trung tâm dữ liệu quốc gia

Trung tâm dữ liệu quốc gia được Luật Dữ liệu 2024 thiết lập với vai trò là đầu mối quản lý tập trung tài nguyên dữ liệu quốc gia, do Chính phủ xây dựng và giao Bộ Công an quản lý, vận hành. Về bản chất, Trung tâm dữ liệu quốc gia là một siêu trung tâm dữ liệu của quốc gia, tích hợp hạ tầng công nghệ thông tin, lưu trữ và xử lý dữ liệu phục vụ cả khu vực công lẫn một phần khu vực tư. Để bảo đảm an ninh, an toàn dữ liệu tại Trung tâm dữ liệu quốc gia, cơ chế tổ chức vận hành cần chú trọng các điểm sau:

- **Thứ nhất**, hạ tầng kỹ thuật đạt chuẩn cao về an ninh: Điều 30 Luật Dữ liệu quy định rõ hạ tầng của Trung tâm dữ liệu quốc gia phải đáp ứng tiêu chuẩn trung tâm dữ liệu quốc tế và có khả năng chống chịu các mối đe dọa vật lý (*nhiệt độ, cháy nổ, thiên tai, khủng bố*) cũng như các mối đe dọa mạng. Đặc biệt, phải có giải pháp bảo mật kiểm soát, phát hiện, ngăn chặn tấn công, đột nhập, phá hoại trên không gian mạng. Theo đó, Trung tâm dữ liệu quốc gia sẽ được trang bị các hệ thống an ninh tiên tiến nhất, từ lớp bảo vệ vật lý (*bảo vệ 24/7, kiểm soát ra vào*) đến lớp bảo mật mạng (*firewall thế hệ mới, hệ thống phát hiện xâm nhập*), lớp ứng dụng (*WAF tường lửa ứng dụng web*) và lớp dữ liệu (*mã hóa cơ sở dữ liệu, hệ thống quản lý khóa chuyên dụng*). Trung tâm dữ liệu quốc gia cần đạt tiêu chuẩn tương đương Tier 4 (*theo Uptime Institute*) về độ sẵn sàng và an toàn, tức có dự phòng đầy đủ để không gián đoạn hoạt động ngay cả khi một thành phần gặp sự cố. Luật cũng yêu cầu thiết kế hạ tầng Trung tâm dữ liệu quốc gia phải có mức dự phòng để sẵn sàng mở rộng khi cần thiết. Điều này có nghĩa là cơ chế vận hành phải thường xuyên theo dõi tải, năng lực hệ thống và kích hoạt kịch bản mở rộng (*thêm máy chủ, thêm dung lượng lưu trữ*) trước khi xảy ra tình trạng quá tải, một cách chủ động bảo đảm dịch vụ dữ liệu luôn thông suốt.



Mô hình hệ thống quản lý định danh và truy cập (IAM). Ảnh: Bizfly Cloud

- **Thứ hai**, tổ chức vận hành và quản trị dữ liệu tập trung: Trung tâm dữ liệu quốc gia có trách nhiệm tích hợp, đồng bộ, lưu trữ, phân tích, khai thác dữ liệu từ các cơ quan nhà nước để tạo lập và quản trị Cơ sở Dữ liệu tổng hợp quốc gia. Nói cách khác, Trung tâm dữ liệu quốc gia đóng vai trò như một “data hub” kết nối các bộ, ngành, địa phương. Cơ chế vận hành đòi hỏi có quy trình chuẩn cho việc tiếp nhận dữ liệu từ các cơ quan (*thông qua nền tảng tích hợp, chia sẻ dữ liệu quốc gia*); gắn nhãn phân loại dữ liệu khi đưa vào (*xác định dữ liệu đó là dữ liệu mở, dùng chung hay dữ liệu hạn chế; có thuộc loại quan trọng, cốt lõi hay không*); lưu trữ trên phân vùng tương ứng với cấp độ bảo mật phù hợp.

■ Ví dụ: dữ liệu thường xuyên sử dụng có thể lưu trên hệ thống online tốc độ cao, dữ liệu ít dùng có thể lưu hệ thống nearline; dữ liệu mật/nhạy cảm phải lưu trong phân vùng mã hóa riêng, hạn chế tài khoản truy cập.

Một cơ chế quan trọng là kiểm soát truy cập theo mô hình tập trung: Trung tâm dữ liệu quốc gia cần vận hành một hệ thống quản lý định danh và truy cập (IAM) dùng chung cho các Cơ sở dữ liệu Quốc gia, để đảm bảo mọi lượt truy cập Cơ sở dữ liệu tổng hợp Quốc gia đều qua xác thực, phân quyền chặt chẽ. Điều 31 Luật Dữ liệu giao Trung tâm dữ liệu quốc gia nhiệm vụ quản trị, vận hành hạ tầng



kỹ thuật, hạ tầng CNTT và sàn dữ liệu tại trung tâm. Do đó, về tổ chức nhân sự, Trung tâm dữ liệu quốc gia có các bộ phận chuyên môn: Phòng Hậu cần, Phòng An ninh, an toàn hệ thống, Phòng Quản trị dữ liệu, Trung tâm Sáng tạo và khai thác dữ liệu,... Mỗi đơn vị thực hiện một chức năng nhưng phối hợp dưới cơ chế quản lý tập trung của Trung tâm dữ liệu quốc gia.

- **Thứ ba**, giám sát chất lượng và an toàn dữ liệu: Theo Luật, Trung tâm dữ liệu quốc gia phải giám sát việc bảo đảm chất lượng dữ liệu và hoạt động điều phối, chia sẻ dữ liệu. Đồng thời phải xây dựng hệ thống chỉ số đo lường, đánh giá hiệu suất quản trị dữ liệu. Điều này bao hàm việc thiết lập các chỉ số an toàn dữ liệu (*ví dụ số sự cố an ninh/tháng, thời gian xử lý sự cố, phần trăm hệ thống tuân thủ cấu hình an toàn...*) để liên tục đánh giá mức độ an toàn. Hệ thống giám sát tập trung (*SOC*) của Trung tâm dữ liệu quốc gia sẽ theo dõi mọi luồng dữ liệu ra/vào trung tâm, phát hiện kịp thời hành vi bất thường. Ví dụ: nếu có cơ quan kết nối tới Cơ sở dữ liệu tổng hợp mà truy vấn đột biến lượng dữ liệu lớn, hệ thống cảnh báo sẽ kích hoạt để kiểm tra xem đó có phải hành vi hợp lệ hay dấu hiệu lạm dụng. Trung tâm dữ liệu quốc gia cũng cần duy trì kênh thông tin 24/7 để tiếp nhận phản ánh về sự cố an toàn từ các bên sử dụng dịch vụ. Điều 43 Luật Dữ liệu yêu cầu, kênh tiếp nhận thông tin và dịch vụ phải thông suốt, liên tục, nghĩa là người dùng dữ liệu (*các cơ quan, doanh nghiệp khai thác dữ liệu từ trung tâm*) nếu gặp vấn đề (*nếu không truy cập được, nghi ngờ lỗ dữ liệu*) phải được hỗ trợ ngay.

- **Thứ tư**, phối hợp liên ngành trong bảo vệ dữ liệu: Trung tâm dữ liệu quốc gia đặt dưới sự quản lý của Bộ Công an vốn đã được giao nhiệm vụ chủ trì về an ninh mạng, an toàn thông tin. Bên cạnh đó, việc bảo vệ dữ liệu quan trọng còn có sự tham gia của Bộ Quốc phòng và Bộ Khoa học và Công nghệ. Cơ chế vận hành an toàn dữ liệu tại Trung tâm dữ liệu quốc gia do vậy phải có quy trình phối hợp với các đơn vị chuyên trách thuộc các bộ trên. Ví dụ: khi phát hiện tấn công có chủ đích (*APT*) vào hệ thống trung tâm, Trung tâm dữ liệu quốc gia (*Bộ Công an quản lý*) sẽ phối hợp với đơn vị ứng cứu sự cố quốc gia của Bộ Khoa học và Công nghệ và đơn vị tác chiến không gian mạng của Bộ Quốc phòng để xử lý, truy vết



nguồn tấn công. Điều 25 Luật Dữ liệu quy định các chủ quản dữ liệu cốt lõi, quan trọng phải thông báo nguy cơ rủi ro tới Bộ Công an, Bộ Quốc phòng để phối hợp bảo vệ, Trung tâm dữ liệu quốc gia chính là chủ quản những dữ liệu cốt lõi nhất, cơ chế chia sẻ thông tin sự cố với các cơ quan an ninh sẽ càng phải thông suốt. Bên cạnh đó, Trung tâm dữ liệu quốc gia cũng có nhiệm vụ thực hiện hợp tác quốc tế về dữ liệu. Do đó, trung tâm sẽ là đầu mối tham gia các diễn đàn quốc tế về an toàn dữ liệu, hợp tác trao đổi thông tin với các trung tâm dữ liệu lớn trên thế giới để học hỏi kinh nghiệm bảo mật.

**- Thứ năm,** đảm bảo nguồn nhân lực chất lượng cao: Yếu tố con người quyết định sự vận hành an toàn của Trung tâm dữ liệu quốc gia. Điều 32 Luật Dữ liệu khẳng định Nhà nước sẽ bảo đảm nguồn nhân lực cho hoạt động của Trung tâm dữ liệu quốc gia và có cơ chế thu hút đai ngộ nhân tài chất lượng cao. Thực tế, để quản lý một Trung tâm dữ liệu quốc gia đòi hỏi đội ngũ chuyên gia an toàn thông tin trình độ cao, am hiểu cả về quản trị hệ thống lẫn an ninh mạng. Chính phủ đã giao Bộ Công an thành lập Trung tâm dữ liệu quốc gia như một đơn vị mới và trao quyền Bộ trưởng Bộ Công an quy định chức năng, tổ chức bộ máy. Điều này cho thấy trọng trách đảm bảo an ninh, an toàn dữ liệu sẽ do một lực lượng chuyên trách thuộc Bộ Công an phụ trách, có thể hình dung đây là một “đội đặc nhiệm” về dữ liệu gồm các chuyên gia công nghệ, chuyên gia bảo mật hàng đầu tuyển từ nhiều nguồn (*trong lực lượng, trong các cơ quan nhà nước, doanh nghiệp, thậm chí nước ngoài*). Cơ chế vận hành phải chú trọng đào tạo liên tục cho nhân lực, cập nhật kiến thức về các mối đe dọa mới, kỹ năng ứng phó sự cố, kỹ thuật bảo mật tiên tiến. Nhà nước cũng cần có chính sách lương, thưởng, môi trường làm việc tốt để giữ chân nhân tài trong lĩnh vực này.

Tóm lại, cơ chế tổ chức vận hành an toàn dữ liệu tại Trung tâm dữ liệu quốc gia mang tính tổng thể và liên kết từ hạ tầng kỹ thuật bảo mật cao, quy trình quản trị tập trung, giám sát thường trực, phối hợp nhiều cơ quan, cho đến nhân lực tinh nhuệ. Mục tiêu cuối cùng là Trung tâm dữ liệu quốc gia trở thành một “pháo đài số” vững chắc, tập trung kho dữ liệu quốc gia khổng lồ nhưng vẫn được bảo vệ



an toàn tuyệt đối, làm nền tảng cho phát triển Chính phủ số và kinh tế số mà không làm phát sinh rủi ro về an ninh dữ liệu.

#### **7.2.4. Quản lý rủi ro dữ liệu và bảo vệ dữ liệu cốt lõi, cá nhân nhạy cảm**

Quản lý rủi ro dữ liệu là một thành phần thiết yếu trong chương trình an toàn dữ liệu của mọi tổ chức. Mục tiêu quản lý rủi ro là nhận diện những mối nguy có thể đe dọa đến tính bảo mật, toàn vẹn, sẵn sàng của dữ liệu; đánh giá mức độ tác động và triển khai biện pháp giảm thiểu phù hợp. Luật Dữ liệu 2024 chính thức yêu cầu các cơ quan, tổ chức thực hiện quản lý rủi ro dữ liệu. Cụ thể, Điều 25 liệt kê các loại rủi ro chính trong xử lý dữ liệu gồm: rủi ro quyền riêng tư (*vì phạm bảo mật thông tin cá nhân*), rủi ro an ninh mạng (*tấn công mạng, virus, malware*), rủi ro nhận dạng và quản lý truy cập (*xảy ra do lỗ hổng trong xác thực, phân quyền*) và các rủi ro khác. Với mỗi loại rủi ro, tổ chức phải xây dựng kịch bản ứng phó tương ứng.

Quy trình quản lý rủi ro dữ liệu thường bao gồm các bước chính: <sup>(1)</sup>Xác định rủi ro (*liệt kê tài sản dữ liệu và các mối đe dọa, lỗ hổng liên quan*); <sup>(2)</sup>Đánh giá rủi ro (*xác định khả năng xảy ra và mức độ ảnh hưởng, từ đó xếp hạng rủi ro cao, trung bình, thấp*); <sup>(3)</sup>Xử lý rủi ro (*chọn biện pháp: giảm thiểu bằng kiểm soát, chấp nhận, tránh hoặc chuyển giao rủi ro*); và <sup>(4)</sup>Giám sát, rà soát rủi ro thường xuyên (*vì môi trường và mối đe dọa luôn thay đổi*). Theo Khoản 2, Điều 25, các cơ quan nhà nước phải thiết lập cơ chế cảnh báo sớm cho rủi ro phát sinh, tích hợp việc giám sát liên tục để cảnh báo trước khi rủi ro trở thành sự cố. Đồng thời, nếu rủi ro xảy ra (*lộ dữ liệu*), phải có quy trình khắc phục kịp thời và thông báo cho các bên liên quan, bao gồm cả chủ thể dữ liệu bị ảnh hưởng và cơ quan quản lý.

Đặc biệt đối với việc bảo vệ dữ liệu cốt lõi, bởi dữ liệu cốt lõi được xác định là những dữ liệu tối quan trọng, có ảnh hưởng trực tiếp đến an ninh quốc gia, an toàn xã hội, lợi ích công cộng. Ví dụ: có thể bao gồm dữ liệu về an ninh quốc phòng, dữ liệu quản lý hạ tầng trọng yếu, dữ liệu tài chính vĩ mô... Vì tầm quan trọng đặc biệt, dữ liệu cốt lõi đòi hỏi cơ chế bảo vệ nghiêm ngặt nhất. Chính phủ ban hành danh mục 26 dữ liệu cốt lõi, 18 dữ liệu quan trọng và tiêu chí xác định



chúng. Các tổ chức sở hữu, quản lý dữ liệu cốt lõi/quan trọng phải tuân thủ mọi quy định về bảo vệ dữ liệu (*Khoản 3, Điều 27*) và định kỳ đánh giá rủi ro cho các dữ liệu này (*Khoản 4, Điều 25*).



*Hình ảnh: Phó Thủ tướng Nguyễn Chí Dũng - người ký Quyết định số 20/2025/QĐ-TTg của Thủ tướng Chính phủ ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi. Ảnh: Báo Chính phủ*

Trong thực tiễn, bảo vệ dữ liệu cốt lõi có thể gồm các biện pháp như:

- (<sup>1</sup>) Bảo mật cao nhất về kỹ thuật: Lưu trữ dữ liệu cốt lõi trong phân đoạn mạng biệt lập, áp dụng mã hóa hai lớp (ví dụ *vừa mã hóa ở mức ứng dụng, vừa mã hóa ở đĩa vật lý*), giới hạn rất ít tài khoản có quyền truy cập (*nguyên tắc zero standing privilege, chỉ cấp quyền tạm thời khi cần*); theo dõi 100% hoạt động truy cập và kích hoạt cảnh báo thời gian thực.
- (<sup>2</sup>) Kiểm tra nhân sự chặt chẽ: Những người quản trị hoặc có quyền với dữ liệu cốt lõi phải được xác minh TCCT, ký thỏa thuận bảo mật nghiêm ngặt, có thể áp dụng chính sách 4 mắt (*mỗi hành động quan trọng phải được hai người phê duyệt*).
- (<sup>3</sup>) Phương án dự phòng đặc biệt: Dữ liệu cốt lõi cần được sao lưu ra kho dữ liệu an toàn tuyệt đối (có thể là dạng lưu trữ lạnh offline, hoặc lưu trên hệ thống chỉ ghi WORM để không ai sửa xóa được).
- (<sup>4</sup>) Kiểm toán, đánh giá độc lập: Định kỳ kiểm toán độc lập đánh giá việc bảo vệ dữ liệu cốt lõi,



đảm bảo không có lỗ hổng. Thậm chí có thể áp dụng một số công nghệ tiên tiến như theo dõi bất biến (*blockchain*) để ghi lại mọi giao dịch với dữ liệu cốt lõi, nhằm đảm bảo tính toàn vẹn. Mục tiêu cuối cùng là giảm xác suất xảy ra sự cố với dữ liệu cốt lõi xuống mức gần như bằng 0, bởi hậu quả sẽ rất nặng nề.

Giả sử dữ liệu về hệ thống truyền tải điện quốc gia được coi là dữ liệu cốt lõi. Để bảo vệ, hệ thống SCADA quản lý lưới điện sẽ nằm trên mạng biệt lập không kết nối Internet, dữ liệu vận hành được mã hóa và chỉ giải mã trong môi trường thiết bị phần cứng đặc thù. Mọi truy cập từ bên ngoài phải qua nhiều tầng kiểm duyệt và ghi log. Nếu có bất kỳ bất thường nào (*như ai đó cố truy cập từ IP lạ*), hệ thống cảnh báo ngay cho Trung tâm dữ liệu quốc gia và Bộ Công an để phối hợp xử lý. Đây chính là thực thi quy định phối hợp bảo vệ dữ liệu cốt lõi trong luật.

Tiếp đó, đối với dữ liệu cá nhân nhạy cảm như đã định nghĩa, bao gồm những thông tin riêng tư nhất của cá nhân (*sức khỏe, sinh trắc học, đời tư, tài chính, định vị,...*). Khi những thông tin này bị lộ lọt, cá nhân có thể chịu hậu quả trực tiếp như bị phân biệt đối xử, tổn hại danh dự, tài sản hoặc thậm chí an nguy. Do đó, quản lý rủi ro đối với dữ liệu cá nhân nhạy cảm cần đặc biệt chú trọng quyền riêng tư. Một nguyên tắc nền tảng là hạn chế thu thập và sử dụng dữ liệu nhạy cảm trừ khi thật sự cần thiết và có căn cứ pháp lý. Nếu bắt buộc phải xử lý loại dữ liệu này, tổ chức nên thực hiện Đánh giá tác động xử lý dữ liệu cá nhân (*DPIA*) trước, như Luật Bảo vệ Dữ liệu Cá nhân yêu cầu, để lượng hóa các rủi ro và chuẩn bị biện pháp giảm thiểu. Ví dụ: một ứng dụng y tế thu thập dữ liệu hồ sơ bệnh án (*thuộc loại nhạy cảm*) phải đánh giá dữ liệu lưu ở đâu, ai truy cập, nguy cơ lộ qua kênh nào... từ đó mã hóa dữ liệu, ẩn danh thông tin định danh bệnh nhân, đào tạo nhân viên y tế về bảo mật.

