



BỘ CÔNG AN  
TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN

**BÀI DỰ THI**  
*Tìm hiểu*  
**LUẬT DỮ LIỆU**  
**TRONG CÔNG AN NHÂN DÂN**

NHÓM TÁC GIẢ DỰ THI:  
Chiến sĩ An ninh dữ liệu số - T04

Quyển 3

AN NINH, AN TOÀN DỮ LIỆU TRONG KỶ NGUYÊN SỐ

TP. HỒ CHÍ MINH - NĂM 2025

# CHIẾN SĨ AN NINH DỮ LIỆU SỐ



## PHẠM VĂN TỰ

Năm sinh: 29/05/1980

Giới tính: Nam

Dân tộc: Kinh

Cấp bậc: Thượng tá

Chức vụ: Giảng viên chính

Đơn vị: Khoa Ngoại ngữ - Tin học – Trường Đại học An ninh nhân dân

Số điện thoại: 0938.950.948



## MAI HOÀNG NHU

Năm sinh: 10/09/2003

Giới tính: Nam

Dân tộc: Kinh

Cấp bậc: Học viên

Đơn vị: Trung đội D30B1 – Trường Đại học An ninh nhân dân

Số điện thoại: 0814.768.391



## TỐNG GIA KHÁNH

Năm sinh: 16/12/2003

Giới tính: Nam

Dân tộc: Kinh

Cấp bậc: Học viên

Đơn vị: Trung đội D30B2 – Trường Đại học An ninh nhân dân

Số điện thoại: 0904.369.038



## NGUYỄN XUÂN VƯỢNG

Năm sinh: 25/11/2003

Giới tính: Nam

Dân tộc: Kinh

Cấp bậc: Học viên

Đơn vị: Trung đội D30B2 – Trường Đại học An ninh nhân dân

Số điện thoại: 0374.009.946



## ĐẶNG HOÀNG KHẢI

Năm sinh: 21/08/2003

Giới tính: Nam

Dân tộc: Kinh

Cấp bậc: Học viên

Đơn vị: Trung đội D30C2 – Trường Đại học An ninh nhân dân

Số điện thoại: 0346.940.451





## *Mục lục*

|                                                                                                                                                                                                                                             |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>LỜI MỞ ĐẦU</b>                                                                                                                                                                                                                           | <b>05</b>  |
| <b>TÓM TẮT NỘI DUNG</b>                                                                                                                                                                                                                     | <b>07</b>  |
| <b>Câu 7. Quy định về sản phẩm, dịch vụ về dữ liệu? Các giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu?</b>                                                                             | <b>12</b>  |
| <b>7.1. QUY ĐỊNH VỀ SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU</b>                                                                                                                                                                                        | <b>13</b>  |
| 7.1.1. Vì sao phải quy định về sản phẩm, dịch vụ về dữ liệu?                                                                                                                                                                                | 13         |
| 7.1.2. Sản phẩm, dịch vụ về dữ liệu là gì?                                                                                                                                                                                                  | 22         |
| 7.1.3. Quy định của pháp luật Việt Nam về sản phẩm, dịch vụ về dữ liệu                                                                                                                                                                      | 45         |
| 7.1.4. Một số điểm đáng chú ý trong các quy định của pháp luật Việt Nam về sản phẩm, dịch vụ về dữ liệu                                                                                                                                     | 63         |
| <b>7.2. ĐỀ XUẤT MỘT SỐ GIẢI PHÁP BẢO ĐẢM AN NINH DỮ LIỆU, AN TOÀN DỮ LIỆU TRONG ỨNG DỤNG CÁC SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU</b>                                                                                                               | <b>157</b> |
| 7.2.1. Nguy cơ khi ứng dụng sản phẩm, dịch vụ và dữ liệu gây mất an toàn, trật tự xã hội                                                                                                                                                    | 160        |
| 7.2.2. Một số giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu                                                                                                                            | 180        |
| <b>Câu 8. Nội dung quản lý nhà nước về dữ liệu? Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu? Nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030?</b> | <b>224</b> |



# **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

|                                                                                                                                            |            |
|--------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>8.1. NỘI DUNG QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU</b>                                                                                           | <b>227</b> |
| 8.1.1. Nội dung quản lý nhà nước về dữ liệu                                                                                                | 227        |
| 8.1.2. Ý nghĩa của việc quy định nội dung quản lý nhà nước về dữ liệu                                                                      | 245        |
| 8.1.3. Chủ thể, đầu mối quản lý dữ liệu                                                                                                    | 253        |
| <b>8.2. VAI TRÒ, TRÁCH NHIỆM CỦA BỘ CÔNG AN VÀ CÔNG AN CÁC ĐƠN VỊ, ĐỊA PHƯƠNG TRONG CÔNG TÁC QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU</b>               | <b>256</b> |
| 8.2.1. Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu                    | 256        |
| 8.2.2. Vai trò, trách nhiệm của Trung tâm dữ liệu quốc gia trong quản lý nhà nước về dữ liệu                                               | 283        |
| <b>8.3. NHIỆM VỤ TRỌNG TÂM CẦN TẬP TRUNG TRONG GIAI ĐOẠN TỪ NAY ĐẾN NĂM 2030 ĐỂ NÂNG CAO HIỆU QUẢ CÔNG TÁC QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU</b> | <b>289</b> |
| 8.3.1. Bối cảnh và sự cần thiết nâng cao hiệu quả quản lý nhà nước về dữ liệu đến năm 2030                                                 | 289        |
| 8.3.2. Định hướng chiến lược phát triển dữ liệu đến năm 2030                                                                               | 300        |
| 8.3.3. Các nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030 để nâng cao hiệu quả công tác quản lý nhà nước về dữ liệu  | 309        |
| 8.3.4. Đề xuất lộ trình triển khai trong giai đoạn 2025 - 2030 nhằm nâng cao hiệu quả quản lý nhà nước về dữ liệu                          | 342        |
| <b>DANH MỤC TÀI LIỆU THAM KHẢO</b>                                                                                                         | <b>359</b> |





## *Lời mở đầu*

***“Đảm bảo an ninh, an toàn dữ liệu là một nhiệm vụ trọng yếu của công tác bảo vệ an ninh quốc gia trong kỷ nguyên mới”.***

Dữ liệu, trong kỷ nguyên số, không chỉ là thông tin mà đã trở thành một tài nguyên chiến lược của quốc gia. Vai trò của dữ liệu được nhìn nhận sẽ góp phần chuyển đổi cơ cấu nền kinh tế Việt Nam, giúp đất nước phát triển mạnh mẽ và vững vàng trong kỷ nguyên mới. Sự gia tăng không ngừng của dữ liệu đòi hỏi một hành lang pháp lý chặt chẽ để quản lý, khai thác và bảo vệ, đặc biệt là các dữ liệu cốt lõi, dữ liệu quan trọng. Nhận thức rõ tầm quan trọng này, Quốc hội Việt Nam đã ban hành Luật Dữ liệu năm 2024 (Luật số 60/2024/QH15 - chính thức có hiệu lực từ ngày 01/07/2025), được kỳ vọng trở thành trụ cột pháp lý quan trọng để quản lý, chia sẻ và khai thác dữ liệu, là yếu tố then chốt trong chiến lược chuyển đổi số quốc gia. Đây là bước ngoặt quan trọng trong quá trình xây dựng thể chế phát triển kinh tế số, xã hội số và Chính phủ số; đồng thời khẳng định quyết tâm của Việt Nam trong bảo vệ chủ quyền dữ liệu và thúc đẩy đổi mới sáng tạo.

Đối với lực lượng Công an nhân dân, lực lượng nòng cốt trong sự nghiệp bảo vệ an ninh quốc gia, giữ gìn trật tự, an toàn xã hội, việc nghiên cứu, tìm hiểu và nắm vững Luật Dữ liệu là nhiệm vụ đặc biệt quan trọng. Luật Dữ liệu không chỉ không chỉ là công cụ pháp lý điều chỉnh toàn diện công tác quản lý nhà nước về dữ liệu, mà còn xác định rõ vị trí, vai trò, trách nhiệm và quyền hạn của Bộ Công an cùng Công an các đơn vị, địa phương trong tổ chức thực hiện, bảo đảm dữ liệu quốc gia luôn *“đúng - đủ - sạch - sống - thống nhất - dùng chung”*. Qua đó, phục vụ đắc lực cho công tác đấu tranh phòng, chống tội phạm và bảo vệ Tổ quốc trong tình hình mới.





# **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

**Quyển 3: An ninh, an toàn dữ liệu trong kỷ nguyên số** đã phân tích, làm rõ nội dung của 02 câu hỏi sau đây:

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

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

Bài dự thi được xây dựng trên cơ sở nghiên cứu các nội dung của Luật Dữ liệu năm 2024, Thể lệ Cuộc thi và các văn bản quy phạm pháp luật khác có liên quan. Với tinh thần nghiêm túc và trách nhiệm cao, chúng tôi hy vọng bài dự thi sẽ mang lại những đóng góp tích cực cho công tác triển khai thi hành Luật Dữ liệu trong toàn xã hội, đáp ứng yêu cầu của thực tiễn và mục tiêu xây dựng một quốc gia giàu mạnh, hùng cường trong kỷ nguyên số.

Nhóm tác giả trân trọng nhận được sự góp ý của Quý Ban giám khảo và Quý bạn đọc./.

Chào thân ái và quyết thắng!

**Nhóm “Chiến sĩ An ninh dữ liệu số”  
Trường Đại học An ninh nhân dân**





## *Tóm tắt nội dung*

### **QUYỀN 3: AN NINH, AN TOÀN DỮ LIỆU TRONG KỶ NGUYÊN SỐ**

*- Chiến sĩ An ninh dữ liệu số -*

Nhằm giúp Quý Ban Giám khảo và Quý độc giả có góc nhìn trực quan, sinh động và toàn diện khi nghiên cứu *Quyền 3: An ninh, an toàn dữ liệu trong kỷ nguyên số*, nhóm tác giả đã xây dựng bản tóm tắt nội dung hai câu hỏi 07 và 08 như sau:

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

Đến với câu hỏi số 07 trong Bài dự thi “Tìm hiểu Luật Dữ liệu trong Công an nhân dân”, nhóm tác giả đã tập trung làm rõ 02 nội dung chính bao gồm: **(1)** Quy định về sản phẩm, dịch vụ về dữ liệu; **(2)** Đề xuất một số giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu.

**- Phần thứ nhất**, mục “7.1. Quy định về sản phẩm, dịch vụ về dữ liệu”. Qua nghiên cứu, nhóm tác giả đã chia bố cục thành 4 tiết từ 7.1.1 đến 7.1.4, nhằm giúp độc giả hiểu rõ sản phẩm, dịch vụ về dữ liệu là gì; lý do vì sao Việt Nam lại phải quy định về vấn đề này; vấn đề này được pháp luật nước ta quy định như thế nào và có những điểm gì cần chú ý trong các quy định ấy, đặc biệt là Luật Dữ liệu năm 2024 và 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.





# **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

- **Phần thứ hai**, mục “7.2. Đề xuất một số giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu”. Mặc dù đã xuất hiện từ lâu nhưng đây là lần đầu tiên các sản phẩm, dịch vụ về dữ liệu được đưa vào luật một cách cụ thể, chi tiết, cho thấy đây có thể được xem là vấn đề mới đối với nước ta. Tuy nhiên, nhóm tác giả đã nghiên cứu, tổng hợp, phân tích từ thực tiễn các nước trên khắp thế giới, nhận diện **05 nhóm nguy cơ chính** khi ứng dụng sản phẩm, dịch vụ về dữ liệu và từ đó mạnh dạn đề xuất **07 nhóm giải pháp chính** góp phần bảo đảm an ninh, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu ở Việt Nam trong thời gian tới.

Trong đó, **05 nhóm nguy cơ chính** bao gồm:

- (1) *Nguy cơ xâm phạm dữ liệu nhạy cảm và quyền riêng tư của cá nhân từ các sản phẩm, dịch vụ về dữ liệu;*
- (2) *Nguy cơ lợi dụng các sản phẩm, dịch vụ về dữ liệu để thao túng dư luận và lan truyền nội dung sai sự thật;*
- (3) *Nguy cơ tấn công mạng gây gián đoạn hạ tầng số và hệ thống dịch vụ công quốc gia;*
- (4) *Nguy cơ thao túng và giả mạo thông tin từ trí tuệ nhân tạo và công nghệ deepfake;*
- (5) *Nguy cơ lợi dụng sản phẩm, dịch vụ về dữ liệu để thực hiện hành vi vi phạm pháp luật.*

Trên cơ sở đó, nhóm tác giả đề xuất **07 nhóm giải pháp chính** như sau:

- (1) *Hoàn thiện khung pháp lý và quy chuẩn cho an ninh, an toàn dữ liệu;*
- (2) *Tăng cường các biện pháp kỹ thuật - bảo mật dữ liệu;*





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

- (3) Thiết lập tổ chức bảo mật chuyên trách và nâng cao năng lực nhân sự;*
- (4) Bảo vệ quyền lợi của người dùng dữ liệu - đặt con người làm trung tâm trong bảo đảm an ninh, an toàn dữ liệu;*
- (5) Xác định chính xác và xây dựng phương án bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng;*
- (6) Tăng cường giám sát, kiểm tra và xử lý vi phạm;*
- (7) Nâng cao năng lực quốc gia về an ninh, an toàn dữ liệu.*

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

Câu hỏi số 08 là một câu hỏi rất hay khi đề cập đến nội dung của một trong ba chức năng chính của lực lượng Công an nhân dân, đó là *thực hiện quản lý nhà nước về dữ liệu*; đã làm nổi bật tổng thể Bài dự thi “Tìm hiểu Luật Dữ liệu trong Công an nhân dân”. Nghiên cứu nội dung này, nhóm tác giả không chỉ bổ sung kiến thức chuyên môn cần thiết cho công tác sau này, mà còn nắm vững, hiểu sâu về những nội dung liên quan đến dữ liệu - một nguồn tài nguyên chiến lược của quốc gia. Qua đó, nâng cao nhận thức về vai trò, trách nhiệm của bản thân và có định hướng tốt hơn phục vụ triển khai hiệu quả các Chiến lược dữ liệu quốc gia, Chiến lược Chuyển đổi số quốc gia,... góp phần đưa Việt Nam vươn mình trong kỷ nguyên số.

Nhóm tác giả đã bố cục câu hỏi số 08 thành 03 phần, bao gồm: **(1)** Nội dung quản lý nhà nước về dữ liệu; **(2)** Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ





# **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

liệu; (3) Nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030 để nâng cao hiệu quả công tác quản lý nhà nước về dữ liệu.

- **Phần thứ nhất**, mục “8.1. Nội dung quản lý nhà nước về dữ liệu”, đã phân tích **06 nhóm nội dung chính** được Luật Dữ liệu 2024 quy định tại Điều 8, cụ thể:

(1) Xây dựng, ban hành và tổ chức thực hiện Chiến lược dữ liệu quốc gia; văn bản pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật, định mức kinh tế - kỹ thuật, chất lượng dữ liệu;

(2) Tuyên truyền, phổ biến chính sách, pháp luật về dữ liệu; hướng dẫn cơ quan quản lý cơ sở dữ liệu, hệ thống thông tin trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu;

(3) Quản lý, giám sát các hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu, bảo đảm an ninh, an toàn dữ liệu;

(4) Báo cáo, thống kê về dữ liệu; nghiên cứu, ứng dụng khoa học công nghệ về dữ liệu; sản phẩm, dịch vụ về dữ liệu; quản lý, giám sát, phát triển thị trường dữ liệu;

(5) Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về dữ liệu;

(6) Đào tạo, bồi dưỡng, phát triển nguồn nhân lực và hợp tác quốc tế về dữ liệu.

Từ phân tích những nội dung trên, nhóm tác giả rút ra ý nghĩa; đồng thời, trình bày khái quát về chủ thể, đầu mối quản lý nhà nước về dữ liệu.

- **Phần thứ hai**, mục “8.2. Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu”. Qua nghiên cứu nội dung câu hỏi số 06 trong khuôn khổ Bài dự thi





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

“Tìm hiểu Luật Dữ liệu trong Công an nhân dân”, nhận thấy được tầm quan trọng đặc biệt của Trung tâm dữ liệu quốc gia trong công tác quản lý nhà nước về dữ liệu nói riêng, các hoạt động có liên quan đến dữ liệu ở Việt Nam nói chung. Do đó, sẽ là một thiếu sót lớn nếu như không phân tích vai trò, trách nhiệm của chủ thể này, khi nghiên cứu về vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu. Nội dung này được quy định cụ thể, chi tiết tại Điều 21 và Điều 26 của Nghị định số 165/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu.

- **Phần thứ ba**, mục “8.3. Nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030 để nâng cao hiệu quả công tác quản lý nhà nước về dữ liệu”, đã làm rõ **04 vấn đề chính** mà nhóm tác giả cho rằng là thực sự cần thiết để đạt được mục tiêu, yêu cầu của cuộc thi, bao gồm:

- (1) *Bối cảnh và sự cần thiết nâng cao hiệu quả quản lý nhà nước về dữ liệu đến năm 2030;*
- (2) *Định hướng chiến lược phát triển dữ liệu đến năm 2030;*
- (3) *Các nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030 để nâng cao hiệu quả công tác quản lý nhà nước về dữ liệu;*
- (4) *Đề xuất lộ trình triển khai trong giai đoạn 2025 - 2030 nhằm nâng cao hiệu quả quản lý nhà nước về dữ liệu.*

Trên đây là tóm tắt nội dung của **Quyển 3: An ninh, an toàn dữ liệu trong kỷ nguyên số** trong khuôn khổ Bài dự thi “Tìm hiểu Luật Dữ liệu trong Công an nhân dân”. Kính mời Quý Ban Giám khảo và Quý độc giả cùng chuyển sang phần tiếp theo để đi sâu vào các nội dung chi tiết. Trân trọng./.



## *Câu 7*

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





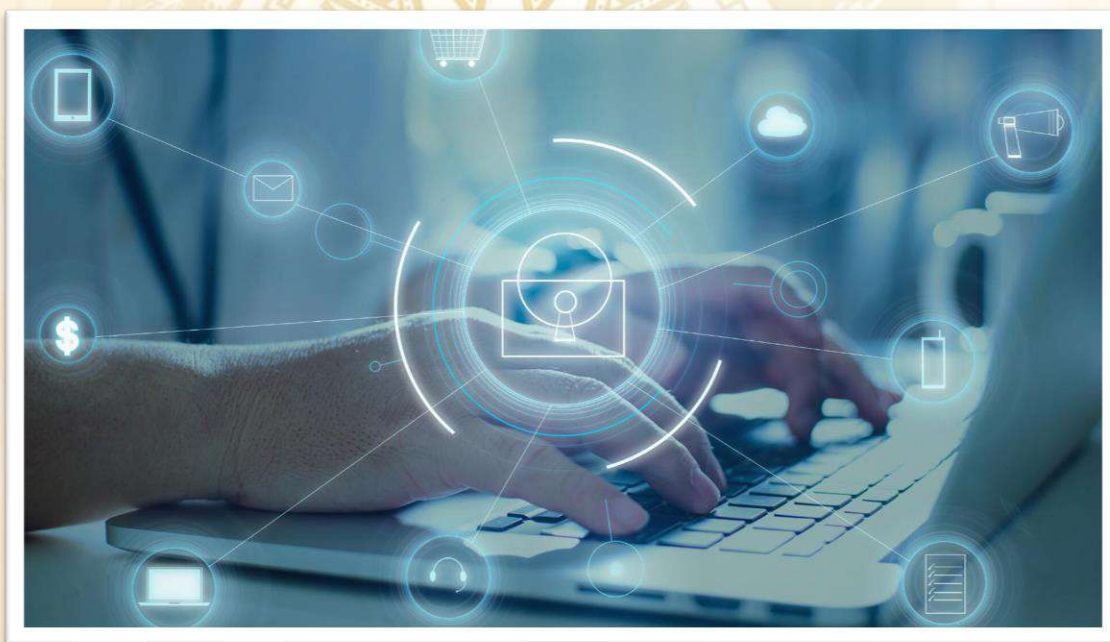


# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

## 7.1. QUY ĐỊNH VỀ SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU

### 7.1.1. Vì sao phải quy định về sản phẩm, dịch vụ về dữ liệu?

**T**rong thế kỷ XXI, khi thế giới chuyển dịch từ nền kinh tế công nghiệp sang nền kinh tế tri thức và kỹ thuật số, dữ liệu nổi lên như một nguồn lực quan trọng, được ví như **“dầu mỏ mới”**. Dữ liệu không chỉ phản ánh hoạt động của xã hội, kinh tế và con người, mà còn là yếu tố đầu vào cho các mô hình trí tuệ nhân tạo, phân tích hành vi người tiêu dùng, dự báo chính sách và phát triển đổi mới sáng tạo. Từ Amazon đến Google, từ các hệ thống chăm sóc y tế đến giao thông thông minh, dữ liệu không chỉ ghi lại quá khứ mà còn tiên đoán tương lai. Đây là bản chất khiến dữ liệu không còn dừng ở **“thông tin”**, mà đã trở thành **“tài sản”**.



