

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 2
KIẾN TẠO



DATA



Hà Nội, năm 2025

BỘ CÔNG AN
CÔNG AN THÀNH PHỐ HÀ NỘI



BÀI DỰ THI

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

Quyển 2
KIẾN TẠO

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 hai – “Kiến tạo” gồm ba nội dung lớn: quy định về các hành vi bị nghiêm cấm và giải pháp xử lý vi phạm hành chính trong lĩnh vực dữ liệu; quy định về khoa học, công nghệ, đổi mới sáng tạo gắn với mục tiêu phát triển đất nước hùng cường; và quy định về thu thập, đồng bộ, kết nối, chia sẻ dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia cùng giải pháp ứng dụng hiệu quả.

...

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



04 HÀNH VI CÁC HÀNH VI BỊ NGHIÊM CẤM

1. Lợi dụng việc xử lý dữ liệu, quản trị dữ liệu, phát triển, kinh doanh, lưu hành sản phẩm, dịch vụ về dữ liệu để xâm phạm đến lợi ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.
2. Cản trở hoặc ngăn chặn trái pháp luật quá trình xử lý dữ liệu, quản trị dữ liệu hoặc tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin phục vụ quản lý, xử lý, quản trị, bảo vệ dữ liệu.
3. Giả mạo, cố ý làm sai lệch, làm mất, làm hư hỏng dữ liệu trong cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội.
4. Cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định của pháp luật.

Điều 10, Luật Dữ liệu 2024
ngày 30/11/2024, (Luật số 60/2024/QH15)



04 HOẠT ĐỘNG

Khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu

1. Hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu phải phù hợp với chiến lược phát triển dữ liệu quốc gia; phát huy nội lực trong hoạt động khoa học, công nghệ và đổi mới sáng tạo; tuân thủ nguyên tắc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu theo quy định của Luật này.
2. Các nền tảng khoa học và công nghệ trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu bao gồm: trí tuệ nhân tạo, điện toán đám mây, chuỗi khối, truyền thông dữ liệu, Internet vạn vật, dữ liệu lớn và công nghệ hiện đại khác.
3. Tập trung nguồn lực quốc gia cho hoạt động phát triển, ứng dụng nền tảng khoa học và công nghệ trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu phục vụ chuyển đổi số quốc gia, bảo đảm quốc phòng, an ninh, phát triển kinh tế - xã hội.
4. Chính phủ quy định việc quản lý, phát triển, thử nghiệm có kiểm soát các hoạt động nghiên cứu, ứng dụng khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu

Điều 24, Luật Dữ liệu 2024
ngày 30/11/2024, (Luật số 60/2024/QH15)



MỤC LỤC

Câu 3: Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu? 1

 3.1. Quy định về hành vi bị nghiêm cấm..... 2

 3.1.1. Giới thiệu khái quát Điều 10 Luật Dữ liệu 2024..... 2

 3.1.2. Các nhóm hành vi bị nghiêm cấm 3

 3.1.3 Kết luận..... 29

 3.2. Giải pháp hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu 30

 3.2.1. Thực trạng quy định pháp luật hiện hành về xử lý vi phạm trong lĩnh vực dữ liệu..... 30

 3.2.2. Đánh giá mức độ đầy đủ, hiệu lực, hiệu quả của các quy định.... 35

 3.2.3. Tính hiệu lực và hiệu quả của các quy định hiện hành 36

 3.2.4. Khoảng trống pháp lý khi Luật Dữ liệu 2024 có hiệu lực 39

 3.2.5. Giải pháp hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu 41

PHỤ LỤC 54

 Đáu tranh, phản bác các quan điểm sai trái về các hành vi bị nghiêm cấm trong Luật Dữ liệu 54

TÀI LIỆU THAM KHẢO 60

Câu 4: Quy định về hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, xử lý, sử dụng dữ liệu? Nhiệm vụ, giải pháp để phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trở thành yếu tố quyết định, là điều kiện tiên quyết đưa nước ta phát triển giàu mạnh, hùng cường trong kỷ nguyên mới - kỷ nguyên vươn mình của Dân tộc? 61

 4.1. Quy định về hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, xử lý, sử dụng dữ liệu 62

 4.1.1. Quy định pháp luật về khoa học, công nghệ và đổi mới sáng tạo trong lĩnh vực dữ liệu 62

 4.1.2. Vai trò của khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, bảo vệ, khai thác dữ liệu 67



4.2. Nhiệm vụ, giải pháp để phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trở thành yếu tố quyết định, là điều kiện tiên quyết đưa nước ta phát triển giàu mạnh, hùng cường trong kỷ nguyên mới - kỷ nguyên vươn mình của Dân tộc	73
4.2.1. Nhiệm vụ và giải pháp phát triển khoa học, công nghệ và đổi mới sáng tạo và chuyển đổi số theo Nghị quyết 57-NQ/TW	73
4.2.2. Kiến nghị hoàn thiện pháp luật và chính sách phát triển dữ liệu bền vững gắn với đổi mới sáng tạo, đảm bảo chủ quyền số quốc gia	81
PHỤ LỤC	88
<i>Phản bác quan điểm xuyên tạc “Luật Dữ liệu b López áng tạo”</i>	88
TÀI LIỆU THAM KHẢO	96
Câu 5: Quy định về thu thập, cập nhật, đồng bộ, kết nối, chia sẻ, khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia? Giải pháp tăng cường ứng dụng Cơ sở dữ liệu tổng hợp quốc gia phục vụ hoạt động của cơ quan nhà nước và đáp ứng nhu cầu phát triển kinh tế - xã hội?	97
5.1. Quy định về thu thập, cập nhật, đồng bộ, kết nối, chia sẻ, khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia	98
5.1.1. Tổng quan	98
5.1.2. Quy định về thu thập, cập nhật, đồng bộ, kết nối, chia sẻ, khai thác, sử dụng dữ liệu	100
5.2. Giải pháp tăng cường ứng dụng Cơ sở dữ liệu tổng hợp quốc gia phục vụ hoạt động của cơ quan nhà nước và đáp ứng nhu cầu phát triển kinh tế - xã hội	116
5.2.1. Hoàn thiện thể chế và chính sách	116
5.2.2. Đầu tư hạ tầng và công nghệ	120
5.2.3. Chuẩn hóa và nâng cao chất lượng dữ liệu	126
5.2.4. Phát triển nguồn nhân lực và nâng cao nhận thức	129
5.2.5. Ứng dụng trong cơ quan nhà nước và kinh tế - xã hội	133
KẾT LUẬN	141
PHỤ LỤC	144
<i>Phản bác quan điểm sai trái “Việt Nam xâm phạm quyền riêng tư”</i>	144
TÀI LIỆU THAM KHẢO	151



Câu 3: Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu?





Câu 3: Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu?

Trả lời

3.1. Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024

3.1.1. Giới thiệu khái quát Điều 10 Luật Dữ liệu 2024

Luật Dữ liệu 2024 (*Luật số 60/2024/QH15*) được Quốc hội thông qua ngày 30/11/2024 và sẽ có hiệu lực từ 01/7/2025. Đây là văn bản pháp luật đầu tiên của Việt Nam quy định một cách toàn diện về quản trị, phát triển, bảo vệ và sử dụng dữ liệu số trong bối cảnh chuyển đổi số quốc gia. Điều 10 của Luật này đã liệt kê các hành vi bị nghiêm cấm trong hoạt động dữ liệu số, nhằm thiết lập những ranh giới pháp lý rõ ràng ngăn ngừa việc lạm dụng dữ liệu gây hại cho an ninh quốc gia, trật tự xã hội cũng như xâm phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân. Cụ thể, Điều 10 Luật Dữ liệu 2024 quy định bốn nhóm hành vi bị nghiêm cấm, bao gồm:

"1. Lợi dụng việc xử lý dữ liệu, quản trị dữ liệu, phát triển, kinh doanh, lưu hành sản phẩm, dịch vụ về dữ liệu để xâm phạm đến lợi ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Cản trở hoặc ngăn chặn trái pháp luật quá trình xử lý dữ liệu, quản trị dữ liệu hoặc tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin phục vụ quản lý, xử lý, quản trị, bảo vệ dữ liệu.

3. Giả mạo, có ý làm sai lệch, làm mất, làm hư hỏng dữ liệu trong cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội.

4. Có ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định của pháp luật."



Những hành vi này phản ánh các nguy cơ tiêu cực trong thời đại số, từ việc sử dụng dữ liệu làm công cụ xâm hại an ninh quốc gia cho đến các hành vi phá hoại hệ tầng dữ liệu, thao túng thông tin công và vi phạm nghĩa vụ cung cấp dữ liệu.

Việc Luật Dữ liệu đưa ra các điều cấm này là cần thiết để bảo đảm an toàn dữ liệu và trật tự pháp lý trong lĩnh vực số. Trước đó, một số luật liên quan như Luật An ninh mạng 2018 và các quy định về bảo vệ dữ liệu cá nhân cũng đã đề cập tới những hành vi tương tự. Luật An ninh mạng nghiêm cấm việc sử dụng không gian mạng để xâm phạm an ninh quốc gia, trật tự xã hội hoặc quyền lợi hợp pháp của cá nhân, tổ chức. Nghị định 13/2023/NĐ-CP cũng quy về việc nghiêm cấm xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam. Như vậy, Điều 10 Luật Dữ liệu 2024 đã tiếp nối và cụ thể hóa các nguyên tắc đã có, đồng thời thiết lập hành lang pháp lý thống nhất để xử lý nghiêm mọi hành vi lạm dụng dữ liệu.

3.1.2. Các nhóm hành vi bị nghiêm cấm

3.1.2.1. Lợi dụng hoạt động xử lý, quản trị, phát triển dữ liệu để xâm phạm lợi ích quốc gia, dân tộc, quyền con người

Khoản 1 Điều 10 Luật Dữ liệu 2024 nghiêm cấm hành vi “*lợi dụng việc xử lý dữ liệu, quản trị dữ liệu, phát triển, kinh doanh, lưu hành sản phẩm, dịch vụ về dữ liệu để xâm phạm đến lợi ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân*”.

Nói cách khác, bất kỳ ai sử dụng dữ liệu hoặc hoạt động liên quan đến dữ liệu như một phương tiện nhằm chống lại Nhà nước, xâm hại lợi ích dân tộc, gây mất ổn định xã hội, hoặc vi phạm quyền hợp pháp của người khác đều đang thực hiện hành vi bị cấm. Quy định này có phạm vi rất rộng, bao quát từ việc tạo ra, chia sẻ dữ liệu có nội dung xấu độc cho đến việc lợi dụng công nghệ dữ liệu để xâm phạm nhân quyền.

Quy định trên của Luật Dữ liệu 2024 tương đồng với các điều cấm trong pháp luật hiện hành. Ví dụ: Luật An ninh mạng 2018 cấm sử dụng không gian mạng để tuyên truyền chống Nhà nước, xuyên tạc lịch sử, kích động phá hoại khôi



đại đoàn kết, hoặc đưa thông tin sai sự thật gây hoang mang, xâm phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân. Tương tự, khoản 1 Điều 7 Luật Bảo vệ Dữ liệu Cá nhân 2025 cũng cấm việc xử lý dữ liệu cá nhân nhằm chống lại Nhà nước hoặc gây ảnh hưởng đến quốc phòng, an ninh quốc gia, trật tự an toàn xã hội và quyền, lợi ích hợp pháp của người khác. Nghị định 13/2023/NĐ-CP cũng có quy định cấm xử lý dữ liệu cá nhân để tạo ra thông tin nhằm chống Nhà nước hoặc xâm phạm an ninh, trật tự, quyền lợi hợp pháp của tổ chức, cá nhân. Bộ luật Hình sự cũng quy định hành vi lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân có nội hàm tương tự. Những điểm tương đồng này cho thấy Luật Dữ liệu 2024 nhất quán trong việc ngăn chặn mọi hành vi lợi dụng dữ liệu hay không gian mạng để xâm phạm an ninh quốc gia và quyền con người.



Hình ảnh: Đối tượng Đậu Thị Tâm bị Công an thành phố Hà Nội xử lý về hành vi lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân. Ảnh: Báo Nhân dân

*** Dấu hiệu vi phạm:**

Hành vi lợi dụng hoạt động xử lý, quản trị, phát triển dữ liệu để xâm phạm lợi ích quốc gia, dân tộc, quyền con người có dấu hiệu cốt lõi là mục đích xấu



hoặc trái pháp luật khi sử dụng dữ liệu. Thay vì khai thác dữ liệu phục vụ phát triển kinh tế - xã hội hay lợi ích chính đáng, đối tượng vi phạm sẽ “lợi dụng” hoạt động dữ liệu (*nhiều thu thập, phân tích, chia sẻ hoặc kinh doanh dữ liệu*) nhằm xâm hại các lợi ích được pháp luật bảo vệ. Những dấu hiệu cụ thể có thể bao gồm:

- **Một là**, tạo ra hoặc phát tán thông tin, dữ liệu có nội dung chống phá Nhà nước, gây phuơng hại đến lợi ích quốc gia, dân tộc. Ví dụ: lợi dụng dữ liệu về tình hình kinh tế - xã hội để thổi phồng, bóp méo thành những luận điệu sai trái, xuyên tạc chủ trương của Đảng và Nhà nước. Đây là hành vi đặc biệt nguy hiểm vì có thể kích động bất ổn chính trị và chia rẽ khối đoàn kết dân tộc. Luật An ninh mạng xếp các hành vi như tuyên truyền chống Nhà nước, phá hoại khối đại đoàn kết, xúc phạm tôn giáo, chủng tộc... trên không gian mạng vào nhóm bị nghiêm cấm, cho thấy việc sử dụng dữ liệu thông tin vào mục đích đó là vi phạm nghiêm trọng.

- **Hai là**, lợi dụng dữ liệu để xâm phạm quyền con người, quyền công dân hoặc lợi ích hợp pháp của tổ chức, cá nhân. Điều này có thể biểu hiện qua việc sử dụng dữ liệu cá nhân, dữ liệu riêng tư nhằm đe dọa, tống tiền, bôi nhọ danh dự người khác; hoặc sử dụng dữ liệu để phân biệt đối xử, xâm phạm quyền bình đẳng. Ví dụ: một doanh nghiệp công nghệ nếu thu thập dữ liệu người dùng rồi sử dụng để phân tích khuynh hướng tôn giáo, chính trị của họ và cung cấp cho bên thứ ba nhằm mục đích sách nhiễu, định kiến thì đó là hành vi vi phạm quyền con người. Theo Luật Bảo vệ Dữ liệu Cá nhân 2025, mọi hoạt động xử lý dữ liệu cá nhân phải bảo đảm không xâm phạm quyền riêng tư, nhân phẩm và nghiêm cấm sử dụng dữ liệu cá nhân của người khác hoặc cho người khác sử dụng dữ liệu của mình để vi phạm pháp luật.

- **Ba là**, lợi dụng dữ liệu để gây phuơng hại an ninh, trật tự, an toàn xã hội. Dấu hiệu này thường gắn với việc sử dụng dữ liệu thông tin sai sự thật hoặc trái phép để gây rối loạn xã hội. Ví dụ: kẻ xấu có thể lợi dụng dữ liệu giả (*deepfake, thông tin giả mạo*) tung lên mạng xã hội nhằm kích động chống đối, gây hoang mang trong dân chúng. Thực tế đã từng xảy ra các trường hợp đối tượng tung tin giả về tình hình dịch bệnh, thiên tai hoặc sự cố an ninh, khiến cộng đồng hoảng



sợ và gây khó khăn cho quản lý xã hội. Luật An ninh mạng nghiêm cấm hành vi đăng tải thông tin sai sự thật gây hoang mang, thiệt hại cho hoạt động kinh tế - xã hội hoặc gây khó khăn cho hoạt động của cơ quan nhà nước. Đây là dấu hiệu rõ ràng để nhận diện vi phạm: nếu một cá nhân/tổ chức đưa lên mạng dữ liệu thông tin không xác thực, bịa đặt dẫn đến hậu quả bất ổn xã hội, thì đó chính là “lợi dụng dữ liệu xâm phạm... trật tự, an toàn xã hội” như Điều 10 đã nêu.

Như vậy, ranh giới pháp lý ở đây nằm ở mục đích và hậu quả của việc sử dụng dữ liệu. Hoạt động xử lý, kinh doanh dữ liệu vì mục đích hợp pháp (*ví dụ nghiên cứu thị trường, cải thiện dịch vụ công*) được pháp luật khuyến khích. Nhưng nếu hoạt động đó bị lợi dụng làm phương tiện vi phạm pháp luật, xâm hại lợi ích quốc gia hoặc quyền cá nhân, thì đã chuyển thành hành vi bị nghiêm cấm. Điểm mấu chốt là xác định ý đồ chủ quan (*có ý*) và tác động tiêu cực đến các lợi ích được pháp luật bảo vệ.

* *Mức độ nguy hiểm:*

Hành vi lợi dụng dữ liệu để xâm phạm lợi ích quốc gia, dân tộc hay quyền con người được đánh giá là đặc biệt nguy hiểm.

- **Thứ nhất**, nó có thể gây phuơng hại nghiêm trọng đến an ninh quốc gia - ví dụ như tiết lộ dữ liệu mật, truyền bá thông tin phản động làm suy giảm niềm tin vào chính quyền hoặc kích động bạo loạn. An ninh mạng bị đe dọa trực tiếp khi dữ liệu bị biến thành vũ khí cho các hoạt động chống phá.

- **Thứ hai**, hành vi này xâm phạm thô bạo các quyền con người, quyền công dân cơ bản như quyền được bảo vệ danh dự, nhân phẩm, quyền riêng tư, quyền tự do tín ngưỡng... Bằng cách lạm dụng dữ liệu (*ví dụ công bố dữ liệu đời tư để bôi nhọ người khác, hoặc sử dụng dữ liệu cá nhân trong các chiến dịch quấy rối*), đối tượng vi phạm có thể gây tổn hại nặng nề cho cá nhân nạn nhân, cả về tinh thần lẫn vật chất.

- **Thứ ba**, xét về phạm vi ảnh hưởng, những hành vi kiểu này thường lan truyền rất nhanh trên môi trường số, khiến hậu quả xã hội trở nên khó kiểm soát.



Chỉ một dữ liệu thông tin giả mạo được đăng tải, trong thời gian ngắn có thể tiếp cận hàng triệu người, gây hoang mang và hiểu lầm diện rộng.

Vì vậy, pháp luật quy định chế tài nghiêm khắc đối với hành vi này.

* **Chế tài xử lý:**

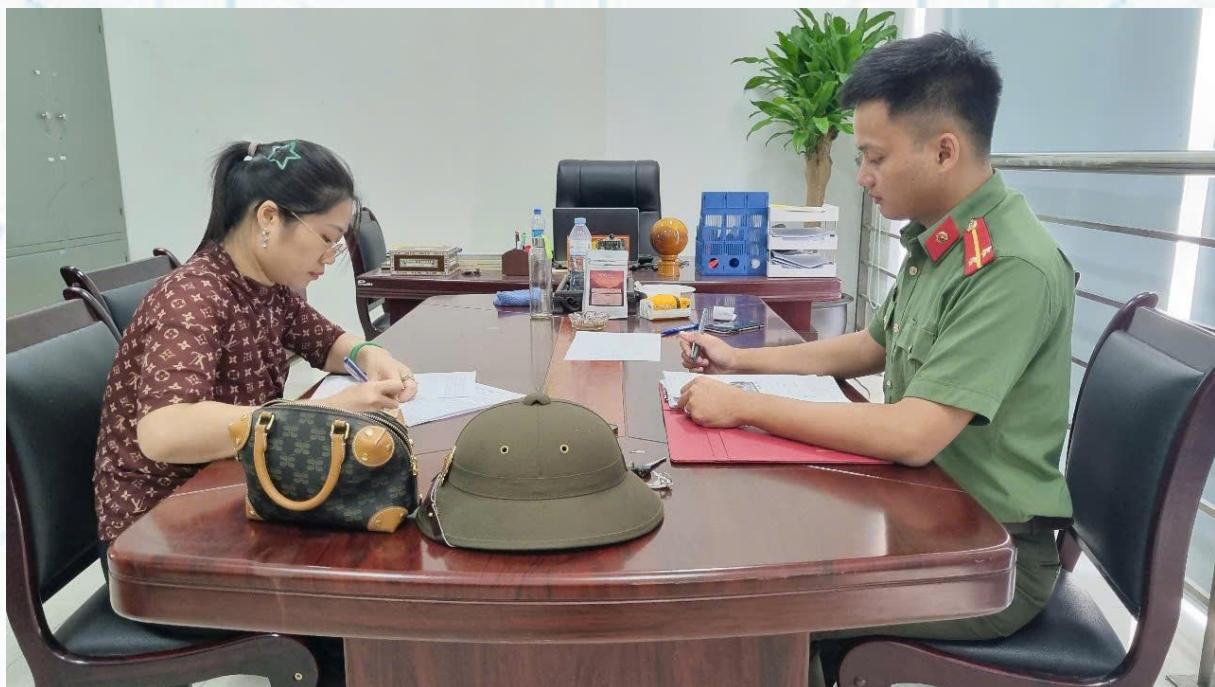
Về xử lý vi phạm, tùy tính chất mức độ, hành vi lợi dụng dữ liệu xâm phạm lợi ích quốc gia, quyền con người có thể bị xử phạt hành chính hoặc truy cứu trách nhiệm hình sự. Ở mức hành chính, Nghị định 15/2020/NĐ-CP quy định phạt tiền từ 10 đến 20 triệu đồng (*đối với tổ chức*) đối với hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin giả mạo, sai sự thật, vu khống, xúc phạm uy tín cơ quan, tổ chức hoặc danh dự cá nhân. Đây chính là chế tài dành cho các trường hợp tung tin giả, thông tin xấu độc trên môi trường mạng - một biểu hiện thường gặp của nhóm hành vi. Ngoài phạt tiền, tổ chức vi phạm có thể bị tước giấy phép hoạt động một thời gian; cá nhân vi phạm thì bị phạt tiền bằng một nửa mức của tổ chức. Nghiêm trọng hơn, nếu hành vi đủ yếu tố cấu thành tội phạm (*ví dụ Tội tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam Điều 88 Bộ luật Hình sự; Tội làm, tang trữ, phát tán hoặc tuyên truyền thông tin, tài liệu, vật phẩm nhằm chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam theo Điều 117 Bộ luật Hình sự hoặc Tội lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân theo Điều 331 Bộ luật Hình sự*), người vi phạm có thể bị phạt tù nhiều năm. Rõ ràng, hệ thống pháp luật đã đặt ranh giới đỏ đối với việc lợi dụng dữ liệu xâm phạm an ninh quốc gia và quyền con người, với chế tài từ hành chính đến hình sự.

Ví dụ thực tiễn: Trong thực tế, thời gian qua ở Việt Nam đã xảy ra nhiều vụ lợi dụng dữ liệu trên internet để truyền bá thông tin sai trái và tất cả đều bị xử lý nghiêm.

Trong đợt bão Yagi năm 2024, một số đối tượng đăng tải, chia sẻ thông tin sai sự thật về tình hình bão, gây hoang mang trong dư luận. Ngay sau đó, Công an thành phố Hà Nội đã triệu tập những người liên quan. Kết quả xác định đây là thông tin giả mạo. Căn cứ Nghị định 15/2020/NĐ-CP, hành vi “Cung cấp, chia sẻ



thông tin bịa đặt, gây hoang mang trong Nhân dân, kích động bạo lực, tội ác, tệ nạn xã hội, đánh bạc hoặc phục vụ đánh bạc” bị phạt tiền mức 7.5 triệu đồng (*mức trung bình cho cá nhân*). Trường hợp này minh họa rõ việc lợi dụng dữ liệu (*thông tin điện tử*) để xâm phạm lợi ích công cộng, gây rối loạn thông tin xã hội



Hình ảnh: Công an thành phố Hà Nội làm việc với trường hợp đăng tải thông tin sai sự thật liên quan đợt bão Yagi năm 2024. Ảnh: Tác giả

Tương tự, tháng 7/2024 tại Thái Nguyên, một số đối tượng lan truyền thông tin nhiều nam giới bị lây nhiễm HIV từ một nữ nhân viên Công ty TNHH Samsung Electronics Việt Nam Thái Nguyên. Cùng với thông tin này, một video ghi lại hình ảnh nhạy cảm được cho là của nữ nhân viên cũng được chia sẻ, phát tán trên nhiều mạng xã hội. Đây là hành vi lợi dụng dữ liệu cá nhân (*hình ảnh*) của người khác, xuyên tạc thành thông tin gây hoang mang dư luận và xúc phạm uy tín ngành y. Công an tỉnh Thái Nguyên đã điều tra, làm rõ và khởi tố hình sự 06 cá nhân về tội lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân theo Điều 331 Bộ luật Hình sự.



Hình ảnh: Công an tỉnh Thái Nguyên làm việc với các trường hợp lan truyền thông tin sai sự thật. Ảnh: Báo Thanh niên

Qua các phân tích và ví dụ trên, có thể thấy nhóm hành vi Lợi dụng hoạt động xử lý, quản trị, phát triển dữ liệu để xâm phạm lợi ích quốc gia, dân tộc, quyền con người là nhóm vi phạm rộng và nguy hiểm bậc nhất trong lĩnh vực dữ liệu. Pháp luật Việt Nam đã quy định rõ ràng để phòng ngừa và xử lý nhóm hành vi này, nhằm bảo vệ vững chắc an ninh quốc gia, trật tự xã hội cũng như các quyền con người trong kỷ nguyên số.

3.1.2.2. Cản trở, phá hoại hoạt động xử lý và hệ thống dữ liệu

Khoản 2 Điều 10 Luật Dữ liệu 2024 cấm các hành vi “cản trở hoặc ngăn chặn trái pháp luật quá trình xử lý dữ liệu, quản trị dữ liệu hoặc tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin phục vụ quản lý, xử lý, quản trị, bảo vệ dữ liệu”. Nhóm hành vi này tập trung vào việc xâm hại đến quy trình và hạ tầng kỹ thuật của hoạt động dữ liệu, bao gồm: ⁽¹⁾Cản trở, ngăn chặn trái phép quá trình xử lý hoặc quản trị dữ liệu; ⁽²⁾Tấn công, truy cập trái phép nhằm chiếm đoạt hoặc phá hoại cơ sở dữ liệu, hệ thống thông tin liên quan đến dữ liệu. Đây



thực chất là các hành vi xâm nhập, phá hoại trên không gian mạng nhằm vào hệ thống dữ liệu, thuộc phạm vi an toàn thông tin mạng và an ninh mạng.

Quy định này có mối liên hệ chặt chẽ với Luật An ninh mạng 2018 và pháp luật về an toàn thông tin. Cụ thể, Luật An ninh mạng liệt kê một loạt hành vi bị nghiêm cấm, trong đó đáng chú ý là: “*Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia*”. Luật cũng cấm hành vi phát tán phần mềm gây hại, xâm nhập trái phép vào hệ thống thông tin, cơ sở dữ liệu của người khác. Những nội dung này tương ứng trực tiếp với phần “tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin” mà Luật Dữ liệu 2024 đề cập. Ngoài ra, Luật An toàn thông tin mạng 2015 và các văn bản dưới luật (như Nghị định 15/2020/NĐ-CP) cũng quy định các chế tài hành chính đối với hành vi cản trở, gây rối loạn hoạt động của mạng, hệ thống thông tin. Ví dụ: Điều 75 Nghị định 15/2020/NĐ-CP (được hợp nhất năm 2022) phạt tiền đến 170 triệu đồng cho hành vi “*phá hoại cơ sở hạ tầng thông tin hoặc phá hoại thông tin trên môi trường mạng*”. Như vậy, có thể thấy pháp luật Việt Nam đã có hệ thống điều chỉnh đầy đủ nhằm bảo vệ hạ tầng và hoạt động của hệ thống dữ liệu trước các hành vi cản trở, tấn công.

* **Dấu hiệu vi phạm:**

Hành vi cản trở, phá hoại hoạt động xử lý và hệ thống dữ liệu có hai dạng chính với dấu hiệu nhận biết riêng:

- **Một là**, cản trở hoặc ngăn chặn trái phép quá trình xử lý, quản trị dữ liệu: Dạng này có thể hiểu là gây khó khăn, gián đoạn hoặc đình trệ cho hoạt động xử lý dữ liệu mà lẽ ra phải diễn ra thông suốt. Dấu hiệu nhận biết là hành vi không được phép của pháp luật nhưng cố tình ngăn cản luồng dữ liệu hoặc làm gián đoạn chức năng hệ thống. Ví dụ: một cá nhân phát tán phần mềm độc hại (*virus, ransomware*) vào hệ thống cơ sở dữ liệu của doanh nghiệp khiến quá trình xử lý dữ liệu bị tê liệt, không thể thực hiện được; hoặc một nhân viên bất mãn cố ý xóa dữ liệu, thay đổi mật khẩu hệ thống nhằm cản trở hoạt động bình thường của cơ



quan. Những hành vi này đều trái pháp luật, bởi không ai được phép cản trở trái phép việc vận hành dữ liệu vốn đã hợp pháp. Luật An ninh mạng đã nhấn mạnh: hành vi “cản trở, gây rối loạn hoạt động của mạng viễn thông, Internet, mạng máy tính, hệ thống thông tin” bị nghiêm cấm. Nếu một người tung ra công cụ tấn công từ chối dịch vụ (*DDoS*) làm tắc nghẽn mạng của một công dịch vụ dữ liệu công cộng, khiến người dân không truy cập được dịch vụ, đó chính là dấu hiệu của hành vi cản trở trái phép quá trình xử lý dữ liệu.



Hình ảnh: 02 đối tượng HTB và KTT bị CAT Hòa Bình khởi tố về hành vi "Mua bán phần mềm để sử dụng vào mục đích trái pháp luật" và "Xâm nhập trái phép vào mạng máy tính của người khác" năm 2024. Ảnh: Báo Chính phủ

- Hai là, tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin về dữ liệu: Đây là dạng hành vi tin tặc (*hacker*), xâm nhập bất hợp pháp vào hệ thống dữ liệu nhằm chiếm quyền kiểm soát, đánh cắp dữ liệu hoặc phá hủy hệ thống. Dấu hiệu rõ ràng nhất là các hành động như đột nhập trái phép qua lỗ hổng bảo mật, cài mã độc, đánh cắp thông tin đăng nhập, xóa hoặc mã hóa dữ liệu nhằm



đòi tiền chuộc, hoặc phá hoại phần cứng, phần mềm của cơ sở dữ liệu. Điều hình như các cuộc tấn công mạng vào website, cơ sở dữ liệu của cơ quan, doanh nghiệp để lấy cắp dữ liệu khách hàng, hoặc làm tê liệt dịch vụ. Theo Luật An ninh mạng, hành vi “xâm nhập trái phép vào hệ thống thông tin, cơ sở dữ liệu của người khác” và “chiếm quyền điều khiển, làm sai lệch, ngưng trệ hệ thống thông tin quan trọng” đều là hành vi bị cấm đặc biệt. Do đó, nếu phát hiện dấu hiệu truy cập bất hợp pháp, thay đổi hay đánh cắp dữ liệu trong hệ thống mà không được sự cho phép của chủ quản hệ thống, có thể xác định đó là hành vi phá hoại hoạt động xử lý và hệ thống dữ liệu.

Cần phân biệt rằng các hành vi can thiệp hệ thống dữ liệu có sự cho phép hợp pháp (ví dụ: cơ quan điều tra tiến hành trích xuất dữ liệu theo lệnh khám xét, hoặc quản trị viên hệ thống tạm ngưng xử lý dữ liệu để bảo trì) thì không bị xem là vi phạm. Chỉ khi thiếu căn cứ pháp luật và gây thiệt hại cho tính liên tục, toàn vẹn của hệ thống dữ liệu thì hành vi mới bị coi là “cản trở trái pháp luật” hoặc “tấn công, phá hoại”.

* Mức độ nguy hiểm:

Các hành vi cản trở, tấn công hệ thống dữ liệu được xem là hành vi nguy hiểm cho xã hội trong lĩnh vực công nghệ thông tin. Chúng gây ra nhiều hệ lụy nghiêm trọng:

- **Thứ nhất**, đe dọa an ninh, an toàn thông tin quốc gia. Nếu mục tiêu tấn công là các hệ thống thông tin quan trọng (cơ sở dữ liệu quốc gia, hạ tầng thông tin trọng yếu trong lĩnh vực tài chính, năng lượng, hàng không, quốc phòng...), hậu quả có thể rất nghiêm trọng. Một cuộc tấn công mạng có chủ đích có thể làm tê liệt dịch vụ công thiết yếu, rò rỉ bí mật nhà nước hoặc làm sai lệch dữ liệu quan trọng, đe dọa an ninh quốc gia. Ví dụ: hệ thống thông tin quản lý điều độ điện lưới hoặc giao thông hàng không nếu bị tin tặc chiếm quyền điều khiển có thể dẫn đến thảm họa. Do đó, Luật An ninh mạng xem việc phá hoại hệ thống thông tin quan trọng quốc gia là hành vi đặc biệt nghiêm trọng, có thể cấu thành các tội phạm như tấn công mạng hoặc khủng bố mạng.



- **Thứ hai**, thiệt hại kinh tế và gián đoạn dịch vụ xã hội. Khi hệ thống dữ liệu của doanh nghiệp, ngân hàng, bệnh viện... bị tấn công hoặc bị cản trở hoạt động, các dịch vụ cung cấp cho người dân sẽ bị gián đoạn. Ví dụ: một cuộc tấn công ransomware (*mã độc tống tiền*) mã hóa toàn bộ cơ sở dữ liệu bệnh viện sẽ khiến bệnh viện tê liệt hoạt động, bệnh nhân không được chăm sóc kịp thời, thậm chí nguy hiểm đến tính mạng cộng đồng. Thiệt hại kinh tế cũng rất lớn: theo thống kê, năm 2023 đã ghi nhận 13.900 vụ tấn công mạng vào các hệ thống tại Việt Nam, trung bình hơn 1.100 vụ mỗi tháng. Các cuộc tấn công này bao gồm cả việc đánh cắp dữ liệu và phá hoại hệ thống, gây tổn thất tài chính trực tiếp (*chi phí khắc phục, tiền chuộc dữ liệu*) lẫn gián tiếp (*gián đoạn kinh doanh, mất niềm tin khách hàng*).



Hình ảnh: Thiếu tướng Nguyễn Văn Giang - phó cục trưởng Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Bộ Công an - A05 trình bày tham luận "Thực trạng, chiêu trò lừa đảo của tội phạm mạng - Giải pháp ngăn ngừa". Ảnh: Báo Tuổi trẻ



- **Thứ ba**, hành vi này xâm phạm nghiêm trọng quyền, lợi ích hợp pháp của chủ thể dữ liệu và chủ sở hữu dữ liệu. Chủ thể dữ liệu có quyền được bảo vệ thông tin cá nhân, còn chủ sở hữu dữ liệu (*cơ quan, doanh nghiệp*) có quyền tài sản đối với dữ liệu của mình. Khi tin tặc chiếm đoạt dữ liệu cá nhân (*thông tin tài khoản, thẻ ngân hàng...*) và phát tán ra chợ đen, quyền riêng tư của hàng triệu người bị xâm hại và họ có thể trở thành nạn nhân của lừa đảo, trộm cắp danh tính. Đây là vi phạm nghiêm trọng quyền bảo mật dữ liệu cá nhân và gây hoang mang cho rất nhiều người.

* Chế tài xử lý:

Vì tính chất nguy hiểm như trên, chế tài đối với hành vi cản trở, phá hoại hoạt động xử lý và hệ thống dữ liệu rất nghiêm khắc. Về hành chính, Nghị định 15/2020/NĐ-CP quy định phạt tiền 140-170 triệu đồng đối với hành vi phá hoại hạ tầng thông tin hoặc phá hoại thông tin trên mạng. Mức phạt này là rất cao, thể hiện quyết tâm răn đe các vi phạm. Ngoài ra, hành vi truy cập trái phép, thay đổi, xóa bỏ nội dung thông tin của người khác trên mạng; cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn truy nhập trái phép... bị phạt từ 30 đến 50 triệu đồng. Đây đều là các mức phạt áp dụng cho tổ chức; cá nhân vi phạm sẽ chịu mức bằng một nửa. Song song đó, hình phạt bổ sung có thể bao gồm tịch thu tang vật, phương tiện vi phạm, hoặc trực xuất nếu người vi phạm là người nước ngoài. Về hình sự, Bộ luật Hình sự hiện hành có các tội danh như Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (*Điều 289*), Tội phát tán virus tin học (*Điều 290*) với khung hình phạt tù phạt tiền đến 5-12 năm tù tùy mức độ thiệt hại, Tội phá hoại cơ sở vật chất - kỹ thuật của nước CHXHCN Việt Nam (*Điều 303*) nếu nhắm vào hạ tầng quan trọng, có thể phạt tù từ 10 năm đến chung thân. Những chế tài này nhằm bảo đảm rằng hành vi tấn công, phá hoại hệ thống dữ liệu sẽ bị trừng trị thích đáng, tương xứng với hậu quả có thể gây ra.

Thực tế cho thấy Việt Nam đã phải đổi mới với không ít cuộc tấn công vào hệ thống dữ liệu những năm qua. Một ví dụ tiêu biểu là vụ tin tặc tấn công đồng



lộat các sân bay Nội Bài, Tân Sơn Nhất ngày 29/7/2016. Nhóm hacker 1937CN (được cho là từ Trung Quốc) đã xâm nhập hệ thống màn hình hiển thị và hệ thống phát thanh của sân bay, chèn các nội dung xuyên tạc, kích động về vấn đề Biển Đông. Sự cố này khiến nhiều hành khách hoảng hốt, hoạt động tại sân bay gián đoạn trong một thời gian ngắn. Đồng thời, website của Vietnam Airlines cũng bị chiếm quyền kiểm soát, trang chủ bị thay đổi hoàn toàn và hacker công bố đã lấy được dữ liệu hơn 400.000 khách hàng của hãng. Đây chính là hành vi tấn công, chiếm đoạt và phá hoại hệ thống thông tin, cơ sở dữ liệu ở quy mô lớn. Ngay sau đó, các cơ quan chức năng Việt Nam và chuyên gia đã vào cuộc ứng cứu, khôi phục hệ thống sau vài giờ. Vụ việc cảnh báo về mức độ nguy hiểm của hành vi tấn công mạng đối với an ninh quốc gia. Nếu hệ thống kiểm soát không lưu hoặc điều hành bay bị xâm nhập, hậu quả có thể thảm khốc. Rất may, trong vụ 2016, hacker chỉ chiếm được hệ thống màn hình thông tin, không xâm hại được hệ thống điều hành bay và an ninh sân bay. Tuy vậy, dữ liệu khách hàng bị lộ đã gây ảnh hưởng tiêu cực và thiệt hại uy tín đáng kể.

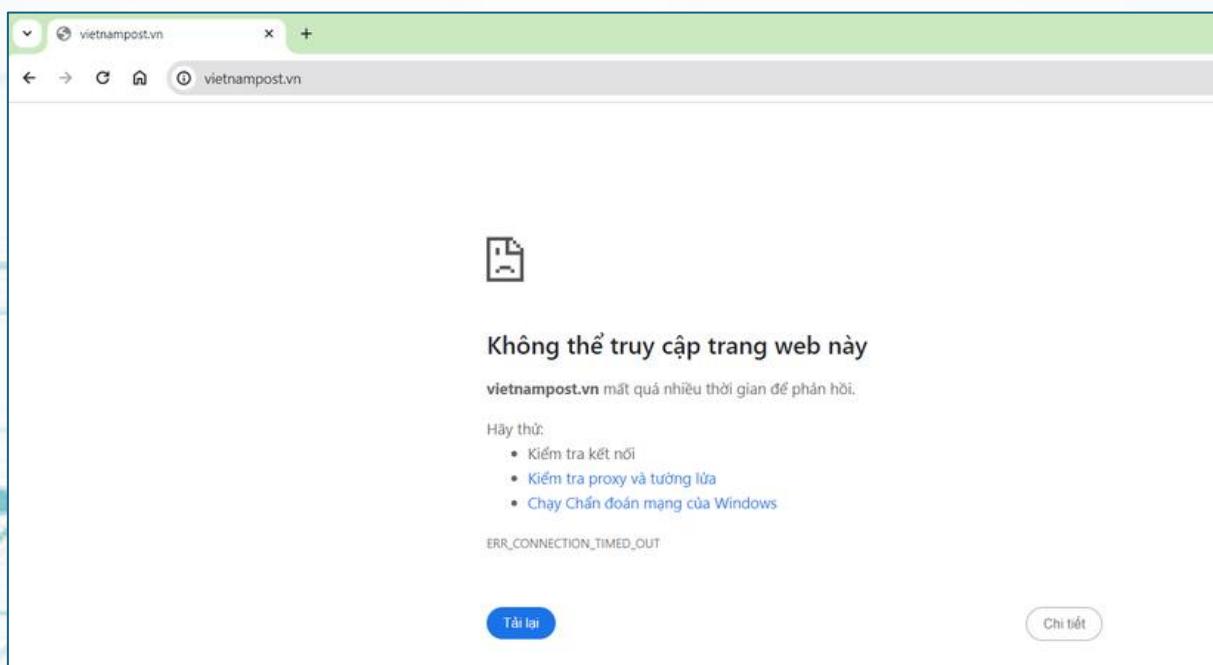


Hình ảnh: Dữ liệu 400.000 khách hàng của Vietnam Airlines bị đăng lên mạng năm 2016. Ảnh: Báo Vnexpress



Một ví dụ khác là các cuộc tấn công từ chối dịch vụ tháng 04/6/2024, Hệ thống thông tin của Bưu điện Việt Nam bị tê liệt vì hacker tấn công, kết quả toàn bộ hệ thống thông tin của Bưu điện Việt Nam (*Vietnam Post*) không thể truy cập được. Hệ thống bị tê liệt bao gồm website của không chỉ Tổng công ty Bưu điện Việt Nam vietnampost.vn, sàn TMĐT của Bưu điện Việt Nam tmdt.vnpost.vn và tất cả các website của bưu điện 63 tỉnh thành với định dạng tên miền vnpost.vn.

Đặc biệt, hệ thống thông tin liên quan hành chính công do Vietnam Post ([https://hcc.vnpost.vn](http://hcc.vnpost.vn)) đảm trách cũng tê liệt. Đây là hoạt động đóng vai trò đặc biệt quan trọng là “cánh tay nối dài” trong thực hiện cải cách hành chính, giúp người dân và các tổ chức, doanh nghiệp thuận tiện hơn, giảm thời gian chờ đợi và chi phí đi lại trong thực hiện các thủ tục hành chính tại tất cả các lĩnh vực.



Hình ảnh: Website vietnampost.vn của Tổng công ty Bưu điện Việt Nam không thể truy cập được - ảnh chụp trưa ngày 04/6/2024. Ảnh: Tạp chí Viettimes

Song song với hành vi tấn công, cũng có những vi phạm cản trở hoạt động dữ liệu từ bên trong tổ chức. Ví dụ: năm 2023, một công ty tố 2 nhân viên Gen Z xóa dữ liệu của công ty khi nghỉ việc, cụ thể 2 nhân viên đã vò vò Google Drive của công ty để xóa toàn bộ thông tin, hình ảnh, dữ liệu liên quan đến đại lý, cộng tác viên của công ty, gây thiệt hại lớn cho công ty; vụ việc được đăng báo để cảnh



báo, tuy nhiên không tiến hành xử lý hành chính, hình sự. Tuy nhiên có thể xác định hành vi này không những vi phạm Luật Dữ liệu 2024 mà còn cấu thành tội phạm hình sự như đã nêu.



Hình ảnh: Lịch sử truy cập của 02 nhân viên xóa dữ liệu của Công ty sau khi nghỉ việc. Ảnh: Báo Dân trí

Tóm lại, hành vi cản trở, phá hoại hoạt động xử lý và hệ thống dữ liệu để cập đến các hành vi tấn công, phá hoại kỹ thuật đối với hệ thống dữ liệu, có tính chất cố ý trực tiếp gây thiệt hại cho hạ tầng dữ liệu. Đây là nhóm hành vi nguy hiểm cao, bị pháp luật nghiêm cấm và chế tài mạnh mẽ. Các cá nhân, tổ chức cần nâng cao cảnh giác, tuân thủ quy định về an toàn thông tin để không tiếp tay hoặc rơi vào tình huống vi phạm pháp luật ở nhóm hành vi này.

3.1.2.3. Giả mạo, làm sai lệch, làm hư hỏng dữ liệu của cơ quan Nhà nước, tổ chức chính trị - xã hội

- Khoản 3 Điều 10 Luật Dữ liệu 2024 quy định cấm “*giả mạo, cố ý làm sai lệch, làm mất, làm hư hỏng dữ liệu trong cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội*”. Có thể thấy đối tượng dữ liệu được bảo vệ ở đây là dữ liệu trong các cơ sở dữ liệu của cơ quan công quyền và tổ chức chính trị - xã hội. Hành vi bị cấm bao gồm: *giả mạo dữ liệu, làm sai lệch dữ liệu, làm mất dữ liệu và làm hư hỏng dữ liệu*. Điểm chung của các hành vi này là đều liên quan đến việc thay đổi hoặc làm tổn hại tính nguyên vẹn của dữ liệu công một cách cố ý và trái phép.



Quy định này nhằm bảo vệ độ tin cậy và toàn vẹn của dữ liệu do các cơ quan công quyền quản lý. Trước đây, các hành vi tương tự cũng đã được đề cập trong một số văn bản pháp luật chuyên ngành. Ví dụ: Nghị định 144/2021/NĐ-CP về xử phạt vi phạm hành chính lĩnh vực an ninh, trật tự đã có quy định: phạt tiền 2-4 triệu đồng đối với hành vi “*có ý không cung cấp, cung cấp không đầy đủ, sai sự thật hoặc giả mạo thông tin, giấy tờ, tài liệu phục vụ xây dựng, cập nhật cơ sở dữ liệu quốc gia về dân cư*”. Đồng thời phạt 4-6 triệu đồng nếu “*làm sai lệch sổ sách, hồ sơ, giấy tờ, tài liệu, dữ liệu và thông tin công dân trong Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu cư trú, Cơ sở dữ liệu căn cước công dân*”. Quy định này cho thấy ngay trong mảng dữ liệu dân cư, việc giả mạo, làm sai lệch dữ liệu đã bị xử phạt khá nặng. Ngoài ra, Luật An ninh mạng cũng đề cập hành vi “*làm sai lệch hệ thống thông tin quan trọng về an ninh quốc gia*” là hành vi bị nghiêm cấm. Bộ luật Hình sự thì có tội danh Làm giả con dấu, tài liệu của cơ quan, tổ chức (Điều 341) áp dụng cho trường hợp làm giả giấy tờ, tài liệu. Tuy nhiên, trong môi trường số, giả mạo dữ liệu điện tử cũng nguy hiểm không kém. Vì vậy, Luật Dữ liệu 2024 đã cập nhật và đặt ra chế tài cho hành vi giả mạo, sai lệch, hủy hoại dữ liệu điện tử của cơ quan, tổ chức chính trị.

* **Dấu hiệu vi phạm:**

Hành vi Giả mạo, làm sai lệch, làm hư hỏng dữ liệu của cơ quan Nhà nước, tổ chức chính trị - xã hội tập trung vào dữ liệu của các cơ quan Đảng, Nhà nước, đoàn thể, nên có thể hiểu rằng dữ liệu công (*dữ liệu chính thức*) là đối tượng cần bảo vệ. Các hành vi cụ thể:

- **Một là**, giả mạo dữ liệu: là việc tạo ra dữ liệu giả hoặc làm giả dữ liệu gốc sao cho nó trông giống thật, nhằm lừa dối người khác. Dấu hiệu là dữ liệu được tạo ra không phải do cơ quan có thẩm quyền phát hành nhưng lại mạo danh, giả danh cơ quan đó. Ví dụ: làm giả công văn điện tử của UBND, làm giả chữ ký số, con dấu điện tử trên một tài liệu, hoặc tạo một bản sao dữ liệu nhưng thay đổi nội dung để giả làm dữ liệu thật. Trong bối cảnh công nghệ, giả mạo dữ liệu có thể thực hiện bằng cách copy cấu trúc dữ liệu thật rồi thay đổi một số trường thông



tin. Dấu hiệu nhận biết là sự không khớp với dữ liệu gốc (*nếu đổi chiếu*) hoặc vi phạm quy trình xác thực (*chữ ký số không hợp lệ, mã kiểm tra không đúng...*). Trường hợp điển hình là một người tạo ra email giả mạo địa chỉ thư điện tử công vụ của lãnh đạo cơ quan để gửi chỉ đạo giả, kèm theo tập tin có dữ liệu bị chỉnh sửa nội dung. Đây là hành vi giả mạo dữ liệu điện tử của cơ quan nhà nước.