Biện pháp kỹ thuật thông dụng để bảo vệ dữ liệu nhạy cảm là khử định danh/ẩn danh hóa. Khi dữ liệu cá nhân đã được khử định danh (*xóa hoặc mã hóa các thông tin nhận dạng như tên, số CCCD, số điện thoại, mã số thuế...*), thì dữ liệu đó không còn được xem là dữ liệu cá nhân nữa theo luật. Điều này rất hữu



ích để tổ chức có thể phân tích, khai thác giá trị dữ liệu mà giảm thiểu rủi ro xâm phạm riêng tư. Ví dụ: một công ty có thể chia sẻ tập dữ liệu khách hàng đã ẩn danh với đối tác để nghiên cứu xu hướng thị trường, thay vì đưa dữ liệu thô có thông tin khách hàng cụ thể. Bên cạnh ẩn danh, có thể áp dụng đồng bộ hóa hoặc làm mờ dữ liệu nhạy cảm trong môi trường thử nghiệm, báo cáo.

Quản lý truy cập dữ liệu cá nhân nhạy cảm cũng cần nghiêm ngặt tương tự dữ liệu cốt lõi, chỉ những ai thực sự có nhiệm vụ liên quan mới được quyền truy cập và mọi truy cập đều được ghi lại. Các hệ thống thông tin chứa dữ liệu nhạy cảm (*ví dụ hệ thống ngân hàng có thông tin khách hàng VIP, hệ thống bệnh viện có hồ sơ bệnh nhân*) nên có cơ chế theo dõi truy cập, nếu nhân viên nào cố tra cứu hồ sơ không thuộc phạm vi công việc của mình, hệ thống sẽ cảnh báo hoặc chặn. Thực tế đã có trường hợp nhân viên y tế tò mò xem bệnh án của người nổi tiếng, vi phạm này cần bị ngăn chặn và xử lý kỷ luật nghiêm minh.

Luật pháp cũng hỗ trợ bảo vệ dữ liệu nhạy cảm qua các chế tài mạnh. Nghị định 13/2023 và Luật Bảo vệ dữ liệu cá nhân 2025 đều quy định xử phạt nặng với vi phạm liên quan dữ liệu nhạy cảm. Dự kiến xử phạt vi phạm bảo vệ dữ liệu cá nhân có thể lên đến hàng trăm triệu đồng, kèm biện pháp đình chỉ hoạt động xử lý dữ liệu. Những chế tài này răn đe tổ chức, cá nhân không được tùy tiện thu thập, tiết lộ dữ liệu riêng tư của người khác.

Tóm lại, quản lý rủi ro dữ liệu đòi hỏi một cách tiếp cận có hệ thống và chủ động. Đặc biệt với dữ liệu cốt lõi và dữ liệu cá nhân nhạy cảm, hai nhóm dữ liệu nếu xảy ra sự cố sẽ gây hậu quả lớn cần áp dụng các biện pháp bảo vệ tăng cường từ cấp độ chính sách (*hạn chế ai được thu thập, ai được xử lý*), cấp độ con người (*độ tin cậy nhân sự*), đến cấp độ kỹ thuật (*mã hóa mạnh, hạn chế truy cập, giám sát liên tục*). Luật pháp đã đưa ra những yêu cầu nền tảng, nhưng việc triển khai thực tế mới quyết định hiệu quả bảo vệ. Các tổ chức nên xây dựng danh mục rủi ro trọng yếu riêng cho dữ liệu cốt lõi, dữ liệu nhạy cảm của mình và đầu tư thích đáng nguồn lực (*tài chính, công nghệ, con người*) để quản trị các rủi ro đó. Việc



này không chỉ tuân thủ pháp luật mà còn bảo vệ uy tín, tài sản của chính tổ chức trước những sự cố đáng tiếc.

### **7.2.5. Mô hình và kinh nghiệm quốc tế tiêu biểu về bảo đảm an toàn dữ liệu và phát triển thị trường dữ liệu**

Các quốc gia trên thế giới đã và đang xây dựng nhiều mô hình, khung pháp lý khác nhau để vừa bảo đảm an toàn dữ liệu, vừa thúc đẩy phát triển thị trường dữ liệu. Có thể kể đến một số kinh nghiệm tiêu biểu:

#### **- Liên minh châu Âu:**

Liên minh Châu Âu được xem là tiêu chuẩn vàng về bảo vệ dữ liệu cá nhân. Quy định chung về bảo vệ dữ liệu (*GDPR*) có hiệu lực từ 2018 áp dụng trên toàn Liên minh Châu Âu, yêu cầu mọi hoạt động xử lý dữ liệu cá nhân (*thu thập, lưu trữ, chia sẻ, mua bán...*) phải dựa trên một căn cứ pháp lý hợp lệ. Sự đồng thuận (*consent*) của người dùng là căn cứ quan trọng nhất cho các giao dịch dữ liệu thương mại. GDPR nghiêm cấm mua bán dữ liệu cá nhân nếu không có sự đồng ý rõ ràng của chủ thẻ dữ liệu, vi phạm có thể bị phạt đến 20 triệu Euro hoặc 4% doanh thu toàn cầu, tùy mức cao hơn. GDPR cũng trao cho người dân nhiều quyền (*quyền được biết, quyền xóa dữ liệu, quyền phản đối xử lý...*) buộc các công ty phải tôn trọng. Nhờ GDPR, thị trường dữ liệu ở Liên minh Châu Âu phát triển trên nền tảng minh bạch và tin cậy, người dân tin tưởng hơn khi chia sẻ dữ liệu, còn doanh nghiệp có khuôn khổ rõ ràng để khai thác dữ liệu hợp pháp (*ví dụ mô hình ngân hàng dữ liệu nơi cá nhân có thể ủy thác dữ liệu của mình cho bên thứ ba quản lý an toàn và cho phép sử dụng*). Một hệ quả là các vụ vi phạm dữ liệu tại Liên minh Châu Âu bị xử phạt rất nặng, tạo sức ép buộc doanh nghiệp đầu tư cho an ninh dữ liệu. Ví dụ: năm 2019 công ty Google bị CNIL (*cơ quan bảo vệ dữ liệu Pháp*) phạt 50 triệu Euro vì thiếu minh bạch khi thu thập dữ liệu người dùng. Đức thậm chí hình sự hóa hành vi mua bán dữ liệu nhạy cảm, người có ý bán dữ liệu sức khỏe, sinh trắc học... có thể chịu án tù đến 3 năm. Nhờ những biện pháp mạnh mẽ, Liên minh Châu Âu đang xây dựng một thị trường dữ liệu



minh bạch, an toàn, quyền riêng tư cá nhân được tôn trọng như một quyền con người cơ bản.

**- Mỹ:**

Khác với Liên minh Châu Âu, Mỹ chưa có luật bảo vệ dữ liệu cá nhân ở cấp liên bang, mà tiếp cận theo kiểu phân mảnh, quy định theo ngành (*ví dụ luật HIPAA bảo vệ dữ liệu y tế, GLBA bảo vệ dữ liệu tài chính, COPPA bảo vệ dữ liệu trẻ em*) và theo bang. Cách tiếp cận này ưu tiên sự linh hoạt, tạo môi trường pháp lý ít rào cản để ngành công nghiệp dữ liệu phát triển mạnh (*Mỹ là nơi đặt trụ sở các “đại gia” dữ liệu như Google, Facebook...*). Tuy nhiên, điều đó cũng khiến vấn đề quyền riêng tư đôi khi bị xem nhẹ. Gần đây, một số bang tiên phong ban hành luật tương tự GDPR, tiêu biểu là California với CCPA (*Luật Quyền Riêng tư Người tiêu dùng California 2018*) và CPRA 2020. Các luật này trao quyền cho người dân từ chối việc bán dữ liệu cá nhân của mình. Đáng chú ý, định nghĩa “bán” trong CCPA rất rộng, không chỉ là giao dịch lấy tiền, mà bao gồm cả chia sẻ dữ liệu để đổi lấy lợi ích thương mại (*nhiều chia sẻ cho nền tảng quảng cáo đổi lấy dịch vụ*). Điều này buộc các công ty phải minh bạch hơn trong việc chia sẻ dữ liệu người dùng. Dù chưa có luật liên bang, áp lực bảo vệ dữ liệu ở Mỹ cũng tăng sau những vụ bê bối lớn (*ví dụ vụ Equifax 2017 làm lộ thông tin 147 triệu khách hàng, hay vụ Facebook-Meta 2022 bị kiện vì chia sẻ dữ liệu người dùng trái phép cho bên quảng cáo*). Kết quả là thị trường dữ liệu Mỹ đang tự điều chỉnh: nhiều doanh nghiệp tự đưa ra chính sách bảo mật chặt chẽ hơn để tránh rủi ro pháp lý và giữ chân khách hàng. Ngoài ra, Mỹ thúc đẩy phát triển công nghệ an toàn dữ liệu qua khu vực tư, rất nhiều giải pháp mã hóa, bảo mật được các công ty Mỹ nghiên cứu, cung cấp cho toàn thế giới, góp phần nâng cao mặt bằng an ninh dữ liệu chung.

**- Singapore:**

Singapore có Đạo luật Bảo vệ Dữ liệu Cá nhân (*PDPA*) 2012, được đánh giá là hiện đại và hiệu quả hàng đầu châu Á. PDPA yêu cầu các tổ chức khi thu thập, sử dụng, tiết lộ dữ liệu cá nhân đều phải được sự đồng ý của cá nhân, trừ



một số ngoại lệ hợp pháp. Singapore không cấm mua bán dữ liệu bằng từ ngữ cụ thể, nhưng trên thực tế PDPA đòi hỏi có consent cho bất kỳ việc tiết lộ nào, do đó mua bán thông tin mà thiếu sự đồng ý là bất hợp pháp. PDPA cũng có quy định về danh sách “Do Not Call” cấm mua bán danh sách liên lạc cho mục đích quảng cáo nếu người trong danh sách đã đăng ký chặn quảng cáo. Sau sửa đổi năm 2022, mức phạt vi phạm PDPA tăng lên tới 1 triệu SGD hoặc 10% doanh thu hàng năm của tổ chức (*mức nào cao hơn*), cho thấy sự nghiêm khắc của Singapore trong bảo vệ dữ liệu cá nhân. Về phát triển thị trường dữ liệu, Singapore chọn cách phát triển các sàn giao dịch dữ liệu chuyên ngành. Chính phủ Singapore không lập một sàn dữ liệu tập trung duy nhất, mà hỗ trợ hình thành những nền tảng theo lĩnh vực, ví dụ: SGFinDex - nền tảng chia sẻ dữ liệu tài chính cho phép người dân tổng hợp thông tin tài chính cá nhân từ các ngân hàng và cơ quan chính phủ một cách an toàn; SGTraDex - sàn giao dịch dữ liệu ngành vận tải và thương mại; hay ADEX - nền tảng trao đổi dữ liệu không đồng bộ phục vụ quảng cáo. Mỗi sàn này chịu sự quản lý của cơ quan tương ứng (*ví dụ SGFinDex do Cơ quan Tiền tệ Singapore MAS giám sát*) với các quy tắc chặt về an ninh và bảo mật dữ liệu. Singapore cũng là trung tâm đặt nhiều trung tâm dữ liệu khu vực của các tập đoàn lớn, nhờ có môi trường pháp lý ổn định và hạ tầng an toàn. Chính phủ áp dụng nguyên tắc “Secure by Design” trong các dịch vụ công nghệ, đảm bảo mọi hệ thống Chính phủ thông minh (*Smart Nation*) đều được thiết kế tích hợp an ninh ngay từ đầu. Nhờ đó, Singapore xây dựng được uy tín về an toàn dữ liệu, vừa bảo vệ được người dân, vừa thu hút đầu tư vào lĩnh vực dữ liệu (*các doanh nghiệp yên tâm đặt trung tâm dữ liệu tại Singapore vì tin tưởng pháp luật và hạ tầng nơi đây*).

#### - Nhật Bản:

Nhật Bản có Luật Bảo vệ Thông tin Cá nhân (*APPI*) ban hành từ 2003, sửa đổi nhiều lần (*đặc biệt 2017 và 2020*) để theo kịp chuẩn quốc tế. APPI yêu cầu sự đồng ý của cá nhân trước khi chia sẻ dữ liệu cho bên thứ ba và tăng cường cơ chế “opt-out” cá nhân có quyền từ chối việc doanh nghiệp sử dụng dữ liệu của mình cho mục đích khác. Nhật Bản cũng thắt chặt xử phạt: vi phạm APPI có thể bị phạt



hành chính tới 100 triệu yên (*khoảng 18 tỷ VNĐ*). Nhật Bản được Liên minh Châu Âu công nhận đạt mức “tương đương” GDPR, cho phép luân chuyển dữ liệu Liên minh Châu Âu-Nhật tự do, đây là lợi thế lớn cho kinh tế số Nhật. Để khuyến khích phát triển thị trường dữ liệu, Nhật Bản đưa ra mô hình “Information Bank” (*Nhà hàng thông tin*) các doanh nghiệp được cấp phép làm trung gian quản lý dữ liệu cá nhân cho người dân, tương tự ngân hàng quản lý tiền. Người dân có thể ủy thác dữ liệu của mình cho Information Bank, đơn vị này sẽ xử lý, chia sẻ dữ liệu với bên thứ ba thay cho cá nhân theo các hạn mức được đồng ý và cá nhân có thể nhận lợi ích (*phần thưởng, tiền*) đổi lại. Mô hình này giúp người dân kiểm soát dữ liệu tốt hơn và tạo giao dịch dữ liệu một cách an toàn. Chính phủ Nhật cũng thúc đẩy sáng kiến “Data Free Flow with Trust” trong khuôn khổ G20, nhằm thiết lập các nguyên tắc toàn cầu để dữ liệu có thể lưu chuyển qua biên giới thuận lợi nhưng vẫn đảm bảo tin cậy (*trust*). Về an ninh dữ liệu, Nhật Bản chú trọng đến bảo vệ cơ sở hạ tầng thông tin quan trọng (*Critical Information Infrastructure*) - có hệ thống luật và hướng dẫn riêng, yêu cầu các đơn vị vận hành hạ tầng (*điện, viễn thông, tài chính, giao thông*) phải tuân thủ chuẩn mực an ninh cao, báo cáo sự cố cho cơ quan quản lý ngay và phối hợp trong ứng cứu. Cách làm này tương tự nhiều nước phát triển, giúp bảo vệ những dữ liệu và hệ thống cốt lõi của quốc gia. Nhìn chung, Nhật Bản là ví dụ cân bằng tốt giữa quyền riêng tư cá nhân và khai thác dữ liệu thúc đẩy kinh tế, bảo vệ dữ liệu cá nhân nghiêm để người dân tin tưởng, từ đó họ sẵn sàng cho phép doanh nghiệp sử dụng dữ liệu trong phạm vi được đồng ý, tạo ra giá trị mới.

#### **- Trung Quốc:**

Trung Quốc thiết lập khung pháp lý chặt chẽ, yêu cầu đồng ý rõ ràng để xử lý dữ liệu cá nhân, cấm tiết lộ hoặc bán dữ liệu trái phép, vi phạm có thể phạt tới 5% doanh thu. Trung Quốc cũng kiểm soát chặt dòng dữ liệu ra nước ngoài (*yêu cầu doanh nghiệp xin phép khi chuyển dữ liệu người dùng ra ngoài*). Nhờ thị trường nội địa lớn, Trung Quốc đang phát triển mạnh ngành công nghiệp dữ liệu trong nước, đồng thời sử dụng luật để bảo hộ dữ liệu người dân khỏi các công ty nước ngoài.



- **Hàn Quốc:**

Luật Bảo vệ Thông tin Cá nhân (*PIPA*) của Hàn Quốc với nổi tiếng là một trong những luật nghiêm khắc nhất châu Á, yêu cầu đồng ý, giới hạn chuyển dữ liệu ra ngoài, vi phạm có thể tù đến 6 năm. Hàn Quốc có Cơ quan bảo vệ dữ liệu riêng (*PIPC*) rất tích cực xử phạt các công ty lớn (ví dụ 2021 phạt *Facebook*, *Netflix* hàng triệu USD vì vi phạm quyền người dùng).



• *Hàn Quốc phạt Netflix vì thu thập thông tin của hơn 5 triệu người trái phép.*

Ảnh: [Abei.gov.vn](http://Abei.gov.vn)

**7.2.6. Giải pháp hợp tác quốc tế và nâng cao năng lực nhân lực**

An toàn dữ liệu là vấn đề mang tính toàn cầu, các mối đe dọa trên không gian mạng không biên giới. Vì vậy, hợp tác quốc tế có ý nghĩa then chốt giúp Việt Nam nâng cao năng lực bảo vệ dữ liệu. Đồng thời, yếu tố con người, năng lực chuyên môn của đội ngũ nhân lực là nhân tố quyết định sự thành công của mọi chính sách, giải pháp kỹ thuật. Để đảm bảo an ninh an toàn dữ liệu, cần tập trung một số nội dung:



**- Thứ nhất, hợp tác quốc tế về an toàn dữ liệu:**

+ **Một là**, Việt Nam cần tích cực tham gia xây dựng các chuẩn mực, thỏa thuận quốc tế về dữ liệu. Ví dụ: xem xét gia nhập Công ước 108+ của Hội đồng châu Âu về bảo vệ dữ liệu cá nhân, một công ước mở cho các nước ngoài châu Âu nhằm hài hòa tiêu chuẩn bảo vệ dữ liệu toàn cầu. Tham gia Sáng kiến Data Free Flow with Trust, cùng thảo luận cách thức trao đổi dữ liệu qua biên giới an toàn, có kiểm soát. Ngoài ra, Việt Nam cũng nên hiện diện tích cực tại các diễn đàn ASEAN, APEC về an ninh mạng và bảo mật thông tin. Việc hài hòa luật pháp Việt Nam với chuẩn mực khu vực sẽ thúc đẩy thura nhận lẫn nhau, giúp dòng chảy dữ liệu xuyên biên giới (*phục vụ thương mại, đầu tư*) thông suốt hơn mà vẫn an toàn.

+ **Hai là**, ký kết hợp tác song phương với các quốc gia phát triển. Việt Nam đã có những bước đi như ký Biên bản ghi nhớ (*MOU*) với Mỹ về an toàn thông tin mạng. Cụ thể, tháng 11/2024, Cục An toàn thông tin (*Bộ Thông tin và Truyền thông - hiện đã giải thể, chuyển chức năng về Bộ Công an*) đã ký MOU với Cơ quan An ninh mạng và Cơ sở hạ tầng Mỹ (*CISA*) để hợp tác bảo vệ hạ tầng số quan trọng. Đại diện hai bên nhấn mạnh hợp tác và chia sẻ thông tin là “chìa khóa” để bảo vệ thành công hạ tầng và nâng cao năng lực an ninh mạng. Việc hợp tác với những tổ chức giàu kinh nghiệm như CISA giúp Việt Nam tăng cường khả năng bảo vệ lợi ích quốc gia, đóng góp vào tương lai an toàn, thịnh vượng hơn trên toàn cầu. Tương tự, Việt Nam có thể mở rộng hợp tác với cơ quan tương ứng của Liên minh Châu Âu (*ENISA*), Nhật Bản (*JP-CERT*) hoặc Hàn Quốc (*KISA*) trong các lĩnh vực: trao đổi chuyên gia, chia sẻ thông tin về lỗ hổng bảo mật, phối hợp ứng cứu sự cố xuyên biên giới. Những hợp tác này sẽ giúp Việt Nam tiếp cận kiến thức, công nghệ mới nhanh hơn, cũng như nhận được hỗ trợ khi xảy ra tấn công quy mô lớn (*ví dụ phối hợp truy vết nguồn tấn công từ nước ngoài*).