***Dữ liệu là tài sản chiến lược của quốc gia - Ảnh: VNEconomy***

Theo Tổ chức Hợp tác và Phát triển Kinh tế (OECD), dữ liệu đáp ứng ba đặc điểm cốt lõi để được coi là một loại tài sản trong nền kinh tế số, bao





gồm: **(1)** có thể sở hữu, **(2)** có thể giao dịch, và **(3)** có thể định giá<sup>1</sup>. Đây là ba điều kiện kinh điển trong học thuyết về tài sản trong luật dân sự và kinh tế học. Trên thực tế, hàng nghìn doanh nghiệp khởi nghiệp trên toàn cầu đã và đang tận dụng dữ liệu như một dạng “nguyên liệu thô”, nó tương tự như nguyên vật liệu đầu vào trong sản xuất công nghiệp để phát triển ra các sản phẩm và dịch vụ có giá trị. Có thể kể đến như Google Maps - một hệ thống bản đồ số toàn cầu dựa trên dữ liệu định vị; Apple Health - nền tảng hồ sơ sức khỏe cá nhân sử dụng dữ liệu sinh trắc học; hay Ant Financial - công ty công nghệ tài chính Trung Quốc nổi tiếng với mô hình chấm điểm tín dụng xã hội dựa trên hành vi trực tuyến của người dùng...

Và Việt Nam cũng không đứng ngoài xu thế và sớm xác định rằng “*Dữ liệu là tài nguyên quốc gia, là nguồn lực, động lực phát triển trong kỷ nguyên số*”<sup>2</sup>. Tại Quyết định số 142/QĐ-TTg ngày 2/2/2024 phê duyệt Chiến lược dữ liệu quốc gia đến năm 2030 đã đề ra quan điểm chỉ đạo: “*Dữ liệu là nguồn tài nguyên mới, là yếu tố then chốt cho chuyển đổi số quốc gia, tạo ra giá trị mới thúc đẩy phát triển kinh tế - xã hội, nâng cao năng lực cạnh tranh quốc gia và phục vụ lợi ích người dân*”. Vai trò trung tâm và quan trọng của dữ liệu càng được thể hiện rõ nét trong Luật Dữ liệu năm 2024, qua định nghĩa tại Điều 6, khoản 1: “*Dữ liệu là tài nguyên, Nhà nước có chính sách huy động mọi nguồn lực để làm giàu dữ liệu, phát triển dữ liệu trở thành tài sản*”. Tuy nhiên, dữ liệu thô (raw data) chỉ thực sự trở nên có giá trị khi được xử lý, phân tích, khai thác, và đặc biệt là khi nó có thể chuyển

<sup>1</sup> OECD (2019), *Data in the Digital Age*, OECD Going Digital Policy Note, <https://www.oecd.org/going-digital/data-in-the-digital-age.pdf>, truy cập ngày 29/7/2025.

<sup>2</sup> Hà Văn (2023), *Thủ tướng: Dữ liệu là tài nguyên quốc gia, là nguồn lực, động lực phát triển trong kỷ nguyên số*, Báo Điện tử Chính phủ, <https://baochinhphu.vn/thu-tuong-du-lieu-la-tai-nguyen-quoc-gia-la-nguon-luc-dong-luc-phat-trien-trong-ky-nguyen-so-1022302251236115.htm>, truy cập ngày 31/7/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

hóa thành sản phẩm hoặc dịch vụ cụ thể phục vụ các hoạt động kinh tế - xã hội. Chính nhu cầu này dẫn tới sự hình thành của các mô hình sản phẩm, dịch vụ về dữ liệu như: trung gian dữ liệu (LiveRamp, Dawex...), dịch vụ phân tích dữ liệu (Palantir Technologies, Tableau...), nền tảng chia sẻ dữ liệu (GAIA-X, Smart Dubai Data Exchange...), hay sàn dữ liệu (AWS Data Exchange, Ocean Protocol...).



***Thủ tướng Phạm Minh Chính phát biểu kết luận Hội nghị trực tuyến toàn quốc và phiên họp lần thứ 5 của Ủy ban Quốc gia và Tổ công tác triển khai Đề án 06 của Chính phủ - Ảnh: Nhật Bắc***

Trên thế giới, nhiều quốc gia và khu vực đã phát triển các khung pháp lý toàn diện để điều chỉnh dữ liệu như một loại hàng hóa “đặc biệt”. Tại Liên minh châu Âu (EU), ngoài Quy định Bảo vệ Dữ liệu Chung (General Data Protection Regulation) điều chỉnh quyền riêng tư, EU còn ban hành Đạo luật Quản trị dữ liệu (Data Governance Act - 2022) và Đạo luật dữ liệu





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

(Data Act - 2023) nhằm thúc đẩy tính minh bạch và khả năng tái sử dụng dữ liệu nhằm phục vụ chia sẻ dữ liệu công - tư, có thể hiểu đơn giản như cơ quan nhà nước chia sẻ dữ liệu giao thông cho doanh nghiệp vận tải số. Trong chiến lược dữ liệu châu Âu (European Data Strategy) và đặc biệt là trong Đạo luật Quản trị dữ liệu, Ủy ban châu Âu (European Commission) đã chính thức công nhận các dịch vụ chia sẻ dữ liệu (data-sharing services) là một loại hình dịch vụ đặc thù, đóng vai trò trung gian trong hệ sinh thái dữ liệu và phải đăng ký, kiểm soát theo quy định pháp lý cụ thể. Theo Điều 10 và Điều 11 của Đạo luật Quản trị dữ liệu, các tổ chức cung cấp dịch vụ chia sẻ dữ liệu, bao gồm nền tảng cho phép các tổ chức chia sẻ dữ liệu công/tư hoặc dữ liệu do cá nhân tạo ra, phải đăng ký với cơ quan có thẩm quyền quốc gia, chịu điều kiện về minh bạch, bảo mật, độc lập và tuân thủ các nguyên tắc xử lý dữ liệu của EU như không trích xuất lợi ích từ nội dung dữ liệu mà chỉ đóng vai trò hạ tầng kết nối<sup>3</sup>.



***Quy định bảo vệ dữ liệu chung (GDPR) của EU - Ảnh: Youth & Partners***

<sup>3</sup> EUR-Lex (n.d.), *Regulation - 2022/868 - EN - EUR-Lex*, EUR-Lex.europa.eu, <https://eur-lex.europa.eu/eli/reg/2022/868/oj>, truy cập ngày 31/7/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Bên cạnh đó, *Trung Quốc* là một trong những quốc gia sớm xác lập dữ liệu như tài sản có thể giao dịch, đồng thời cũng là quốc gia xây dựng hệ thống pháp lý điều tiết rất chặt chẽ như: Luật An ninh Dữ liệu (Data Security Law, 2021), Luật Bảo vệ Thông tin Cá nhân (Personal Information Protection Law, 2021)... Tại Trung Quốc, dữ liệu được xem là “*tư liệu sản xuất mới*” của nền kinh tế số, bên cạnh đất đai, lao động, vốn và công nghệ. Trung Quốc thậm chí xây dựng cơ chế định giá dữ liệu và đẩy mạnh hoàn thiện, phát triển thị trường cho dữ liệu. Nói cách khác, dữ liệu không còn là “thông tin” phục vụ quản lý, mà là đầu vào sản xuất mang tính cấu trúc, có khả năng định giá, sở hữu, giao dịch và sinh lợi<sup>4</sup>.

Trong khi đó, Hoa Kỳ lại tiếp cận theo hướng thị trường hóa linh hoạt hơn, cho phép các nền tảng dữ liệu hoạt động tự do và chỉ can thiệp khi có rủi ro về quyền riêng tư hoặc cạnh tranh không lành mạnh. Cho đến nay, Hoa Kỳ vẫn chưa ban hành một đạo luật toàn quốc mang tính bao quát và hệ thống về bảo vệ dữ liệu cá nhân và dữ liệu phi cá nhân, tương đương với Quy định Bảo vệ Dữ liệu Chung của EU hay Luật An ninh Dữ liệu của Trung Quốc. Thay vào đó, hệ thống pháp luật về dữ liệu tại Hoa Kỳ mang tính phân mảnh, được quy định theo hai hướng: **Thứ nhất**, quy định theo từng bang, tiêu biểu là Đạo luật Quyền riêng tư của người tiêu dùng California (California Consumer Privacy Act - CCPA). **Thứ hai**, quy định theo ngành nghề, ví dụ như Health Insurance Portability and Accountability Act (HIPAA) cho lĩnh vực y tế, Gramm-Leach-Bliley Act (GLBA) cho dịch vụ tài chính, và Children’s Online Privacy Protection Act (COPPA) cho dữ liệu

<sup>4</sup> State Council of the People’s Republic of China (2021), *Opinions on Building a More Complete Factor Market System* (关于构建更加完善的要素市场化配置体制机制的意见), Gov.cn, [https://www.gov.cn/zhengce/2020-04/09/content\\_5500622.htm](https://www.gov.cn/zhengce/2020-04/09/content_5500622.htm), truy cập ngày 31/7/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

trẻ em... Mô hình quản lý này phản ánh triết lý pháp lý của Hoa Kỳ: chính phủ liên bang chủ yếu thực hiện hậu kiểm, tức chỉ can thiệp khi xảy ra khiếu nại, vi phạm quyền riêng tư nghiêm trọng, hoặc dấu hiệu cạnh tranh không lành mạnh; trong khi các doanh nghiệp, đặc biệt là các tập đoàn công nghệ lớn như Google, Meta, Amazon, lại có quyền tự chủ tương đối cao trong việc thu thập, xử lý và khai thác thương mại dữ liệu. Các chính sách nội bộ do doanh nghiệp thiết lập thường đóng vai trò chính trong việc định hướng quyền truy cập và sử dụng dữ liệu của người dùng, trong khi vai trò của Nhà nước chỉ phát huy khi xuất hiện tranh chấp hoặc vụ việc gây dư luận lớn<sup>5</sup>.



***Một số quyền được quy định trong Đạo luật Quyền riêng tư  
của người tiêu dùng California - Ảnh: dropsuite.com***

Trước khi Luật Dữ liệu năm 2024 được ban hành, dữ liệu tại Việt Nam chỉ được điều chỉnh gián tiếp bởi các văn bản như Luật An ninh mạng năm 2018, Nghị định 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ

<sup>5</sup> Federal Trade Commission (2023), *Data privacy enforcement actions*, <https://www.ftc.gov>, truy cập ngày 01/8/2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

dữ liệu cá nhân, hoặc Luật Giao dịch điện tử năm 2023 và mới nhất là Luật Bảo vệ dữ liệu cá nhân năm 2025. Tuy nhiên, các văn bản này chủ yếu tập trung vào khía cạnh an ninh, bảo mật, trong khi chưa có hệ thống quy phạm điều chỉnh các hoạt động kinh doanh dữ liệu, chưa công nhận đầy đủ quyền sở hữu dữ liệu, và càng thiếu khung pháp lý về các loại hình sản phẩm hay dịch vụ khai thác giá trị của dữ liệu. Qua rà soát, trước khi Luật Dữ liệu được ban hành, có rất nhiều luật quy định về cơ sở dữ liệu (bao gồm cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành) và nhiều luật khác có nội dung quy định liên quan đến dữ liệu như Luật Giao dịch điện tử, Luật An ninh mạng, Luật An toàn thông tin mạng, Luật Viễn thông, Luật Công nghệ thông tin, dự thảo Luật Công nghiệp công nghệ số...

Qua phân tích, thống kê tại các văn bản luật nêu trên thì các luật này đã quy định về các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành với các nội dung và thành tố như: Trường thông tin có trong cơ sở dữ liệu (có cơ sở dữ liệu đã quy định rõ các trường thông tin, có cơ sở dữ liệu có quy định nhưng chưa cụ thể các trường thông tin và có cơ sở dữ liệu không quy định các trường thông tin); mô tả, định nghĩa về cơ sở dữ liệu (có cơ sở dữ liệu đã được nêu rõ mô tả, định nghĩa cụ thể, có cơ sở dữ liệu có quy định nhưng chưa cụ thể và có cơ sở dữ liệu không được định nghĩa); hình thức khai thác, chia sẻ (có cơ sở dữ liệu đã được quy định cụ thể về hình thức khai thác, chia sẻ dữ liệu, có cơ sở dữ liệu có quy định nhưng chưa cụ thể về hình thức khai thác, chia sẻ và có cơ sở dữ liệu không quy định). Việc thiếu khung pháp lý điều chỉnh hoạt động thương mại dữ liệu trong thời gian dài đã dẫn đến nhiều hệ lụy như: khai thác dữ liệu trái phép, mua bán dữ liệu cá nhân không kiểm soát, và hạn chế cơ hội phát triển thị trường dữ liệu số an toàn, minh bạch...

Cần phải nhấn mạnh rằng, trước năm 2024, Việt Nam chưa quy định





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

sản phẩm, dịch vụ liên quan đến dữ liệu đang phát triển trên thế giới như sản phẩm giao dịch dữ liệu, dịch vụ trung gian dữ liệu, dịch vụ phân tích, tổng hợp dữ liệu... Trong khi đó, việc thiết lập thị trường dữ liệu, xây dựng và phát triển các sản phẩm, dịch vụ liên quan đến dữ liệu hiện nay lại có vai trò rất quan trọng, nó được xem là yếu tố đột phá để từng bước tạo lập và thúc đẩy mở thị trường dữ liệu, lấy thị trường dữ liệu làm động lực phát triển dữ liệu và kích thích, thúc đẩy chuyển đổi số các ngành, các lĩnh vực, tăng năng lực cạnh tranh, bảo đảm cho tiến trình chuyển đổi số ở nước ta. Chính vì vậy, sự ra đời của Luật Dữ liệu năm 2024, đặc biệt với việc dành trọn “*Chương IV: Sản phẩm, dịch vụ về dữ liệu*”, đánh dấu lần đầu tiên pháp luật Việt Nam công nhận dữ liệu là tài sản và thừa nhận các hoạt động thương mại với dữ liệu là hợp pháp, có thể phát triển thành ngành kinh tế.



***Internet vạn vật - Ảnh: Thư viện pháp luật***

Việc đưa vào luật các loại hình như dịch vụ trung gian dữ liệu, dịch vụ phân tích dữ liệu, hay sản phẩm dữ liệu không chỉ là hành vi luật hóa thực tiễn, mà





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

còn tạo khung pháp lý để điều tiết, bảo vệ và phát triển thị trường dữ liệu một cách lành mạnh, hợp pháp. Đồng thời, việc coi dữ liệu là tài sản cũng đã dẫn đến một hệ quả tất yếu là cần có khung pháp lý và chính sách cụ thể để dữ liệu có thể được sở hữu, chuyển nhượng, định giá và khai thác thương mại. Không dừng ở quyền riêng tư, Luật Dữ liệu 2024 còn đặt nền móng cho hình thành thị trường dịch vụ dữ liệu, tương tự thị trường chứng khoán hay thị trường tài chính. Đây là hướng tiếp cận hiện đại, phù hợp với xu thế toàn cầu về quản trị dữ liệu và phát triển kinh tế số.



***Bảo đảm an ninh, an toàn dữ liệu trong kỷ nguyên số - Ảnh: VnEconomy***





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Việc quy định rõ ràng về sản phẩm và dịch vụ dữ liệu không chỉ nhằm hợp pháp hóa hoạt động khai thác dữ liệu trong các lĩnh vực như tài chính, y tế, giao thông hay thương mại điện tử, mà còn tạo ra hành lang pháp lý rõ ràng để thúc đẩy đổi mới sáng tạo, bảo vệ quyền lợi của cá nhân và tổ chức, đồng thời tăng cường năng lực kiểm soát rủi ro liên quan đến quyền riêng tư, an ninh mạng và thao túng thị trường dữ liệu. Tuy vậy, thực tiễn triển khai thời gian tới khả năng cao vẫn phải đối mặt với nhiều thách thức, từ hạn chế kỹ thuật, thiếu hụt mô hình kinh doanh dữ liệu bền vững, cho đến văn hóa sử dụng dữ liệu còn yếu và năng lực hậu kiểm dịch vụ chưa đồng bộ giữa các cấp quản lý. Do đó, việc quy định về sản phẩm, dịch vụ dữ liệu cần gắn liền với các chính sách, cơ sở hạ tầng và nâng cao nhận thức xã hội về giá trị và trách nhiệm trong khai thác dữ liệu.

### **7.1.2. Sản phẩm, dịch vụ về dữ liệu là gì?**

Trong bối cảnh dữ liệu ngày càng đóng vai trò thiết yếu trong mọi lĩnh vực từ tài chính, y tế đến giáo dục, công nghiệp thì việc tạo ra các sản phẩm và dịch vụ dựa trên dữ liệu đã trở thành một xu thế chủ đạo trong nền kinh tế số. Theo 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 (gọi tắt là Nghị định số 169/2025/NĐ-CP): “*Sản phẩm, dịch vụ về dữ liệu là sản phẩm, dịch vụ được tạo thành từ dữ liệu hoặc sử dụng dữ liệu là nguồn tài nguyên chính để phát triển, ứng dụng, giao dịch*”.

Trong kỷ nguyên vươn mình của dân tộc, khi dữ liệu đã và đang trở thành “*tư liệu sản xuất*” cốt lõi, việc hiểu rõ sự khác biệt giữa các mô hình khai thác dữ liệu là điều cần thiết để thiết kế, hoạch định chính sách, triển khai các giải pháp công nghệ và phát triển mô hình kinh tế phù hợp. Tuy nhiên, hai khái niệm “*sản phẩm dữ liệu*” và “*dịch vụ dữ liệu*” vẫn còn khá



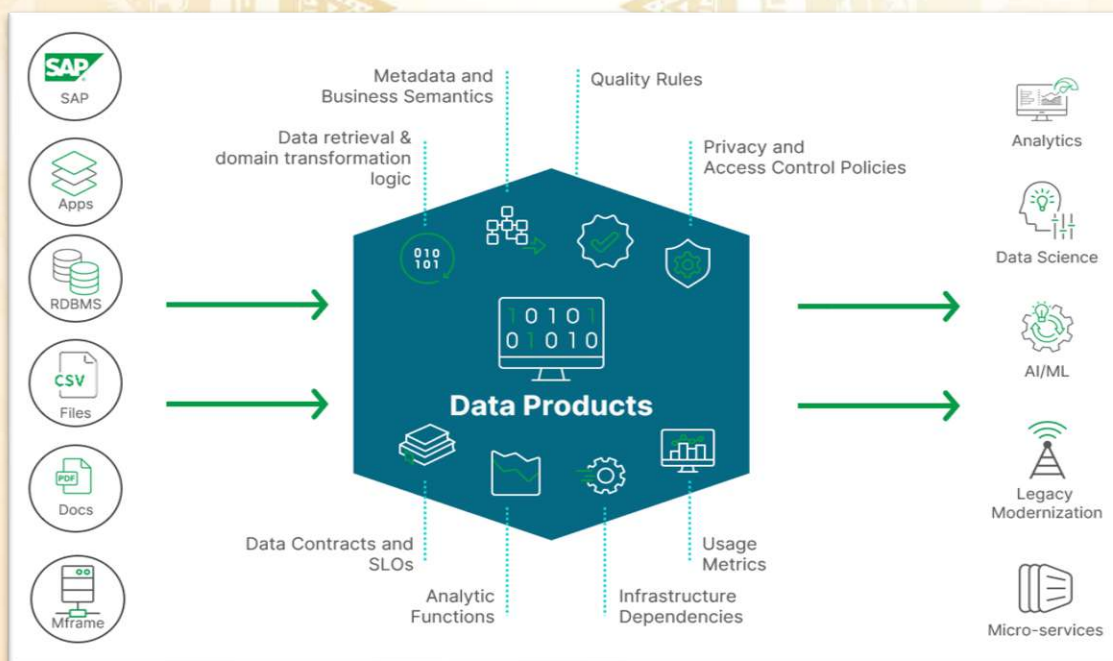


## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

mới, chưa phổ biến rộng rãi; việc tiếp cận, nghiên cứu vẫn còn những hạn chế nhất định. Do đó, không chỉ nghiên cứu, phân tích, làm rõ mà việc phân biệt rõ ràng giữa hai khái niệm này là rất quan trọng để đảm bảo việc tuân thủ pháp luật và khai thác giá trị dữ liệu một cách hiệu quả. Mặc dù cả hai đều liên quan đến việc cung cấp và sử dụng dữ liệu, chúng lại khác nhau về bản chất, hình thức, mục đích và cách thức người dùng sử dụng.