- **Hai là**, cố ý làm sai lệch dữ liệu: tức là thay đổi, chỉnh sửa dữ liệu gốc một cách trái phép khiến dữ liệu không còn đúng như ban đầu. Dấu hiệu là dữ liệu có thật trong hệ thống nhưng bị sửa đổi nội dung (*thêm, bớt, sửa số liệu, văn bản*) hoặc nhập dữ liệu sai vào hệ thống. Ví dụ: một cán bộ có quyền truy cập hệ thống hộ tịch có ý sửa ngày sinh của một cá nhân trong Cơ sở dữ liệu dân cư; hoặc một nhân viên phòng tài nguyên môi trường cố tình cập nhật sai thông tin thửa đất trong cơ sở dữ liệu đất đai (*như chỉnh sửa diện tích, chủ sở hữu*) nhằm trực lợi. Hành vi này thường để lại dấu vết trong log hệ thống nếu có cơ chế giám sát (*ví dụ ai là người chỉnh sửa dữ liệu, vào thời điểm nào*). Làm sai lệch dữ liệu bao hàm cả việc nhập số liệu không chính xác, làm thông kê sai. Theo pháp luật về thông kê, việc cố ý báo cáo số liệu thống kê sai cũng là vi phạm (*phạt 3-7 triệu đồng theo khoản 4, Điều 5, Nghị định 95/2016/NĐ-CP*). Tóm lại, bất kỳ sự can thiệp nào khiến dữ liệu của cơ quan nhà nước không phản ánh đúng sự thật khách quan như vốn có đều có thể xem là hành vi làm sai lệch. Dấu hiệu nhận biết là sự mâu thuẫn, bất hợp lý trong dữ liệu (*ví dụ sổ sách giấy tờ một đằng, dữ liệu điện tử một nẻo*) hoặc khi phát hiện ra người không có thẩm quyền nhưng lại chỉnh sửa dữ liệu.

- **Ba là**, làm mất dữ liệu: tức là xóa bỏ hoặc khiến dữ liệu không còn tồn tại trong hệ thống khi chưa được phép. Dấu hiệu: dữ liệu đang có bị biến mất một cách bất thường. Ví dụ: một nhân viên CNTT không được phép nhưng đã xóa toàn bộ cơ sở dữ liệu lưu trữ hồ sơ công chức, khiến cơ quan mất dữ liệu quan trọng. Hoặc trường hợp tin tặc xâm nhập xóa dữ liệu lưu trữ của cơ quan (*cũng có thể xem là “làm mất” dữ liệu*). Hành vi làm mất dữ liệu có thể do cố ý phá hoại hoặc nhằm che giấu sai phạm (*xóa dữ liệu giao dịch chứng từ để phi tang*). Dấu



hiệu nhận biết thường rõ ràng: dữ liệu không còn, hoặc dung lượng cơ sở dữ liệu giảm đột ngột, log hệ thống cho thấy lệnh “delete” (*xóa*) được thực hiện trái phép.

- **Bốn là**, làm hư hỏng dữ liệu: tức là làm tổn hại dữ liệu đến mức nó không sử dụng được, không đọc được, hoặc bị lỗi. Khác với “mất” (*dữ liệu không còn*), “hư hỏng” có thể hiểu là dữ liệu vẫn còn nhưng bị biến dạng hoặc lỗi. Ví dụ: một người cố ý ghi đè dữ liệu rác lên tập tin cơ sở dữ liệu của cơ quan làm cho file dữ liệu bị hỏng cấu trúc, không thể mở hay khôi phục; hoặc cố tình mã hóa (*encrypt*) dữ liệu mà không cung cấp khóa, biến dữ liệu thành dạng vô nghĩa. Hành vi này cũng có thể do phần cứng bị phá hoại (*vd: làm hỏng đĩa cứng chứa dữ liệu*) hoặc phần mềm (*vd: dùng script làm lỗi toàn bộ bảng dữ liệu*). Dấu hiệu: hệ thống báo lỗi không truy cập được dữ liệu, dữ liệu bị mã hóa lạ, hoặc chất lượng dữ liệu suy giảm (*ví dụ hình ảnh, tài liệu bị hỏng, không đọc được*).

Tất cả các hành vi trên đều phải xảy ra trong phạm vi cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Mặt trận TQVN, đoàn thể mới thuộc nhóm hành vi vi phạm điểm này. Điều này nhấn mạnh tính chất công của dữ liệu, tức dữ liệu được coi là tài sản công, cần bảo vệ. Nếu ai đó giả mạo, làm sai lệch dữ liệu thuần túy cá nhân của người khác (*ví dụ giả mạo email cá nhân, sửa điểm trong cơ sở dữ liệu của một công ty tư nhân*) thì sẽ không áp vào khoản 3 Điều 10, mà có thể xử lý dưới góc độ khác (*vi phạm quyền cá nhân, hoặc xâm phạm tài sản công dân*). Còn khi dữ liệu thuộc về cơ quan công quyền, hành vi xâm hại sẽ bị xử lý nghiêm theo khoản 3 Điều 10.

* **Mức độ nguy hiểm:**

Hành vi giả mạo, sai lệch hay hủy hoại dữ liệu công gây nguy hiểm ở nhiều khía cạnh:

- **Thứ nhất**, xâm hại đến hoạt động quản lý nhà nước và làm giảm niềm tin công chúng. Dữ liệu của cơ quan nhà nước thường được sử dụng làm căn cứ ra quyết định quản lý, điều hành (*ví dụ dữ liệu dân cư dùng cấp CCCD, dữ liệu đất đai dùng cấp sổ đỏ, dữ liệu giáo dục dùng xét tốt nghiệp...*). Nếu dữ liệu này bị làm giả hoặc làm sai lệch, các quyết định hành chính, pháp lý dựa trên đó sẽ sai



theo, dẫn đến hậu quả dây chuyền. Ví dụ: nếu dữ liệu hộ khẩu bị sửa sai, một người không đủ điều kiện có thể được nhập hộ khẩu trái phép; hoặc nếu dữ liệu văn bằng chứng chỉ bị giả mạo, sẽ có người dùng bằng giả lọt vào bộ máy. Những điều này ảnh hưởng nghiêm trọng đến trật tự quản lý nhà nước. Hơn nữa, khi các vụ giả mạo dữ liệu công bị phát hiện, người dân sẽ mất niềm tin vào hệ thống thông tin của Nhà nước, hoài nghi tính chính xác của giấy tờ, hồ sơ điện tử do cơ quan công quyền cung cấp. Điều đó có thể cản trở quá trình chuyển đổi số và dịch vụ công trực tuyến (*vì người dân không tin dữ liệu điện tử nữa, lại muốn quay về giấy tờ trực tiếp*).

- **Thứ hai**, tiếp tay cho tham nhũng, tiêu cực. Thực tế, nhiều vụ án tham nhũng, lạm dụng chức vụ đều liên quan đến việc làm sai lệch hồ sơ, dữ liệu. Ví dụ: một số cán bộ đã chỉnh sửa dữ liệu quy hoạch đất đai, xóa tên khỏi danh sách thu hồi đất hoặc thêm dự án “ma” vào hệ thống để hợp thức hóa giấy tờ, trực lợi tài sản nhà nước. Hành vi này không chỉ vi phạm pháp luật dữ liệu mà còn cấu thành các tội về chức vụ (*giả mạo trong công tác, lợi dụng chức vụ...*). Dữ liệu sai lệch là công cụ che giấu hành vi phạm tội, do đó mức nguy hiểm rất cao. Nếu không kiểm soát chặt, dữ liệu công bị thao túng sẽ tạo kẽ hở cho các đường dây tham nhũng, gây thất thoát tài sản nhà nước hoặc xâm phạm quyền lợi của công dân lương thiện.

- **Thứ ba**, gây hậu quả nghiêm trọng về pháp lý và kinh tế. Dữ liệu công thường có giá trị pháp lý. Ví dụ: dữ liệu hộ tịch xác nhận tình trạng hôn nhân, dữ liệu lý lịch tư pháp xác nhận tiền án. Khi dữ liệu này bị giả mạo hoặc làm mất, quyền lợi công dân có thể bị ảnh hưởng trực tiếp. Một trường hợp xấu, nếu dữ liệu tiền án của một người bị làm sai lệch (*xoá án tích bất hợp pháp*), người đó có thể lọt việc rà soát TCCT và được tuyển dụng, bổ nhiệm vào vị trí nhạy cảm, đây là mối nguy cho an ninh. Hoặc nếu dữ liệu kinh tế vĩ mô bị làm giả, sai lệch (*ví dụ số liệu báo cáo sai*), Chính phủ có thể ban hành chính sách không phù hợp, gây thiệt hại kinh tế trên diện rộng. Như vậy, mức độ nguy hiểm không chỉ dừng ở phạm vi một cơ sở dữ liệu, mà còn lan sang các quyết sách và lợi ích chung của xã hội.



* Chế tài xử lý:

Pháp luật hiện hành đã có các chế tài nhất định cho nhóm hành vi này. Về hành chính, ngoài các mức phạt nêu ở Nghị định 144/2021/NĐ-CP (*phạt đến 6 triệu đồng cho làm sai lệch dữ liệu dân cư*), Nghị định 15/2020/NĐ-CP (*sửa đổi 2022*) cũng phạt 80-100 triệu đồng đối với việc sử dụng công nghệ thông tin để giả mạo thông tin, tài liệu trong giao kết hợp đồng viễn thông. Đây là trường hợp giả mạo thông tin thuê bao di động, một dạng dữ liệu gốc do doanh nghiệp viễn thông quản lý nhưng cũng ảnh hưởng đến cơ sở dữ liệu của Bộ Công an. Về hình sự, tùy hành vi cụ thể: nếu làm giả giấy tờ, tài liệu cơ quan thì có tội làm giả tài liệu (*Điều 341 Bộ luật Hình sự*) với khung phạt đến 7 năm tù. Nếu hành vi xâm phạm dữ liệu ở mức độ nguy hiểm (*ví dụ xâm nhập máy tính cơ quan để sửa điểm thi, cắp không bằng tốt nghiệp*), có thể truy tố tội xâm nhập trái phép mạng máy tính (*Điều 289 Bộ luật Hình sự*) như đã đề cập, mức phạt tù đến 12 năm. Một trường hợp khác: nếu hành vi làm sai lệch dữ liệu của cán bộ, công chức nhằm vụ lợi, có thể bị xử lý về tội giả mạo trong công tác (*Điều 359 Bộ luật Hình sự, tối đa 20 năm tù nếu gây hậu quả rất nghiêm trọng*). Nhìn chung, tùy mục đích và hậu quả, hành vi giả mạo, làm sai lệch, làm hư hỏng dữ liệu của cơ quan Nhà nước, tổ chức chính trị - xã hội có thể bị xử lý hành chính hoặc hình sự rất nghiêm khắc.



Hình ảnh: Trang Fanpage và văn bản giả mạo Bộ Tài chính. Ảnh: TC Hải Quan



Thực tế đã có nhiều vụ việc trong thực tế liên quan đến việc giả mạo, làm sai lệch dữ liệu của cơ quan nhà nước:

Ví dụ như việc giả mạo văn bản, tài liệu của cơ quan nhà nước. Ngày 31/3/2025, Bộ Tài chính cảnh báo trang Facebook có tên “Tiếp nhận Xử lý Thu hồi và Hoàn trả vốn treo” có cá nhân xanh của Facebook làm giả “Giấy xác nhận kết quả thu hồi của Bộ Tài chính” để phục vụ hoạt động lừa đảo.

Hoặc như vụ việc mới xảy ra cuối năm 2024 vừa qua, Cơ quan Công an tỉnh Thanh Hóa khởi tố vụ án, bắt giữ 16 đối tượng là nhân viên công ty bảo hiểm, nhân viên y tế làm việc tại bệnh viện tuyến huyện về hành vi cấu kết lập hồ sơ giả nhầm rút tiền bảo hiểm trái phép.

STT	Khoa	Họ tên	Năm sinh	Địa chỉ	Vào viện	Ra viện	Bệnh
1	Truyền nhiễm	Dương Thị Hiền	1990	Đông Vệ	4/11/2021	14/11/2021	Viêm phổi cấp
2	Truyền nhiễm	Lê Văn Long	1986	Đông Vệ	17/8/2021	26/8/2021	Ngộ độc thức ăn
3	Nội	Lê Thị Duyên	1994	Minh Sơn, Ngọc Lặc	7/4/2023	16/4/2023	Viêm ruột
4	Nội	Lê Thị Thắng	1982	Thiệu Tiên, Thiệu Hoá	2/3/2023	11/3/2023	Viêm phế quản cấp
5	Nội	Dương Thị Hiền	1990	Đông Vệ	22/6/2021	2/7/2021	Ngộ độc thức ăn
6	Nội	Lê Hồng Quân	1984	Quang Trung, Ngọc Lặc	23/3/2023	1/4/2023	Nhiễm khuẩn đường tiết niệu
7	Nội	Lương Khắc Chung	1988	Thạch Cẩm, Thạch Thành	7/4/2023	16/4/2023	Nhiễm độc thức ăn
8	Nội	Bùi Thị Huyền Trang	1991	Ngọc Trao	8/3/2023	18/3/2023	Viêm phổi cấp
9	Nội	Đinh Thị Hà	1968	Thiệu Tiên, Thiệu Hoá	6/3/2023	16/3/2023	Viêm phế quản cấp
10	Nhi	Nguyễn Phạm Bảo An	2019	Trường Thi	5/4/2024	15/4/2024	Viêm phế quản
11	Nhi	Nguyễn Phạm Bảo An	2019	Trường Thi	2/11/2022	12/11/2022	Viêm phổi
12	Nhi	Dương Văn Gia Huy	2020	Thiệu Dương	29/3/2023	8/4/2023	Viêm phế quản cấp
13	Nội	Hà Thị Quê	1975	Thiệu Tiên, Thiệu Hoá			
14	Ngoại	Phạm Thị Đỗ Anh	1987	Trường Thi	21/3/2024	31/3/2024	Ngộ độc thức ăn
15	Ngoại	Dương Thị Hiền	1990	Đông Vệ	1/4/2024	11/4/2024	Áp xe mông trái
16	Ngoại	Lê Thị Oanh	1979	Thị Bình, Triệu Sơn	12/1/2024	22/01/2024	Ngộ độc thức ăn
17	Ngoại	Lê Trọng Chung	1971	Lam Sơn	12/1/2024	22/01/2024	Nhiễm khuẩn tiết niệu
18	Ngoại	Hác Thị Yên	1990	Thị Xuân	15/1/2024	25/1/2024	Ngộ độc thức ăn
19	Ngoại	Nguyễn Văn Hoà	2005	Quảng Xương	1/12/2024	1/2/2024	Viêm bàng quang cấp
20	Ngoại	Lê Thị Đào	1964	Quảng Hưng	15/01/2024	25/01/2024	Áp xe nách trái

Hình ảnh: Danh sách công khai 20 bệnh án giả tại Bệnh viện Đa khoa TP Thanh Hóa (nay là Bệnh viện Đa khoa Hạc Thành) với mục đích chiếm đoạt tiền cùi các công ty bảo hiểm. Ảnh: Công an tỉnh Thanh Hóa

Những ví dụ trên nhấn mạnh rằng việc bảo vệ tính xác thực và toàn vẹn của dữ liệu công là hết sức quan trọng. Bất cứ hành vi giả mạo, chỉnh sửa hay hủy hoại dữ liệu nào đều có thể để lại hậu quả dài lâu và phải trả giá đắt bằng pháp lý. Do đó, Luật Dữ liệu 2024 và các văn bản liên quan đặt ra ranh giới rõ ràng: dữ liệu của cơ quan, tổ chức công tuyệt đối không được xâm hại, việc cập nhật, chỉnh



sửa phải tuân đúng quy trình và thẩm quyền; mọi sự can thiệp trái phép sẽ bị xử lý nghiêm minh.

3.1.2.4. Có ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu khi có nghĩa vụ

Khoản 4 Điều 10 Luật Dữ liệu 2024 cấm “có ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định của pháp luật”. Đây là nhóm hành vi tập trung vào trách nhiệm cung cấp dữ liệu của các tổ chức, cá nhân khi pháp luật yêu cầu. Có hai hành vi cụ thể bị cấm: ⁽¹⁾Cung cấp dữ liệu sai lệch một cách cố ý; ⁽²⁾Không cung cấp dữ liệu khi pháp luật quy định phải cung cấp. Nói cách khác, khi có nghĩa vụ phải cung cấp thông tin, dữ liệu cho cơ quan có thẩm quyền hoặc cho hệ thống cơ sở dữ liệu chung, thì chủ thể phải cung cấp đầy đủ, chính xác, kịp thời; nếu cố tình cung cấp sai hoặc từ chối cung cấp, đó là hành vi vi phạm.

Quy định này rất cần thiết trong bối cảnh Việt Nam đang xây dựng Chính phủ điện tử và các cơ sở dữ liệu quốc gia. Nhiều văn bản pháp luật đã xác định nghĩa vụ cung cấp dữ liệu. Ví dụ: Điều 18 Luật Dữ liệu 2024 quy định: “Tổ chức, cá nhân phải cung cấp dữ liệu cho cơ quan nhà nước khi có yêu cầu của cơ quan có thẩm quyền” trong một số trường hợp đặc thù (*nhiều ứng phó khẩn cấp, phòng chống khủng bố*). Hoặc Luật Bảo vệ Dữ liệu Cá nhân 2025 nêu nghĩa vụ của chủ thể dữ liệu là “cung cấp đầy đủ, chính xác dữ liệu cá nhân của mình theo quy định của pháp luật, theo hợp đồng hoặc khi đồng ý cho phép xử lý dữ liệu cá nhân”. Điều này có nghĩa nếu cá nhân đã đồng ý cung cấp thông tin (*ví dụ điền vào biểu mẫu cấp giấy tờ*) thì phải cung cấp đúng sự thật. Nghị định 144/2021/NĐ-CP, cũng phạt 2-4 triệu đồng nếu công dân “cố ý không cung cấp hoặc cung cấp không đầy đủ, sai sự thật thông tin phục vụ xây dựng cơ sở dữ liệu quốc gia về dân cư”. Quy định này rất sát với tinh thần của khoản 4 Điều 10. Ngoài ra, trong lĩnh vực khác, có thể kể: Nghị định 119/2020/NĐ-CP (*xử phạt báo chí*) phạt nặng hành vi không cung cấp thông tin cho báo chí khi có yêu cầu theo luật; hoặc Nghị định 166/2018/NĐ-CP phạt hành vi không cung cấp hoặc cung cấp sai thông tin trong điều tra thống kê... Rõ ràng, việc cung cấp dữ liệu đầy đủ, đúng đắn theo yêu cầu



pháp luật là nghĩa vụ được quy định ở nhiều nơi, Luật Dữ liệu 2024 đã khẳng định nguyên tắc chung: cấm cố ý làm sai hoặc trốn tránh nghĩa vụ này.

* **Dấu hiệu vi phạm:**

Để hiểu rõ hành vi cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu khi có nghĩa vụ, cần xác định khi nào có nghĩa vụ cung cấp dữ liệu và hành vi sai phạm là gì:

- **Một là**, nghĩa vụ cung cấp dữ liệu theo quy định pháp luật: Thông thường, nghĩa vụ này phát sinh trong các trường hợp như: cung cấp dữ liệu cho cơ quan nhà nước có thẩm quyền khi họ yêu cầu (ví dụ cơ quan điều tra yêu cầu doanh nghiệp cung cấp dữ liệu giao dịch; Sở Văn hóa, Thể thao yêu cầu mạng xã hội cung cấp dữ liệu người dùng vi phạm; hoặc đơn giản là công dân phải khai báo dữ liệu cá nhân trung thực khi làm thủ tục hành chính); hoặc cung cấp dữ liệu vào các hệ thống cơ sở dữ liệu bắt buộc (ví dụ doanh nghiệp viễn thông phải kết nối, cung cấp dữ liệu thuê bao di động vào Cơ sở dữ liệu thông tin thuê bao tập trung của Bộ Công an). Cũng có trường hợp nghĩa vụ theo hợp đồng hoặc thỏa thuận nhưng “theo quy định pháp luật” có nghĩa nhà nước đã quy định rõ trong luật hoặc văn bản dưới luật. Khi những tình huống đó xảy ra, chủ thể không được từ chối hoặc cung cấp thông tin giả.

- **Hai là**, cung cấp dữ liệu sai lệch (*một cách cố ý*): Dấu hiệu là dữ liệu được cung cấp khác với thực tế hoặc khác với dữ liệu gốc, do người cung cấp biết rõ nhưng vẫn làm. “Sai lệch” nghĩa là sai về nội dung, không đúng sự thật hoặc không đúng với yêu cầu. Ví dụ: khi kê khai thông tin vào hệ thống đăng ký kinh doanh, doanh nghiệp cố ý nhập sai vốn điều lệ, sai ngành nghề so với thực tế nhằm được cấp giấy phép dễ dàng. Hoặc nghiêm trọng hơn, một công ty khi được cơ quan thuế yêu cầu nộp dữ liệu sổ sách, đã cung cấp bản dữ liệu đã chỉnh sửa (*che giấu doanh thu thật*). Tất cả các tình huống đó đều là cung cấp dữ liệu sai lệch. Điều kiện là cố ý, tức người cung cấp biết sai mà vẫn cung cấp, chứ không phải nhầm lẫn vô ý. Trường hợp vô ý, nhầm lẫn có thể được xem xét giảm nhẹ hoặc không bị coi là vi phạm nếu kịp thời đính chính. Dấu hiệu nhận biết thường dựa



vào đối chiếu khi cơ quan chức năng kiểm tra và phát hiện mâu thuẫn giữa dữ liệu được cung cấp với dữ liệu thực tế. Ví dụ: đối chiếu hồ sơ gốc và dữ liệu đã nộp, thấy không trùng khớp.

- **Ba là**, không cung cấp dữ liệu khi có nghĩa vụ: Dấu hiệu ở đây là sự không thực hiện hành vi cung cấp, mặc dù pháp luật yêu cầu phải làm. Ví dụ: Chính phủ quy định doanh nghiệp phải định kỳ báo cáo, cung cấp dữ liệu về lao động cho Sở Lao động - Thương binh và Xã hội, nhưng một doanh nghiệp không gửi báo cáo, né tránh việc cung cấp thông tin lao động. Hoặc một nhà cung cấp dịch vụ viễn thông không kết nối chia sẻ cơ sở dữ liệu thuê bao với cơ quan quản lý mặc dù đã có lệnh, tức là từ chối cung cấp dữ liệu. Lưu ý, không cung cấp ở đây chủ yếu nói về trường hợp có yêu cầu cụ thể hoặc có quy định bắt buộc. Nếu pháp luật không yêu cầu mà chủ thể không cung cấp thì không thể xem là vi phạm. Do đó, dấu hiệu tiên quyết là phải xác định có văn bản quy phạm hoặc văn bản yêu cầu cá biệt bắt buộc cung cấp dữ liệu. Ví dụ: Điều 18 Luật Dữ liệu 2024 cho phép cơ quan có thẩm quyền yêu cầu cung cấp dữ liệu trong tình huống khẩn cấp, vậy nếu doanh nghiệp bị yêu cầu mà không cung cấp thì vi phạm. Hoặc quy định về cơ sở dữ liệu tổng hợp quốc gia buộc các bộ ngành phải cung cấp dữ liệu đầu vào, nếu một bộ ngành cố tình không chia sẻ dữ liệu của mình vào hệ thống chung, đó cũng là vi phạm nghĩa vụ cung cấp (*hiện Chính phủ đang hoàn thiện hành lang pháp lý cho việc chia sẻ dữ liệu giữa các cơ quan nhà nước*).

Nhìn chung, quy định cấm cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu khi có nghĩa vụ hướng tới việc đảm bảo dòng chảy thông tin thông suốt và trung thực trong các mối quan hệ pháp lý. Dữ liệu phải được cung cấp đúng và đủ để việc quản lý, ra quyết định chính xác. Dấu hiệu vi phạm nhóm này thường bị phát hiện khi có sự sai lệch, thiếu hụt thông tin mà lẽ ra phải có.

* Mức độ nguy hiểm:

So với các nhóm hành vi trước, hành vi cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu khi có nghĩa vụ có thể nhìn bề ngoài ít nghiêm trọng hơn



(vì không trực tiếp phá hoại hay chống phá), nhưng thực tế cũng gây ra những nguy cơ lớn nếu phổ biến:

- **Thứ nhất**, làm suy giảm hiệu lực quản lý và chất lượng dịch vụ công: Khi một cá nhân/tổ chức không cung cấp dữ liệu theo yêu cầu, cơ quan chức năng sẽ thiếu thông tin để ra quyết định hoặc thực thi nhiệm vụ. Ví dụ: nếu một doanh nghiệp không nộp dữ liệu quan trắc môi trường, cơ quan môi trường sẽ không biết doanh nghiệp có xả thải vượt chuẩn hay không để xử lý kịp thời, gây nguy cơ ô nhiễm môi trường kéo dài. Hoặc nếu các bộ ngành không chịu chịu chia sẻ dữ liệu chuyên ngành vào Cơ sở dữ liệu tổng hợp quốc gia, Chính phủ sẽ không có bức tranh đầy đủ để điều hành, điều này cản trở mục tiêu chuyển đổi số đồng bộ. Về dài hạn, những "khoảng trống thông tin" do hành vi không cung cấp dữ liệu tạo ra sẽ khiến hệ thống dữ liệu quốc gia bị khiếm khuyết, phân mảnh, ảnh hưởng đến hiệu quả phục vụ người dân.

- **Thứ hai**, gây sai lệch trong hoạch định chính sách và thực thi pháp luật: Dữ liệu không đầy đủ hoặc sai lệch do chủ thể cung cấp cố ý sẽ khiến các báo cáo, thống kê trở nên thiếu chính xác. Nếu nhiều đơn vị vì thành tích mà báo cáo sai (ví dụ cung cấp số liệu giảm nghèo không đúng thực tế, khai man chỉ tiêu kinh tế), các cấp lãnh đạo có thể ban hành chính sách không phù hợp, gây lãng phí nguồn lực hoặc bỏ sót vấn đề cần giải quyết. Chính vì vậy, luật thống kê và các quy định về báo cáo đều nghiêm cấm việc báo cáo sai. Bên cạnh đó, trong hoạt động tư pháp, nếu người giám định cung cấp tài liệu sai sự thật dẫn đến án oan, sai, thì hậu quả cực kỳ nghiêm trọng (có thể bị phạt tù 1-3 năm theo Điều 382 Bộ luật Hình sự). Tóm lại, tính trung thực của dữ liệu là nền tảng của nhà nước pháp quyền; bất kỳ sự cố ý sai lệch nào cũng bào mòn nền tảng đó.

- **Thứ ba**, xâm phạm quyền lợi của các bên liên quan: Khi một người không cung cấp dữ liệu cá nhân đầy đủ, chính xác theo yêu cầu, chính họ hoặc người khác có thể chịu thiệt. Ví dụ: nếu một bệnh nhân che giấu thông tin bệnh sử khi khám bệnh (cung cấp thiếu dữ liệu y tế), bác sĩ có thể chẩn đoán sai, gây hại sức khỏe chính bệnh nhân. Hoặc nếu doanh nghiệp không cung cấp dữ liệu lao động,



người lao động có thẻ không được đảm bảo quyền lợi (*vì cơ quan Bảo hiểm xã hội không nắm thông tin để thu bảo hiểm, sau này người lao động sẽ khó khăn trong hưởng chính sách*). Ngoài ra, hành vi không cung cấp dữ liệu cũng thường đi đôi với sự thiếu minh bạch, tạo môi trường cho tiêu cực (*ví dụ doanh nghiệp không nộp dữ liệu tài chính có thẻ đang trốn thuế...*).

Chế tài đối với hành vi này hiện chủ yếu ở mức hành chính. Nghị định 144/2021 phạt tối đa 4 triệu đồng nếu có ý không cung cấp hoặc cung cấp sai thông tin cho cơ sở dữ liệu dân cư. Nghị định 15/2020/NĐ-CP (*Sửa đổi năm 2022*) cũng có nhiều điều khoản phạt hành vi không cung cấp dữ liệu theo yêu cầu của cơ quan quản lý. Ví dụ: phạt 80-100 triệu đồng nếu doanh nghiệp viễn thông không đảm bảo truy nhập cơ sở dữ liệu thuê bao cho cơ quan chức năng kiểm tra, hoặc phạt 20-30 triệu đồng nếu không cung cấp dữ liệu hạ tầng kỹ thuật viễn thông theo yêu cầu của cơ quan nhà nước. Những mức phạt này cho thấy việc không cung cấp dữ liệu theo nghĩa vụ bị coi là vi phạm nghiêm trọng trong lĩnh vực chuyên ngành, đặc biệt khi liên quan an ninh (*thuê bao điện thoại gắn với an ninh trật tự, nên không cung cấp thông tin thuê bao cho Bộ Công an kiểm tra sẽ bị phạt rất nặng*). Về hình sự, khó có tội danh độc lập cho hành vi này, nhưng nếu việc không cung cấp dữ liệu đồng nghĩa với che giấu tội phạm hoặc cản trở điều tra, thì có thể bị xử lý về các tội tương ứng (*nhiều Tội không tố giác tội phạm, Tội che giấu tội phạm nếu dữ liệu đó lê ra phải cung cấp để tố giác*).

Trong đợt dịch COVID-19, có trường hợp cá nhân không khai báo trung thực lịch trình di chuyển hoặc tình trạng sức khỏe, dẫn đến làm lây lan dịch bệnh. Một ví dụ: tháng 2/2020, bệnh nhân số 34 ở Bình Thuận không cung cấp đầy đủ thông tin về những người mình đã tiếp xúc, khiến cơ quan y tế không truy vết kịp một số F1, gây bùng phát ổ dịch địa phương. Đây là trường hợp nghĩa vụ cung cấp thông tin được quy định trong Luật Phòng chống bệnh truyền nhiễm, việc không tuân thủ đã gây hậu quả nghiêm trọng, đủ dấu hiệu cấu thành Tội làm lây lan dịch bệnh nguy hiểm.



3.1.3 Kết luận

- **Thứ nhất**, Điều 10 Luật Dữ liệu 2024 phản ánh quan điểm nhất quán của Nhà nước về bảo vệ an ninh, trật tự trong không gian dữ liệu số. Mọi hành vi sử dụng dữ liệu để xâm hại lợi ích quốc gia, quyền con người, hay phá hoại hạ tầng dữ liệu, gian dối trong cung cấp thông tin đều bị đặt ngoài vòng pháp luật. Điều này tạo khung pháp lý vững chắc để xử lý các thách thức an ninh phi truyền thống trong kỷ nguyên số.

- **Thứ hai**, bốn nhóm hành vi cấm nêu trên có ranh giới rõ ràng giữa hoạt động hợp pháp và vi phạm. Hoạt động xử lý dữ liệu được coi là hợp pháp khi phục vụ mục đích chính đáng, tôn trọng quyền và lợi ích hợp pháp của mọi bên và tuân thủ quy trình pháp luật. Khi mục đích bị lệch lạc (*nhằm chống phá, xâm hại*) hoặc phương thức thủ đoạn trái phép (*tấn công, giả mạo, che giấu thông tin*), thì đó là hành vi vi phạm. Nhận thức đúng ranh giới này giúp các tổ chức, cá nhân hành xử đúng luật trong thu thập, chia sẻ, sử dụng dữ liệu.

- **Thứ ba**, mức độ nguy hiểm của các hành vi cấm rất cao, do dữ liệu ngày nay là tài sản chiến lược và huyết mạch của xã hội số. Một hành vi vi phạm về dữ liệu có thể gây hậu quả lan rộng hơn nhiều so với các vi phạm truyền thống (ví dụ *tin giả lan truyền online nhanh hơn tin đồn trực tiếp; tấn công mạng có thể gây thiệt hại hàng loạt cùng lúc*). Do đó, pháp luật đã và đang quy định những chế tài nghiêm khắc tương ứng, từ phạt hành chính hàng trăm triệu đồng đến truy cứu hình sự với mức án tù nặng nhằm răn đe, phòng ngừa hữu hiệu.

- **Thứ tư**, thực tiễn Việt Nam vài năm qua cho thấy nhiều bài học kinh nghiệm: sự cần thiết của việc nâng cao nhận thức và trách nhiệm về cung cấp thông tin trung thực; tầm quan trọng của bảo mật hệ thống dữ liệu trước nguy cơ tấn công; cũng như sự phối hợp liên ngành trong xử lý các vụ việc vi phạm. Các vụ giả mạo văn bản, tấn công hệ thống sân bay, vi phạm dữ liệu dân cư... đã được xử lý kịp thời, nhưng cũng đặt ra yêu cầu tiếp tục hoàn thiện thể chế và nâng cao năng lực thực thi pháp luật trong lĩnh vực dữ liệu.



Kết luận lại, việc quy định các hành vi bị nghiêm cấm trong Luật Dữ liệu 2024 là bước đi kịp thời và cần thiết, tạo nền tảng pháp lý cho sự phát triển bền vững của kinh tế số, chính phủ số tại Việt Nam. Các cá nhân, tổ chức cần tuân thủ nghiêm những quy định này, đồng thời Nhà nước cần đẩy mạnh tuyên truyền, phổ biến luật để toàn xã hội hiểu rõ và cùng tham gia phòng chống các hành vi vi phạm. Chỉ khi đó, những giá trị tích cực của dữ liệu mới được phát huy tối đa, còn mặt trái, rủi ro của dữ liệu sẽ được kiểm soát, giữ vững an ninh quốc gia và quyền lợi của nhân dân trong thời đại số hóa.

3.2. Giải pháp hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu

3.2.1. Thực trạng quy định pháp luật hiện hành về xử lý vi phạm trong lĩnh vực dữ liệu

Tại Việt Nam, việc xử lý vi phạm hành chính được điều chỉnh thống nhất bởi Luật Xử lý vi phạm hành chính. Luật này quy định nguyên tắc, thẩm quyền, thủ tục xử phạt và các hình thức chế tài hành chính áp dụng cho mọi lĩnh vực, bao gồm lĩnh vực dữ liệu. Theo Luật Xử lý vi phạm hành chính, chỉ những hành vi vi phạm được quy định cụ thể trong các văn bản pháp luật (*Nghị định của Chính phủ*) mới có thể bị xử phạt hành chính; mức phạt tiền tối đa cũng được ấn định theo lĩnh vực quản lý. Luật Xử lý vi phạm hành chính hiện hành (năm 2012, sửa đổi 2025) giới hạn mức phạt tiền tối đa theo từng lĩnh vực và quy định nguyên tắc phân biệt mức phạt giữa cá nhân và tổ chức (*thông thường mức phạt với tổ chức gấp đôi cá nhân*). Trong lĩnh vực bảo vệ dữ liệu, hiện chưa có một văn bản chuyên biệt nào liệt kê đầy đủ các hành vi vi phạm và chế tài tương ứng; việc xử phạt chủ yếu dựa vào các nghị định xử phạt trong lĩnh vực công nghệ thông tin, an toàn thông tin mạng, hoặc bảo vệ quyền lợi người tiêu dùng, thương mại điện tử... phù hợp với tính chất từng vụ việc. Điều này dẫn đến tình trạng chế tài còn chưa đầy đủ, toàn diện để làm cơ sở xử phạt mọi hành vi vi phạm liên quan tới dữ liệu trong thực tiễn.

Một số luật chuyên ngành đã bước đầu đề cập trách nhiệm bảo vệ dữ liệu, nhưng mới dừng ở nguyên tắc chung. Luật An ninh mạng 2018 đặt ra các nghĩa



vụ bảo vệ an ninh quốc gia trên không gian mạng, trong đó có yêu cầu bảo vệ dữ liệu quan trọng, dữ liệu người dùng... Luật An ninh mạng nghiêm cấm các hành vi tấn công mạng, gián điệp mạng, chiếm đoạt thông tin trái phép,... Tuy nhiên, về chế tài, Luật chỉ quy định chung rằng người vi phạm luật này “tùy theo tính chất, mức độ mà bị xử lý kỷ luật, xử phạt hành chính hoặc truy cứu hình sự”. Các hướng dẫn thi hành Luật An ninh mạng (*nhiều Nghị định 53/2022/NĐ-CP*) chủ yếu tập trung vào biện pháp kỹ thuật (*nhiều lưu trú dữ liệu trong nước, xác thực người dùng*), chưa có quy định chi tiết về mức phạt hành chính cho từng hành vi vi phạm an ninh mạng (*Đã có dự thảo từ 2024, nhưng chưa được thông qua*). Tương tự, Luật An toàn thông tin mạng 2015 quy định bảo vệ thông tin cá nhân trên mạng và an toàn hệ thống thông tin, nhưng việc xử phạt các vi phạm của luật này được giao cho Chính phủ quy định trong nghị định xử phạt lĩnh vực an toàn thông tin mạng. Hiện nay, chế tài với vi phạm an toàn thông tin mạng và thông tin cá nhân trên mạng được tích hợp chủ yếu trong Nghị định 15/2020/NĐ-CP, do Bộ Thông tin và Truyền thông ban hành trước đó.

Nghị định 15/2020/NĐ-CP (*sửa đổi, bổ sung bởi Nghị định 14/2022/NĐ-CP và Nghị định 211/2025/NĐ-CP*): Đây là nghị định quan trọng quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tàn số vô tuyến điện, công nghệ thông tin, an toàn thông tin mạng và giao dịch điện tử. Nghị định 15/2020/NĐ-CP đã dành một Mục riêng (*Mục 3 Chương III*) quy định về xử phạt hành vi vi phạm liên quan đến thông tin cá nhân trên môi trường mạng. Cụ thể:

- Thu thập, sử dụng thông tin cá nhân trái phép: Phạt tiền từ 10 - 20 triệu đồng với hành vi thu thập thông tin cá nhân mà không được sự đồng ý của chủ thẻ hoặc tiếp tục cung cấp cho bên thứ ba khi chủ thẻ đã yêu cầu dừng. Phạt 40 - 60 triệu đồng với hành vi sử dụng thông tin cá nhân sai mục đích, hoặc chia sẻ, phát tán, kinh doanh thông tin cá nhân của người khác trái phép (*bao gồm mua bán dữ liệu cá nhân*). Đây là mức phạt đã được tăng lên theo Nghị định 14/2022/NĐ-CP (*trước đó chỉ 20-30 triệu*) nhằm răn đe mạnh hơn đối với việc mua bán, sử dụng dữ liệu cá nhân trái phép.



- Vi phạm quy định về cập nhật, chỉnh sửa, hủy bỏ dữ liệu cá nhân: Phạt từ 10 - 20 triệu nếu không thông báo cho chủ thẻ dữ liệu khi hủy bỏ dữ liệu hoặc không có biện pháp bảo vệ thích hợp do lỗi kỹ thuật. Phạt từ 20 - 30 triệu nếu không cho phép chủ thẻ dữ liệu thực hiện quyền truy cập, chỉnh sửa, xóa dữ liệu của họ hoặc không xóa dữ liệu khi đã hết mục đích. Thậm chí phạt 30 - 50 triệu nếu không áp dụng biện pháp quản lý/kỹ thuật bảo vệ dữ liệu cá nhân theo quy định.

- Vi phạm quy định về bảo đảm an toàn thông tin cá nhân trên mạng: Phạt từ 10 - 20 triệu đồng nếu không tuân thủ đầy đủ tiêu chuẩn kỹ thuật về an toàn thông tin; phạt 20 - 30 triệu nếu vi phạm nghiêm trọng hơn tiêu chuẩn kỹ thuật; và lên đến 50 - 70 triệu đồng nếu không kịp thời áp dụng biện pháp khắc phục khi xảy ra sự cố mất an toàn thông tin mạng. Các mức phạt này hướng đến việc buộc tổ chức, doanh nghiệp phải đảm bảo biện pháp bảo mật, an ninh kỹ thuật khi xử lý dữ liệu người dùng.

Có thể thấy Nghị định 15/2020/NĐ-CP (*sửa đổi* 2022) đã bước đầu quy định khá cụ thể các hành vi xâm phạm dữ liệu cá nhân trên không gian mạng và mức xử phạt tương ứng, với mức phạt cao nhất đến 60 triệu đồng cho một số vi phạm nghiêm trọng (*ví dụ thu thập, phát tán, kinh doanh dữ liệu người khác trái phép*). Ngoài phạt tiền, nghị định này còn cho phép áp dụng biện pháp khắc phục hậu quả như buộc hủy bỏ thông tin cá nhân đã thu thập trái phép. Tuy nhiên, phạm vi của Nghị định 15/2020/NĐ-CP chỉ giới hạn trong lĩnh vực do Bộ Thông tin và truyền thông (*cũ*) quản lý (*bưu chính, viễn thông, CNTT, an toàn mạng...*). Các vi phạm ngoài phạm vi này (*chẳng hạn mua bán dữ liệu khách hàng trong lĩnh vực ngân hàng, y tế, giáo dục...*) thì khó áp dụng Nghị định 15, mà phải tìm căn cứ trong các nghị định xử phạt lĩnh vực khác (*nhiều thương mại, bảo vệ người tiêu dùng, y tế...*). Thực tế, nhiều hành vi mua bán dữ liệu cá nhân đã diễn ra công khai nhưng chưa bị xử lý do thiếu quy định pháp luật điều chỉnh thống nhất. Các doanh nghiệp ở nhiều lĩnh vực tự ý thu thập, phân tích dữ liệu khách hàng để kinh doanh, chuyển dữ liệu cho bên thứ ba mà không có chế tài xử phạt rõ ràng nếu vi phạm.



Trước tình trạng lộ lọt và mua bán dữ liệu cá nhân ngày càng nghiêm trọng, Chính phủ 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 lần đầu tiên quy định một cách có hệ thống về khái niệm dữ liệu cá nhân cơ bản, nhạy cảm; quyền và nghĩa vụ của chủ thể dữ liệu; điều kiện xử lý dữ liệu cá nhân; chuyển dữ liệu ra nước ngoài; trách nhiệm của các bên liên quan trong bảo vệ dữ liệu cá nhân. Tuy nhiên, về xử lý vi phạm, Nghị định 13/2023/NĐ-CP cũng chỉ nêu nguyên tắc chung: cơ quan, tổ chức, cá nhân vi phạm về bảo vệ dữ liệu cá nhân tùy mức độ có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc truy cứu hình sự. Nghị định này không quy định trực tiếp mức phạt tiền cụ thể cho từng hành vi vi phạm, mà vẫn phải áp dụng theo các nghị định xử phạt hiện hành tương ứng (*Nghị định ND 15/2020/NĐ-CP, Nghị định 98/2020/NĐ-CP về thương mại...*). Do đó, trong giai đoạn 2023-2025, việc xử phạt các vi phạm về dữ liệu cá nhân vẫn dựa trên khung chế tài cũ (*mức phạt tối đa 60-70 triệu đồng cho vi phạm hành chính*).

Bước tiến quan trọng nhất là Luật Bảo vệ Dữ liệu cá nhân 2025 (*Luật số 91/2025/QH15*) được Quốc hội thông qua ngày 26/6/2025, lần đầu tiên đưa vấn đề bảo vệ dữ liệu cá nhân lên tầm luật. Luật Bảo vệ Dữ liệu cá nhân 2025 (*có hiệu lực từ 1/1/2026*) mở rộng và chi tiết hóa các quy định của Nghị định 13, đồng thời đưa ra các chế tài mạnh mẽ hơn. Đáng chú ý, Luật đã xác định mức phạt tiền tối đa rất cao cho vi phạm trong lĩnh vực dữ liệu cá nhân, cụ thể: hành vi mua bán dữ liệu cá nhân bị cấm tuyệt đối và có thể bị phạt hành chính tối đa 10 lần khoản thu bất hợp pháp do hành vi đó mang lại. Trường hợp không xác định được khoản thu, tổ chức vi phạm có thể bị phạt đến 3 tỷ đồng, cá nhân đến 1,5 tỷ đồng. Đối với hành vi chuyên dữ liệu cá nhân ra nước ngoài trái phép, mức phạt tối đa lên tới 5% tổng doanh thu của năm liền kề trước đó của tổ chức vi phạm (*nếu không xác định được doanh thu thì có thể phạt đến 3 tỷ đồng*). Ngoài ra, các hành vi vi phạm khác về bảo vệ dữ liệu cá nhân (*như xử lý dữ liệu không có căn cứ pháp lý, vi phạm quyền của chủ thể dữ liệu...*) có mức phạt tối đa chung là 3 tỷ đồng đối với tổ chức. Đây là các mức chế tài cao đột biến so với khung phạt hiện hành (*chỉ vài chục triệu*



đồng), cho thấy quyết tâm tăng tính răn đe của nhà làm luật Việt Nam. Luật cũng giao Chính phủ quy định phương pháp tính khoản thu để làm căn cứ áp dụng mức phạt 10 lần nói trên. Tuy nhiên, cần lưu ý rằng Luật Bảo vệ dữ liệu cá nhân 2025 chưa có hiệu lực ngay (*phải đến 2026*) và để áp dụng được các mức phạt này trên thực tế, cần ban hành nghị định xử phạt mới làm cơ sở pháp lý cụ thể.

Khác với Luật Bảo vệ dữ liệu cá nhân tập trung vào dữ liệu cá nhân, Luật Dữ liệu 2024 điều chỉnh rộng hơn về dữ liệu số nói chung, bao gồm dữ liệu do cơ quan, tổ chức, cá nhân tạo lập, thu thập; quản trị, khai thác dữ liệu; phát triển Chính phủ số, kinh tế số. Luật Dữ liệu đề ra các khái niệm như dữ liệu dùng chung, dữ liệu mở, dữ liệu quan trọng, dữ liệu cốt lõi và thiết lập cơ chế Trung tâm dữ liệu quốc gia, Cơ sở dữ liệu tổng hợp quốc gia nhằm kết nối, chia sẻ dữ liệu giữa các cơ quan. Về nguyên tắc, Luật Dữ liệu yêu cầu bảo đảm an ninh, an toàn dữ liệu trong suốt vòng đời dữ liệu. Tuy nhiên, tương tự nhiều luật khác, Luật Dữ liệu 2024 không quy định chi tiết về chế tài xử phạt khi vi phạm các nghĩa vụ của luật này, mà giao Chính phủ hướng dẫn. Nghị định 165/2025/NĐ-CP (*ngày 30/6/2025*) đã được ban hành để quy định chi tiết thi hành Luật Dữ liệu. Nghị định này chủ yếu hướng dẫn về phân loại dữ liệu quan trọng, dữ liệu cốt lõi, việc xây dựng, vận hành Trung tâm dữ liệu quốc gia, chia sẻ dữ liệu...; không tập trung vào chế tài xử phạt vi phạm. Thực tế, Luật Dữ liệu 2024 có phạm vi rất rộng, bao gồm quản lý dữ liệu công của Nhà nước và dữ liệu số của mọi chủ thể, nhưng hệ thống chế tài cho các hành vi vi phạm luật này hiện chưa rõ ràng. Các hành vi như không tuân thủ quy định về chia sẻ dữ liệu, vi phạm quy định về quản trị dữ liệu hoặc làm lộ dữ liệu quan trọng... sẽ cần được bổ sung vào các văn bản xử phạt vi phạm hành chính sắp tới thì mới có cơ sở chế tài khi luật có hiệu lực.

Tóm lại, hệ thống pháp luật hiện hành về xử lý vi phạm hành chính trong lĩnh vực dữ liệu ở Việt Nam bao gồm nhiều lớp quy phạm: Luật Xử lý vi phạm hành chính làm nền tảng chung; các luật chuyên ngành (*An ninh mạng, An toàn thông tin mạng, Bảo vệ dữ liệu cá nhân...*) đưa ra nguyên tắc và nghĩa vụ; các nghị định của Chính phủ (*nhiều Nghị định 15/2020/NĐ-CP, Nghị định*



98/2020/NĐ-CP, Nghị định 13/2023/NĐ-CP...) quy định hành vi vi phạm cụ thể và mức xử phạt. Dù đã có những quy định bước đầu về xử phạt hành vi xâm phạm dữ liệu cá nhân, pháp luật hiện hành vẫn còn phân tán, chưa theo kịp thực tiễn. Chế tài hành chính đối với vi phạm trong lĩnh vực dữ liệu phần lớn dừng ở mức cảnh cáo, phạt tiền với hạn mức không cao; chưa có quy định riêng cho nhiều hành vi mới phát sinh ngoài phạm vi. Điều này dẫn đến hiệu lực, hiệu quả răn đe của pháp luật chưa như mong muốn.