Hình ảnh: Cục An toàn thông tin đã ký MOU với Cơ quan An ninh mạng và Cơ sở hạ tầng Mỹ (CISA). Ảnh: Tạp chí VnEconomy

+ **Ba là**, tham gia mạng lưới ứng cứu sự cố, chia sẻ tình báo an ninh: Ở cấp độ kỹ thuật, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) và các đội ứng cứu sự cố của Việt Nam nên tích cực trong các mạng lưới như APCERT (*Diễn đàn ứng cứu sự cố khu vực châu Á - TBD*) hoặc FIRST (*Diễn đàn ứng cứu sự cố toàn cầu*). Qua đó, Việt Nam có thể nhận cảnh báo sớm về các chiến dịch tấn công mới, mẫu mã độc mới từ cộng đồng quốc tế. Ngoài ra, hợp tác với các hãng công nghệ lớn (*Microsoft, Google, Facebook...*) cũng giúp xử lý nhanh các vụ lạm dụng dữ liệu trên nền tảng toàn cầu. Thực tế, trong các vụ lộ thông tin thẻ tín dụng, dữ liệu người dùng trên dark web, các Đội ứng cứu sự cố an toàn thông tin (CERT) Việt Nam đã phối hợp với đối tác quốc tế truy tìm và cảnh báo cho người dùng kịp thời.

+ **Bốn là**, hợp tác xây dựng hạ tầng kỹ thuật và tiêu chuẩn: Việt Nam có thể mời gọi sự hỗ trợ quốc tế trong việc thiết kế, triển khai các dự án trọng điểm như Trung tâm dữ liệu quốc gia, Hệ thống Cloud Government... Các nước tiên tiến và công ty hàng đầu có nhiều kinh nghiệm triển khai an toàn mà ta có thể học hỏi. Song song đó, Việt Nam nên áp dụng tiêu chuẩn quốc tế (*ISO 27001, ISO 27701 về quản lý ATTT và bảo vệ dữ liệu cá nhân; PCI-DSS trong lĩnh vực thanh*



toán...) để tạo tiếng nói chung với đối tác toàn cầu. Việc tuân thủ tiêu chuẩn quốc tế giúp doanh nghiệp Việt Nam dễ xuất khẩu dịch vụ dữ liệu ra nước ngoài và nhận được sự tin cậy của khách hàng quốc tế.

**- Thứ hai, nâng cao năng lực nhân lực về an toàn dữ liệu:**

+ **Một là**, đào tạo chuyên gia và đội ngũ thực thi pháp luật: Luật Dữ liệu, Luật Bảo vệ Dữ liệu cá nhân... mới ban hành đặt ra nhu cầu lớn về nguồn nhân lực hiểu biết sâu cả về pháp lý lẫn kỹ thuật dữ liệu. Cần xây dựng các chương trình đào tạo, chứng chỉ chuyên biệt về quản trị dữ liệu an toàn. Ví dụ: huấn luyện đội ngũ cán bộ tại Trung tâm dữ liệu quốc gia, NCSC về các công nghệ quản trị dữ liệu lớn, kỹ năng phân tích dữ liệu để giám sát an toàn. Với khói thực thi pháp luật (*Cục An ninh mạng và phòng chống tội phạm công nghệ cao - Bộ Công an và Thanh tra Chính phủ*), cần đào tạo nâng cao về điều tra số, pháp y kỹ thuật số, am hiểu các phương thức vi phạm mới (*nhiều tội phạm sử dụng dark web mua bán dữ liệu*). Nhà nước có thể gửi cán bộ sang các nước phát triển để học tập, hoặc mời chuyên gia quốc tế sang Việt Nam tổ chức các khóa huấn luyện chuyên sâu. Bên cạnh đó, khuyến khích cán bộ tham gia các kỳ thi, chứng chỉ quốc tế như CIPP/E (*chuyên gia luật bảo vệ dữ liệu châu Âu*), CISSP, CISM (*chuyên gia quản lý an ninh thông tin*) để đạt chuẩn mực toàn cầu.

+ **Hai là**, phát triển chương trình học thuật và nghiên cứu: Các trường đại học nên bổ sung hoặc mở mới chuyên ngành về an toàn thông tin, bảo mật dữ liệu. Hiện đã có một số trường đào tạo ATTT ở bậc đại học, nhưng nội dung về an toàn dữ liệu (*data security*) cần cập nhật thêm các môn về bảo vệ quyền riêng tư, mật mã ứng dụng, quản trị dữ liệu lớn an toàn. Việc kết hợp kiến thức giữa khoa học dữ liệu và an toàn thông tin là xu hướng cần thiết (*nhiều nơi trên thế giới đã hình thành liên ngành Privacy Engineering - Kỹ thuật bảo mật riêng tư*). Nhà nước có thể tài trợ để tài nghiên cứu phát triển các công cụ nội địa phục vụ bảo vệ dữ liệu: như phần mềm quét phát hiện dữ liệu nhạy cảm trong hệ thống, công cụ đánh giá tuân thủ quy định bảo vệ dữ liệu cho doanh nghiệp,... Các kết quả nghiên cứu này



vừa tạo ra sản phẩm Make in Vietnam, vừa giúp nâng cao trình độ đội ngũ khoa học công nghệ trong nước.

+ **Ba là**, nâng cao nhận thức và kỹ năng của nhân viên và người dân: Yếu tố con người thường là mắt xích yếu nhất trong chuỗi an toàn dữ liệu. Do vậy cần thường xuyên tổ chức các chương trình tuyên truyền, tập huấn về bảo mật dữ liệu cho nhân viên ở mọi cấp và cho cộng đồng. Đối với nhân viên doanh nghiệp/cơ quan, cần cung cấp khóa học hàng năm về các quy tắc bảo vệ dữ liệu (*không chia sẻ mật khẩu, không sao chép dữ liệu khách hàng ra thiết bị cá nhân, cảnh giác email lừa đảo...*) như các khóa học [binhdanhocvuso.gov.vn](http://binhdanhocvuso.gov.vn). Cập nhật cho họ về các mối đe dọa mới (ví dụ *ransomware tống tiền dữ liệu*) và cách xử lý khi nghi ngờ sự cố (*báo ngay bộ phận CNTT, không tự ý khắc phục gây xóa dấu vết*).

The screenshot shows the homepage of the website [binhdanhocvuso.gov.vn](http://binhdanhocvuso.gov.vn). The header includes the logo of the Ministry of Public Security and the text "BỘ CÔNG AN NỀN TẢNG BÌNH DÂN HỌC VỤ SỐ". The top navigation bar has links for "Hướng dẫn học", "Khám phá khóa học", "Khóa học của tôi", and a user profile icon. Below the header, a message states: "Sử dụng và luyện thi theo ngân hàng câu hỏi mới của Bộ Công an. Học liệu do Bộ Xây dựng và Bộ Công an cung cấp trên nền tảng Bình dân học vụ số." The main content area displays several training modules:

- KHOA HỌC VỀ NGHỊ QUYẾT 57**: Tổng hợp tài liệu về Nghị quyết số 57-NQ/TW (đang xây dựng). NQ57 C06. Bắt đầu: 31/12/2024.
- HỖ TRỢ TRIỂN KHAI CHÍNH QUYỀN ĐỊA PHƯƠNG 2 CẤP**: Hỗ trợ triển khai chính quyền địa phương 2 cấp. C0602 C06. Bắt đầu: 01/01/2025.
- ĐÀO TẠO LUẬT HÌNH SỰ**: Đào tạo Luật Hình sự. V0301 C06, V03. Bắt đầu: 01/01/2025.
- AN TOÀN THÔNG TIN**: Các kiến thức cơ bản. Kiến thức cơ bản về an toàn thông tin. ATTT02 Trưởng CNTT&TT - ĐHBKN. Bắt đầu: 31/03/2025.
- PHÁP LUẬT GIAO THÔNG ĐƯỜNG BỘ**: Hệ thống báo hiệu đường bộ. Pháp luật giao thông đường bộ - Hệ thống báo hiệu đường bộ. mqc02.
- PROMPT ENGINEERING**: Làm chủ AI với Prompt Engineering. AI01.
- ĐÀO DỤC NGƯỜI LÁI XE, VĂN HÓA GIAO THÔNG VÀ PHÒNG CHỐNG TÁC HẠI CỦA RƯỢU BIA, KỸ NĂNG PHÒNG CHÁY, CHỮA CHÁY VÀ CỨU NẠN, CỨU HỘ**: Đào đức người lái xe, văn hóa giao thông và phòng chống tác hại của rượu bia, kỹ năng phòng cháy, chữa cháy và cứu nạn, cứu hộ. mqc05.
- PHÁP LUẬT GIAO THÔNG ĐƯỜNG BỘ**: NHỮNG NỘI DUNG CƠ BẢN CỦA LUẬT GIAO THÔNG ĐƯỜNG BỘ. Cục quản lý vật liệu. Pháp luật giao thông đường bộ - Luật Trật tự, an toàn giao thông đường bộ. mqc01.

Hình ảnh: Giao diện trang web [binhdanhocvuso.gov.vn](http://binhdanhocvuso.gov.vn) hiện đã triển khai tới 100% lãnh đạo, cán bộ, chiến sĩ Công an thành phố Hà Nội. Ảnh: Tác giả



Hình ảnh: Lễ phát động phong trào và nền tảng Bình dân học vụ số. Ảnh: Trung tâm Dữ liệu quốc gia về dân cư

Đối với người dân, cần đẩy mạnh chiến dịch trên phương tiện truyền thông về quyền của chủ thể dữ liệu theo luật mới, khuyến khích người dân thực thi quyền (*hỏi các công ty đang lưu dữ liệu gì về mình, yêu cầu xóa nếu không cần thiết*). Đồng thời hướng dẫn người dân bảo vệ dữ liệu cá nhân trong sinh hoạt số, cẩn trọng khi cung cấp thông tin trên mạng, dùng các tính năng bảo mật (*mã hóa tin nhắn, đặt mật khẩu mạnh*). Chính phủ Singapore là ví dụ điển hình về giáo dục cộng đồng, họ thường xuyên diễn tập phòng thủ mạng ở cấp quốc gia và tập trận giả định tình huống rò rỉ dữ liệu để rèn phản xạ cho các cơ quan và doanh nghiệp. Việt Nam cũng có thể tổ chức các cuộc thi, diễn tập an toàn thông tin quy mô lớn, lồng ghép kịch bản bảo vệ dữ liệu để các bên cùng nâng cao kỹ năng.



Hình ảnh: Cuộc Tập trận Phòng thủ Cơ sở Hạ tầng Quan trọng tại Singapore vào cuối năm 2024 thu hút hơn 200 người tham gia từ quân đội, an ninh mạng và các cơ quan khác. Ảnh: BQP SINGAPORE

+ **Bốn là**, phát triển hệ sinh thái nhân lực an toàn dữ liệu: Cần hình thành một cộng đồng chuyên gia trong nước về bảo vệ dữ liệu để chia sẻ kiến thức, hỗ trợ lẫn nhau. Ví dụ thành lập Hiệp hội hoặc Câu lạc bộ các Data Protection Officer (*DPO*) vị trí đang được đề xuất trong các tổ chức lớn theo Luật Bảo vệ dữ liệu cá nhân (*người phụ trách bảo vệ dữ liệu cá nhân*). Từ cộng đồng này, có thể xây dựng bộ thông lệ tốt, tài liệu hướng dẫn áp dụng cho các doanh nghiệp Việt Nam. Ngoài ra, hợp tác công tư trong đào tạo là hướng đi quan trọng: doanh nghiệp lớn có thể phối hợp với trường đại học xây dựng Trung tâm đổi mới sáng tạo về an toàn dữ liệu, nơi sinh viên, chuyên gia cùng nghiên cứu dự án thực tế. Điều này không chỉ nâng cao năng lực mà còn tạo sản phẩm, giải pháp phục vụ thị trường. Nhà nước nên có chính sách khuyến khích, hỗ trợ tài chính cho các chương trình như vậy.

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



*Hình ảnh: Hiệp hội an ninh mạng quốc gia khởi động chương trình diễn tập an ninh mạng Liên minh Ứng phó, khắc phục sự cố an ninh mạng quốc gia lần thứ nhất, tháng 4/2025. Ảnh: Hiệp hội ANM Quốc gia*

Tóm lại, việc hợp tác quốc tế giúp Việt Nam tiếp thu nhanh kinh nghiệm, công nghệ tiên tiến để đối phó với các thách thức an toàn dữ liệu ngày càng phức tạp. Còn nâng cao năng lực nhân lực là đầu tư dài hạn, đảm bảo chúng ta có đủ chuyên gia và nhận thức đúng đắn để vận hành hệ thống bảo vệ dữ liệu hiệu quả. Hai yếu tố này kết hợp sẽ tạo nền tảng vững chắc cho một môi trường dữ liệu an toàn, tin cậy, thúc đẩy phát triển kinh tế - xã hội trong kỷ nguyên số.

## 7.2.7. Tổng hợp rủi ro an toàn dữ liệu và biện pháp bảo vệ tương ứng; Sơ đồ quy trình bảo mật

*Bảng: tóm tắt các loại rủi ro phổ biến đối và biện pháp bảo vệ*

Loại rủi ro dữ liệu	Biện pháp bảo vệ tương ứng
Rủi ro quyền riêng tư: Rò rỉ, lạm dụng dữ liệu cá nhân của	Tuân thủ chặt chẽ luật bảo vệ dữ liệu cá nhân (yêu cầu đồng ý của chủ thể trước khi thu thập, chia sẻ). - Ân danh, mã hóa dữ liệu cá nhân nhạy cảm trước khi lưu trữ, chia sẻ.



Loại rủi ro dữ liệu	Biện pháp bảo vệ tương ứng
khách hàng, nhân viên. Ví dụ: lộ thông tin nhạy cảm ( <i>sức khỏe, tài chính</i> ) ra công chúng.	<ul style="list-style-type: none"> <li>- Giới hạn truy cập dữ liệu cá nhân chỉ cho nhân sự có thẩm quyền; triển khai cơ chế giám sát truy cập (<i>log ai xem dữ liệu nào</i>).</li> <li>- Đào tạo nhân viên về bảo mật thông tin cá nhân; có chế tài nghiêm với vi phạm.</li> </ul>
Rủi ro an ninh mạng: Tấn công mạng từ bên ngoài ( <i>hacking, malware</i> ) nhằm đánh cắp, phá hoại dữ liệu. Ví dụ: tấn công SQL injection vào cơ sở dữ liệu, mã độc mã hóa đòi tiền chuộc.	<ul style="list-style-type: none"> <li>Triển khai tường lửa, hệ thống phát hiện/phòng chống xâm nhập (<i>IDS/IPS</i>) để chặn lọc truy cập nguy hiểm.</li> <li>- Cập nhật bản vá bảo mật thường xuyên cho hệ thống, và các lỗ hổng phần mềm.</li> <li>- Cài đặt phần mềm chống virus, anti-malware trên các máy chủ, máy trạm.</li> <li>- Áp dụng kiến trúc mạng an toàn (<i>phân vùng DMZ, nội bộ; dịch vụ quan trọng đặt sau nhiều lớp firewall</i>).</li> <li>- Thực hiện kiểm thử xâm nhập định kỳ để phát hiện điểm yếu trước khi hacker khai thác.</li> </ul>
Rủi ro về định danh và truy cập: Truy cập trái phép do quản lý danh tính kém. Ví dụ: lộ mật khẩu quản trị, nhân viên tò mò xem dữ liệu không thuộc thẩm quyền.	<ul style="list-style-type: none"> <li>Triển khai xác thực đa yếu tố (<i>MFA</i>) cho tài khoản quan trọng; định kỳ đổi mật khẩu và dùng mật khẩu mạnh.</li> <li>- Thiết lập quyền truy cập tối thiểu: mỗi người chỉ được quyền trên dữ liệu cần thiết.</li> <li>- Xây dựng quy trình xác thực và phân quyền tập trung (<i>IAM</i>); đóng hoặc khóa các tài khoản không dùng.</li> <li>- Giám sát hành vi đăng nhập: cảnh báo đăng nhập bất thường (<i>sai mật khẩu nhiều lần, đăng nhập ngoài giờ</i>).</li> <li>- Ghi log và kiểm tra log truy cập dữ liệu quan trọng để phát hiện hành vi lạm dụng.</li> </ul>
Rủi ro mất mát, hư hỏng dữ liệu: Sự cố kỹ thuật ( <i>hỏng ổ cứng, lỗi phần mềm</i> ) hoặc thảm họa ( <i>cháy nổ, lũ lụt</i> ) gây mất dữ liệu; tấn	<ul style="list-style-type: none"> <li>- Thực hiện sao lưu dữ liệu định kỳ và lưu trữ backup ở vị trí an toàn (<i>offline/offsite</i>); kiểm tra tính toàn vẹn của bản sao lưu.</li> <li>- Xây dựng kế hoạch phục hồi thảm họa (<i>DR</i>): có trung tâm dữ liệu dự phòng, thường xuyên diễn tập khôi phục.</li> <li>- Sử dụng hệ thống lưu trữ có dự phòng (<i>RAID, cluster</i>) để một lỗi phần cứng không làm mất dữ liệu.</li> </ul>