### **7.1.2.1. Sản phẩm dữ liệu (data product)**

Theo Wikipedia, “*sản phẩm dữ liệu*” là một tài sản dữ liệu có tính tiêu chuẩn hóa, có thể tái sử dụng, có chức năng cụ thể và được thiết kế nhằm mang lại giá trị rõ ràng cho người dùng... Chúng bao gồm tập dữ liệu, mô hình, quy trình xử lý, siêu dữ liệu và tuân thủ theo nguyên tắc FAIR: Findable (có thể tìm thấy), Accessible (có thể truy cập), Interoperable (có thể tương tác), and Reusable (có thể tái sử dụng)<sup>6</sup>.



**Minh họa sản phẩm dữ liệu - Ảnh: Qlik**

<sup>6</sup> Wikipedia (2025), *Sản phẩm dữ liệu*, [https://en.wikipedia.org/wiki/Data\\_product](https://en.wikipedia.org/wiki/Data_product), truy cập ngày 31/07/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Theo DataCamp (2023), “*sản phẩm dữ liệu*” là một sản phẩm kỹ thuật hoặc công nghệ được xây dựng trên nền tảng dữ liệu nhằm giúp người dùng đưa ra quyết định nhanh chóng, chính xác và ít phụ thuộc vào các kỹ năng phân tích phức tạp. Không giống như dữ liệu thô chỉ phục vụ cho nhà phân tích hoặc kỹ sư dữ liệu, sản phẩm dữ liệu được thiết kế để phục vụ trực tiếp cho người dùng cuối, kể cả khi họ không có chuyên môn sâu về dữ liệu<sup>7</sup>.

Như vậy, có thể thấy rằng, khái niệm “*sản phẩm dữ liệu*” dùng để chỉ các kết quả có thể khai thác từ dữ liệu gốc thông qua quá trình xử lý, tổng hợp hoặc mô hình hóa. Sản phẩm dữ liệu là những “đầu ra” hữu ích được tạo ra từ dữ liệu sau khi đã được xử lý, tổ chức và trình bày một cách rõ ràng, chuyên nghiệp. Giống như một sản phẩm công nghệ, sản phẩm dữ liệu có thể được “đóng gói”, mô tả chi tiết, dễ chia sẻ và sử dụng lại nhiều lần. Chúng có thể là bản đồ dữ liệu, báo cáo, thống kê, mô hình trí tuệ nhân tạo, hoặc công cụ phân tích dự báo thị trường... Bất kỳ kết quả đầu ra nào do nhóm dữ liệu tạo ra và được bên sử dụng dữ liệu tiêu thụ đều có thể được coi là một “sản phẩm dữ liệu”. Tuy nhiên, không phải cứ tạo ra bảng biểu hoặc báo cáo là đã có “sản phẩm dữ liệu” mà nó phải bao gồm nhiều đặc điểm và thuộc tính bổ trợ như sau nhằm giúp dễ tìm kiếm, dễ sử dụng và dễ quản lý hơn theo thời gian so với một bảng dữ liệu, báo cáo hay mô hình thông thường:

+ ***Có thể tìm kiếm được (Discoverable)***: Người dùng có thể dễ dàng tra cứu qua các danh mục dữ liệu, tránh tình trạng “dữ liệu tối” là những dữ liệu bị bỏ quên, tồn tại nguyên mà không được khai thác, không tạo ra giá trị, lãng phí.

+ ***Có địa chỉ định danh (Addressable)***: Mỗi sản phẩm dữ liệu cần có

<sup>7</sup> Pykes, K. (2024), *What Is a Data Product? Concepts and Best Practices*, DataCamp.com, <https://www.datacamp.com/blog/data-product>, truy cập ngày 1/8/2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

một mã định danh/ địa chỉ duy nhất để nhóm khác có thể truy cập và sử dụng. Địa chỉ này có thể là một địa chỉ kết nối kèm tên cơ sở dữ liệu và tên bảng, nếu đó là một bảng trong cơ sở dữ liệu; một đường dẫn S3 URI đến một file Parquet, nếu file đó nằm trong kho lưu trữ Amazon S3 hoặc một đường dẫn HTTP URL, nếu đó là một báo cáo của Looker.

+ ***Đáng tin cậy và theo dõi được (Trustworthy & Observable)***: Hiện thị nguồn gốc, lịch sử cập nhật, những chuyển đổi đã áp dụng để tính toán các trường của sản phẩm dữ liệu hiện tại. Tức là, bất cứ ai cũng có thể xem được dữ liệu này đến từ đâu, được cập nhật lần cuối khi nào và đã được xử lý như thế nào để ra kết quả cuối cùng. Nhờ vậy, người dùng sẽ tin tưởng hơn vào độ chính xác và giá trị của dữ liệu.

+ ***Tự mô tả (Self-describing)***: Sản phẩm dữ liệu cần tự giải thích được bản thân nó. Nó phải bao gồm thông tin mô tả về mục đích sử dụng, ý nghĩa của từng trường dữ liệu và cách dữ liệu được tạo ra. Ngoài ra, nó cũng cần có thông tin về phiên bản để những người dùng cũ vẫn có thể sử dụng mà không gặp lỗi.

+ ***Có khả năng tương tác (Interoperable)***: Hỗ trợ truy xuất thông qua SQL, API, hoặc các định dạng file rõ ràng... giúp người dùng có thể trích xuất dữ liệu và đưa vào các sản phẩm dữ liệu khác hoặc sử dụng cho mục đích của riêng họ.

+ ***Đảm bảo bảo mật và được quản lý (Secure & Governed)***: Một sản phẩm dữ liệu cần được xác định các cơ chế để kiểm soát quyền truy cập dữ liệu mà nó chứa, kiểm tra nhật ký truy cập và có cách xử lý đặc biệt đối với thông tin nhạy cảm (như thông tin cá nhân) để đảm bảo tuân thủ các quy định của pháp luật.

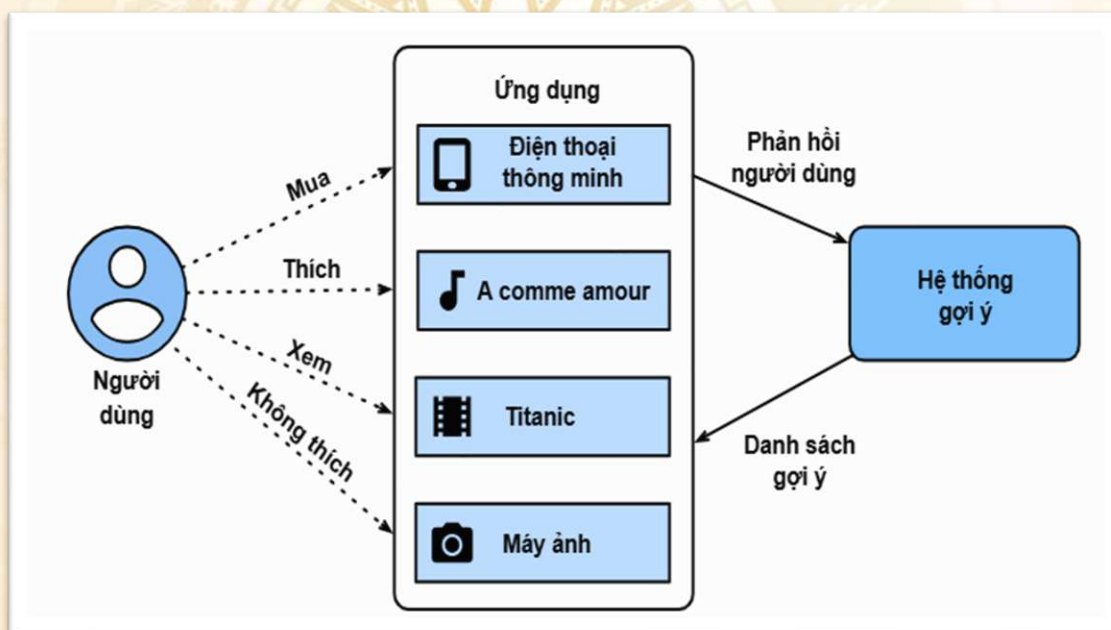




## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Những đặc điểm vừa được trình bày là nền tảng lý thuyết cho việc xây dựng một sản phẩm dữ liệu hiệu quả. Để minh chứng cho tính ứng dụng của các đặc tính này, chúng ta sẽ khảo sát một số ví dụ thực tiễn trên thế giới, nhằm làm rõ cách thức những nguyên lý này được triển khai trong thực tế:

+ Một dạng sản phẩm dữ liệu phổ biến là hệ thống đề xuất nội dung (recommendation systems), sử dụng dữ liệu hành vi để cá nhân hóa trải nghiệm người dùng. Chẳng hạn, nền tảng Spotify triển khai tính năng “Discover Weekly”, một danh sách được tạo tự động mỗi tuần dựa trên thói quen nghe nhạc và các mô hình học máy. Tương tự, Netflix sử dụng lịch sử xem phim để đề xuất nội dung phù hợp, qua đó tăng thời gian sử dụng và mức độ hài lòng của người dùng.



### ***Minh họa quá trình Đề xuất - Ảnh: Internet***

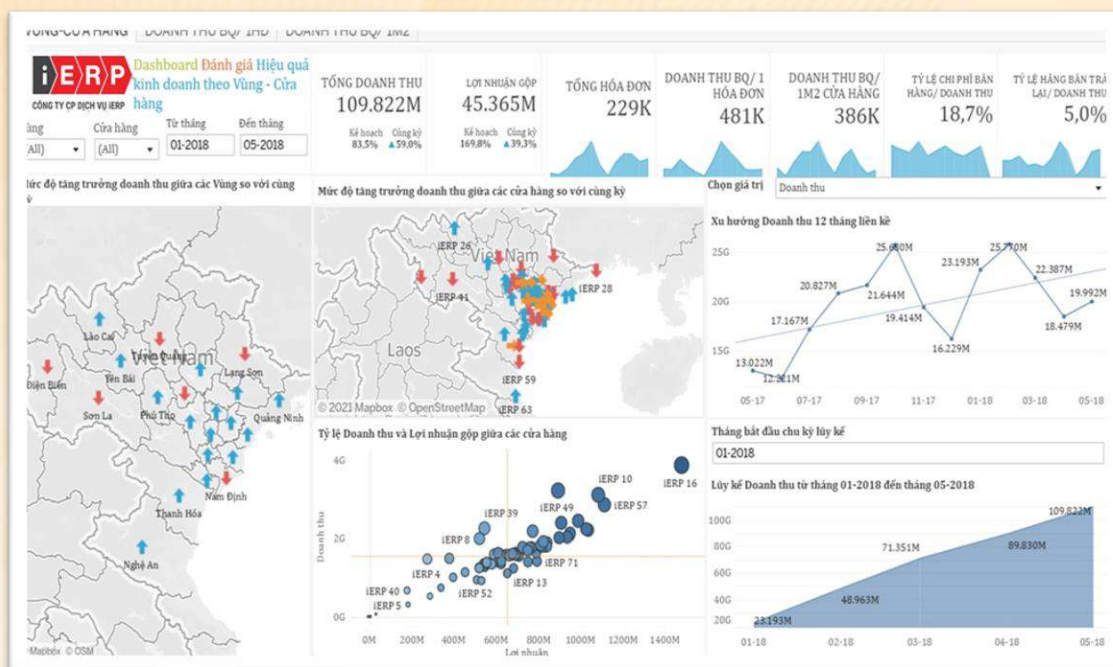
+ Một nhóm sản phẩm khác là bảng điều khiển phân tích dữ liệu (interactive dashboards), cung cấp cái nhìn tổng quan và tức thời về các chỉ số vận hành, giúp nhà quản trị đưa ra quyết định nhanh chóng. Ví dụ, Google Analytics cho phép doanh nghiệp theo dõi lưu lượng truy cập theo thời gian





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU Trong công an nhân dân

thực, trong khi Tableau cung cấp bảng biểu tương tác phục vụ phân tích bán hàng, tài chính hoặc marketing<sup>8</sup>.



## Tableau ngành bán lẻ - Báo cáo doanh thu cửa hàng - Ảnh: iERP

+ Ngoài ra, nhiều doanh nghiệp còn tích hợp mô hình dự báo (predictive models) vào quy trình vận hành để tự động hóa ra quyết định. Điển hình là Salesforce với hệ thống Einstein AI, hỗ trợ dự báo khả năng chuyển đổi khách hàng tiềm năng. Một ví dụ khác là Google Maps, nơi dữ liệu lịch sử giao thông và vị trí thực tế được xử lý để dự đoán thời gian đến nơi (ETA)<sup>9</sup>.

+ Không chỉ dừng lại ở ứng dụng nội bộ, sản phẩm dữ liệu còn được thương mại hóa trên các nền tảng như AWS Data Exchange, nơi doanh nghiệp có thể mua hoặc cấp quyền truy cập vào các bộ dữ liệu đã được chuẩn hóa; ví dụ: dữ liệu khí hậu, tài chính, nhân khẩu học... Đây là minh chứng

<sup>8</sup> Informatica (n.d.), *What is Data Services: Definition*, Informatica.com, <https://www.informatica.com/services-and-training/glossary-of-terms/data-services-definition.html>, truy cập ngày 01/8/2025.

<sup>9</sup> Zimmergren (2025), *Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework*, Microsoft.com, <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework>, truy cập ngày 31/7/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

cho việc dữ liệu sau khi được xử lý có thể trở thành một hàng hóa, có thể trao đổi, định giá và cấp phép sử dụng<sup>10</sup>.

+ Trong đời sống cá nhân, các ứng dụng như Apple Health hay MyFitnessPal cung cấp các sản phẩm dữ liệu cá nhân hóa, giúp người dùng theo dõi sức khỏe, vận động và chế độ ăn uống. Các sản phẩm này khai thác dữ liệu sinh trắc học và hành vi người dùng, xử lý chúng thông qua mô hình và biểu đồ, rồi hiển thị dưới dạng đơn giản, dễ hiểu, tạo ra giá trị cụ thể cho từng cá nhân [66].

Từ các ví dụ nêu trên, có thể thấy rằng sản phẩm dữ liệu có thể tồn tại dưới nhiều hình thức, từ bảng biểu, mô hình, giao diện lập trình ứng dụng đến ứng dụng hoàn chỉnh, nhưng điểm chung là chúng đều được xây dựng dựa trên dữ liệu đã qua xử lý, có thể sử dụng lại, đo lường hiệu quả rõ ràng và mang tính ứng dụng cao. Đây cũng là nền tảng cho sự phát triển của các thị trường dữ liệu và các mô hình kinh doanh mới dựa trên dữ liệu.

### MỘT SỐ SẢN PHẨM DỮ LIỆU TIÊU BIỂU TRÊN THẾ GIỚI

| Loại sản phẩm dữ liệu                                                 | Ví dụ tiêu biểu          | Tổ chức phát triển | Mục đích chính                                                      |
|-----------------------------------------------------------------------|--------------------------|--------------------|---------------------------------------------------------------------|
| <b>Hệ thống đề xuất nội dung</b><br>( <i>Recommendation Systems</i> ) | Discover Weekly          | Spotify            | Gợi ý cá nhân hóa theo hành vi người nghe                           |
|                                                                       | Gợi ý phim trên nền tảng | Netflix            | Tăng mức độ gắn kết, tối ưu thời gian xem và trải nghiệm người dùng |
| <b>Bảng điều khiển phân tích</b>                                      | Google Analytics         | Google             | Theo dõi và phân tích dữ liệu truy cập website theo thời gian thực  |

<sup>10</sup> DevX (n.d.), Data Services, <https://www.devx.com/terms/data-services/>, truy cập ngày 31/7/2025.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

| Loại sản phẩm dữ liệu                                                          | Ví dụ tiêu biểu                 | Tổ chức phát triển        | Mục đích chính                                                                |
|--------------------------------------------------------------------------------|---------------------------------|---------------------------|-------------------------------------------------------------------------------|
| <i>(Interactive Dashboards)</i>                                                | Tableau Dashboard               | Salesforce                | Hỗ trợ ra quyết định trong bán hàng, tài chính, marketing                     |
| <b>Mô hình dự báo</b><br><i>(Predictive Models)</i>                            | Einstein AI                     | Salesforce                | Dự đoán khả năng chuyển đổi khách hàng tiềm năng                              |
|                                                                                | ETA (Dự đoán thời gian đến nơi) | Google Maps               | Ước lượng chính xác thời gian di chuyển dựa trên dữ liệu giao thông và vị trí |
| <b>Bộ dữ liệu thương mại hóa</b><br><i>(Commercial Data Assets)</i>            | AWS Data Exchange               | Amazon Web Services (AWS) | Cung cấp bộ dữ liệu chuẩn hóa cho các tổ chức sử dụng                         |
|                                                                                | Bloomberg Terminal              | Bloomberg                 | Cung cấp dữ liệu tài chính và thị trường thời gian thực                       |
| <b>Ứng dụng dữ liệu cá nhân hóa</b><br><i>(Personalized Data Applications)</i> | Apple Health                    | Apple                     | Tổng hợp, hiển thị và phân tích dữ liệu sức khỏe người dùng từ thiết bị đeo   |
|                                                                                | MyFitnessPal                    | Under Armour              | Cá nhân hóa kế hoạch ăn uống, tập luyện dựa trên dữ liệu sinh trắc            |





Đối với Việt Nam, mặc dù trước đây chưa có khung pháp lý chuyên biệt và đầy đủ về sản phẩm, dịch vụ dữ liệu, nhưng trên thực tế, nhiều cơ quan, tổ chức, cá nhân tại Việt Nam đã chủ động triển khai các ứng dụng và nền tảng dữ liệu, tạo ra những sản phẩm và dịch vụ dữ liệu đa dạng. Các hệ thống này tuy chưa được định danh rõ ràng theo thuật ngữ pháp lý trước khi Luật Dữ liệu năm 2024 được ban hành, nhưng đã thể hiện rõ những đặc trưng cốt lõi như: thu thập, xử lý, phân tích dữ liệu để tạo ra giá trị kinh tế hoặc giá trị sử dụng, có thể thương mại hóa hoặc cung cấp dưới dạng dịch vụ nền tảng. Sự xuất hiện ngày càng nhiều của các mô hình gợi ý nội dung, bảng điều khiển phân tích, nền tảng thương mại dữ liệu, hay dịch vụ xác thực điện tử cho thấy hệ sinh thái dữ liệu tại Việt Nam đang phát triển vô cùng mạnh mẽ và ngày càng đa dạng.

Trong những năm gần đây, nhiều doanh nghiệp và tổ chức tại Việt Nam đã phát triển các sản phẩm dữ liệu phục vụ cho các mục đích thương mại, công cộng và cá nhân. Một lĩnh vực tiêu biểu là hệ thống đề xuất nội dung, điển hình ứng dụng nghe nhạc Zing MP3 do VNG phát triển được tích hợp cơ chế đề xuất bài hát dựa trên lịch sử nghe và hành vi của người dùng, nhằm cá nhân hóa trải nghiệm âm nhạc tương tự như Spotify<sup>11</sup>. Tương tự, nền tảng VTVGo của Đài Truyền hình Việt Nam sử dụng mô hình gợi ý chương trình truyền hình theo thói quen người xem để tăng thời gian sử dụng và mức độ tương tác<sup>12</sup>.

<sup>11</sup> Tiểu Minh (2020), *Ứng dụng nghe nhạc Việt được tích hợp trí tuệ nhân tạo*, Báo Pháp Luật TP.HCM, <https://plo.vn/ky-nguyen-so/ung-dung-nghe-nhac-viet-duoc-tich-hop-tri-tue-nhan-tao-post594743.html>, truy cập ngày 31/7/2025.

<sup>12</sup> Chu Anh (2023), *Nền tảng truyền hình số quốc gia VTVgo - Vươn mình cạnh tranh OTT quốc tế*, vtv.vn, <https://vtv.vn/truyen-hinh/nen-tang-truyen-hinh-so-quoc-gia-vtvgo-vuon-minh-can-tranh-ott-quoc-te-20230608-033031842.htm>, truy cập ngày 31/07/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Trong khối nhà nước, bảng điều khiển phân tích dữ liệu đã được triển khai rộng rãi để phục vụ điều hành và giám sát. Ví dụ, Ngân hàng Nhà nước Việt Nam đã xây dựng hệ thống tổng hợp các chỉ số vĩ mô như lãi suất, tỷ giá, tín dụng... thành “*dashboard*” nhằm hỗ trợ ra quyết định chính sách tiền tệ<sup>13</sup>. Bên cạnh đó, trong giai đoạn dịch bệnh COVID-19, Bộ Y tế đã ứng dụng bảng điều khiển phân tích dịch tễ để theo dõi ca nhiễm, năng lực bệnh viện và tốc độ tiêm chủng theo thời gian thực<sup>14</sup>.