3.2.2. Đánh giá mức độ đầy đủ, hiệu lực, hiệu quả của các quy định hiện có

Nhìn chung, pháp luật hiện hành về xử phạt vi phạm trong lĩnh vực dữ liệu chưa đầy đủ và bao quát hết các dạng hành vi vi phạm. Như đã đề cập, các nghị định xử phạt hiện nay chủ yếu điều chỉnh các vi phạm trong lĩnh vực viễn thông, công nghệ thông tin và giao dịch điện tử. Trong khi đó, nhiều hành vi xâm phạm dữ liệu xảy ra ngoài các lĩnh vực này chưa có chế tài rõ ràng. Ví dụ: hành vi mua bán dữ liệu khách hàng ngân hàng, bảo hiểm, giáo dục... trước năm 2023 rất khó xử phạt vì không nằm trong danh mục vi phạm của Nghị định 15/2020/NĐ-CP. Mặc dù Luật Bảo vệ quyền lợi người tiêu dùng 2010 có quy định cấm tiết lộ thông tin của người tiêu dùng nếu không được đồng ý, nhưng Nghị định 98/2020/NĐ-CP (*xử phạt thương mại, bảo vệ người tiêu dùng*) chỉ phạt việc vi phạm về bảo mật thông tin khách hàng (*Không triển khai các biện pháp đảm bảo an toàn, bảo mật cho giao dịch thanh toán của khách hàng*) ở mức tối đa 30 triệu đồng và ít được áp dụng trên thực tế. Theo một nghiên cứu, nhiều vụ rò rỉ, mua bán dữ liệu cá nhân quy mô lớn đã diễn ra mà “nhiều hành vi chưa được xử lý vì thiếu quy định pháp luật” để chế tài. Các doanh nghiệp tự thu thập và phân tích dữ liệu khách hàng, rồi trao đổi, mua bán các “gói dữ liệu” chứa thông tin cá nhân (*danh sách khách hàng điện lực, viễn thông, danh sách phụ huynh học sinh, thông tin khách VIP các ngành...*) một cách công khai trên mạng, nhưng pháp luật chưa theo kịp để xử phạt kịp thời. Điều này cho thấy khoảng trống pháp lý về xử lý vi phạm dữ liệu trước đây là khá lớn.



Đối với dữ liệu không thuộc loại “cá nhân”, khoảng trống pháp lý lại càng rõ. Luật An ninh mạng 2018 yêu cầu bảo vệ dữ liệu quan trọng liên quan an ninh quốc gia, nhưng chưa có nghị định xử phạt vi phạm hành chính dành riêng cho hành vi vi phạm như không tuân thủ yêu cầu lưu trữ dữ liệu tại Việt Nam, không xóa thông tin vi phạm theo yêu cầu cơ quan chức năng... Tương tự, Luật Dữ liệu 2024 đặt ra nhiều nghĩa vụ (*phân loại dữ liệu, chia sẻ dữ liệu dùng chung, bảo vệ dữ liệu cốt lõi*), nhưng hiện chưa có chế tài nếu chủ thẻ (*cơ quan hoặc doanh nghiệp*) không thực hiện những nghĩa vụ này. Ví dụ: nếu một cơ quan nhà nước không kết nối, chia sẻ dữ liệu với Trung tâm dữ liệu quốc gia theo luật định, hoặc một tổ chức không bảo đảm an toàn đối với dữ liệu quan trọng do mình quản lý dẫn đến lộ泄, thì hiện nay sẽ rất khó xác định xử phạt theo nghị định nào (*có thể chỉ bị phê bình, kỷ luật nội bộ*). Pháp luật hiện có chủ yếu tập trung vào dữ liệu cá nhân, còn việc bảo vệ các loại dữ liệu số khác (*dữ liệu doanh nghiệp, dữ liệu phi cá nhân*) gần như bỏ ngỏ trong chế tài hành chính.

3.2.3. *Tính hiệu lực và hiệu quả của các quy định hiện hành*

Ở những khía cạnh đã có quy định, việc thực thi chế tài còn nhiều hạn chế:

- **Trước hết**, mức xử phạt tiền hiện hành còn thấp, chưa đủ sức răn đe đối với nhiều hành vi vi phạm dữ liệu. Mức phạt cao nhất 60-70 triệu đồng trong Nghị định 15/2020/NĐ-CP (*tương đương khoảng 2.500 - 3.000 USD*) bị đánh giá là quá nhẹ so với lợi ích thu được từ việc mua bán, khai thác dữ liệu cá nhân. Nghiên cứu so sánh cho thấy Liên minh Châu Âu có thể phạt tới 20 triệu Euro (*khoảng 500 tỷ VND*) cho vi phạm dữ liệu cá nhân (*theo GDPR*), trong khi Việt Nam chỉ phạt vài chục triệu đồng, con số này không đáng kể đối với các doanh nghiệp lớn. Chính vì mức phạt thấp, nhiều tổ chức xem việc vi phạm (*bán thông tin khách hàng, gửi spam quảng cáo*) như “chi phí kinh doanh” chấp nhận được. Việc tăng mức phạt lên 40-60 triệu tại Nghị định 14/2022/NĐ-CP cũng chỉ nâng cao phần nào, chưa thực sự tạo cú huých lớn về răn đe. Trên thực tế, tình trạng rao bán dữ liệu cá nhân tràn lan trên mạng vẫn diễn ra, gây bức xúc trong xã hội.



DATA KHÁCH HÀNG UY TÍN, CHẤT LƯỢNG

Công khai · 45K thành viên · 8 bài viết/ngày

1 người bạn là thành viên

[Tham gia](#)

DATA KHÁCH HÀNG

Công khai · 41K thành viên · 10+ bài viết/ngày

[Tham gia](#)

GenZ làm Data (Data Analysts / Data Scientist / Data Engineer

)

Công khai · 51K thành viên · 10 bài viết/ngày

[Tham gia](#)

Xóm Data - Cùng học Data Analyst / Data Engineer / Data Scientist

Công khai · 31K thành viên · 6 bài viết/ngày

1 người bạn là thành viên

[Tham gia](#)

Hình ảnh: "Chợ" dữ liệu tràn công khai trên mạng xã hội. Ảnh: Tác giả

- Thứ hai, số vụ xử phạt vi phạm dữ liệu được công khai còn rất ít. Trong 2 năm 2019-2022, Bộ Công an đã phát hiện hàng trăm tổ chức, cá nhân tham gia bán dữ liệu cá nhân và triệt phá một số đường dây lớn (*chiếm đoạt gần 1.300 GB dữ liệu cá nhân đủ loại*), nhưng các trường hợp này hầu hết được xử lý hình sự hoặc ngăn chặn hành vi. Một phần nguyên nhân là những kẻ buôn dữ liệu thường hoạt động bí mật, ẩn danh; khi bị phát hiện quy mô lớn thì có thể bị truy tố tội hình sự (ví dụ: “*đưa hoặc sử dụng trái phép thông tin trên mạng máy tính*” theo Điều 288 Bộ luật Hình sự). Trong khi đó, các vi phạm hành chính nhỏ lẻ (ví dụ công ty A lộ dữ liệu 10.000 khách hàng do lỗi bảo mật) thường khó phát hiện hoặc khó chứng minh thủ phạm rõ ràng. Có thể nói, việc xử lý hành vi mua bán thông tin cá nhân gấp khăn do nhiều nguyên nhân, nhất là khó truy ra đầu mối người làm lộ, bán dữ liệu trong chuỗi vi phạm. Việc thiếu cơ chế giám sát và chứng cứ kỹ thuật (*nhiều nhật ký hệ thống, truy vết*) khiến nhiều vụ lộ lọt dữ liệu rơi vào im lặng, không xử phạt được ai.



Hình ảnh: 03 đối tượng bị Công an TP Huế bắt về hành vi đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. Ảnh: Báo Ấp Bắc



Hình ảnh: Bị can Lại Thị Phương cùng chồng bị cáo buộc thu thập, mua bán trái phép gần 1.300 GB dữ liệu cá nhân. Ảnh: Báo Thanh niên

- **Thứ ba**, sự chồng chéo, phân tán trong quản lý cũng làm giảm hiệu lực của chế tài. Trước năm 2023, Bộ Thông tin và Truyền thông chịu trách nhiệm quản lý an toàn thông tin cá nhân trên mạng (theo Luật An toàn thông tin mạng



2015), còn Bộ Công an quản lý an ninh mạng (*Luật An ninh mạng 2018*). Vi phạm dữ liệu cá nhân trên mạng xã hội, website thì Thanh tra Bộ TTTT có thể xử phạt theo Nghị định 15/2020/NĐ-CP. Nhưng nếu vi phạm xảy ra tại một doanh nghiệp không thuộc lĩnh vực công nghệ thông tin (*ví dụ một công ty bán lẻ làm lộ thông tin khách hàng*), Thanh tra Thông tin truyền thông khó can thiệp, còn quản lý ngành khác lại không có quy định chế tài tương tự. Sự thiếu phối hợp này dẫn đến nhiều vụ việc không ai xử lý. Từ 2023, Nghị định 13/2023/NĐ-CP giao rõ Bộ Công an là cơ quan chủ trì bảo vệ dữ liệu cá nhân, nhưng cơ chế thực thi cụ thể (*nhân sự, đơn vị chuyên trách, quy trình tiếp nhận khiếu nại*) vẫn đang trong giai đoạn hình thành. Trong khi đó, cơ quan giám sát độc lập về bảo vệ dữ liệu (*như mô hình Ủy ban dữ liệu cá nhân ở các nước*) chưa có; người dân muốn phản ánh vi phạm phải gửi tới công an (*Cục An ninh mạng và PCTP CNC*) theo nghị định.

Tóm lại, pháp luật hiện hành về xử lý vi phạm dữ liệu chưa đáp ứng đầy đủ yêu cầu thực tiễn. Các quy định hiện có chưa bao trùm hết các hành vi vi phạm, mức phạt lại nhẹ, khiến tính răn đe hạn chế. Việc thực thi cũng gặp khó khăn do hạn chế về kỹ thuật và phối hợp. Chính vì vậy, Quốc hội và Chính phủ đã nhận thấy cần thiết phải hoàn thiện khuôn khổ pháp luật, mà minh chứng là việc ban hành Luật Bảo vệ dữ liệu cá nhân 2025 với chế tài nặng hơn. Tuy nhiên, vẫn còn những khoảng trống pháp lý nhất định, đặc biệt khi Luật Dữ liệu 2024 bắt đầu có hiệu lực.

3.2.4. Khoảng trống pháp lý khi Luật Dữ liệu 2024 có hiệu lực

Luật Dữ liệu 2024 tạo hành lang pháp lý cho quản trị dữ liệu trong bối cảnh chuyển đổi số, đặt ra nhiều yêu cầu pháp lý mới đối với cơ quan, tổ chức về thu thập, chia sẻ, quản trị và bảo vệ dữ liệu số. Khi luật này có hiệu lực (từ 7/2025), một số quy định hiện hành có thể bộc lộ khoảng trống hoặc chưa kịp thích ứng:

- **Thứ nhất**, Luật Dữ liệu quy định về phân loại dữ liệu quan trọng, dữ liệu cốt lõi (*các dữ liệu có ảnh hưởng lớn đến quốc phòng, an ninh, kinh tế, trật tự xã hội...*). Tuy nhiên, hậu quả pháp lý khi vi phạm các quy định này chưa rõ. Ví dụ: nếu một doanh nghiệp sở hữu dữ liệu quan trọng nhưng không tuân thủ biện pháp



bảo vệ đặc thù, hoặc một cá nhân sử dụng trái phép dữ liệu cốt lõi gây nguy hại (*dù không phải bí mật nhà nước*) thì hiện không có điều khoản xử phạt hành chính cụ thể cho hành vi này. Có thể tình huống nghiêm trọng sẽ bị truy cứu hình sự (*nếu cấu thành tội phạm như “cố ý làm lộ bí mật nhà nước” hoặc “xâm nhập trái phép...*”), nhưng nguồng hình sự rất cao, còn chế tài hành chính lại thiếu nếu vi phạm chưa đến mức tội phạm; đặc biệt trong bối cảnh thực hiện tinh thần Nghị quyết 66-NQ/TW không hình sự hóa quan hệ kinh tế.

- **Thứ hai**, việc Luật Dữ liệu yêu cầu các bộ, ngành, địa phương kết nối với Trung tâm dữ liệu quốc gia, chia sẻ dữ liệu dùng chung, không được cát cứ thông tin. Tuy vậy, nếu một cơ quan chậm trễ hoặc từ chối chia sẻ dữ liệu theo yêu cầu của Trung tâm dữ liệu quốc gia hay của Chính phủ, thì chưa có quy định chế tài cụ thể. Trong bộ máy nhà nước, việc xử lý vi phạm của cơ quan thường thông qua biện pháp kỷ luật hành chính đối với cá nhân có trách nhiệm, chứ khó phạt tiền cơ quan đó. Luật Xử lý vi phạm hành chính cho phép xử phạt cơ quan nhà nước nếu vi phạm ngoài nhiệm vụ được giao, nhưng việc này ít xảy ra và cũng chưa có khung phạt cho hành vi như không kết nối chia sẻ dữ liệu.

- **Thứ ba**, Luật Dữ liệu khuyến khích cung cấp dữ liệu mở (*open data*) cho công cộng. Song nếu cơ quan hay doanh nghiệp thuộc diện phải cung cấp dữ liệu mở mà không thực hiện (*hoặc cung cấp dữ liệu không chính xác, không cập nhật*), pháp luật chưa quy định xử phạt. Tính cưỡng chế của nghĩa vụ dữ liệu mở hiện thấp, vì thiếu cả chế tài lẫn cơ chế kiểm tra.

- **Thứ tư**, Luật Dữ liệu đề cập khái niệm mới như sàn dữ liệu, dịch vụ trung gian dữ liệu (*kết nối bên cung và bên cầu dữ liệu*). Đây là lĩnh vực hoàn toàn mới, chưa có tiền lệ quản lý. Nếu các tổ chức trung gian dữ liệu vi phạm (*ví dụ mua bán dữ liệu không phép, làm lộ dữ liệu trao đổi trên sàn...*), hiện chưa có quy định xử phạt riêng. Hành vi của họ có thể bị xem xét dưới góc độ vi phạm bảo vệ dữ liệu cá nhân (*nếu liên quan*), hoặc vi phạm điều kiện kinh doanh (*trung gian dữ liệu thuộc ngành nghề có điều kiện*), nhưng khung pháp lý cụ thể còn rất thiếu.



- **Thứ năm**, Luật Dữ liệu 2024 có điều khoản về mối quan hệ với luật khác, theo đó trường hợp luật khác có quy định khác thì phải nêu rõ áp dụng luật nào. Dữ liệu cá nhân về nguyên tắc sẽ do Luật Bảo vệ dữ liệu cá nhân 2025 điều chỉnh chuyên sâu. Tuy nhiên, khi cả hai luật đều có hiệu lực (*từ 2025 và 2026*), có thể nảy sinh câu hỏi: một hành vi vi phạm liên quan dữ liệu cá nhân nhưng đồng thời vi phạm quy định của Luật Dữ liệu (*ví dụ: Doanh nghiệp viễn thông lộ thông tin người sử dụng*) thì xử phạt theo luật nào? Nếu xử phạt theo Luật Bảo vệ dữ liệu cá nhân (*sẽ có nghị định xử phạt riêng*), còn vi phạm Luật Dữ liệu lại chưa có chế tài, dễ dẫn đến thiếu thống nhất. Cần có hướng dẫn phân định rõ để tránh bối rối vi phạm hoặc chồng chéo chế tài.

- **Thứ sáu**, thiếu quy định về trách nhiệm bồi thường và khắc phục trong môi trường dữ liệu mới. Luật Dữ liệu tập trung vào thúc đẩy khai thác dữ liệu, chưa quy định rõ về trách nhiệm khi xảy ra sự cố dữ liệu không phải dữ liệu cá nhân (*ví dụ sự cố mất mát dữ liệu quan trọng của quốc gia do lỗi quản trị*). Pháp luật hiện thời cũng chưa có quy định riêng về thông báo và ứng phó sự cố rò rỉ dữ liệu phi cá nhân. Ví dụ: nếu một doanh nghiệp quản lý cơ sở dữ liệu lớn (*nhiều dữ liệu bẩn đồ, dữ liệu giao thông*) bị tấn công làm gián đoạn, thì họ có nghĩa vụ thông báo cho ai và nếu chậm thông báo hoặc che giấu sự cố thì có bị phạt không?

Những khoảng trống trên cho thấy hệ thống pháp luật cần được cập nhật, bổ sung đồng bộ khi Luật Dữ liệu 2024 và Luật Bảo vệ dữ liệu cá nhân 2025 đi vào hiệu lực. Nếu không, sẽ có hiện tượng “luật có mà phạt không” tức là luật đặt ra nghĩa vụ nhưng không có chế tài đảm bảo thực thi. Để khắc phục các hạn chế và lấp đầy khoảng trống nêu trên, việc xây dựng các giải pháp hoàn thiện pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu là rất cấp thiết.

3.2.5. Giải pháp hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu

Dựa trên phân tích thực trạng và khoảng trống pháp lý, có thể đề xuất một số giải pháp nhằm xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu như sau:



3.2.5.1. Ban hành nghị định chuyên ngành về xử phạt vi phạm trong lĩnh vực dữ liệu

Cần sớm xây dựng và ban hành một Nghị định chuyên biệt quy định xử phạt vi phạm hành chính trong lĩnh vực dữ liệu, nhất là dữ liệu cá nhân, để hệ thống hóa và bổ sung các chế tài còn thiếu. Hiện nay, các quy định xử phạt liên quan dữ liệu nằm rải rác ở nhiều nghị định khác nhau (*Nghị định 15/2020/NĐ-CP, Nghị định 98/2020/NĐ-CP, Nghị định 91/2009/NĐ-CP...*). Một nghị định chuyên ngành sẽ giúp tập trung đầy đủ nhất các hành vi vi phạm về dữ liệu và thống nhất mức xử phạt. Đề xuất này cũng đã được các chuyên gia luật và cơ quan quản lý đặt ra, cần xây dựng ngay một hệ thống quy định riêng về hành vi vi phạm và chế tài xử phạt trong lĩnh vực bảo vệ dữ liệu cá nhân để có căn cứ pháp lý đầy đủ, toàn diện nhất.

Nghị định chuyên ngành này nên bao quát cả vi phạm về dữ liệu cá nhân và vi phạm về dữ liệu số nói chung (*dữ liệu quan trọng, dữ liệu dùng chung,...*). Có thể cấu trúc nghị định thành các chương mục tương ứng: một chương về vi phạm quy định bảo vệ dữ liệu cá nhân; một chương về vi phạm các quy định của Luật Dữ liệu 2024 (*về quản trị, chia sẻ, sử dụng dữ liệu số...*). Như vậy, nghị định sẽ là cầu nối triển khai Luật Bảo vệ dữ liệu cá nhân 2025 và Luật Dữ liệu 2024 trên phương diện chế tài hành chính.

* Nội dung cụ thể cần quy định:

- **Thứ nhất**, nhóm hành vi xâm phạm dữ liệu cá nhân: Các hành vi đã có tại Nghị định 15/2020/NĐ-CP (*thu thập trái phép, sử dụng sai mục đích, tiết lộ, mua bán thông tin cá nhân...*) cần được kê thửa và mở rộng. Nghị định mới sẽ cập nhật mức phạt theo Luật Bảo vệ dữ liệu cá nhân 2025, tức là tăng trần phạt lên đến 3 tỷ đồng hoặc tính theo phần trăm doanh thu đối với vi phạm nghiêm trọng. Ví dụ: hành vi mua bán dữ liệu cá nhân trái phép trước đây phạt 60 triệu đồng, thì nay có thể quy định mức phạt tối đa 3 tỷ hoặc 10 lần lợi nhuận thu được (*tùy số nào lớn hơn*). Hành vi chuyển dữ liệu cá nhân ra nước ngoài không phép trước đây chưa có chế tài rõ, nay có thể phạt đến 5% doanh thu năm trước của tổ chức vi



phạm. Việc không thực hiện yêu cầu của chủ thẻ dữ liệu (*nhu không xóa dữ liệu khi có yêu cầu hợp lệ*) cũng nên được bổ sung rõ với mức phạt tương xứng (*có thể 50-100 triệu đồng đối với tổ chức*).

- **Thứ hai**, nhóm hành vi vi phạm quy định của Luật Dữ liệu 2024: Bổ sung các hành vi như không phân loại, đánh giá dữ liệu quan trọng/cốt lõi theo quy định; không thực hiện biện pháp bảo vệ đặc thù cho dữ liệu quan trọng, dữ liệu cốt lõi; từ chối chia sẻ dữ liệu dùng chung không có lý do chính đáng; vi phạm quy định về vận hành Trung tâm dữ liệu quốc gia, cơ sở dữ liệu quốc gia (*ví dụ: không tuân thủ kiến trúc, kết nối; làm sai lệch dữ liệu*)... Những hành vi này trước nay chưa có trong bất kỳ nghị định xử phạt nào, do đó cần được quy định mới. Mức phạt đề xuất có thể phân theo tính chất hậu quả, vi phạm gây ảnh hưởng nhỏ phạt vài chục triệu, vi phạm cản trở nghiêm trọng chuyển đổi số quốc gia có thể phạt đến hàng trăm triệu.

- **Thứ tư**, nhóm hành vi vi phạm quy định an ninh, an toàn dữ liệu: Quy định các chế tài nếu tổ chức không tuân thủ yêu cầu về bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng (*theo Luật An ninh mạng*), chẳng hạn không thực hiện kiểm tra đánh giá an ninh mạng định kỳ, không lưu trữ dữ liệu người dùng Việt Nam theo yêu cầu. Hiện các hành vi này chưa có chế tài hành chính cụ thể; nghị định mới có thể bổ sung để phối hợp đồng bộ với Luật An ninh mạng. Điều này vừa lập khoảng trống, vừa tạo sức ép cho các nền tảng công nghệ lớn tuân thủ luật (*tránh tình trạng “có luật nhưng khó phạt” với các mạng xã hội xuyên biên giới*).

Nghị định mới cũng cần xác định rõ cơ quan có thẩm quyền lập biên bản và xử phạt. Đối với vi phạm dữ liệu cá nhân, Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao đóng vai trò chủ trì theo Luật Bảo vệ dữ liệu cá nhân. Bên cạnh đó, do dữ liệu liên quan đa ngành, có thể phân cấp: Thanh tra chính phủ cũng có quyền xử phạt vi phạm về dữ liệu trong phạm vi quản lý của mình, phối hợp với Bộ Công an. Ví dụ: nếu một bệnh viện vi phạm bảo mật dữ liệu bệnh án, Thanh tra chính phủ (*phụ trách lĩnh vực Y tế*) có thể xử phạt theo



nghị định này, đồng thời báo cáo Bộ Công an quản lý chung. Quy định phân quyền rõ ràng sẽ tránh chồng chéo và bao quát hết các lĩnh vực.

Việc ban hành nghị định chuyên ngành không chỉ để nội luật hóa Luật Bảo vệ dữ liệu cá nhân 2025 mà còn thể hiện cam kết của Việt Nam trong bảo vệ dữ liệu tương tự quốc tế. Nhiều nước đã có văn bản tập trung về xử phạt vi phạm dữ liệu cá nhân. Ví dụ, Singapore có Đạo luật PDPA kèm các hướng dẫn phạt tiền, Liên minh Châu Âu có GDPR với khung phạt rõ ràng theo doanh thu. Việc Việt Nam quy định phạt tới 5% doanh thu hoặc 3 tỷ đồng với vi phạm dữ liệu cá nhân là bước tiến lớn, cần được cụ thể hóa trong nghị định để có hiệu lực thực thi. Nghị định này nên được ban hành trước khi Luật Bảo vệ dữ liệu cá nhân có hiệu lực (1/1/2026), lý tưởng là trong năm 2025, để các cơ quan kịp chuẩn bị áp dụng.

3.2.5.2. Xây dựng bảng phân loại hành vi và mức phạt chi tiết, minh bạch

Để hỗ trợ việc áp dụng pháp luật thuận lợi, cần xây dựng bảng liệt kê các hành vi vi phạm cụ thể và khung mức phạt tương ứng, kèm căn cứ pháp lý, làm tài liệu hướng dẫn cho cơ quan thực thi và đối tượng tuân thủ. Việc hệ thống hóa thành bảng sẽ giúp minh bạch hóa chế tài, người dân và doanh nghiệp dễ hiểu rõ hành vi nào bị phạt bao nhiêu, tránh trường hợp quy định rải rác khó tra cứu. Ví dụ:

Hành vi vi phạm (lĩnh vực dữ liệu)	Khung xử phạt hành chính hiện hành/proposed (phạt tiền)	Căn cứ pháp lý hiện hành (nếu có)
Thu thập dữ liệu cá nhân của người khác không có sự đồng ý đúng phạm vi, mục đích.	10 - 20 triệu đồng đối với mỗi hành vi vi phạm. (<i>Đề xuất giữ nguyên mức hiện hành đối với vi phạm lần đầu, cá nhân vi phạm</i>).	Điểm a, Khoản 1, Điều 84 Nghị định 15/2020/NĐ-CP sửa đổi 2022
Sử dụng dữ liệu cá nhân đã thu thập sai mục đích, vượt phạm vi đồng ý; hoặc tiếp tục sử dụng, cung cấp cho	40 - 60 triệu đồng (<i>mức phạt tối thiểu theo Nghị định 14/2022/NĐ-CP</i>) đối với hành vi vi phạm thông thường. Nếu vi phạm có quy	Điểm a, Khoản 2, Điều 84 Nghị định 15/2020/NĐ-CP; Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025.,



bên thứ ba khi chủ thẻ đã rút consent.	mô lớn hoặc nhằm trực lợi: đề xuất phạt 100 - 200 triệu đồng (<i>theo Luật mới</i>).	
Thu thập, phát tán, mua bán dữ liệu cá nhân trái phép (bao gồm dữ liệu cơ bản và nhạy cảm)	<i>Hiện hành:</i> 40 - 60 triệu đồng đối với tổ chức. <i>Đề xuất (theo Luật mới):</i> Phạt tối đa 10 lần khoản thu bất hợp pháp do hành vi vi phạm, hoặc đến 3 tỷ đồng nếu không xác định được khoản thu; cá nhân vi phạm tối đa 1,5 tỷ đồng.	Điểm c, Khoản 2, Điều 84 Nghị định 15/2020/NĐ-CP; Khoản 3, Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025.
Không thực hiện yêu cầu xóa dữ liệu cá nhân của chủ thẻ dữ liệu; không cho phép chủ thẻ truy cập, chỉnh sửa dữ liệu của họ theo quy định.	20 - 30 triệu đồng đối với vi phạm không dẫn đến hậu quả nghiêm trọng; có thể đến 50 triệu đồng nếu vi phạm nhiều hò sơ hoặc gây ảnh hưởng quyền lợi rộng.	Điểm a, b, Khoản 2, Điều 85 Nghị định 15/2020/NĐ-CP. (<i>Luật Bảo vệ dữ liệu cá nhân 2025 cũng đòi hỏi tôn trọng quyền chủ thẻ</i>).
Không áp dụng biện pháp kỹ thuật, quản lý để bảo vệ dữ liệu cá nhân (ví dụ: <i>không có hệ thống bảo mật, không mã hóa dữ liệu nhạy cảm</i>)	30 - 50 triệu đồng đối với mỗi hành vi vi phạm về bảo đảm an toàn dữ liệu. Nếu dẫn đến lộ lọt dữ liệu thực tế: áp dụng mức phạt cao nhất và buộc khắc phục hậu quả (<i>cài đặt bổ sung biện pháp bảo mật</i>).	Khoản 3, Điều 85; khoản 3,4, Điều 86 Nghị định 15/2020/NĐ-CP
Chuyển dữ liệu cá nhân ra nước ngoài không thông báo hoặc không được phép (<i>theo yêu cầu luật</i>)	<i>Hiện chưa có mức phạt cụ thể. Đề xuất:</i> Phạt đến 5% tổng doanh thu năm trước của tổ chức thực hiện hành vi; trường hợp không xác định được doanh thu thì phạt đến 3 tỷ đồng.	Khoản 4, Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025. (<i>Nghị định mới sẽ quy định chi tiết phương thức tính phạt</i>).



Không phân loại và thực hiện bảo vệ dữ liệu quan trọng/cốt lõi theo quy định (Luật Dữ liệu)	<i>Chưa có chế tài hiện hành. Đề xuất: Phạt 50 - 100 triệu đồng đối với tổ chức không thực hiện phân loại dữ liệu quan trọng; phạt 100 - 200 triệu nếu không áp dụng biện pháp bảo vệ dữ liệu quan trọng, dẫn đến nguy cơ mất an toàn.</i>	<i>(Sẽ quy định trong nghị định mới dưới Luật Dữ liệu 2024).</i>
Không chia sẻ dữ liệu thuộc diện “dữ liệu dùng chung” theo yêu cầu của cơ quan có thẩm quyền (theo Luật Dữ liệu)	<i>Chưa có chế tài. Đề xuất: Phạt 30 - 50 triệu đồng đối với mỗi lần vi phạm không cung cấp/chia sẻ dữ liệu dùng chung khi có yêu cầu hợp pháp, nếu gây cản trở kết nối dữ liệu quốc gia.</i>	<i>(Sẽ quy định trong nghị định mới dưới Luật Dữ liệu).</i>
Thiết lập, vận hành hệ thống thu thập dữ liệu cá nhân trái pháp luật (ví dụ: tạo phần mềm/website để lấy cắp dữ liệu người dùng)	<i>Chưa có chế tài hành chính rõ, có thể xử lý hình sự nếu nghiêm trọng. Đề xuất: Bổ sung chế tài phạt hành chính 100 - 200 triệu đồng đối với tổ chức thiết lập hệ thống thu thập DLCN trái phép (trường hợp chưa đến mức truy cứu hình sự). Tịch thu phương tiện vi phạm.</i>	<i>(Đề xuất mới; hành vi này có thể cấu thành tội phạm trong Bộ luật Hình sự nếu quy mô lớn, nhưng cần chế tài hành chính cho trường hợp dưới mức hình sự).</i>

Như bảng trên cho thấy, nhiều hành vi mới hoặc nghiêm trọng đòi hỏi mức phạt đề xuất cao hơn hẳn hiện nay, phù hợp với trừng phạt mà luật mới cho phép. Bảng phân loại chi tiết sẽ giúp cơ quan xử phạt dễ tra cứu và áp dụng thống nhất trên toàn quốc. Đồng thời, bảng công khai cũng giúp các doanh nghiệp, tổ chức tự đổi chiếu để tuân thủ, vì họ biết rõ vi phạm nào sẽ bị phạt bao nhiêu, tránh được



tâm lý cho rằng vi phạm dữ liệu “không ai phạt”. Minh bạch hóa chế tài theo hướng này sẽ góp phần nâng cao hiệu quả răn đe và phòng ngừa.

3.2.5.3. *Bổ sung cơ chế truy vết kỹ thuật: nhật ký dữ liệu, xác thực và mã hóa bắt buộc*

Một trong những khó khăn lớn hiện nay trong xử lý vi phạm dữ liệu là khó truy tìm nguồn gốc và thu thập bằng chứng. Nhiều vụ lộ lọt dữ liệu không xác định được chính xác ai đã truy cập, sao chép trái phép dữ liệu, do hệ thống không có nhật ký (*log*) đầy đủ hoặc không có cơ chế theo dõi. Vì vậy, pháp luật cần bổ sung quy định buộc các tổ chức, doanh nghiệp triển khai các biện pháp kỹ thuật hỗ trợ truy vết và bảo mật dữ liệu, cụ thể:

- **Thứ nhất**, yêu cầu lưu trữ nhật ký truy cập dữ liệu. Các hệ thống thông tin, cơ sở dữ liệu (*đặc biệt chứa dữ liệu cá nhân, dữ liệu quan trọng*) phải thiết lập nhật ký sự kiện ghi lại mọi hoạt động truy cập, chỉnh sửa, xóa, truyền xuất dữ liệu. Nhật ký phải lưu giữ trong thời gian tối thiểu (*ví dụ 1-2 năm*) để phục vụ điều tra khi cần. Nếu đơn vị nào không thiết lập hoặc không lưu giữ nhật ký sẽ bị coi là vi phạm hành chính về yêu cầu bảo đảm an toàn dữ liệu. Hiện Nghị định 15/2020/NĐ-CP đã có chế tài phạt 20 - 30 triệu đồng nếu không tuân thủ tiêu chuẩn kỹ thuật đảm bảo an toàn thông tin, quy định này có thể diễn giải bao gồm cả việc không có lưu trữ nhật ký. Tuy nhiên nên quy định cụ thể hơn trong nghị định mới: ví dụ: phạt đến 50 triệu đồng nếu không có hệ thống nhật ký theo dõi truy cập dữ liệu cá nhân. Điều này sẽ tạo căn cứ pháp lý rõ để xử phạt những đơn vị lơ là khâu giám sát.

- **Thứ hai**, quy định về xác thực và phân quyền. Bắt buộc các hệ thống quản lý dữ liệu nhạy cảm phải có cơ chế xác thực người dùng mạnh (*nhiều xác thực 2 yếu tố*) và phân quyền truy cập hợp lý. Việc này nhằm giảm nguy cơ truy cập trái phép và xác định được chính xác danh tính người truy cập dữ liệu. Nếu xảy ra rò rỉ, từ nhật ký và hệ thống xác thực có thể biết tài khoản nào, thời điểm nào đã truy xuất dữ liệu. Pháp luật nên quy định cụ thể: “Cơ quan, tổ chức xử lý dữ liệu cá nhân phải áp dụng phương thức xác thực phù hợp và phân quyền truy cập theo



nguyên tắc tối thiểu”; vi phạm quy định này (ví dụ *cấp quyền tràn lan, dùng tài khoản dùng chung không xác thực*) sẽ bị xử phạt hành chính. Hiện tại, mới có yêu cầu chung “áp dụng biện pháp kỹ thuật quản lý”, cần chi tiết hóa hơn.

- **Thứ ba**, bắt buộc mã hóa đối với dữ liệu nhạy cảm. Dữ liệu cá nhân nhạy cảm (*như sinh trắc, sức khỏe, tài chính*) hoặc dữ liệu quan trọng nên được mã hóa khi lưu trữ và truyền gửi. Pháp luật có thể bổ sung: tổ chức lưu trữ các loại dữ liệu này mà không mã hóa hoặc bảo vệ bằng giải pháp tương đương sẽ bị xử phạt. Điều này tăng cường an ninh, nếu dữ liệu bị lộ nhưng mã hóa, hậu quả giảm đáng kể. Nhiều chuẩn mực quốc tế (ISO 27001) cũng yêu cầu mã hóa dữ liệu nhạy cảm. Luật Dữ liệu 2024 đã định nghĩa khái niệm mã hóa dữ liệu và giải mã, tạo cơ sở để yêu cầu thực thi biện pháp này.

- **Thứ tư**, cơ chế giám sát kỹ thuật từ phía cơ quan quản lý. Bên cạnh yêu cầu tự triển khai của doanh nghiệp, cơ quan quản lý (*như Bộ Công an, Bộ Khoa học và Công nghệ*) có thể thiết lập hệ thống kỹ thuật giúp phát hiện sớm việc mua bán dữ liệu trái phép trên mạng. Ví dụ: sử dụng công cụ quét các diễn đàn hacker, mạng xã hội để tìm từ khóa rao bán dữ liệu, qua đó kịp thời điều tra. Hoạt động này mang tính nghiệp vụ nhiều hơn, nhưng pháp luật có thể tạo hành lang (ví dụ: *cho phép thu thập thông tin trên không gian mạng nhằm phát hiện vi phạm dữ liệu mà không xem đó là xâm phạm riêng tư*). Đồng thời, khuyến khích hợp tác công tư, các doanh nghiệp mạng, viễn thông nên phối hợp cung cấp thông tin khi cơ quan chức năng truy vết vụ việc.

Tóm lại, cơ chế truy vết kỹ thuật phải được luật hóa ở mức nghị định hoặc thông tư bắt buộc. Khi đã có yêu cầu pháp lý, cơ quan có thẩm quyền mới có cơ sở xử phạt nếu đơn vị không đáp ứng (ví dụ *một công ty không lưu nhật ký sẽ bị phạt vì vi phạm tiêu chuẩn bảo mật*). Về lâu dài, việc này tạo thói quen tuân thủ chuẩn bảo mật, giúp xây dựng môi trường dữ liệu an toàn hơn. Đồng thời, khi sự cố xảy ra, nhật ký và biện pháp xác thực sẽ cung cấp bằng chứng hỗ trợ xử lý vi phạm nhanh chóng, nâng cao hiệu quả thực thi pháp luật.



3.2.5.4. Thiết lập cơ chế bảo vệ người tố giác và kênh tiếp nhận phản ánh vi phạm trực tuyến

Để phát hiện kịp thời và xử lý nghiêm các vi phạm dữ liệu, không thể chỉ trông chờ vào thanh tra hay công an tự điều tra, mà cần sự tham gia của chính người dân, người trong cuộc. Tuy nhiên, hiện nay nhiều nhân viên, người dân ngại tố cáo hành vi vi phạm (*ví dụ nhân viên công ty biết sép đang bán dữ liệu khách hàng nhưng sợ mất việc nên im lặng*). Do đó, cần có cơ chế khuyến khích và bảo vệ người tố giác trong lĩnh vực dữ liệu, cũng như thuận tiện hóa việc gửi phản ánh tố cáo qua mạng.

- **Một là**, Luật Tố cáo 2018 đã có quy định chung về bảo vệ người tố cáo (*bảo mật danh tính, bảo vệ vị trí công tác, tính mạng khi cần thiết*). Tuy nhiên, cần vận dụng cụ thể trong lĩnh vực dữ liệu. Cơ quan chức năng (Bộ Công an) cần ban hành quy trình đảm bảo giữ kín thông tin người báo cáo vi phạm dữ liệu. Ví dụ: nếu một chuyên viên IT tố giác công ty đang lén bán thông tin khách hàng, cơ quan tiếp nhận phải giấu tên người này trong quá trình điều tra và nếu công ty đó tìm cách trả thù (*sa thải, đe dọa*) thì sẽ bị xử lý nghiêm. Có thể bổ sung trong nghị định xử phạt: hành vi cản trở, trả thù người tố cáo vi phạm về dữ liệu sẽ bị phạt tiền và xử lý theo Luật Tố cáo. Điều này tạo niềm tin để người biết sai phạm dám lên tiếng.

- **Hai là**, ngoài bảo vệ, nên xem xét cơ chế khen thưởng xứng đáng cho cá nhân phát hiện, cung cấp thông tin giúp xử lý vụ vi phạm dữ liệu nghiêm trọng. Ví dụ: thường một tỷ lệ phần trăm trên số tiền phạt thu được, hoặc bằng hiện vật/văn bằng ghi nhận (*hiện tại đã có quy định về việc trích phần trăm phạt vi phạm giao thông cho người phát hiện, tuy nhiên chưa được hướng dẫn thực hiện, nếu áp dụng vào trong Luật này, cần phải triển khai đồng bộ ngay từ đầu*). Việc thưởng này giống như một số lĩnh vực khác (*phát hiện buôn lậu, gian lận thuế...*). Tuy nhiên, do tính chất dữ liệu khá nhạy cảm, có thể thận trọng áp dụng theo từng trường hợp được duyệt.



- **Ba là**, Bộ Công an và các cơ quan liên quan nên thiết lập cổng thông tin hoặc đường dây nóng dành riêng cho tiếp nhận phản ánh vi phạm dữ liệu. Hiện tại, Cục An ninh mạng (A05) có trang web/cổng thông tin nhưng người dân chưa biết nhiều. Cần đẩy mạnh truyền thông về một địa chỉ tin cậy, ví dụ: một cổng tiếp nhận khiếu nại về dữ liệu cá nhân trên trang của Bộ Công an. Trên cổng đó, chủ thẻ dữ liệu có thể gửi phản ánh nếu cho rằng dữ liệu của mình bị xâm phạm (*bị gọi điện quảng cáo làm phiền do lô số, phát hiện thông tin cá nhân bị đăng lên mạng...*). Quy trình xử lý cần công khai việc sau khi nhận, cơ quan nào xử lý, thời hạn bao lâu phải phản hồi.

Bên cạnh đó, có thể tích hợp kênh này vào Cổng Dịch vụ công quốc gia để người dân dễ sử dụng. Ví dụ: bổ sung mục “Phản ánh vi phạm về dữ liệu cá nhân” trên hệ thống tiếp nhận phản ánh kiến nghị của Chính phủ. Việc này tương tự như cách Chính phủ tiếp nhận phản ánh về spam, cuộc gọi rác (*thông qua đầu số, website của Cục An toàn thông tin Bộ Thông tin và Truyền thông trước kia*). Sự thuận tiện trong phản ánh trực tuyến sẽ giúp cơ quan chức năng thu thập được nhiều manh mối vi phạm từ cộng đồng, thay vì đợi đến khi hậu quả lớn mới phát hiện.

- **Thứ năm**, quy định pháp luật nên đặt thời hạn xử lý đôi với phản ánh vi phạm dữ liệu. Ví dụ: trong vòng 30 ngày kể từ ngày nhận được phản ánh, cơ quan chức năng phải kiểm tra, xác minh và trả lời kết quả (*tương tự Luật Khiếu nại, Tố cáo quy định thời hạn giải quyết*). Nếu chậm trễ, người có trách nhiệm có thể bị nhắc nhở. Điều này nhằm tránh tình trạng đơn thư bị bỏ qua, giúp tăng niềm tin công chúng.

Tóm lại, xây dựng cơ chế tố giác thuận tiện và an toàn là giải pháp then chốt để huy động xã hội giám sát vi phạm dữ liệu. Khi người dân tích cực tố cáo và được bảo vệ, các tổ chức sẽ dè chừng hơn trong việc vi phạm, đồng thời cơ quan quản lý cũng có thêm nhiều nguồn thông tin để xử lý. Đây là một trụ cột mềm nhưng rất quan trọng hỗ trợ cho các trụ cột cứng là chế tài pháp luật.



3.2.5.5. Đào tạo và tăng cường nguồn lực giám sát, xử phạt vi phạm dữ liệu

Yếu tố con người đóng vai trò quyết định trong hiệu lực thực thi pháp luật. Việc có luật tốt, chế tài nghiêm minh cũng vô nghĩa nếu thiếu nhân lực có năng lực để áp dụng. Do đó, cần chú trọng đào tạo, phát triển nguồn nhân lực cho công tác giám sát, thanh tra và xử lý vi phạm trong lĩnh vực dữ liệu, bao gồm:

- **Thứ nhất**, đào tạo chuyên sâu cho cán bộ thực thi pháp luật. Các cán bộ thanh tra, công an, kiểm sát viên liên quan cần được bồi dưỡng kiến thức chuyên môn về pháp luật bảo vệ dữ liệu và kỹ năng điều tra số. Đây là lĩnh vực mới, phức tạp, đòi hỏi hiểu biết cả về pháp lý lẫn công nghệ. Bộ Công an nên tổ chức các khóa huấn luyện cho lực lượng An ninh mạng, Cảnh sát kinh tế về nhận diện hành vi vi phạm dữ liệu, cách thu thập chứng cứ điện tử, kỹ thuật phân tích dữ liệu. Bộ Khoa học và Công nghệ cũng cần đào tạo nghiệp vụ phát hiện các chiêu thức xâm phạm dữ liệu trên môi trường mạng. Việc đào tạo có thể kết hợp với chuyên gia quốc tế, học hỏi kinh nghiệm từ các nước có cơ quan bảo vệ dữ liệu mạnh (*nhu Uỷ ban GDPR châu Âu, Uỷ ban PDPC Singapore...*).

- **Thứ hai**, thành lập hoặc củng cố đơn vị chuyên trách. Mặc dù Luật Bảo vệ dữ liệu cá nhân 2025 giao Bộ Công an là đầu mối quản lý nhà nước về bảo vệ dữ liệu cá nhân, nhưng để thực hiện hiệu quả, có thể cần một Cơ quan chuyên trách với nhiệm vụ tương tự cơ quan bảo vệ dữ liệu độc lập. Đơn vị này sẽ tiếp nhận khiếu nại, thanh tra định kỳ các tổ chức lớn về việc tuân thủ luật dữ liệu và ra quyết định xử phạt vi phạm hành chính. Hiện nay, lực lượng chuyên trách về an ninh mạng (A05) đã có nhưng nhiệm vụ rất rộng (*bao gồm chống tội phạm mạng*). Cần bổ sung biện chế và phân công một nhóm chuyên trách về bảo vệ dữ liệu cá nhân trong đó. Đồng thời, tại các địa phương, có thể giao Phòng An ninh mạng Công an tỉnh, Thanh tra tỉnh đảm nhiệm một phần công tác kiểm tra, xử phạt vi phạm dữ liệu trên địa bàn.

- **Thứ ba**, tăng cường phối hợp liên ngành. Vi phạm dữ liệu xảy ra trong mọi lĩnh vực, nên thanh tra các bộ ngành phải biết phối hợp. Giải pháp là thiết lập cơ chế phối hợp thường xuyên giữa Bộ Công an với Bộ Khoa học và Công nghệ,



Bộ Tư pháp, Bộ Công thương, Ngân hàng Nhà nước... về bảo vệ dữ liệu. Có thể thành lập một Ban chỉ đạo liên ngành hoặc tổ công tác do Bộ Công an chủ trì để trao đổi thông tin, thống nhất cách xử lý những vụ phức tạp (*ví dụ vụ lô dữ liệu thẻ ngân hàng thì cần phối hợp Ngân hàng nhà nước; vụ lô dữ liệu khám chữa bệnh thì cần Bộ Y tế hỗ trợ...*). Phối hợp tốt sẽ giúp nâng cao hiệu quả xử lý, tránh bỏ lọt hoặc xử phạt chòng chéo.

- **Thứ tư**, đào tạo nhận thức cho doanh nghiệp và người dân. Bên cạnh đào tạo công chức, cũng cần tổ chức tuyên truyền, tập huấn cho chính các tổ chức, doanh nghiệp, đối tượng phải tuân thủ pháp luật dữ liệu. Nhiều doanh nghiệp vừa và nhỏ hiện chưa có nhân sự phụ trách bảo vệ dữ liệu. Nhà nước có thể hỗ trợ bằng cách phát hành sổ tay hướng dẫn tuân thủ về bảo vệ dữ liệu cá nhân, tổ chức các hội thảo cho doanh nghiệp về trách nhiệm và chế tài pháp luật mới (*nhiều giới thiệu Luật Dữ liệu 2024, Luật Bảo vệ dữ liệu cá nhân 2025*). Khi doanh nghiệp hiểu rõ nghĩa vụ và chế tài nghiêm khắc, họ sẽ chủ động tuân thủ, giảm nguy cơ vi phạm xảy ra. Người dân cũng cần được phổ biến kiến thức để tự bảo vệ dữ liệu của mình và biết cách tố giác khi quyền lợi bị xâm phạm.

- **Thứ năm**, đầu tư cơ sở vật chất, công nghệ. Cuối cùng, nguồn lực không chỉ là con người mà còn là công cụ hỗ trợ. Cần đầu tư cho các cơ quan thực thi các phòng lab kỹ thuật số, phần mềm phân tích dữ liệu, công cụ phát hiện xâm nhập... phục vụ điều tra các vụ việc phức tạp (*ví dụ phân tích dữ liệu log lớn để tìm thủ phạm*). Đồng thời, ngân sách cũng cần dành cho hệ thống tiếp nhận phản ánh trực tuyến như đã nêu, duy trì đường dây nóng. Khi nguồn lực vật chất đảm bảo, cán bộ được trang bị tốt, việc phát hiện và xử phạt vi phạm dữ liệu sẽ hiệu quả, chuẩn xác hơn.

Những giải pháp trên đây có mối quan hệ chặt chẽ và đồng bộ với nhau. Từ ban hành nghị định chuyên ngành cung cấp nền tảng pháp lý đầy đủ; bảng hành vi - mức phạt làm rõ nội dung áp dụng; biện pháp kỹ thuật truy vết đảm bảo khả năng phát hiện, thu thập chứng cứ; cơ chế tố giác và bảo vệ người tố cáo huy động



sự tham gia của xã hội đến đào tạo nguồn lực giúp pháp luật đi vào cuộc sống một cách hiệu quả.

Việc hoàn thiện pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu là yêu cầu cấp bách trong bối cảnh chuyển đổi số và nền kinh tế dữ liệu. Với hành lang pháp lý đủ mạnh và thực thi nghiêm minh, các hành vi xâm phạm dữ liệu sẽ được ngăn chặn, xử lý kịp thời, nghiêm minh, qua đó bảo vệ tốt hơn quyền và lợi ích hợp pháp của cá nhân về dữ liệu, đồng thời thúc đẩy phát triển kinh tế số an toàn, bền vững ở Việt Nam. Các đề xuất trên cần được nghiên cứu sâu hơn và sớm thể chế hóa, nhằm lấp đầy những khoảng trống hiện tại, đưa pháp luật Việt Nam tiệm cận với chuẩn mực tiên bộ quốc tế trong lĩnh vực bảo vệ dữ liệu.