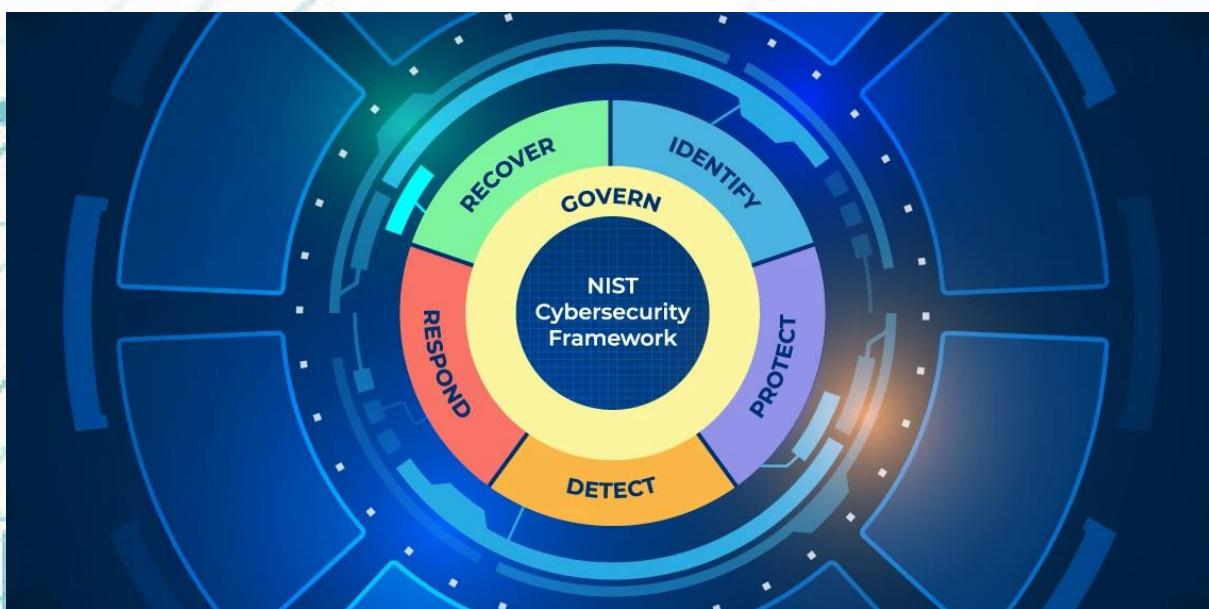
Loại rủi ro dữ liệu	Biện pháp bảo vệ tương ứng
công ransomware mã hóa làm dữ liệu không truy cập được.	<ul style="list-style-type: none"> <li>- Triển khai giải pháp chống mã hóa ransomware: cập nhật AV, cài đặt máy bị nhiễm, lưu backup offline.</li> <li>- Điều 30 Luật Dữ liệu yêu cầu hạ tầng dữ liệu có dự phòng, sẵn sàng cao - tuân thủ điều này giúp giảm thiểu rủi ro mất dữ liệu do sự cố.</li> </ul>
Rủi ro tính toàn vẹn dữ liệu: Dữ liệu bị sửa đổi, làm sai lệch một cách cố ý hoặc vô ý. Ví dụ: nhân viên nhập sai làm hỏng bộ dữ liệu, hacker sửa số liệu giao dịch.	<ul style="list-style-type: none"> <li>- Phân quyền chỉ cho phép chỉnh sửa dữ liệu với người có trách nhiệm; áp dụng nguyên tắc bốn mắt với thao tác nhạy cảm (ví dụ cần hai người duyệt mới được sửa/hủy dữ liệu quan trọng).</li> <li>- Sử dụng cơ chế ghi nhật ký (<i>audit trail</i>) mọi thay đổi dữ liệu và định kỳ soát xét log để phát hiện chỉnh sửa bất thường.</li> <li>- Đối với dữ liệu quan trọng, dùng chữ ký số hoặc hash checksum để phát hiện nếu bị sửa trái phép (so sánh checksum định kỳ).</li> <li>- Thực hiện kiểm tra chất lượng dữ liệu thường xuyên, phát hiện kịp thời dữ liệu sai lệch và khôi phục từ bản lưu trước đó.</li> </ul>
Rủi ro nội gián: Người trong tổ chức lợi dụng quyền hạn để trục lợi hoặc gây hại. Ví dụ: nhân viên IT sao chép cơ sở dữ liệu khách hàng bán ra ngoài.	<ul style="list-style-type: none"> <li>- Thực hiện phân tách nhiệm vụ: không một cá nhân nào được quyền truy cập toàn bộ hệ thống/dữ liệu một mình.</li> <li>- Giám sát chặt hoạt động của người dùng nội bộ, đặc biệt với tài khoản đặc quyền (<i>admin, DBA</i>) - dùng giải pháp UEBA để phát hiện hành vi bất thường.</li> <li>- Áp dụng chính sách luân chuyển vị trí và kiểm tra lịch sử: hạn chế việc một nhân viên quản lý một mảng dữ liệu quá lâu không giám sát.</li> <li>- Xây dựng văn hóa bảo mật và đạo đức dữ liệu, kết hợp chế tài nghiêm minh: nếu phát hiện nhân viên truy xuất dữ liệu trái phép sẽ bị kỷ luật hoặc truy tố hình sự (theo Điều 288 Bộ luật Hình sự về tội đưa hoặc sử dụng trái phép thông tin mạng).</li> <li>- Bảo vệ về mặt kỹ thuật: mã hóa dữ liệu để dù nội gián lấy được file cũng khó sử dụng; sử dụng watermark trên tài liệu để truy ra nguồn rò rỉ</li> </ul>
Rủi ro không tuân thủ pháp luật: Bị phạt do vi phạm các quy định bảo vệ dữ liệu, dẫn tới thiệt hại tài chính và uy	<ul style="list-style-type: none"> <li>Cập nhật hiểu biết pháp luật: doanh nghiệp cần có bộ phận pháp chế hoặc thuê chuyên gia tư vấn để luôn nắm rõ nghĩa vụ theo Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân...</li> <li>Bổ nhiệm nhân sự phụ trách bảo vệ dữ liệu (<i>DPO</i>) để giám sát việc tuân thủ trong tổ chức, làm đầu mối làm việc với cơ quan quản lý.</li> </ul>



Loại rủi ro dữ liệu	Biện pháp bảo vệ tương ứng
tín. Ví dụ: công ty không xin phép người dùng khi dùng dữ liệu, vi phạm GDPR và bị phạt.	<ul style="list-style-type: none"> <li>- Thiết lập quy trình đánh giá tác động bảo mật và quyền riêng tư trước khi triển khai dự án mới (<i>theo yêu cầu DPIA của luật</i>).</li> <li>- Thực hiện kiểm toán nội bộ định kỳ về bảo vệ dữ liệu, kịp thời khắc phục sai sót trước khi bị thanh tra.</li> <li>- Xây dựng kế hoạch và tập dượt ứng phó sự cố dữ liệu (<i>data breach response</i>) để nếu xảy ra, có thể thông báo cơ quan chức năng và người dùng trong thời hạn luật định (<i>VĐ 72 giờ theo Luật Bảo vệ dữ liệu cá nhân</i>).</li> </ul>

Như vậy, tùy từng nhóm rủi ro mà sẽ có tập hợp biện pháp phù hợp theo nguyên tắc phòng ngừa - phát hiện - phản ứng - khắc phục. Mục tiêu là tạo nhiều lớp bảo vệ để giảm xác suất rủi ro và giảm thiểu thiệt hại nếu rủi ro xảy ra.

Có thể tham khảo quy trình bảo mật dữ liệu theo chu trình NIST (Mỹ) gồm 5 chức năng liên tục: Xác định (*Identify*) các tài sản dữ liệu và nguy cơ; Bảo vệ (*Protect*) bằng biện pháp kỹ thuật/kiểm soát; Phát hiện (*Detect*) kịp thời các sự cố, bất thường; Phản hồi (*Respond*) nhanh chóng để giảm thiểu tác động; và Phục hồi (*Recover*) hệ thống dữ liệu trở lại hoạt động bình thường. Chu trình này lặp lại liên tục, tạo nên một vòng đòn quản trị an toàn dữ liệu nâng cao.



Hình ảnh: Quy trình bảo mật liên tục để nâng cao an toàn dữ liệu. Ảnh: Mi2



Trong thực tiễn, các tổ chức nên nội dung dung hóa quy trình trên bằng những hoạt động cụ thể, ví dụ: bước Xác định, tiến hành kiểm kê dữ liệu, phân loại mức độ nhạy cảm; bước Bảo vệ, áp dụng các biện pháp ở bảng trên (*mã hóa, kiểm soát truy cập...*); bước Phát hiện, vận hành hệ thống giám sát, cảnh báo sớm; bước Phản hồi, có đội ứng cứu sự cố, quy trình thông báo; bước Phục hồi, có phương án khôi phục từ backup, đánh giá lại thiệt hại. Việc thực hiện quy trình như vậy giúp đảm bảo tính liên tục và chu trình của công tác bảo mật, luôn cải tiến và thích ứng với mối đe dọa mới, không xem an toàn dữ liệu là việc làm một lần rồi xong.



## KẾT LUẬN

Trong bối cảnh chuyển đổi số sâu rộng, dữ liệu đã trở thành tài sản cốt lõi của quốc gia, doanh nghiệp và mỗi cá nhân. Bảo đảm an ninh, an toàn dữ liệu không chỉ là yêu cầu pháp lý bắt buộc (*theo Luật Dữ liệu 2024 và các văn bản liên quan*) mà còn là yếu tố sống còn để phát triển kinh tế số bền vững, xây dựng niềm tin số trong xã hội. Lần đầu tiên vai trò Trung tâm dữ liệu quốc gia, Cơ sở dữ liệu tổng hợp Quốc gia và các quy định cụ thể về bảo vệ dữ liệu được luật hóa. Những giải pháp kỹ thuật, công nghệ từ mã hóa, định danh, sandbox đến giám sát an ninh đã được đề xuất nhằm hiện thực hóa yêu cầu luật định. Cơ chế vận hành an toàn dữ liệu tại Trung tâm dữ liệu quốc gia được thiết kế đồng bộ từ hạ tầng, quy trình, nhân lực đến phối hợp liên ngành, thể hiện quyết tâm bảo vệ an toàn cho kho dữ liệu quốc gia. Công tác quản lý rủi ro dữ liệu và bảo vệ dữ liệu cốt lõi, dữ liệu nhạy cảm cũng được nhấn mạnh như một ưu tiên, với nhiều biện pháp kiểm soát đặc thù. Thông qua việc tham khảo mô hình quốc tế (EU, Mỹ, Singapore, Nhật Bản...), có thể thấy Việt Nam đang đi đúng hướng khi kết hợp chặt chẽ giữa bảo vệ dữ liệu và phát triển thị trường dữ liệu, bảo vệ tốt thì người dân, doanh nghiệp mới tin tưởng chia sẻ và khai thác dữ liệu, từ đó thị trường dữ liệu mới phát triển. Tuy nhiên, cũng nhìn ra rằng việc triển khai hiệu quả còn nhiều thách thức, đòi hỏi nỗ lực liên tục, đầu tư nghiêm túc cả về công nghệ và con người.

Để hoàn thiện hơn nữa hành lang pháp lý và năng lực đảm bảo an toàn dữ liệu tại Việt Nam, tác giả đưa ra một số kiến nghị cụ thể:

- **Thứ nhất**, sớm hoàn thành hệ thống các các nghị định, thông tư hướng dẫn chi tiết Luật Dữ liệu, đặc biệt về phân loại dữ liệu (*tiêu chí dữ liệu cốt lõi, quan trọng*), quy chế vận hành Trung tâm dữ liệu quốc gia, quy định về sàn giao dịch dữ liệu... Sự rõ ràng trong hướng dẫn sẽ giúp các cơ quan, doanh nghiệp áp dụng thống nhất, tránh lúng túng. Đồng thời rà soát, điều chỉnh các văn bản pháp luật liên quan (*Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018, Nghị*



định 13/2023/NĐ-CP...) để đồng bộ, không chồng chéo với Luật Dữ liệu và Luật Bảo vệ Dữ liệu cá nhân mới.

- **Thứ hai**, tăng cường năng lực thực thi và giám sát pháp luật, giám sát việc tuân thủ của các tổ chức. Cần phát huy vai trò thanh tra, kiểm tra định kỳ việc bảo vệ dữ liệu tại các đơn vị trọng điểm (*ngân hàng, viễn thông, cơ quan lớn*). Song song, triển khai hệ thống báo cáo sự cố dữ liệu quốc gia: các tổ chức phải định kỳ báo cáo tình hình an toàn dữ liệu, sự cố (*nếu có*) để cơ quan quản lý tổng hợp bức tranh chung và cảnh báo kịp thời xu hướng rủi ro.

- **Thứ ba**, cơ quan chức năng nên ban hành các bộ tiêu chuẩn, hướng dẫn kỹ thuật về an toàn dữ liệu phù hợp với Việt Nam (*dựa trên ISO 27001, NIST...*). Ví dụ: tiêu chuẩn về mã hóa dữ liệu trong cơ quan nhà nước; hướng dẫn phân loại và gán nhãn dữ liệu; hướng dẫn về đánh giá tác động bảo mật (*cho DPIA*)... Những tài liệu này giúp các tổ chức có cơ sở áp dụng cụ thể, tránh làm qua loa hoặc không đầy đủ. Bộ Khoa học và Công nghệ cùng Bộ Công an có thể phối hợp biên soạn sổ tay “Hướng dẫn bảo vệ dữ liệu trong cơ quan/tổ chức”, phổ biến rộng rãi.

- **Thứ tư**, đẩy mạnh hợp tác công tư trong bảo vệ dữ liệu, khuyến khích các doanh nghiệp cung cấp giải pháp an toàn thông tin tham gia hỗ trợ khôi Chính phủ. Ví dụ: xây dựng mạng lưới chuyên gia (*tương tự Tổ chuyên gia bảo mật của NCSC*) tư vấn miễn phí khi cơ quan nhà nước triển khai hệ thống dữ liệu mới. Thiết lập các kênh trao đổi giữa cơ quan quản lý và doanh nghiệp lớn về những nguy cơ mới, phương thức bảo vệ mới. Nhà nước cũng có thể đặt hàng doanh nghiệp nghiên cứu phát triển giải pháp Make in Vietnam cho các vấn đề như giám sát dữ liệu lớn, phân tích hành vi bất thường trong hệ thống,...

- **Thứ năm**, phát triển thị trường dịch vụ an toàn dữ liệu song song với phát triển thị trường dữ liệu, hình thành hệ sinh thái dịch vụ bảo mật dữ liệu đi kèm. Chính phủ có thể hỗ trợ (*về chính sách thuế, thử nghiệm sandbox*) cho các startup cung cấp dịch vụ như: dịch vụ tuân thủ GDPR/PDPA cho doanh nghiệp Việt, dịch vụ đánh giá an ninh dữ liệu, dịch vụ cung cấp Data Clean Room (*môi trường chia sẻ dữ liệu an toàn giữa các bên*)... Khi các dịch vụ này phát triển, ngay cả doanh



nghiệp vừa và nhỏ cũng có thể thuê ngoài để bảo vệ dữ liệu của mình tốt hơn, nâng mặt bằng an toàn chung.

- **Thứ sáu**, nâng cao nhận thức xã hội và trách nhiệm người đứng đầu bằng các chiến dịch truyền thông, hội thảo, chương trình đào tạo về an toàn dữ liệu hướng tới đối tượng lãnh đạo cấp cao của tổ chức (*CEO, Giám đốc CNTT, Giám đốc dữ liệu*). Giúp họ hiểu rằng đầu tư cho an toàn dữ liệu không phải chi phí chìm mà là đầu tư bắt buộc để bảo vệ tài sản và uy tín. Đề cao trách nhiệm người đứng đầu: nếu đơn vị để lộ lọt dữ liệu nghiêm trọng do lơ là, người đứng đầu phải chịu chế tài (*như phạt hành chính nặng, công khai xin lỗi khách hàng*). Có như vậy, văn hóa “An toàn dữ liệu là ưu tiên số 1” mới được thiết lập từ trên xuống.

- **Thứ bảy**, Việt Nam nên chủ động đề xuất ký kết hiệp định song phương hoặc đa phương về bảo vệ dữ liệu với các đối tác thương mại lớn. Ví dụ: làm việc với Liên minh Châu Âu để được công nhận tương đương GDPR (*giúp doanh nghiệp Việt xử lý dữ liệu công dân Liên minh Châu Âu thuận lợi hơn*); hợp tác với ASEAN để xây dựng Khung luân chuyển dữ liệu xuyên biên giới ASEAN an toàn (*tương tự APEC có hệ thống CBPR - quy tắc bảo mật xuyên biên giới*). Đồng thời, đóng góp tiếng nói trong việc định hình Bộ quy tắc ứng xử về dữ liệu toàn cầu tại Liên Hợp Quốc nếu có. Điều này vừa nâng cao vị thế Việt Nam, vừa đảm bảo chúng ta không bị đứng ngoài các dòng chảy dữ liệu quốc tế quan trọng.

- **Thứ tám**, kiến nghị Chính phủ xây dựng một Hệ sinh thái an toàn dữ liệu bao gồm: Trung tâm dữ liệu quốc gia an toàn làm nòng cốt; mạng lưới các Trung tâm đáp ứng sự cố dữ liệu vùng miền; cơ sở hạ tầng mật mã quốc gia vững mạnh do Ban Cơ yếu Chính phủ phụ trách (*cung cấp giải pháp ký số, xác thực tin cậy*); cùng với đó là hệ thống tiêu chuẩn, chứng nhận về an toàn dữ liệu cho sản phẩm Công nghệ thông tin. Ví dụ: trong hệ sinh thái này, các sản phẩm phần mềm khi xử lý dữ liệu cá nhân có thể cần được chứng nhận đáp ứng yêu cầu bảo vệ dữ liệu (*privacy-by-design*) trước khi ra thị trường. Hệ sinh thái còn bao hàm yếu tố nhân lực như mạng lưới các trường đại học, viện nghiên cứu, doanh nghiệp phối hợp tạo nguồn nhân lực chất lượng. Khi một hệ sinh thái đồng bộ hình thành, an toàn



dữ liệu sẽ trở thành một thuộc tính tự nhiên của mọi sản phẩm, dịch vụ số, tạo niềm tin cho người sử dụng và đối tác.

Nhìn chung, bảo đảm an ninh, an toàn dữ liệu là hành trình liên tục, cần sự cam kết mạnh mẽ từ Chính phủ, nỗ lực từ doanh nghiệp và sự tham gia của mỗi người dân. Với việc luật pháp đã có những bước tiến lớn và các giải pháp kỹ thuật, tổ chức đang dần được triển khai, chúng ta có cơ sở để tin rằng mục tiêu xây dựng một hệ sinh thái dữ liệu an toàn, tin cậy tại Việt Nam là khả thi. Thực hiện tốt các kiến nghị trên sẽ giúp hoàn thiện hơn nữa nền tảng pháp lý, nâng cao năng lực bảo vệ dữ liệu, góp phần thúc đẩy thị trường dữ liệu phát triển đồng thời bảo đảm vững chắc chủ quyền số và an ninh quốc gia trong kỷ nguyên số.



## PHỤ LỤC

### *Phản bác các quan điểm sai sự thật về sản phẩm, dịch vụ về dữ liệu*

Dữ liệu đang trở thành tài nguyên chiến lược trong quá trình xây dựng và bảo vệ Tổ quốc xã hội chủ nghĩa, là “tài nguyên mới”, “năng lượng mới” của nền kinh tế số. Thực hiện chỉ đạo của Bộ Chính trị tại Nghị quyết số 57-NQ/TW về chuyển đổi số quốc gia, Đảng và Nhà nước đã nhanh chóng hoàn thiện khung pháp lý về quản lý và phát triển dữ liệu. Điểm nhấn là Luật Dữ liệu 2024 (số 60/2024/QH15) được Quốc hội thông qua, có hiệu lực từ 1/7/2025, là đạo luật chuyên biệt đầu tiên quy định toàn diện về dữ liệu số - từ xây dựng, bảo vệ, xử lý đến chia sẻ, sử dụng và cả các sản phẩm, dịch vụ dữ liệu. Tiếp đó, Luật Bảo vệ dữ liệu cá nhân 2025 và Nghị định 13/2023/NĐ-CP về quản lý dữ liệu cá nhân lần lượt được ban hành nhằm bảo vệ quyền lợi của công dân trong môi trường số. Những chính sách này đều nhằm xây dựng môi trường dữ liệu minh bạch, an toàn, thúc đẩy phát triển kinh tế số bền vững.

Tuy nhiên, trong bối cảnh đó lại xuất hiện những luận điệu xuyên tạc, sai sự thật từ một số trang mạng nước ngoài và thế lực thù địch. Họ lợi dụng việc Việt Nam hoàn thiện luật về dữ liệu để dựng lên viễn cảnh “cơ quan chức năng thu thập dữ liệu cá nhân tùy tiện”, “dữ liệu trở thành công cụ kiểm soát xã hội” hay “giam hãm thị trường công nghệ trong tay nhà nước”... Những thông tin này không chỉ thiếu cơ sở pháp lý mà còn lệch lạc so với thực tiễn chính sách của Đảng và Nhà nước ta.

Luật Dữ liệu 2024 mở ra khung pháp lý đầu tiên cho thị trường dữ liệu tại Việt Nam. Luật quy định 03 nhóm dịch vụ về dữ liệu căn bản trong Chương IV (Điều 39-43), gồm <sup>(1)</sup>sản phẩm, dịch vụ dữ liệu, <sup>(2)</sup>trung gian dữ liệu, <sup>(3)</sup>phân tích, tổng hợp dữ liệu và 02 điều về sàn giao dịch dữ liệu, trách nhiệm của tổ chức thực hiện. Đây là những thành phần thiết yếu của “thị trường dữ liệu” nơi dữ liệu được trao đổi, mua bán và tạo ra giá trị mới. Luật quy định chi tiết điều kiện kinh doanh, giới hạn chủ thể cung cấp và trách nhiệm pháp lý cho từng loại hình, nhằm khuyến khích phát triển đồng thời đảm bảo an toàn, bảo mật trong giao dịch dữ liệu. Chẳng



hạn, dịch vụ xác thực điện tử tương tự “công chứng số” chỉ được cung cấp bởi các đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước đủ điều kiện, nhằm đảm bảo tính chính xác và độ tin cậy cao đối với dữ liệu quan trọng. Điều này hoàn toàn phù hợp với xu hướng quốc tế, nhiều nước giao cho cơ quan nhà nước hoặc đơn vị được ủy quyền thực hiện dịch vụ xác thực điện tử (ví dụ Singapore với Singpass, Hàn Quốc với chứng minh thư điện tử).