***Trung tâm thông tin chỉ huy Cục Cảnh sát giao thông - Ảnh: Báo Nhân dân***

Đối với lĩnh vực năng lượng và giao thông, nhiều tổ chức trong nước đã phát triển mô hình dự báo ứng dụng dữ liệu lớn (Big Data) và trí tuệ nhân tạo (AI). Camera giao thông ứng dụng AI do các kỹ sư Viettel High Tech

<sup>13</sup> Trang (2025), *Ngành Ngân hàng tiếp tục tiên phong trong chuyển đổi số, cùng đất nước bước vào kỷ nguyên mới*, Tạp Chí Ngân Hàng, <https://tapchinganhang.gov.vn/nganh-ngan-hang-tiep-tuc-tien-phong-trong-chuyen-doi-so-cung-dat-nuoc-buoc-vao-ky-nguyen-moi-16085.html>, truy cập ngày 31/07/2025.

<sup>14</sup> Bộ Y tế (2022), *Kế hoạch phòng chống dịch bệnh truyền nhiễm năm 2022*, Ban hành kèm theo Quyết định số 165/QĐ-BYT ngày tháng năm 2022 của Bộ trưởng Bộ Y tế.





nghiên cứu là một ứng dụng tiêu biểu của dữ liệu thời gian thực vào quản trị đô thị thông minh. Đây được xem là hệ thống “mắt thần” tích hợp công nghệ trí tuệ nhân tạo AI giúp Trung tâm thông tin chỉ huy Cục Cảnh sát giao thông có thể nhận diện được khoảng 20 hành vi vi phạm giao thông, có thể vẽ lại hành trình của một chiếc xe tình nghi gây tai nạn một cách nhanh chóng. Đặc biệt, hệ thống này nhận diện và cảnh báo cả các hành vi gây rối, khuôn mặt đối tượng truy nã<sup>15</sup>.

Về mặt thương mại hóa dữ liệu, Viettel Solutions triển khai nền tảng Data Platform nhằm cung cấp cho các doanh nghiệp những bộ dữ liệu phân tích theo ngành như viễn thông, tài chính, tiêu dùng... được chuẩn hóa và truy cập qua giao diện lập trình ứng dụng<sup>16</sup>. Tương tự, Zalo Ads của Công ty VNG là nền tảng quảng cáo tích hợp mạnh mẽ khả năng khai thác dữ liệu hành vi người dùng từ hệ sinh thái Zalo (bao gồm ứng dụng Zalo, Zing MP3, Báo Mới, Zalo Shop...); từ đó tối ưu hóa việc hiển thị quảng cáo phù hợp với đối tượng mục tiêu. Nền tảng này sử dụng các thuật toán phân nhóm người dùng dựa trên thông tin như độ tuổi, vị trí, sở thích và tương tác trên ứng dụng để tự động điều chỉnh nội dung quảng cáo và hình thức phân phối hiệu quả hơn...

### **7.1.2.2. Dịch vụ dữ liệu (data services)**

Theo từ điển chuyên ngành DevX, “dịch vụ dữ liệu” là các giải pháp và công cụ được sử dụng để quản lý, lưu trữ, xử lý và phân tích dữ liệu trong một tổ chức hoặc hệ thống. Các dịch vụ này thường bao gồm tích hợp dữ liệu, kho

<sup>15</sup> Thanh Hà (2025), *Khám phá hệ thống camera AI tự động phát hiện vi phạm giao thông, hành vi gây rối và đối tượng truy nã*, Báo Điện Tử Tiền Phong, <https://tienphong.vn/kham-pha-he-thong-camera-ai-tu-dong-phat-hien-vi-pham-giao-thong-hanh-vi-gay-roi-va-doi-tuong-truy-na-post1760924.tpo>, truy cập ngày 31/07/2025.

<sup>16</sup> Viettel (n.d.), *Nền tảng dữ liệu lớn Viettel Data Platform (VDP)*, [solutions.viettel.vn, https://solutions.viettel.vn/vi/vi/cong-nghe-thong-tin/nen-tang-du-lieu-lon-viettel-data-platform-vdp.html](https://solutions.viettel.vn/vi/vi/cong-nghe-thong-tin/nen-tang-du-lieu-lon-viettel-data-platform-vdp.html), truy cập ngày 31/07/2025.

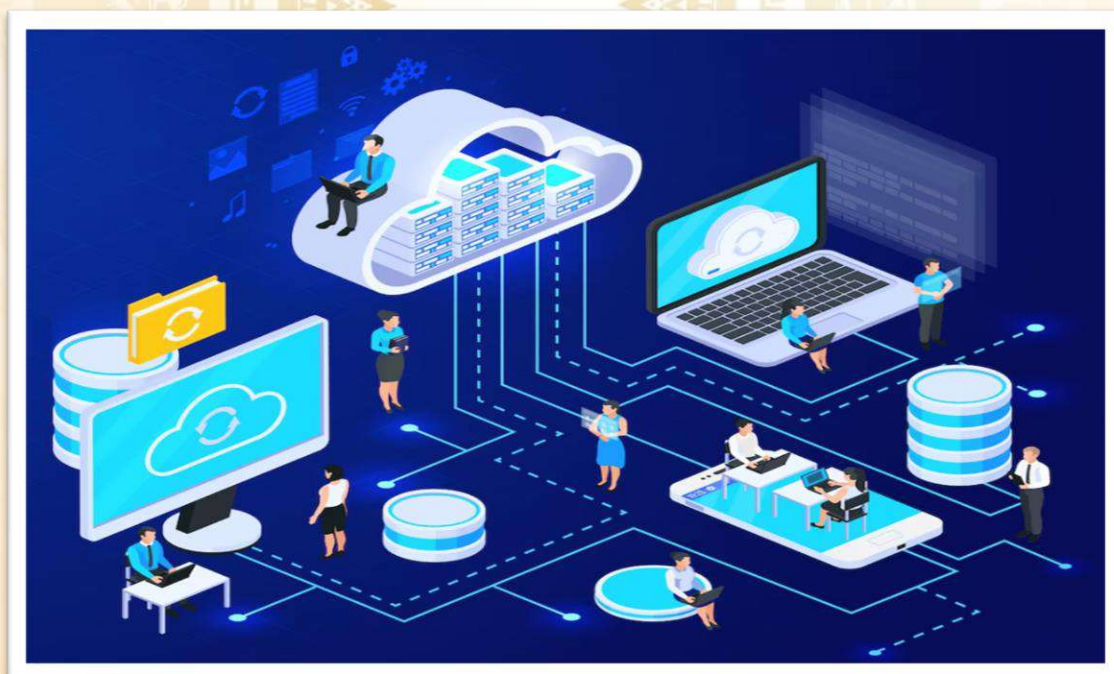




## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

dữ liệu, khai thác dữ liệu, phân tích dữ liệu và chuyển đổi dữ liệu<sup>17</sup>. Dịch vụ dữ liệu hoạt động như một lớp trung gian, có nhiệm vụ tự động hóa các truy vấn và điều phối luồng dữ liệu từ nhiều nguồn lưu trữ khác nhau, đảm bảo dữ liệu đến tay người dùng cuối một cách chính xác, an toàn và kịp thời.

Nói một cách dễ hiểu, dịch vụ dữ liệu là “*cầu nối kỹ thuật số*” giữa nguồn dữ liệu và người sử dụng cuối, hay từ doanh nghiệp, nhà phát triển phần mềm đến người tiêu dùng. Những dịch vụ này không chỉ đơn thuần là truyền dữ liệu, mà còn thực hiện nhiều chức năng khác như chuẩn hóa, lọc, tổng hợp, mã hóa, cung cấp dữ liệu theo thời gian thực, và đảm bảo quyền riêng tư hoặc bảo mật [61]. Khác với sản phẩm dữ liệu - là đầu ra đã hoàn chỉnh và có thể sử dụng ngay - dịch vụ dữ liệu thường là quy trình hỗ trợ có tính nền tảng, giúp các hệ thống khác truy cập hoặc sử dụng dữ liệu dễ dàng, đúng định dạng, đúng thời điểm.



***Minh họa về dịch vụ dữ liệu - Ảnh: Internet***

<sup>17</sup> DevX (2023), *Data Services – Glossary*, <https://www.devx.com>, truy cập ngày 31/07/2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Dịch vụ dữ liệu là một phần không thể thiếu trong hạ tầng dữ liệu hiện đại, được thiết kế nhằm đơn giản hóa quá trình truy cập và sử dụng dữ liệu từ nhiều nguồn khác nhau. Một trong những đặc điểm nổi bật của dịch vụ dữ liệu là khả năng cung cấp dữ liệu theo yêu cầu, thường thông qua các giao diện lập trình ứng dụng (API), phần mềm dạng dịch vụ (SaaS) hoặc giao diện web tương tác. Ví dụ, một nhà phát triển có thể sử dụng API từ nền tảng bất động sản Estatic để truy cập dữ liệu nhà ở tại Mỹ chỉ bằng cách nhập địa chỉ hoặc mã ZIP.

Bên cạnh đó, dịch vụ dữ liệu có khả năng kết nối với nhiều nguồn dữ liệu không đồng nhất, bao gồm hệ thống quản lý quan hệ khách hàng (CRM), nền tảng thương mại điện tử, cảm biến Internet Vạn Vật (IoT) hay các cơ sở dữ liệu truyền thống. Điều này giúp các doanh nghiệp và tổ chức tích hợp dữ liệu liền mạch vào chuỗi giá trị vận hành. Ngoài ra, dịch vụ dữ liệu còn tích hợp chức năng xử lý tự động như làm sạch, chuẩn hóa và kiểm tra chất lượng dữ liệu, giúp tiết kiệm thời gian và đảm bảo tính chính xác của thông tin được cung cấp. Một điểm mạnh quan trọng nữa là khả năng kiểm soát truy cập và bảo mật dữ liệu. Dịch vụ dữ liệu thường cho phép thiết lập quyền truy cập theo vai trò, mã hóa dữ liệu nhạy cảm và lưu vết lịch sử truy cập, điều này đặc biệt quan trọng trong bối cảnh các quy định về bảo vệ dữ liệu cá nhân ngày càng chặt chẽ [49]. Dịch vụ dữ liệu thường có tính tái sử dụng cao, cho phép doanh nghiệp khai thác cùng một hạ tầng dịch vụ cho nhiều mục tiêu khác nhau như phân tích kinh doanh, đào tạo mô hình AI, phát triển sản phẩm số mới...

Hiện nay, nhiều tổ chức công nghệ lớn trên thế giới đã phát triển các dịch vụ dữ liệu mạnh mẽ, đóng vai trò quan trọng trong hệ sinh thái số toàn cầu. Một ví dụ điển hình là AWS Data Exchange của Amazon Web Services





- nền tảng cho phép các doanh nghiệp mua và sử dụng dữ liệu đã chuẩn hóa từ hàng trăm nhà cung cấp. Dữ liệu có thể thuộc nhiều lĩnh vực như tài chính, thời tiết, địa lý, được truy cập thông qua API và được cập nhật liên tục theo thời gian thực [42].

Ở lĩnh vực phân tích, Google BigQuery Data Transfer Service hỗ trợ việc chuyển dữ liệu tự động từ các dịch vụ SaaS phổ biến như Google Ads, YouTube hoặc Google Analytics vào kho dữ liệu BigQuery. Điều này giúp các doanh nghiệp không cần viết mã lập trình mà vẫn đảm bảo luồng dữ liệu luôn được cập nhật sẵn sàng cho phân tích<sup>18</sup>. Một ví dụ nổi bật khác là Snowflake Marketplace, nơi người dùng có thể truy cập các bộ dữ liệu thương mại từ cộng đồng Snowflake, phục vụ cho nhiều mục đích như phân tích thị trường, nghiên cứu người tiêu dùng hoặc đào tạo mô hình AI. Dữ liệu trong Snowflake được chia sẻ theo chuẩn thống nhất, tích hợp trực tiếp vào hệ thống phân tích của người dùng, tạo ra quy trình làm việc liền mạch và hiệu quả<sup>19</sup>.

Trong lĩnh vực tích hợp và xử lý dữ liệu, Informatica Cloud Data Integration là một dịch vụ mạnh mẽ hỗ trợ doanh nghiệp di chuyển dữ liệu từ nhiều hệ thống khác nhau như Salesforce, SAP, Oracle, AWS S3, Azure Blob, Google Cloud Storage..., đồng thời làm sạch, chuyển đổi và kiểm tra chất lượng dữ liệu ngay trong quá trình xử lý. Dịch vụ này đặc biệt phù hợp cho các tổ chức cần đồng bộ dữ liệu từ nhiều đơn vị hoặc triển khai các dự án phân tích quy mô lớn<sup>20</sup>.

<sup>18</sup> Google Cloud (2024), *What is BigQuery Data Transfer Service?*, <https://cloud.google.com/bigquery/docs/dts-introduction>, truy cập ngày 31/7/2025.

<sup>19</sup> Snowflake Inc (2025), *About Snowflake Marketplace, Snowflake Documentation*, <https://docs.snowflake.com/en/>, truy cập ngày 03/08/2025.

<sup>20</sup> Informatica (n.d.), *Cloud Data Integration Overview*, <https://www.informatica.com/products/cloud-integration/cloud-data-integration.html>, truy cập ngày 03/08/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Các ví dụ trên cho thấy dịch vụ dữ liệu không chỉ giúp tiết kiệm thời gian, tăng hiệu quả xử lý, mà còn mở ra tiềm năng thương mại hóa và chia sẻ dữ liệu một cách an toàn, minh bạch, tuân theo quy trình, có cơ chế kiểm soát. Nhờ vậy, dữ liệu không còn chỉ là “nguyên liệu thô”, mà trở thành một loại tài sản có thể khai thác nhiều lần để tạo ra giá trị, phục vụ cho phân tích, dự báo, xây dựng sản phẩm, hoặc thậm chí là đem bán, cho thuê trên các nền tảng thương mại dữ liệu. Đây cũng chính là nền tảng để phát triển các mô hình kinh doanh mới dựa trên dữ liệu, như dịch vụ dữ liệu theo yêu cầu, các chợ dữ liệu trực tuyến, hoặc các công cụ phân tích dữ liệu thời gian thực... Tóm lại, dịch vụ dữ liệu đóng vai trò kết nối giữa dữ liệu và giá trị thực tiễn, giúp tổ chức, doanh nghiệp và cá nhân khai thác dữ liệu một cách thông minh, an toàn và hiệu quả, từ đó thúc đẩy sự phát triển của nền kinh tế số hiện đại.



**Mình họa dịch vụ xử lý dữ liệu của Công ty FSI - Ảnh: FSI**





### **7.1.2.3. Phân biệt sản phẩm dữ liệu và dịch vụ dữ liệu**

Từ những nội dung đã phân tích ở trên, sau đây, nhóm tác giả xin tóm tắt những điểm khác nhau cơ bản về sản phẩm và dịch vụ dữ liệu như sau:

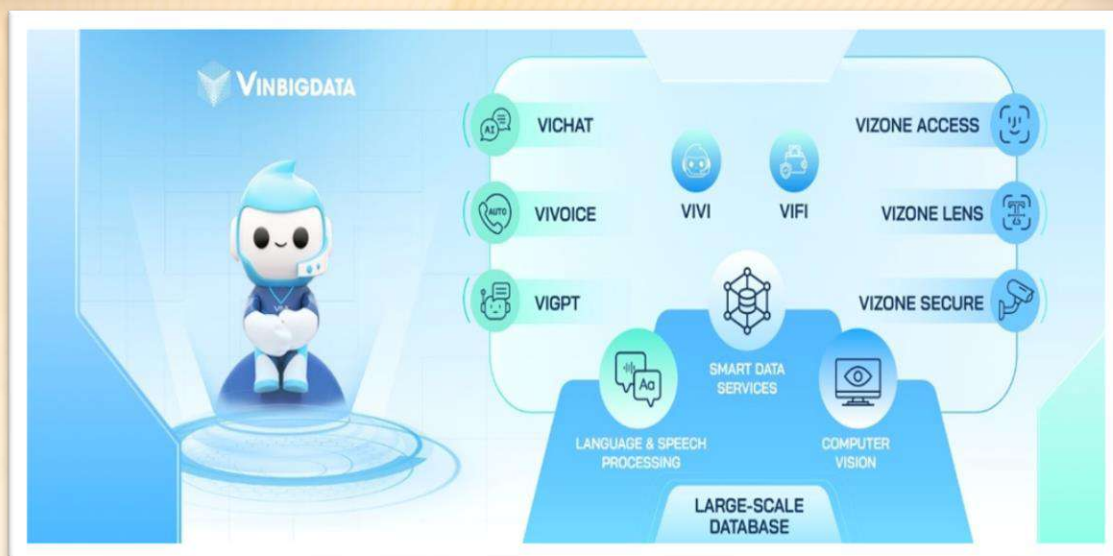
**Thứ nhất**, “sản phẩm dữ liệu” có bản chất giống như một món hàng hữu hình, là kết quả cuối cùng đã được xử lý, tổ chức và đóng gói sẵn sàng để sử dụng. Nó không phải là dữ liệu thô, mà là thông tin đã được làm sạch, chuyển đổi và làm giàu để giải quyết một nhu cầu cụ thể. Sản phẩm dữ liệu có tính chất tĩnh, có thể được lưu trữ và sử dụng nhiều lần. Một sản phẩm dữ liệu thường phải có địa chỉ rõ ràng như một sản phẩm vật chất, nó có một địa chỉ hoặc mã định danh duy nhất (một đường dẫn S3 URI đến file, một URL của báo cáo...); có mô tả chi tiết về nguồn gốc, ý nghĩa của từng trường dữ liệu và cách nó được tạo ra và người dùng có thể kiểm tra được nguồn gốc, thời điểm cập nhật và các quy trình xử lý dữ liệu để tin tưởng vào chất lượng của nó. Sản phẩm dữ liệu ở Việt Nam ngày càng phổ biến, đặc biệt trong các lĩnh vực tài chính, thương mại điện tử và công nghệ. Các sản phẩm này thường là những bộ dữ liệu đã được tinh chỉnh hoặc những báo cáo đã hoàn thiện, sẵn sàng để sử dụng.

+ VinBigdata là đơn vị tiên phong cung cấp các giải pháp trí tuệ nhân tạo dựa trên nền tảng dữ liệu lớn, với các sản phẩm nổi bật như Trợ lý ảo ViVi, ViGPT, ViChat, ViVoice, Vizone, ViFi... Nổi bật với trợ lý ảo ViVi trên các dòng xe VinFast, được huấn luyện trên hàng nghìn giờ dữ liệu tiếng Việt; được xem là một sản phẩm dữ liệu vì nó đã được hoàn thiện và tích hợp vào một ứng dụng cụ thể. Hay nhận diện khuôn mặt là một trong những công nghệ lõi nổi bật được VinBigdata nghiên cứu và phát triển ngay từ những ngày đầu thành lập, hiện được ứng dụng trong nhiều giải pháp, hỗ trợ tích cực cho công tác quản lý an ninh, tối ưu vận hành doanh nghiệp, nâng cao trải nghiệm người dùng.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



### ***Hệ sinh thái VinBigData - Ảnh: VinBigData***

+ Một công ty thương mại điện tử cung cấp một tệp dữ liệu chứa thông tin về tất cả giao dịch mua bán trong quý gần nhất. Dữ liệu này đã được làm sạch, chuẩn hóa và đóng gói thành một file Parquet trên Amazon S3, sẵn sàng để người dùng khác tải về và phân tích.

+ Đội ngũ Marketing xây dựng một bảng điều khiển trên Google Looker, hiển thị các chỉ số về hiệu quả chiến dịch quảng cáo. Bảng điều khiển này là một sản phẩm dữ liệu vì nó đã tổng hợp và trực quan hóa thông tin, cung cấp một sản phẩm hoàn chỉnh để người dùng theo dõi và đánh giá.

+ Một ngân hàng phát triển một mô hình học máy để dự đoán khả năng vỡ nợ của khách hàng. Mô hình này sau khi được huấn luyện và kiểm thử sẽ được đóng gói như một sản phẩm dữ liệu, có thể được tích hợp vào hệ thống thẩm định khoản vay để sử dụng.

+ Trong các dự án phân tích dữ liệu lớn của các tổ chức tài chính tại Việt Nam, sản phẩm đầu ra thường là các kho dữ liệu đã được hợp nhất từ nhiều nguồn. Các kho dữ liệu này sau đó trở thành sản phẩm để các bộ phận khác trong công ty khai thác, phân tích và đưa ra quyết định.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

**Thứ hai, “dịch vụ dữ liệu”** có bản chất là một giải pháp “vô hình”, là một quy trình, một công cụ hoặc một nền tảng cho phép người dùng tương tác và xử lý dữ liệu. Nó không phải là kết quả cuối cùng mà là một phương tiện để người dùng tự tạo ra giá trị từ dữ liệu. Dịch vụ dữ liệu có tính chất động, thường được cung cấp theo nhu cầu của người dùng. Dịch vụ dữ liệu có khả năng tương tác khi nó cung cấp cách thức (API, SQL,...) để người dùng có thể trích xuất dữ liệu và tích hợp vào hệ thống của họ. Đây không phải là một tập tin đã hoàn thiện mà thường là một quá trình liên tục, người dùng có thể tùy chỉnh yêu cầu để nhận được dữ liệu hoặc kết quả mong muốn. Dịch vụ dữ liệu tại Việt Nam chủ yếu được cung cấp bởi các công ty công nghệ và viễn thông lớn, dưới dạng các giải pháp đám mây (Cloud Service) hoặc API. Các dịch vụ này giúp các doanh nghiệp khác có công cụ để quản lý, lưu trữ và xử lý dữ liệu của riêng họ, chẳng hạn như:

+ ***Dịch vụ lưu trữ đám mây từ Viettel IDC, VNPT Cloud, FPT Smart Cloud...*** Đây là những dịch vụ cung cấp hạ tầng để khách hàng có thể lưu trữ, quản lý và vận hành dữ liệu mà không cần đầu tư vào máy chủ vật lý. Khách hàng sử dụng dịch vụ này để tự xây dựng các sản phẩm dữ liệu của riêng mình.