PHỤ LỤC

Đấu tranh, phản bác các quan điểm sai trái về các hành vi bị nghiêm cấm trong Luật Dữ liệu

Trong kỷ nguyên chuyển đổi số, dữ liệu đã trở thành tài sản chiến lược, là “năng lượng mới” của nền kinh tế số và xã hội số. Việc quản lý, khai thác và bảo vệ dữ liệu đòi hỏi một hành lang pháp lý toàn diện. Nhận thức rõ yêu cầu đó, Quốc hội Việt Nam đã thông qua Luật Dữ liệu năm 2024 (*Luật số 60/2024/QH15*) với 451/458 đại biểu tán thành (*chiếm 94,15%*)

Tuy nhiên, ngay sau khi luật được thông qua, một số trang truyền thông nước ngoài và tổ chức thiêng thiêng chí đã đưa ra những luận điệu xuyên tạc về Luật Dữ liệu 2024. Họ quy chụp rằng luật “*mơ hồ, lạm quyền, xâm phạm quyền riêng tư, bóp nghẹt tự do ngôn luận*” và gây tổn hại cho doanh nghiệp. Những chỉ trích này chủ yếu xoay vào quy định cho phép cơ quan nhà nước yêu cầu cung cấp dữ liệu trong tình huống khẩn cấp, đe dọa an ninh quốc gia, thảm họa, chống bạo loạn, khủng bố; cũng như quy định cần có sự chấp thuận của cơ quan chức năng khi chuyển dữ liệu cốt lõi ra nước ngoài. Trên thực tế, những nhận định đó đã cố tình bóp méo mục đích thực sự của luật và bỏ qua bối cảnh pháp lý cũng như thông lệ quốc tế.

Luật Dữ liệu 2024 là văn bản pháp luật đầu tiên của Việt Nam điều chỉnh một cách toàn diện hoạt động quản trị, phát triển và bảo vệ dữ liệu số. Để ngăn ngừa những nguy cơ lạm dụng dữ liệu gây hại, Điều 10 của luật đã liệt kê rõ bốn nhóm hành vi bị nghiêm cấm trong hoạt động dữ liệu số. Cụ thể, bốn nhóm hành vi này gồm:

(1) Lợi dụng hoạt động về dữ liệu để xâm phạm lợi ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự an toàn xã hội, lợi ích công cộng hoặc quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Nói cách khác, luật cấm mọi hành vi sử dụng việc xử lý, quản trị, kinh doanh, phát triển dữ liệu như một công cụ nhằm chống phá Nhà nước, xâm hại lợi ích dân tộc, gây mất ổn định xã hội, hoặc xâm phạm quyền con người, quyền công dân. Quy định này bao quát từ việc tạo ra,



phát tán dữ liệu có nội dung xấu độc (*như tuyên truyền xuyên tạc, kích động*) cho đến việc lợi dụng công nghệ dữ liệu để xâm phạm đời tư, nhân phẩm của người khác. Đây là nhóm hành vi có phạm vi rộng, phản ánh thực tế rằng dữ liệu có thể bị lợi dụng làm vũ khí chống phá an ninh quốc gia hoặc xâm hại quyền con người nếu không được kiểm soát chặt chẽ.

(2) Cản trở hoặc ngăn chặn trái pháp luật quá trình xử lý, quản trị dữ liệu; tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin về dữ liệu. Quy định này nhắm đến các hành vi xâm nhập trái phép, tấn công mạng, đánh cắp hoặc phá hoại dữ liệu và hệ thống hạ tầng dữ liệu. Trong bối cảnh các cơ sở dữ liệu quốc gia và hệ thống thông tin quan trọng trở thành “huyết mạch” của nền kinh tế – xã hội số, việc bảo vệ an toàn hạ tầng dữ liệu là tối quan trọng. Mọi hành vi như hack chiếm quyền truy cập, đánh cắp dữ liệu, cài mã độc mã hóa đòi tiền chuộc, hoặc cản trở dòng chảy dữ liệu phục vụ quản lý đều bị luật nghiêm cấm. Điều này nhằm đảm bảo tính liên tục và tin cậy của các hệ thống dữ liệu, ngăn chặn các nguy cơ như mất dữ liệu diện rộng, rò rỉ thông tin nhạy cảm hay tê liệt dịch vụ công trực tuyến.

(3) Giả mạo, cố ý làm sai lệch, làm mất hoặc làm hư hỏng dữ liệu trong cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị – xã hội. Nhóm hành vi này tập trung bảo vệ tính toàn vẹn của dữ liệu công do các cơ quan công quyền quản lý. Các hành vi bị cấm bao gồm: giả mạo dữ liệu (*tạo dữ liệu giả mạo giống như thật để lừa dối*), làm sai lệch dữ liệu (*sửa đổi trái phép dữ liệu gốc*), làm mất dữ liệu (xoá hoặc làm biến mất dữ liệu khi chưa được phép) và làm hư hỏng dữ liệu (*tác động khiến dữ liệu bị hỏng, không sử dụng được*). Những hành vi này đều xâm hại nghiêm trọng đến độ tin cậy và tính nguyên bản của các hệ thống dữ liệu nhà nước, ví dụ: giả mạo công văn điện tử, sửa só liệu dân cư để trục lợi, xóa bỏ hồ sơ công chức hoặc phá hoại cơ sở dữ liệu quốc gia. Việc luật quy định riêng nhóm hành vi này cho thấy quyết tâm bảo vệ kho dữ liệu công khỏi các hành vi phá hoại hoặc gian dối.



(4) Cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định của pháp luật. Đây là quy định nhằm đảm bảo trách nhiệm trung thực và đầy đủ trong cung cấp dữ liệu của các cơ quan, tổ chức, cá nhân khi pháp luật yêu cầu. Hành vi “cố ý cung cấp dữ liệu sai lệch” nghĩa là chủ thể cố tình đưa ra dữ liệu không đúng sự thật (*thông tin giả, sai số liệu...*) cho cơ quan có thẩm quyền hoặc cho hệ thống dữ liệu chung. Còn “không cung cấp dữ liệu theo quy định” hàm ý việc trốn tránh nghĩa vụ cung cấp, chia sẻ dữ liệu khi pháp luật bắt buộc (*chẳng hạn như một cơ quan từ chối chia sẻ dữ liệu dùng chung phục vụ Chính phủ điện tử, hoặc doanh nghiệp không cung cấp dữ liệu theo yêu cầu báo cáo*). Những hành vi này có thể cản trở quản trị dữ liệu minh bạch, cản trở dịch vụ công và làm giảm hiệu quả điều hành kinh tế – xã hội. Vì vậy, Luật Dữ liệu 2024 nghiêm cấm việc giấu giếm dữ liệu hoặc cung cấp thông tin sai, nhằm đề cao tính minh bạch, chính xác trong hệ thống dữ liệu quốc gia.

Nhìn chung, bốn nhóm hành vi cấm trên phản ánh đầy đủ các nguy cơ tiêu cực trong thời đại số, từ việc sử dụng dữ liệu làm công cụ xâm phạm an ninh quốc gia, phá hoại trật tự xã hội; cho đến tấn công hạ tầng dữ liệu, thao túng thông tin công và vi phạm nghĩa vụ chia sẻ dữ liệu. Đây là những ranh giới “đỏ” mà Luật Dữ liệu đặt ra để định hướng cho mọi chủ thể khi tham gia hoạt động dữ liệu số. Quan trọng hơn, các điều cấm này không phải là điều gì quá mới mẻ hay mơ hồ, chúng kế thừa, cụ thể hóa nhiều nguyên tắc đã được quy định rải rác trong pháp luật hiện hành. Chẳng hạn, Luật An ninh mạng 2018 đã cấm sử dụng không gian mạng để xâm phạm an ninh quốc gia, trật tự an toàn xã hội hoặc quyền lợi hợp pháp của tổ chức, cá nhân. Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân cũng nghiêm cấm xử lý dữ liệu cá nhân nhằm chống lại Nhà nước hoặc xâm phạm an ninh, trật tự. Tương tự, Bộ luật Hình sự hiện hành có tội danh “*lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân*” (Điều 331) với nội hàm tương đồng. Những điểm tương đồng này cho thấy Điều 10 Luật Dữ liệu 2024 nhất quán với tinh thần pháp luật Việt Nam: *kiên quyết ngăn chặn mọi hành vi lợi dụng không gian mạng, lợi dụng dữ liệu để xâm phạm an ninh quốc gia, trật tự xã hội và quyền con người*.



Nhờ sự tiếp nối này, Luật Dữ liệu 2024 đã thiết lập hành lang pháp lý thống nhất để xử lý nghiêm các hành vi lạm dụng dữ liệu mà trước đây nầm rải rác ở nhiều văn bản. Có thể nói, việc liệt kê rõ các nhóm hành vi bị cấm giúp định danh rành mạch những việc “không được làm” trong lĩnh vực dữ liệu, tạo cơ sở cho cơ quan chức năng xử lý vi phạm và răn đe phòng ngừa. Chính sự minh bạch này bác bỏ luận điệu cho rằng luật “mơ hồ, tùy tiện”. Trái lại, điều cấm càng rõ thì hành lang pháp lý càng chặt chẽ, không cho phép lạm quyền tùy hứng. Ví dụ, quy định cấm lợi dụng dữ liệu xâm phạm quyền con người cho thấy luật tôn trọng và bảo vệ quyền riêng tư, danh dự cá nhân, hoàn toàn không “xâm phạm quyền riêng tư” như cáo buộc, mà ngược lại ngăn chặn việc dữ liệu bị dùng để xâm phạm đời tư của công dân. Tương tự, cấm cung cấp dữ liệu sai lệch cũng chính là để bảo vệ quyền được thông tin chính xác của người dân và doanh nghiệp, chống lại nạn tin giả và sự tùy tiện trong quản lý thông tin.

Đặc biệt, nhóm hành vi (1) về lợi dụng dữ liệu chống phá Nhà nước và gây bất ổn xã hội, vốn bị một số đối tượng bên ngoài suy diễn là hạn chế tự do ngôn luận thực chất chỉ nhắm tới những hành vi vi phạm pháp luật nghiêm trọng. Luật Dữ liệu 2024 không hề cấm người dân bày tỏ ý kiến hay trao đổi thông tin hợp pháp; mà chỉ cấm các nội dung xấu độc, thông tin sai sự thật, tuyên truyền chống phá, vốn dĩ cũng đã bị nghiêm cấm theo Luật An ninh mạng và nhiều luật khác. Quy định này tương tự luật của nhiều quốc gia: chẳng hạn Đạo luật Dịch vụ Số (DSA) của Liên minh châu Âu yêu cầu các nền tảng lớn gỡ bỏ tin giả, nội dung độc hại; Hoa Kỳ cũng có các quy định chống khủng bố mạng và chia sẻ thông tin bảo mật; Trung Quốc áp dụng hệ thống quản lý nội dung chặt chẽ. Do đó, không thể coi việc Việt Nam ngăn chặn dữ liệu xấu độc là “đàn áp tự do ngôn luận”. Trên thực tế, Nhà nước luôn nhất quán bảo đảm quyền tự do ngôn luận, tự do Internet miễn là tuân thủ pháp luật, mọi cá nhân đều có thể bày tỏ chính kiến trên không gian mạng, và chỉ những kẻ lợi dụng tự do để xâm hại lợi ích cộng đồng mới bị xử lý. Như Bộ Ngoại giao Việt Nam đã nhiều lần nhấn mạnh, các quyền con người (*trong đó có tự do ngôn luận, quyền riêng tư*) ở Việt Nam luôn được



pháp luật tôn trọng bảo vệ, và không một quốc gia nào cho phép các thế lực chống phá “tự do” kích động, vi phạm pháp luật trên mạng.

Tóm lại, quy định về các hành vi bị nghiêm cấm trong Luật Dữ liệu 2024 là rõ ràng, cần thiết và phù hợp thông lệ chung. Nó tạo nền tảng pháp lý quan trọng để bảo vệ chủ quyền, an ninh quốc gia và trật tự an toàn xã hội trong môi trường số. Đồng thời, các điều cấm này cũng bảo vệ trực tiếp quyền và lợi ích chính đáng của người dân, doanh nghiệp trước các hành vi xâm hại bằng dữ liệu. Những luận điệu cho rằng luật “xâm phạm quyền riêng tư” hay “kiềm chế sáng tạo” là thiếu căn cứ, bởi lẽ mục tiêu của luật là ngăn chặn kẻ xấu lợi dụng dữ liệu xâm phạm quyền riêng tư và kìm hãm sự sáng tạo tiêu cực, chứ không hề cản trở các hoạt động sử dụng dữ liệu hợp pháp, lành mạnh. Chính nhờ hành lang pháp lý này, Việt Nam có thể tự tin thúc đẩy chuyển đổi số toàn diện mà vẫn giữ vững an ninh, an toàn cho không gian mạng quốc gia, đây là tiền đề quan trọng để kinh tế số phát triển bền vững trong tương lai.

Những luận điệu xuyên tạc từ một số tổ chức, đài báo nước ngoài cho rằng Luật Dữ liệu “*mơ hồ, lạm quyền, xâm phạm quyền riêng tư, hạn chế tự do...*” thực chất chỉ là sự áp đặt định kiến, thiếu khách quan. Như phân tích ở trên, mục đích cốt lõi của luật là bảo vệ chủ quyền dữ liệu quốc gia, quyền và lợi ích hợp pháp của người dân trong kỷ nguyên số. Các quy định về hành vi bị cấm hoàn toàn hướng tới ngăn chặn hành vi vi phạm pháp luật nghiêm trọng không hề đụng chạm đến các hoạt động hợp pháp của doanh nghiệp hay đời sống bình thường của người dân. Luật cũng trao quyền tự chủ tối đa cho tổ chức, doanh nghiệp trong triển khai các giải pháp bảo mật và chia sẻ dữ liệu, theo nguyên tắc “hậu kiểm” thay vì “tiền kiểm”. Nhà nước chỉ can thiệp khi phát hiện vi phạm. Đây là điểm tiến bộ, giảm gánh nặng thủ tục và khuyến khích đổi mới sáng tạo, trái ngược với cáo buộc “bóp nghẹt sáng tạo” mà một số luận điệu sai trái đưa ra. Về quyền riêng tư, Việt Nam đang song song xây dựng Luật Bảo vệ dữ liệu cá nhân với các tiêu chuẩn cao, thể hiện cam kết nâng cao quyền của chủ thể dữ liệu phù hợp thông lệ quốc tế. Điều đó khẳng định Nhà nước tuyệt đối tôn trọng và bảo vệ quyền riêng tư của công



dân, những biện pháp như yêu cầu cung cấp dữ liệu trong tình huống khẩn cấp chỉ áp dụng hạn chế, có điều kiện chặt chẽ nhằm kịp thời ứng phó thảm họa, bảo vệ tính mạng người dân, hoàn toàn tương đồng với pháp luật nhiều nước.

Đáng chú ý, Luật Dữ liệu 2024 không những không cản trở phát triển kinh tế mà ngược lại, còn tạo nền tảng cho kinh tế số bùng nổ. Bằng việc thiết lập khung pháp lý về thu thập, chia sẻ và bảo vệ dữ liệu, luật sẽ hình thành “niềm tin số” giữa các chủ thể trong giao dịch điện tử, giúp doanh nghiệp công nghệ Việt Nam chuyên nghiệp hóa quản trị dữ liệu và nâng cao năng lực cạnh tranh, hội nhập quốc tế. Nhiều doanh nghiệp đã đón nhận luật như một cơ hội để phát triển sản phẩm dữ liệu số phục vụ chính phủ điện tử, kinh tế số, xã hội số.Thêm nữa, luật được thiết kế với tư duy khuyến khích khai thác dữ liệu, Nhà nước chỉ đóng vai trò kiến tạo, hậu kiểm, nên sẽ không kìm hãm đổi mới sáng tạo mà còn tạo động lực thúc đẩy kinh tế dữ liệu. Những lo ngại về “tác động xấu tới đầu tư nước ngoài” cũng không có cơ sở, bởi lẽ một môi trường số an toàn, có pháp luật bảo vệ rõ ràng mới thực sự hấp dẫn nhà đầu tư. Thực tế, luật nhằm bảo vệ cả quyền lợi của nhà đầu tư nước ngoài tham gia kinh tế số Việt Nam khỏi các rủi ro mất an toàn dữ liệu.

Tóm lại, Luật Dữ liệu 2024 là bước đi chiến lược thể hiện tầm nhìn của Đảng và Nhà nước về bảo vệ an ninh quốc gia song hành với phát triển chính phủ số, kinh tế số. Cùng với việc nhanh chóng hoàn thiện chế tài xử lý vi phạm và nâng cao hiệu quả thực thi, Việt Nam đang tiến những bước vững chắc để quản lý tốt dữ liệu và không gian mạng, góp phần bảo đảm an ninh quốc gia và quyền lợi hợp pháp của công dân trong thời đại số. Bên cạnh đó, Việt Nam luôn nhất quán chủ trương tôn trọng, bảo vệ các quyền tự do cơ bản của con người, trong đó có quyền tự do ngôn luận, tự do Internet; đồng thời tích cực cập nhật luật pháp để mỗi người dân được an toàn trên không gian mạng. Những luận điệu xuyên tạc về Luật Dữ liệu sẽ không thể phủ nhận một sự thật rằng: bảo vệ chủ quyền số và quyền lợi người dân trong kỷ nguyên số là trách nhiệm chính đáng của mọi quốc gia, và Luật Dữ liệu 2024 chính là nỗ lực mạnh mẽ của Việt Nam để thực hiện trách nhiệm đó. Đây là sự thật không thể bóp méo



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. Bộ Luật Hình sự 2015 (*sửa đổi, bổ sung 2017, 2025*);
6. Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân;
7. Nghị định số 15/2020/NĐ-CP (*sửa đổi bổ sung 2022 và 2025*) quy định xử phạt vi phạm hành chính lĩnh vực CNTT, các mức phạt liên quan đến thông tin giả, tấn công mạng;
8. Nguyễn Bình, "Khắc phục khoảng trống pháp luật về dữ liệu", Báo Đại biểu Nhân dân, 2024.
9. Hồng Minh, "Luật Dữ liệu xây dựng niềm tin số và thúc đẩy chuyển đổi số toàn diện", Báo Nhân dân, 2025;
10. Phạm Thị Thanh Tâm, Phước Minh Hiệp "Tiếp tục hoàn thiện hệ thống pháp luật về bảo vệ dữ liệu cá nhân hướng tới mục tiêu hội nhập và kinh tế số", Tạp chí Cộng sản, 2025
11. Phương Oanh, "Sự thật không thể bóp méo", TTXVN, 2024;



Câu 4: Quy định về hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, xử lý, sử dụng dữ liệu? Nhiệm vụ, giải pháp để phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trở thành yếu tố quyết định, là điều kiện tiên quyết đưa nước ta phát triển giàu mạnh, hùng cường trong kỷ nguyên mới - kỷ nguyên vươn mình của Dân tộc?





Câu 4: Quy định về hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, xử lý, sử dụng dữ liệu? Nhiệm vụ, giải pháp để phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trở thành yếu tố quyết định, là điều kiện tiên quyết đưa nước ta phát triển giàu mạnh, hùng cường trong kỷ nguyên mới - kỷ nguyên vươn mình của Dân tộc?

Trả lời

4.1. Quy định về hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, xử lý, sử dụng dữ liệu

4.1.1. Quy định pháp luật về khoa học, công nghệ và đổi mới sáng tạo trong lĩnh vực dữ liệu

Luật Dữ liệu 2024 xác lập nhiều chính sách khuyến khích việc ứng dụng khoa học công nghệ và đổi mới sáng tạo trong hoạt động về dữ liệu. Ngay tại Điều 6 về Chính sách của Nhà nước, luật khẳng định “Dữ liệu là tài nguyên” và Nhà nước huy động mọi nguồn lực để “làm giàu dữ liệu, phát triển dữ liệu trở thành tài sản”. Luật ưu tiên phát triển dữ liệu phục vụ chuyển đổi số quốc gia gắn với bảo đảm quốc phòng, an ninh; đầu tư xây dựng Cơ sở dữ liệu tổng hợp quốc gia và Trung tâm dữ liệu quốc gia đáp ứng yêu cầu Chính phủ số, kinh tế số, xã hội số. Đặc biệt, khoản 5 Điều 6 nhấn mạnh Nhà nước khuyến khích cơ quan, tổ chức, cá nhân “đầu tư, nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, đổi mới sáng tạo, ứng dụng trong lĩnh vực dữ liệu; xây dựng trung tâm lưu trữ, xử lý dữ liệu tại Việt Nam; phát triển thị trường dữ liệu”. Đây là cơ sở pháp lý quan trọng khuyến khích hoạt động Khoa học, Công nghệ và đổi mới sáng tạo để phát triển hạ tầng và hệ sinh thái dữ liệu trong nước.

Luật Dữ liệu cũng đề cao hợp tác quốc tế về Khoa học và Công nghệ trong lĩnh vực dữ liệu. Điều 7 liệt kê các nội dung hợp tác quốc tế bao gồm: đào tạo nhân lực; nghiên cứu khoa học, ứng dụng Khoa học và Công nghệ trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; chuyển giao công nghệ tiên tiến, đầu tư hạ tầng trung tâm dữ liệu; tham gia xây dựng tiêu chuẩn quốc tế về



dữ liệu;.... Như vậy, Việt Nam khuyến khích trao đổi tri thức và công nghệ với các nước nhằm bắt kịp xu hướng quản trị dữ liệu hiện đại. Ở cấp độ quản lý nhà nước, Điều 8 Luật Dữ liệu xác định nội dung quản lý nhà nước bao gồm việc “nghiên cứu, ứng dụng khoa học và công nghệ về dữ liệu; phát triển sản phẩm, dịch vụ về dữ liệu; quản lý, giám sát, phát triển thị trường dữ liệu”. Cơ quan quản lý cũng có trách nhiệm đào tạo nguồn nhân lực và hợp tác quốc tế về dữ liệu, thể hiện sự tích hợp giữa chính sách dữ liệu với phát triển Khoa học và Công nghệ và nguồn nhân lực chất lượng cao.



Hình ảnh: Tổng Bí thư Tô Lâm, Trưởng Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số phát biểu chỉ đạo.

Ảnh: TTXVN

Quan trọng nhất, Điều 24 Luật Dữ liệu 2024 quy định cụ thể về “Hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu”. Luật yêu cầu các hoạt động Khoa học, Công nghệ và



đổi mới sáng tạo trong lĩnh vực dữ liệu phải phù hợp với Chiến lược dữ liệu quốc gia, phát huy nội lực và tuân thủ các nguyên tắc quản trị dữ liệu. Khoản 2 Điều 24 liệt kê các nền tảng khoa học công nghệ cốt lõi cho dữ liệu, bao gồm: trí tuệ nhân tạo (*AI*), điện toán đám mây, chuỗi khối (*blockchain*), truyền thông dữ liệu, Internet vạn vật (*IoT*), dữ liệu lớn (*Big Data*) và các công nghệ hiện đại khác. Đây đều là những công nghệ tiên phong của cách mạng công nghiệp 4.0, được luật xác định là nền tảng để xây dựng, xử lý và khai thác dữ liệu. Luật yêu cầu tập trung nguồn lực quốc gia để phát triển, ứng dụng các nền tảng này phục vụ chuyển đổi số, bảo đảm quốc phòng, an ninh và phát triển kinh tế - xã hội. Đồng thời, Chính phủ sẽ ban hành quy định chi tiết để quản lý, phát triển và thử nghiệm có kiểm soát các hoạt động nghiên cứu, ứng dụng khoa học, công nghệ và đổi mới sáng tạo về dữ liệu. Những quy định này thể hiện quyết tâm của Nhà nước trong việc thúc đẩy nghiên cứu và ứng dụng công nghệ mới (*nhiều AI, Big Data...*) vào toàn bộ chu trình dữ liệu, nhưng vẫn có cơ chế kiểm soát rủi ro phù hợp.

Luật Dữ liệu 2024 và Nghị định 160/2025/NĐ-CP quy định về Quỹ phát triển quốc gia còn tạo cơ chế tài chính hỗ trợ Khoa học và Công nghệ về dữ liệu. Điều 29 luật giao thành lập Quỹ Phát triển dữ liệu Quốc gia (*quỹ tài chính nhà nước ngoài ngân sách*) nhằm thúc đẩy phát triển, khai thác, ứng dụng và quản trị dữ liệu quốc gia. Trên thực tế, Chính phủ đã ban hành Nghị định 160/2025/NĐ-CP để triển khai quỹ này với vốn điều lệ tối thiểu 1.000 tỷ đồng, do Bộ Công an quản lý. Quỹ sẽ hỗ trợ nghiên cứu, phát triển hạ tầng dữ liệu, thúc đẩy ứng dụng các công nghệ mới như AI, Big Data, blockchain, đặc biệt quan tâm đến khu vực nông thôn, miền núi, hải đảo. Đây được kỳ vọng là động lực tài chính mạnh mẽ để rút ngắn khoảng cách số giữa các vùng miền và khuyến khích đổi mới sáng tạo trong việc khai thác dữ liệu. Song song đó, Luật Dữ liệu áp dụng phương thức quản lý theo hướng “hậu kiểm” thay vì “tiền kiểm”, cơ quan nhà nước không can thiệp trước vào hoạt động xử lý, kinh doanh dữ liệu mà chủ yếu giám sát và xử lý vi phạm khi có dấu hiệu sai phạm. Cách tiếp cận này giảm gánh nặng thủ tục hành



chính, trao quyền tự chủ cho doanh nghiệp trong bảo mật và chia sẻ dữ liệu, từ đó khuyến khích đổi mới sáng tạo trong lĩnh vực dữ liệu.

Trong khi đó, Luật Khoa học, Công nghệ và Đổi mới sáng tạo 2025 tạo khung pháp lý toàn diện thúc đẩy hoạt động Khoa học, Công nghệ và đổi mới sáng tạo, đồng thời có những quy định cụ thể liên quan đến dữ liệu và chuyển đổi số. Luật này mở rộng phạm vi so với Luật Khoa học và Công nghệ 2013 trước đây, bổ sung mạnh mẽ yếu tố đổi mới sáng tạo và các cơ chế linh hoạt để thúc đẩy nghiên cứu, ứng dụng công nghệ. Về chuyển đổi số trong khoa học và công nghệ, luật mới quy định riêng một điều (*Điều 20*) về chuyển đổi số trong hoạt động Khoa học, Công nghệ và đổi mới sáng tạo. Nhà nước được giao nhiệm vụ “thúc đẩy chuyển đổi số toàn diện trong lĩnh vực Khoa học, Công nghệ và đổi mới sáng tạo” thông qua phát triển hạ tầng số, cung cấp dịch vụ công trực tuyến, số hóa dữ liệu và tự động hóa quy trình nghiệp vụ nhằm nâng cao hiệu quả, minh bạch. Nhà nước khuyến khích ứng dụng công nghệ dữ liệu lớn (*Big Data*) và trí tuệ nhân tạo để nâng cao hiệu quả hoạt động Khoa học, Công nghệ và đổi mới sáng tạo. Đồng thời, Chính phủ đầu tư xây dựng và vận hành Nền tảng số quản lý Khoa học, Công nghệ và đổi mới sáng tạo quốc gia cũng như Hệ thống thông tin quốc gia về Khoa học, Công nghệ và đổi mới sáng tạo, bảo đảm kết nối tập trung để lưu trữ, chia sẻ và công khai kết quả hoạt động Khoa học, Công nghệ và đổi mới sáng tạo cho cộng đồng. Quy định này cho thấy pháp luật yêu cầu ứng dụng công nghệ số và quản trị dữ liệu trong chính hoạt động quản lý khoa học (*ví dụ: sử dụng nền tảng số quốc gia để thu thập dữ liệu thống kê, báo cáo về nhiệm vụ Khoa học và Công nghệ, chia sẻ thông tin kết quả nghiên cứu, qua đó minh bạch và tăng tính liên thông của dữ liệu khoa học*).

Luật Khoa học, Công nghệ và đổi mới sáng tạo 2025 cũng đề cao việc mở và chia sẻ dữ liệu khoa học. Cụ thể, Điều 32 của luật khuyến khích việc chia sẻ dữ liệu, phương pháp, kết quả nghiên cứu khoa học, trong đó nhấn mạnh sử dụng và phát triển công nghệ nguồn mở, đồng thời bảo đảm minh bạch, dễ tiếp cận nhưng vẫn tôn trọng quyền sở hữu trí tuệ và bảo vệ dữ liệu cá nhân. Nhà nước sẽ



xây dựng hạ tầng kỹ thuật đáp ứng yêu cầu chia sẻ dữ liệu và công bố kết quả nghiên cứu khoa học một cách bảo mật, có khả năng tương tác và tái sử dụng. Doanh nghiệp và cộng đồng được khuyến khích tham gia sử dụng, đóng góp dữ liệu và kết quả nghiên cứu vào các dự án nguồn mở. Đây chính là định hướng khoa học mở (*open science*), tận dụng sức mạnh của dữ liệu và tri thức chia sẻ để thúc đẩy sáng tạo.

Đặc biệt, để tạo môi trường thử nghiệm thuận lợi cho đổi mới sáng tạo, Luật Khoa học, Công nghệ và đổi mới sáng tạo 2025 đưa ra cơ chế “thử nghiệm có kiểm soát” (*regulatory sandbox*). Theo luật, cơ quan có thẩm quyền có thể cho phép tổ chức, doanh nghiệp thử nghiệm các công nghệ, giải pháp, sản phẩm, dịch vụ, mô hình kinh doanh mới mà pháp luật chưa có quy định, trong phạm vi và thời gian giới hạn. Luật đặt ra nguyên tắc thử nghiệm phải công khai, bình đẳng và tuân thủ yêu cầu về an ninh, an toàn. Đáng chú ý, luật còn có quy định miễn trừ hoặc loại trừ trách nhiệm pháp lý cho các cá nhân, tổ chức tham gia thử nghiệm nếu đã tuân thủ đúng quy định sandbox và hành động với “động cơ trong sáng, vì lợi ích chung”. Ví dụ: luật miễn trách nhiệm dân sự, hành chính hoặc thậm chí hình sự đối với rủi ro trong nghiên cứu, thử nghiệm, áp dụng tiến bộ Khoa học và Công nghệ khi các chủ thể đã tuân thủ quy trình thử nghiệm có kiểm soát. Quy định khoan dung này giúp các nhà khoa học, doanh nghiệp yên tâm thử nghiệm những ý tưởng đột phá, kể cả trong lĩnh vực dữ liệu (*ví dụ thử nghiệm thuật toán AI mới trên dữ liệu*), mà không sợ bị xử phạt nếu xảy ra rủi ro ngoài ý muốn. Đây chính là công cụ pháp lý để thúc đẩy đổi mới sáng tạo, tạo không gian cho công nghệ mới phát triển.

Cuối cùng, Luật Khoa học, Công nghệ và đổi mới sáng tạo 2025 đã đồng bộ với Luật Dữ liệu 2024 về quản trị dữ liệu trong hoạt động khoa học. Luật quy định khi kết quả nhiệm vụ Khoa học và Công nghệ có lưu trữ, xử lý dữ liệu cốt lõi, dữ liệu quan trọng hoặc dữ liệu chuyển xuyên biên giới thì việc quản lý phải tuân thủ Luật Dữ liệu. Tương tự, việc chuyển giao ra nước ngoài các kết quả nghiên cứu có chứa loại dữ liệu nhạy cảm này cũng phải theo quy định của Luật



Dữ liệu. Như vậy, luật Khoa học, Công nghệ và đổi mới sáng tạo đã tạo mối liên hệ chặt chẽ với Luật Dữ liệu để bảo đảm rằng các dữ liệu quan trọng quốc gia thu được từ nghiên cứu khoa học được bảo vệ và quản lý an toàn, tuân thủ các yêu cầu về chủ quyền dữ liệu. Điều này cho thấy sự thống nhất của hệ thống pháp luật, thúc đẩy nghiên cứu khoa học dựa trên dữ liệu, nhưng đồng thời đặt ra khuôn khổ quản trị dữ liệu an toàn theo Luật Dữ liệu.

Tóm lại, hai đạo luật mới đã xây dựng một hành lang pháp lý đồng bộ, Luật Dữ liệu 2024 định hướng phát triển dữ liệu gắn liền với Khoa học, Công nghệ và đổi mới sáng tạo, còn Luật Khoa học, Công nghệ và đổi mới sáng tạo 2025 cung cấp cơ chế, chính sách để Khoa học, Công nghệ và đổi mới sáng tạo phát huy vai trò trong kỷ nguyên dữ liệu và chuyển đổi số.

4.1.2. Vai trò của khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, bảo vệ, khai thác dữ liệu

4.1.2.1. Dữ liệu là nguồn lực cho kỷ nguyên khoa học công nghệ.

Trong thời đại cách mạng công nghiệp 4.0, dữ liệu được định vị là “tư liệu sản xuất” mới, là nguyên liệu đầu vào cho nhiều hoạt động khoa học, công nghệ và sáng tạo. Nghị quyết 57-NQ/TW (2024) của Bộ Chính trị xác định rõ: “*Làm giàu, khai thác tối đa tiềm năng của dữ liệu, đưa dữ liệu thành tư liệu sản xuất chính, thúc đẩy phát triển nhanh cơ sở dữ liệu lớn, công nghiệp dữ liệu, kinh tế dữ liệu*”. Quan điểm này nhấn mạnh dữ liệu không chỉ là sản phẩm phụ của hoạt động số hóa, mà thực sự là tài nguyên chiến lược quyết định năng lực cạnh tranh quốc gia trong kỷ nguyên số. Thực tế cho thấy, những bước tiến trong trí tuệ nhân tạo (AI), học máy hay phân tích big data phụ thuộc mật thiết vào lượng dữ liệu khổng lồ được thu thập và xử lý. Vì vậy, muốn phát triển khoa học công nghệ và đổi mới sáng tạo, Việt Nam phải chú trọng xây dựng hạ tầng dữ liệu và cơ chế quản trị dữ liệu hiệu quả. Nghị quyết 57-NQ/TW đã chỉ rõ một trong những trọng tâm cốt lõi là dữ liệu và công nghệ chiến lược, trong đó thể chế phải “đi trước một bước”. Điều này giải thích vì sao cùng với chiến lược phát triển Khoa học và Công



nghệ, Trung ương đã thúc đẩy nhanh việc xây dựng Luật Dữ liệu 2024 nhằm tạo nền tảng pháp lý cho quản trị và khai thác dữ liệu.



Hình ảnh: Đồng chí Thiếu tướng Nguyễn Ngọc Cường, Cục trưởng Cục Cảnh sát QLHC về TTXH quán triệt nội dung Nghị quyết 57-NQ/TW và chuyên đề “Kỷ nguyên phát triển mới - Kỷ nguyên vươn mình của dân tộc Việt Nam”.

Ảnh: Trang TTĐT Cục C06

4.1.2.2. Khoa học, công nghệ hỗ trợ xây dựng và bảo vệ dữ liệu.

Việc xây dựng các hệ thống dữ liệu lớn, các trung tâm dữ liệu, nền tảng chia sẻ... đòi hỏi ứng dụng mạnh mẽ thành tựu khoa học và công nghệ. Điều 24 Luật Dữ liệu 2024 quy định riêng về hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ và sử dụng dữ liệu. Luật nhấn mạnh phải “tập trung nguồn lực quốc gia cho phát triển, ứng dụng các nền tảng khoa học và công nghệ” phục vụ chuyển đổi số, đảm bảo an ninh, kinh tế - xã hội. Các nền tảng công nghệ được liệt kê bao gồm trí tuệ nhân tạo, điện toán đám mây, chuỗi khối (*blockchain*), truyền thông dữ liệu, Internet vạn vật (*IoT*), dữ liệu lớn (*big data*) và các công nghệ hiện đại khác. Đây chính là những công cụ then chốt để xây dựng hạ tầng dữ liệu tiên tiến, trong đó ⁽¹⁾AI giúp tự động phân loại, làm



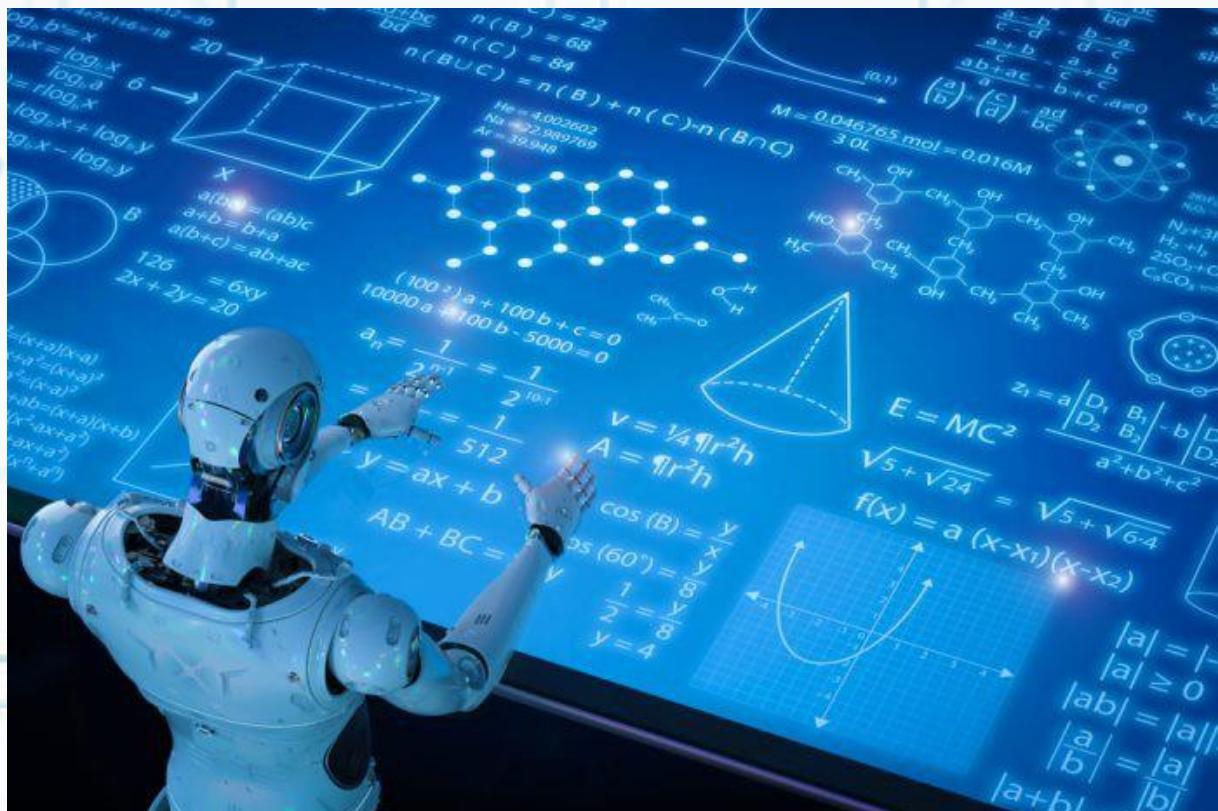
sạch dữ liệu; ⁽²⁾điện toán đám mây tạo khả năng lưu trữ, xử lý linh hoạt trên quy mô lớn; ⁽³⁾blockchain hỗ trợ xác thực và bảo mật chuỗi dữ liệu; ⁽⁴⁾IoT cung cấp nguồn dữ liệu không lồ thời gian thực từ các thiết bị kết nối. Nhờ khoa học và công nghệ, việc thu thập, xử lý dữ liệu trở nên hiệu quả hơn, giảm chi phí và sai sót. Ví dụ: áp dụng thuật toán AI có thể nhanh chóng phát hiện dữ liệu bất thường hoặc rò rỉ để kịp thời bảo vệ (*phòng chống tấn công mạng vào cơ sở dữ liệu*). Luật Dữ liệu cũng yêu cầu Chính phủ quy định việc thử nghiệm có kiểm soát các hoạt động Khoa học, Công nghệ và đổi mới sáng tạo về dữ liệu, cho phép sandbox để thử các công nghệ dữ liệu mới nhưng phải trong khuôn khổ giám sát để tránh rủi ro. Song song với xây dựng, khoa học và công nghệ cũng góp phần bảo vệ dữ liệu thông qua các giải pháp kỹ thuật như mã hóa dữ liệu mạnh (*crypto*), hệ thống sao lưu và phục hồi, tường lửa thế hệ mới, hệ thống phát hiện xâm nhập (*IDS/IPS*)... Luật Dữ liệu quy định dữ liệu thuộc danh mục bí mật nhà nước phải mã hóa bằng mật mã cơ yếu khi lưu trữ, truyền trên mạng, cho thấy vai trò cốt lõi của công nghệ mã hóa trong bảo vệ dữ liệu nhạy cảm. Như vậy, Khoa học và Công nghệ vừa là công cụ kiến tạo hạ tầng dữ liệu, vừa là lá chắn kỹ thuật bảo vệ dữ liệu trước các nguy cơ.

4.1.2.3. Đổi mới sáng tạo thúc đẩy khai thác và sử dụng dữ liệu.

Dữ liệu mở ra những hướng đi mới cho đổi mới sáng tạo, đồng thời chính đổi mới sáng tạo lại tạo ra phương thức khai thác dữ liệu hiệu quả hơn. Một hệ sinh thái đổi mới sáng tạo mạnh sẽ tận dụng được nguồn dữ liệu dồi dào để tạo ra các sản phẩm, dịch vụ mới. Luật Khoa học, Công nghệ và Đổi mới sáng tạo 2025 đặc biệt khuyến khích chia sẻ dữ liệu khoa học: “*Nhà nước khuyến khích chia sẻ dữ liệu, phương pháp, kết quả nghiên cứu khoa học, bao gồm sử dụng và phát triển công nghệ nguồn mở, bảo đảm minh bạch, dễ tiếp cận, đồng thời bảo đảm quyền sở hữu trí tuệ, bảo vệ dữ liệu cá nhân*”. Khoản này có nghĩa việc mở dữ liệu nghiên cứu (*open data*) sẽ thúc đẩy sáng tạo, nhưng phải cân bằng với việc bảo vệ dữ liệu cá nhân và quyền sở hữu trí tuệ, một sự hài hòa giữa tự do học thuật và an toàn dữ liệu. Luật Khoa học, Công nghệ và đổi mới sáng tạo 2025 cũng giao



nhiệm vụ xây dựng hạ tầng kỹ thuật để chia sẻ dữ liệu khoa học trên phạm vi quốc gia, đồng thời khuyến khích doanh nghiệp, cộng đồng tham gia đóng góp dữ liệu, kết quả nghiên cứu nguồn mở. Điều này sẽ làm phong phú thêm kho dữ liệu chung, từ đó giới nghiên cứu, khởi nghiệp có thể khai thác để tạo ra sản phẩm đổi mới sáng tạo.



Khoa học công nghệ thúc đẩy khai thác, sử dụng dữ liệu trong trí tuệ nhân tạo.

Ảnh: Techtalk.vn

4.1.2.4. Bản thân dữ liệu khi được chia sẻ rộng rãi sẽ kích thích các mô hình kinh doanh mới

Theo một nghiên cứu trên Tạp chí ICT Vietnam (*Hệ sinh thái dữ liệu: Chia sẻ dữ liệu mở ra sự đổi mới*), “hệ sinh thái dữ liệu” giúp khám phá những giá trị ẩn và thúc đẩy đà xuât giá trị vượt trội cho doanh nghiệp. Ví dụ: các công ty khởi nghiệp có thể kết hợp các bộ dữ liệu mở của chính phủ (như dữ liệu khí tượng, giao thông) với dữ liệu người dùng để sáng tạo dịch vụ thông minh (dự báo thời tiết theo nhu cầu, ứng dụng giao thông tối ưu...). Nếu không có dữ liệu mở và luồng dữ liệu minh bạch, nhiều vấn đề sẽ “khó nhìn thấy” và mô hình kinh doanh



sáng tạo khó nảy sinh. Do đó, việc mở dữ liệu và tạo hệ sinh thái dữ liệu gồm các bên cùng chia sẻ dữ liệu vì lợi ích chung là rất quan trọng. Hệ sinh thái này bao gồm bên cung cấp dữ liệu, bên sử dụng dữ liệu, các nền tảng trung gian, tất cả phối hợp để tạo nên giá trị mới từ dữ liệu.

4.1.2.5. Minh chứng trong chính sách mới ban hành.

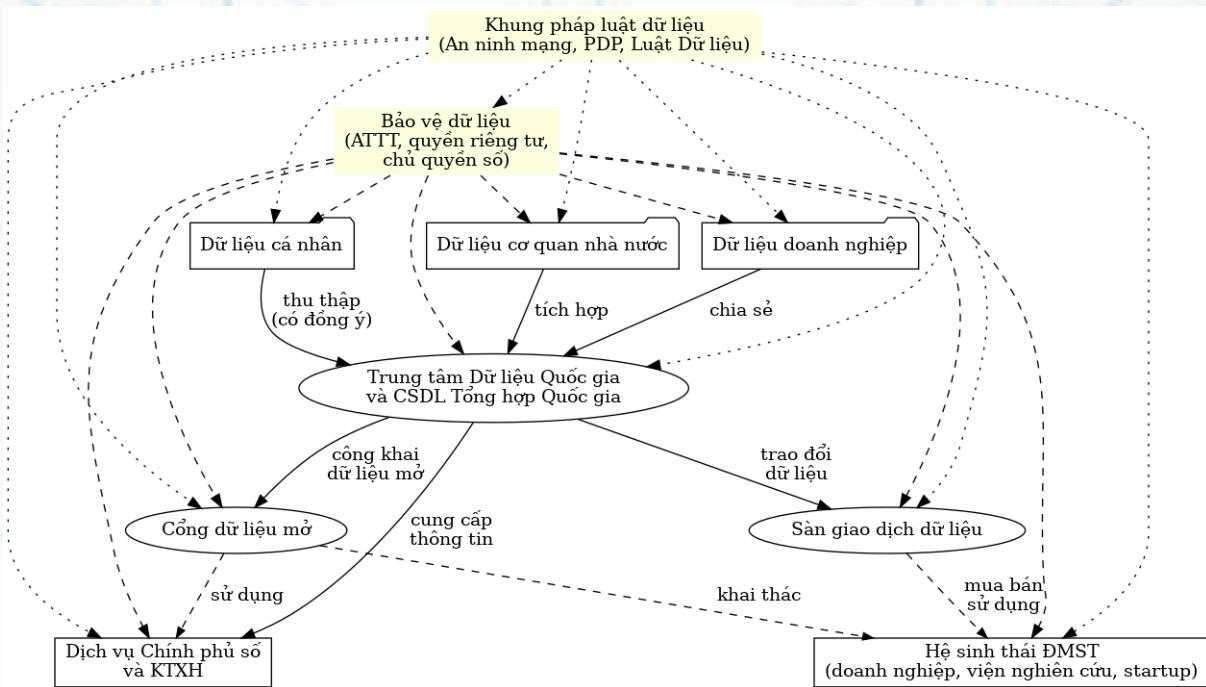
Luật Dữ liệu 2024 phản ánh rõ sự kết hợp giữa định hướng đổi mới sáng tạo và chính sách dữ liệu. Điều 24 Luật Dữ liệu yêu cầu hoạt động khoa học, công nghệ và đổi mới sáng tạo về dữ liệu phải phù hợp chiến lược phát triển dữ liệu quốc gia và “phát huy nội lực trong khoa học, công nghệ và đổi mới sáng tạo”. Nhà nước ưu tiên nguồn lực quốc gia cho các công nghệ dữ liệu để phục vụ chuyển đổi số và phát triển kinh tế - xã hội. Đây chính là tư duy lấy đổi mới sáng tạo làm động lực: đầu tư nghiên cứu phát triển các công nghệ chiến lược về dữ liệu (*AI, cloud, blockchain...*) để làm chủ công nghệ lõi. Tháng 7/2025, khi Luật Dữ liệu có hiệu lực, Bộ Công an đã thành lập mới 2 đơn vị trực thuộc Trung tâm dữ liệu quốc gia: Trung tâm Sáng tạo, khai thác dữ liệu và Phòng An ninh, an toàn hệ thống. Trung tâm Sáng tạo, khai thác dữ liệu được định vị là “bộ não đổi mới sáng tạo trong lĩnh vực dữ liệu”, với nhiệm vụ thúc đẩy khai thác dữ liệu quốc gia an toàn, hiệu quả. Động thái này cho thấy việc quản lý dữ liệu không chỉ đơn thuần hành chính, mà còn gắn chặt với sáng tạo, nghiên cứu để tìm ra giá trị mới từ dữ liệu. Bên cạnh đó, Quỹ Phát triển dữ liệu quốc gia vừa được thành lập theo Nghị định 160/2025/NĐ-CP, là quỹ tài chính ngoài ngân sách nhằm “thúc đẩy phát triển, khai thác, ứng dụng, quản trị dữ liệu quốc gia”, do Bộ Công an quản lý. Quỹ này có thể tài trợ cho các dự án khởi nghiệp dữ liệu, dự án nghiên cứu sử dụng dữ liệu lớn, qua đó tạo môi trường thuận lợi cho đổi mới sáng tạo dựa trên dữ liệu.