Luật Dữ liệu cũng thể chế hóa quyền tài sản về dữ liệu, tạo cơ hội thị trường cho các doanh nghiệp công nghệ phát triển sản phẩm, dịch vụ mới. Cụ thể, Luật khuyến khích phát triển mạnh các sản phẩm, dịch vụ dữ liệu số và quy định ưu đãi cho doanh nghiệp trong lĩnh vực này tương tự như ngành công nghệ cao (*ưu đãi thuế, đất đai, vốn*). Đồng thời, Luật Dữ liệu áp dụng nguyên tắc “khung khổ chung và chuyên ngành” để tránh mâu thuẫn với hệ thống pháp luật hiện hành: mọi hoạt động liên quan dữ liệu cá nhân, an ninh mạng, thương mại điện tử... đều phải tuân thủ quy định của các luật chuyên ngành tương ứng. Ví dụ, dịch vụ phân tích dữ liệu có sử dụng dữ liệu cá nhân phải tuân thủ Luật Bảo vệ dữ liệu cá nhân, hoạt động của sàn giao dịch dữ liệu phải phù hợp với Luật Thương mại điện tử và Luật Giao dịch điện tử, những dịch vụ về an toàn thông tin mạng tuân theo Luật An toàn thông tin mạng, dữ liệu mật thuộc lĩnh vực cơ yếu, quân sự tuân theo Luật Cơ yếu, Luật Quốc phòng, Luật An ninh mạng....

Đáng chú ý, Luật Dữ liệu loại trừ một số sản phẩm, dịch vụ dữ liệu thuộc lĩnh vực đặc thù ra khỏi phạm vi điều chỉnh. Cụ thể, các hoạt động liên quan đến dữ liệu điện tử thương mại, viễn thông, công nghiệp công nghệ thông tin, công nghiệp quốc phòng, an ninh mạng... tiếp tục thực hiện theo pháp luật chuyên ngành. Quy định này khẳng định Luật Dữ liệu chỉ tập trung điều chỉnh thị trường dữ liệu mới, không ôm đùm tất cả mà tôn trọng ranh giới với các luật hiện hành.

Trên thực tế, ngay từ trước khi Luật Dữ liệu được ban hành, Nhà nước đã bổ sung ngành nghề “Kinh doanh sản phẩm, dịch vụ trung gian dữ liệu” và “Kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu” vào danh mục kinh doanh có điều kiện trong Luật Đầu tư. Điều này cho thấy rõ các dịch vụ dữ liệu mới sẽ phải đăng



ký và đáp ứng điều kiện pháp lý chặt chẽ trước khi được kinh doanh. Việc quản lý này đảm bảo chỉ những tổ chức đủ năng lực và tuân thủ luật mới được hoạt động, tránh tình trạng “giao dịch dữ liệu tràn lan không kiểm soát”.

Thực tiễn quốc tế cũng cho thấy xu hướng tương tự. Liên minh châu Âu đã ban hành Đạo luật Quản trị Dữ liệu nhằm thiết lập một “không gian dữ liệu chung” an toàn, trong đó các tổ chức trung gian dữ liệu phải đảm bảo trung lập, minh bạch và không trực lợi tiếp từ dữ liệu. Nhiều nước châu Á như Singapore, Hàn Quốc đã xây dựng hệ thống định danh điện tử quốc gia và yêu cầu các nền tảng dữ liệu tuân thủ tiêu chuẩn bảo mật nghiêm ngặt. Việt Nam cũng theo đuổi mô hình tương đồng, lập Trung tâm Dữ liệu Quốc gia và cơ sở dữ liệu tổng hợp quốc gia đáp ứng tiêu chuẩn quốc tế về hạ tầng và an toàn thông tin

Một số luận điệu cho rằng Luật Dữ liệu là “mở đường” cho cơ quan nhà nước thu thập dữ liệu cá nhân vô giới hạn hoặc “độc quyền” toàn bộ các dịch vụ dữ liệu. Thực tế hoàn toàn ngược lại. Chính sách của chúng ta khuyến khích phát triển đa dạng sản phẩm, dịch vụ dữ liệu trong khuôn khổ pháp lý rõ ràng. Các quy định về cấm và điều kiện được công khai minh bạch: Luật Dữ liệu nghiêm cấm các sản phẩm, dịch vụ xâm phạm an ninh, quốc phòng, quyền riêng tư; đồng thời quy định dữ liệu cá nhân không được coi là hàng hóa thông thường và cấm mua bán tùy tiện. Điều này hoàn toàn phù hợp thông lệ quốc tế mà Bộ trưởng Bộ Công an Đại tướng Lương Tam Quang đã nhấn mạnh: “Dữ liệu cá nhân là tài nguyên đặc biệt, gắn với quyền nhân thân, quyền riêng tư... không thể coi đây là hàng hóa tài sản thông thường”. Luật Bảo vệ Dữ liệu cá nhân và Luật Dữ liệu đều thể chế hóa quan điểm đó: trao quyền cho cá nhân kiểm soát dữ liệu của mình, đồng thời cấm tuyệt đối hành vi mua bán, kinh doanh dữ liệu cá nhân tùy tiện. Theo Tiến sĩ Lê Văn Hải (Ban Cơ yếu Chính phủ), Luật Dữ liệu cùng Luật Bảo vệ Dữ liệu cá nhân tạo ra hành lang pháp lý toàn diện để thu thập, chia sẻ đồng thời bảo vệ dữ liệu một cách xuyên biên giới, góp phần hình thành “niềm tin số” giữa các bên tham gia giao dịch điện tử. Vì vậy, luận điệu cho rằng việc hoàn thiện pháp luật



dữ liệu là nhằm tăng cường kiểm soát hay bỏ lọt dữ liệu cá nhân của công dân là hoàn toàn sai sự thật.



*Hình ảnh: Đại tướng Lương Tam Quang, Bộ trưởng Bộ Công an phát biểu trước Quốc hội về vấn đề bảo vệ dữ liệu cá nhân. Ảnh: Báo ANTĐ*

Bên cạnh quy định phát triển thị trường dữ liệu, hệ thống pháp luật mới cũng đặt trọng tâm vào việc đảm bảo an ninh, an toàn dữ liệu. Luật Dữ liệu 2024 quy định ngay từ cấp luật những giải pháp kỹ thuật, tổ chức và chính sách tổng thể nhằm phòng ngừa rủi ro và bảo vệ dữ liệu trên mọi khía cạnh xử lý.

Về pháp lý, Luật yêu cầu phân loại dữ liệu rõ ràng: cơ quan nhà nước phân định dữ liệu “dùng chung, dùng riêng, dữ liệu mỏ” và đặc biệt xác định danh mục dữ liệu quan trọng, dữ liệu cốt lõi liên quan đến quốc phòng, an ninh, kinh tế vĩ mô.... Các dữ liệu quan trọng và cốt lõi này phải được bảo vệ ở mức cao nhất, tuân thủ quy định tại Điều 27 Luật Dữ liệu về các biện pháp bảo vệ dữ liệu (xây dựng chính sách nội bộ, quản lý truy cập, mã hóa, sao lưu, đào tạo...). Đồng thời, Điều 25 Luật Dữ liệu giao cho cơ quan chuyên trách (thuộc Bộ Công an, Bộ Quốc phòng) phối hợp thường xuyên đánh giá rủi ro, giám sát sớm các mối đe dọa trên không



gian mạng. Như vậy, pháp luật buộc các cơ quan nhà nước và doanh nghiệp xử lý dữ liệu phải tự chủ đảm bảo an toàn thông tin, có cơ chế cảnh báo và phối hợp với lực lượng an ninh mạng khi cần thiết, thay vì để lỗ hổng dữ liệu bị khai thác.

Luật Dữ liệu cũng đề ra trách nhiệm cụ thể cho Trung tâm Dữ liệu quốc gia với vai trò là hạt nhân của hệ thống quản lý dữ liệu quốc gia. Hạ tầng của Trung tâm này phải đáp ứng tiêu chuẩn quốc tế về trung tâm dữ liệu, từ thiết bị đến bảo vệ vật lý (chống bom đạn, khủng bố, thiên tai). Bên cạnh đó, Trung tâm phải có các giải pháp an ninh mạng, kiểm soát truy cập, dự phòng tài nguyên để đảm bảo tính liên tục, ổn định của hệ thống. Điều 30 và 31 của Luật Dữ liệu quy định rõ nhiệm vụ của Trung tâm trong lưu trữ, khai thác và giám sát chất lượng dữ liệu, đồng thời chịu trách nhiệm thực hiện các biện pháp bảo vệ dữ liệu. Nhờ vậy, Trung tâm Dữ liệu quốc gia vừa là nơi lưu trữ tập trung an toàn, vừa là đầu mối giám sát an toàn dữ liệu quốc gia. Việc xây dựng cơ sở dữ liệu tổng hợp quốc gia cũng phải tuân thủ các tiêu chuẩn an toàn thông tin và bảo vệ dữ liệu cá nhân, đảm bảo kết nối thông suốt với các hệ thống khác mà không ảnh hưởng đến an ninh mạng.

Về giải pháp kỹ thuật và tổ chức, Nhà nước thúc đẩy việc triển khai các biện pháp công nghệ hiện đại: sử dụng các giao thức mã hóa mạnh (ví dụ AES-256) trong lưu trữ và truyền dẫn, áp dụng tường lửa thế hệ mới, phát hiện xâm nhập (IDS/IPS), kiểm toán hệ thống, xử lý nhật ký truy cập.... Mọi quy trình xử lý dữ liệu quan trọng phải được thực hiện theo hợp đồng và hồ sơ lưu trữ chặt chẽ. Công tác đào tạo, nâng cao ý thức về an toàn dữ liệu cho cán bộ công chức và người dân cũng được quan tâm; các quy định pháp luật khuyến khích doanh nghiệp đầu tư vào hệ thống bảo mật dữ liệu nội bộ. Thực tế từ các vụ lộ lọt dữ liệu cho thấy, nhiều sự cố không phải do thiếu quy định mà do sơ suất của chính người dùng và tổ chức. Khảo sát của Cục An toàn thông tin (Năm 2021, Bộ Thông tin và Truyền thông trước đây) cho thấy hơn 80% nguyên nhân lộ lọt dữ liệu cá nhân xuất phát từ sự bất cẩn của người dùng (như cung cấp số điện thoại, địa chỉ công khai trên mạng mà không kiểm soát). Vì vậy, bên cạnh chế pháp lý, công tác tuyên truyền, nâng cao nhận thức cộng đồng về bảo vệ dữ liệu cá nhân được



đặc biệt chú trọng. Như báo chí Nhà nước đã phản ánh, Chính phủ và các cơ quan chức năng thường xuyên tổ chức chiến dịch huấn luyện, tập huấn, và thiết lập kênh tiếp nhận phản ánh về an ninh mạng để người dân chủ động phòng ngừa, kịp thời ứng phó với nguy cơ mất an toàn dữ liệu.

Đối với các giải pháp hợp tác quốc tế và nâng cao năng lực, chúng ta tích cực trao đổi kinh nghiệm với các nước phát triển và tuân thủ chuẩn mực toàn cầu. Luật Dữ liệu cho phép việc chia sẻ dữ liệu giữa tổ chức trong và ngoài nước khi đáp ứng quy định an toàn, đồng thời thống nhất quy định cho tổ chức nước ngoài tham gia xử lý dữ liệu liên quan Việt Nam. Luật Bảo vệ dữ liệu cá nhân (dự kiến có hiệu lực từ 1/1/2026) sẽ bổ sung thêm cơ chế cấp chứng nhận, thẩm định đánh giá tác động dữ liệu, và quy định chặt chẽ về chuyển dữ liệu ra nước ngoài. Song song đó, Việt Nam tham gia các hiệp định quốc tế liên quan và triển khai một số hoạt động hợp tác (diễn đàn, hội nghị, thỏa thuận) về an toàn dữ liệu để cập nhật công nghệ bảo mật mới như trí tuệ nhân tạo, blockchain, đồng thời hỗ trợ nguồn lực cho doanh nghiệp quốc phòng-công nghệ nghiên cứu giải pháp bảo vệ cơ sở dữ liệu quan trọng.

Ngoài ra, thông tin xuyên tạc cho rằng Việt Nam không chú trọng đảm bảo an ninh dữ liệu, hay coi nhẹ quyền riêng tư của người dân là hoàn toàn không chính xác. Thực tế, Luật Dữ liệu và hệ thống văn bản liên quan đề ra yêu cầu rất nghiêm ngặt về bảo mật. Đặc biệt, Luật được xây dựng theo hướng hậu kiểm - trao quyền cho doanh nghiệp tự thiết kế giải pháp bảo mật và chỉ can thiệp khi phát hiện vi phạm. Điều này vừa giảm gánh nặng thủ tục hành chính, vừa khuyến khích đổi mới sáng tạo trong việc phòng ngừa rủi ro. Mặt khác, Nhà nước sẵn sàng xử lý nghiêm các hành vi xâm phạm dữ liệu cá nhân theo quy định của Luật An ninh mạng, Luật An toàn thông tin mạng và Luật Bảo vệ dữ liệu cá nhân. Những cảnh báo về nguy cơ “dữ liệu bị thu thập tùy tiện” hoàn toàn không trùng khớp với quy định thực tế. Chỉ trong các tình huống khẩn cấp (*thiên tai, dịch bệnh, an ninh quốc gia*), mới có cơ chế cho cơ quan nhà nước yêu cầu cung cấp dữ liệu mà không cần sự đồng ý của chủ thể - nhưng ngay cả trong trường hợp đó cũng



phải đặt trong khuôn khổ pháp luật chặt chẽ. Các cơ quan được trao quyền này chỉ gồm những chức danh cấp cao (*Bộ trưởng, Chủ tịch UBND tỉnh, Giám đốc Trung tâm Dữ liệu Quốc gia, Giám đốc Công an tỉnh...*) và phải có văn bản nêu rõ mục đích, loại dữ liệu, cơ sở pháp lý, thời hạn cung cấp. Ở những trường hợp thông thường, mọi tổ chức, doanh nghiệp đều được khuyến khích chia sẻ dữ liệu tự nguyện vì lợi ích chung (y tế, môi trường, nghiên cứu khoa học...) và chỉ khi có sự đồng thuận của chủ thẻ dữ liệu hoặc chủ sở hữu.

Trong bối cảnh “thế giới phẳng” của thông tin hiện nay, các luận điệu vu cáo Việt Nam về dữ liệu cũng so sánh thiếu căn cứ với các nước khác. Trái lại, Việt Nam đang cùng cả khu vực hướng đến mục tiêu chung: phát triển kinh tế số bền vững gắn liền với bảo vệ dữ liệu cá nhân và an ninh mạng. Như Bộ trưởng Công an Lương Tam Quang từng khẳng định, trên thế giới đã có khoảng 150 quốc gia ban hành luật bảo vệ dữ liệu cá nhân - một xu hướng tất yếu trong thời đại số. Chính phủ Việt Nam xác định bảo vệ dữ liệu cá nhân là nhiệm vụ trọng tâm, thể hiện từ việc soạn thảo dự thảo Luật Bảo vệ dữ liệu cá nhân trên tinh thần cầu thi, nghiên cứu kỹ lưỡng kinh nghiệm quốc tế và lấy ý kiến rộng rãi. Sự minh bạch trong xây dựng chính sách, cùng chế tài xử lý nghiêm khắc với hành vi mua bán, lộ lọt dữ liệu cá nhân, là minh chứng cho thấy Việt Nam không hề “lỏng lẻo” trong vấn đề này. Ngược lại, chúng ta đang tiếp thu thông lệ quốc tế để hoàn thiện pháp luật, song vẫn bảo đảm phù hợp với điều kiện Việt Nam.

Việt Nam đang bước vào kỷ nguyên chuyển đổi số với quyết tâm cao, lấy dữ liệu làm trung tâm của phát triển kinh tế - xã hội. Các văn bản pháp luật mới nhất (*Luật Dữ liệu 2024, Luật BV Dữ liệu cá nhân 2025, Nghị định 13/2023...*) đã thiết lập hành lang pháp lý toàn diện cho quản trị, khai thác và bảo vệ dữ liệu.

Trên cơ sở đó, Chính phủ và các bộ ngành triển khai nhiều giải pháp đồng bộ: xây dựng Trung tâm Dữ liệu quốc gia, ban hành tiêu chuẩn kỹ thuật, cơ chế giám sát, hợp tác quốc tế và đầu tư cơ sở hạ tầng kỹ thuật hiện đại. Tất cả những chính sách này đều nhằm biến dữ liệu thành tài sản quốc gia, vừa phát



huy lợi ích kinh tế - xã hội, vừa đảm bảo chủ quyền, an ninh, quyền riêng tư của mỗi người dân.

Trước những âm mưu lợi dụng công nghệ để xuyên tạc, kích động hoang mang dư luận, mỗi cán bộ, đảng viên và người dân cần nâng cao cảnh giác, chủ động tìm hiểu thông tin chính thống. Chúng ta hoàn toàn có cơ sở để tin rằng, pháp luật về dữ liệu tại Việt Nam được xây dựng công phu, thận trọng và tiến bộ, theo đúng quan điểm của Đảng và Nhà nước, phát triển kinh tế số nhưng phải song hành với bảo vệ quyền con người. Những thông tin trái chiều cẩn cứ chỉ nhằm hạ thấp chủ trương đúng đắn của ta và gây nhiễu loạn nhận thức xã hội. Vì vậy, mỗi người cần tìm hiểu kỹ các quy định đã được công bố chính thức và thực tế triển khai của hệ thống pháp luật này, qua đó trang bị niềm tin vững chắc rằng Việt Nam đang đi đúng đường lối trong công cuộc làm giàu dữ liệu, bảo đảm an ninh, an toàn trong kỷ nguyên số.



## TÀI LIỆU THAM KHẢO

1. Luật Dữ liệu (*Luật số 60/2024/QH15*);
2. Luật An ninh mạng (*Luật số 24/2018/QH14*);
3. Luật An toàn thông tin mạng (*Luật số 86/2015/QH13*);
4. Luật Bảo vệ dữ liệu cá nhân (*Luật số 91/2025/QH15*) Luật sửa đổi, bổ sung một số điều của Luật Quy hoạch, Luật Đầu tư, Luật Đầu tư theo phương thức đối tác công tư và Luật Đầu thầu (*Luật số 57/2024/QH15*);
5. Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân;
6. Nghị quyết số 57-NQ/TW ngày 22/12/2024 về phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;
7. Nghị định số 169/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định hoạt động khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ về dữ liệu;
9. Quyết định số 20/2025/QĐ-TTg ngày 01/7/2025 của Thủ tướng Chính phủ ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi;
10. Đinh Phạm Minh Nghĩa, Nguyễn Kim Ngân, Vũ Thị Mỹ Hà - Trường Đại học Luật Hà Nội, Kinh nghiệm Singapore về tích hợp thông tin dân cư, 2025.