+ ***API chia sẻ dữ liệu của các cơ quan Nhà nước:*** Nền tảng tích hợp và chia sẻ dữ liệu quốc gia (NDXP) cung cấp các API để các cơ quan, tổ chức có thể truy cập và chia sẻ dữ liệu một cách an toàn, minh bạch. Ví dụ, API cho phép đồng bộ thông tin giấy phép lái xe từ Bộ Giao thông vận tải đến Cơ sở dữ liệu quốc gia về dân cư. Đây là một dịch vụ vì nó cung cấp công cụ để các hệ thống khác tương tác với dữ liệu.

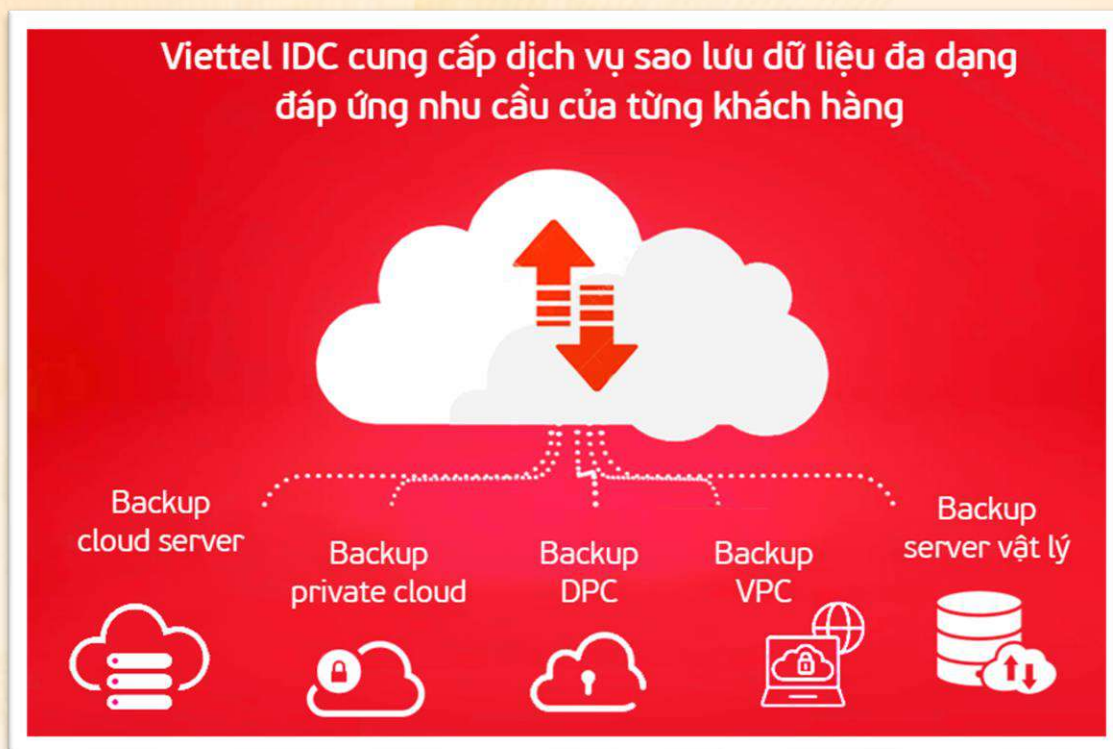
+ ***Các dịch vụ phân tích dữ liệu theo yêu cầu:*** Các công ty như EVOTEK cung cấp dịch vụ phân tích dữ liệu cho các tổ chức tài chính, giúp





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

họ xây dựng kho dữ liệu và thực hiện các nghiệp vụ phân tích kinh doanh. Đây là dịch vụ vì khách hàng thuê chuyên gia và công cụ để giải quyết một bài toán dữ liệu cụ thể, thay vì mua một tập dữ liệu đóng gói sẵn.



*Ảnh: Viettel IDC*

### TỔNG QUAN SO SÁNH GIỮA SẢN PHẨM DỮ LIỆU VÀ DỊCH VỤ DỮ LIỆU

| Tiêu chí          | Sản phẩm dữ liệu<br>(Data Product)                                                                                                                             | Dịch vụ dữ liệu (Data Service)                                                                                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Định nghĩa</b> | Một đơn vị dữ liệu đã được xử lý, đóng gói và hoàn thiện, sẵn sàng để sử dụng. Nó giống như một “món hàng” đã được chế biến sẵn, có tính chất tĩnh và độc lập. | Một giải pháp hoặc một hệ thống cung cấp hạ tầng để lưu trữ, xử lý và truyền tải dữ liệu theo nhu cầu. Nó giống như một “nhà bếp” với đầy đủ công cụ để người dùng tự chế biến. |





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

| Tiêu chí                 | Sản phẩm dữ liệu<br>(Data Product)                                                                                                                                                                        | Dịch vụ dữ liệu (Data Service)                                                                                                                                          |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Đối tượng sử dụng</b> | Các nhà phân tích dữ liệu, quản lý, và người dùng nghiệp vụ không chuyên về kỹ thuật, những người cần thông tin để ra quyết định.                                                                         | Các kỹ sư dữ liệu, nhà phát triển hệ thống và ứng dụng, những người cần công cụ để xây dựng và tích hợp dữ liệu vào các hệ thống.                                       |
| <b>Cách thức sử dụng</b> | Truy cập và tiêu thụ trực tiếp thông qua các bảng điều khiển, báo cáo, hoặc các tệp dữ liệu đã được đóng gói.                                                                                             | Tích hợp vào hệ thống của mình, sử dụng API hoặc các giao thức để truy vấn và xử lý dữ liệu theo thời gian thực.                                                        |
| <b>Ví dụ</b>             | Bảng điều khiển kinh doanh trên Microsoft Power BI, mô hình AI đã được huấn luyện để dự đoán hành vi khách hàng, hoặc một tập dữ liệu thống kê dân số đã được làm sạch.                                   | Một API thời tiết cung cấp dữ liệu theo thời gian thực, một nền tảng lưu trữ và phân tích dữ liệu đám mây, hoặc một dịch vụ streaming dữ liệu như Apache Kafka.         |
| <b>Tư duy phát triển</b> | “Dữ liệu là một sản phẩm” (Data as a Product) - tập trung vào việc tạo ra một sản phẩm hoàn chỉnh, có phiên bản, siêu dữ liệu và người chịu trách nhiệm rõ ràng để có thể tái sử dụng và bảo trì lâu dài. | “Dữ liệu là một dịch vụ” (Data as a Service) - tập trung vào việc xây dựng một hệ thống mạnh mẽ, linh hoạt và có khả năng mở rộng cao để phục vụ các nhu cầu khác nhau. |
| <b>Cách định giá</b>     | Trả phí theo đơn vị sản phẩm hoặc trả phí bản quyền.                                                                                                                                                      | Trả phí theo chu kỳ (đăng ký gói dịch vụ hàng tháng), hoặc theo                                                                                                         |





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

| Tiêu chí                            | Sản phẩm dữ liệu<br>(Data Product)                                                                                                                       | Dịch vụ dữ liệu (Data Service)                                                                                                                                 |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     |                                                                                                                                                          | mức độ sử dụng tài nguyên (số lần gọi API, dung lượng lưu trữ...).                                                                                             |
| <b>Vai trò pháp lý tại Việt Nam</b> | Được coi là một loại tài sản số, có thể được mua bán và cấp phép sử dụng. Các giao dịch này cần tuân thủ các quy định về quyền sở hữu và bảo vệ dữ liệu. | Được coi là một loại hình kinh doanh đặc thù, cần tuân thủ các quy định về đăng ký kinh doanh, kiểm soát kỹ thuật và bảo mật trong quá trình cung cấp dịch vụ. |
| <b>Yêu cầu kỹ thuật</b>             | Tối ưu hóa cho việc hiển thị và trực quan hóa, đảm bảo độ tin cậy và nguồn gốc dữ liệu rõ ràng để người dùng dễ dàng kiểm tra.                           | Đáp ứng khả năng truyền tải dữ liệu lớn, có tính phân tán và đảm bảo an toàn, bảo mật dữ liệu trong quá trình kết nối và xử lý.                                |

Việc phân biệt rõ ràng giữa sản phẩm dữ liệu và dịch vụ dữ liệu không chỉ mang tính học thuật, mà còn có ý nghĩa thiết thực và chiến lược trong quản trị dữ liệu, xây dựng chính sách pháp lý và triển khai các mô hình kinh doanh dữ liệu hiện đại. Dưới đây là một số nội dung thể hiện rõ *ý nghĩa của sự phân biệt* này:

**Một là**, đây là cơ sở cho xây dựng chính sách và hành lang pháp lý rõ ràng. Trong bối cảnh các quốc gia trên thế giới, bao gồm cả Việt Nam, đang nỗ lực thiết lập khung pháp lý về dữ liệu, việc xác định đâu là sản phẩm và đâu là dịch vụ giúp tránh sự chồng lấn, mập mờ trong quản lý. Trong Luật Dữ liệu Việt Nam năm 2024, cả sản phẩm và dịch vụ dữ liệu đều là đối tượng được điều chỉnh: **(1)** Sản phẩm dữ liệu có thể được quy định như tài sản số, hay “hàng hóa số”, có thể sở hữu, cấp phép sử dụng, định giá và giao dịch.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Việc này đặt ra yêu cầu pháp lý về bản quyền, định danh, chất lượng dữ liệu và trách nhiệm của bên cung cấp. **(2)** Dịch vụ dữ liệu thuộc nhóm dịch vụ số đặc thù, cần có giấy phép, tiêu chuẩn kỹ thuật và cơ chế hậu kiểm, nhằm bảo vệ an toàn thông tin, chống độc quyền và bảo vệ người tiêu dùng dữ liệu.

Như vậy, việc hiểu rõ bản chất của từng loại hình giúp các bên liên quan (từ người tạo ra đến người sử dụng) tuân thủ đúng các quy định về an ninh mạng, bảo vệ dữ liệu cá nhân, và các nghĩa vụ pháp lý liên quan, qua đó thúc đẩy một nền kinh tế số an toàn và bền vững.

**Hai là**, định hướng mô hình kinh doanh dữ liệu hiệu quả. Từ góc độ doanh nghiệp, việc phân biệt rõ giữa sản phẩm và dịch vụ dữ liệu đóng vai trò như kim chỉ nam cho việc xây dựng chiến lược khai thác, thương mại hóa dữ liệu và xác lập giá trị kinh doanh cốt lõi. Đây là tiền đề để tổ chức định hình mô hình, định giá phù hợp và tối ưu hóa dòng doanh thu từ tài nguyên dữ liệu mà mình sở hữu. Chẳng hạn, nếu một tổ chức sở hữu hệ thống dashboard phân tích, API dữ liệu bán cho đối tác thứ ba, hoặc mô hình trí tuệ nhân tạo phục vụ dự báo hành vi thì đây là những sản phẩm dữ liệu. Chúng có thể được “đóng gói” và phân phối như hàng hóa số, có giấy phép sử dụng rõ ràng và được định giá theo giá trị sử dụng. Ngược lại, nếu doanh nghiệp vận hành một nền tảng cho phép người dùng truy cập, xử lý hoặc đồng bộ hóa dữ liệu theo yêu cầu như một dịch vụ truy vấn theo thời gian thực, thì đó là dịch vụ dữ liệu. Loại hình này thường được định giá theo mức tiêu thụ, số lượt truy cập, băng thông hoặc mô hình đăng ký.

Như vậy, việc hiểu đúng và áp dụng phân biệt sản phẩm hay dịch vụ dữ liệu không chỉ giúp doanh nghiệp xác lập rõ định vị thị trường mà còn tối ưu hóa lợi thế cạnh tranh trong nền kinh tế dữ liệu.

**Ba là**, hỗ trợ triển khai hệ sinh thái dữ liệu và kiến trúc kỹ thuật số. Trong quá trình thiết kế và vận hành hệ sinh thái dữ liệu số, sự phân biệt





giữa sản phẩm dữ liệu và dịch vụ dữ liệu mang lại giá trị thực tiễn rõ ràng, đặc biệt trong việc phân tầng người dùng và tối ưu kiến trúc kỹ thuật. Sản phẩm dữ liệu thường phục vụ các nhóm người tiêu dùng dữ liệu (data consumers) như nhà quản lý, nhà nghiên cứu, chuyên gia phân tích hoặc khách hàng doanh nghiệp. Đây là các đầu ra có cấu trúc rõ ràng như báo cáo, dashboard, hoặc mô hình... giúp hỗ trợ ra quyết định, giám sát vận hành hoặc hoạch định chiến lược. Trong khi đó, dịch vụ dữ liệu lại hướng đến nhóm kỹ thuật, bao gồm kỹ sư dữ liệu, nhà phát triển phần mềm hoặc các hệ thống AI... nhằm cung cấp dữ liệu thô, truyền dẫn liên tục, hoặc xử lý truy vấn theo thời gian thực. Đây là lớp nền tảng hạ tầng dữ liệu, bảo đảm khả năng kết nối, tự động hóa và mở rộng hệ thống. Chính sự phân tách rõ ràng giữa hai loại hình này là tiền đề để các tổ chức xây dựng kiến trúc dữ liệu phân tầng, đảm bảo tính mở rộng, tính bảo mật và tính linh hoạt cao trong phối hợp đa bên, đa phương.

**Bốn là**, tăng cường minh bạch và tin cậy trong giao dịch dữ liệu. Khi dữ liệu trở thành một loại tài sản và hàng hóa có thể trao đổi trong nền kinh tế số, việc phân định rõ giữa sản phẩm dữ liệu và dịch vụ dữ liệu góp phần nâng cao mức độ minh bạch, xây dựng lòng tin giữa các chủ thể trong hệ sinh thái.

Cụ thể, việc xác định đúng bản chất của từng loại hình sẽ giúp các bên liên quan, bao gồm nhà cung cấp, người tiêu dùng và cơ quan quản lý hiểu rõ phạm vi trách nhiệm, quyền lợi, và nghĩa vụ pháp lý tương ứng. Điều này đóng vai trò quan trọng trong việc đề xuất đúng loại hợp đồng, xác định hình thức cấp phép phù hợp và định giá chính xác cho từng loại tài nguyên dữ liệu. Hơn thế nữa, việc phân biệt rõ ràng còn tạo tiền đề để thúc đẩy giao dịch dữ liệu minh bạch, thúc đẩy hoạt động chia sẻ, tái sử dụng dữ liệu có





kiểm soát, qua đó gia tăng hiệu quả vận hành và đổi mới sáng tạo trong toàn bộ hệ thống kinh tế số.

### **7.1.3. Quy định của pháp luật Việt Nam về sản phẩm, dịch vụ về dữ liệu**

Trong bối cảnh chuyển đổi số, sản phẩm dữ liệu và dịch vụ dữ liệu đã trở thành đối tượng điều chỉnh của khung pháp lý Việt Nam nhằm bảo đảm vừa thúc đẩy đổi mới sáng tạo vừa quản lý chặt chẽ hoạt động khai thác dữ liệu. Luật Dữ liệu 2024 (Luật số 60/2024/QH15) cùng với Nghị định số 169/2025/NĐ-CP đã thiết lập nền tảng pháp lý toàn diện cho lĩnh vực này. Sau đây là nội dung trích dẫn các điều, khoản được quy định trong hai văn bản nói trên có liên quan đến sản phẩm, dịch vụ về dữ liệu, nhằm đưa ra góc nhìn khách quan, toàn diện và chính xác nhất khi phân tích, làm rõ.

**Thứ nhất**, trong Luật dữ liệu năm 2024, cụ thể tại Chương IV (Sản phẩm, dịch vụ về dữ liệu) gồm 05 điều (từ Điều 39 đến Điều 43), quy định về: **(1)** Sản phẩm, dịch vụ về dữ liệu; **(2)** sản phẩm, dịch vụ trung gian dữ liệu; **(3)** sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu; **(4)** sản dữ liệu; **(5)** trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu, sản dữ liệu.

#### **Điều 39. Sản phẩm, dịch vụ về dữ liệu**

1. Sản phẩm, dịch vụ về dữ liệu trong hoạt động trung gian dữ liệu, phân tích, tổng hợp dữ liệu, xác thực điện tử, sản dữ liệu thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Dịch vụ xác thực điện tử thực hiện việc xác thực dữ liệu trong các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống định danh và xác thực điện tử do đơn vị sự nghiệp công lập, doanh nghiệp nhà nước đáp ứng điều kiện cung cấp dịch vụ.





3. Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu được hưởng ưu đãi như các doanh nghiệp hoạt động trong lĩnh vực công nghệ cao, đổi mới sáng tạo, khởi nghiệp sáng tạo, công nghiệp công nghệ số.

4. Các sản phẩm, dịch vụ khác về dữ liệu trong hoạt động giao dịch điện tử, viễn thông, an ninh mạng, an toàn thông tin mạng, công nghiệp công nghệ số, cơ yếu, công nghiệp quốc phòng, an ninh và động viên công nghiệp thực hiện theo quy định của pháp luật có liên quan.

5. Chính phủ quy định chi tiết Điều này.

### **Điều 40. Sản phẩm, dịch vụ trung gian dữ liệu**

1. Sản phẩm, dịch vụ trung gian dữ liệu là sản phẩm, dịch vụ nhằm thiết lập mối quan hệ thương mại giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng sản phẩm, dịch vụ, thông qua thỏa thuận nhằm mục đích trao đổi, chia sẻ, truy cập dữ liệu, thực hiện các quyền của chủ thể dữ liệu, chủ sở hữu dữ liệu, người dùng dữ liệu.

2. Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu phải được đăng ký hoạt động và quản lý theo quy định của pháp luật về đầu tư; trừ trường hợp cung cấp sản phẩm, dịch vụ trung gian dữ liệu trong nội bộ tổ chức.

3. Chính phủ quy định chi tiết Điều này.

### **Điều 41. Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu**

1. Sản phẩm phân tích, tổng hợp dữ liệu là kết quả của quá trình phân tích, tổng hợp dữ liệu thành thông tin chuyên sâu hữu ích ở các cấp độ khác nhau theo yêu cầu của bên sử dụng sản phẩm. Dịch vụ phân tích, tổng hợp dữ liệu là hoạt động phân tích, tổng hợp dữ liệu theo yêu cầu của bên sử dụng dịch vụ.

2. Tổ chức kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có thể gây nguy hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã





*hội, đạo đức xã hội, sức khỏe của cộng đồng phải đăng ký hoạt động, quản lý theo quy định của pháp luật về đầu tư.*

*Trường hợp có kết nối, chia sẻ với cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành để kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu phải được quản lý theo quy định của pháp luật.*

*3. Chính phủ quy định chi tiết Điều này.*

#### **Điều 42. Sàn dữ liệu**

*1. Sàn dữ liệu là nền tảng cung cấp tài nguyên liên quan đến dữ liệu để phục vụ nghiên cứu, phát triển khởi nghiệp, đổi mới sáng tạo; cung cấp các sản phẩm, dịch vụ liên quan đến dữ liệu phục vụ phát triển kinh tế - xã hội; là môi trường để giao dịch, trao đổi dữ liệu và các sản phẩm, dịch vụ liên quan đến dữ liệu.*

*2. Tổ chức cung cấp dịch vụ sàn dữ liệu là đơn vị sự nghiệp công lập, doanh nghiệp nhà nước đáp ứng điều kiện cung cấp dịch vụ và được cấp phép thành lập theo quy định của pháp luật.*

*3. Dữ liệu không được phép giao dịch bao gồm:*

- a) Dữ liệu gây nguy hại đến quốc phòng, an ninh, đối ngoại, cơ yếu;*
- b) Dữ liệu không được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác;*
- c) Dữ liệu khác bị cấm giao dịch theo quy định của pháp luật.*

*4. Chính phủ quy định chi tiết Điều này.*

#### **Điều 43. Trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu, sàn dữ liệu**

*1. Cung cấp dịch vụ cho tổ chức, cá nhân trên cơ sở thỏa thuận bằng hợp đồng cung cấp dịch vụ.*





2. Bảo đảm kênh tiếp nhận thông tin và việc sử dụng dịch vụ thông suốt, liên tục.

3. Thực hiện quản lý, kiểm tra, giám sát an toàn dữ liệu, bảo mật dữ liệu thường xuyên; phòng ngừa, ngăn chặn và xử lý rủi ro dữ liệu; giám sát hành vi có thể ảnh hưởng đến việc bảo vệ dữ liệu.