4.1.2.6. Sơ đồ hệ sinh thái dữ liệu và đổi mới sáng tạo:

Dữ liệu từ khu vực công và tư (*cơ quan nhà nước, doanh nghiệp*) và dữ liệu cá nhân được tích hợp qua Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia. Một phần dữ liệu được công khai qua cổng dữ liệu mở, phần khác giao dịch qua sàn dữ liệu. Các chủ thể trong hệ sinh thái đổi mới sáng tạo (*doanh nghiệp,*



viện nghiên cứu, startup) khai thác nguồn dữ liệu này để tạo sản phẩm, dịch vụ mới; đồng thời dữ liệu phục vụ dịch vụ công và phát triển kinh tế - xã hội. Khung pháp luật (Luật Dữ liệu, ANM, PDP...) cùng các biện pháp kỹ thuật bảo đảm bảo vệ dữ liệu (an ninh mạng, quyền riêng tư, chủ quyền số) cho toàn hệ sinh thái.



Hình ảnh: Sơ đồ hệ sinh thái dữ liệu - Trung tâm dữ liệu quốc gia và Cơ sở dữ liệu tổng hợp Quốc gia.Ảnh: Tạp chí TT&TT

Như vậy, khoa học, công nghệ vừa cung cấp phương tiện để xây dựng và củng cố hạ tầng dữ liệu (hệ thống lưu trữ, bảo mật, phân tích hiện đại), vừa là lĩnh vực hưởng lợi từ dữ liệu khi có nguồn dữ liệu lớn để nghiên cứu (ví dụ ứng dụng AI trên dữ liệu y tế để tạo thuốc mới). Đổi mới sáng tạo lại càng dựa trên dữ liệu, càng nhiều dữ liệu, càng nhiều ý tưởng mới này sinh và ngược lại, những ý tưởng sáng tạo lại thúc đẩy nhu cầu thu thập thêm dữ liệu, tạo vòng tuần hoàn phát triển. Chính vì lẽ đó, cả Nghị quyết 57-NQ/TW lẫn các Luật Dữ liệu 2024, Luật Khoa học, Công nghệ và Đổi mới sáng tạo 2025 đều nhấn mạnh tính gắn kết hữu cơ giữa chính sách dữ liệu với chính sách phát triển Khoa học, Công nghệ và đổi mới sáng tạo, bảo đảm hai lĩnh vực này hỗ trợ lẫn nhau hướng tới mục tiêu chung là phát triển quốc gia nhanh và bền vững trong kỷ nguyên số.



4.2. Nhiệm vụ, giải pháp để phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trở thành yếu tố quyết định, là điều kiện tiên quyết đưa nước ta phát triển giàu mạnh, hùng cường trong kỷ nguyên mới - kỷ nguyên vươn mình của Dân tộc

4.2.1. *Nhiệm vụ và giải pháp phát triển khoa học, công nghệ và đổi mới sáng tạo và chuyển đổi số theo Nghị quyết 57-NQ/TW*

Nghị quyết 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị đặt mục tiêu đến năm 2030 và tầm nhìn 2045 đưa Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số trở thành động lực chính của phát triển quốc gia. Để đạt mục tiêu này, Nghị quyết đề ra 7 nhóm nhiệm vụ và giải pháp trọng tâm:

4.2.1.1. *Nâng cao nhận thức, đổi mới tư duy và quyết tâm chính trị về phát triển Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số*

Cấp ủy Đảng, chính quyền các cấp phải có nhận thức đầy đủ tầm quan trọng của chuyển đổi số, Khoa học, Công nghệ và đổi mới sáng tạo; người đứng đầu phải trực tiếp chỉ đạo và cán bộ, đảng viên phải gương mẫu thực hiện. Nội dung chuyển đổi số, phát triển Khoa học, Công nghệ và đổi mới sáng tạo phải được đưa vào chương trình công tác hàng năm của từng cơ quan, đơn vị, địa phương và kết quả thực hiện sẽ là tiêu chí đánh giá cán bộ. Song song, cần đẩy mạnh tuyên truyền, giáo dục để tạo sự đồng thuận xã hội và khơi dậy tinh thần sáng tạo trong nhân dân, doanh nghiệp. Triển khai, phát động các phong trào như “học tập số”, khởi nghiệp sáng tạo, cải tiến năng suất... đồng thời tôn vinh kịp thời những nhà khoa học, nhà sáng chế, doanh nghiệp có thành tích, dù là sáng kiến nhỏ nhất. Đây là giải pháp “mềm” nhưng nền tảng: tạo chuyển biến về nhận thức và văn hóa đổi mới sáng tạo trong toàn xã hội.



Hình ảnh: Đồng chí Trần Thanh Mẫn chủ trì Hội nghị Nâng cao nhận thức, đột phá đổi mới tư duy về vị trí, vai trò của khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số. Ảnh: TTĐT Đảng bộ TP. Hồ Chí Minh

4.2.1.2. Hoàn thiện thể chế, tháo gỡ rào cản để Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số phát triển thuận lợi.

Quán triệt tinh thần “xoá bỏ mọi tư tưởng, quan niệm, rào cản đang cản trở sự phát triển; đưa thể chế thành một lợi thế cạnh tranh”. Cụ thể, cần sửa đổi, bổ sung đồng bộ các quy định pháp luật về khoa học công nghệ, đầu tư, mua sắm công, ngân sách, sở hữu trí tuệ, thuế... theo hướng tháo gỡ điểm nghẽn, giải phóng nguồn lực và khuyến khích đổi mới. Thủ tục quản lý nhiệm vụ Khoa học và Công nghệ sẽ được cải cách, đơn giản hóa tối đa thủ tục hành chính; giao quyền tự chủ cho các tổ chức Khoa học và Công nghệ sử dụng kinh phí nghiên cứu. Tiếp cận một cách mở và sáng tạo trong thể chế, cho phép thí điểm chính sách với vấn đề mới, chấp nhận rủi ro và độ trễ trong nghiên cứu Khoa học và Công nghệ. Đặc biệt, Nhà nước sẽ có cơ chế sandbox để doanh nghiệp thử nghiệm công nghệ mới dưới sự giám sát của Nhà nước, kèm chính sách miễn trừ trách nhiệm nếu xảy ra thiệt hại ngoài ý muốn trong quá trình thử nghiệm. Cùng với đó, hình thành các quỹ đầu tư mạo hiểm cho khởi nghiệp sáng tạo, ươm tạo công nghệ và chuyển đổi số. Nâng cao hiệu quả quản lý nhà nước về Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số, sắp xếp lại các viện nghiên cứu, trường đại học theo hướng gắn kết nghiên cứu với đào tạo; đầu tư nâng cấp các viện hàn lâm và các trung



tâm đổi mới sáng tạo trọng điểm quốc gia; sáp nhập hoặc giải thể những tổ chức Khoa học và Công nghệ hoạt động không hiệu quả. Nhà nước có chính sách hỗ trợ các tổ chức Khoa học và Công nghệ công lập hoạt động hiệu quả, trao quyền tự chủ về tổ chức, tài chính, nhân sự; cho phép nhà khoa học thành lập doanh nghiệp để thương mại hóa kết quả nghiên cứu. Nhóm giải pháp này nhằm tạo môi trường thèm khát thông thoáng, linh hoạt, khuyến khích đổi mới và loại bỏ các quy định lỗi thời cản trở sáng tạo.

4.2.1.3. Tăng cường đầu tư, hoàn thiện hạ tầng Khoa học, Công nghệ và đổi mới sáng tạo và hạ tầng số quốc gia.

Nhà nước ban hành Chương trình phát triển công nghệ và công nghiệp chiến lược, thành lập Quỹ đầu tư phát triển công nghiệp chiến lược, ưu tiên các lĩnh vực như quốc phòng, không gian, năng lượng, môi trường, công nghệ sinh học, trí tuệ nhân tạo, vật liệu tiên tiến, bán dẫn, công nghệ lượng tử, robot, tự động hóa.... Chính phủ dành ít nhất 15% ngân sách chi sự nghiệp Khoa học và Công nghệ để phục vụ nghiên cứu công nghệ chiến lược và có cơ chế hợp tác công tư (PPP) để phát triển các công nghệ này. Song song, xây dựng chiến lược nghiên cứu, ứng dụng Khoa học và Công nghệ trong khai thác không gian biển, không gian vũ trụ; phát triển hạ tầng năng lượng mới, năng lượng sạch để bảo đảm an ninh năng lượng cho Khoa học và Công nghệ. Phát triển hệ thống phòng thí nghiệm trọng điểm quốc gia tập trung cho công nghệ chiến lược, khuyến khích doanh nghiệp và tổ chức đầu tư xây dựng phòng thí nghiệm, trung tâm R&D.

Về hạ tầng số, Nhà nước đẩy mạnh ứng dụng và phát triển công nghệ số trên mọi lĩnh vực. Chính sách khuyến khích đầu tư, mua sắm, thuê dịch vụ số; có cơ chế đặc biệt để đào tạo, thu hút nhân tài số trong và ngoài nước. Xây dựng và dùng chung các nền tảng số quốc gia, vùng, bảo đảm liên thông dữ liệu giữa các ngành, lĩnh vực trên môi trường số, qua đó thúc đẩy hệ sinh thái kinh tế số.

Về viễn thông - ICT, định hướng phát triển hạ tầng Internet băng thông rộng tốc độ cao, mở rộng phủ sóng 5G/6G toàn quốc, phát triển hạ tầng truyền dẫn dữ liệu qua vệ tinh, tích hợp cảm biến và công nghệ số vào hạ tầng thiết yếu.



Đặc biệt, có chính sách hỗ trợ doanh nghiệp trong nước xây dựng trung tâm dữ liệu, điện toán đám mây và thu hút doanh nghiệp nước ngoài đặt trung tâm dữ liệu tại Việt Nam. Sớm hoàn thành và đưa vào hoạt động Trung tâm dữ liệu quốc gia, xây dựng thêm các trung tâm dữ liệu vùng. Phát huy hiệu quả dữ liệu quốc gia, dữ liệu bộ ngành, địa phương, bảo đảm liên thông, tích hợp, chia sẻ. Song song, xây dựng cơ chế để dữ liệu trở thành nguồn lực sản xuất quan trọng, trong đó pháp luật sẽ xác định quyền sở hữu, quyền kinh doanh dữ liệu và cách phân chia giá trị thu được từ dữ liệu. Phát triển kinh tế dữ liệu, thị trường dữ liệu và các sàn giao dịch dữ liệu, hướng tới hình thành ngành công nghiệp dữ liệu lớn của Việt Nam. Đồng thời phát triển mạnh mẽ ứng dụng AI dựa trên dữ liệu lớn trong các ngành trọng điểm.

4.2.1.4. Phát triển nguồn nhân lực chất lượng cao và trọng dụng nhân tài.

Nhân lực là yếu tố quyết định thành công. Do vậy, cần đổi mới căn bản giáo dục - đào tạo để cung cấp nguồn nhân lực chất lượng cao cho Khoa học, Công nghệ và đổi mới sáng tạo, chuyển đổi số. Cụ thể, có chính sách hấp dẫn (*tín dụng, học bổng, miễn giảm học phí*) thu hút học sinh, sinh viên giỏi theo học các ngành toán, lý, hóa, sinh, kỹ thuật và công nghệ then chốt, đặc biệt ở bậc sau đại học. Triển khai các chương trình đào tạo tài năng trong những lĩnh vực trọng điểm. Nhà nước ban hành cơ chế đặc thù thu hút nhân tài người Việt ở nước ngoài và chuyên gia quốc tế trình độ cao về làm việc tại Việt Nam. Các ưu đãi đặc biệt có thể bao gồm: nhập quốc tịch, điều kiện sở hữu nhà đất, thu nhập, môi trường làm việc... đủ hấp dẫn để giữ chân các nhà khoa học đầu ngành, các “tổng công trình sư” có khả năng dẫn dắt những nhiệm vụ Khoa học và Công nghệ quốc gia. Đồng thời, xây dựng và kết nối mạng lưới chuyên gia, nhà khoa học trong và ngoài nước để tận dụng chất xám toàn cầu. Với lĩnh vực mũi nhọn như trí tuệ nhân tạo (AI), sẽ xây dựng một số trường, trung tâm đào tạo tiên tiến chuyên sâu về AI để đào tạo nhân lực trình độ cao. Khuyến khích hợp tác công tư trong đào tạo nhân lực công nghệ số, phát triển nền tảng giáo dục số, mô hình đại học số, nâng cao năng lực số toàn dân. Song song, phát triển đội ngũ giảng viên, nhà khoa học có đủ



năng lực giảng dạy các lĩnh vực cơ bản lẫn công nghệ mới (*như chip bán dẫn, vi mạch, AI...*), đầy mạnh liên kết với đại học uy tín nước ngoài, hiện đại hóa chương trình và phương pháp đào tạo. Tất cả nhằm xây dựng thế hệ nguồn nhân lực có kỹ năng, sáng tạo, đáp ứng yêu cầu của kỷ nguyên số.

4.2.1.5. Thực đẩy chuyển đổi số trong hoạt động của hệ thống chính trị, nâng cao hiệu quả quản trị quốc gia.

Các cơ quan Đảng, Nhà nước phải tiên phong trong chuyển đổi số. Phải có lộ trình đưa toàn bộ hoạt động của cơ quan trong hệ thống chính trị lên môi trường số, bảo đảm liên thông, đồng bộ và bảo mật. Xây dựng nền tảng số dùng chung quốc gia, phát triển hệ thống giám sát, điều hành thông minh để nâng cao quản lý công. Đổi mới toàn diện việc giải quyết thủ tục hành chính theo hướng cung cấp dịch vụ công trực tuyến toàn trình, cá nhân hóa và dựa trên dữ liệu, không phụ thuộc địa giới hành chính. Điều này đòi hỏi ứng dụng mạnh mẽ các giải pháp chính phủ điện tử, khai thác các cơ sở dữ liệu dùng chung để phục vụ người dân tốt hơn.

Thu hút nhân lực Khoa học và Công nghệ và chuyển đổi số vào làm việc trong các cơ quan nhà nước (*có chính sách đặc thù về tuyển dụng, đãi ngộ để giữ chân người giỏi*). Bên cạnh đó, phát triển các nền tảng số an toàn, thúc đẩy hình thành công dân số; xây dựng một số mạng xã hội Việt Nam, tạo không gian mạng lành mạnh mang bản sắc Việt. Để quản lý rủi ro xã hội, cần xây dựng bộ quy tắc ứng xử trên không gian mạng, giảm thiểu tác động tiêu cực của công nghệ số. Ứng dụng công nghệ số để giám sát, thu thập dữ liệu về tài nguyên, môi trường phục vụ quản lý bền vững. Đặc biệt quan trọng là bảo đảm an toàn, an ninh mạng và chủ quyền quốc gia trên không gian mạng, bảo vệ an ninh dữ liệu của tổ chức, cá nhân. Quân đội và công an được giao nhiệm vụ từng bước ứng dụng công nghệ số trong chỉ huy tác chiến, làm chủ công nghệ cao để bảo vệ Tổ quốc trên không gian mạng. Đồng thời, đẩy mạnh phòng chống tội phạm công nghệ cao, lừa đảo trực tuyến; xây dựng thế trận quốc phòng, an ninh Nhân dân trên không gian mạng vững chắc.



Hình ảnh: Hội nghị Ban Chỉ đạo Chuyển đổi số trong các cơ quan đảng.

Ảnh: Báo Chính phủ

4.2.1.6. Thúc đẩy mạnh mẽ Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số trong doanh nghiệp.

Thứ nhất, có ưu đãi đặc biệt cho doanh nghiệp (*đặc biệt Doanh nghiệp vừa và nhỏ*) đầu tư cho chuyển đổi số, nghiên cứu, ứng dụng Khoa học và Công nghệ, đổi mới công nghệ nhằm nâng cao hiệu quả sản xuất kinh doanh. Đồng thời, thúc đẩy chuyển giao tri thức và đào tạo nhân lực Khoa học và Công nghệ thông qua doanh nghiệp FDI - nghĩa là tận dụng khu vực FDI để lan tỏa công nghệ cho doanh nghiệp trong nước.

- **Thứ hai**, xây dựng hệ sinh thái khởi nghiệp đổi mới sáng tạo: có chính sách đủ mạnh khuyến khích tinh thần khởi nghiệp về Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số, kết hợp với hỗ trợ, thu hút startup trong và ngoài nước khởi nghiệp tại Việt Nam.

- **Thứ ba**, hình thành một số doanh nghiệp công nghệ số chiến lược quy mô lớn của Việt Nam, đóng vai trò dẫn dắt hạ tầng số và chuyển đổi số quốc gia. Để



làm vậy, sẽ có cơ chế, chính sách hỗ trợ các doanh nghiệp công nghệ số nội địa phát triển (*về vốn, nhân lực*), cơ chế giao nhiệm vụ trọng điểm về chuyển đổi số cho các doanh nghiệp này, cũng như ưu đãi về đất đai, tín dụng, thuế để họ mạnh dạn nghiên cứu, thử nghiệm, sản xuất sản phẩm công nghệ số. Nhà nước cũng định hướng phát triển một số khu công nghiệp công nghệ số tập trung.

- **Thứ tư**, khuyến khích doanh nghiệp tái đầu tư cho R&D: thông qua các ưu đãi thuế thu nhập doanh nghiệp đối với chi phí nghiên cứu khoa học, phát triển công nghệ (*luật Khoa học, Công nghệ và đổi mới sáng tạo 2025 cũng đã cho phép doanh nghiệp được tính chi phí R&D vào chi phí được trừ khi tính thuế*).

- **Thứ năm**, thúc đẩy tiêu dùng số và sản xuất thông minh: khuyến khích người dân, doanh nghiệp sử dụng sản phẩm, dịch vụ trên môi trường số, phấn đấu kinh tế số chiếm tối thiểu 20% GDP vào 2025 và 30% vào 2030 (*theo các mục tiêu Quốc gia*). Đồng thời, đẩy mạnh sản xuất thông minh trong các ngành trọng điểm như nông nghiệp, tài chính, giáo dục, y tế, giao thông, logistics... để tăng năng suất và giá trị gia tăng. Tất cả những giải pháp trên nhằm tạo một cộng đồng doanh nghiệp số năng động, nơi doanh nghiệp Việt Nam vừa là đối tượng thụ hưởng chuyển đổi số (*nâng cao hiệu quả hoạt động*), vừa là tác nhân tạo ra sản phẩm, dịch vụ công nghệ số phục vụ xã hội.



Hình ảnh: Hội nghị Chuyển đổi số trong doanh nghiệp hướng tới nền kinh tế số bền vững.Ảnh: Bộ Kế hoạch và Đầu tư



4.2.1.7. *Tăng cường hợp tác quốc tế về Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số.*

Đẩy mạnh hợp tác nghiên cứu khoa học, phát triển công nghệ với các quốc gia tiên tiến, đặc biệt trong các lĩnh vực công nghệ mới như AI, công nghệ sinh học, công nghệ lượng tử, bán dẫn, năng lượng nguyên tử.... Đồng thời, có chính sách chủ động mua và tiếp nhận chuyển giao công nghệ tiên tiến phù hợp điều kiện Việt Nam. Nước ta tích cực tham gia xây dựng các quy tắc, tiêu chuẩn quốc tế về công nghệ mới để bảo đảm lợi ích quốc gia và an toàn cho mình. Khi tham gia các hiệp định quốc tế, chú trọng đưa nội dung nâng cao năng lực công nghệ và chuyển giao công nghệ vào các thỏa thuận. Những định hướng này cho thấy Việt Nam không “đóng cửa” tự phát triển mà sẽ hòa mình vào dòng chảy công nghệ thế giới, tranh thủ tri thức nhân loại để phát triển nhanh hơn, đồng thời đóng góp vào việc định hình luật chơi toàn cầu về công nghệ.



Hình ảnh: Trung tâm chuyển đổi số TP. Hồ Chí Minh ký kết hợp tác với Tổng lãnh sự quán Vương quốc Anh và Bắc Ai-len hợp tác trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số. Ảnh: Báo Nhân dân

Bảy nhóm nhiệm vụ, giải pháp nêu trên có mối quan hệ chặt chẽ và toàn diện, từ nhận thức, thể chế, hạ tầng, nhân lực, ứng dụng trong nhà nước và doanh



nghiệp, đến hội nhập quốc tế. Đây chính là “kim chỉ nam” để các cơ quan từ Trung ương tới địa phương xây dựng kế hoạch hành động cụ thể. Thực tế, ngay sau Nghị quyết 57, Chính phủ đã giao xây dựng Chương trình hành động triển khai Nghị quyết và Quốc hội cũng ban hành Nghị quyết 193/2025/QH15 thí điểm một số cơ chế, chính sách đặc biệt nhằm tạo đột phá cho Khoa học, Công nghệ và đổi mới sáng tạo, chuyển đổi số. Điều đó cho thấy quyết tâm chính trị rất lớn trong việc hiện thực hóa Nghị quyết 57, đưa Khoa học, Công nghệ và đổi mới sáng tạo và chuyển đổi số trở thành động lực chủ yếu của tăng trưởng.

4.2.2. Kiến nghị hoàn thiện pháp luật và chính sách phát triển dữ liệu bền vững gắn với đổi mới sáng tạo, đảm bảo chủ quyền số quốc gia

4.2.2.1. Hoàn thiện hệ thống pháp luật về dữ liệu

Để triển khai hiệu quả Luật Dữ liệu 2024 và thích ứng với bối cảnh dữ liệu biến đổi nhanh, Việt Nam cần tiếp tục hoàn thiện khung pháp luật theo hướng đồng bộ, linh hoạt và tiên tiến. Trước hết, cần sửa đổi các luật có liên quan để lồng ghép các quy định mới về dữ liệu. Luật An ninh mạng có thể bổ sung điều khoản yêu cầu phối hợp với cơ quan quản lý dữ liệu quốc gia (*Trung tâm dữ liệu quốc gia*) trong việc bảo vệ dữ liệu quan trọng, tránh tình trạng mỗi bên làm một hướng. Luật Giao dịch điện tử (*sửa đổi 2023*) nên được hướng dẫn thi hành theo hướng công nhận giá trị pháp lý của dữ liệu số trong các giao dịch dân sự, thương mại (ví dụ: *thừa nhận hợp đồng dữ liệu điện tử là hợp đồng hợp pháp*). Luật Sở hữu trí tuệ cần nghiên cứu cơ chế bảo hộ cơ sở dữ liệu (*database right*) - có thể bổ sung một mục riêng bảo hộ những tập hợp dữ liệu được đầu tư đáng kể về công sức, chi phí, qua đó khuyến khích doanh nghiệp đầu tư thu thập, làm giàu dữ liệu. Ngoài ra, nên xem xét ban hành quy định về quyền riêng tư và an toàn thông tin trên mạng ở cấp độ Luật (*hợp nhất và mở rộng Luật An toàn thông tin mạng, Luật An ninh mạng hiện hành*) để điều chỉnh những vấn đề mới như dữ liệu cá nhân trên không gian mạng xã hội, dữ liệu sinh trắc học, định danh điện tử... bảo đảm quyền con người trong môi trường số phù hợp Hiến pháp.



Về văn bản dưới luật, Chính phủ và các bộ cần nhanh chóng ban hành thông tư hướng dẫn chi tiết các nội dung Luật Dữ liệu giao. Ví dụ: danh mục dữ liệu quan trọng, dữ liệu cốt lõi do Thủ tướng ban hành cần sớm được xây dựng, với sự tham mưu của Bộ Công an và các cơ quan liên quan. Danh mục này nên liệt kê cụ thể những nhóm dữ liệu thuộc an ninh quốc gia, ngoại giao, tài chính vĩ mô, sức khỏe cộng đồng... để làm căn cứ áp dụng các biện pháp bảo vệ đặc thù. Tiếp đó, quy trình đánh giá tác động và cấp phép chuyển dữ liệu xuyên biên giới (*theo Điều 23 Luật Dữ liệu*) cần được quy định rõ trong nghị định (*thực tế Nghị định 165/2025/NĐ-CP đã đề cập mẫu hồ sơ, báo cáo đánh giá tác động chuyển dữ liệu xuyên biên giới*). Việc phân công trách nhiệm quản lý nhà nước về dữ liệu cũng phải minh bạch: nên xác định rõ vai trò của Bộ Công an (*quản lý Trung tâm dữ liệu quốc gia, bảo vệ dữ liệu trọng yếu*), Bộ Khoa học và Công nghệ (*quản lý hạ tầng kết nối, tiêu chuẩn kỹ thuật dữ liệu, cổng dữ liệu mở, thúc đẩy khai thác dữ liệu cho nghiên cứu, đổi mới*).... Có thể xem xét cơ chế thành lập một Ủy ban quốc gia về dữ liệu hoặc trao thêm quyền cho Ủy ban Chuyển đổi số quốc gia để điều phối chung các chính sách dữ liệu, tránh cát cứ theo ngành.



Hình ảnh: Tổng Bí thư Tô Lâm cùng các đồng chí lãnh đạo, nguyên lãnh đạo Đảng, Nhà nước thăm khu trưng bày tại Hội nghị toàn quốc về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển. Ảnh: Tạp chí Cộng sản



4.2.2.2. Chính sách phát triển dữ liệu bền vững gắn với đổi mới sáng tạo

Phát triển dữ liệu bền vững đòi hỏi một tầm nhìn dài hạn, kết hợp giữa đầu tư hạ tầng, phát triển nhân lực và cơ chế khuyến khích đổi mới.

- **Trước hết**, Nhà nước cần đầu tư xây dựng và vận hành hiệu quả Trung tâm dữ liệu quốc gia và các trung tâm dữ liệu vùng theo đúng tinh thần Nghị quyết 57 và Luật Dữ liệu. Hạ tầng dữ liệu phải đáp ứng tiêu chuẩn quốc tế, đảm bảo an toàn, dự phòng và “xanh” (*tiết kiệm năng lượng*). Song song đó, phát triển Cơ sở dữ liệu tổng hợp quốc gia đòi hỏi thu thập, tích hợp hầu hết các cơ sở dữ liệu hiện có của bộ, ngành, địa phương. Quá trình này nên được thực hiện tuân tự theo lộ trình Thủ tướng phê duyệt, ưu tiên tích hợp các Cơ sở dữ liệu Quốc gia cốt lõi (*dân cư, đất đai, doanh nghiệp, tài chính công,...*) trong giai đoạn đầu, sau đó mở rộng sang dữ liệu chuyên ngành. Để dữ liệu “sống” và tăng giá trị theo thời gian, chính sách phải khuyến khích cập nhật, bổ sung dữ liệu liên tục. Một ý tưởng là xây dựng cơ chế “crowdsourcing dữ liệu” cho phép doanh nghiệp, người dân đóng góp dữ liệu vào kho dữ liệu mở quốc gia và được hưởng lợi (ví dụ *hưởng ưu đãi hoặc danh hiệu nếu đóng góp dữ liệu hữu ích*).

- **Thứ hai**, kết hợp đổi mới sáng tạo, mô hình vườn ươm dữ liệu có thể được phát triển: Nhà nước cung cấp một phần dữ liệu mở chất lượng cao và hạ tầng tính toán, các doanh nghiệp khởi nghiệp và viện nghiên cứu có thể đăng ký tham gia “vườn tạo” các giải pháp trên nền dữ liệu đó. Mô hình này tương tự vườn ươm công nghệ nhưng trọng tâm là dữ liệu, giúp khám phá tiềm năng dữ liệu vào các ứng dụng mới.Thêm vào đó, chính sách ưu đãi thuế, tín dụng cho doanh nghiệp dữ liệu nên được thiết kế. Ví dụ: doanh nghiệp đầu tư cho hoạt động R&D dữ liệu hoặc thành lập phòng thí nghiệm dữ liệu có thể được khấu trừ thuế thu nhập doanh nghiệp ở mức cao (*Luật Khoa học, Công nghệ và đổi mới sáng tạo 2025 đã có quy định chi phí nghiên cứu được trừ thuế, có thể bổ sung cụ thể cho lĩnh vực dữ liệu*). Cũng có thể thành lập các giải thưởng đổi mới sáng tạo về dữ liệu cấp quốc gia để vinh danh tổ chức, cá nhân xuất sắc



trong khai thác dữ liệu phục vụ kinh tế - xã hội, qua đó thúc đẩy phong trào sáng tạo dựa trên dữ liệu.

- **Thứ ba**, phát triển nhân lực dữ liệu. Cần có chiến lược đào tạo bài bản “nhà khoa học dữ liệu”, chuyên gia phân tích dữ liệu trong các trường đại học và viện nghiên cứu. Đồng thời, nâng cao nhận thức và kỹ năng về dữ liệu cho cán bộ công chức và cộng đồng doanh nghiệp. Nghị quyết 57 nhấn mạnh việc “có cơ chế, chính sách đặc biệt về nhân tài” và thu hút nhân lực trình độ cao trong lĩnh vực chuyên đổi số. Vì vậy, kiến nghị xây dựng chương trình học bổng, đãi ngộ để thu hút người giỏi về dữ liệu làm việc cho các cơ quan nhà nước trọng yếu (*nhiều Trung tâm dữ liệu quốc gia, Cục An ninh mạng...*). Song song, đẩy mạnh hợp tác quốc tế về đào tạo, trao đổi chuyên gia dữ liệu, học hỏi các nước đi trước.



Hình ảnh: Hội nghị Sơ kết công tác của phát triển khoa học công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06. Nguồn ảnh: Báo Chính phủ

4.2.2.3. Đảm bảo chủ quyền số quốc gia

Chủ quyền số là khía cạnh then chốt khi nói đến phát triển dữ liệu trong bối cảnh toàn cầu hóa. Việt Nam cần thực thi các biện pháp để vừa hội nhập, chia sẻ dữ liệu phục vụ phát triển, vừa giữ vững quyền tự chủ, kiểm soát đối với dữ liệu quốc gia. Trước hết, tiếp tục duy trì và hoàn thiện yêu cầu nội địa hóa dữ liệu quan



trọng. Những dữ liệu được xác định là “cốt lõi” đối với an ninh quốc gia (*nhiều dữ liệu về quốc phòng, an ninh, thông tin tài chính quốc gia, dân cư chiến lược*) phải được lưu trữ, xử lý trên lãnh thổ Việt Nam (*không có ngoại lệ*). Nghị định hướng dẫn Luật Dữ liệu có thể sẽ quy định chi tiết tiêu chí và danh mục dữ liệu phải lưu trữ trong nước, cũng như quy trình đánh giá an ninh dữ liệu trước khi cho phép chuyển ra nước ngoài. Công tác này đòi hỏi năng lực thẩm định và phối hợp giữa cơ quan an ninh, cơ quan chủ quản dữ liệu và chuyên gia công nghệ. Kế tiếp, Việt Nam cần xây dựng năng lực hạ tầng độc lập: bảo đảm các trung tâm dữ liệu trong nước đạt chuẩn, có khả năng phục vụ nhu cầu lưu trữ, điện toán của các doanh nghiệp và cơ quan nhà nước, giảm phụ thuộc vào dịch vụ điện toán đám mây nước ngoài. Nghị quyết 57/TW chỉ rõ cần thu hút doanh nghiệp nước ngoài đặt trung tâm dữ liệu, điện toán đám mây tại Việt Nam và hình thành hạ tầng tính toán đạt tiêu chuẩn quốc tế, tiêu chuẩn xanh. Điều này hàm ý vừa hợp tác quốc tế, vừa đặt điều kiện để các công ty ngoại giao phần vào hạ tầng dữ liệu nội địa thay vì chỉ đưa dữ liệu ra ngoài.

Một yếu tố khác của chủ quyền số là an ninh dữ liệu và an ninh mạng. Phải xây dựng năng lực tự chủ về công nghệ an ninh mạng, như Nghị quyết 57 đề ra: “từng bước tự chủ công nghệ chiến lược; ưu tiên nguồn lực đầu tư cho phát triển công nghệ”, trong đó có công nghệ bảo vệ dữ liệu. Việt Nam nên đầu tư phát triển các sản phẩm an ninh mạng “Make in Vietnam” (*thiết bị tường lửa, hệ thống phát hiện xâm nhập, nền tảng phân tích giám sát*) để triển khai trong các hệ thống dữ liệu quốc gia, tránh nguy cơ bị cài cắm lỗ hổng từ sản phẩm ngoại nhập. Đồng thời, thiết lập quy trình kiểm toán, đánh giá an ninh dữ liệu định kỳ cho các cơ quan, doanh nghiệp quản lý dữ liệu cốt lõi. Luật Dữ liệu đã yêu cầu chủ quản dữ liệu cốt lõi phải định kỳ đánh giá rủi ro và báo cáo cơ quan an ninh phối hợp bảo vệ. Quy định này cần thực thi nghiêm, có thể bằng cách giao Bộ Công an, Bộ Quốc phòng tổ chức thanh tra an ninh dữ liệu hàng năm tại các đơn vị trọng yếu.



Hình ảnh: Lực lượng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao tác chiến trên không gian mạng. Ảnh: Tạp chí Cộng sản

Mặt khác, để bảo vệ chủ quyền số, Việt Nam phải tích cực tham gia định hình luật chơi quốc tế về dữ liệu. Hiện nay, các khuôn khổ như CPTPP, RCEP... đều có chương về thương mại điện tử, trong đó có quy định không cản trở luân chuyển dữ liệu xuyên biên giới một cách phi lý. Việt Nam nên tận dụng các ngoại lệ về an ninh và trật tự công cộng trong các hiệp định này để duy trì quy định bảo vệ dữ liệu quan trọng. Song song, chuẩn bị năng lực thương thảo các hiệp định song phương về chia sẻ dữ liệu (ví dụ dữ liệu hành pháp, tư pháp) bảo đảm có đi có lại, tôn trọng luật pháp mỗi bên. Một kiến nghị cụ thể là xúc tiến đàm phán thỏa thuận với Liên minh Châu Âu về công nhận tương đương bảo vệ dữ liệu cá nhân (*Adequacy Decision*), điều này giúp dữ liệu cá nhân có thể chuyển giữa Liên minh Châu Âu-Việt Nam thuận lợi phục vụ thương mại, đồng thời khẳng định vị thế Việt Nam về bảo vệ quyền riêng tư.

Cuối cùng, không thể không nhắc đến vai trò của nhận thức xã hội trong đảm bảo chủ quyền số. Cần triển khai các chương trình tuyên truyền để nâng cao ý thức của doanh nghiệp và người dân về an ninh dữ liệu. Mỗi cá nhân, tổ chức



hiểu rõ giá trị dữ liệu của mình và quốc gia, từ đó chủ động bảo vệ (*như không tùy tiện cung cấp dữ liệu nhạy cảm cho đối tác nước ngoài, cảnh giác với gián điệp dữ liệu*). Chỉ khi toàn xã hội cùng chung tay, chủ quyền số quốc gia mới được củng cố vững chắc từ gốc rễ.

Tóm lại, các kiến nghị trên đây nhằm xây dựng một hệ sinh thái pháp luật và chính sách dữ liệu hoàn chỉnh, luật pháp rõ ràng, đầy đủ và hài hòa; chính sách thúc đẩy đầu tư, nhân lực, hạ tầng cho dữ liệu; đồng thời mọi biện pháp đều đặt trong mục tiêu tối thượng là phát triển đất nước dựa trên đổi mới sáng tạo, gắn liền với bảo vệ vững chắc chủ quyền quốc gia trong kỷ nguyên số. Việc triển khai những kiến nghị này đòi hỏi quyết tâm và phối hợp chặt chẽ từ Chính phủ, Quốc hội đến các bộ ngành, địa phương, cùng sự tham gia của cộng đồng doanh nghiệp và xã hội. Đây chính là chìa khóa để Việt Nam khai thác tối đa “mỏ vàng” dữ liệu cho phát triển bền vững, đồng thời tự tin, tự chủ trong không gian số toàn cầu.



PHỤ LỤC

Phản bác quan điểm xuyên tạc “Luật Dữ liệu bóp nghẹt sáng tạo”

Phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số được Đảng và Nhà nước ta xác định là yếu tố quyết định, điều kiện tiên quyết và thời cơ tốt nhất để Việt Nam trở thành quốc gia giàu mạnh, hùng cường trong kỷ nguyên mới - kỷ nguyên vươn mình của dân tộc. Nhận thức rõ tầm quan trọng đó, thời gian qua nước ta đã xây dựng một hệ thống chính sách, pháp luật đồng bộ nhằm thúc đẩy các lĩnh vực này, nổi bật là việc ban hành Luật Dữ liệu 2024, văn bản pháp luật đầu tiên điều chỉnh toàn diện về quản trị, phát triển, bảo vệ và khai thác dữ liệu số. Luật Dữ liệu cùng các đạo luật liên quan như Luật An ninh mạng 2018, Luật An toàn thông tin mạng 2015, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, và mới đây là Luật Khoa học, Công nghệ và Đổi mới sáng tạo 2025, đã tạo nền tảng pháp lý vững chắc cho công cuộc chuyển đổi số quốc gia.

Tuy nhiên, song hành với những nỗ lực đó, các thế lực thù địch và một số truyền thông nước ngoài thiếu thiện chí không ngừng tìm cách xuyên tạc bản chất các chính sách quản lý dữ liệu và Internet của Việt Nam. Ngay sau khi Quốc hội thông qua Luật Dữ liệu (ngày 30/11/2024), những kênh như RFA, BBC, VOA và tổ chức phản động Việt Tân đã quy chụp rằng luật này sẽ “gây tổn hại cho các công ty nước ngoài”, “xâm phạm quyền riêng tư” và “bóp nghẹt sự sáng tạo”. Họ cố tình xoáy vào các quy định yêu cầu tổ chức, cá nhân cung cấp dữ liệu cho cơ quan nhà nước trong tình huống đặc biệt (khẩn cấp, đe doạ an ninh quốc gia, thảm họa, chống bạo loạn/khổng bố) và quy định phải được chấp thuận mới chuyển giao dữ liệu cốt lõi ra nước ngoài, nhằm bóp méo mục đích thực sự của luật. Thực chất, những luận điệu này đã “thay đen đổi trắng” bản chất vấn đề. Mục tiêu của việc tăng cường quản lý dữ liệu ở Việt Nam là bảo vệ chủ quyền và an ninh quốc gia, đảm bảo khả năng ứng phó kịp thời với tình huống khẩn cấp, bảo vệ người dân trước nguy cơ khủng bố, bạo loạn, đồng thời bảo đảm an ninh, an toàn thông tin và bảo vệ các tài sản số quan trọng của quốc gia. Việc ban hành Luật Dữ liệu là hết sức cần thiết, không chỉ để bảo vệ đất nước và duy trì ổn định xã hội, mà còn để bảo vệ quyền lợi



của người dân và nhà đầu tư nước ngoài tham gia kinh tế số Việt Nam. Song song đó, Việt Nam đang xây dựng Luật Bảo vệ dữ liệu cá nhân 2025 nhằm nâng cao hơn nữa quyền và lợi ích hợp pháp của người dân đối với dữ liệu, cụ thể hóa cam kết quốc tế của Việt Nam trong việc bảo đảm quyền con người.

BBC NEWS TIẾNG VIỆT

Tin chính Việt Nam Thế giới Kinh tế Thể thao Video

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



GETTYIMAGES/VGP

Tin chính

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

4 giờ trước

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

5 giờ trước

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

15 tháng 8 năm 2025

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

Thực tế, nhiều nước trên thế giới cũng có luật về quản lý, khai thác dữ liệu: Liên minh Châu Âu có Đạo luật Dữ liệu áp dụng trên 27 nước, Hàn Quốc có Luật Dữ liệu mở, Trung Quốc có Luật Bảo vệ Thông tin cá nhân... cho thấy Việt Nam không hề “đi ngược dòng”, mà đang theo kịp xu thế chung nhằm xây dựng môi trường số an toàn, lành mạnh, bền vững. Tương tự, khi Chính phủ ban hành Nghị định 147/2024/NĐ-CP về quản lý dịch vụ Internet (trong đó quy định xác thực danh tính người dùng trên mạng xã hội), các đối tượng xấu cũng lu loa rằng đây là “xâm phạm quyền riêng tư”, “hạn chế tự do ngôn luận, tự do Internet”. Họ cố tình bỏ qua thực tế rằng nhiều quốc gia cũng áp dụng biện pháp quản lý chặt chẽ không gian mạng: Trung Quốc yêu cầu đăng ký tên thật khi dùng mạng xã hội từ năm 2017, Mỹ có các quy định về an ninh mạng và chống khủng bố trực tuyến, Liên minh Châu Âu ban hành Đạo luật Dịch vụ Kỹ thuật số (DSA) yêu cầu các



tập đoàn công nghệ lớn chịu trách nhiệm pháp lý cao hơn trong việc xử lý tin giả, nội dung độc hại trên mạng.

Trong bối cảnh xã hội bùng nổ kéo theo tin giả, lừa đảo trực tuyến tràn lan, chỉ 9 tháng đầu 2024, Bộ TT&TT đã ghi nhận hơn 22.200 lượt phản ánh về lừa đảo trực tuyến (*hơn 80% vụ chiếm đoạt tài sản qua các hình thức lừa đảo số, và 70% diễn ra trên mạng xã hội như Zalo, Facebook*) thì Nghị định 147 ra đời như “lá chắn” mới, cùng với Luật An ninh mạng 2018 và các quy định liên quan, giúp bảo vệ chủ quyền, an ninh quốc gia và bảo vệ người dân trước những mối đe dọa từ thế giới ảo. Có thể khẳng định: trong thế giới ngày càng số hóa, việc quản lý tốt dữ liệu và không gian mạng là yêu cầu cấp thiết để bảo vệ an ninh quốc gia và quyền lợi hợp pháp của người dân. Nhà nước Việt Nam nhất quán tôn trọng và bảo đảm các quyền tự do cơ bản của con người, trong đó có tự do ngôn luận, tự do báo chí, tự do tiếp cận thông tin và tự do Internet. Đồng thời, Việt Nam tích cực hoàn thiện pháp luật nhằm bảo vệ quyền của người dân được an toàn trên không gian mạng. Đó là sự thật không thể bóp méo, những luận điệu cố tình xuyên tạc chính sách dữ liệu và Internet ở Việt Nam thực chất chỉ là thủ đoạn nhằm kích động chống phá chế độ, kìm hãm đà phát triển của đất nước

Luật Dữ liệu năm 2024 (Luật số 60/2024/QH15) được Quốc hội thông qua với tỷ lệ tán thành rất cao (94,15%) và sẽ có hiệu lực từ 01/7/2025. Đây là đạo luật đầu tiên xác lập hành lang pháp lý toàn diện về dữ liệu số, trong đó đặc biệt nhấn mạnh việc ứng dụng khoa học-công nghệ và đổi mới sáng tạo ở mọi khâu của chu trình dữ liệu. Ngay Điều 6 về Chính sách của Nhà nước đã khẳng định “Dữ liệu là tài nguyên”, Nhà nước huy động mọi nguồn lực để “làm giàu dữ liệu, phát triển dữ liệu trở thành tài sản”. Luật ưu tiên phát triển dữ liệu phục vụ chuyển đổi số quốc gia gắn với bảo đảm quốc phòng, an ninh; đầu tư xây dựng Cơ sở dữ liệu tổng hợp quốc gia và Trung tâm dữ liệu quốc gia đáp ứng yêu cầu Chính phủ số, kinh tế số, xã hội số. Đặc biệt, khoản 5 Điều 6 nêu rõ Nhà nước khuyến khích cơ quan, tổ chức, cá nhân “đầu tư, nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, đổi mới sáng tạo, ứng dụng trong lĩnh vực dữ liệu; xây dựng trung tâm



lưu trữ, xử lý dữ liệu tại Việt Nam; phát triển thị trường dữ liệu”. Đây là cơ sở pháp lý rất quan trọng để thúc đẩy hoạt động khoa học-công nghệ (KH-CN) và đổi mới sáng tạo nhằm phát triển hạ tầng và hệ sinh thái dữ liệu trong nước.

Luật Dữ liệu 2024 cũng đề cao hợp tác quốc tế về khoa học, công nghệ trong lĩnh vực dữ liệu. Điều 7 liệt kê các nội dung hợp tác như: đào tạo nhân lực; nghiên cứu khoa học, ứng dụng khoa học, công nghệ trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; chuyển giao công nghệ tiên tiến, đầu tư hạ tầng trung tâm dữ liệu; tham gia xây dựng tiêu chuẩn quốc tế về dữ liệu....

Như vậy, Việt Nam khuyến khích trao đổi tri thức và công nghệ với các nước nhằm nắm bắt xu hướng quản trị dữ liệu hiện đại. Ở cấp quản lý nhà nước, Điều 8 Luật Dữ liệu xác định nội dung quản lý nhà nước về dữ liệu bao gồm việc “nghiên cứu, ứng dụng khoa học và công nghệ về dữ liệu; phát triển sản phẩm, dịch vụ về dữ liệu; quản lý, giám sát, phát triển thị trường dữ liệu”. Các cơ quan quản lý cũng có trách nhiệm đào tạo nguồn nhân lực và hợp tác quốc tế về dữ liệu. Điều này thể hiện sự tích hợp giữa chính sách dữ liệu với phát triển khoa học, công nghệ và nguồn nhân lực chất lượng cao ngay trong khuôn khổ luật.

Quan trọng nhất, Luật Dữ liệu 2024 dành Điều 24 để quy định cụ thể về “Hoạt động khoa học, công nghệ và đổi mới sáng tạo trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu”. Luật yêu cầu các hoạt động khoa học, công nghệ và đổi mới sáng tạo trong lĩnh vực dữ liệu phải phù hợp với Chiến lược dữ liệu quốc gia, phát huy nội lực và tuân thủ các nguyên tắc quản trị dữ liệu. Khoản 2 Điều 24 liệt kê các nền tảng khoa học, công nghệ cốt lõi cho dữ liệu, bao gồm: trí tuệ nhân tạo (AI), điện toán đám mây, chuỗi khối (blockchain), truyền thông dữ liệu, Internet vạn vật (IoT), dữ liệu lớn (Big Data) và các công nghệ hiện đại khác. Đây đều là những công nghệ tiên phong của cuộc Cách mạng công nghiệp 4.0, được luật xác định là nền tảng để xây dựng, xử lý và khai thác dữ liệu. Luật yêu cầu tập trung nguồn lực quốc gia để phát triển, ứng dụng các nền tảng này phục vụ chuyển đổi số, bảo đảm quốc phòng, an ninh và phát triển kinh tế-xã hội. Đồng thời, giao Chính phủ ban hành quy định chi tiết để quản lý, phát triển và thử nghiệm



có kiểm soát các hoạt động nghiên cứu, ứng dụng khoa học, công nghệ và đổi mới sáng tạo về dữ liệu. Nói cách khác, luật mở đường cho việc thử nghiệm những công nghệ mới như AI, Big Data... trong lĩnh vực dữ liệu thông qua cơ chế “sandbox” (thử nghiệm trong phạm vi kiểm soát), nhằm thúc đẩy sáng tạo nhưng vẫn có cơ chế kiểm soát rủi ro hợp lý.

Cùng với chính sách khuyến khích, Luật Dữ liệu 2024 còn tạo cơ chế tài chính hỗ trợ phát triển khoa học, công nghệ về dữ liệu. Điều 29 luật giao Chính phủ thành lập Quỹ Phát triển dữ liệu Quốc gia (quỹ tài chính nhà nước ngoài ngân sách) nhằm thúc đẩy phát triển, khai thác, ứng dụng và quản trị dữ liệu quốc gia. Thực hiện luật, Chính phủ đã ban hành Nghị định 160/2025/NĐ-CP để triển khai quỹ này với vốn điều lệ tối thiểu 1.000 tỷ đồng, do Bộ Công an quản lý. Quỹ sẽ tài trợ cho các hoạt động nghiên cứu, phát triển hạ tầng dữ liệu, thúc đẩy ứng dụng các công nghệ mới (AI, Big Data, blockchain...), đặc biệt chú trọng hỗ trợ khu vực nông thôn, miền núi, hải đảo nhằm thu hẹp khoảng cách số. Song song đó, Luật Dữ liệu áp dụng phương thức quản lý theo hướng “hậu kiểm” thay vì “tiền kiểm”: cơ quan nhà nước không can thiệp trước vào hoạt động xử lý, kinh doanh dữ liệu, mà chủ yếu giám sát và xử lý khi có dấu hiệu vi phạm. Cách tiếp cận này giảm gánh nặng thủ tục hành chính, trao quyền tự chủ nhiều hơn cho doanh nghiệp trong bảo mật và chia sẻ dữ liệu, qua đó khuyến khích đổi mới sáng tạo trong lĩnh vực dữ liệu.