**Câu 8: Nội dung quản lý nhà nước về dữ liệu? Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu? Nhiệm vụ trọng tâm cần tập trung trong gian đoạn từ nay đến năm 2030?**





**Câu 8: Nội dung quản lý nhà nước về dữ liệu? Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu? Nhiệm vụ trọng tâm cần tập trung trong gian đoạn từ nay đến năm 2030?**

**Trả lời**

**8.1. Nội dung quản lý nhà nước về dữ liệu**

Trong kỷ nguyên số, dữ liệu được định vị là nguồn tài nguyên chiến lược mới, quyết định năng lực quản trị quốc gia, phát triển kinh tế - xã hội và bảo đảm quốc phòng - an ninh. Việt Nam đã ban hành Luật Dữ liệu 2024 đạo luật đầu tiên quy định toàn diện về dữ liệu số. Việc tổ chức quản lý nhà nước hiệu quả đối với dữ liệu, đặc biệt là vai trò của Bộ Công an và lực lượng Công an các cấp, có ý nghĩa then chốt trong thực thi Luật Dữ liệu và thúc đẩy chuyển đổi số quốc gia.

Điều 8 Luật Dữ liệu 2024 quy định quản lý nhà nước về dữ liệu số bao gồm nhiều nội dung toàn diện từ thể chế đến kỹ thuật, cụ thể:

- **Thứ nhất**, xây dựng chiến lược và thể chế: Xây dựng, ban hành và thực thi Chiến lược dữ liệu quốc gia; xây dựng văn bản quy phạm pháp luật về dữ liệu; ban hành các tiêu chuẩn, quy chuẩn kỹ thuật và định mức kinh tế - kỹ thuật, tiêu chí chất lượng liên quan đến dữ liệu.
- **Thứ hai**, tuyên truyền, hướng dẫn và phổ biến pháp luật: Tuyên truyền, phổ biến chính sách, pháp luật về dữ liệu; hướng dẫn các cơ quan, tổ chức trong việc xây dựng, phát triển, bảo vệ, quản trị, xử lý và sử dụng dữ liệu.
- **Thứ ba**, quản lý, giám sát toàn diện dữ liệu: Quản lý và giám sát các hoạt động thu thập, tạo lập, xây dựng, phát triển, bảo vệ, quản trị, xử lý, lưu trữ, phân tích, chia sẻ và khai thác dữ liệu; đảm bảo an ninh, an toàn dữ liệu trong suốt vòng đời dữ liệu. Việc bảo đảm chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh mạng, an ninh dữ liệu và an toàn thông tin của tổ chức, cá nhân được xem là yêu cầu xuyên suốt trong quá trình phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số.



- **Thứ tư**, thống kê, nghiên cứu, phát triển thị trường dữ liệu: Thực hiện báo cáo, thống kê về dữ liệu; thúc đẩy nghiên cứu khoa học - công nghệ về dữ liệu; quản lý các sản phẩm, dịch vụ liên quan đến dữ liệu, kể cả các sàn giao dịch dữ liệu; giám sát và phát triển thị trường dữ liệu phục vụ phát triển kinh tế - xã hội.

- **Thứ năm**, thanh tra, kiểm tra, giải quyết vi phạm: Tiến hành thanh tra, kiểm tra chuyên ngành về dữ liệu; giải quyết khiếu nại, tố cáo và xử lý các vi phạm pháp luật trong hoạt động về dữ liệu.

- **Thứ sáu**, phát triển nhân lực và hợp tác quốc tế: Đào tạo, bồi dưỡng nguồn nhân lực chuyên môn về dữ liệu; tăng cường hợp tác quốc tế trong chia sẻ, khai thác và bảo vệ dữ liệu.

Đáng chú ý, quản lý nhà nước về dữ liệu còn bao hàm việc bảo vệ dữ liệu cá nhân. Theo Luật Bảo vệ Dữ liệu Cá nhân 2025, các quyền, nghĩa vụ và trách nhiệm của cơ quan, tổ chức, cá nhân liên quan đến dữ liệu cá nhân được quy định rõ. Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý các hành vi vi phạm liên quan. Việc quản lý dữ liệu phải tuân thủ chặt chẽ pháp luật về an toàn thông tin mạng, an ninh mạng và bảo vệ dữ liệu cá nhân, nhằm bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

## 8.2. Vai trò, trách nhiệm của Bộ Công an và Công an các cấp trong quản lý dữ liệu

### 8.2.1. Bộ Công an là cơ quan đầu mối quản lý nhà nước về dữ liệu

Bộ Công an được giao giữ vai trò cơ quan đầu mối thống nhất quản lý nhà nước về dữ liệu trên phạm vi cả nước (*trừ lĩnh vực thuộc quản lý của Bộ Quốc phòng*). Cụ thể, Điều 8 Luật Dữ liệu 2024 quy định Bộ Công an chịu trách nhiệm trước Chính phủ trong việc thực hiện quản lý nhà nước về dữ liệu số, phối hợp với các bộ, ngành khác và UBND cấp tỉnh để triển khai các nhiệm vụ quản lý dữ liệu. Điều này có nghĩa Bộ Công an đóng vai trò trung tâm trong xây dựng thể chế, chính sách về dữ liệu; hướng dẫn, kiểm tra việc thực thi pháp



luật về dữ liệu; và đôn đốc, giám sát việc bảo đảm an ninh, an toàn dữ liệu trên toàn quốc.

Trong lĩnh vực bảo vệ dữ liệu cá nhân, Bộ Công an là cơ quan chuyên trách. Cụ thể, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) Bộ Công an được giao nhiệm vụ là cơ quan chuyên trách bảo vệ dữ liệu cá nhân, giúp Bộ Công an thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân. A05 có thẩm quyền tiếp nhận, thẩm định các hồ sơ đánh giá tác động xử lý dữ liệu cá nhân cũng như hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài; có quyền yêu cầu tạm dừng hoặc ngừng việc chuyển dữ liệu ra nước ngoài nếu phát hiện vi phạm hoặc nguy cơ đe doạ đến an ninh quốc gia. Bên cạnh đó, Bộ Công an cũng chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng; phòng, chống tội phạm mạng và phối hợp xử lý các thông tin, nội dung vi phạm pháp luật (ví dụ: thông tin xâm hại trẻ em trên mạng) để bảo vệ dữ liệu và không gian mạng an toàn.

Đồng thời, một trọng trách mới, rất quan trọng của Bộ Công an là xây dựng và quản lý Trung tâm dữ liệu quốc gia, đây là hạ tầng “lõi” của chuyển đổi số quốc gia. Theo Nghị quyết số 175/NQ-CP ngày 30/10/2023, Chính phủ đã phê duyệt Đề án Trung tâm dữ liệu quốc gia, giao Bộ Công an thành lập Trung tâm dữ liệu quốc gia là đơn vị tương đương cấp Cục trực thuộc Bộ Công an. Tháng 2/2025, Bộ Công an đã công bố thành lập Trung tâm này, trực tiếp do Bộ trưởng Bộ Công an chỉ đạo. Trung tâm dữ liệu quốc gia có nhiệm vụ xây dựng, quản lý, khai thác và vận hành hạ tầng kỹ thuật để tích hợp, đồng bộ, lưu trữ, chia sẻ, phân tích và điều phối dữ liệu từ các cơ quan nhà nước, hình thành kho dữ liệu về con người (*dữ liệu dân cư, hộ tịch, căn cước,...*) và kho dữ liệu tổng hợp quốc gia từ các cơ sở dữ liệu của bộ, ngành. Dữ liệu tại Trung tâm dữ liệu quốc gia sẽ là nền tảng cốt lõi để cung cấp các dịch vụ dữ liệu phục vụ hoạch định chính sách, xây dựng Chính phủ số, phát triển kinh tế - xã hội số, bảo đảm quốc phòng an ninh; đồng thời Trung tâm cung cấp hạ tầng công nghệ thông tin dùng chung cho các cơ quan Đảng, Nhà nước và tổ chức chính trị -



xã hội có nhu cầu khai thác dữ liệu, góp phần nâng cao hiệu quả, tiết kiệm chi phí và bảo đảm an ninh mạng.

Để thực hiện vai trò này, Bộ Công an chịu trách nhiệm đầu tư cơ sở vật chất, hạ tầng kỹ thuật cho Trung tâm dữ liệu quốc gia. Luật Dữ liệu quy định Nhà nước ưu tiên bố trí đất đai, trụ sở, ngân sách để xây dựng và vận hành Trung tâm dữ liệu quốc gia cũng như cơ sở dữ liệu tổng hợp quốc gia. Bộ Công an đã lên kế hoạch phát triển Trung tâm dữ liệu quốc gia theo lộ trình 3 giai đoạn: 2023-2025 (*xây dựng cơ sở hạ tầng ban đầu*), 2026-2028 (*mở rộng quy mô, nâng cao năng lực*) và 2029-2030 (*phát triển hoàn thiện*). Bộ Công an cũng được giao nhiệm vụ phối hợp ban hành Khung quản trị dữ liệu tổng thể và Bộ tiêu chuẩn về kiến trúc cơ sở dữ liệu để các bộ, ngành, địa phương tuân thủ khi tích hợp vào Trung tâm (*hoàn thành trong tháng 8/2025*). Ngoài ra, Trung tâm dữ liệu quốc gia dưới sự quản lý của Bộ Công an có trách nhiệm hướng dẫn các cơ quan áp dụng tiêu chuẩn dữ liệu, giám sát chất lượng dữ liệu chia sẻ về Trung tâm và điều phối việc kết nối, đồng bộ dữ liệu từ các cơ sở dữ liệu quốc gia, chuyên ngành.

Nhằm đảm bảo vận hành an toàn, Bộ Công an còn tổ chức các đơn vị chuyên môn trong Trung tâm dữ liệu quốc gia, như Phòng An ninh, an toàn hệ thống, để bảo vệ an ninh mạng và an toàn thông tin cho toàn bộ hạ tầng dữ liệu quốc gia. Bộ trưởng Bộ Công an đã quán triệt yêu cầu hạ tầng của Trung tâm dữ liệu quốc gia phải hiện đại, đồng bộ, an toàn tuyệt đối, sẵn sàng vận hành chính thức từ ngày 19/8/2025 theo tiến độ đề ra.

Bên cạnh những nhiệm vụ trên, Bộ Công an còn chủ trì xây dựng, trình ban hành các văn bản quy phạm pháp luật hướng dẫn thi hành Luật Dữ liệu (*nghị định, thông tư*); định ra cơ chế phối hợp liên ngành trong quản trị dữ liệu; xây dựng Cổng dữ liệu quốc gia và sàn giao dịch dữ liệu mở; đồng thời quyết định các mức chi phí kết nối, chia sẻ dữ liệu. Bộ cũng đặc biệt chú trọng phát triển đội ngũ cán bộ dữ liệu, hướng dẫn công tác phân loại dữ liệu tại các cơ quan; tổ chức đào tạo, bồi dưỡng cán bộ chuyên trách về quản trị, phân tích, bảo mật dữ liệu; và có cơ



ché thu hút nhân tài công nghệ thông tin, khoa học dữ liệu phục vụ lâu dài trong lực lượng Công an nhân dân.

### 8.2.2. Công an các đơn vị, địa phương

Lực lượng Công an ở các đơn vị, địa phương (*Công an tỉnh, thành phố, xã, phường...*) có trách nhiệm cụ thể trong phạm vi địa bàn mình quản lý nhằm thực thi hiệu quả các chính sách về dữ liệu:

- **Trước hết**, phải triển khai thi hành Luật Dữ liệu tại cơ sở: Công an các tỉnh/thành phố hợp với UBND cùng cấp xây dựng và phát triển các cơ sở dữ liệu thuộc phạm vi quản lý của địa phương, đảm bảo kết nối đồng bộ với Trung tâm dữ liệu quốc gia theo lộ trình chung. Các cơ sở dữ liệu quan trọng phục vụ quản lý nhà nước (*nhiều cơ sở dữ liệu dân cư, căn cước, hộ khẩu, dữ liệu an ninh trật tự...*) do Công an quản lý sẽ được chuyển đổi, tích hợp về Trung tâm dữ liệu quốc gia theo hướng dẫn của Bộ Công an. Tuy nhiên, Công an địa phương vẫn tiếp tục vận hành, khai thác cơ sở dữ liệu trong phạm vi nhiệm vụ của mình, đồng thời phối hợp với Trung tâm dữ liệu quốc gia để đảm bảo an ninh, an toàn thông tin cho dữ liệu.

- **Thứ hai**, thực hiện nhiệm vụ quản lý, khai thác cơ sở dữ liệu chuyên ngành: Công an các đơn vị nghiệp vụ ở trung ương và địa phương đang là chủ quản nhiều cơ sở dữ liệu quốc gia quan trọng (*nhiều Cơ sở dữ liệu Quốc gia về dân cư, Cơ sở dữ liệu căn cước công dân, Cơ sở dữ liệu đăng ký phương tiện, lý lịch tư pháp,...*). Trách nhiệm của các đơn vị này là cập nhật, duy trì dữ liệu “đúng, đủ, sạch, sống”, thường xuyên kiểm tra, giám sát chất lượng dữ liệu và thực hiện đồng bộ dữ liệu về Trung tâm dữ liệu quốc gia. Đồng thời, Công an địa phương phối hợp với các sở, ban ngành để thúc đẩy chia sẻ dữ liệu giữa các hệ thống thông tin trên địa bàn phục vụ giải quyết thủ tục hành chính, dịch vụ công.



Hình ảnh: Bộ trưởng Bộ Công an Tô Lâm (2023) phát biểu tại Phiên họp lần thứ 5 Ủy ban Quốc gia về chuyển đổi số và Tổ công tác triển khai Đề án 06.

Ảnh: Báo Chính phủ

- **Thứ ba**, bảo đảm an ninh dữ liệu tại địa phương: Công an tỉnh, thành phố là lực lượng nòng cốt trong bảo vệ an ninh mạng, an toàn dữ liệu tại địa bàn. Theo Luật An ninh mạng, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao các địa phương có trách nhiệm phối hợp với A05 để kiểm tra, đánh giá an ninh mạng đối với các hệ thống thông tin quan trọng; phòng ngừa, phát hiện và đấu tranh với tội phạm mạng và các hành vi xâm phạm dữ liệu. Giám đốc Công an cấp tỉnh có quyền yêu cầu các cơ quan, tổ chức trên địa bàn cung cấp dữ liệu cần thiết cho công tác điều tra, an ninh theo quy định pháp luật, đồng thời có thẩm quyền xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng, an toàn thông tin trên địa bàn.

- **Thứ tư**, thực hiện nhiệm vụ tuyên truyền, hướng dẫn người dân và doanh nghiệp: Công an cơ sở (*đặc biệt là lực lượng quản lý hành chính, an ninh trật tự*) tổ chức tuyên truyền rộng rãi về các quy định của pháp luật liên quan đến dữ liệu



(chẳng hạn quy định về đăng ký, khai thác thông tin dân cư, bảo vệ dữ liệu cá nhân...). Khi triển khai các hệ thống dữ liệu mới (như hệ thống định danh và xác thực điện tử, dịch vụ công trực tuyến), Công an địa phương đóng vai trò hướng dẫn người dân, doanh nghiệp thực hiện, qua đó nâng cao nhận thức và ý thức chấp hành pháp luật về dữ liệu trong xã hội.

Như vậy, từ trung ương đến địa phương, lực lượng Công an nhân dân giữ vai trò nòng cốt, vừa là cơ quan quản lý nhà nước chuyên trách về dữ liệu, vừa là đơn vị triển khai trực tiếp các hệ thống dữ liệu phục vụ Chính phủ số. Sự phối hợp đồng bộ giữa Bộ Công an và Công an các cấp quyết định hiệu quả thực thi các chính sách quản lý dữ liệu trong thực tiễn.

### **8.3. Nhiệm vụ trọng tâm giai đoạn 2025-2030: Chuyển đổi số, phát triển NDC và hệ sinh thái dữ liệu an toàn**

Giai đoạn 2025-2030 sẽ là thời kỳ bản lề triển khai chiến lược dữ liệu quốc gia và chuyển đổi số một cách toàn diện tại Việt Nam. Nhiều văn bản định hướng đã đề ra các mục tiêu và nhiệm vụ cụ thể cho giai đoạn này, tiêu biểu là Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng 2030 (*Quyết định 749/QĐ-TTg ngày 03/6/2020*) và đặc biệt Chiến lược Dữ liệu Quốc gia đến năm 2030 (*Quyết định 142/QĐ-TTg ngày 02/02/2024*). Dựa trên những định hướng đó cũng như nhiệm vụ do Luật Dữ liệu đặt ra, có thể xác định một số nhiệm vụ trọng tâm sau:

#### **8.3.1. Hoàn thiện thể chế pháp luật về dữ liệu**

Nhiệm vụ trước mắt (2025) là ban hành đồng bộ văn bản hướng dẫn thi hành Luật Dữ liệu bảo đảm hiệu lực đồng thời với thời điểm luật có hiệu lực. Các văn bản này quy định chi tiết về tiêu chuẩn dữ liệu, phân loại dữ liệu (*dữ liệu cốt lõi, dữ liệu quan trọng quốc gia, dữ liệu mở...*), cơ chế chia sẻ dữ liệu và khai thác dữ liệu, cũng như quy trình vận hành Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp. Song song, cần sớm ban hành Nghị định hướng dẫn thực hiện Luật Bảo vệ Dữ liệu Cá nhân để thay thế nghị định hiện hành, hướng dẫn cụ thể việc thực hiện, tạo cơ sở vững chắc cho các hoạt động thực tế. Nghị định này sẽ phải quy định cụ thể các trường hợp xử lý dữ liệu cá nhân không cần sự đồng ý, thẩm quyền của cơ quan



quản lý, chế tài xử phạt... nhằm tương thích với chuẩn mực quốc tế và thực tiễn trong nước. Ngoài ra, việc hợp nhất Luật An ninh mạng 2018 và Luật An toàn thông tin mạng 2015 cũng đang được Bộ Công an đề xuất, nhằm tạo một môi trường pháp lý thống nhất về an ninh, an toàn mạng, tránh chồng chéo. Giai đoạn đến 2030 sẽ chứng kiến hệ thống pháp luật dữ liệu được hoàn thiện đồng bộ: Luật Giao dịch điện tử (*sửa đổi 2023*) có hiệu lực 2024 cũng chứa một số quy định mới về định danh số, hợp đồng dữ liệu; Luật Lưu trữ cũng tính đến lưu trữ dữ liệu số lâu dài; các thông tư ngành sẽ ban hành tiêu chuẩn dữ liệu ngành. Tất cả tạo nên hành lang pháp lý đầy đủ cho kinh tế dữ liệu và xã hội dữ liệu phát triển.

### **8.3.2. Xây dựng và phát triển hạ tầng Trung tâm dữ liệu quốc gia**

Đây là nhiệm vụ xuyên suốt từ 2023 đến 2030, được chia thành 3 giai đoạn rõ rệt như đã đề cập. Giai đoạn 1 (2023-2025) tập trung xây dựng cơ sở ban đầu, thành lập bộ máy Trung tâm dữ liệu quốc gia, xây dựng các trung tâm dữ liệu giai đoạn 1, tích hợp thí điểm một số cơ sở dữ liệu lớn (*dân cư, doanh nghiệp, đất đai...*) vào hệ thống. Đến Giai đoạn 2 (2026-2028), nhiệm vụ là mở rộng quy mô, hoàn thiện thêm các trung tâm dữ liệu vùng, chuyển dần nhiều hệ thống bộ ngành về Trung tâm dữ liệu quốc gia, mở rộng dung lượng lưu trữ và năng lực xử lý. Giai đoạn 3 (2029-2030), hướng tới phát triển hoàn chỉnh, Trung tâm dữ liệu quốc gia đạt hiệu suất cao, ứng dụng AI và Big Data vào quản trị dữ liệu; kết nối toàn diện với các hệ thống thông tin các cấp; trở thành “trái tim” của hạ tầng số quốc gia như tầm nhìn đặt ra.