4. Tuân thủ quy định của pháp luật về an toàn thông tin mạng, pháp luật về an ninh mạng, pháp luật về giao dịch điện tử và quy định khác của pháp luật có liên quan.

5. Chính phủ quy định chi tiết Điều này.

**Thứ hai**, 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 đã đưa ra những quy định tương đối cụ thể, chi tiết đối với **(1)** Sản phẩm, dịch vụ trung gian dữ liệu (từ Điều 23 đến Điều 26); **(2)** Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu (từ Điều 27 đến Điều 31); **(3)** Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu (từ Điều 32 đến Điều 35). Ngoài ra, Nghị định này cũng quy định về thẩm quyền, hồ sơ, trình tự, thủ tục cấp, cấp đổi, cấp lại, thu hồi Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sản dữ liệu, Giấy chứng nhận đủ điều kiện kinh doanh sản phẩm, dịch vụ trung gian dữ liệu, Giấy chứng nhận đủ điều kiện kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu, Giấy chứng nhận đủ điều kiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu (Chương VI) và trách nhiệm Quản lý nhà nước về hoạt động khoa học công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ về dữ liệu (Chương VII); tuy nhiên, trong phạm vi nghiên cứu, nhóm tác giả xin phép không đề cập đến nội dung này.





### **Chương III**

#### **SẢN PHẨM, DỊCH VỤ TRUNG GIAN DỮ LIỆU**

##### **Điều 23. Sản phẩm, dịch vụ trung gian dữ liệu**

1. Sản phẩm trung gian dữ liệu được tổ chức cung cấp sản phẩm, dịch vụ cung cấp hạ tầng, trang thiết bị, ứng dụng, phần mềm phục vụ chủ thể dữ liệu, chủ sở hữu dữ liệu thực hiện hoạt động quy định tại Điều 24 Nghị định này.

2. Dịch vụ trung gian dữ liệu được tổ chức cung cấp sản phẩm, dịch vụ cung cấp để phục vụ hoạt động trung gian dữ liệu kết nối, truyền dẫn, truy cập và xử lý dữ liệu điện tử giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng sản phẩm, dịch vụ về dữ liệu bảo đảm an toàn, hiệu quả và đúng định dạng.

3. Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu giữa bên sử dụng dịch vụ với cơ quan nhà nước được đăng ký quản lý và cấp phép theo quy định tại Nghị định này.

4. Sản phẩm, dịch vụ trung gian dữ liệu tại Nghị định này không bao gồm dịch vụ điện toán đám mây, dịch vụ trung tâm dữ liệu, việc cung cấp sản phẩm, dịch vụ trung gian dữ liệu trong nội bộ tổ chức và các sản phẩm, dịch vụ đã được quy định tại các văn bản quy phạm pháp luật khác.

##### **Điều 24. Nội dung hoạt động trung gian dữ liệu**

1. Đại diện cho chủ thể dữ liệu, chủ sở hữu dữ liệu để thực hiện kết nối, chia sẻ, trao đổi, truy cập dữ liệu với bên sử dụng dịch vụ.

2. Tư vấn, đánh giá tác động việc xử lý dữ liệu, việc cung cấp dịch vụ trung gian dữ liệu giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng dịch vụ dữ liệu.

3. Dịch vụ quản trị dữ liệu để ủy thác thay mặt cho chủ thể dữ liệu, chủ sở hữu dữ liệu để kết nối, chia sẻ, trao đổi, truy cập dữ liệu với bên sử dụng dữ liệu.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

4. Đại lý kết nối, chia sẻ, trao đổi, truy cập dữ liệu giữa bên chủ thể dữ liệu, chủ sở hữu dữ liệu với bên sử dụng dữ liệu.

5. Dịch vụ cung cấp hạ tầng, trang thiết bị, ứng dụng, phần mềm, dịch vụ truyền đưa và các loại hình khác để phục vụ hoạt động trung gian dữ liệu.

6. Dịch vụ hỗ trợ, kiểm soát các thuộc tính của dữ liệu bảo đảm quyền riêng tư, dữ liệu nhạy cảm, dữ liệu cá nhân, đánh giá rủi ro đối với hoạt động chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng theo quy định của pháp luật trong hoạt động trung gian dữ liệu.

7. Dịch vụ hợp tác, chia sẻ dữ liệu để phục vụ kết nối, chia sẻ, khai thác, truy cập dữ liệu theo quy định của pháp luật.

8. Thẩm định điều kiện tham gia sản dữ liệu của các chủ thể có liên quan; tính hợp pháp và việc đáp ứng điều kiện tham gia giao dịch của sản phẩm, dịch vụ dữ liệu; khả năng đáp ứng yêu cầu trong việc bảo đảm an ninh, an toàn khi sử dụng sản phẩm dữ liệu.

9. Các hoạt động khác thực hiện theo quy định hoạt động thử nghiệm có kiểm soát để đánh giá, phân tích bổ sung vào hoạt động trung gian dữ liệu.

**Điều 25. Điều kiện đối với tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu giữa bên sử dụng dịch vụ với cơ quan nhà nước**

1. Tổ chức quy định tại khoản 3 Điều 23 Nghị định này bao gồm đơn vị sự nghiệp, doanh nghiệp được thành lập và hoạt động theo pháp luật Việt Nam, đáp ứng các điều kiện quy định tại khoản 2, khoản 3, khoản 4 Điều này.

2. Điều kiện về nhân sự:

a) Người đứng đầu đơn vị sự nghiệp hoặc người đại diện theo pháp luật của doanh nghiệp là công dân Việt Nam, thường trú tại Việt Nam; có trình độ đại học trở lên, có ít nhất 03 năm kinh nghiệm công tác liên quan đến quản lý dữ liệu và không thuộc một trong các trường hợp quy định tại các điểm a, b và c khoản 1 Điều 9 Nghị định này;





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

b) Có ít nhất 05 người có trình độ đại học trở lên và có một trong những chứng chỉ, chứng nhận về khoa học dữ liệu, phân tích dữ liệu, quản lý, quản trị dữ liệu, tư vấn, môi giới, xúc tiến thương mại; quản trị tài sản; thẩm định dữ liệu.

3. Điều kiện về cơ sở vật chất, trang thiết bị kỹ thuật, quy trình quản lý cung cấp dịch vụ và phương án bảo đảm an ninh, trật tự.

Tổ chức đề nghị cấp Giấy chứng nhận đủ điều kiện kinh doanh sản phẩm, dịch vụ trung gian dữ liệu phải có hạ tầng, trang thiết bị sử dụng được đặt tại Việt Nam, được kiểm định an ninh an toàn thông tin theo quy định của pháp luật và có Đề án hoạt động cung cấp sản phẩm dịch vụ bao gồm các nội dung chính sau:

- a) Phương án, quy trình hoạt động cung cấp dịch vụ trung gian dữ liệu bao gồm thuyết minh hệ thống công nghệ thông tin;
- b) Phương án kỹ thuật về giải pháp công nghệ;
- c) Phương án lưu trữ, bảo đảm tính toàn vẹn dữ liệu, bảo đảm an ninh an toàn thông tin của hệ thống cung cấp dịch vụ;
- d) Phương án bảo vệ dữ liệu tổ chức, cá nhân;
- đ) Phương án bảo đảm an ninh, trật tự;
- e) Phương án về thanh toán;
- g) Phương án thẩm định dữ liệu;
- h) Phương án sử dụng dịch vụ về định danh và xác thực điện tử;
- i) Phương án phòng cháy và chữa cháy, dự phòng thảm họa và bảo đảm vận hành ổn định, thông suốt dịch vụ trung gian dữ liệu;
- k) Thuyết minh về trang thiết bị kỹ thuật được sử dụng.

4. Điều kiện về tài chính:





*Ký quỹ tại một ngân hàng thương mại hoạt động tại Việt Nam không dưới 05 tỷ đồng để giải quyết các rủi ro và các khoản đền bù có thể xảy ra trong quá trình cung cấp sản phẩm, dịch vụ do lỗi của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu và thanh toán chi phí tiếp nhận và duy trì cơ sở dữ liệu của tổ chức, doanh nghiệp trong trường hợp bị thu hồi giấy phép.*

## **Điều 26. Trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu**

- 1. Chứng minh trách nhiệm thông qua việc kết nối, chia sẻ, trao đổi, truy cập dữ liệu và bảo vệ dữ liệu, bảo vệ dữ liệu cá nhân theo quy định pháp luật.*
- 2. Thông báo cho tổ chức, cá nhân là chủ sở hữu dữ liệu, chủ thể dữ liệu, bên sử dụng dữ liệu về mục đích cung cấp sản phẩm, dịch vụ trung gian dữ liệu và đảm bảo các quyền của cá nhân theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.*
- 3. Việc thu thập, sử dụng hoặc tiết lộ dữ liệu cá nhân cho các mục đích hợp pháp và phải được chủ thể dữ liệu đồng ý.*
- 4. Bảo đảm dữ liệu chính xác, đầy đủ từ chủ thể dữ liệu, chủ sở hữu dữ liệu cung cấp cho bên sử dụng dịch vụ.*
- 5. Bảo đảm việc truy cập dữ liệu đúng mục đích, đúng đối tượng, khai thác đúng theo hợp đồng đã ký kết.*
- 6. Thực hiện các biện pháp bảo vệ, bảo mật hợp lý để bảo vệ dữ liệu cá nhân trong quyền sở hữu của tổ chức, bao gồm ngăn chặn truy cập, thu thập, sử dụng, tiết lộ trái phép hoặc các rủi ro tương tự.*
- 7. Giới hạn việc lưu trữ dữ liệu cá nhân trong thời gian cần thiết và xử lý thông tin cá nhân đúng cách khi không còn cần thiết cho mục đích kinh doanh hoặc pháp lý.*





8. Bảo đảm giới hạn chuyển giao dữ liệu cá nhân xuyên biên giới theo các yêu cầu của quy định, bảo đảm rằng tiêu chuẩn bảo vệ tương đương với tiêu chuẩn theo yêu cầu pháp luật có liên quan.

9. Thông báo vi phạm dữ liệu tới tổ chức, cá nhân bị ảnh hưởng ngay khi có thể nếu có vi phạm dữ liệu có khả năng gây ra tác hại đáng kể cho cá nhân hoặc có quy mô đáng kể.

10. Bảo đảm khả năng chuyển dữ liệu tới đúng bên sử dụng dữ liệu theo đúng thỏa thuận đã ký kết.

11. Bảo đảm khả năng tư vấn, đánh giá tác động việc xử lý dữ liệu, thẩm định dữ liệu, các hình thức thanh toán linh hoạt, quy định về thuế, phí, giá theo quy định của hoạt động thương mại điện tử.

12. Tổ chức tham gia hoạt động trung gian dữ liệu phải thực hiện việc xác thực danh tính theo quy định pháp luật về định danh và xác thực điện tử.

#### **Chương IV**

### **SẢN PHẨM, DỊCH VỤ PHÂN TÍCH, TỔNG HỢP DỮ LIỆU**

#### **Điều 27. Các cấp độ phân tích, tổng hợp dữ liệu**

1. Cấp độ 1: Việc phân tích, tổng hợp dữ liệu do con người trực tiếp thực hiện, sử dụng thiết bị, phần mềm không tích hợp trí tuệ nhân tạo.

2. Cấp độ 2: Việc phân tích, tổng hợp dữ liệu do con người trực tiếp thực hiện và có hỗ trợ một phần bởi trí tuệ nhân tạo.

3. Cấp độ 3: Việc phân tích, tổng hợp dữ liệu thực hiện hoàn toàn bởi trí tuệ nhân tạo, có sự giám sát của con người trong quá trình thực hiện.

4. Cấp độ 4: Việc phân tích, tổng hợp dữ liệu thực hiện hoàn toàn bởi trí tuệ nhân tạo, không có sự giám sát của con người.





**Điều 28. Quản lý sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu**

1. Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu sau đây phải được cấp Giấy chứng nhận đủ điều kiện kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu bao gồm:

a) Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu thuộc nhóm cấp độ 3, cấp độ 4 trong hệ thống thông tin của cơ quan nhà nước.

Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có thể gây nguy hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, sức khỏe của cộng đồng;

b) Cung cấp các sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có kết nối, chia sẻ với cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành;

c) Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có sử dụng dữ liệu cốt lõi, dữ liệu quan trọng.

2. Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu không thuộc khoản 1 Điều này gửi thông báo về Bộ Công an khi thực hiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu và được đề nghị Bộ Công an thẩm định, đánh giá để hưởng ưu đãi đối với sản phẩm, dịch vụ đó như các doanh nghiệp hoạt động trong lĩnh vực công nghệ cao, đổi mới sáng tạo, khởi nghiệp sáng tạo, công nghiệp công nghệ số; chính sách ưu đãi phát triển hoạt động khoa học, công nghệ và đổi mới sáng tạo về dữ liệu bao gồm:

a) Trợ lý ảo, hệ thống trí tuệ nhân tạo tạo sinh, hệ thống phân tích các nội dung tự động về video, hình ảnh, tin tức, bài viết và các sản phẩm, dịch vụ tương tự khác có tương tác trực tiếp đến bên sử dụng dịch vụ, có nguy cơ gợi ý, định hướng bên sử dụng dịch vụ đến các nội dung sai lệch;

b) Các sản phẩm, dịch vụ phân tích, tổng hợp các dữ liệu nhạy cảm của cá nhân có quy mô dữ liệu từ 01 triệu cá nhân trở lên;





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

c) Các sản phẩm, dịch vụ phân tích, tổng hợp cấp độ 3, cấp độ 4, thực hiện tự động trong các hệ thống công nghiệp, sản xuất chiếm 20% cơ cấu sử dụng trong ngành công nghiệp, sản xuất đó trở lên;

d) Đạt quy mô nhất định về dữ liệu phục vụ huấn luyện mô hình phân tích, tổng hợp dữ liệu 10 TB dữ liệu trở lên.

3. Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu tại Nghị định này không bao gồm việc cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu trong nội bộ tổ chức và các sản phẩm, dịch vụ đã được quy định tại các văn bản quy phạm pháp luật khác.



***Trợ lý ảo, tương lai cho hoạt động hành chính,  
dịch vụ công tại Việt Nam - Ảnh: CellphoneS***

**Điều 29. Điều kiện kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu**

*Tổ chức kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu phải đáp ứng các điều kiện sau:*





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

1. Là đơn vị sự nghiệp, doanh nghiệp được thành lập và hoạt động theo pháp luật Việt Nam.

2. Điều kiện về nhân sự

Người đứng đầu đơn vị sự nghiệp, người đại diện theo pháp luật của doanh nghiệp là công dân Việt Nam, thường trú tại Việt Nam; có trình độ đại học trở lên, có ít nhất 03 năm kinh nghiệm công tác liên quan đến quản lý dữ liệu và không thuộc một trong các trường hợp quy định tại các điểm a, b và c khoản 1 Điều 9 Nghị định này.

Có đội ngũ quản lý, điều hành đáp ứng được yêu cầu chuyên môn phân tích, tổng hợp dữ liệu; có cán bộ kỹ thuật chịu trách nhiệm chính có chứng chỉ, chứng nhận hoàn thành khóa học về một trong các chuyên môn sau: Khoa học dữ liệu, phân tích dữ liệu, quản lý, quản trị dữ liệu; thẩm định dữ liệu hoặc có tối thiểu 03 năm kinh nghiệm về: Khoa học dữ liệu, phân tích dữ liệu, quản lý, quản trị dữ liệu; thẩm định dữ liệu.

3. Có hệ thống trang thiết bị, cơ sở vật chất và công nghệ sản xuất phù hợp với phương án kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu.

4. Có phương án kinh doanh gồm các nội dung: Phạm vi đối tượng cung cấp sản phẩm, dịch vụ; loại hình sản phẩm dự kiến cung cấp; sự đáp ứng tiêu chuẩn, quy chuẩn kỹ thuật liên quan đối với từng loại sản phẩm, dịch vụ; các tính năng kỹ thuật cơ bản của sản phẩm, dịch vụ.

### **Điều 30. Các tiêu chí thẩm định sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu**

1. Thẩm định nguồn dữ liệu để phân tích, tổng hợp đúng quy định của pháp luật.

2. Thẩm định mô hình, công thức phân tích, tổng hợp dữ liệu không tác động, định hướng người dùng ảnh hưởng đến an ninh, quốc phòng, trật tự an





*toàn xã hội, an toàn của các hệ thống công nghiệp, hệ thống thông tin quan trọng quốc gia, sức khỏe cộng đồng, giao thông, môi trường, tư pháp, công cộng.*

*3. Thẩm định về độ chính xác của mô hình phân tích, tổng hợp dữ liệu.*

### **Điều 31. Trách nhiệm của tổ chức kinh doanh, cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu**

*1. Cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu cho tổ chức, cá nhân trên cơ sở thỏa thuận bằng hợp đồng cung cấp sản phẩm, dịch vụ theo quy định; chịu trách nhiệm về sản phẩm, dịch vụ cung cấp.*

*2. Trong quá trình cung cấp sản phẩm hoặc dịch vụ phân tích, tổng hợp dữ liệu bên cung cấp sản phẩm, dịch vụ phải cung cấp và bảo đảm bên sử dụng nắm bắt rõ các nội dung sau:*

*a) Tên, thông tin liên hệ và cách thức tiếp cận thông tin liên quan của bên cung cấp sản phẩm, dịch vụ;*

*b) Chức năng, mục đích, phạm vi sử dụng và cơ chế vận hành của sản phẩm, dịch vụ;*

*c) Tác động, rủi ro có thể ảnh hưởng đến quyền và lợi ích của bên sử dụng dịch vụ;*

*d) Thông tin về Giấy chứng nhận đủ điều kiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu hoặc Giấy chứng nhận đủ điều kiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu;*

*đ) Quyền và nghĩa vụ bên sử dụng dịch vụ.*

*3. Tuân thủ các quy định của pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng, an ninh mạng, an ninh dữ liệu, giao dịch điện tử, tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu, bảo mật thông tin, bảo đảm tính chính xác của việc cung cấp dịch vụ; ban hành quy trình hoạt động kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu và được sự đồng ý của cơ quan quản lý nhà nước về dữ liệu.*





# **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

4. Tuân thủ phương án, quy trình hoạt động kinh doanh sản phẩm, dịch vụ đã được phê duyệt.

5. Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu quy định tại Điều 28 Nghị định này phải gửi báo cáo định kỳ về việc cung cấp sản phẩm, dịch vụ theo mẫu BC01 tại Phụ lục ban hành kèm theo Nghị định này cho Bộ Công an (qua Trung tâm dữ liệu quốc gia) trước ngày 20 tháng 12 hằng năm (số liệu báo cáo tính từ ngày 15 tháng 12 năm trước đến hết ngày 14 tháng 12 năm báo cáo) hoặc báo cáo đột xuất khi được yêu cầu (nộp trực tiếp hoặc qua dịch vụ bưu chính hoặc phương thức trực tuyến).

## **Chương V**

### **SÀN DỮ LIỆU**

#### **Điều 32. Hoạt động của sàn dữ liệu**

*Hoạt động của sàn dữ liệu bao gồm:*

1. *Cung cấp tài nguyên liên quan đến dữ liệu để phục vụ nghiên cứu, phát triển khởi nghiệp, đổi mới sáng tạo; cung cấp các dịch vụ liên quan đến dữ liệu phục vụ phát triển kinh tế xã hội:*

- a) Dữ liệu trong cơ sở dữ liệu chuyên ngành, Cơ sở dữ liệu quốc gia;*
- b) Dữ liệu do cơ quan, tổ chức, cá nhân khác cung cấp.*

2. *Cung cấp dịch vụ:*

*a) Dịch vụ chào mua, chào bán, giới thiệu, đại diện, đại lý, tư vấn, môi giới, hỗ trợ định giá, hỗ trợ kỹ thuật, hỗ trợ đàm phán, ký kết giao dịch dữ liệu, sản phẩm, dịch vụ về dữ liệu;*

*b) Dịch vụ đấu giá dữ liệu;*

*c) Dịch vụ cung cấp môi trường để giao dịch, trao đổi dữ liệu và các sản phẩm, dịch vụ liên quan đến dữ liệu.*

**Điều 33. Cung cấp sản phẩm, dịch vụ dữ liệu lên sàn dữ liệu để giao dịch**





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

1. Các sản phẩm, dịch vụ dữ liệu của tổ chức, cá nhân trên sàn dữ liệu hoạt động theo cơ chế thị trường, được hỗ trợ định giá bởi tổ chức cung cấp dịch vụ sàn dữ liệu hoặc các tổ chức khác có chức năng định giá theo nhu cầu.