Bên cạnh Luật Dữ liệu 2024, việc Quốc hội thông qua Luật Khoa học, Công nghệ và Đổi mới sáng tạo 2025 đã tạo khung pháp lý toàn diện để thúc đẩy hoạt động khoa học, công nghệ và đổi mới sáng tạo, đồng thời bổ sung nhiều quy định gắn với chuyển đổi số và dữ liệu. Luật mới mở rộng phạm vi điều chỉnh, nhấn mạnh mẽ yếu tố đổi mới sáng tạo và đưa ra các cơ chế linh hoạt nhằm khuyến khích nghiên cứu, ứng dụng công nghệ. Đáng chú ý, luật dành riêng Điều 20 quy định về chuyển đổi số trong hoạt động khoa học, công nghệ và đổi mới sáng tạo. Nhà nước được giao nhiệm vụ “thúc đẩy chuyển đổi số toàn diện trong lĩnh vực khoa học, công nghệ và đổi mới sáng tạo” thông qua phát triển hạ tầng



số, cung cấp dịch vụ công trực tuyến, số hóa dữ liệu và tự động hóa quy trình nghiệp vụ nhằm nâng cao hiệu quả, minh bạch. Luật khuyến khích ứng dụng công nghệ dữ liệu lớn (Big Data) và trí tuệ nhân tạo để tăng cường hiệu quả hoạt động khoa học, công nghệ và đổi mới sáng tạo. Đồng thời, Chính phủ sẽ đầu tư xây dựng và vận hành Nền tảng số quản lý khoa học, công nghệ và đổi mới sáng tạo quốc gia cũng như Hệ thống thông tin quốc gia về khoa học, công nghệ và đổi mới sáng tạo, bảo đảm kết nối tập trung để lưu trữ, chia sẻ và công khai kết quả hoạt động khoa học, công nghệ cho cộng đồng. Quy định này cho thấy pháp luật yêu cầu ứng dụng công nghệ số và quản trị dữ liệu ngay trong hoạt động quản lý khoa học, ví dụ: sử dụng nền tảng số quốc gia để thu thập dữ liệu thông kê nhiệm vụ khoa học, công nghệ, chia sẻ thông tin kết quả nghiên cứu, qua đó minh bạch hóa và liên thông dữ liệu khoa học.

Luật khoa học, công nghệ và ĐMST 2025 cũng đề cao việc mở và chia sẻ dữ liệu khoa học. Cụ thể, Điều 32 khuyến khích chia sẻ dữ liệu, phương pháp, kết quả nghiên cứu khoa học, trong đó nhấn mạnh phát triển công nghệ nguồn mở, đồng thời bảo đảm minh bạch, dễ tiếp cận nhưng vẫn tôn trọng quyền sở hữu trí tuệ và bảo vệ dữ liệu cá nhân. Nhà nước sẽ xây dựng hạ tầng kỹ thuật đáp ứng yêu cầu chia sẻ dữ liệu và công bố kết quả nghiên cứu khoa học một cách bảo mật, có khả năng tương tác và tái sử dụng. Doanh nghiệp và cộng đồng được khuyến khích tham gia sử dụng, đóng góp dữ liệu và kết quả nghiên cứu vào các dự án nguồn mở. Đây chính là định hướng khoa học mở (open science), tận dụng sức mạnh của dữ liệu và tri thức chia sẻ để thúc đẩy sáng tạo.

Đặc biệt, nhằm tạo môi trường thuận lợi cho đổi mới sáng tạo, Luật khoa học, công nghệ và ĐMST 2025 đưa ra cơ chế “thử nghiệm có kiểm soát” (sandbox). Theo đó, cơ quan có thẩm quyền có thể cho phép tổ chức, doanh nghiệp thử nghiệm các công nghệ, giải pháp, sản phẩm, dịch vụ, mô hình kinh doanh mới chưa có quy định pháp luật, trong phạm vi và thời gian giới hạn. Nguyên tắc thử nghiệm phải công khai, bình đẳng và tuân thủ yêu cầu về an ninh, an toàn. Đáng chú ý, luật quy định miễn trừ hoặc loại trừ trách nhiệm pháp lý cho các cá nhân,



tổ chức tham gia thử nghiệm nếu đã tuân thủ đúng quy định sandbox và hành động với động cơ trong sáng, vì lợi ích chung. Ví dụ: luật cho phép miễn trách nhiệm dân sự, hành chính, thậm chí hình sự đối với rủi ro phát sinh trong quá trình nghiên cứu, thử nghiệm, ứng dụng tiến bộ khoa học, công nghệ khi các chủ thể đã tuân thủ quy trình sandbox. Quy định khoan dung pháp lý này giúp các nhà khoa học, doanh nghiệp yên tâm thử nghiệm những ý tưởng đột phá (kể cả trong lĩnh vực dữ liệu, ví dụ thử nghiệm thuật toán AI mới trên tập dữ liệu), không lo bị xử phạt nếu xảy ra rủi ro ngoài ý muốn. Đây chính là công cụ pháp lý để thúc đẩy đổi mới sáng tạo, tạo không gian cho công nghệ mới phát triển.

Cuối cùng, Luật Khoa học, công nghệ và đổi mới sáng tạo 2025 đã đồng bộ với Luật Dữ liệu 2024 về quản trị dữ liệu trong hoạt động khoa học. Luật quy định khi kết quả nhiệm vụ khoa học, công nghệ có lưu trữ, xử lý dữ liệu cốt lõi, dữ liệu quan trọng hoặc dữ liệu chuyển xuyên biên giới thì việc quản lý phải tuân thủ Luật Dữ liệu 2024. Tương tự, việc chuyển giao ra nước ngoài các kết quả nghiên cứu có chứa loại dữ liệu nhạy cảm này cũng phải theo quy định của Luật Dữ liệu. Như vậy, Luật khoa học, công nghệ và đổi mới sáng tạo đã tạo mối liên hệ chặt chẽ với Luật Dữ liệu nhằm bảo đảm dữ liệu quan trọng quốc gia thu được từ nghiên cứu khoa học được bảo vệ và quản lý an toàn, đáp ứng yêu cầu chủ quyền dữ liệu. Điều này thể hiện sự thống nhất của hệ thống pháp luật, vừa thúc đẩy nghiên cứu khoa học dựa trên dữ liệu, vừa đặt ra khuôn khổ quản trị dữ liệu an toàn theo Luật Dữ liệu.

Tóm lại, hai đạo luật mới đã xây dựng một hành lang pháp lý đồng bộ: Luật Dữ liệu 2024 định hướng phát triển dữ liệu gắn liền với khoa học, công nghệ và đổi mới sáng tạo, còn Luật khoa học, công nghệ và ĐMST 2025 cung cấp cơ chế, chính sách để khoa học, công nghệ và đổi mới sáng tạo phát huy vai trò trong kỷ nguyên dữ liệu và chuyển đổi số. Đó là nền tảng để Việt Nam từng bước thiết lập thị trường dữ liệu, thúc đẩy chuyển đổi số quốc gia, đưa dữ liệu trở thành động lực cho phát triển kinh tế-xã hội. Các chính sách tiến bộ này khẳng định quyết tâm của Nhà nước ta trong việc huy động sức mạnh khoa học-công nghệ cho công cuộc chuyển đổi



số, đồng thời bác bỏ những luận điệu xuyên tạc cho rằng Việt Nam “b López ngọt sáng tạo”. Trái lại, pháp luật Việt Nam đang tạo mọi điều kiện thuận lợi, hỗ trợ tối đa cho sự phát triển lĩnh vực dữ liệu và công nghệ, hướng tới mục tiêu sớm đưa nước ta trở thành một quốc gia số, một nền kinh tế số thịnh vượng.



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 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.
7. Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.
8. Vũ Trọng Lâm, "Hoàn thiện thể chế thúc đẩy đột phá phát triển khoa học, công nghệ và đổi mới sáng tạo", Tạp chí Cộng sản, 2025.



Câu 5: Quy định về thu thập, cập nhật, đồng bộ, kết nối, chia sẻ, khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia? Giải pháp tăng cường ứng dụng Cơ sở dữ liệu tổng hợp quốc gia phục vụ hoạt động của cơ quan nhà nước và đáp ứng nhu cầu phát triển kinh tế - xã hội?





Câu 5: Quy định về thu thập, cập nhật, đồng bộ, kết nối, chia sẻ, khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia? Giải pháp tăng cường ứng dụng Cơ sở dữ liệu tổng hợp quốc gia phục vụ hoạt động của cơ quan nhà nước và đáp ứng nhu cầu phát triển kinh tế - xã hội?

Trả lời

5.1. Quy định về thu thập, cập nhật, đồng bộ, kết nối, chia sẻ, khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia

5.1.1. Tổng quan

5.1.1.1. Phạm vi điều chỉnh và đối tượng áp dụng

Luật Dữ liệu quy định về dữ liệu số, bao gồm việc xây dựng, phát triển, bảo vệ, quản trị, xử lý và sử dụng dữ liệu. Luật này áp dụng đối với các cơ quan, tổ chức, cá nhân Việt Nam và các cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam hoặc trực tiếp tham gia/liên quan đến hoạt động dữ liệu số tại Việt Nam. Cơ sở dữ liệu tổng hợp quốc gia là tập hợp dữ liệu được Chính phủ xây dựng và quản lý tập trung, thống nhất tại Trung tâm dữ liệu quốc gia.



Hình ảnh: Sinh viên Đại học Thái Nguyên được huy động đến hỗ trợ các phường, xã của Thái Nguyên số hóa dữ liệu hộ tịch (2024). Ảnh: Báo Thái nguyên



5.1.1.2. Các loại dữ liệu và tiêu chí xác định

- Dữ liệu số: Dữ liệu về sự vật, hiện tượng, sự kiện, bao gồm một hoặc kết hợp các dạng âm thanh, hình ảnh, chữ số, chữ viết, ký hiệu được thể hiện dưới dạng kỹ thuật số.

- Dữ liệu cá nhân: Thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm. Dữ liệu cá nhân sau khi khử nhận dạng không còn là dữ liệu cá nhân.

+ Dữ liệu cá nhân cơ bản: là dữ liệu cá nhân phản ánh các yếu tố nhân thân, lai lịch phổ biến, thường xuyên sử dụng trong các giao dịch, quan hệ xã hội, thuộc danh mục do Chính phủ ban hành. Ví dụ: họ tên, ngày sinh, giới tính, nơi ở, quốc tịch, hình ảnh, số điện thoại, số định danh, tình trạng hôn nhân, thông tin gia đình, tài khoản số, lịch sử hoạt động trên không gian mạng và các thông tin khác gắn liền với cá nhân.

+ Dữ liệu cá nhân nhạy cảm: Dữ liệu gắn liền với quyền riêng tư, khi bị xâm phạm sẽ ảnh hưởng trực tiếp đến quyền, lợi ích hợp pháp của cá nhân. Ví dụ: quan điểm chính trị/tôn giáo, tình trạng sức khỏe, nguồn gốc chủng tộc/dân tộc, đặc điểm di truyền, thuộc tính vật lý/sinh học riêng, đời sống tình dục, dữ liệu về tội phạm, thông tin khách hàng tài chính/ngân hàng, dữ liệu vị trí và các dữ liệu đặc thù khác.

- Dữ liệu dùng chung: Dữ liệu được tiếp cận, chia sẻ, khai thác, sử dụng chung trong các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội.

- Dữ liệu dùng riêng: Dữ liệu được tiếp cận, chia sẻ, khai thác, sử dụng trong phạm vi nội bộ của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội.

- Dữ liệu mở: Dữ liệu mà mọi cơ quan, tổ chức, cá nhân có nhu cầu đều được tiếp cận, chia sẻ, khai thác, sử dụng. Cơ quan nhà nước phải công bố danh



mục dữ liệu mở và tổ chức công khai dữ liệu mở, trừ trường hợp bị cấm công khai do liên quan đến an ninh quốc gia, quyền riêng tư, bí mật thương mại.

- **Dữ liệu gốc:** Dữ liệu được tạo lập trong quá trình hoạt động của cơ quan, tổ chức, cá nhân hoặc thu thập, tạo lập từ số hóa bản chính giấy tờ, tài liệu, các dạng vật chất khác.

- **Dữ liệu quan trọng:** Dữ liệu có thể tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng, thuộc danh mục do Thủ tướng Chính phủ ban hành.

- **Dữ liệu cốt lõi:** Dữ liệu quan trọng trực tiếp tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng, thuộc danh mục do Thủ tướng Chính phủ ban hành.

5.1.2. Quy định về thu thập, cập nhật, đồng bộ, kết nối, chia sẻ, khai thác, sử dụng dữ liệu

5.1.2.1. Thu thập, cập nhật và đồng bộ dữ liệu

Điều 34 Luật Dữ liệu quy định, Dữ liệu được thu thập, cập nhật, đồng bộ vào Cơ sở dữ liệu tổng hợp quốc gia, bao gồm: ⁽¹⁾*Dữ liệu mở*; ⁽²⁾*Dữ liệu dùng chung của cơ quan nhà nước*; ⁽³⁾*Dữ liệu dùng riêng của cơ quan nhà nước theo quyết định của Thủ tướng Chính phủ để phục vụ nhiệm vụ quốc phòng, an ninh, đối ngoại, cơ yếu, phát triển kinh tế - xã hội, chuyển đổi số, lợi ích quốc gia, lợi ích công cộng*; ⁽⁴⁾*Dữ liệu của cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội khi được chủ sở hữu dữ liệu đồng ý*; ⁽⁵⁾*Dữ liệu khác do tổ chức, cá nhân cung cấp*.

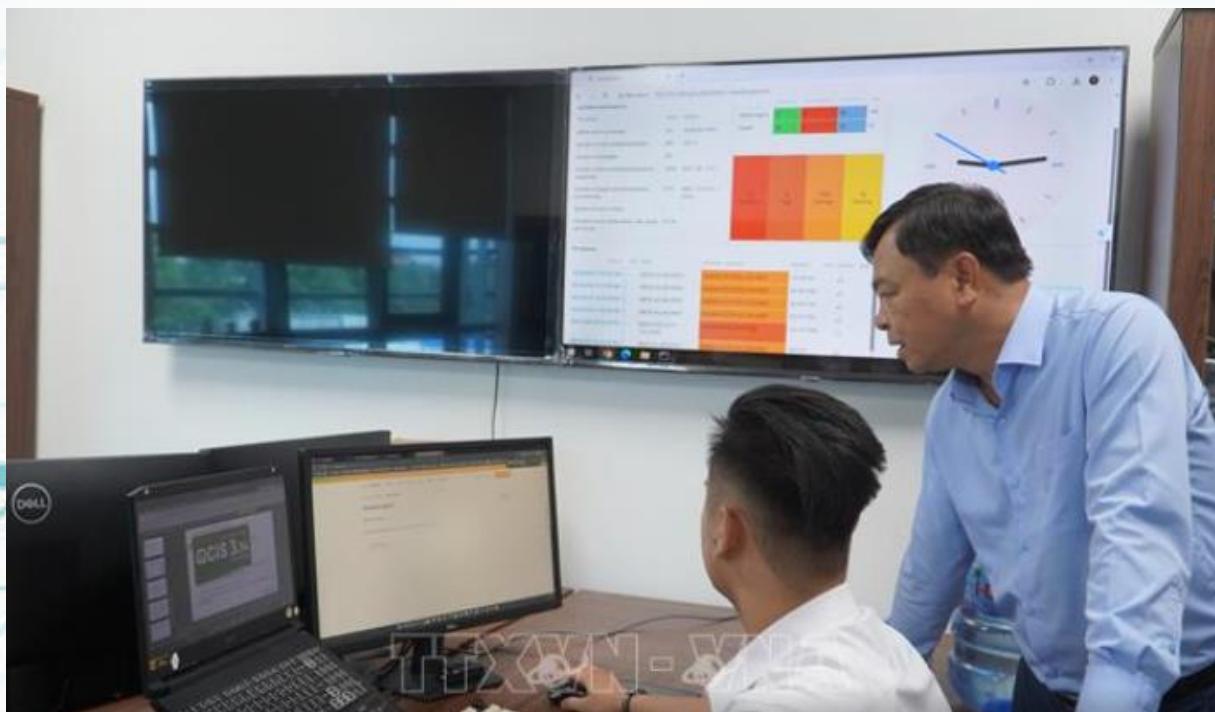
- **Nguồn thu thập:** Dữ liệu có thể được thu thập, tạo lập từ các nguồn trực tiếp tạo lập, số hóa giấy tờ, tài liệu và các dạng vật chất khác. Đối với cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội, dữ liệu được thu thập để xây dựng cơ sở dữ liệu theo quy định pháp luật hoặc quyết định của cấp có thẩm quyền, sử dụng thống nhất bảng mã danh mục dùng chung và thống nhất với dữ liệu chủ trong cơ sở dữ liệu quốc gia. Dữ liệu đã có trong các cơ sở dữ liệu được kết nối, chia sẻ thì không thu thập lại.



- Yêu cầu khi thu thập:
 - + Phải được sự đồng ý của chủ thẻ dữ liệu trước khi thu thập, trừ trường hợp pháp luật có quy định khác.
 - + Chỉ được thu thập, xử lý dữ liệu cá nhân đúng phạm vi, mục đích cụ thể, rõ ràng, bảo đảm tuân thủ quy định của pháp luật.
 - + Thông tin chỉ được tạo lập và nhập vào cơ sở dữ liệu quốc gia khi thông tin đó được kiểm tra mức độ chính xác.
 - + Việc thu thập dữ liệu để tạo lập dữ liệu chủ của cơ sở dữ liệu quốc gia thuộc trách nhiệm của cơ quan theo phân cấp quản lý nhà nước ngành, lĩnh vực hoặc địa bàn.
 - Đồng bộ dữ liệu vào Cơ sở dữ liệu tổng hợp quốc gia:
 - + Dữ liệu được thu thập, cập nhật, đồng bộ vào Cơ sở dữ liệu tổng hợp quốc gia bao gồm dữ liệu mở, dữ liệu dùng chung của cơ quan nhà nước, dữ liệu dùng riêng của cơ quan nhà nước theo quyết định của Thủ tướng Chính phủ (*để phục vụ nhiệm vụ quốc phòng, an ninh, đối ngoại, cơ yếu, phát triển kinh tế - xã hội, chuyển đổi số, lợi ích quốc gia, lợi ích công cộng*), dữ liệu của cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội khi được chủ sở hữu dữ liệu đồng ý, dữ liệu khác do tổ chức, cá nhân cung cấp.
 - + Nguồn đồng bộ bao gồm từ quá trình thực hiện thủ tục hành chính/dịch vụ công, từ các cơ sở dữ liệu khác, hoặc được số hóa/cung cấp/tích hợp bởi cá nhân/tổ chức.
 - + Trung tâm dữ liệu quốc gia phối hợp kiểm tra dữ liệu khi thu thập, cập nhật, đồng bộ để bảo đảm tính chính xác, thống nhất. Trường hợp không thống nhất, Trung tâm dữ liệu quốc gia sẽ phối hợp để kiểm tra, đối soát và cập nhật.
 - Cập nhật dữ liệu:
 - + Bao gồm bổ sung và điều chỉnh dữ liệu.
 - + Nguồn cập nhật là kết quả giải quyết thủ tục hành chính, đề xuất sửa đổi/bổ sung của cơ quan/tổ chức/cá nhân và các cơ sở dữ liệu liên quan khác.



- + Dữ liệu chủ phải được cập nhật ngay khi kết thúc nghiệp vụ hoặc quy trình giải quyết thủ tục hành chính.
- + Dữ liệu tham chiếu đến dữ liệu chủ phải được cập nhật kịp thời theo mọi thay đổi của dữ liệu chủ.
- + Cơ quan chủ quản cơ sở dữ liệu quốc gia chịu trách nhiệm về sai sót, thay đổi phát sinh trong quá trình quản lý, lưu trữ và chia sẻ dữ liệu.
- + Cơ quan nhà nước phải thường xuyên kiểm tra, giám sát, khắc phục sai sót; thực hiện đồng bộ dữ liệu và phối hợp cập nhật, điều chỉnh, bảo đảm chất lượng dữ liệu.
- Chất lượng dữ liệu: Bảo đảm tính chính xác, hợp lệ, toàn vẹn, đầy đủ, cập nhật kịp thời, thống nhất của dữ liệu.



Hình ảnh: Kiểm tra Công tác cập nhật dữ liệu tại Trung tâm dữ liệu vùng Đồng bằng sông Cửu Long. Ảnh: Thông tấn xã Việt Nam

5.1.2.2. Lưu trữ dữ liệu

- Địa điểm lưu trữ:
 - + Cơ sở dữ liệu quốc gia phải được lưu trữ trên cơ sở hạ tầng của Trung tâm dữ liệu quốc gia.



- + Cơ sở dữ liệu chuyên ngành và các cơ sở dữ liệu khác của cơ quan nhà nước có thể lưu trữ trên hạ tầng của Trung tâm dữ liệu quốc gia hoặc hạ tầng của cơ quan/tổ chức khác đáp ứng tiêu chuẩn trung tâm dữ liệu.
- + Dữ liệu dùng riêng và dữ liệu thuộc lĩnh vực quốc phòng, an ninh, đối ngoại, cơ yếu được lưu trữ trên hạ tầng của Trung tâm dữ liệu quốc gia khi có sự đồng ý của chủ sở hữu dữ liệu.
- + Các tổ chức, cá nhân không thuộc cơ quan nhà nước có thể thỏa thuận lưu trữ dữ liệu trên hạ tầng của Trung tâm dữ liệu quốc gia thông qua hợp đồng cung cấp dịch vụ.



Hình ảnh: Trung tâm dữ liệu Viettel Hòa Lạc là trung tâm lưu trữ dữ liệu lớn nhất Việt Nam hiện nay. Ảnh: Báo Tuổi trẻ

- Trách nhiệm lưu trữ:
 - + Chủ sở hữu dữ liệu quy định thời hạn lưu trữ cụ thể đối với dữ liệu do mình thu thập, tạo lập.
 - + Cơ quan nhà nước phải ban hành quy trình kỹ thuật về lưu trữ dữ liệu do mình quản lý, bảo đảm lưu trữ dữ liệu an toàn.



- + Dữ liệu cá nhân của người lao động phải lưu trữ trong thời hạn theo quy định của pháp luật hoặc theo thỏa thuận.
- + Dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng chỉ được lưu trữ trong khoảng thời gian cần thiết để phục vụ mục đích thu thập, sau đó phải xóa, hủy.
- + Thông điệp dữ liệu có thể được lưu trữ dưới dạng này nếu có thể truy cập, sử dụng để tham chiếu, được lưu trong khuôn dạng khởi tạo/gửi/nhận hoặc khuôn dạng thể hiện chính xác thông tin và cho phép xác định nguồn gốc, người gửi/nhận, thời gian gửi/nhận.
- Thành phần dữ liệu được lưu trữ tại Trung tâm dữ liệu quốc gia:
 - + Dữ liệu tổng hợp từ các cơ sở dữ liệu quốc gia.
 - + Dữ liệu thông tin liên quan đến con người từ các cơ sở dữ liệu quốc gia, bộ, ngành, địa phương và dữ liệu khác do các cơ quan, tổ chức, cá nhân đồng bộ về, bao gồm: dữ liệu định danh cá nhân (*giấy tờ tùy thân, thông tin cá nhân, y tế, sinh trắc, ADN, việc làm, học bạ*) và dữ liệu thu thập từ kết quả tổng hợp, phân tích, khai thác dữ liệu của công dân.

5.1.2.3. Quản trị và quản lý dữ liệu

- Quản trị dữ liệu: Bao gồm xây dựng chính sách, kế hoạch, chương trình, quy trình, tiêu chuẩn về dữ liệu của chủ sở hữu/chủ quản dữ liệu để quản lý dữ liệu một cách liên tục, hiệu quả, bảo đảm tính đầy đủ, chính xác, toàn vẹn, nhất quán, thống nhất, được chuẩn hóa, an toàn, bảo mật, kịp thời của dữ liệu.
- Quản lý dữ liệu: Là việc tổ chức thực hiện quản trị dữ liệu.
- Trách nhiệm:
 - + Chủ sở hữu dữ liệu, chủ quản dữ liệu là cơ quan nhà nước có trách nhiệm phối hợp với Trung tâm dữ liệu quốc gia thực hiện quản trị, quản lý dữ liệu.
 - + Trung tâm dữ liệu quốc gia chịu trách nhiệm quản trị toàn bộ hạ tầng công nghệ thông tin, cơ sở dữ liệu của vùng chuyên dụng và các hạng mục dùng



chung, thực hiện vận hành hạ tầng công nghệ thông tin, hệ thống nền tảng điện toán đám mây của vùng dùng chung.

+ Các bộ, ngành, địa phương và tổ chức chính trị xã hội tiếp tục quản lý cơ sở dữ liệu trong hệ thống của mình và phối hợp bảo đảm an ninh an toàn thông tin.

+ Cơ quan quản lý cơ sở dữ liệu xây dựng Khung quản trị, quản lý dữ liệu chi tiết bao gồm cơ chế quản lý dữ liệu chủ, hoạt động xử lý dữ liệu, chất lượng dữ liệu, siêu dữ liệu, kiến trúc dữ liệu, kết nối/chia sẻ, bảo vệ dữ liệu, phát triển/khai thác/sử dụng dữ liệu, triển khai/kiểm soát/giám sát.

+ Bộ Công an xây dựng chính sách quản lý dữ liệu chủ được đồng bộ vào Cơ sở dữ liệu tổng hợp quốc gia và các quy trình liên quan.

5.1.2.4. Truy cập và truy xuất dữ liệu

- Truy cập dữ liệu: Hoạt động tiếp cận, tác động tới dữ liệu theo đúng quyền được giao, bao gồm đọc, ghi, sửa, xóa, thực thi và các loại truy cập khác.

- Truy xuất dữ liệu: Hoạt động truy cập và trích xuất dữ liệu, bao gồm thủ công, tự động, theo thời gian thực và các loại truy xuất khác.

- Nguyên tắc: Bảo đảm hợp pháp, tuân thủ quy trình kỹ thuật, chỉ truy cập/truy xuất dữ liệu trong phạm vi quyền được giao và cần thiết cho mục đích xác định.

- Trách nhiệm của cơ quan nhà nước: Cung cấp công cụ và phân quyền truy cập, truy xuất dữ liệu để bảo đảm an ninh, an toàn, bảo vệ dữ liệu. Phải ban hành quy trình kỹ thuật về truy cập, truy xuất dữ liệu, bao gồm quản lý thông tin đăng ký sử dụng, phân quyền, lịch sử truy cập và công cụ.

5.1.2.5. Kết nối, chia sẻ và điều phối dữ liệu

Điều 36 Luật Dữ liệu quy định về kết nối, chia sẻ dữ liệu với Cơ sở dữ liệu tổng hợp quốc gia, trong đó: ⁽¹⁾Các cơ sở dữ liệu quốc gia khác, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội kết nối với Cơ sở dữ liệu tổng hợp quốc gia thông qua Nền tảng chia sẻ, điều phối dữ liệu; Nền tảng



tích hợp, chia sẻ dữ liệu quốc gia; nền tảng tích hợp, chia sẻ dữ liệu cấp bộ, cấp tỉnh, mạng Internet, mạng máy tính, hệ thống thông tin; ⁽²⁾ Việc kết nối, chia sẻ dữ liệu giữa Cơ sở dữ liệu tổng hợp quốc gia và các cơ sở dữ liệu khác phải bảo đảm hiệu quả, an toàn, phù hợp với chức năng, nhiệm vụ, quyền hạn của cơ quan, tổ chức, cá nhân theo quy định của pháp luật; ⁽³⁾ Việc kết nối, chia sẻ dữ liệu giữa Cơ sở dữ liệu tổng hợp quốc gia với hệ thống thông tin khác được thực hiện trên cơ sở thống nhất bằng văn bản giữa Bộ Công an và chủ sở hữu dữ liệu. Ngoài ra, quy định Chính phủ quy định chi tiết các nội dung này.

- Nguyên tắc: Chủ sở hữu dữ liệu, chủ quản dữ liệu kết nối, chia sẻ dữ liệu cho người dùng dữ liệu theo quy định của pháp luật hoặc theo thỏa thuận, bằng cách trực tiếp hoặc thông qua một bên trung gian. Việc kết nối, chia sẻ phải bảo đảm hiệu quả, an toàn, phù hợp chức năng, nhiệm vụ, quyền hạn của cơ quan, tổ chức, cá nhân.

- Phương thức chia sẻ: Qua vật mang tin, tải về qua môi trường mạng, hoặc trực tuyến/tự động qua kết nối hệ thống thông tin.

- Nền tảng: Các hệ thống trung gian bao gồm Nền tảng tích hợp, chia sẻ dữ liệu quốc gia; hạ tầng kết nối, chia sẻ dữ liệu cấp Bộ, cấp tỉnh theo Khung kiến trúc tổng thể quốc gia số. Nền tảng chia sẻ, điều phối dữ liệu của Trung tâm dữ liệu quốc gia phục vụ kết nối, tích hợp, chia sẻ và điều phối dữ liệu giữa Trung tâm dữ liệu quốc gia với các cơ quan, tổ chức, cá nhân.

- Dữ liệu phải chia sẻ: Dữ liệu sử dụng chung, dữ liệu mở trong cơ quan nhà nước mặc định phải được chia sẻ cho các cơ quan nhà nước để phục vụ quản lý nhà nước khi có đề nghị.

- Trách nhiệm chia sẻ:

+ Cơ quan nhà nước có trách nhiệm kết nối, chia sẻ dữ liệu với cơ quan, tổ chức khác; không cung cấp thông tin qua văn bản giấy đối với thông tin đã khai thác qua kết nối/chia sẻ.

+ Trung tâm dữ liệu quốc gia điều phối dữ liệu của Cơ sở dữ liệu tổng hợp quốc gia.



- + Các bộ, ngành, địa phương có trách nhiệm đồng bộ dữ liệu thuộc phạm vi quản lý về Trung tâm dữ liệu quốc gia.
- + Các bộ, ngành, địa phương khi có nhu cầu về khai thác dữ liệu phải bảo đảm dữ liệu chỉ được khai thác tại phiên truy cập, không được phép lưu trữ và chia sẻ các trường thông tin không thuộc thông tin chuyên ngành đơn vị mình quản lý và phải bảo đảm an ninh an toàn, đúng mục đích.
- Hỗ trợ: Cơ quan nhà nước thực hiện các biện pháp hỗ trợ chủ sở hữu dữ liệu kết nối, chia sẻ dữ liệu (*xây dựng hệ thống thông tin, quy trình/ứng dụng, hỗ trợ đường truyền, kinh phí, nhân lực, đào tạo*).



Hình ảnh: Bộ Công an và Bộ Tài nguyên và Môi trường kết nối cơ sở dữ liệu quốc gia về dân cư và cơ sở dữ liệu quốc gia về đất đai. Ảnh: Báo Chính phủ

5.1.2.6. Khai thác và sử dụng dữ liệu

Điều 35 Luật Dữ liệu quốc gia quy định về khai thác và sử dụng Cơ sở dữ liệu tổng hợp quốc gia, cụ thể: ⁽¹⁾*Cơ sở dữ liệu tổng hợp quốc gia được xây dựng phục vụ việc khai thác, sử dụng chung đáp ứng hoạt động của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội; phục*



vụ thực hiện thủ tục hành chính, dịch vụ công, phục vụ chỉ đạo điều hành của Chính phủ; phục vụ công tác thống kê, hoạch định chính sách, xây dựng quy hoạch, chiến lược phát triển kinh tế - xã hội, quốc phòng, an ninh, đối ngoại, cơ yếu, đấu tranh phòng, chống tội phạm, xử lý vi phạm pháp luật; phục vụ nhu cầu khai thác, sử dụng, ứng dụng dữ liệu của tổ chức, cá nhân; ⁽²⁾Dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia có giá trị khai thác và sử dụng như dữ liệu gốc.

- Mục đích:

+ Phục vụ hoạt động của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội.

+ Phục vụ thực hiện thủ tục hành chính, dịch vụ công.

+ Phục vụ chỉ đạo điều hành của Chính phủ, công tác thống kê, hoạch định chính sách, xây dựng quy hoạch, chiến lược phát triển kinh tế - xã hội, quốc phòng, an ninh, đối ngoại, cơ yếu, đấu tranh phòng, chống tội phạm, xử lý vi phạm pháp luật.

+ Phục vụ nhu cầu khai thác, sử dụng, ứng dụng dữ liệu của tổ chức, cá nhân, phát triển kinh tế số, xã hội số.

- Đối tượng khai thác: Cơ quan Đảng, Quốc hội, Chính phủ, Tòa án, Viện kiểm sát, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội từ trung ương đến cấp xã và các tổ chức, cá nhân.

- Cách thức khai thác:

+ Kết nối, chia sẻ dữ liệu trực tiếp với Cơ sở dữ liệu tổng hợp quốc gia (*Trung tâm dữ liệu quốc gia cấp tài khoản*).

+ Qua Cổng dữ liệu quốc gia, Cổng Dịch vụ công quốc gia, cổng thông tin điện tử, hệ thống thông tin giải quyết thủ tục hành chính, nền tảng định danh và xác thực điện tử, ứng dụng định danh quốc gia, thiết bị/phương tiện/phần mềm do Trung tâm dữ liệu quốc gia cung cấp.

+ Bằng văn bản yêu cầu khai thác, cung cấp thông tin.

+ Các cơ sở dữ liệu quốc gia thực hiện đồng bộ, cập nhật dữ liệu về Cơ sở dữ liệu tổng hợp quốc gia để cung cấp dưới dạng dữ liệu dùng chung, dữ liệu mở.



- Giá trị pháp lý: Dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia có giá trị khai thác và sử dụng như dữ liệu gốc. Dữ liệu chủ trong cơ sở dữ liệu quốc gia, cơ sở dữ liệu của bộ, ngành, địa phương có giá trị sử dụng chính thức, tương đương văn bản giấy.

- Chủ thể dữ liệu: Có quyền yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân cung cấp dữ liệu cá nhân của mình.

- Khuyến khích: Khuyến khích cá nhân, tổ chức chia sẻ, cung cấp dữ liệu của mình cho cơ quan nhà nước vì lợi ích chung, chăm sóc sức khỏe, biến đổi khí hậu, cải thiện giao thông, tổng hợp số liệu thống kê, cải thiện dịch vụ công, hoạch định chính sách hoặc nghiên cứu khoa học.

5.1.2.7. Mã hóa và giải mã dữ liệu

- Mã hóa: Chuyển đổi dữ liệu cá nhân sang dạng không nhận biết được nếu không giải mã; dữ liệu cá nhân sau khi mã hóa vẫn là dữ liệu cá nhân.

- Giải mã: Chuyển đổi dữ liệu đã mã hóa từ định dạng không nhận biết được sang định dạng nhận biết được.

- Quy định:

+ Dữ liệu cá nhân là bí mật nhà nước phải được mã hóa, giải mã theo quy định của pháp luật về bảo vệ bí mật nhà nước và pháp luật về cơ yếu.

+ Chủ sở hữu dữ liệu, chủ quản dữ liệu quyết định việc mã hóa/giải mã dữ liệu.

+ Cơ quan nhà nước có thẩm quyền được quyền áp dụng biện pháp để giải mã dữ liệu mà không cần chủ sở hữu/chủ quản dữ liệu đồng ý trong các trường hợp khẩn cấp, nguy cơ đe dọa an ninh quốc gia, thảm họa, phòng chống bạo loạn/khung bối.

+ Tổ chức, cá nhân được sử dụng một hoặc nhiều giải pháp mã hóa và quy trình mã hóa, giải mã phù hợp, bao gồm mã hóa khi truyền tải/lưu trữ, trên thiết bị số, giải pháp bảo mật phần cứng, quy trình giải mã yêu cầu xác thực và giải pháp ghi lại hoạt động mã hóa/giải mã.



5.1.2.8. Khử nhận dạng và xóa/hủy dữ liệu

- Khử nhận dạng: Quá trình thay đổi hoặc xóa thông tin để tạo ra dữ liệu mới không thể xác định hoặc không thể giúp xác định được một con người cụ thể. Cơ quan, tổ chức, cá nhân khử nhận dạng dữ liệu cá nhân phải kiểm soát, giám sát chặt chẽ quá trình, ngăn chặn truy cập trái phép, sao chép, chiếm đoạt, làm lộ, làm mất dữ liệu. Không được tái nhận dạng dữ liệu cá nhân sau khi đã được khử nhận dạng, trừ trường hợp pháp luật có quy định khác.

- Xóa/Hủy dữ liệu:

- + Chủ thẻ dữ liệu có quyền yêu cầu xóa, hủy dữ liệu cá nhân của mình.
- + Việc xóa dữ liệu cá nhân được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thẻ dữ liệu, trừ trường hợp pháp luật có quy định khác.
- + Các trường hợp không áp dụng xóa dữ liệu: Pháp luật không cho phép xóa, dữ liệu được xử lý bởi cơ quan nhà nước có thẩm quyền phục vụ hoạt động nhà nước, dữ liệu đã được công khai, dữ liệu phục vụ yêu cầu pháp lý/nghiên cứu khoa học/thông kê, trong tình trạng khẩn cấp về quốc phòng/an ninh/trật tự an toàn xã hội/thảm họa/dịch bệnh, nguy cơ đe dọa an ninh/quốc phòng chưa đến mức ban bố tình trạng khẩn cấp, phòng chống bạo loạn/khung bối/tội phạm, hoặc ứng phó tình huống khẩn cấp đe dọa tính mạng/sức khỏe/an toàn.
- + Bên Kiểm soát/Xử lý dữ liệu cá nhân không được cô ý khôi phục trái phép dữ liệu đã bị xóa, hủy.
- + Trường hợp doanh nghiệp chia, tách, sáp nhập, hợp nhất, giải thể hoặc cơ quan/tổ chức/đơn vị hành chính được tổ chức lại, chuyển đổi hình thức sở hữu doanh nghiệp nhà nước, dữ liệu cá nhân được chuyển giao theo quy định của pháp luật. Khi tổ chức lại/giải thể tổ chức quản lý dữ liệu cốt lõi/quan trọng, chủ quản dữ liệu phải áp dụng biện pháp bảo đảm an toàn dữ liệu, báo cáo phương án xử lý dữ liệu và thông tin bên tiếp nhận cho cơ quan có thẩm quyền.

5.1.2.9. Chuyển giao dữ liệu xuyên biên giới

- Quy định chung: Cơ quan, tổ chức, cá nhân được tự do chuyển dữ liệu từ nước ngoài về Việt Nam, xử lý dữ liệu của nước ngoài tại Việt Nam và được Nhà nước bảo vệ các quyền và lợi ích hợp pháp.



- Phạm vi: Chuyển dữ liệu cốt lõi, dữ liệu quan trọng xuyên biên giới bao gồm chuyển dữ liệu đang lưu trữ tại Việt Nam ra nước ngoài, cơ quan/tổ chức/cá nhân Việt Nam chuyển dữ liệu cho tổ chức/cá nhân nước ngoài và sử dụng nền tảng ngoài lãnh thổ Việt Nam để xử lý dữ liệu.

- Yêu cầu: Phải bảo đảm quốc phòng, an ninh, bảo vệ lợi ích quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của chủ thể dữ liệu, chủ sở hữu dữ liệu theo quy định pháp luật Việt Nam và điều ước quốc tế.

- Đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới:

+ Phải gửi hồ sơ đánh giá tác động đến Bộ Công an (*hoặc Bộ Quốc phòng đối với dữ liệu quân sự, quốc phòng, cơ yếu*).

+ Hồ sơ bao gồm Báo cáo đánh giá tác động và các văn bản liên quan, nêu rõ tính hợp pháp, sự cần thiết, rủi ro, trách nhiệm các bên.

+ Đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an sẽ kiểm tra, đánh giá hồ sơ trong thời hạn 10 ngày (*không quá 15 ngày đối với hồ sơ phức tạp*) và thông báo kết quả. Sau khi đạt, chủ quản dữ liệu quyết định việc chuyển dữ liệu.

+ Việc đánh giá tập trung vào rủi ro đối với an ninh quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của cá nhân/tổ chức, chính sách bảo vệ an toàn dữ liệu của quốc gia nhận dữ liệu, quy mô/phạm vi/loại dữ liệu, nguy cơ bị giả mạo/phá hủy/rò rỉ/mất/sử dụng bất hợp pháp và trách nhiệm các bên.

+ Phải sửa đổi, bổ sung hồ sơ khi có thay đổi về mục đích, phương pháp, phạm vi, loại dữ liệu, chính sách bảo vệ dữ liệu ở quốc gia nhận dữ liệu, hoặc kéo dài thời gian lưu trữ dữ liệu cốt lõi/quan trọng.

+ Bộ Quốc phòng, Bộ Công an có thể yêu cầu ngừng hoạt động chuyển, xử lý dữ liệu cốt lõi/quan trọng nếu phát hiện dữ liệu được sử dụng vào hoạt động xâm phạm quốc phòng, an ninh, lợi ích quốc gia/công cộng, quyền/lợi ích hợp pháp của chủ thể dữ liệu.

- Các trường hợp không phải thực hiện quy định về đánh giá tác động chuyển dữ liệu xuyên biên giới: Chuyển dữ liệu cá nhân xuyên biên giới của cơ quan nhà



nước có thẩm quyền; cơ quan, tổ chức lưu trữ dữ liệu cá nhân của người lao động trên dịch vụ điện toán đám mây; chủ thẻ dữ liệu cá nhân tự chuyển dữ liệu của mình xuyên biên giới; và các trường hợp khác theo quy định của Chính phủ.

- Các trường hợp được phép cung cấp dữ liệu cá nhân ra nước ngoài trong tình huống khẩn cấp hoặc theo hợp đồng mà không cần đánh giá tác động trước: Phải gửi đánh giá tác động sau 15 ngày kể từ ngày thực hiện.

5.1.2.10. Đánh giá và quản lý rủi ro dữ liệu

- Các loại rủi ro: Rủi ro quyền riêng tư, rủi ro an ninh mạng, rủi ro nhận dạng và quản lý truy cập và các rủi ro khác trong xử lý dữ liệu.

- Trách nhiệm và biện pháp:

+ Cơ quan nhà nước phải xác định, thiết lập cơ chế cảnh báo sớm về rủi ro và xây dựng biện pháp bảo vệ dữ liệu.

+ Chủ quản dữ liệu tự đánh giá, xác định rủi ro và thực hiện các biện pháp bảo vệ dữ liệu; kịp thời khắc phục rủi ro và thông báo cho chủ thẻ dữ liệu.

+ Chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải định kỳ tiến hành đánh giá rủi ro và thông báo tới đơn vị chuyên trách về an ninh mạng, an toàn thông tin thuộc Bộ Công an, Bộ Quốc phòng. Báo cáo đánh giá rủi ro phải có sẵn để phục vụ kiểm tra, đánh giá của cơ quan có thẩm quyền.

+ Biện pháp phòng ngừa rủi ro bao gồm sao lưu dữ liệu, bảo trì/nâng cấp hệ thống định kỳ, áp dụng biện pháp bảo vệ dữ liệu, phân cấp truy cập chặt chẽ, sử dụng hệ thống giám sát xâm nhập, cài đặt phần mềm bảo mật, xây dựng phương án xử lý sự cố, đào tạo/tập huấn kỹ năng bảo vệ dữ liệu.

+ Bộ Công an thiết lập cơ chế giám sát rủi ro an toàn dữ liệu, xây dựng tiêu chuẩn giám sát, cảnh báo sớm và phối hợp xây dựng phương tiện kỹ thuật giám sát. Bộ Công an cũng xây dựng cơ chế báo cáo, chia sẻ thông tin rủi ro an toàn dữ liệu, khuyến khích các tổ chức cung cấp dịch vụ bảo mật chia sẻ thông tin.



5.1.2.11. Quản lý nhà nước về dữ liệu và Trung tâm dữ liệu quốc gia

- Cơ quan quản lý: 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 thực hiện quản lý nhà nước về dữ liệu, trừ nội dung thuộc phạm vi quản lý của Bộ Quốc phòng. Bộ Quốc phòng chịu trách nhiệm quản lý nhà nước về dữ liệu thuộc phạm vi quản lý của mình.

- Trung tâm dữ liệu quốc gia:

+ Là trung tâm dữ liệu do Chính phủ xây dựng, quản lý, khai thác và vận hành, chịu sự quản lý trực tiếp của Bộ trưởng Bộ Công an.

+ Vai trò: Tích hợp, đồng bộ, lưu trữ, khai thác, chia sẻ, phân tích và điều phối tất cả các dữ liệu tổng hợp từ các cơ sở dữ liệu quốc gia, dữ liệu liên quan đến con người.

+ Cung cấp hạ tầng công nghệ thông tin cho các cơ quan Đảng, Quốc hội, cơ quan nhà nước và các tổ chức chính trị - xã hội khi có nhu cầu.

+ Thiết lập Cổng dữ liệu quốc gia là đầu mối công bố thông tin, dữ liệu mở và tiếp nhận dữ liệu từ tổ chức/cá nhân vì lợi ích chung.

+ Có trách nhiệm 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.

+ Cán bộ, chiến sĩ làm việc tại Trung tâm dữ liệu quốc gia được hưởng mức hỗ trợ là 500.000 đồng/ngày làm việc từ nguồn thu phí khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia sau khi nộp vào ngân sách nhà nước.

+ Hạ tầng Trung tâm dữ liệu quốc gia được phân thành vùng dùng chung (*phục vụ bộ ngành, địa phương, người dân, doanh nghiệp khai thác dữ liệu mở và dùng chung*) và vùng chuyên dụng (*lưu trữ dữ liệu bí mật nhà nước chuyên ngành và dữ liệu được phân tích đồng bộ ra vùng dùng chung*).

- Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân: Do Bộ Công an xây dựng, quản lý, vận hành để cung cấp thông tin, tuyên truyền, tiếp nhận hồ sơ/dữ liệu, cảnh báo, xử lý vi phạm liên quan đến bảo vệ dữ liệu cá nhân.



5.1.2.12. Hành vi bị nghiêm cấm và xử lý vi phạm

- Hành vi bị nghiêm cấm:
 - + Xử lý dữ liệu cá nhân trái quy định của pháp luật, nhằm chống Nhà nước, gây ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội, quyền/lợi ích hợp pháp của cơ quan/tổ chức/cá nhân.
 - + Cản trở hoạt động bảo vệ dữ liệu cá nhân.
 - + Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để vi phạm pháp luật.
 - + Sử dụng dữ liệu cá nhân của người khác, cho người khác sử dụng dữ liệu cá nhân của mình để thực hiện hành vi trái pháp luật.
 - + Mua, bán dữ liệu cá nhân, trừ trường hợp luật có quy định khác.
 - + Chiếm đoạt, cố ý làm lộ, làm mất dữ liệu cá nhân.
 - + Giả mạo, cố ý làm sai lệch, làm mất, làm hư hỏng dữ liệu trong cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội.
 - + Cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định.
 - + Xóa, hủy dữ liệu cá nhân đã được khử nhận dạng để tái nhận dạng.
 - + Không được tái nhận dạng dữ liệu cá nhân sau khi đã được khử nhận dạng.
 - + Cố ý khôi phục trái phép dữ liệu cá nhân đã bị xóa, hủy.
 - + Sử dụng dữ liệu vị trí cá nhân của tổ chức, cá nhân không liên quan.
 - + Sử dụng, phát triển hệ thống xử lý dữ liệu lớn, trí tuệ nhân tạo, chuỗi khối, vũ trụ ảo, điện toán đám mây có sử dụng dữ liệu cá nhân để gây tổn hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc xâm phạm đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản của người khác.
 - + Tiết lộ thông tin thuộc danh mục bí mật nhà nước, bí mật đời tư của cá nhân, bí mật khác mà chưa đến mức truy cứu trách nhiệm hình sự.



Minh Chien

5 tháng 8 lúc 14:18 ·

...

Bên mình bán data UY TÍN, nói không với lừa đảo. Data được BẢO HÀNH 1 đổi 1 số bị thuê bao.

Bên mình bán các loại data:

- + Data khách chuyên quan tâm lĩnh vực đầu tư BDS.
- + Data các DOANH NGHIỆP & GIÁM ĐỐC DOANH NGHIỆP ở TP.HCM và HÀ NỘI.
- + Data GIÁO VIÊN.