Song song xây dựng vật lý, cần phát triển nền tảng dữ liệu quốc gia trên Trung tâm dữ liệu quốc gia. Chiến lược dữ liệu quốc gia giao nhiệm vụ xây dựng các nền tảng chia sẻ, điều phối dữ liệu dùng chung trên Trung tâm dữ liệu quốc gia, đặc biệt là nâng cấp Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (*NDXP*) hiện có để kết nối tất cả bộ, ngành, địa phương. Đến 2030, phần đầu 100% các bộ, địa phương kết nối vào Trung tâm dữ liệu quốc gia và *NDXP*, 100% Cơ sở dữ liệu Quốc gia và Cơ sở dữ liệu chuyên ngành trọng điểm được lưu trữ tại Trung tâm dữ liệu quốc gia hoặc trên hạ tầng điện toán đám mây đáp ứng tiêu chuẩn (*theo*



tinh thần Quyết định 942/QĐ-TTg năm 2021 về phát triển Chính phủ số). Chất lượng hạ tầng Trung tâm dữ liệu quốc gia cũng được nâng cao theo hướng “xanh” và thông minh: sử dụng giải pháp tiết kiệm năng lượng, quản lý nhiệt hiệu quả (theo Green Data Center Roadmap mà IMDA Singapore khuyến nghị), đồng thời áp dụng tự động hóa trong vận hành (AI Ops). Các chỉ số đảm bảo: Uptime Tier-III+, an toàn cấp độ 4 (theo Nghị định 85/2016/NĐ-CP), băng thông mạng nội địa lớn để người dân truy cập dịch vụ dữ liệu mượt mà.

### **8.3.3. Tích hợp và hoàn thiện các cơ sở dữ liệu quốc gia, chuyên ngành**

Dữ liệu chỉ có giá trị khi đầy đủ và chính xác. Giai đoạn tới cần tập trung nguồn lực hoàn thiện các Cơ sở dữ liệu Quốc gia cốt lõi đã được phê duyệt trong danh mục (*dân cư, đất đai, doanh nghiệp, tài chính, bảo hiểm, cán bộ công chức, tư pháp, y tế, giáo dục, thống kê tổng hợp...*). Chiến lược Dữ liệu quốc gia 2030 nhấn mạnh ưu tiên hoàn thiện các Cơ sở dữ liệu Quốc gia nền tảng và các Cơ sở dữ liệu trong danh mục nhiệm vụ chuyển đổi số ngành, lĩnh vực. Điều này đồng nghĩa, đến hết 2025, Cơ sở dữ liệu Quốc gia về dân cư phải hoàn thiện dữ liệu 100% dân số, Cơ sở dữ liệu đất đai hoàn thành giai đoạn I (*quản lý đất đai số ở tất cả tỉnh*), Cơ sở dữ liệu doanh nghiệp liên thông đăng ký kinh doanh - thuế - hải quan, Cơ sở dữ liệu tài chính hình thành kho dữ liệu ngân sách, Cơ sở dữ liệu bảo hiểm kết nối liên thông với y tế, lao động. Việc này đang được đẩy mạnh qua các đề án chuyển đổi số bộ ngành. Ví dụ: Mục tiêu cụ thể năm 2025 của ngành Tài nguyên là phải hoàn thành xây dựng dữ kiện số 100% dữ liệu đất đai, chia sẻ liên thông toàn quốc (Nghị quyết 18-NQ/TW 2022).

Khi các Cơ sở dữ liệu được hoàn thiện rời rạc, nhiệm vụ tiếp theo là tích hợp đồng bộ vào Cơ sở dữ liệu tổng hợp Quốc gia tại Trung tâm dữ liệu quốc gia. Theo Luật Dữ liệu, Thủ tướng sẽ quyết định lộ trình tích hợp này và cần ban hành quyết định lộ trình giai đoạn 2025-2030, ưu tiên tích hợp dữ liệu các lĩnh vực thiết yếu trước (*dân cư, doanh nghiệp, đất*). Việc tích hợp đòi hỏi khắc phục thách thức về chuẩn hóa dữ liệu (*hiện dữ liệu ở các bộ, tỉnh định dạng khác nhau, mã định danh chưa thống nhất*). Do vậy, một nhiệm vụ là xây dựng Bộ tiêu chuẩn, quy chuẩn kỹ



thuật về dữ liệu quốc gia (*Bộ Công an chủ trì ban hành*) áp dụng chung. Bộ trưởng Bộ Công an đã chỉ đạo Trung tâm dữ liệu quốc gia sớm “xây dựng, triển khai Bộ tiêu chuẩn quy hoạch kiến trúc các Cơ sở dữ liệu về phân cấp, phân loại dữ liệu; quy hoạch kho lưu trữ; thiết lập chính sách an ninh, an toàn thông tin cho từng loại dữ liệu”. Có thể hiểu, mỗi loại dữ liệu (*dân cư, y tế, tài chính, bí mật...*) sẽ có mô hình kiến trúc tương ứng trong Trung tâm dữ liệu quốc gia (*phân vùng dữ liệu, phân quyền truy cập*) và tiêu chuẩn bảo mật phù hợp (*mã hóa, ẩn danh, sao lưu...*). Dự kiến đến 2030, danh mục dữ liệu quốc gia mở cũng sẽ hình thành, những dữ liệu công bố công khai để người dân, doanh nghiệp khai thác (*ví dụ dữ liệu thống kê kinh tế - xã hội, dữ liệu bản đồ, khí tượng...*). Theo Luật Dữ liệu, dữ liệu mở của cơ quan nhà nước và dữ liệu dùng chung sẽ được cập nhật vào kho dữ liệu mở dùng chung trên Trung tâm dữ liệu quốc gia để cung cấp rộng rãi. Mục tiêu đến 2030, hầu hết các cơ quan công quyền có cổng dữ liệu mở liên thông với cổng dữ liệu quốc gia (*data.gov.vn*), cung cấp hàng ngàn bộ dữ liệu mở cho cộng đồng.

#### **8.3.4. Phát triển các ứng dụng và dịch vụ dữ liệu, thúc đẩy kinh tế dữ liệu**

Khi hạ tầng và dữ liệu đã sẵn sàng, trọng tâm chuyển sang khai thác dữ liệu phục vụ phát triển. Bộ Công an xác định Trung tâm dữ liệu quốc gia sẽ “phát huy cao độ giá trị của dữ liệu nhằm tạo động lực đổi mới sáng tạo, nâng cao hiệu suất lao động, năng lực cạnh tranh quốc gia”. Cụ thể, một nhiệm vụ là xây dựng “sàn dữ liệu” và “cổng dữ liệu mở”, đây có thể hiểu là nền tảng marketplace cho phép các bộ, địa phương và doanh nghiệp mua bán, trao đổi dữ liệu một cách hợp pháp. Chiến lược dữ liệu quốc gia nêu rõ phải xây dựng các chính sách để đưa dữ liệu trở thành một loại tài sản được pháp luật bảo vệ và hình thành thị trường dữ liệu. Trong giai đoạn tới, Nhà nước sẽ nghiên cứu ban hành cơ chế mua - bán dữ liệu giữa cơ quan nhà nước với doanh nghiệp, hay giữa doanh nghiệp với nhau, dưới sự quản lý (*ví dụ yêu cầu đăng ký giao dịch trên sàn, trả phí qua quỹ phát triển dữ liệu*). Chính phủ thành lập Quỹ Phát triển Dữ liệu Quốc gia với nguồn vốn ngân sách 1000 tỷ (*theo Điều 29 Luật Dữ liệu và Nghị định 160/2025/NĐ-CP*) nhằm hỗ trợ tài chính cho các dự án khai thác dữ liệu, đổi mới sáng tạo về dữ liệu.



Bên cạnh đó, các dịch vụ dữ liệu mới sẽ được triển khai, dịch vụ định danh và xác thực điện tử (*qua Cơ sở dữ liệu dân cư*) mở rộng cho khu vực tư; dịch vụ chia sẻ dữ liệu chuyên sâu theo yêu cầu từng ngành; dịch vụ phân tích dữ liệu lớn hỗ trợ ra quyết định (*ví dụ phân tích dữ liệu giao thông để quy hoạch đô thị*)... Đặc biệt, tận dụng năng lực Trung tâm dữ liệu quốc gia, hướng tới năm 2030 sẽ triển khai các dự án trí tuệ nhân tạo dựa trên dữ liệu chính phủ, xây dựng trợ lý ảo cho công chức, hệ thống dự báo kinh tế vĩ mô, hay ứng dụng học máy (*machine learning*) để cải thiện dịch vụ công. Để làm được điều đó, Trung tâm dữ liệu quốc gia đã xúc tiến hợp tác với các doanh nghiệp công nghệ chiến lược (*26 đối tác ký kết*) và tổ chức các không gian sáng tạo (*innovation hub*) quy tụ chuyên gia dữ liệu. Mục tiêu là hình thành hệ sinh thái khởi nghiệp dữ liệu gắn với Trung tâm dữ liệu quốc gia, mọi ý tưởng khởi nghiệp có thể sử dụng dữ liệu giả lập hoặc nền tảng do Trung tâm dữ liệu quốc gia cung cấp để phát triển sản phẩm.

Đến 2030, Việt Nam phấn đấu trở thành trung tâm dữ liệu khu vực ASEAN. Điều này có nghĩa thu hút các công ty dịch vụ dữ liệu, điện toán đám mây đặt trung tâm dữ liệu tại Việt Nam, đồng thời thúc đẩy dòng chảy dữ liệu xuyên biên giới phục vụ thương mại. Trong giai đoạn 2025-2030, Bộ Công an cùng Bộ Khoa học và Công nghệ dự kiến đàm phán các hiệp định/quy tắc chia sẻ dữ liệu với các nước (*nhất là trong khuôn khổ ASEAN, APEC*), tạo thuận lợi cho doanh nghiệp Việt làm dịch vụ dữ liệu ở ngoài và ngược lại. Việc đạt tiêu chuẩn quốc tế (*như GDPR adequacy, APEC CBPR*) trong bảo vệ dữ liệu cá nhân cũng là đích hướng tới để Việt Nam hội nhập dòng chảy dữ liệu toàn cầu.

#### **8.3.5. Bảo đảm an ninh, an toàn dữ liệu trong quá trình chuyển đổi**

Cùng với việc mở rộng khai thác dữ liệu, không thể xem nhẹ nhiệm vụ bảo vệ dữ liệu. Giai đoạn 2025-2030 sẽ phải đổi mới nhiều thách thức an ninh mới, tội phạm mạng nhắm vào kho dữ liệu lớn, nguy cơ lộ lọt dữ liệu cá nhân trên diện rộng, xung đột giữa yêu cầu chia sẻ dữ liệu và bảo mật. Do vậy, nhiệm vụ trọng tâm là củng cố năng lực bảo vệ dữ liệu. Bộ Công an sẽ triển khai các biện pháp như áp dụng xác thực đa yếu tố và mã hóa cho truy cập dữ liệu nhạy cảm; triển



khai hệ thống giám sát an toàn dữ liệu theo thời gian thực tại Trung tâm dữ liệu quốc gia; thường xuyên kiểm tra, đánh giá an ninh các hệ thống kết nối vào Trung tâm dữ liệu quốc gia (*theo Điều 27 Luật Dữ liệu*); huấn luyện đội ngũ quản trị dữ liệu các cấp về quy tắc bảo vệ dữ liệu cá nhân và phản ứng sự cố. Về pháp luật, sẽ ban hành quy định phân loại mức độ an toàn dữ liệu (*có thể theo 4 cấp độ tương tự phân loại hệ thống thông tin*). Đặc biệt chú trọng bảo vệ dữ liệu cốt lõi và dữ liệu quan trọng: nhóm này sẽ có cơ chế sao lưu riêng, có kế hoạch khôi phục thảm họa (*DRP*) và thường xuyên diễn tập ứng phó sự cố.

Ngoài ra, cần phát huy vai trò của Hiệp hội Dữ liệu Quốc gia (*thành lập tháng 10/2023, gồm nhiều doanh nghiệp công nghệ lớn*), tổ chức xã hội nghề nghiệp giúp kết nối chính sách với doanh nghiệp, thúc đẩy sáng kiến bảo mật dữ liệu từ khu vực tư nhân. Hiệp hội này có thể phối hợp với Bộ Công an tổ chức các chương trình nâng cao nhận thức cho doanh nghiệp về bảo vệ dữ liệu, xây dựng bộ quy tắc đạo đức sử dụng dữ liệu,... nhấn mạnh vai trò cầu nối giữa chính phủ - doanh nghiệp - nhà khoa học trong phát triển hệ sinh thái dữ liệu an toàn.



Hình ảnh: Hội Dữ liệu Quốc gia tổ chức Tọa đàm “Xử lý và phân tích dữ liệu – Động lực cho chuyển đổi số quốc gia”. Ảnh: Hội Dữ liệu Quốc gia



Tóm lại, bức tranh giai đoạn 2025-2030 sẽ là Luật Dữ liệu có hiệu lực tạo nền tảng pháp lý; Trung tâm dữ liệu quốc gia hoàn thiện hạ tầng và tích hợp phần lớn các cơ sở dữ liệu quan trọng; hệ sinh thái dữ liệu được kích hoạt với các dịch vụ giá trị gia tăng, thị trường dữ liệu sôi động và an ninh dữ liệu được kiểm soát tốt nhờ cơ chế phối hợp đa ngành và công nghệ bảo mật tiên tiến. Mục tiêu cuối cùng là đến 2030, Việt Nam trở thành “quốc gia số an toàn”, dữ liệu góp phần chuyển đổi cơ cấu kinh tế, đưa đất nước đạt mức thu nhập trung bình cao, kinh tế số chiếm 30% GDP (*mục tiêu Chương trình Chuyển đổi số Quốc gia*), xếp hạng Chính phủ điện tử thuộc nhóm 50 nước dẫn đầu.

Để đạt được mục tiêu đó đó, trong mỗi năm từ nay đến 2030, các nhiệm vụ cần được cụ thể hóa và giám sát thực hiện qua chương trình hành động hàng năm của Ủy ban Quốc gia về Chuyển đổi số. Ví dụ: năm 2025 đặt chủ đề “Chuyển đổi số toàn diện để tạo ra động lực tăng trưởng mới”, bao gồm hoàn thành Trung tâm dữ liệu quốc gia giai đoạn cơ sở, tích hợp ít nhất 30% Cơ sở dữ liệu Quốc gia vào Trung tâm dữ liệu quốc gia, thử nghiệm sàn dữ liệu mở. Còn các năm 2026-2028 sẽ dồn sức cho mở rộng phạm vi dịch vụ dữ liệu tới từng người dân (*mỗi người dân có thể tra cứu dữ liệu cá nhân qua ứng dụng VN eID chặng hạn*). Chính phủ sẽ cần ban hành những đề án chuyên đề như Đề án Xây dựng Văn hóa dữ liệu trong cơ quan nhà nước; Đề án Nâng cao năng lực phân tích dữ liệu cho cán bộ; Kế hoạch quốc gia về Nhân lực khoa học dữ liệu... Bộ Công an cũng đã lên kế hoạch bồi dưỡng, đào tạo đội ngũ cán bộ dữ liệu với tư duy đổi mới sáng tạo, đủ kiến thức kỹ thuật và pháp lý để vận hành hệ thống. Thậm chí, cơ chế thu hút nhân tài trong và ngoài nước về làm việc tại Trung tâm dữ liệu quốc gia, hay hợp tác với các tập đoàn lớn (*IBM, Microsoft, Google*) cũng cần triển khai để tranh thủ chất xám quốc tế.

Tóm lại, giai đoạn 2025-2030 là thời gian tăng tốc để hiện thực hóa “tài nguyên dữ liệu” thành động lực phát triển. Các nhiệm vụ trọng tâm từ hoàn thiện thể chế, xây dựng hạ tầng, phát triển dữ liệu đến bảo đảm an toàn đã được xác định khá rõ ràng qua luật, chiến lược. Vẫn đề mấu chốt là sự quyết liệt trong chỉ



đạo và phối hợp thực thi với tinh thần “đã nói là phải làm, đã cam kết là phải thực hiện, đặt Trung tâm dữ liệu quốc gia trở thành ‘trái tim’, ‘bộ não’ của kỷ nguyên thịnh vượng mới”. Điều này đòi hỏi vai trò tiên phong gương mẫu của Bộ Công an, đồng thời sự vào cuộc đồng bộ của các bộ, ngành, địa phương và cả cộng đồng doanh nghiệp, người dân.

### **8.3.3. Kết luận và kiến nghị**

Công tác quản lý nhà nước về dữ liệu số tại Việt Nam đang bước vào giai đoạn chuyển mình mạnh mẽ, với việc ban hành Luật Dữ liệu 2024 và triển khai Trung tâm dữ liệu quốc gia thuộc Bộ Công an. Bộ Công an được xác định là cơ quan đầu mối thống nhất quản lý nhà nước về dữ liệu, giữ vai trò “nhạc trưởng” trong điều phối phát triển các cơ sở dữ liệu, vận hành hạ tầng tập trung và bảo đảm an ninh, an toàn dữ liệu trên phạm vi quốc gia. Mô hình Trung tâm dữ liệu quốc gia là bước đi đột phá, tạo nền tảng kỹ thuật và tổ chức để tích hợp, đồng bộ dữ liệu từ các bộ ngành, cung cấp hạ tầng chia sẻ dùng chung và hình thành kho dữ liệu tổng hợp phục vụ Chính phủ số. Cơ chế điều phối liên ngành đã được thiết lập thông qua các quy định pháp luật về bảo vệ dữ liệu cá nhân và an ninh mạng, cùng với các ban chỉ đạo chuyển đổi số, giúp gắn kết lực lượng Công an với các bộ, ngành trong việc giám sát, xử lý các vi phạm và ứng phó rủi ro về dữ liệu.

Giai đoạn 2025-2030 được định hình bởi những nhiệm vụ chiến lược: hoàn thiện khung pháp lý dữ liệu (*ban hành văn bản hướng dẫn Luật Dữ liệu, Luật Bảo vệ Dữ liệu Cá nhân*), xây dựng hoàn chỉnh hạ tầng Trung tâm dữ liệu quốc gia qua 3 giai đoạn và tích hợp hầu hết các cơ sở dữ liệu quan trọng vào Trung tâm dữ liệu quốc gia, phát triển hệ sinh thái dữ liệu an toàn, biến dữ liệu trở thành tài sản mang lại giá trị kinh tế và được bảo vệ chặt chẽ bằng công nghệ và pháp luật.

Việc tham khảo kinh nghiệm các nước cho thấy Việt Nam đang đi đúng hướng trong việc tập trung hóa đầu mối quản lý (*nhiều Hàn Quốc*), đồng thời cần chú trọng quyền riêng tư và tính minh bạch (*nhiều Singapore*) để tạo lòng tin xã hội với các chính sách dữ liệu.



Để hiện thực hóa các mục tiêu trên, tác giả đề xuất một số kiến nghị như sau:

- **Thứ nhất**, về thể chế và tổ chức: Thành lập sớm Ban Chỉ đạo Quốc gia về Dữ liệu số (*Nghị quyết số 214/NQ-CP ngày 23/7/2025*) do Thủ tướng đứng đầu, để chỉ đạo thống nhất các bộ, ngành, địa phương trong triển khai Luật Dữ liệu và Chiến lược dữ liệu quốc gia. Nghiên cứu khả năng thành lập Ủy ban Bảo vệ Dữ liệu cá nhân độc lập trực thuộc Chính phủ sau khi ban hành Luật Bảo vệ Dữ liệu Cá nhân, nhằm tăng cường hiệu quả giám sát việc tuân thủ và xử lý vi.