2. Cơ quan nhà nước cung cấp sản phẩm, dịch vụ dữ liệu thu phí/giá theo quy định pháp luật; lựa chọn sàn dữ liệu để cung cấp sản phẩm, dịch vụ; tổ chức đấu giá dữ liệu với giá khởi điểm không thấp hơn phí đầu vào cho sản phẩm, dịch vụ dữ liệu.

3. Các sản phẩm, dịch vụ dữ liệu trên sàn dữ liệu bảo đảm xác thực nguồn gốc dữ liệu; tổ chức cung cấp dịch vụ sàn dữ liệu hoặc tổ chức khác có chức năng xác thực nguồn gốc dữ liệu có trách nhiệm thực hiện xác thực nguồn gốc dữ liệu.

4. Tổ chức, cá nhân chịu trách nhiệm về sản phẩm, dịch vụ cung cấp lên sàn dữ liệu; tổ chức cung cấp dịch vụ sàn dữ liệu có trách nhiệm thẩm định các sản phẩm, dịch vụ dữ liệu bảo đảm tuân thủ theo quy định pháp luật.

5. Các cơ quan, tổ chức, doanh nghiệp cung cấp sản phẩm, dịch vụ về dữ liệu phải thực hiện thông qua sàn dữ liệu trừ các trường hợp pháp luật có quy định khác.

6. Dữ liệu không được phép giao dịch bao gồm:

- a) Dữ liệu thuộc danh mục dữ liệu cốt lõi, dữ liệu quan trọng;
- b) Dữ liệu không được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác;
- c) Dữ liệu khác bị cấm giao dịch theo quy định của pháp luật.

**Điều 34. Điều kiện cấp Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn dữ liệu**

*Tổ chức cung cấp hoạt động sàn dữ liệu phải đáp ứng các điều kiện sau:*





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

1. Là đơn vị sự nghiệp công lập, doanh nghiệp nhà nước được thành lập và hoạt động theo pháp luật Việt Nam, đáp ứng các điều kiện quy định tại khoản 2, khoản 3, khoản 4 Điều này.

### 2. Điều kiện về nhân sự

a) Người đứng đầu tổ chức, người đại diện theo pháp luật của doanh nghiệp có trình độ đại học trở lên, trực tiếp hoạt động quản lý tại các trung tâm dữ liệu, có ít nhất 03 năm kinh nghiệm công tác liên quan đến quản lý dữ liệu và không thuộc một trong các trường hợp quy định tại các điểm a, b và c khoản 1 Điều 9 Nghị định này;

b) Có ít nhất 05 người có trình độ đại học trở lên, trong đó có ít nhất 40% làm việc chính thức, 30% có chứng chỉ, chứng nhận hoàn thành khóa học về: khoa học dữ liệu, phân tích dữ liệu, quản lý, quản trị dữ liệu, tư vấn, môi giới, xúc tiến thương mại; quản trị tài sản; thẩm định dữ liệu.

3. Điều kiện về cơ sở vật chất, trang thiết bị kỹ thuật, quy trình quản lý cung cấp dịch vụ và phương án bảo đảm an ninh, trật tự

Có hạ tầng, trang thiết bị sử dụng được đặt tại Việt Nam, được kiểm định an ninh an toàn thông tin theo quy định của pháp luật và có Đề án hoạt động sản dữ liệu bao gồm các nội dung chính sau:

a) Phương án, quy trình hoạt động sản dữ liệu bao gồm thuyết minh hệ thống công nghệ thông tin;

b) Phương án kỹ thuật về giải pháp công nghệ;

c) Phương án lưu trữ, bảo đảm tính toàn vẹn dữ liệu, bảo đảm an ninh, an toàn thông tin của hệ thống cung cấp dịch vụ;

d) Phương án bảo vệ dữ liệu tổ chức, cá nhân;

đ) Phương án bảo đảm an ninh, trật tự;

e) Phương án về thanh toán;





- g) Phương án thẩm định dữ liệu;
- h) Phương án sử dụng dịch vụ về định danh và xác thực điện tử;
- i) Phương án phòng cháy và chữa cháy, dự phòng thảm họa và bảo đảm vận hành ổn định, thông suốt;

k) Thuyết minh về trang thiết bị kỹ thuật được sử dụng.

4. Trường hợp tổ chức hoạt động đấu giá dữ liệu thì tổ chức cung cấp dịch vụ sàn dữ liệu phải có giấy phép cung cấp dịch vụ đấu giá tài sản theo quy định của pháp luật.

### **Điều 35. Trách nhiệm của tổ chức cung cấp dịch vụ sàn dữ liệu**

1. Kiểm tra, đánh giá việc đáp ứng điều kiện tham gia sàn dữ liệu của các chủ thể có liên quan; tính hợp pháp và việc đáp ứng điều kiện tham gia giao dịch của sản phẩm, dịch vụ dữ liệu; khả năng đáp ứng yêu cầu trong việc bảo đảm an ninh, an toàn khi sử dụng sản phẩm dữ liệu, cụ thể như sau:

a) Điều kiện tham gia giao dịch của các chủ thể có liên quan gồm: Năng lực hành vi dân sự của cá nhân; năng lực pháp luật dân sự của pháp nhân;

b) Tính hợp pháp và việc đáp ứng điều kiện tham gia giao dịch của sản phẩm, dịch vụ dữ liệu gồm: Nguồn tạo ra sản phẩm, dịch vụ; đối tượng, nội dung, phương pháp, quy trình tạo ra sản phẩm, dịch vụ; xác định các yêu cầu liên quan đến hạn chế hoặc không hạn chế trong lưu thông, lưu hành sản phẩm, dịch vụ;

c) Đáp ứng yêu cầu bảo đảm an ninh, an toàn khi sử dụng sản phẩm dữ liệu gồm: tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật đối với sản phẩm, dịch vụ dữ liệu; việc tiếp nhận, lưu trữ và xử lý dữ liệu.

2. Giám sát hoạt động trên sàn dữ liệu, quyết định đình chỉ tham gia của các bên, tiếp tục niêm yết và chấm dứt niêm yết các sản phẩm, dịch vụ dữ liệu; giải quyết tranh chấp; giám sát, kịp thời phát hiện, xử lý, ngăn chặn,





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

*báo cáo các vi phạm pháp luật; phối hợp với các cơ quan quản lý nhà nước có liên quan trong việc kiểm tra, điều tra và thu thập chứng cứ.*

*3. Ban hành quy chế hoạt động và công khai niêm yết trên trang thông tin điện tử của mình. Quy chế hoạt động phải bao gồm các nội dung chính:*

- a) Điều kiện tham gia và trách nhiệm các bên tham gia sàn;*
- b) Quy trình giao dịch;*
- c) Yêu cầu về việc bảo đảm bí mật thông tin, chống hành vi gian lận;*
- d) Quản lý rủi ro, xử lý khiếu nại tranh chấp, bảo vệ dữ liệu cá nhân;*
- đ) Điều kiện về sản phẩm, dịch vụ về dữ liệu được đưa lên sàn dữ liệu.*

*4. Thiết lập hệ thống bảo đảm an toàn giao dịch dữ liệu theo quy định của pháp luật; hướng dẫn các bên tham gia trên sàn thực hiện bảo vệ dữ liệu, truy xuất nguồn gốc, xác định rủi ro, kiểm tra tuân thủ và sử dụng các biện pháp hiệu quả để bảo vệ dữ liệu cá nhân, quyền riêng tư cá nhân, bí mật thương mại, và dữ liệu quan trọng theo quy định của nhà nước.*

*5. Xây dựng kế hoạch ứng phó khẩn cấp đối với các sự cố an toàn dữ liệu, tiến hành sao lưu khôi phục thảm họa của các hệ thống và cơ sở dữ liệu quan trọng và định kỳ thực hiện các cuộc diễn tập khẩn cấp về an toàn dữ liệu, tăng khả năng ứng phó với các sự cố an toàn dữ liệu; bảo đảm kênh tiếp nhận thông tin và việc sử dụng dịch vụ liên tục 24 giờ trong ngày và 07 ngày trong tuần; tuân thủ phương án, quy trình hoạt động đã được phê duyệt.*

*6. Xây dựng bộ thông số kỹ thuật để đánh giá và quản lý chất lượng sản phẩm, dịch vụ dữ liệu, hệ thống chỉ số đánh giá tài sản dữ liệu, hỗ trợ định giá sản phẩm, dịch vụ dữ liệu.*

*7. Gửi báo cáo định kỳ 06 tháng trước ngày 20 tháng 6 (số liệu báo cáo tính từ ngày 15 tháng 12 năm trước đến hết ngày 14 tháng 6 năm báo cáo), định kỳ 01 năm trước ngày 20 tháng 12 (số liệu báo cáo tính từ ngày 15 tháng*





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

12 năm trước đến hết ngày 14 tháng 12 năm báo cáo) hoặc khi có yêu cầu về việc cung cấp dịch vụ sản dữ liệu theo mẫu BC02 tại Phụ lục ban hành kèm theo Nghị định này cho Bộ Công an (qua Trung tâm dữ liệu quốc gia).

Trên đây là **nội dung trích dẫn các điều, khoản có liên quan đến sản phẩm, dịch vụ về dữ liệu** được quy định trong Luật dữ liệu năm 2025 và 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.

### **7.1.4. Một số điểm đáng chú ý trong các quy định của pháp luật Việt Nam về sản phẩm, dịch vụ về dữ liệu**

#### **7.1.4.1. Về một số khái niệm**

Luật Dữ liệu năm 2024 đã quy định về các sản phẩm, dịch vụ về dữ liệu và giao Chính phủ quy định chi tiết để quản lý đối với tổ chức cung cấp sản phẩm, dịch vụ liên quan đến dữ liệu. Việc quản lý, phát triển các sản phẩm, dịch vụ mới về dữ liệu sẽ góp phần thiết lập thị trường dữ liệu, thúc đẩy chuyển đổi số trong các ngành, các lĩnh vực của nền kinh tế, chuyển đổi phương thức giao tiếp giữa cơ quan nhà nước với tổ chức, cá nhân và các quan hệ xã hội trên môi trường số.

Tuy nhiên, các văn bản quy phạm pháp luật hiện hành nói chung, Luật dữ liệu năm 2024 nói riêng vẫn chưa đưa ra được các khái niệm pháp lý đối với “sản phẩm dữ liệu” và “dịch vụ dữ liệu” một cách cụ thể, chi tiết và rõ ràng. Chỉ duy nhất trong Nghị định số 169/2025/NĐ-CP có đề cập: “*Sản phẩm, dịch vụ về dữ liệu là sản phẩm, dịch vụ được tạo thành từ dữ liệu hoặc sử dụng dữ liệu là nguồn tài nguyên chính để phát triển, ứng dụng, giao dịch*”, nhưng vẫn chưa thật sự làm rõ các khái niệm này như đã phân tích ở trên, qua đó gây khó khăn trong việc tiếp cận, sử dụng và khai thác có hiệu quả, phục vụ phát triển nền kinh tế số.





#### 7.1.4.2. Về sản phẩm, dịch vụ trung gian dữ liệu

Trong hệ sinh thái dữ liệu hiện đại, sản phẩm và dịch vụ trung gian dữ liệu đóng vai trò hết sức quan trọng trong việc kết nối giữa các chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng. Luật Dữ liệu năm 2024 định nghĩa: “Sản phẩm, dịch vụ trung gian dữ liệu là sản phẩm, dịch vụ nhằm thiết lập mối quan hệ thương mại giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng sản phẩm, dịch vụ, thông qua thỏa thuận nhằm mục đích trao đổi, chia sẻ, truy cập dữ liệu, thực hiện các quyền của chủ thể dữ liệu, chủ sở hữu dữ liệu, người dùng dữ liệu”. Tổ chức cung cấp các sản phẩm, dịch vụ trung gian dữ liệu phải đăng ký hoạt động và chịu sự quản lý theo quy định của pháp luật về đầu tư, trừ trường hợp cung cấp trong nội bộ tổ chức.



*Sản phẩm, dịch vụ trung gian dữ liệu là khái niệm lần đầu tiên được đề cập - Ảnh: Internet*





## *- Vai trò của sản phẩm, dịch vụ trung gian dữ liệu trong kỷ nguyên số hiện nay*

Trong kỷ nguyên số hiện nay, với sự bùng nổ của kết nối và dữ liệu, các sản phẩm và dịch vụ trung gian dữ liệu giữ vai trò như một cầu nối quan trọng, giúp luồng dữ liệu lưu chuyển liên thông và hiệu quả giữa các hệ thống khác nhau. Thay vì mỗi cặp hệ thống phải kết nối trực tiếp với nhau (dễ dẫn đến mạng lưới chằng chịt, phức tạp), giải pháp trung gian tạo một đầu mối tập trung để tiếp nhận, chuyển đổi và phân phối dữ liệu. Nhờ đó, các ứng dụng, cơ sở dữ liệu và hệ thống thông tin trong cơ quan, tổ chức, doanh nghiệp có thể tích hợp và tương tác liền mạch mà không cần quá nhiều kết nối tùy chỉnh riêng lẻ.

Đáng chú ý, trung gian dữ liệu có khả năng chuyên đổi định dạng dữ liệu giữa các hệ thống, đảm bảo dữ liệu gửi đi được biến đổi phù hợp với yêu cầu của hệ thống nhận. Quá trình này giúp thông tin được truyền tải chính xác và an toàn, hạn chế lỗi do không tương thích định dạng. Chẳng hạn, một nền tảng tích hợp có thể tự động chuyển đổi dữ liệu từ định dạng của hệ thống ERP sang định dạng phù hợp với ứng dụng CRM, giúp hai hệ thống này chia sẻ thông tin trơn tru mà không cần can thiệp thủ công<sup>21</sup>. Việc sử dụng dịch vụ trung gian dữ liệu giúp giảm bớt độ phức tạp so với việc xây dựng kết nối trực tiếp giữa từng cặp hệ thống. Các tổ chức có thể dựa vào một nền tảng tích hợp tiêu chuẩn hóa do bên trung gian cung cấp, thay vì phải lập trình kết nối cho từng hệ thống một. Điều này tiết kiệm chi phí và giảm rủi ro bởi các giải pháp trung gian thường đã được kiểm thử, tối ưu, và cập nhật thường xuyên, giúp hạn chế sự cố do kết nối tùy biến thủ công gây ra.

<sup>21</sup> CRMVIET (2024), *Tích hợp CRM ERP: Hướng dẫn chi tiết*, <https://crmviet.vn/tich-hop-crm-erp-huong-dan-chi-tiet/>, truy cập ngày 10/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



### ***Tương quan hệ thống CRM và ERP - Ảnh: Internet***

Bên cạnh vai trò tích hợp, bảo mật và quản lý dữ liệu cũng là một chức năng then chốt của các sản phẩm, dịch vụ trung gian dữ liệu. Các giải pháp này thường được trang bị tính năng bảo mật nâng cao như mã hóa dữ liệu, xác thực quyền truy cập và giám sát hoạt động bất thường. Nhờ đó, dữ liệu được bảo vệ khỏi truy cập trái phép và đảm bảo tính toàn vẹn trên suốt hành trình di chuyển của nó. Chẳng hạn, công nghệ mã hóa đầu cuối giúp dữ liệu không thể bị sửa đổi trên đường truyền, phòng ngừa nguy cơ gian lận hoặc rò rỉ thông tin.

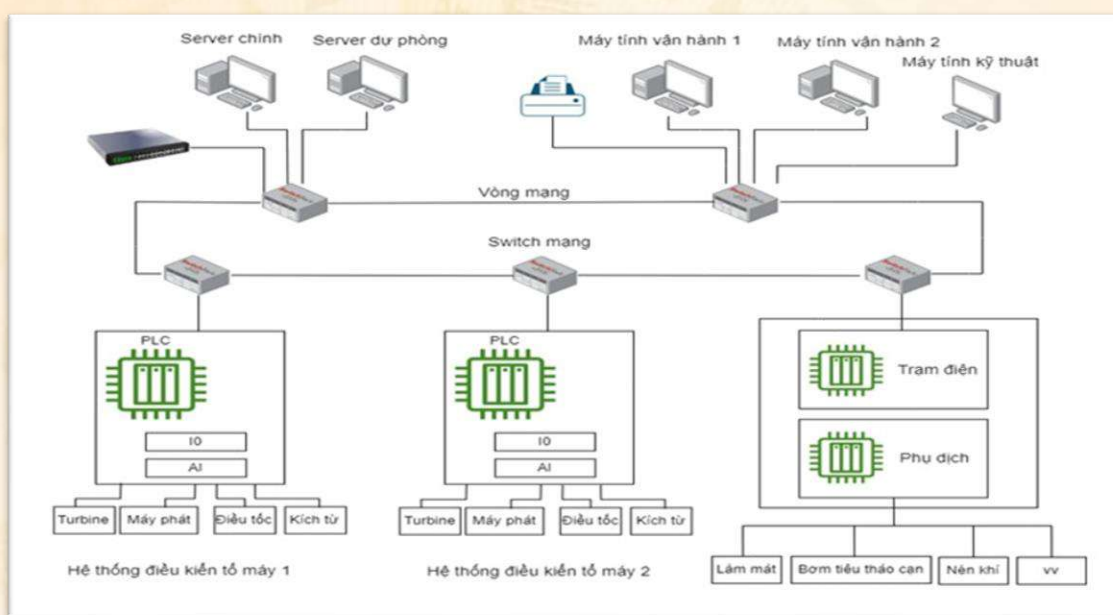
Ngoài ra, trung gian dữ liệu còn giúp các tổ chức đáp ứng yêu cầu pháp lý và quyền riêng tư trong quá trình chia sẻ thông tin. Thông qua hợp đồng và thỏa thuận rõ ràng, bên trung gian có thể đảm bảo các quyền của chủ thể dữ liệu được tôn trọng, dữ liệu chỉ được sử dụng cho mục đích hợp pháp và các bên liên quan đều được bảo vệ quyền lợi. Ví dụ, trong lĩnh vực năng lượng, đã có trường hợp các bên trung gian dữ liệu đứng ra thu thập dữ liệu





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

tiêu thụ điện của người dùng và chia sẻ cho đơn vị dịch vụ tài chính để phân tích, nhưng vẫn tuân thủ các biện pháp ẩn danh và bảo mật nhằm bảo vệ quyền riêng tư của khách hàng. Những “*cầu nối trung gian*” đó giúp khai thác giá trị dữ liệu một cách hiệu quả, đồng thời giữ vững niềm tin và tuân thủ các chuẩn mực về an toàn thông tin.



***Hệ thống điều khiển nhà máy thủy điện - Ảnh: Tạp chí Công Thương***

***- Sản phẩm, dịch vụ trung gian dữ liệu được quy định như thế nào kể từ ngày 01/7/2025?***

Tại Việt Nam, khung pháp lý cho sản phẩm, dịch vụ trung gian dữ liệu đã được quy định rõ ràng trong Luật Dữ liệu năm 2024 (có hiệu lực từ ngày 01/7/2025). Cụ thể, Điều 40 của luật này định nghĩa sản phẩm, dịch vụ trung gian dữ liệu là những sản phẩm, dịch vụ nhằm thiết lập mối quan hệ thương mại giữa các bên liên quan đến dữ liệu, bao gồm *chủ thể dữ liệu*, *chủ sở hữu dữ liệu* và *bên sử dụng dữ liệu*. Sự kết nối này được thực hiện thông qua các thỏa thuận, với mục tiêu tạo điều kiện thuận lợi cho việc trao đổi, chia sẻ và truy cập dữ liệu, cũng như giúp các bên thực thi quyền đối với dữ liệu của





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

mình. Nói cách khác, trung gian dữ liệu đóng vai trò như *nhà môi giới dữ liệu*, đứng giữa để dàn xếp việc giao dịch dữ liệu giữa bên có dữ liệu và bên cần dữ liệu trên cơ sở hợp đồng thương mại.

Bên cạnh định nghĩa, pháp luật cũng đặt ra yêu cầu quản lý đối với các tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu. Theo Điều 40 Luật Dữ liệu 2024, các tổ chức kinh doanh dịch vụ trung gian dữ liệu phải đăng ký hoạt động và chịu sự quản lý theo quy định của pháp luật về đầu tư. Điều này có nghĩa là doanh nghiệp muốn cung cấp dịch vụ môi giới, kết nối dữ liệu cần được cơ quan có thẩm quyền cấp phép tương tự như các ngành nghề đầu tư kinh doanh có điều kiện. Ngoại lệ duy nhất là trường hợp dịch vụ trung gian dữ liệu được triển khai *nội bộ trong một tổ chức* không bắt buộc đăng ký như một ngành kinh doanh độc lập. Quy định này nhằm bảo đảm rằng các hoạt động trung gian dữ liệu diễn ra minh bạch, có sự giám sát của Nhà nước, qua đó bảo vệ tốt hơn quyền lợi của các bên tham gia thị trường dữ liệu.