Xem thêm

Item Number	Description
1	Mua thời trang cao cấp
2	Nạp game
3	Giám đốc Hà Nội
4	Giám đốc (ko có địa chỉ)
5	Ngân hàng
6	Univision
7	Đầu tư vàng
8	Đầu tư BDS
9	Đồng kiếm oto
10	Điền ở Quảng Ninh
11	Data Doanh nghiệp
12	Chứng khoán
13	Bảo hiểm XH
14	BDS Phú Quốc
15	Data phong thủy
16	Bảo hiểm NT
17	Ngân hàng MSB
18	Người có thu nhập cao
19	An phủ
20	Spa
21	5G tài khoản ngân hàng
22	Sinh viên
23	Phụ huynh học sinh
24	Nhân viên văn phòng
25	Facebook bán vàng bạc
26	Phú Mỹ Hưng
27	techcombank
28	5G cước
29	the pride hà đông
30	Nhà cho thuê
31	Thuê bao Viettel
32	Vinhome
33	Vinhome time city park hill
34	Vinhome D'Capital Trần Duy Hưng
35	Xe hơi
36	Email

7

41 bình luận

Thích

Bình luận

Gửi

Chia sẻ

Hình ảnh: Việc mua bán dữ liệu cá nhân được thực hiện công khai trên mạng xã hội. Ảnh: Tác giả

- Xử lý vi phạm: Tổ chức, cá nhân vi phạm quy định bảo vệ dữ liệu cá nhân có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, xử lý hình sự tùy theo tính chất, mức độ, hậu quả; nếu gây thiệt hại thì phải bồi thường. Mức phạt tiền tối đa đối với tổ chức gấp 02 lần mức phạt tiền đối với cá nhân.

+ Cá nhân, tổ chức có thể bị buộc hủy bỏ thông tin cá nhân do vi phạm.

+ Bên Kiểm soát/Xử lý dữ liệu cá nhân phải lập biên bản xác nhận vi phạm và phối hợp với Bộ Công an (*Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*) xử lý.



+ Tổ chức, cá nhân phải thông báo cho Bộ Công an khi phát hiện vi phạm, dữ liệu bị xử lý sai mục đích, không bảo đảm quyền chủ thể dữ liệu.

Các quy định này nhằm đảm bảo an ninh, an toàn dữ liệu, bảo vệ quyền riêng tư cá nhân và thúc đẩy phát triển kinh tế - xã hội dựa trên dữ liệu số tại Việt Nam.

5.2. Giải pháp tăng cường ứng dụng Cơ sở dữ liệu tổng hợp quốc gia phục vụ hoạt động của cơ quan nhà nước và đáp ứng nhu cầu phát triển kinh tế - xã hội

5.2.1. Hoàn thiện thể chế và chính sách

5.2.1.1. Sửa đổi, bổ sung pháp luật và văn bản hướng dẫn

Để Cơ sở dữ liệu tổng hợp quốc gia thực sự phát huy hiệu quả, hệ thống pháp luật cần được hoàn thiện, đồng bộ với Luật Dữ liệu 2024. Trước hết, cần ban hành các nghị định, thông tư hướng dẫn thi hành Luật Dữ liệu. Ngay sau khi Luật Dữ liệu được thông qua cuối năm 2024, Chính phủ đã ban hành Nghị định 165/2025/NĐ-CP (30/6/2025) quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu. Nghị định này cùng với Nghị định 47/2024/NĐ-CP về danh mục cơ sở dữ liệu quốc gia và Nghị định 194/2025/NĐ-CP về kết nối, chia sẻ dữ liệu số đã tạo khung pháp lý nền tảng cho việc xây dựng Cơ sở dữ liệu tổng hợp Quốc gia. Trong đó, Nghị định 47/2024/NĐ-CP quy định rõ các Cơ sở dữ liệu Quốc gia phải được đồng bộ về Cơ sở dữ liệu tổng hợp Quốc gia và cách thức xây dựng, cập nhật, khai thác chúng. Nghị định 194/2025/NĐ-CP (hiệu lực 19/8/2025) bổ sung các quy định về khai thác, chia sẻ dữ liệu giữa các hệ thống, qua đó yêu cầu dữ liệu từ Cơ sở dữ liệu Quốc gia sau khi đồng bộ về Cơ sở dữ liệu tổng hợp Quốc gia sẽ được cung cấp dưới dạng dữ liệu dùng chung, dữ liệu mở cho cơ quan, tổ chức, cá nhân khai thác. Bên cạnh đó, cần sửa đổi các luật liên quan để thống nhất nguyên tắc quản trị dữ liệu. Ví dụ: Điều 44 Luật Dữ liệu 2024 đã sửa Luật Giao dịch điện tử 2023 theo hướng bổ sung Trung tâm dữ liệu quốc gia và các nền tảng chia sẻ dữ liệu vào kiến trúc hạ tầng kết nối quốc gia, bảo đảm mọi hệ thống cấp bộ, tính có thể kết nối thông qua Trung tâm dữ liệu quốc gia thay vì kết nối chéo phức tạp. Đồng thời, Luật Dữ liệu cũng bổ sung quy định về phí khai thác dữ liệu: phụ lục



Luật Phí và lệ phí được cập nhật thêm khoản phí khai thác thông tin trong Cơ sở dữ liệu tổng hợp Quốc gia, do Bộ Tài chính quản lý. Việc này tạo cơ chế tài chính để tái đầu tư cho hạ tầng dữ liệu và phản ánh quan điểm coi dữ liệu là tài sản có giá trị kinh tế. Ngoài ra, cần ban hành các thông tư, tiêu chuẩn kỹ thuật hướng dẫn để thống nhất quy trình kết nối, chia sẻ dữ liệu giữa các cơ quan nhà nước, tránh mỗi nơi thực hiện một kiểu. Bộ Công an với vai trò cơ quan đầu mối quản lý nhà nước về dữ liệu cần sớm phối hợp với Bộ Khoa học và Công nghệ và các bộ ngành khác ban hành các quy chế chia sẻ dữ liệu, hướng dẫn kỹ thuật thực thi (*như kết nối qua Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NDXP)*). Nhìn chung, việc sửa đổi, bổ sung pháp luật phải đảm bảo nguyên tắc “một lần khai báo, nhiều nơi sử dụng” thông tin người dân, doanh nghiệp đã có trong Cơ sở dữ liệu Quốc gia thì các cơ quan không được yêu cầu cung cấp lại dưới bất kỳ hình thức nào, trừ trường hợp pháp luật chuyên ngành có quy định đặc thù. Đây là yêu cầu quan trọng để cải cách thủ tục hành chính và tránh lãng phí trong thu thập dữ liệu.

5.2.1.2. Tiếp cận mở và thí điểm (sandbox) trong khai thác dữ liệu

Chính sách dữ liệu cần chuyển từ tư duy quản lý chặt sang tiếp cận mở, khuyến khích đổi mới sáng tạo. Luật Dữ liệu 2024 đã đưa ra khái niệm “dữ liệu mở” dữ liệu mà mọi cơ quan, tổ chức, cá nhân đều có thể tiếp cận và sử dụng. Theo luật, các cơ quan nhà nước có trách nhiệm công bố thông tin về dữ liệu mình quản lý và điều kiện tiếp cận trên môi trường mạng, đồng thời 100% cơ quan bộ, tỉnh phải cung cấp dữ liệu mở đảm bảo chất lượng trước 2030. Việc xây dựng Cổng dữ liệu quốc gia do Trung tâm dữ liệu quốc gia triển khai sẽ là đầu mối công bố dữ liệu mở, cung cấp dữ liệu mở nhằm tăng cường minh bạch, thúc đẩy sáng tạo và phát triển kinh tế - xã hội. Song song với mở dữ liệu, cần có cơ chế thử nghiệm có kiểm soát (*regulatory sandbox*) cho các mô hình khai thác dữ liệu mới.

Nhiều quốc gia đã áp dụng sandbox để doanh nghiệp thử nghiệm dịch vụ, mô hình kinh doanh dữ liệu trong khung pháp lý giới hạn, từ đó giúp nhà quản lý hoàn thiện chính sách. Tại Việt Nam, khái niệm thử nghiệm có kiểm soát lần đầu tiên được luật hóa trong Luật Khoa học, Công nghệ và Đổi mới sáng tạo 2025 cho



phép triển khai mô hình, công nghệ mới trong phạm vi giới hạn, có giám sát. Chính phủ nên nghiên cứu áp dụng cơ chế sandbox trong lĩnh vực dữ liệu, ví dụ: cho phép một số doanh nghiệp công nghệ thử nghiệm giải pháp phân tích dữ liệu lớn của Cơ sở dữ liệu tổng hợp Quốc gia hoặc phát triển dịch vụ API mở trên dữ liệu chính phủ trong môi trường thí điểm, trước khi triển khai diện rộng. Cơ chế này sẽ tháo gỡ rào cản pháp lý cho các sáng kiến dùng dữ liệu, đồng thời giúp cơ quan quản lý đánh giá rủi ro và hoàn thiện khung pháp luật về chia sẻ dữ liệu. Bên cạnh sandbox, cũng cần chính sách khuyến khích dữ liệu mở cộng đồng (*crowdsourcing data*): thu hút cá nhân, tổ chức đóng góp dữ liệu cho Nhà nước. Luật Dữ liệu đã khuyến khích tổ chức, cá nhân cung cấp dữ liệu do mình sở hữu cho cơ quan nhà nước và Trung tâm dữ liệu quốc gia có thể xây dựng cơ chế để các doanh nghiệp, người dân chia sẻ dữ liệu vì lợi ích chung, phục vụ nghiên cứu, hoạch định chính sách.



Hình ảnh: UBND Thành phố Hà Nội tổ chức lắng nghe ý kiến chuyên gia, nhà khoa học trong thực hiện nhiệm vụ thử nghiệm Sandbox. Ảnh: Báo KTĐT



5.2.1.3. Chính sách về quyền sở hữu dữ liệu và thúc đẩy kinh doanh dữ liệu

Luật Dữ liệu 2024 tạo nền tảng pháp lý quan trọng khi lần đầu tiên thừa nhận quyền sở hữu dữ liệu và coi quyền của chủ sở hữu dữ liệu là một loại quyền tài sản. Chủ sở hữu dữ liệu (*có thể là tổ chức, cá nhân*) có quyền quyết định việc xây dựng, phát triển, quản trị, xử lý, sử dụng dữ liệu và trao đổi giá trị dữ liệu do mình sở hữu. Điều này mở đường cho việc hình thành thị trường dữ liệu, nơi dữ liệu được mua bán, trao đổi hợp pháp. Để hiện thực hóa, Nhà nước cần sớm ban hành chính sách định giá dữ liệu và phân phối giá trị dữ liệu một cách công bằng. Hiện nay, một số dữ liệu công đã có giá phí sử dụng do Nhà nước quy định (*ví dụ dữ liệu dân cư, dữ liệu doanh nghiệp*). Như đã nêu, Luật Dữ liệu đã bổ sung danh mục phí khai thác thông tin Cơ sở dữ liệu tổng hợp Quốc gia và các Cơ sở dữ liệu Quốc gia khác. Tuy nhiên, cơ chế định giá cần linh hoạt dựa trên loại dữ liệu, phạm vi và mục đích sử dụng. Chính phủ có thể giao Bộ Tài chính phối hợp Bộ Công an (*cơ quan quản lý dữ liệu*) xây dựng khung định giá dữ liệu: dữ liệu phục vụ lợi ích công cộng có thể miễn phí; dữ liệu dùng chung giữa các cơ quan nhà nước có thể thu phí thấp (*hoặc không thu phí để khuyến khích chia sẻ*); dữ liệu kinh doanh chuyên sâu có thể định giá theo thị trường. Quan trọng là đảm bảo phân phối lợi ích: cơ quan, đơn vị thu thập dữ liệu gốc có thể được chia sẻ một phần phí khi dữ liệu của họ được khai thác trong Cơ sở dữ liệu tổng hợp Quốc gia. Ngoài ra, cần làm rõ quyền và trách nhiệm của các chủ thẻ liên quan: chủ thẻ dữ liệu (*người mà dữ liệu phản ánh*) có quyền gì trong việc dữ liệu của họ được khai thác? Luật Dữ liệu đã quy định nguyên tắc bảo đảm quyền con người, quyền công dân trong hoạt động dữ liệu và yêu cầu bảo vệ dữ liệu cá nhân trong mọi quá trình xử lý. Đặc biệt, đối với dữ liệu cá nhân, việc kinh doanh khai thác phải tuân thủ các quy định bảo vệ riêng tư. Hiện Việt Nam đã có Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, đòi hỏi sự đồng ý của chủ thẻ dữ liệu khi chia sẻ dữ liệu cá nhân trừ một số ngoại lệ. Vì vậy, chính sách kinh doanh dữ liệu cần cân bằng giữa khai thác giá trị dữ liệu với bảo vệ quyền riêng tư. Cơ sở dữ liệu tổng hợp Quốc gia nên ưu tiên cung cấp dữ liệu phi danh (*đã loại bỏ thông tin định*



danh cá nhân) hoặc dữ liệu tổng hợp, thống kê cho mục đích nghiên cứu, kinh doanh. Trong trường hợp dữ liệu cá nhân cần khai thác (*ví dụ xác thực danh tính cho dịch vụ tài chính*), phải có cơ chế cho phép và giám sát chặt chẽ, theo Luật Dữ liệu, tổ chức, cá nhân chỉ được khai thác dữ liệu cá nhân trong Cơ sở dữ liệu tổng hợp Quốc gia khi có sự đồng ý của Trung tâm dữ liệu quốc gia và của chính chủ thể dữ liệu. Về dài hạn, Nhà nước nên khuyến khích thành lập các doanh nghiệp dữ liệu chuyên cung cấp dịch vụ xử lý, phân tích dữ liệu; xây dựng sàn giao dịch dữ liệu quốc gia nhằm kết nối bên cung và cầu dữ liệu. Luật Dữ liệu cũng đề cập việc phát triển thị trường dữ liệu và sản phẩm, dịch vụ dữ liệu số; do đó, việc cụ thể hóa bằng các văn bản dưới luật về mô hình hoạt động của sàn dữ liệu, điều kiện kinh doanh dịch vụ dữ liệu là rất cần thiết. Tóm lại, nhóm giải pháp thê chế tập trung vào việc tạo hành lang pháp lý đầy đủ, linh hoạt để Cơ sở dữ liệu tổng hợp Quốc gia vận hành suôn sẻ, dữ liệu được chia sẻ và khai thác tối đa giá trị trong khuôn khổ pháp luật.

5.2.2. Đầu tư hạ tầng và công nghệ

5.2.2.1. Nâng cấp Trung tâm dữ liệu quốc gia

Hạ tầng kỹ thuật giữ vai trò quyết định trong việc triển khai hiệu quả Cơ sở dữ liệu tổng hợp Quốc gia. Luật Dữ liệu xác định Nhà nước ưu tiên đầu tư xây dựng Trung tâm dữ liệu quốc gia đáp ứng yêu cầu Chính phủ số, kinh tế số, xã hội số. Thực tế, Chính phủ đã giao Bộ Công an chủ trì triển khai xây dựng Trung tâm dữ liệu quốc gia, thể hiện qua việc Bộ Công an là cơ quan đầu mối quản lý nhà nước về dữ liệu. Việc nâng cấp Trung tâm dữ liệu quốc gia cần toàn diện trên các mặt: phần cứng, mạng và điện toán đám mây.

Thứ nhất, Trung tâm dữ liệu quốc gia phải có hạ tầng máy chủ mạnh mẽ, lưu trữ lớn, sẵn sàng tích hợp dữ liệu từ mọi bộ ngành. Theo quy định tại Điều 30 Luật Dữ liệu, cơ sở hạ tầng Trung tâm dữ liệu quốc gia phải đảm bảo tiêu chuẩn trung tâm dữ liệu hiện đại, có khả năng chống chịu cao (*chống bom đạn, thiên tai*), bảo vệ môi trường và tiết kiệm năng lượng. Điều này cho thấy yêu cầu đầu tư cơ sở vật chất đặc thù, ví dụ xây dựng trung tâm dữ liệu tại các khu vực an toàn,



trang bị hệ thống nguồn điện dự phòng, hệ thống làm mát và phòng chống cháy nổ đạt chuẩn.

- **Thứ hai**, về hạ tầng mạng, Trung tâm dữ liệu quốc gia cần mạng lưới băng thông cao và an toàn kết nối tới các bộ, ngành, tỉnh thành. Mô hình tối ưu là kiến trúc đa trung tâm dữ liệu (*multi-region*): ngoài trung tâm chính đặt tại Hà Nội, cần có các trung tâm dữ liệu vùng (*miền Bắc, Trung, Nam*) kết nối đồng bộ. Chiến lược Dữ liệu quốc gia 2030 đề ra mục tiêu đến năm 2030, 100% các Trung tâm dữ liệu quốc gia, trung tâm dữ liệu vùng, trung tâm dữ liệu lớn quốc gia được kết nối thành mạng lưới chia sẻ năng lực tính toán, xử lý dữ liệu lớn trên cả nước. Điều này định hướng phát triển một mạng lưới quốc gia về dữ liệu, các trung tâm chia sẻ tài nguyên, hỗ trợ lẫn nhau về lưu trữ và tính toán (*có thể thông qua công nghệ điện toán đám mây liên thông*).

- **Thứ ba**, Trung tâm dữ liệu quốc gia phải tiên phong triển khai điện toán đám mây chính phủ. Nghị định 165/2025/NĐ-CP nhấn mạnh Trung tâm dữ liệu quốc gia xây dựng hạ tầng điện toán đám mây và triển khai theo các vùng chức năng để phục vụ nhu cầu cơ quan nhà nước một cách linh hoạt, bảo đảm phát triển các phân hệ tích hợp, đồng bộ dữ liệu với yêu cầu cao về bảo mật. Hạ tầng đám mây này cần đáp ứng 100% nhu cầu lưu trữ, kết nối, chia sẻ dữ liệu của Việt Nam cũng như các yêu cầu an toàn thông tin theo Luật An toàn thông tin mạng. Việc chuyển các hệ thống CNTT bộ ngành lên nền tảng đám mây tại Trung tâm dữ liệu quốc gia sẽ tăng tính sẵn sàng và tiết kiệm chi phí do dùng chung hạ tầng. Tuy nhiên, quá trình này cần lộ trình phù hợp, Điều 46 Luật Dữ liệu cho phép các cơ quan có Cơ sở dữ liệu Quốc gia đã đầu tư hạ tầng riêng tiếp tục sử dụng hệ thống hiện có đến khi Trung tâm dữ liệu quốc gia đủ điều kiện tiếp nhận. Thủ tướng sẽ quyết định lộ trình chuyển đổi đó. Do vậy, trong 2-3 năm đầu, cần đầu tư nâng cấp Trung tâm dữ liệu quốc gia song song dẫn các bộ ngành dần di chuyển Cơ sở dữ liệu sang hạ tầng mới hoặc kết nối về Trung tâm dữ liệu quốc gia. Ngoài ra, Trung tâm dữ liệu quốc gia phải cung cấp dịch vụ hạ tầng đa dạng cho các cơ quan, từ dịch vụ đặt máy chủ (*co-location*), cho đến dịch vụ máy chủ ảo, lưu trữ,



an ninh mạng. Điều này đòi hỏi đầu tư đồng bộ cả phần cứng mạng (*router, firewall thế hệ mới*), hệ thống lưu trữ SAN/NAS dung lượng lớn và nền tảng ảo hóa, quản lý đám mây (*ví dụ OpenStack hoặc giải pháp tương đương*) để cung cấp máy chủ ảo theo yêu cầu. Tóm lại, việc nâng cấp Trung tâm dữ liệu quốc gia không chỉ là xây thêm máy chủ, mà là thiết lập một hạ tầng Trung tâm dữ liệu quốc gia hiện đại, linh hoạt, làm nền tảng vững chắc cho mọi ứng dụng dữ liệu.

5.2.2.2 Áp dụng công nghệ tiên tiến, mã hóa, định danh và trí tuệ nhân tạo:

Song song với đầu tư hạ tầng, việc tích hợp những công nghệ mới sẽ tăng cường hiệu quả quản lý và khai thác Cơ sở dữ liệu tổng hợp Quốc gia.

- **Trước hết**, công nghệ mã hóa dữ liệu phải được áp dụng xuyên suốt để bảo vệ thông tin nhạy cảm. Luật Dữ liệu định nghĩa rõ “mã hóa dữ liệu” là chuyển dữ liệu sang dạng không nhận biết được và yêu cầu triển khai các giải pháp kỹ thuật bảo vệ dữ liệu trong toàn bộ quá trình xử lý. Trung tâm dữ liệu quốc gia nên sử dụng các thuật toán mã hóa mạnh (*ví dụ AES-256*) cho dữ liệu lưu trữ và TLS/SSL cho dữ liệu truyền trên mạng, đảm bảo mã hóa khi lưu trữ và khi truyền tải (*data at rest và in transit*). Bên cạnh đó, cần xây dựng hệ thống quản lý khóa mã hóa tập trung, phân quyền chặt chẽ để chỉ những dịch vụ/hệ thống được cấp phép mới có thể giải mã dữ liệu tương ứng.

- **Thứ hai**, công nghệ định danh và xác thực đóng vai trò then chốt trong truy cập Cơ sở dữ liệu tổng hợp Quốc gia. Với hàng triệu giao dịch dữ liệu mỗi ngày giữa các cơ quan và với người dân, cần một hệ thống định danh điện tử tin cậy để xác định đúng đối tượng truy cập và phân quyền phù hợp. Hiện nay, Việt Nam đã có Nền tảng định danh và xác thực điện tử (*eID*) do Bộ Công an triển khai (*ứng dụng VNNeID*). Cơ sở dữ liệu tổng hợp Quốc gia cần tích hợp chặt chẽ với nền tảng này, mọi người dùng (*cán bộ hoặc công dân*) khi truy cập dữ liệu đều qua xác thực eID, đảm bảo đúng người, đúng quyền. Theo Nghị định 194/2025/NĐ-CP, các cách thức khai thác Cơ sở dữ liệu Quốc gia bao gồm truy cập trực tuyến qua Cổng dữ liệu quốc gia, Cổng Dịch vụ công quốc gia, Cổng thông tin điện tử của cơ quan dữ liệu, ứng dụng định danh quốc gia (*VNNeID*) và



nền tảng xác thực điện tử. Điều này cho thấy vai trò của hệ thống định danh điện tử trong kiến trúc khai thác Cơ sở dữ liệu tổng hợp Quốc gia. Mỗi truy cập cần được ghi nhật ký (*log*) để truy vết và kiểm soát.

- **Thứ ba**, ứng dụng trí tuệ nhân tạo (*AI*) và phân tích dữ liệu lớn sẽ nâng tầm giá trị của Cơ sở dữ liệu tổng hợp Quốc gia. Với khối lượng dữ liệu tập trung khổng lồ, Trung tâm dữ liệu quốc gia nên thiết lập các hệ thống phân tích dữ liệu hiệu năng cao. Nghị định 165/2025/NĐ-CP đã nêu rõ Trung tâm dữ liệu quốc gia phải thiết lập hạ tầng tính toán hiệu suất cao và hệ thống phân tích dữ liệu phục vụ công tác quản lý, với các mô hình phân tích dự báo khai thác từ Cơ sở dữ liệu tổng hợp Quốc gia. Như vậy, cần triển khai các cụm máy chủ GPU, nền tảng big data (*Hadoop, Spark*) và các công cụ AI/ML để xử lý dữ liệu phi cấu trúc, dữ liệu thời gian thực. Ví dụ: AI có thể được dùng để phân tích xu hướng xã hội từ dữ liệu dân cư, dự báo kinh tế dựa trên dữ liệu doanh nghiệp, hoặc phát hiện gian lận trong dữ liệu bảo hiểm, tài chính công. Việc tích hợp AI cũng giúp tự động hóa quản trị; ví dụ AI hỗ trợ làm sạch và chuẩn hóa dữ liệu, phát hiện dữ liệu sai lệch để cảnh báo. Tuy nhiên, ứng dụng AI đòi hỏi có hạ tầng tính toán tương xứng (*như đề cập ở trên*) và đội ngũ chuyên gia phân tích dữ liệu đủ mạnh. Ngoài ra, công nghệ blockchain cũng có thể cân nhắc trong một số trường hợp để đảm bảo tính bất biến và minh bạch của dữ liệu chia sẻ, nhất là khi chia sẻ với khu vực tư. Ví dụ: một blockchain riêng (*private blockchain*) có thể dùng để ghi lại mọi giao dịch truy xuất dữ liệu liên bộ, giúp kiểm toán dễ dàng. Tóm lại, việc áp dụng công nghệ tiên tiến từ mã hóa, định danh đến AI sẽ giúp Cơ sở dữ liệu tổng hợp Quốc gia vận hành an toàn, thông minh hơn, tối ưu hóa quy trình xử lý và tạo ra giá trị gia tăng từ dữ liệu.

5.2.2.3. Kiến trúc bảo mật đa tầng (mô hình ba lớp)

An ninh dữ liệu là ưu tiên hàng đầu khi xây dựng Cơ sở dữ liệu tổng hợp Quốc gia, bởi đây sẽ là kho dữ liệu tập trung của quốc gia. Do đó, cần một kiến trúc bảo mật nhiều lớp, đảm bảo phòng thủ chiều sâu. Mô hình phổ biến là bảo



mật 3 lớp từ ngoại vi đến nội bộ (*Hà tầng và Mạng - Ứng dụng và Điểm cuối - Dữ liệu*) kết hợp các giải pháp kỹ thuật tương ứng.

- **Thứ nhất**, lớp bảo mật hạ tầng và mạng bảo vệ chu vi hệ thống. Đây là lớp phòng thủ tuyến đầu, tập trung vào ngăn chặn các tấn công từ bên ngoài vào trung tâm dữ liệu và mạng chính phủ. Giải pháp triển khai gồm tường lửa thế hệ mới (*Next-Gen Firewall*) để kiểm soát lưu lượng mạng, hệ thống phát hiện/ngăn chặn xâm nhập (*IDS/IPS*) để nhận diện và chặn các hành vi tấn công mạng. Bên cạnh đó, cần có giải pháp chống tấn công DDoS bảo vệ băng thông của Trung tâm dữ liệu quốc gia trước các cuộc tấn công từ chối dịch vụ phân tán. Mạng Trung tâm dữ liệu quốc gia cũng nên được phân đoạn (*network segmentation*) thành các vùng (*zone*) riêng biệt cho từng nhóm hệ thống (*vùng DMZ cho dịch vụ công, vùng nội bộ cho Cơ sở dữ liệu tổng hợp Quốc gia, vùng quản trị,...*). Việc phân đoạn giúp nếu một vùng bị xâm nhập, kẻ tấn công không dễ lan sang vùng khác. Lớp hạ tầng còn bao gồm bảo mật vật lý, kiểm soát ra vào trung tâm dữ liệu bằng sinh trắc học, camera giám sát, hệ thống báo cháy tự động... đáp ứng tiêu chuẩn an ninh Tier 3 hoặc Tier 4 cho data center. Luật Dữ liệu cũng yêu cầu hạ tầng Trung tâm dữ liệu quốc gia phải có giải pháp kiểm soát, phát hiện, ngăn chặn đột nhập, phá hoại, bảo đảm hệ thống có dự phòng và sẵn sàng mở rộng.

- **Thứ hai**, lớp bảo mật ứng dụng và điểm cuối bảo vệ các máy chủ và phần mềm. Lớp này bảo vệ các máy chủ, ứng dụng và thiết bị đầu cuối (*máy trạm*) truy cập hệ thống. Trên các máy chủ ứng dụng và cơ sở dữ liệu, cần thường xuyên kiểm tra, vá lỗ hổng bảo mật (*patch management*) để tránh bị khai thác. Triển khai các giải pháp bảo mật ứng dụng web (*Web Application Firewall - WAF*) để lọc các cuộc tấn công như SQL injection, XSS đối với các cổng dịch vụ công và API kết nối. Đối với điểm cuối (*endpoint*) như máy tính cán bộ, cần cài giải pháp Endpoint Detection và Response (*EDR*) để giám sát hành vi bất thường, ngăn chặn malware, ransomware xâm nhập. Hệ thống quản lý danh tính và truy cập (*IAM*) cũng thuộc lớp này, đảm bảo mỗi người dùng chỉ được truy cập những dữ liệu, chức năng theo vai trò của mình. Việc phân quyền truy cập theo nguyên tắc đủ



dùng (*least privilege*) kết hợp xác thực đa yếu tố (*MFA*) sẽ giảm nguy cơ rò rỉ dữ liệu do lạm quyền. Luật Dữ liệu yêu cầu cơ quan quản lý dữ liệu phải cung cấp công cụ và phân quyền truy cập để bảo đảm an toàn, khuyến khích áp dụng rộng rãi các biện pháp xác thực an toàn. Ngoài ra, lớp này cũng bao gồm bảo mật thiết bị di động nếu có truy cập từ xa: sử dụng VPN an toàn, xác thực thiết bị đáng tin cậy (*trusted device*).

- **Thứ ba**, lớp bảo mật dữ liệu bảo vệ chính dữ liệu quan trọng. Đây là lớp trọng yếu, bảo vệ trực tiếp các dữ liệu lưu trong Cơ sở dữ liệu tổng hợp Quốc gia. Trước hết, thực hiện mã hóa dữ liệu nhạy cảm ở mức cơ sở dữ liệu hoặc file hệ thống, dữ liệu công dân, doanh nghiệp, tài chính... nên được mã hóa bằng thuật toán mạnh. Kèm theo đó là triển khai quản lý khóa an toàn và hạn chế số người có quyền giải mã. Tiếp theo, cần chính sách phân loại dữ liệu theo mức độ quan trọng (*cốt lõi, quan trọng, thông thường*) và áp dụng biện pháp bảo vệ tương ứng. Dữ liệu cốt lõi, quan trọng đòi hỏi bảo mật cao hơn, có thể lưu ở khu vực riêng, giới hạn truy cập theo thời gian thực. Một giải pháp hữu ích là hệ thống ngăn ngừa mất mát dữ liệu (*DLP*) nhằm giám sát và ngăn chặn hành vi rò rỉ dữ liệu ra ngoài (*qua email, USB, in ấn...*).Thêm nữa, thiết lập cơ chế sao lưu và phục hồi (*backup và recovery*) thường xuyên cho Cơ sở dữ liệu tổng hợp Quốc gia. Các bản sao lưu nên được mã hóa và lưu trữ tại địa điểm cách ly, phòng khi trung tâm chính gặp sự cố vẫn có thể khôi phục dữ liệu. Trung tâm dữ liệu quốc gia cũng nên có kế hoạch phục hồi thảm họa (*disaster recovery*) ở cấp quốc gia: duy trì một site dự phòng (*đặt ở nơi địa lý khác*) để đảm bảo tính liên tục của dịch vụ trong tình huống xấu.

- **Cuối cùng**, quan trọng không kém là giám sát an ninh 24/7. Trung tâm dữ liệu quốc gia cần có hệ thống giám sát bảo mật tập trung để thu thập nhật ký từ các thiết bị, ứng dụng ở cả 3 lớp trên, phân tích và cảnh báo sớm nguy cơ. Luật Dữ liệu yêu cầu thiết lập hệ thống bảo vệ dữ liệu thông nhất để đánh giá rủi ro an ninh và cảnh báo sớm trên phạm vi toàn quốc. Song song, xây dựng đội ứng cứu sự cố luôn sẵn sàng cô lập và xử lý nếu phát hiện tấn công. Với kiến trúc bảo mật



đa tầng như trên, Cơ sở dữ liệu tổng hợp Quốc gia sẽ được bảo vệ nhiều lớp, hạn chế tối đa khả năng bị tấn công thành công. Điều này đặc biệt quan trọng vì chỉ một lỗ hổng ở bất kỳ lớp nào cũng có thể đe dọa an toàn cho kho dữ liệu quốc gia.



Hình ảnh: Trung tâm dữ liệu và nền tảng điện toán đám mây của CMC Telecom đạt chuẩn an toàn thông tin cấp độ 4. Ảnh: Bộ Khoa học và Công nghệ

5.2.3. Chuẩn hóa và nâng cao chất lượng dữ liệu

5.2.3.1 Áp dụng tiêu chuẩn kỹ thuật trong quản lý dữ liệu

Chất lượng dữ liệu quyết định trực tiếp đến hiệu quả khai thác Cơ sở dữ liệu tổng hợp Quốc gia. Do đó, việc chuẩn hóa dữ liệu theo các tiêu chuẩn, quy chuẩn kỹ thuật chung là ưu tiên hàng đầu. Điều 28 Luật Dữ liệu 2024 quy định về tiêu chuẩn, quy chuẩn kỹ thuật cho dữ liệu. Theo đó, tiêu chuẩn về dữ liệu bao gồm tiêu chuẩn cho hệ thống thông tin, phần cứng, phần mềm, quy trình vận hành, đảm bảo chất lượng và bảo vệ dữ liệu - được công bố hoặc thừa nhận áp dụng tại Việt Nam. Còn quy chuẩn kỹ thuật về dữ liệu là các quy chuẩn cho những yếu tố tương tự, do cơ quan có thẩm quyền xây dựng và ban hành để áp dụng trong nước. Như vậy, có thể hiểu tiêu chuẩn gồm cả tiêu chuẩn quốc tế (*ISO, IEC...*) mà Việt Nam chấp nhận, còn quy chuẩn là những quy định kỹ thuật bắt buộc áp dụng trong phạm vi quốc gia. Bộ Công an được giao chủ trì ban hành danh mục các tiêu



chuẩn, quy chuẩn kỹ thuật về dữ liệu (*trừ lĩnh vực quốc phòng, cơ yếu*). Trên cơ sở đó, các cơ quan quản lý Cơ sở dữ liệu Quốc gia và Cơ sở dữ liệu chuyên ngành phải xây dựng các tiêu chuẩn, quy chuẩn cụ thể cho dữ liệu thuộc phạm vi mình quản lý, tuân theo danh mục chung đã ban hành. Trong quá trình triển khai, cần ưu tiên áp dụng các tiêu chuẩn quốc tế uy tín: ví dụ ISO/IEC 27001 về hệ thống quản lý an ninh thông tin (*đảm bảo an toàn dữ liệu*), ISO/IEC 25012 về chất lượng dữ liệu (*định nghĩa các thuộc tính chất lượng như tính đầy đủ, chính xác, nhất quán của dữ liệu*), ISO/IEC 11179 về quản lý siêu dữ liệu (*metadata*)... Bên cạnh đó, các tiêu chuẩn quốc gia (*TCVN*) trong lĩnh vực CNTT cũng phải được cập nhật phù hợp xu thế chuyển đổi số. Một ví dụ quan trọng là tiêu chuẩn về mã định danh dữ liệu: cần có danh mục mã dùng chung (*mã tỉnh, mã ngành, mã giới tính, mã quốc gia...*) áp dụng thống nhất trên toàn bộ hệ thống. Nghị định 47/2024 đã yêu cầu khi tạo lập dữ liệu trong Cơ sở dữ liệu Quốc gia phải sử dụng thống nhất các bảng mã danh mục dùng chung do cơ quan có thẩm quyền ban hành. Nếu mỗi bộ ngành dùng một mã khác nhau (ví dụ *mã tỉnh của Bộ Y tế khác mã tỉnh của Bộ GD&ĐT*) sẽ gây khó khăn khi tích hợp dữ liệu. Do đó, chuẩn hóa danh mục, mã định danh là việc cần làm sớm nhằm đảm bảo tính tương thích. Ngoài ra, các chuẩn về định dạng dữ liệu (*nhiều JSON, XML, CSV theo quy định của NDXP*), chuẩn giao thức kết nối (*API, web services RESTful hoặc SOAP, tuân thủ Khung kiến trúc Chính phủ điện tử*) cũng cần thống nhất. Luật Giao dịch điện tử mới (*sửa đổi 2023*) đã xác định kiến trúc chia sẻ dữ liệu quốc gia bao gồm nền tảng tích hợp quốc gia và hạ tầng kết nối dữ liệu bộ, tỉnh theo Khung kiến trúc tổng thể Chính phủ số. Điều này có nghĩa việc kết nối, chia sẻ phải tuân theo các chuẩn giao thức và mô hình dữ liệu chung do Bộ KH&CN ban hành. Tóm lại, áp dụng tiêu chuẩn kỹ thuật giúp dữ liệu trong Cơ sở dữ liệu tổng hợp Quốc gia có “ngôn ngữ chung”, dễ dàng kết nối, trao đổi và duy trì chất lượng đồng đều.

5.2.3.2 Quy trình kiểm soát chất lượng dữ liệu toàn diện

Để Cơ sở dữ liệu tổng hợp Quốc gia trở thành “nguồn dữ liệu tin cậy duy nhất” cho mọi hoạt động, cần thiết lập quy trình quản lý chất lượng dữ liệu khép



kín từ thu thập → xử lý → lưu trữ → khai thác. Điều 12 Luật Dữ liệu quy định về bảo đảm chất lượng dữ liệu, trong đó nêu rõ chất lượng dữ liệu bao gồm tính chính xác, hợp lệ, toàn vẹn, đầy đủ, cập nhật kịp thời và thống nhất. Trách nhiệm đảm bảo chất lượng được đặt trước tiên lên cơ quan nhà nước quản lý CSDL. Các cơ quan này phải xây dựng quy trình và triển khai các biện pháp kiểm soát chất lượng. Cụ thể: ⁽¹⁾Hướng dẫn và áp dụng đồng bộ các tiêu chuẩn quốc gia về bảo đảm chất lượng dữ liệu, thiết lập quy trình đảm bảo chất lượng cho Cơ sở dữ liệu minh quản lý. ⁽²⁾ Thường xuyên kiểm tra, giám sát dữ liệu; phối hợp cập nhật, hiệu chỉnh sai sót để đảm bảo dữ liệu luôn chính xác, đầy đủ trong quá trình khai thác. Trên thực tế, để thực hiện những yêu cầu này, nên xây dựng một chu trình quản lý chất lượng dữ liệu rõ ràng.

Bước đầu tiên, khi thu thập dữ liệu ban đầu, cần có khâu kiểm tra hợp lệ (*validation*): ví dụ khi nhập thông tin dân cư phải đúng định dạng (*số CMND/CCCD đủ độ dài, ngày sinh hợp lệ, mã tỉnh tồn tại,...*). Các nguồn dữ liệu đưa vào Cơ sở dữ liệu tổng hợp Quốc gia gồm kết quả thủ tục hành chính, dữ liệu đồng bộ từ Cơ sở dữ liệu khác, dữ liệu số hóa từ tài liệu..., do đó khâu thu thập cần kết hợp cả kiểm tra tự động và kiểm định thủ công để sàng lọc lỗi. Bước tiếp theo, trong xử lý và tích hợp, phải đảm bảo nhất quán dữ liệu. Luật quy định Trung tâm dữ liệu quốc gia phối hợp kiểm tra dữ liệu khi thu thập, cập nhật, đồng bộ để bảo đảm tính chính xác, thống nhất; nếu phát hiện dữ liệu từ các nguồn không khớp, phải đối soát và cập nhật lại trong các Cơ sở dữ liệu liên quan. Ví dụ: nếu Cơ sở dữ liệu dân cư cho thấy một người đã mất nhưng Cơ sở dữ liệu bảo hiểm xã hội vẫn ghi đang hưởng lương hưu, hệ thống cần phát hiện mâu thuẫn này và điều phối cập nhật kịp thời.

Để làm được, cần xây dựng các quy tắc nghiệp vụ (*business rules*) tự động kiểm tra chéo dữ liệu giữa các nguồn.Thêm nữa, khâu xử lý còn bao gồm chuẩn hóa dữ liệu: thống nhất đơn vị đo, định dạng (ví dụ *ngày tháng năm*), loại bỏ dữ liệu trùng lặp dư thừa. Bước lưu trữ dữ liệu cũng có yêu cầu, Cơ sở dữ liệu Quốc gia bắt buộc lưu trữ trên hạ tầng Trung tâm dữ liệu quốc gia, còn Cơ sở dữ liệu chuyên ngành có thể lưu trên hạ tầng riêng nếu đáp ứng tiêu chuẩn trung tâm dữ



liệu. Dù lưu ở đâu, dữ liệu cốt lõi, quan trọng phải tuân thủ quy định bảo vệ đặc biệt. Các cơ quan cần quy định thời gian cập nhật từng loại dữ liệu (*theo thời gian thực, hàng ngày, hàng tháng*) để tránh dữ liệu “cũ” gây sai lệch. Cuối cùng, ở khâu khai thác, cần cơ chế phản hồi và hiệu chỉnh. Người dùng dữ liệu (*cơ quan, doanh nghiệp, người dân*) nếu phát hiện sai sót trong dữ liệu phải có cách báo cho cơ quan quản lý để cập nhật. Luật Dữ liệu cho phép cơ quan, tổ chức, cá nhân đề xuất sửa đổi, bổ sung thông tin trong Cơ sở dữ liệu Quốc gia, đồng thời yêu cầu thông tin từ kết quả thủ tục hành chính phải đồng bộ vào Cơ sở dữ liệu Quốc gia ngay sau khi thực hiện xong thủ tục.

Như vậy, nếu công dân thay đổi địa chỉ đăng ký qua thủ tục hành chính, dữ liệu địa chỉ trong Cơ sở dữ liệu dân cư và các Cơ sở dữ liệu liên quan phải cập nhật ngay. Một chu trình PDCA (*Plan-Do-Check-Act*) có thể áp dụng: lập kế hoạch chất lượng (*Plan*), thu thập và xử lý (*Do*), kiểm tra giám sát thường xuyên (*Check*) và khắc phục, cải tiến (*Act*). Việc kiểm tra định kỳ chất lượng có thể đo bằng các chỉ số chất lượng dữ liệu (*data quality metrics*) như tỷ lệ lỗi, tỷ lệ trùng lặp, mức độ đầy đủ... Trung tâm dữ liệu quốc gia được giao nhiệm vụ giám sát chất lượng dữ liệu, xây dựng hệ thống chỉ số đo lường đánh giá hiệu suất quản trị dữ liệu. Những chỉ số này sẽ giúp nhận biết điểm yếu để cải thiện liên tục. Tóm lại, thông qua chuẩn hóa và quy trình kiểm soát chất lượng nghiêm ngặt, Cơ sở dữ liệu tổng hợp Quốc gia mới đảm bảo cung cấp dữ liệu “đúng, đủ, sạch” phục vụ các hoạt động quản lý và phát triển.

5.2.4. Phát triển nguồn nhân lực và nâng cao nhận thức

5.2.4.1. Đào tạo chuyên gia dữ liệu và an ninh mạng

Yếu tố con người có tính quyết định đến thành bại của việc triển khai Cơ sở dữ liệu tổng hợp Quốc gia. Do vậy, cần phát triển mạnh mẽ nguồn nhân lực chuyên trách về dữ liệu và an toàn thông tin. Trước hết, cần hình thành đội ngũ chuyên gia quản trị dữ liệu tại các bộ, ngành và địa phương. Những người này am hiểu cả nghiệp vụ lẫn công nghệ, chịu trách nhiệm quản lý chất lượng và khai thác dữ liệu trong lĩnh vực được giao. Luật Dữ liệu nhấn mạnh việc đào



tạo, bồi dưỡng nâng cao năng lực cho người làm công tác dữ liệu, đồng thời có cơ chế thu hút nhân lực trình độ cao để phát triển dữ liệu quốc gia.

Thực hiện điều này, Chính phủ có thể chỉ đạo mở các khóa đào tạo chuyên sâu về quản trị dữ liệu, khoa học dữ liệu cho cán bộ CNTT hiện có trong khu vực công. Các trường đại học cần cập nhật chương trình đào tạo về khoa học dữ liệu, phân tích dữ liệu lớn gắn với nhu cầu của cơ quan nhà nước. Song song, cần phát triển đội ngũ chuyên gia an ninh mạng phụ trách bảo vệ Cơ sở dữ liệu tổng hợp Quốc gia. Những chuyên gia này phải thành thạo về bảo mật hệ thống, phòng chống tấn công mạng, quản trị các thiết bị an ninh (*firewall, IDS/IPS, SIEM...*). Luật Dữ liệu đã liệt kê “đào tạo, bồi dưỡng, phát triển, quản lý nguồn nhân lực” là một trong các biện pháp bảo vệ dữ liệu bắt buộc. Điều đó cho thấy yêu cầu không chỉ đào tạo kiến thức, mà còn xây dựng cơ chế quản lý nhân sự làm việc với dữ liệu (*phân cấp quyền hạn rõ ràng, giám sát tuân thủ*). Một đề xuất cụ thể là thiết lập chương trình Chứng nhận chuyên gia dữ liệu quốc gia, qua đó tổ chức thi và cấp chứng chỉ cho cán bộ đạt kỹ năng quản trị dữ liệu theo tiêu chuẩn. Tương tự, có thể phối hợp với các tổ chức như ISC², ISACA để đào tạo và chứng nhận chuyên gia an ninh thông tin (*ví dụ chứng chỉ CISSP, CISM*) cho nhân sự chủ chốt. Ngoài đào tạo trong nước, cần cử nhân sự đi học tập ở các nước phát triển có kinh nghiệm về quản lý dữ liệu số, nhằm tiếp thu kiến thức mới. Về dài hạn, nên đưa nội dung dữ liệu số vào chương trình đào tạo công chức, viên chức như một kỹ năng căn bản trong chính phủ số.

5.2.4.2 Chính sách thu hút và đai ngộ nhân tài:

Bên cạnh đào tạo tại chỗ, Nhà nước cần chính sách đủ mạnh để thu hút nhân tài về dữ liệu từ thị trường lao động. Các chuyên gia giỏi về khoa học dữ liệu, quản lý hệ thống lớn thường được doanh nghiệp săn đón, do đó khu vực nhà nước phải có cơ chế đai ngộ phù hợp để cạnh tranh. Luật Dữ liệu đã nêu Nhà nước có cơ chế thu hút nhân lực trình độ cao để xây dựng, phát triển dữ liệu quốc gia và đảm bảo nguồn nhân lực cho hoạt động của Trung tâm dữ liệu quốc gia, có chế độ đai ngộ với nhân lực chất lượng cao. Cụ thể hóa điều này, Chính phủ có thể xem xét một số giải pháp: ⁽¹⁾Tuyên dụng đặc cách hoặc hợp đồng linh hoạt các chuyên gia giỏi



ngoài khu vực công, bỏ bớt các rào cản hành chính trong tuyển dụng.⁽²⁾ Chính sách lương, thưởng cạnh tranh, cho phép trả lương tương xứng với trình độ và hiệu quả công việc, cao hơn khung chung nếu cần, kèm thưởng dự án, thưởng sáng kiến. Có thể sử dụng Quỹ phát triển dữ liệu quốc gia để hỗ trợ kinh phí cho các hoạt động phát triển dữ liệu, kể cả trả thù lao chuyên gia.⁽³⁾ Môi trường làm việc hấp dẫn: Xây dựng Trung tâm dữ liệu quốc gia theo mô hình tổ chức khoa học công nghệ hoặc doanh nghiệp nhà nước để có cơ chế linh hoạt, trao quyền chủ động cho nhân sự sáng tạo. Khuyến khích văn hóa “dữ liệu mở” trong cơ quan, giảm tư duy cục bộ.⁽⁴⁾ Hợp tác công tư về nhân lực, thuê chuyên gia từ doanh nghiệp tư vấn tham gia các dự án triển khai Cơ sở dữ liệu tổng hợp Quốc gia; đồng thời đưa cán bộ nhà nước sang doanh nghiệp công nghệ thực tập nâng cao kỹ năng. Một hướng khác là phát triển mạng lưới chuyên gia dữ liệu Việt Nam trên toàn cầu, mời gọi chuyên gia Việt Kiều, chuyên gia quốc tế tham gia theo hình thức cố vấn từ xa hoặc về nước làm việc ngắn hạn cho các dự án dữ liệu quốc gia. Bằng những chính sách linh hoạt và đai ngô phù hợp, chúng ta có thể xây dựng được đội ngũ nhân sự vừa hồng vừa chuyên, đủ sức đảm đương nhiệm vụ chuyển đổi số dựa trên dữ liệu.



Hình ảnh: Tọa đàm khoa học "Đào tạo ngành Khoa học Dữ liệu - Triển vọng và Xu hướng" do Học viện Ngân hàng tổ chức. Ảnh: Báo TTTĐ



5.2.4.3. Nâng cao nhận thức cộng đồng về giá trị dữ liệu

Để Cơ sở dữ liệu tổng hợp Quốc gia được ứng dụng rộng rãi và bền vững, không chỉ giới chuyên môn mà toàn xã hội cần hiểu rõ vai trò và cách thức sử dụng dữ liệu. Do đó, cần triển khai các chương trình truyền thông, giáo dục nhằm nâng cao nhận thức cộng đồng về “văn hóa dữ liệu”.