- **Thứ hai**, về tiêu chuẩn, công nghệ: Khẩn trương ban hành Danh mục tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu cho các ngành. Bộ Công an phối hợp Bộ KH&CN xây dựng các tiêu chuẩn về định dạng dữ liệu mở, siêu dữ liệu, API, giao thức kết nối... áp dụng thống nhất toàn quốc. Đẩy nhanh triển khai nền tảng tích hợp chia sẻ dữ liệu cấp bộ, tỉnh (*LGSP*) ở những nơi chưa có, bảo đảm đến 2025 tất cả các địa phương kết nối được với Trung tâm dữ liệu quốc gia. Về công nghệ, đầu tư áp dụng mạnh mẽ các giải pháp AI và tự động hóa trong quản trị dữ liệu (*ví dụ AI để dò tìm dữ liệu trùng lặp, sai lệch giữa các hệ thống; công cụ data lineage để truy vết nguồn gốc dữ liệu; công nghệ blockchain để đảm bảo tính toàn vẹn và chống chối bỏ khi chia sẻ dữ liệu - tham khảo nền tảng NDACChain - chuỗi khối quốc gia được giới thiệu tại lễ ra mắt đơn vị mới của Trung tâm dữ liệu quốc gia*).

- **Thứ ba**, về an ninh, an toàn dữ liệu: Xây dựng và ban hành quy chế phân loại dữ liệu theo mức độ nhạy cảm (*thấp, trung bình, cao, tối mật*) tương ứng với yêu cầu bảo vệ. Tăng cường giải pháp bảo mật ngay từ thiết kế cho Trung tâm dữ liệu quốc gia và các hệ thống kết nối: áp dụng mã hóa end-to-end cho dữ liệu nhạy cảm, triển khai hệ thống Quản lý khóa mã quốc gia (*phối hợp Ban Cơ yếu Chính phủ*) để phục vụ mã hóa dữ liệu dùng chung. Thực hiện định kỳ 6 tháng/lần các cuộc kiểm tra, diễn tập an ninh mạng tại Trung tâm dữ liệu quốc gia và các hệ thống trọng yếu có kết nối, với sự tham gia của nhiều lực lượng (*A05, NCSC, đội ứng cứu sự cố*). Thiết lập kênh phối hợp 24/7 giữa Trung tâm điều hành an toàn của Trung tâm dữ liệu quốc gia với Trung tâm Giám sát an toàn không gian mạng quốc gia để trao đổi thông tin tình báo mạng kịp thời. Về nhân lực, xây dựng cơ chế đãi ngộ



đặc biệt (*luong, phụ cấp*) cho chuyên gia an ninh dữ liệu tại Trung tâm dữ liệu quốc gia để thu hút người giỏi, kể cả chuyên gia Việt kiều và nước ngoài.

- **Thứ tư**, về khai thác dữ liệu và dịch vụ công: Rà soát, tái cấu trúc các thủ tục hành chính dựa trên việc khai thác dữ liệu từ Trung tâm dữ liệu quốc gia. Nguyên tắc là công dân, doanh nghiệp “không phải khai báo lại dữ liệu mà Nhà nước đã có”. Từ 2025 trở đi, mọi dịch vụ công trực tuyến mức 4 phải kết nối nền tảng định danh và chia sẻ dữ liệu để tự động điền thông tin. Đến 2030, phấn đấu 100% dịch vụ công sử dụng dữ liệu dùng chung từ Trung tâm dữ liệu quốc gia (*dữ liệu dân cư, doanh nghiệp, đất đai...*). Phát triển các ứng dụng dữ liệu phục vụ người dân: ví dụ: ứng dụng cho phép mỗi công dân xem tổng hợp các thông tin của mình do các cơ quan lưu giữ (*hồ sơ sức khỏe, quá trình đóng thuế, bảo hiểm...*), qua đó vừa minh bạch vừa giúp người dân kiểm tra và yêu cầu điều chỉnh nếu sai.



Các bộ, cơ quan không được yêu cầu người dân khai báo lại những thông tin đã có tại Cơ sở dữ liệu quốc gia về dân cư. Ảnh: Báo Chính phủ

- **Thứ năm**, phát triển thị trường và nhân lực dữ liệu: Sớm nghiên cứu ban hành Đề án phát triển thị trường dữ liệu tại Việt Nam, trong đó thí điểm cho phép một số doanh nghiệp công nghệ cao tham gia trao đổi dữ liệu phi cá nhân với Trung tâm dữ liệu quốc gia (*theo mô hình sandbox*). Xây dựng cơ chế giá dữ liệu,



hợp đồng dữ liệu mẫu và chính sách khuyến khích doanh nghiệp chia sẻ dữ liệu. Hỗ trợ Hiệp hội Dữ liệu Quốc gia tổ chức các hội thảo, cuộc thi đổi mới sáng tạo về dữ liệu thường niên, tạo sân chơi cho startup và cộng đồng AI khai thác dữ liệu mở của chính phủ để tạo sản phẩm mới (*như hackathon dữ liệu*). Về nhân lực, đưa nội dung khoa học dữ liệu và quản trị dữ liệu vào chương trình đào tạo công chức, đặc biệt với cán bộ quy hoạch làm chuyển đổi số tại các bộ, tỉnh. Khuyến khích hợp tác giữa Trung tâm dữ liệu quốc gia và các trường đại học mở ngành phân tích dữ liệu, bảo đảm nguồn cung nhân lực chất lượng cao cho hệ thống cơ quan nhà nước trong 5-10 năm tới.

Nhìn chung, việc quản lý và phát triển tài nguyên dữ liệu quốc gia là một hành trình lâu dài, đòi hỏi sự đồng bộ về nhận thức, quyết tâm về hành động và linh hoạt trong chính sách. Với nền móng pháp lý và tổ chức đã được đặt ra (*Luật Dữ liệu, Trung tâm dữ liệu quốc gia*), Việt Nam có cơ hội bứt phá để dữ liệu thật sự trở thành động lực cho chuyển đổi số và tăng trưởng kinh tế - xã hội bền vững. Bộ Công an, với vai trò được Đảng, Nhà nước tin cậy giao phó, cần tiếp tục phát huy tinh thần chủ động, phối hợp hiệu quả cùng các ban ngành, vừa đảm bảo an ninh quốc gia trên không gian mạng, vừa kiến tạo môi trường thuận lợi cho đổi mới sáng tạo dựa trên dữ liệu, đưa Việt Nam tiến vào kỷ nguyên số một cách tự chủ, an toàn và thịnh vượng.



## PHỤ LỤC

### *Phản bác thông tin sai sự thật liên quan đến việc QLNN về dữ liệu*

Trong kỷ nguyên số, dữ liệu không chỉ là “nhiên liệu” của đổi mới sáng tạo mà còn là tài nguyên chiến lược, quyết định năng lực quản trị quốc gia, sức cạnh tranh của nền kinh tế và hiệu quả phục vụ người dân, doanh nghiệp. Việc ban hành Luật Dữ liệu 2024 đã thiết lập khuôn khổ pháp lý toàn diện, xác định rõ nội dung quản lý nhà nước về dữ liệu, cơ chế phối hợp và vai trò đầu mối của Bộ Công an (*trừ lĩnh vực thuộc Bộ Quốc phòng*), qua đó thống nhất hành động, bảo đảm an ninh, an toàn dữ liệu song hành với phát triển Chính phủ số, kinh tế số, xã hội số.

Điều 8 Luật Dữ liệu quy định đầy đủ các “trụ cột” quản lý: <sup>(1)</sup>xây dựng, ban hành và tổ chức thực hiện Chiến lược dữ liệu quốc gia, hệ thống văn bản quy phạm pháp luật, tiêu chuẩn, quy chuẩn; <sup>(2)</sup>tuyên truyền, hướng dẫn thực thi; <sup>(3)</sup>quản lý, giám sát toàn bộ vòng đời dữ liệu gắn với bảo đảm an ninh, an toàn dữ liệu; <sup>(4)</sup>báo cáo - thống kê - nghiên cứu - phát triển thị trường dữ liệu; <sup>(5)</sup>thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo, xử lý vi phạm; <sup>(6)</sup>đào tạo nhân lực và hợp tác quốc tế. Cách tiếp cận này thể hiện tầm nhìn tổng thể: dữ liệu phải được quản trị bằng luật lệ, tiêu chuẩn và kỷ luật vận hành, không thể phó mặc cho tự phát hoặc chỉ nhìn dưới lăng kính kỹ thuật.

Đồng thời, Luật xác lập nguyên tắc nền tảng: bảo đảm quyền con người, quyền công dân, công khai, minh bạch, bình đẳng trong tiếp cận, khai thác dữ liệu; thu thập phải chính xác, có kế thừa, đi kèm bảo vệ dữ liệu chặt chẽ và kết nối - chia sẻ hiệu quả để phục vụ dịch vụ công, thủ tục hành chính và hoạt động của các chủ thể. Đây là câu trả lời trực diện trước các luận điệu xuyên tạc cho rằng quản lý dữ liệu nhằm “độc quyền thông tin”: luật đặt trách nhiệm bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân lên hàng đầu.

Luật quy định 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 trong quản lý nhà nước về dữ liệu; Bộ Quốc phòng quản lý phần việc thuộc phạm vi mình; các bộ, cơ



quan ngang bộ, UBND cấp tỉnh xây dựng, phát triển cơ sở dữ liệu và phối hợp với Bộ Công an thực hiện quản lý nhà nước. Như vậy, đây là cơ chế phân công - phối hợp - kiểm soát nhiệm vụ, chứ không phải “tập trung quyền lực thông tin” vào một cơ quan như các thông tin sai lệch quy chụp.

Trên thực tiễn triển khai, nghiên cứu đã chỉ rõ trách nhiệm ở hai tầng: <sup>(1)</sup>Bộ Công an là trung tâm xây dựng thể chế, tiêu chuẩn; hướng dẫn, kiểm tra, giám sát an ninh, an toàn dữ liệu; xây dựng và vận hành Trung tâm dữ liệu quốc gia; điều phối kết nối, chia sẻ dữ liệu; đào tạo lực lượng chuyên trách; <sup>(2)</sup>Công an các đơn vị, địa phương - tổ chức thi hành Luật tại cơ sở, quản lý các cơ sở dữ liệu chuyên ngành (*dân cư, căn cước, đăng ký, an ninh trật tự...*), bảo đảm dữ liệu “đúng, đủ, sạch, sống”, đồng bộ về Trung tâm Dữ liệu quốc gia; đồng thời nòng cốt bảo đảm an ninh mạng, an toàn dữ liệu, phối hợp xử lý vi phạm và tuyên truyền, hướng dẫn người dân, doanh nghiệp sử dụng dịch vụ số an toàn.

Một điểm đáng chú ý, Luật giao Bộ Công an chủ trì công bố danh sách cơ quan cung cấp dữ liệu, danh mục dữ liệu, bảng mã dùng chung để xã hội tra cứu, khai thác, cơ chế này tăng tính minh bạch và khả năng tương tác giữa các hệ thống dữ liệu. Việc kết nối - chia sẻ - điều phối dữ liệu cũng được quy định chặt chẽ, có thể huy động thẩm quyền của Thủ tướng trong tình huống đột xuất, cấp bách (*thiên tai, dịch bệnh...*) nhằm bảo vệ lợi ích công cộng, đồng thời vẫn giữ nguyên tắc sử dụng đúng mục đích, bảo đảm an ninh, an toàn.

Về cung cấp dữ liệu cho cơ quan nhà nước, Luật chỉ rõ những trường hợp đặc biệt, hữu hạn (*ứng phó tình trạng khẩn cấp; nguy cơ đe dọa an ninh quốc gia chưa đến mức ban bố khẩn cấp; thảm họa; phòng, chống bạo loạn, khủng bố*). Cơ quan tiếp nhận phải sử dụng đúng mục đích, bảo đảm an ninh, an toàn dữ liệu, hủy ngay khi không còn cần thiết và thông báo cho chủ thể/đơn vị đã cung cấp (*trừ trường hợp bí mật nhà nước, bí mật công tác*). Đây là hàng rào pháp lý nhằm răn đe lạm dụng, bảo vệ quyền và lợi ích hợp pháp của người dân, doanh nghiệp.

Nghiên cứu và thực tiễn triển khai cho thấy Trung tâm dữ liệu quốc gia là hạ tầng cốt lõi của chuyển đổi số quốc gia, được xây dựng theo lộ trình: 2023-



2025 (*hạ tầng ban đầu*), 2026-2028 (*mở rộng, nâng năng lực*), 2029-2030 (*hoàn thiện, tối ưu*). Nhiệm vụ song hành gồm: ban hành Khung quản trị dữ liệu tổng thể, Bộ tiêu chuẩn kiến trúc cơ sở dữ liệu để các bộ, ngành, địa phương tích hợp, đồng bộ; tổ chức điều phối dữ liệu; giám sát chất lượng dữ liệu; bảo đảm an ninh, an toàn hệ thống ở cấp quốc gia.

Cùng với đó, Nghị quyết số 175/NQ-CP về Đề án Trung tâm Dữ liệu quốc gia, các nhiệm vụ Chính phủ giao đã được thông tin rộng rãi trên báo chí chính thống, Trung tâm Dữ liệu quốc gia tích hợp và chia sẻ dữ liệu liên thông, cung cấp nền tảng dùng chung, tạo động lực cải cách thủ tục hành chính, thúc đẩy đổi mới sáng tạo và kinh tế số. Nhấn mạnh Trung tâm Dữ liệu quốc gia là “hệ sinh thái dữ liệu dùng chung của quốc gia”, có ý nghĩa kết nối đồng bộ và phá bỏ tình trạng cát cứ dữ liệu - một điểm then chốt để bác bỏ quan điểm sai lệch cho rằng mô hình mới “khép kín” hay “độc quyền”.

Ở tầm chiến lược, Chiến lược Dữ liệu quốc gia đến năm 2030 đặt mục tiêu: hoàn thiện thể chế, mở dữ liệu theo lộ trình, phát triển thị trường dữ liệu, hình thành các sàn giao dịch dữ liệu, chuẩn hóa - liên thông dữ liệu giữa bộ, ngành, địa phương; phát triển nguồn nhân lực dữ liệu; mở rộng hợp tác quốc tế và trao đổi dữ liệu xuyên biên giới theo pháp luật Việt Nam và điều ước quốc tế. Khẳng định Luật Dữ liệu 2024 tạo khuôn khổ pháp lý cho các trực nhiệm vụ này, là điều kiện để đưa dữ liệu thành tài sản, thúc đẩy tăng trưởng mới.

Những nội dung trên xé rách hoàn toàn các luận điệu xuyên tạc, sai trái của các thế lực thù địch, các loại đối tượng:

- Thứ nhất, xuyên tạc Luật Dữ liệu “tập trung quyền kiểm soát thông tin” là sai bản chất. Luật ghi rõ Chính phủ thống nhất quản lý, phân định đầu mối (*Bộ Công an*) và phạm vi (*Bộ Quốc phòng; các bộ, ngành, địa phương*). Mô hình này nhằm rõ người - rõ việc - rõ trách nhiệm, bảo đảm an ninh dữ liệu đi cùng khả năng khai thác, chia sẻ phục vụ phát triển.

Thứ hai, suy diễn “thu thập, sử dụng dữ liệu tùy tiện” không phù hợp với Luật. Chỉ trong trường hợp đặc biệt, hữu hạn vì lợi ích công (*khẩn cấp, an ninh*



quốc gia, thảm họa, chống khủng bố) mới yêu cầu cung cấp dữ liệu mà không cần sự đồng ý và cơ quan nhận dữ liệu phải dùng đúng mục đích, bảo đảm an ninh, an toàn, hủy khi không còn cần thiết, có cơ chế trách nhiệm giải trình rất cụ thể.

Thứ ba, gán ghép “độc quyền hạ tầng” là khiên cưỡng. Luật nêu Nhà nước khuyến khích tổ chức, cá nhân đầu tư, nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ dữ liệu, xây dựng trung tâm lưu trữ, xử lý tại Việt Nam, phát triển thị trường dữ liệu, tạo không gian cạnh tranh, hợp tác công-tư lành mạnh.

Thứ tư, quy chụp “mơ hồ khái niệm” không có cơ sở. Luật đã định nghĩa rõ ràng các thuật ngữ “dữ liệu quan trọng”, “dữ liệu cốt lõi” và giao Chính phủ quy định tiêu chí; đồng thời chuẩn hóa phân loại dữ liệu theo mức độ chia sẻ và mức độ quan trọng để có cơ chế bảo vệ tương ứng.

Thứ năm, luận điệu “không minh bạch” bị bác bỏ bởi chính thiết kế luật và thực tiễn công khai, danh mục dữ liệu mở, công dữ liệu, công khai có điều kiện theo Luật Tiếp cận thông tin; báo chí chính thống liên tục thông tin về Trung tâm Dữ liệu quốc gia, Chiến lược dữ liệu, lộ trình triển khai. Luật Dữ liệu phản ánh đậm nét yêu cầu minh bạch, liên thông, coi dữ liệu là động lực của cải cách, phục vụ người dân, doanh nghiệp.

Luật Dữ liệu 2024 đã xác lập nội dung quản lý nhà nước về dữ liệu một cách đầy đủ, hiện đại; khẳng định vai trò đầu mối của Bộ Công an trong tổng thể cơ chế Chính phủ thống nhất quản lý, các bộ, ngành, địa phương cùng thực hiện; đồng thời mở đường cho một hạ tầng dữ liệu quốc gia an toàn, liên thông, phục vụ người dân, doanh nghiệp. Đến năm 2030, trọng tâm là <sup>(1)</sup>hoàn thiện thể chế, chuẩn hóa và liên thông dữ liệu; <sup>(2)</sup>vận hành Trung tâm Dữ liệu quốc gia; <sup>(3)</sup>phát triển dữ liệu mở và thị trường dữ liệu; <sup>(4)</sup>bảo đảm an ninh, an toàn dữ liệu <sup>(5)</sup>phát triển nhân lực dữ liệu, tạo nền tảng bền vững cho chính phủ số, kinh tế số, xã hội số. Những xuyên tạc, hiểu sai nếu có, đều bị thực tế pháp lý và triển khai bác bỏ, quản lý dữ liệu ở Việt Nam là để bảo vệ quyền và lợi ích hợp pháp của người dân, doanh nghiệp, đồng thời thúc đẩy phát triển đất nước trong kỷ nguyên số.



## TÀI LIỆU THAM KHẢO

1. Luật Dữ liệu (*Luật số 60/2024/QH15*);
2. Luật An ninh mạng (*Luật số 24/2018/QH14*);
3. Luật An toàn thông tin mạng (*Luật số 86/2015/QH13*);
4. Luật Bảo vệ dữ liệu cá nhân (*Luật số 91/2025/QH15*);
5. Nghị quyết số 175/NQ-CP ngày 30/10/2023 phê duyệt Đề án Trung tâm dữ liệu quốc gia;
6. Quyết định số 749/QĐ-TTg ngày 03/6/2020 của Thủ tướng Chính phủ phê duyệt Chương trình Chuyển đổi số quốc gia đến 2025, định hướng 2030;
7. Báo Chính phủ, Bộ Công an thành lập Trung tâm dữ liệu quốc gia, 2025;
8. Báo Chính phủ, Bộ Công an xây dựng mô hình tổ chức, bố trí nhân sự để quản lý và vận hành Trung tâm dữ liệu quốc gia, 2023;
9. Bộ Khoa học và Công nghệ, Chiến lược dữ liệu quốc gia - Tầm nhìn đến năm 2030, 2025;
10. Uyên Hương, Thành Đạt, Trung tâm dữ liệu quốc gia - Bộ Công an ra mắt hai đơn vị mới, 2025.