- **Trước hết**, đối với đội ngũ lãnh đạo, quản lý các cấp cần nhấn mạnh chuyển đổi số là chuyển đổi dựa trên dữ liệu, dữ liệu là tài sản chiến lược của tổ chức. Việc ra quyết định dựa trên dữ liệu (*data-driven decision making*) phải trở thành thói quen trong quản trị công. Các khóa bồi dưỡng lãnh đạo nên bổ sung nội dung về khai thác dữ liệu, phân tích dữ liệu hỗ trợ chính sách.

- **Thứ hai**, đối với công chức, viên chức trong hệ thống, mỗi người cần ý thức trách nhiệm trong chia sẻ dữ liệu liên thông, thay vì tư duy “cát cứ dữ liệu”. Luật Dữ liệu quy định dữ liệu dùng chung, dữ liệu mở trong cơ quan nhà nước mặc định phải chia sẻ cho cơ quan khác khi có yêu cầu hợp lý, trừ phi từ chối phải có căn cứ pháp luật rõ ràng. Tinh thần này cần được quán triệt đến từng cán bộ để xóa bỏ rào cản cục bộ. Các bộ ngành có thể tổ chức các buổi tập huấn nội bộ về lợi ích của Cơ sở dữ liệu tổng hợp Quốc gia. Ví dụ chia sẻ dữ liệu dân cư giúp tiết kiệm thời gian xử lý hồ sơ, giảm phiền hà cho dân...

- **Thứ ba**, phải tuyên truyền để doanh nghiệp và người dân hiểu quyền lợi khi sử dụng các dịch vụ dữ liệu số do Nhà nước cung cấp, đồng thời hiểu trách nhiệm bảo vệ dữ liệu cá nhân. Ví dụ: cần hướng dẫn người dân sử dụng ứng dụng VNNeID, VssID để tích hợp các thông tin cá nhân (*BHYT, giấy tờ lái xe...*) phục vụ giao dịch hành chính. Kết quả triển khai Đề án 06 cho thấy việc tích hợp thẻ Bảo hiểm y tế vào căn cước công dân gắn chip và ứng dụng VNNeID giúp người dân đi khám chữa bệnh không cần mang thẻ giấy, giảm thủ tục và gian lận. Những hiệu quả thiết thực này cần được truyền thông rộng rãi trên báo chí, mạng xã hội để người dân thấy lợi ích của việc dùng dữ liệu số. Đồng thời, cũng cần cảnh báo người dân về các nguy cơ khi làm lộ dữ liệu cá nhân, khuyến khích họ chủ động bảo vệ thông tin của mình (*nhiều không chia sẻ mã OTP, cẩn trọng khi cung cấp*



thông tin trên mạng). Nhà nước có thể phát động các chiến dịch như “Ngày dữ liệu mở”, tổ chức hackathon về dữ liệu để cộng đồng tham gia sáng tạo ứng dụng từ dữ liệu mở chính phủ. Đây vừa là cách quảng bá kho dữ liệu quốc gia, vừa thu hút giới trẻ, startup quan tâm đến lĩnh vực dữ liệu. Ngoài ra, hợp tác với các tổ chức quốc tế, viện nghiên cứu để tổ chức hội nghị, hội thảo về chuyển đổi số và quản trị dữ liệu cũng giúp nâng cao nhận thức xã hội ở tầm vĩ mô. Tóm lại, xây dựng thành công Cơ sở dữ liệu tổng hợp Quốc gia đòi hỏi sự chuyển biến nhận thức từ trên xuống dưới, từ trong ra ngoài - để mọi người cùng hiểu rằng dữ liệu là tài sản chung và việc khai thác, bảo vệ nó cần sự chung tay của cả cộng đồng.

5.2.5. *Ứng dụng trong cơ quan nhà nước và kinh tế - xã hội*

5.2.5.1. *Thúc đẩy chuyển đổi số trong cơ quan nhà nước*

Cơ sở dữ liệu tổng hợp quốc gia là nền tảng quan trọng để hiện thực hóa Chính phủ số, do đó việc ứng dụng nó trước tiên phải diễn ra mạnh mẽ trong các cơ quan nhà nước. Một trong những mục tiêu đến năm 2030 là 100% các Cơ sở dữ liệu Quốc gia ưu tiên được số hóa, kết nối, chia sẻ với kho dữ liệu tổng hợp tại Trung tâm dữ liệu quốc gia và trên toàn quốc. Điều này có nghĩa các bộ, ngành phải khai thác Cơ sở dữ liệu tổng hợp Quốc gia như một trục liên thông dữ liệu trong mọi hoạt động. Cụ thể, các phần mềm quản lý và điều hành trong cơ quan (*quản lý nhân sự, tài chính, nghiệp vụ chuyên ngành*) cần tích hợp chức năng truy xuất dữ liệu từ Cơ sở dữ liệu tổng hợp Quốc gia thay vì yêu cầu nhập liệu thủ công. Ví dụ: khi một cán bộ xử lý hồ sơ doanh nghiệp, hệ thống của Bộ Tài chính có thể tự động tra cứu thông tin công ty từ Cơ sở dữ liệu đăng ký doanh nghiệp (đã nằm trong Cơ sở dữ liệu tổng hợp Quốc gia) thay vì yêu cầu doanh nghiệp nộp bản sao giấy Đăng ký kinh doanh. Việc tái sử dụng dữ liệu giúp giảm rất nhiều thời gian và sai sót. Theo Chiến lược dữ liệu quốc gia, mục tiêu đặt ra là 80% dữ liệu về kết quả thủ tục hành chính được tái sử dụng, chia sẻ giữa các cơ quan, đảm bảo người dân và doanh nghiệp chỉ phải cung cấp thông tin một lần khi làm dịch vụ công.



Hình ảnh: Lãnh đạo Bộ Nội vụ cùng lãnh đạo các đơn vị bấm nút công bố hoàn thành việc xây dựng Cơ sở dữ liệu quốc gia về cán bộ, công chức, viên chức trong các cơ quan nhà nước. Ảnh: Báo Chính phủ

Để đạt được, các hệ thống một cửa điện tử, Cổng dịch vụ công từ trung ương đến địa phương phải kết nối chặt với Cơ sở dữ liệu tổng hợp Quốc gia. Khi người dân nộp hồ sơ trực tuyến, hệ thống nên tự động điền sẵn các thông tin cơ bản (họ tên, CCCD, hộ khẩu...) từ Cơ sở dữ liệu dân cư, hoặc thông tin doanh nghiệp từ Cơ sở dữ liệu đăng ký kinh doanh, để người dân không phải khai báo lại. Bên cạnh thủ tục hành chính, Cơ sở dữ liệu tổng hợp Quốc gia còn phục vụ công tác chỉ đạo điều hành. Các cơ quan có thể khai thác dữ liệu tổng hợp để xây dựng báo cáo thông minh, bảng thông tin điều hành (dashboard) hỗ trợ lãnh đạo ra quyết định. Ví dụ: Thủ tướng Chính phủ có thể dùng bảng điều khiển hiển thị các chỉ số kinh tế - xã hội theo thời gian thực được lấy từ Cơ sở dữ liệu tổng hợp Quốc gia (dữ liệu từ Bộ Tài chính, Ngân hàng nhà nước, Bộ Nội vụ... tích hợp). Việc này hiện nay còn hạn chế do dữ liệu phân tán, nhưng với Cơ sở dữ liệu tổng hợp Quốc gia, khả năng tổng hợp sẽ nhanh hơn nhiều. Hơn nữa, trong quản lý nội bộ, các tác vụ như báo cáo thống kê, chế độ báo cáo có thể được tự động hóa nhờ dữ liệu sẵn có. Luật Dữ liệu cho phép Cơ sở dữ liệu tổng hợp Quốc gia cung cấp thông tin để làm báo cáo điều tra, khảo sát mà không cần triển khai các cuộc điều tra thủ công, từ đó giảm tải các thủ tục thẩm định chỉ tiêu, phương án điều tra thống kê.



Nói cách khác, dữ liệu số sẽ thay thế một phần công việc hành chính giấy tờ, giúp bộ máy vận hành hiệu quả và minh bạch hơn. Điều kiện tiên quyết là lãnh đạo các cơ quan phải cam kết và chỉ đạo quyết liệt việc sử dụng dữ liệu, coi dữ liệu là cơ sở cho mọi quyết sách, giảm dần sự phụ thuộc vào báo cáo giấy hay kinh nghiệm chủ quan.

5.2.5.2. Cải cách thủ tục hành chính dựa trên dữ liệu

Một lợi ích rõ rệt của Cơ sở dữ liệu tổng hợp Quốc gia là tạo bước đột phá trong cải cách thủ tục hành chính. Khi các Cơ sở dữ liệu Quốc gia (*dân cư, doanh nghiệp, đất đai, bảo hiểm, tư pháp...*) được kết nối vào Cơ sở dữ liệu tổng hợp Quốc gia, việc xác minh thông tin trong quá trình giải quyết TTHC sẽ nhanh chóng và chính xác hơn. Thay vì yêu cầu người dân, doanh nghiệp nộp nhiều loại giấy tờ, cán bộ có thể tra cứu dữ liệu trực tuyến. Thực tế, Chính phủ đã chỉ đạo thực hiện Đề án 06 về ứng dụng dữ liệu dân cư, định danh điện tử để phục vụ chuyển đổi số quốc gia, mà một nội dung quan trọng là thay thế giấy tờ bằng dữ liệu số. Ví dụ: Khi làm thủ tục đăng ký kết hôn, thay vì nộp bản sao CMND, sổ hộ khẩu, giấy xác nhận độc thân..., người dân chỉ cần cung cấp mã định danh, cán bộ Tư pháp sẽ tra cứu thông tin công dân (*dân cư*), tình trạng hôn nhân (*từ Cơ sở dữ liệu hộ tịch*) trên hệ thống. Việc này cắt giảm giấy tờ, đồng thời loại bỏ khả năng giả mạo.

Theo quy định mới, nếu cơ quan nhà nước đã được chia sẻ dữ liệu chủ (*dữ liệu gốc*) trong Cơ sở dữ liệu Quốc gia hoặc Cơ sở dữ liệu bộ ngành, thì không được yêu cầu người dân, tổ chức cung cấp lại thông tin tương đương bằng giấy tờ. Đây là nguyên tắc “Only Once” mỗi thông tin chỉ khai báo một lần mà Chính phủ đang quyết tâm thực hiện. Kết quả nhẫn tiền là cắt giảm thủ tục, thời gian cho người dân, doanh nghiệp. Theo thống kê của Bộ Công an, việc kết nối Cơ sở dữ liệu dân cư giúp rút ngắn trung bình 20% - 30% thời gian xử lý nhiều dịch vụ công do bỏ qua khâu nhập liệu và kiểm chứng giấy tờ thủ công.Thêm nữa, dịch vụ công trực tuyến mức 4 sẽ thuận tiện hơn vì dữ liệu có thể kiểm tra qua mạng thay vì yêu cầu bản giấy. Một ví dụ điển hình: tích hợp Bảo hiểm y tế vào CCCD. Từ 01/6/2025, Bảo hiểm xã hội Việt Nam ngừng cấp thẻ Bảo hiểm y tế giấy; người dân đi khám chữa



bệnh có thẻ dùng ứng dụng VNNeID hoặc xuất trình CCCD gắn chip (*đã tích hợp thông tin Bảo hiểm y tế*) thay cho thẻ giấy. Nhờ kết nối Cơ sở dữ liệu dân cư và Cơ sở dữ liệu Bảo hiểm y tế, quy trình kiểm tra thẻ Bảo hiểm y tế tại bệnh viện trở nên nhanh gọn (*quét mã QR trên CCCD hoặc tra cứu số định danh*).

Theo ngành Bảo hiểm xã hội, điều này giảm hàng chục triệu lượt in thẻ mỗi năm, tiết kiệm chi phí và thời gian chờ. Một lợi ích khác của ứng dụng dữ liệu là giám sát và đánh giá quá trình giải quyết thủ tục hành chính. Cơ sở dữ liệu tổng hợp Quốc gia lưu vết các giao dịch dữ liệu giữa các cơ quan, do đó có thể theo dõi được hồ sơ đang ở đâu, khâu nào chậm trễ. Kết hợp với hệ thống xử lý hồ sơ điện tử, lãnh đạo có thể phát hiện điểm nghẽn để chấn chỉnh, nâng cao chất lượng phục vụ. Hơn nữa, khi dữ liệu hành chính được tập trung, có thể tiến tới tự động hóa một số quyết định hành chính dựa trên dữ liệu. Ví dụ: phạt nguội giao thông có thể tự động ra quyết định dựa trên dữ liệu camera và Cơ sở dữ liệu phương tiện; hoặc cấp một số giấy phép con có thể duyệt tự động nếu dữ liệu đáp ứng tiêu chí (*nhiều cấp mã số thuế doanh nghiệp ngay lập tức sau khi nhận dữ liệu đăng ký kinh doanh từ Cơ sở dữ liệu Quốc gia về đăng ký Doanh nghiệp*). Tóm lại, khai thác Cơ sở dữ liệu tổng hợp Quốc gia sẽ tạo nên bước chuyển từ nền hành chính “xin-cho” sang nền hành chính phục vụ, minh bạch hơn vì mọi thông tin đều có thể kiểm chứng trên hệ thống chung.



Hình ảnh: Cơ quan Bảo hiểm xã hội ngừng cấp BHYT giấy, triển khai tích hợp trên ứng dụng VssID và VNNeID. Ảnh: Báo Lao động



5.2.5.3. Ứng dụng dữ liệu phục vụ kinh doanh và khởi nghiệp đổi mới sáng tạo

Không chỉ khu vực công, khu vực tư nhân cũng sẽ hưởng lợi lớn từ Cơ sở dữ liệu tổng hợp Quốc gia thông qua việc tiếp cận kho dữ liệu mở và dữ liệu dùng chung. Nền kinh tế hiện đại dựa nhiều vào dữ liệu số như một yếu tố đầu vào cho sản xuất kinh doanh. Khi Chính phủ mở dữ liệu về dân cư, doanh nghiệp, giao thông, khí tượng... các doanh nghiệp có thể tạo ra sản phẩm, dịch vụ mới từ những dữ liệu này. Ví dụ: dữ liệu mở về giao thông đô thị (*cảm biến, camera*) có thể giúp doanh nghiệp phát triển ứng dụng điều hướng giao thông, dịch vụ gọi xe tối ưu; dữ liệu thống kê dân số và thu nhập theo khu vực giúp công ty bán lẻ quyết định vị trí mở cửa hàng; dữ liệu đăng ký doanh nghiệp cho phép các fintech đánh giá tín nhiệm doanh nghiệp một cách nhanh chóng. Thực tế, Luật Dữ liệu và Nghị định 47/2025/NĐ-CP đã tạo cơ sở để dữ liệu từ Cơ sở dữ liệu tổng hợp Quốc gia được cung cấp dưới dạng dữ liệu mở, dữ liệu dùng chung cho mọi tổ chức, cá nhân khai thác hợp pháp. Các startup đổi mới sáng tạo có thể tận dụng nguồn dữ liệu công này để bứt phá. Ví dụ: startup về AI có thể dùng dữ liệu tổng hợp phi danh (*ẩn danh*) từ Cơ sở dữ liệu y tế để huấn luyện mô hình chẩn đoán bệnh; startup về thương mại điện tử có thể kết nối API đến Cơ sở dữ liệu địa chỉ, mã bưu chính quốc gia để chuẩn hóa địa chỉ giao hàng.

Trung tâm dữ liệu quốc gia theo luật còn có nhiệm vụ hỗ trợ tổ chức, cá nhân trong xử lý dữ liệu; xây dựng trung tâm đổi mới sáng tạo về khoa học dữ liệu; phát triển hệ sinh thái khởi nghiệp dữ liệu. Điều này cho thấy Chính phủ định hướng tạo điều kiện tối đa cho doanh nghiệp khai thác dữ liệu. Một minh chứng là Công dữ liệu quốc gia sẽ không chỉ cung cấp dữ liệu miễn phí mà có thể cung cấp dịch vụ dữ liệu (*data services*) cao cấp (ví dụ *API truy cập dữ liệu thời gian thực, dịch vụ phân tích dữ liệu theo yêu cầu có thu phí*). Thông qua đó, các doanh nghiệp, đặc biệt startup nhỏ không phải tự xây dựng hạ tầng dữ liệu từ đầu, mà có thể sử dụng dịch vụ sẵn có để phát triển nhanh sản phẩm của mình. Ngoài ra, Cơ sở dữ liệu tổng hợp Quốc gia còn giúp khu vực tư tiết kiệm chi phí tuân thủ khi giao dịch với chính phủ. Doanh nghiệp khởi nghiệp thường gặp khó vì thủ tục



pháp lý phức tạp; nhưng nếu dữ liệu được chia sẻ, nhiều thủ tục sẽ đơn giản. Ví dụ: trước đây khi xin giấy phép kinh doanh có điều kiện, doanh nghiệp phải nộp nhiều loại giấy xác nhận (*an ninh trật tự, phòng cháy chữa cháy...*); nay các giấy này có thể kiểm tra trên hệ thống dữ liệu liên thông giữa các cơ quan, doanh nghiệp không phải chạy vạy lấy từng giấy.

Thêm nữa, dịch vụ công trực tuyến tốt hơn cũng tạo môi trường kinh doanh thuận lợi, kích thích khởi nghiệp. Cơ sở dữ liệu tổng hợp Quốc gia cũng tạo ra ngành nghề kinh doanh mới "dịch vụ dữ liệu". Các công ty có thể tham gia làm đại lý phân phối dữ liệu mở, tư vấn phân tích dữ liệu cho doanh nghiệp khác, một thị trường mà ở các nước phát triển rất sôi động. Nhà nước cần nhận thức rằng việc chia sẻ dữ liệu không làm mất đi giá trị, ngược lại càng lan tỏa thì dữ liệu càng sinh lợi. Tất nhiên, ranh giới giữa dữ liệu mở và dữ liệu giới hạn cũng phải rõ ràng, dữ liệu nhạy cảm liên quan an ninh, quốc phòng hay bí mật kinh doanh cá nhân sẽ không được tùy tiện cung cấp. Nhưng số còn lại, nếu được dùng đúng mục đích, sẽ trở thành “dầu mỏ” cho nền kinh tế số.



Hình ảnh: Các đơn vị, địa phương sử dụng dữ liệu của CSDL Quốc gia. Nguồn
Báo Chính phủ



5.2.5.4. Ví dụ thực tích hợp dữ liệu dân cư, bảo hiểm, y tế

Để minh họa cụ thể lợi ích của Cơ sở dữ liệu tổng hợp Quốc gia, có thể xem xét trường hợp tích hợp dữ liệu dân cư, bảo hiểm xã hội và y tế - những lĩnh vực liên quan mật thiết tới đời sống dân sinh. Trước đây, mỗi cơ quan vận hành một Cơ sở dữ liệu riêng: Bộ Công an quản lý Cơ sở dữ liệu Quốc gia về dân cư (*CCCD, hộ khẩu...*), Bảo hiểm xã hội Việt Nam quản lý Cơ sở dữ liệu người tham gia Bảo hiểm xã hội, Bảo hiểm y tế, Bộ Y tế có Cơ sở dữ liệu bệnh án điện tử phân tán... Sự rắc rối này gây phiền hà khiến người dân đi khám bệnh phải mang thẻ Bảo hiểm y tế, giấy tờ tùy thân; bệnh viện khó tra cứu lịch sử khám chữa bệnh nếu chuyển tuyến; các thủ tục Bảo hiểm xã hội phải xác minh nhân thân mất thời gian.

Từ năm 2021, Cơ sở dữ liệu Quốc gia về dân cư đi vào hoạt động và Đề án 06 thúc đẩy kết nối liên thông với các ngành. Đến nay, dữ liệu thẻ Bảo hiểm y tế đã được đồng bộ một phần với Cơ sở dữ liệu dân cư: số CCCD gắn chip được bổ sung vào Cơ sở dữ liệu Bảo hiểm y tế và ngược lại mã số Bảo hiểm y tế được liên kết với công dân trong Cơ sở dữ liệu dân cư. Nhờ đó, ứng dụng VNNeID có thể hiển thị thông tin thẻ Bảo hiểm y tế của công dân sau khi họ thực hiện vài bước tích hợp. Khi người dân đi khám bệnh, chỉ cần dùng ứng dụng VNNeID (*hoặc xuất trình CCCD*) là bệnh viện tra được ngay thông tin bảo hiểm hợp lệ. Theo thống kê của Bảo hiểm xã hội, đến giữa 2023, hầu hết cơ sở khám chữa bệnh trên toàn quốc đã chấp nhận sử dụng CCCD thay thẻ Bảo hiểm y tế. Điều này không những tiện lợi cho người dân (*không lo quên hay mất thẻ*), mà còn giúp Bảo hiểm xã hội giảm chi phí in ấn, quản lý thẻ giấy và hạn chế tình trạng mượn thẻ Bảo hiểm y tế đi khám (*do CCCD là duy nhất cho từng người*). Tiến xa hơn, Bộ Y tế đang triển khai hồ sơ sức khỏe điện tử kết nối các bệnh viện. Tương lai, khi hồ sơ sức khỏe (*chứa lịch sử khám chữa bệnh, đơn thuốc*) được liên thông và tích hợp vào Cơ sở dữ liệu tổng hợp Quốc gia, mỗi người dân có thể xem toàn bộ lịch sử y tế của mình qua ứng dụng, bác sĩ ở các tuyến cũng tra cứu được để điều trị tốt hơn. Về Bảo hiểm xã hội, dữ liệu dân cư giúp làm sạch tình trạng trùng số sổ hoặc kê khai sai thông tin.



Một ví dụ khác, tích hợp dữ liệu cho phép dịch vụ công liên thông, khi làm thủ tục đăng ký khai sinh, hệ thống có thể đồng thời cấp mã số Bảo hiểm y tế cho trẻ em (vì đã có sẵn dữ liệu cha mẹ từ dân cư và chính sách Bảo hiểm y tế cho trẻ dưới 6 tuổi) liên thông các thủ tục hành chính (*khai sinh, hộ khẩu, Bảo hiểm y tế*) dựa trên chia sẻ dữ liệu. Như vậy, giá trị cộng hưởng (*synergy*) xuất hiện rõ khi các Cơ sở dữ liệu dân cư, Bảo hiểm xã hội, y tế được tích hợp.



Hình ảnh: Chi nhánh Trung tâm Phục vụ hành chính công số 1 Hà Nội. Nguồn
CTTĐT Hà Nội

Từ góc độ quản lý, Nhà nước có cái nhìn toàn diện hơn, biết được bao nhiêu phần trăm dân số có Bảo hiểm y tế, phân bổ sử dụng dịch vụ y tế ra sao; kiểm soát tốt hơn việc quỹ Bảo hiểm y tế bị lạm dụng... Từ góc độ người dân, các dịch vụ được cá nhân hóa và thuận tiện. Đây chỉ là một ví dụ, tiềm năng tích hợp dữ liệu còn rất lớn trong các lĩnh vực khác như giáo dục (*liên thông dữ liệu học sinh sinh viên với dân cư và an sinh xã hội*), tư pháp (*lý lịch tư pháp liên thông với dữ liệu tòa án, thi hành án*), đô thị (*dữ liệu đất đai, xây dựng kết nối với dân cư để quản lý nhà ở*)... Với nền tảng Cơ sở dữ liệu tổng hợp Quốc gia, việc tích hợp đa ngành sẽ dễ dàng hơn nhiều so với trước, giúp một dữ liệu phục vụ nhiều mục đích, thúc đẩy chính phủ số và xã hội số phát triển.



KẾT LUẬN

Cơ sở dữ liệu tổng hợp quốc gia giữ vai trò như “trái tim” của hạ tầng dữ liệu Việt Nam trong kỷ nguyên số. Cơ sở dữ liệu tổng hợp Quốc gia không đơn thuần là kho lưu trữ thông tin, mà là động lực chiến lược để hiện đại hóa quản trị nhà nước và kích thích sáng tạo kinh doanh. Việc tập trung, liên thông dữ liệu từ các lĩnh vực khác nhau cho phép Chính phủ ra quyết định nhanh hơn, chính xác hơn dựa trên bức tranh toàn diện, đồng thời mở ra không gian phát triển mới cho nền kinh tế số và xã hội số. Có thể nói, Cơ sở dữ liệu tổng hợp Quốc gia là kết cấu hạ tầng mềm quan trọng ngang tầm với hạ tầng cứng (*điện, đường, viễn thông*) trong phát triển quốc gia.

Tuy nhiên, để triển khai thành công Cơ sở dữ liệu tổng hợp Quốc gia, có một số điều kiện tiên quyết cần được đảm bảo. Trước hết là khung thể chế đầy đủ và thực thi nghiêm túc. Luật Dữ liệu 2024 đã tạo nền móng pháp lý, nhưng hiệu quả phụ thuộc vào việc ban hành kịp thời các văn bản hướng dẫn (*nghị định, thông tư*) cũng như sự tuân thủ của các cơ quan. Việc kết nối, chia sẻ dữ liệu cần được coi là nghĩa vụ pháp lý của mỗi cơ quan công quyền, có chế tài rõ ràng nếu không thực hiện hoặc cản trở chia sẻ. Cùng với đó, hạ tầng kỹ thuật phải sẵn sàng, Trung tâm dữ liệu quốc gia cần được đầu tư đúng mức về tài chính, công nghệ để đủ năng lực tiếp nhận và xử lý dữ liệu toàn quốc. Điều kiện không kém phần quan trọng là nhân lực, những người “kỹ sư dữ liệu” vận hành hệ thống phải được đào tạo bài bản, có đạo đức nghề nghiệp và tinh thần phụng sự. Nếu thiếu nhân lực giỏi, dù công nghệ hiện đại cũng khó phát huy. Bên cạnh nội lực, hợp tác quốc tế, học hỏi mô hình từ các nước đi trước, tranh thủ hỗ trợ kỹ thuật và chuyên giao công nghệ (*như tham gia xây dựng tiêu chuẩn dữ liệu quốc tế*) cũng là yếu tố nên tận dụng. Cuối cùng, sự đồng thuận và tham gia của xã hội sẽ quyết định tính bền vững của Cơ sở dữ liệu tổng hợp Quốc gia. Khi người dân, doanh nghiệp nhận thức được lợi ích và tin tưởng vào hệ thống dữ liệu quốc gia, họ sẽ tích cực sử dụng và đóng góp dữ liệu, tạo vòng tuần hoàn giá trị dữ liệu không ngừng.



Nhìn về giai đoạn tới, Việt Nam đã xác định rõ định hướng phát triển dữ liệu đến năm 2030 qua Chiến lược dữ liệu quốc gia. Các mục tiêu cụ thể như kết nối 100% trung tâm dữ liệu, số hóa hoàn toàn các Cơ sở dữ liệu Quốc gia, mọi cơ quan mở dữ liệu, tích hợp 80% dữ liệu thủ tục hành chính là những cột mốc quan trọng. Để đạt được, lộ trình triển khai Cơ sở dữ liệu tổng hợp Quốc gia cần được chia thành các giai đoạn với ưu tiên phù hợp. Giai đoạn 2025-2026 có thể tập trung hoàn thiện nền tảng, ban hành đầy đủ quy định, xây dựng xong Trung tâm dữ liệu quốc gia và tích hợp những Cơ sở dữ liệu Quốc gia thiết yếu (*dân cư, doanh nghiệp, đất đai, tài chính, bảo hiểm...*). Giai đoạn 2027-2028 hướng tới mở rộng kết nối, đưa thêm nhiều Cơ sở dữ liệu bộ ngành, địa phương vào hệ thống; phát triển mạnh Công dữ liệu quốc gia và các dịch vụ dữ liệu cho doanh nghiệp. Giai đoạn 2029-2030 là lúc tối ưu hóa và sáng tạo, khai thác tối đa dữ liệu bằng AI, ra quyết định tự động, hình thành thị trường dữ liệu sôi động. Tầm nhìn xa hơn, Cơ sở dữ liệu tổng hợp Quốc gia sẽ giúp Việt Nam bước vào nền kinh tế dữ liệu, nơi dữ liệu thực sự trở thành tài nguyên mới thúc đẩy tăng trưởng. Để điều đó thành hiện thực, mỗi quyết sách hôm nay cần đặt trọng tâm vào dữ liệu, từ đầu tư hạ tầng, đổi mới giáo dục đến cải cách thủ tục, tất cả phải gắn với việc xây dựng và sử dụng hiệu quả tài sản dữ liệu số quốc gia.

Tóm lại, việc tăng cường ứng dụng Cơ sở dữ liệu tổng hợp Quốc gia không phải là dự án công nghệ thuần túy mà là một chương trình chuyển đổi toàn diện về thể chế, về cách vận hành chính phủ và nền kinh tế. Thành công của chương trình này sẽ góp phần đưa Việt Nam vươn lên trong kỷ nguyên số, xây dựng Chính phủ số minh bạch, hiệu quả và một xã hội số nơi mọi quyết định, sáng kiến đều dựa trên dữ liệu và vì lợi ích của người dân. Chính phủ, doanh nghiệp và người dân với vai trò và trách nhiệm của mình cần tiếp tục chung sức triển khai các giải pháp đã đề ra, biến kho dữ liệu quốc gia thành nguồn lực phát triển cho hiện tại và tương lai. Các mục tiêu đã định cho năm 2030 chỉ còn vài năm phía trước, hành động nhất quán ngay từ bây giờ sẽ quyết định chúng ta có biến dữ liệu thành tài sản và động lực thực sự hay không. Với quyết tâm chính trị cao và sự đồng lòng



của toàn xã hội, tin rằng Cơ sở dữ liệu tổng hợp Quốc gia sẽ phát huy vai trò nền tảng, đưa Việt Nam tiến những bước vững chắc trên con đường chuyển đổi số, phát triển kinh tế - xã hội dựa trên dữ liệu.



PHỤ LỤC

Phản bác quan điểm sai trái "Việt Nam xâm phạm quyền riêng tư"

Trong kỷ nguyên số hiện nay, dữ liệu đã vươn lên trở thành nguồn tài nguyên chiến lược, được ví như “dầu mỏ mới” của nền kinh tế số. Nhận thức rõ tầm quan trọng đặc biệt đó, Đảng và Nhà nước ta đã sớm đề ra chủ trương đẩy mạnh chuyển đổi số quốc gia và xây dựng các hạ tầng dữ liệu cốt lõi. Đại hội XIII của Đảng nhấn mạnh cần “thúc đẩy mạnh mẽ chuyển đổi số quốc gia, phát triển kinh tế số, xã hội số” nhằm tạo bứt phá về năng suất, hiệu quả, sức cạnh tranh của nền kinh tế. Trên tinh thần ấy, việc hình thành Cơ sở dữ liệu tổng hợp quốc gia được xác định là một nhiệm vụ trọng tâm và cấp thiết, đóng vai trò trụ cột cho Chính phủ số, kinh tế số, xã hội số.

Thực tế những năm qua cho thấy, nước ta bước đầu xây dựng được một số cơ sở dữ liệu quốc gia nhưng còn phân tán, cục bộ. Nhiều bộ, ngành thu thập dữ liệu chồng chéo, thiếu mã định danh chung, gây khó khăn cho kết nối, chia sẻ; hạ tầng nhiều nơi chưa đáp ứng yêu cầu, tiềm ẩn lỗ hổng bảo mật. Những hạn chế đó đòi hỏi phải có một giải pháp mang tính đột phá, tổng thể để tích hợp, đồng bộ dữ liệu trên quy mô toàn quốc. Cơ sở dữ liệu quốc gia ra đời chính là để khắc phục các điểm nghẽn đó, xây dựng một kho dữ liệu thống nhất, tin cậy phục vụ quản lý và phát triển.

Tuy nhiên, bên cạnh sự đồng thuận rộng rãi, một số luận điệu thiêng chí từ các thế lực thù địch, truyền thông nước ngoài đã cố tình xuyên tạc chủ trương này. Họ cho rằng Luật Dữ liệu và hệ thống cơ sở dữ liệu quốc gia của Việt Nam “vi phạm quyền riêng tư của công dân, tạo công cụ kiểm soát tập trung, thiếu minh bạch, cản trở phát triển kinh tế, xâm phạm nhân quyền”. Những nhận định sai trái ấy hoàn toàn bỏ qua bối cảnh và mục tiêu tốt đẹp của chính sách dữ liệu ở Việt Nam.



The screenshot shows a news article titled "Nguyễn Xuân Thọ - Miền riêng tư và trách nhiệm của tự do" (Nguyen Xuan Tho - Privacy and responsibility of freedom). The article discusses the right to privacy and its responsibilities. It includes social sharing buttons for Facebook, Twitter, Google+, and others. Below the article, there is a sidebar for "Quốc Dân TV" featuring a video thumbnail for the "Quyết Nghị Đại Hội VNQD Trưởng" (Decision of the National Congress VNQD Leader) and a link to the video.

"baoquocdan" cho rằng Việt Nam xâm phạm quyền riêng tư.Ảnh: Tác giả

Luật Dữ liệu 2024 đã đưa ra định nghĩa và khung pháp lý rõ ràng cho Cơ sở dữ liệu quốc gia. Theo đó, Cơ sở dữ liệu quốc gia là tập hợp dữ liệu được tổng hợp từ các cơ sở dữ liệu quốc gia chuyên ngành và các nguồn khác, do Chính phủ xây dựng và quản lý tập trung, thống nhất tại Trung tâm dữ liệu quốc gia. Cơ sở dữ liệu quốc gia được thiết kế để trở thành kho dữ liệu dùng chung cho toàn bộ hệ thống chính trị và xã hội: phục vụ khai thác, sử dụng trong các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị – xã hội; phục vụ giải quyết thủ tục hành chính, dịch vụ công; hỗ trợ công tác chỉ đạo điều hành, hoạch định chính sách; đồng thời đáp ứng nhu cầu khai thác dữ liệu của mọi tổ chức, cá nhân theo quy định pháp luật. Nói cách khác, Cơ sở dữ liệu quốc gia mang sứ mệnh trở thành “nguồn dữ liệu tin cậy duy nhất” cho cả khu vực công và tư, nhằm xóa bỏ tình trạng cát cứ thông tin, tạo nền tảng cho kết nối thông suốt trên quy mô quốc gia.

Để xây dựng Cơ sở dữ liệu quốc gia, Luật Dữ liệu quy định rõ phạm vi và nguồn dữ liệu được thu thập, cập nhật vào hệ thống này. Cụ thể, Điều 34 Luật Dữ liệu 2024 liệt kê 5 nhóm dữ liệu đưa vào Cơ sở dữ liệu quốc gia, bao gồm: ⁽¹⁾Dữ liệu mở; ⁽²⁾Dữ liệu dùng chung của cơ quan nhà nước; ⁽³⁾Dữ liệu dùng riêng của cơ quan nhà nước do Thủ tướng quyết định (*phục vụ quốc phòng, an ninh, đối ngoại, cơ yếu, phát triển KT-XH, chuyển đổi số, lợi ích quốc gia-công cộng*); ⁽⁴⁾Dữ liệu của cơ quan Đảng, Mặt trận TQ và các tổ chức chính trị-xã hội (khi chủ sở



hữu dữ liệu đồng ý); và ⁽⁵⁾Dữ liệu khác do tổ chức, cá nhân cung cấp. Quy định này cho thấy chỉ những dữ liệu thực sự cần thiết, có giá trị dùng chung mới được đưa vào hệ thống tích hợp tầm quốc gia, tránh việc thu thập tràn lan. Đồng thời, dữ liệu từ các bộ, ngành, địa phương sẽ được “đồng bộ” về Cơ sở dữ liệu quốc gia thay vì tạo ra bộ máy thu thập mới, bảo đảm không thu thập lại những dữ liệu đã có sẵn thông qua kết nối, chia sẻ.

Quan trọng hơn, pháp luật đặc biệt đề cao yếu tố quyền riêng tư và tính hợp pháp trong suốt quá trình thu thập, xử lý dữ liệu. Luật Dữ liệu quán triệt nguyên tắc: việc thu thập dữ liệu cá nhân phải được sự đồng ý của chủ thể dữ liệu, trừ những trường hợp luật định ngoại lệ. Mọi hoạt động xử lý dữ liệu cá nhân đều phải đúng mục đích cụ thể, rõ ràng đã thông báo, bảo đảm tuân thủ pháp luật. Thông tin trước khi nhập vào bất kỳ cơ sở dữ liệu nào cũng phải được kiểm tra mức độ chính xác. Những yêu cầu này thể hiện tinh thần thượng tôn pháp luật và tôn trọng quyền riêng tư ngay từ khâu đầu vào của Cơ sở dữ liệu quốc gia. Trái với luận điệu cho rằng “*hệ thống dữ liệu quốc gia sẽ xâm phạm đời tư công dân*”, chính sách dữ liệu của Việt Nam đã đặt sự đồng ý và lợi ích của người dân làm trọng. Quyền và lợi ích hợp pháp của chủ thể dữ liệu được pháp luật bảo vệ xuyên suốt, từ Luật An ninh mạng 2018 đến Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, và mới đây là Luật Bảo vệ dữ liệu cá nhân 2025 – tất cả đều nhất quán nghiêm cấm hành vi thu thập, sử dụng dữ liệu để xâm phạm quyền riêng tư, nhân phẩm con người. Bất kỳ hành vi lợi dụng dữ liệu để xâm hại an ninh quốc gia hay quyền con người đều bị đặt ngoài vòng pháp luật, với chế tài xử lý nghiêm khắc. Chính khung pháp lý chặt chẽ này đã bác bỏ hoàn toàn cáo buộc vô căn cứ rằng xây dựng Cơ sở dữ liệu quốc gia là vi phạm nhân quyền. Ngược lại, mục tiêu tối thượng là bảo vệ người dân, bảo vệ an ninh và lợi ích quốc gia.

Cơ sở dữ liệu quốc gia sẽ tích hợp, đồng bộ dữ liệu từ các cơ sở dữ liệu quốc gia hiện có (về *dân cư, đất đai, doanh nghiệp, bảo hiểm, giáo dục, y tế,...*) cũng như cơ sở dữ liệu chuyên ngành của các bộ, ngành, địa phương. Dữ liệu sau khi đưa về kho tập trung này sẽ được phân loại thành các dạng: dữ liệu dùng chung



(dùng giữa các cơ quan thuộc khu vực công), dữ liệu mở (công khai cho mọi đối tượng khai thác), dữ liệu dùng riêng (chỉ sử dụng trong nội bộ từng cơ quan), dữ liệu quan trọng, cốt lõi (liên quan quốc phòng, an ninh, lợi ích công)... Việc phân loại và thiết lập cơ chế truy cập tương ứng giúp vừa mở rộng khả năng chia sẻ, vừa đảm bảo an toàn cho những thông tin nhạy cảm. Điều 35 Luật Dữ liệu 2024 quy định rõ các chủ thể được khai thác Cơ sở dữ liệu quốc gia bao gồm: (a) Cơ quan Đảng, Nhà nước và tổ chức chính trị-xã hội được khai thác trong phạm vi chức năng, nhiệm vụ; (b) Chủ thể dữ liệu (công dân) được quyền khai thác dữ liệu về chính mình; và (c) Mọi tổ chức, cá nhân khác – được quyền tự do khai thác dữ liệu mở; được khai thác dữ liệu cá nhân trong Cơ sở dữ liệu quốc gia nếu có sự đồng ý của Trung tâm dữ liệu quốc gia và chính cá nhân đó; và được khai thác các dữ liệu khác khi được Trung tâm dữ liệu quốc gia đồng ý. Quy định này một mặt cho phép doanh nghiệp, người dân tiếp cận kho dữ liệu chung để phục vụ nhu cầu chính đáng, mặt khác vẫn đặt giới hạn bảo vệ dữ liệu cá nhân bằng cơ chế đồng ý hai cấp (*cá nhân + cơ quan quản lý dữ liệu*). Điều này cho thấy tính minh bạch và cởi mở trong chính sách dữ liệu, hầu hết dữ liệu không mật và không riêng tư sẽ dần được mở ra cho toàn xã hội khai thác. Trách nhiệm của Trung tâm dữ liệu quốc gia là như một “nhạc trưởng” điều phối việc kết nối, chia sẻ dữ liệu giữa các hệ thống, đồng thời thẩm định, cho phép các yêu cầu khai thác dữ liệu hợp pháp từ bên ngoài.

Bên cạnh đó, Nhà nước cũng ban hành các quy định chi tiết để bảo đảm sự đồng bộ và an toàn trong kết nối dữ liệu. Ngay sau khi Luật Dữ liệu được Quốc hội thông qua cuối năm 2024, Chính phủ đã ban hành Nghị định 165/2025/NĐ-CP (ngày 30/6/2025) quy định chi tiết thi hành luật này. Đồng thời ban hành Nghị định 47/2024/NĐ-CP về danh mục cơ sở dữ liệu quốc gia và Nghị định 194/2025/NĐ-CP về kết nối, chia sẻ dữ liệu số, qua đó hình thành khung pháp lý thống nhất cho việc xây dựng Cơ sở dữ liệu quốc gia. Trong đó, Nghị định 47/2024/NĐ-CP bắt buộc mọi cơ sở dữ liệu quốc gia đều phải đồng bộ dữ liệu về Cơ sở dữ liệu quốc gia và tuân thủ danh mục dữ liệu dùng chung thống nhất. Còn



Nghị định 194/2025/NĐ-CP (có hiệu lực từ 19/8/2025) quy định chi tiết các phương thức kết nối, chia sẻ và khai thác dữ liệu giữa các hệ thống. Nghị định này yêu cầu dữ liệu từ các cơ sở dữ liệu quốc gia sau khi được đồng bộ về Cơ sở dữ liệu quốc gia sẽ được cung cấp dưới dạng dữ liệu dùng chung, dữ liệu mở để phục vụ mọi cơ quan, tổ chức, cá nhân có nhu cầu khai thác hợp pháp. Quy định này mang ý nghĩa hết sức quan trọng, bảo đảm rằng dữ liệu công thuộc sở hữu nhà nước sẽ được chia sẻ công khai tối đa cho xã hội, tăng tính minh bạch và giá trị sử dụng của dữ liệu. Đây là minh chứng rõ rệt bác bỏ luận điệu xuyên tạc rằng “hệ thống dữ liệu thiếu minh bạch, Nhà nước độc quyền kiểm soát thông tin”. Ngược lại, tính minh bạch được luật hóa bằng việc công khai dữ liệu mở, và cơ chế kiểm soát được thiết lập qua Trung tâm dữ liệu quốc gia để ngăn chặn việc khai thác dữ liệu sai mục đích hoặc trái phép.

Bảo vệ dữ liệu và an ninh hệ thống được đặt lên hàng đầu. Song song với mở rộng chia sẻ, các quy định pháp luật đặt ra yêu cầu rất cao về bảo đảm an ninh, an toàn thông tin cho Cơ sở dữ liệu quốc gia. Luật Dữ liệu 2024 có một chương riêng về bảo vệ dữ liệu và quản trị dữ liệu an toàn, trong đó xác định các nguyên tắc quản lý truy cập, mã hóa, sao lưu dữ liệu quan trọng... Các hành vi xâm phạm, tấn công, phá hoại cơ sở dữ liệu sẽ bị xử lý nghiêm theo luật hình sự. Đặc biệt, Điều 10 Luật Dữ liệu nghiêm cấm hành vi tấn công, chiếm đoạt, làm sai lệch hoặc phá hoại hệ thống cơ sở dữ liệu, cấm cố ý cung cấp dữ liệu sai hoặc không cung cấp dữ liệu khi có nghĩa vụ, cũng như cấm lợi dụng hoạt động dữ liệu để xâm phạm lợi ích Nhà nước, quyền hợp pháp của tổ chức, cá nhân. Như vậy, từ khía cạnh pháp lý, có thể thấy Cơ sở dữ liệu quốc gia được xây dựng trên một nền tảng pháp luật rất vững chắc và tiến bộ: vừa tạo thuận lợi tối đa cho khai thác dữ liệu phục vụ phát triển, vừa đặt ra hành lang an toàn để bảo vệ dữ liệu, bảo vệ quyền riêng tư và lợi ích của toàn xã hội. Chính sự cân bằng này thể hiện tính khoa học trong cách tiếp cận của Việt Nam: cân bằng giữa phát huy giá trị dữ liệu với bảo đảm an ninh, quyền con người. Điều này hoàn toàn bác bỏ những luận điệu sai trái trước đó – thay vì “mất quyền riêng tư” hay “thiếu minh bạch”, Cơ sở dữ liệu



quốc gia sẽ vận hành công khai, minh bạch dưới sự quản lý bằng pháp luật, mọi hành vi lạm dụng đều bị trừng trị, qua đó củng cố niềm tin số cho người dân và doanh nghiệp.

Từ những phân tích trên, có thể khẳng định việc xây dựng và đưa vào vận hành Cơ sở dữ liệu tổng hợp quốc gia là một chủ trương chiến lược đúng đắn của Đảng và Nhà nước ta, đáp ứng đòi hỏi cấp bách của sự nghiệp chuyển đổi số và phát triển đất nước trong tình hình mới. Cơ sở dữ liệu quốc gia được hoạch định trên cơ sở pháp lý vững chắc, phù hợp với xu thế quốc tế và điều kiện thực tiễn Việt Nam, vừa tạo nền móng cho Chính phủ số, kinh tế số, xã hội số, vừa bảo đảm an ninh quốc gia, an toàn thông tin và quyền riêng tư của người dân. Những hiệu quả thực tiễn bước đầu, từ việc đơn giản hóa thủ tục hành chính, tiết kiệm chi phí xã hội đến việc hình thành thị trường dữ liệu sôi động, đã cho thấy tính ưu việt và nhân văn của hệ thống này. Chính sách dữ liệu quốc gia của Việt Nam không nhằm kiểm soát người dân, mà nhằm phục vụ người dân tốt hơn “lấy người dân, doanh nghiệp làm trung tâm” của chuyển đổi số. Mọi luận điệu xuyên tạc về “vi phạm quyền riêng tư” hay “xâm hại nhân quyền” đều đã bị thực tế và hệ thống pháp luật phản bác: quyền riêng tư được bảo vệ nghiêm ngặt bởi Luật Bảo vệ dữ liệu cá nhân; quyền tiếp cận thông tin, giám sát của người dân được bảo đảm qua dữ liệu mở và tính minh bạch của hệ thống và nhân quyền nói chung được đề cao khi Nhà nước sử dụng dữ liệu để bảo vệ an sinh xã hội, quyền lợi chính đáng của mọi người dân.

Có thể nói, Cơ sở dữ liệu quốc gia là minh chứng sinh động cho tầm nhìn “dữ liệu là tài sản, là động lực phát triển” của Đảng ta. Dưới sự lãnh đạo đúng đắn của Đảng, sự quản lý hiệu quả của Nhà nước cùng sự đồng thuận của nhân dân, công cuộc chuyển đổi số với trọng tâm là xây dựng các cơ sở dữ liệu quốc gia sẽ thu được những thành tựu to lớn. Cơ sở dữ liệu quốc gia không chỉ là một hệ thống công nghệ thông tin, mà còn là biểu tượng của một phương thức quản trị mới, khoa học, công khai và vì dân. Qua đó, góp phần xây dựng Nhà nước pháp quyền XHCN Việt Nam ngày càng hiện đại, minh bạch, gần dân; đồng thời tạo nền tảng



vững chắc để kinh tế - xã hội Việt Nam phát triển nhanh và bền vững trong kỷ nguyên số. Chủ trương phát triển dữ liệu và chuyển đổi số của Đảng, Nhà nước ta là hoàn toàn hợp pháp, hợp lý, xuất phát từ lợi ích của quốc gia, dân tộc và phù hợp với xu thế thời đại. Những kết quả tích cực của Cơ sở dữ liệu quốc gia sẽ là câu trả lời thuyết phục nhất, bác bỏ mọi luận điệu sai trái và củng cố niềm tin của toàn xã hội vào con đường phát triển mà Đảng, Nhà nước ta đã lựa chọn, con đường “đưa Việt Nam vươn mình trong kỷ nguyên mới” bằng sức mạnh của tri thức, công nghệ và đoàn kết dân tộc



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*) Nghị định 194/2025/NĐ-CP ngày 18/7/2025 về kết nối, chia sẻ dữ liệu, dữ liệu mở
5. Nghị định 47/2024/NĐ-CP ngày 09/5/2024 về danh mục Cơ sở dữ liệu Quốc gia; xây dựng, cập nhật, duy trì, khai thác, sử dụng Cơ sở dữ liệu Quốc gia
6. Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân
7. Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết thi hành Luật Dữ liệu.
8. Quyết định số 142/QĐ-TTg phê duyệt Chiến lược Dữ liệu quốc gia đến năm 2030
9. Đại Kim, Đẩy nhanh cơ chế Sandbox ở Việt Nam, Báo Nhân dân, 2025
10. Nguyễn Minh Nhật, "Nền kinh tế dữ liệu: Mở ra tương lai của việc tạo ra giá trị dựa trên thông tin", Tạp chí TT&TT, 2024