Nhìn rộng hơn, việc luật hóa hoạt động trung gian dữ liệu cho thấy Việt Nam đã chính thức công nhận dữ liệu là một loại hàng hóa, dịch vụ có thể kinh doanh một cách hợp pháp. Cùng với trung gian dữ liệu, Luật Dữ liệu 2024 còn định danh và điều chỉnh các mô hình kinh doanh dữ liệu khác như dịch vụ phân tích, tổng hợp dữ liệu (Điều 41) và sàn dữ liệu (Điều 42). Đây là những bước đi pháp lý quan trọng nhằm hình thành thị trường dữ liệu minh bạch, an toàn và hiệu quả tại Việt Nam, hòa nhịp với xu hướng chung trên thế giới.

*- Bàn về sự phát triển của sản phẩm, dịch vụ trung gian dữ liệu trong tương lai*

Trong tương lai, cùng với sự tiến bộ không ngừng của công nghệ, các sản phẩm và dịch vụ trung gian dữ liệu dự kiến sẽ có những bước phát triển

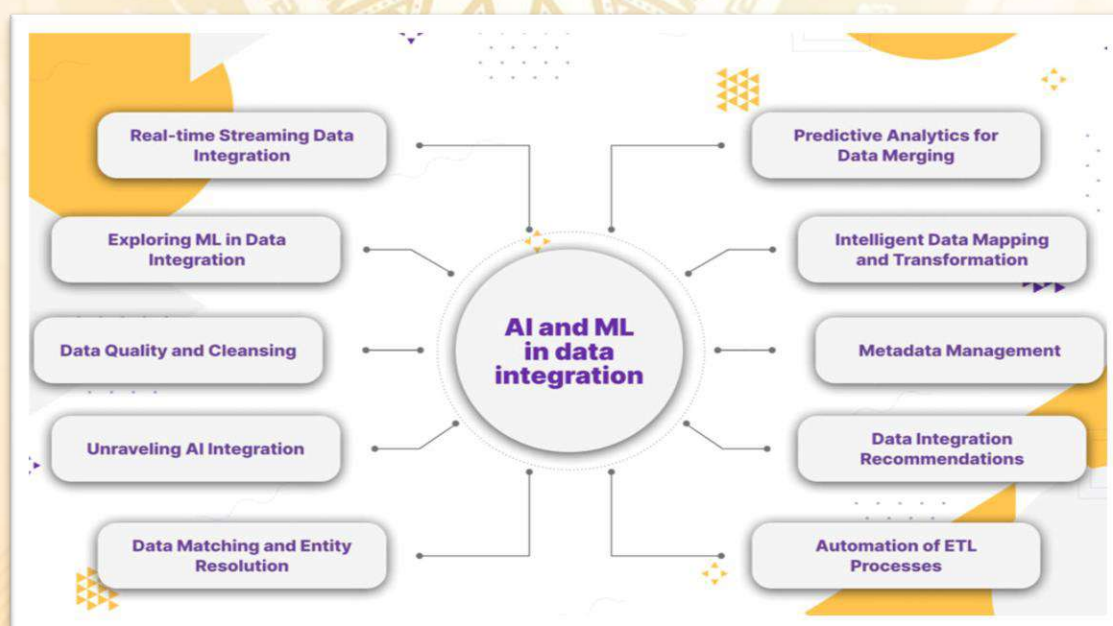




## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

**đột phá**, mang lại nhiều cơ hội mới cho doanh nghiệp trong tối ưu hóa chuỗi giá trị dữ liệu của mình. Dưới đây là một số xu hướng chính:

+ **Tích hợp Trí tuệ Nhân tạo (AI) và Học máy (ML):** AI/ML đang và sẽ được đưa vào các nền tảng trung gian dữ liệu nhằm nâng cao mức độ tự động hóa và tối ưu hóa quy trình xử lý. Nhờ khả năng học hỏi từ dữ liệu và phát hiện quy luật, AI có thể tự động phát hiện các sự cố dữ liệu (ví dụ: dữ liệu trùng lặp, ngoại lệ, giá trị thiếu) và sửa chữa chúng ngay lập tức. Việc này giúp giảm bớt nhu cầu kiểm tra thủ công, đồng thời tăng độ chính xác và tốc độ xử lý dữ liệu. Chẳng hạn, các công cụ AI hiện nay có thể theo dõi luồng dữ liệu theo thời gian thực, phát hiện những điểm bất thường và làm sạch dữ liệu một cách tự động, giúp thông tin luôn đúng đắn, kịp thời cho các hệ thống sử dụng. Không chỉ dừng ở đó, AI còn hỗ trợ tối ưu hóa luồng dữ liệu: hệ thống có thể tự đề xuất các cải tiến trong việc chuyển đổi, luân chuyển dữ liệu dựa trên phân tích lịch sử hoạt động, nhờ đó dòng chảy dữ liệu trở nên thông suốt và hiệu quả hơn.



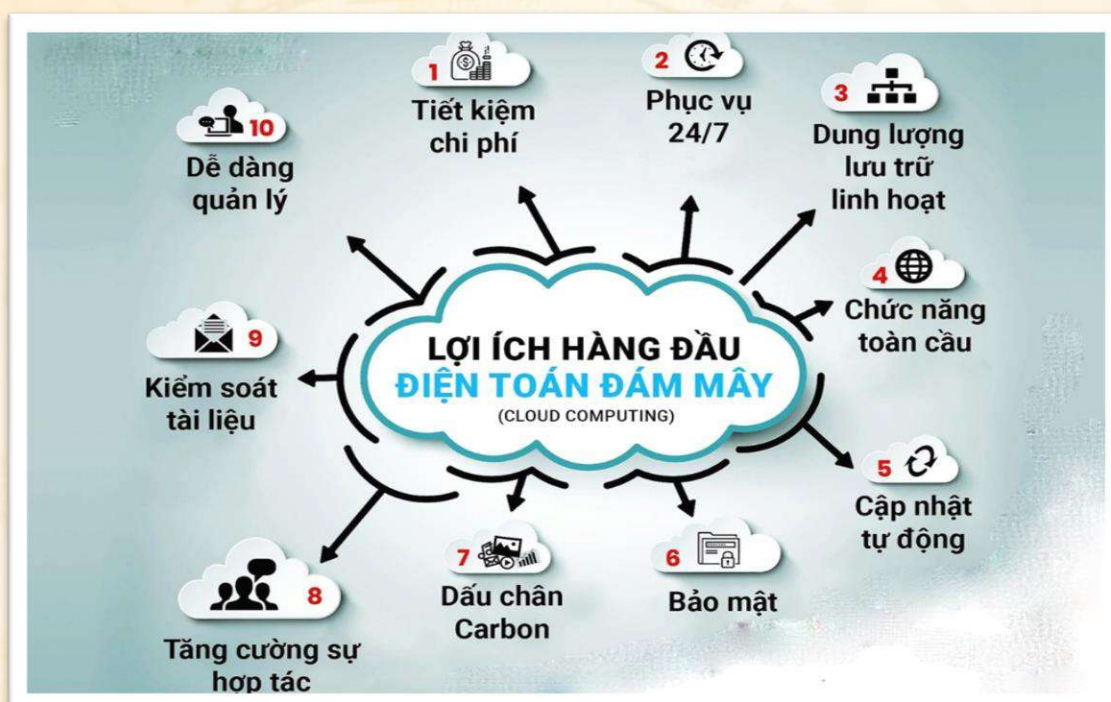
**Trí tuệ nhân tạo và học máy trong tích hợp dữ liệu - Ảnh: Internet**





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Ứng dụng mạnh mẽ của Điện toán Đám mây:** Điện toán đám mây (cloud) được dự báo sẽ tiếp tục là nền tảng lưu trữ và xử lý dữ liệu chủ chốt cho các dịch vụ trung gian. Xu hướng chuyển các hệ thống tích hợp lên đám mây mang lại khả năng mở rộng linh hoạt (tài nguyên có thể tăng giảm theo nhu cầu một cách nhanh chóng) và giúp cơ quan, tổ chức, doanh nghiệp tiết kiệm chi phí đầu tư hạ tầng ban đầu.



**Ứng dụng điện toán đám mây sâu hơn sẽ giúp  
tăng tốc quá trình chuyển đổi số - Ảnh: Internet**

Các nền tảng trung gian dữ liệu dựa trên đám mây (như mô hình *Integration Platform as a Service - iPaaS*) cho phép doanh nghiệp khởi tạo và quản lý các luồng tích hợp trên phạm vi rộng mà không cần lo lắng về việc nâng cấp máy chủ hay bảo trì hệ thống vật lý. Quản lý dữ liệu tập trung trên đám mây cũng giúp việc giám sát, bảo mật và sao lưu dữ liệu thuận tiện hơn, đặc biệt khi kết hợp với các dịch vụ quản trị dữ liệu do nhà cung cấp đám mây hỗ trợ. Một nghiên cứu thực tế cho thấy, việc chủ động tính toán khả năng mở





rộng ngay khi thiết kế hệ thống thông qua nâng cấp hạ tầng hoặc triển khai giải pháp đám mây sẽ giúp quy trình tích hợp sẵn sàng đáp ứng khối lượng dữ liệu tăng lên mà không gặp nút thắt cổ chai<sup>22</sup>. Vì vậy, trong tương lai, điện toán đám mây gần như sẽ là lựa chọn mặc định cho các dịch vụ trung gian dữ liệu muốn vươn tới quy mô lớn và phạm vi triển khai toàn cầu.

+ **Bảo mật và minh bạch dữ liệu nhờ Blockchain:** Công nghệ chuỗi khối (*blockchain*) được xem là một đột phá lớn trong việc đảm bảo tính bảo mật và minh bạch cho các giao dịch dữ liệu qua trung gian. Blockchain hoạt động dựa trên “sổ cái phân tán”, trong đó mọi giao dịch dữ liệu đều được ghi lại thành từng “khối” và liên kết với nhau một cách bất biến. Một khi dữ liệu đã được ghi vào chuỗi khối, không ai có thể tự ý thay đổi nếu không có sự đồng thuận của mạng lưới, giúp ngăn chặn các hành vi giả mạo hoặc chỉnh sửa trái phép dữ liệu<sup>23</sup>. Đồng thời, blockchain sử dụng các thuật toán mã hóa mạnh mẽ để bảo vệ dữ liệu, khiến kẻ xấu không thể đọc hiểu thông tin ngay cả khi đánh cắp được dữ liệu đó. Bên cạnh tính an toàn, blockchain còn mang lại tính minh bạch cao: mọi giao dịch chia sẻ dữ liệu giữa các bên đều được ghi dấu thời gian và lưu vết vĩnh viễn, cho phép tất cả thành viên liên quan có thể kiểm chứng lịch sử giao dịch một cách rõ ràng. Điều này rất hữu ích trong các ngành đòi hỏi sự tin cậy, như chuỗi cung ứng hoặc dịch vụ tài chính, nơi mà blockchain giúp các bên theo dõi luồng dữ liệu và loại bỏ gần như hoàn toàn cơ hội gian lận. Trong tương lai, sự kết hợp giữa trung gian dữ liệu truyền thống với blockchain sẽ tạo ra môi trường trao đổi dữ liệu vừa linh hoạt vừa an toàn, thúc đẩy niềm tin giữa các bên tham gia.

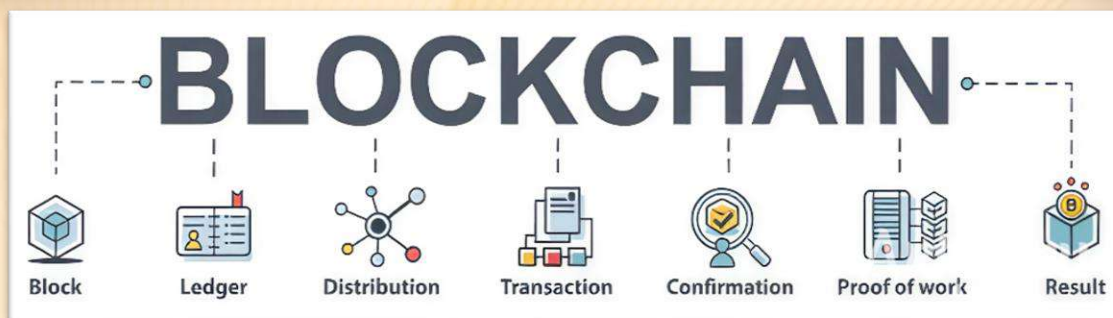
<sup>22</sup> Perfect Data Entry (2024), “Benefits of Cloud-Based Data Integration Tools”, <https://www.perfectdataentry.com/cloud-data-integration>, truy cập ngày 05/08/2025.

<sup>23</sup> IBM (2022), *What is Blockchain Technology?*, <https://www.ibm.com/topics/what-is-blockchain>, truy cập ngày 5/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



### **Blockchain - Giải pháp bảo mật cho hệ thống IoT - Ảnh: ICA Tech**

#### **- Lợi ích của sản phẩm, dịch vụ trung gian dữ liệu**

Việc triển khai các sản phẩm và dịch vụ trung gian dữ liệu mang lại nhiều lợi ích thiết thực từ khâu vận hành nội bộ cho đến tương tác với khách hàng, trung gian dữ liệu giúp nâng cao hiệu quả và độ tin cậy trong quản trị dữ liệu. Dưới đây là những lợi ích nổi bật:

**+ Tối ưu hóa hiệu quả hoạt động:** Nhờ khả năng tự động hóa và chuẩn hóa quy trình, trung gian dữ liệu giúp doanh nghiệp nâng cao hiệu suất làm việc. Thông tin được luân chuyển một cách tự động giữa các hệ thống, loại bỏ nhu cầu nhập liệu thủ công lặp đi lặp lại. Các quy trình tích hợp được chuẩn hóa giúp giảm lỗi từ con người và rút ngắn thời gian thực hiện công việc. Kết quả là dòng công việc (workflow) trở nên trơn tru hơn và nhân viên có thể tập trung vào các tác vụ mang tính chiến lược thay vì xử lý dữ liệu thủ công. Thực tế cho thấy, đồng bộ dữ liệu theo thời gian thực với sự hỗ trợ của AI đã giúp loại bỏ nhiều sai sót nhập liệu và giữ cho toàn bộ hệ thống thông tin của tổ chức cập nhật nhất quán, cho phép ra quyết định nhanh chóng và giảm lãng phí thời gian đối chiếu dữ liệu<sup>24</sup>. Nói cách khác, trung gian dữ liệu góp phần tạo nên một môi trường làm việc hiệu quả hơn, tiết kiệm cả thời gian lẫn chi phí vận hành.

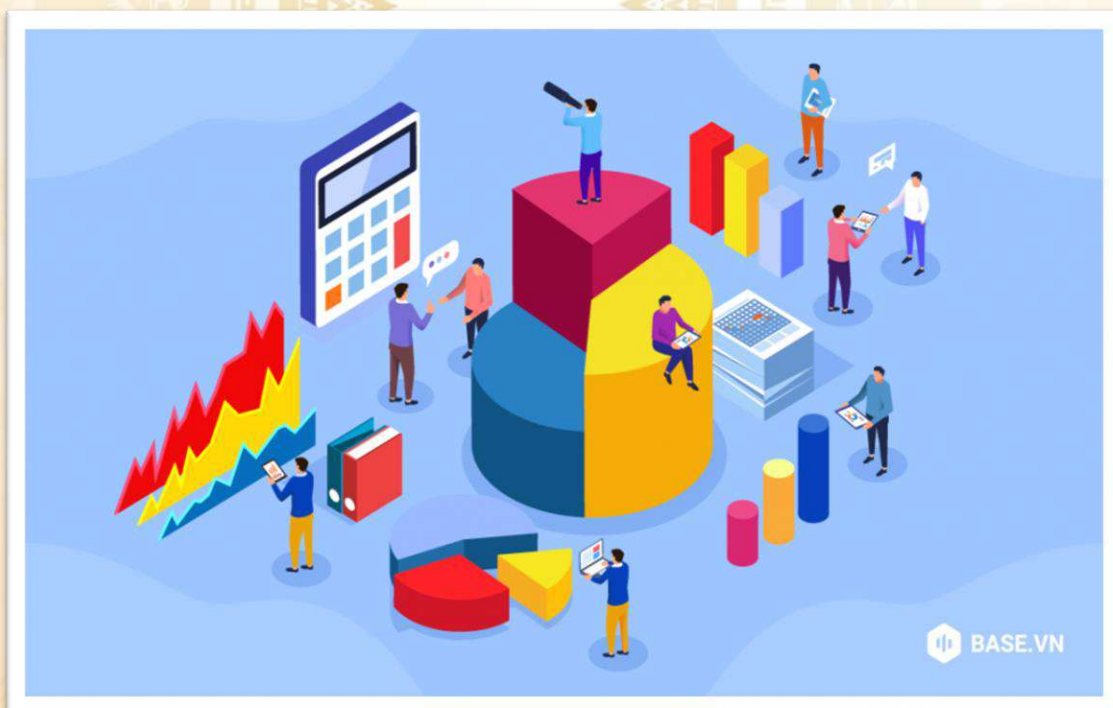
<sup>24</sup> Querio Blog (2023), "Using AI to Improve Data Integration Efficiency", <https://querio.ai/blog/ai-in-data-integration>, truy cập ngày 5/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Đảm bảo tính nhất quán và chính xác của dữ liệu:** Sử dụng giải pháp trung gian đồng nghĩa với việc dữ liệu từ nhiều nguồn khác nhau sẽ được tích hợp liền mạch qua một “bộ lọc” chung. Bộ lọc này thực hiện các bước *làm sạch, chuyển đổi và chuẩn hóa dữ liệu* trước khi phân phối cho các hệ thống đích. Nhờ đó, các sai lệch, trùng lặp hay định dạng không tương thích được xử lý triệt để, giúp thông tin sau cùng đến tay người dùng hoặc hệ thống phân tích có độ chính xác và nhất quán cao. Dữ liệu “đầu vào” tốt sẽ tạo nên đầu ra đáng tin cậy, từ đó nâng cao chất lượng các báo cáo phân tích và quyết định kinh doanh. Chẳng hạn, một công ty khi kết nối dữ liệu bán hàng từ nhiều kênh khác nhau qua một nền tảng trung gian sẽ thu được bức tranh tổng thể thống nhất và chính xác về doanh thu, thay vì các mảng dữ liệu rời rạc có thể mâu thuẫn nhau. Việc này cải thiện đáng kể độ tin cậy của thông tin trong doanh nghiệp.



***Phân tích, tổng hợp dữ liệu là thao tác không thể thiếu để vận hành có hiệu quả dữ liệu để tham mưu, dự báo - Ảnh: Base.vn***





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Tăng cường bảo mật và uy tín:** Các sản phẩm, dịch vụ trung gian dữ liệu thường tích hợp các tính năng bảo mật mạnh mẽ từ mã hóa dữ liệu khi truyền, phân quyền truy cập chặt chẽ cho đến cơ chế giám sát, cảnh báo khi có hoạt động bất thường. Nhờ đó, dữ liệu được bảo vệ khỏi các mối đe dọa an ninh (như truy cập trái phép, rò rỉ dữ liệu) và đảm bảo quyền riêng tư của cá nhân. Việc ngăn ngừa hiệu quả các sự cố mất an toàn thông tin không chỉ giúp doanh nghiệp bảo vệ uy tín thương hiệu mà còn gia tăng niềm tin của khách hàng, đối tác. Ngược lại, nếu để xảy ra vi phạm dữ liệu, lòng tin của khách hàng có thể sụt giảm nghiêm trọng và uy tín thương hiệu sẽ bị tổn hại lâu dài.



***Openscience.vn - nền tảng quản lý và chia sẻ dữ liệu***

***nghiên cứu khoa học và công nghệ dùng chung - Ảnh: VnExpress***

***- Làm thế nào để nâng cao hiệu quả của các sản phẩm, dịch vụ trung gian dữ liệu?***

Để khai thác tối đa tiềm năng của các sản phẩm, dịch vụ trung gian dữ liệu, doanh nghiệp cần có chiến lược đúng đắn và những biện pháp triển khai phù hợp. Dưới đây là một số **giải pháp** và **hướng tiếp cận** giúp nâng cao hiệu quả sử dụng các hệ thống trung gian dữ liệu:





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Ứng dụng AI/ML để tự động hóa thông minh:** Tích hợp trí tuệ nhân tạo và học máy vào giải pháp trung gian dữ liệu giúp hệ thống tự động hóa nhiều tác vụ phức tạp và tối ưu luồng dữ liệu hơn. Ví dụ, AI có thể học từ luồng dữ liệu lịch sử để tự động phát hiện và khắc phục sự cố dữ liệu (như phát hiện dữ liệu bất thường, trùng lặp) ngay khi chúng xuất hiện [67]. Nhờ AI giám sát “mắt thần” 24/7, dữ liệu luôn được kiểm tra chất lượng liên tục, giảm thiểu sai sót mà không cần can thiệp thủ công. Ngoài ra, các thuật toán học máy còn có thể đề xuất cải tiến quy trình tích hợp, tối ưu thứ tự xử lý hoặc cách thức truyền dữ liệu để đạt hiệu suất cao nhất. Việc chủ động đưa AI/ML vào trung gian dữ liệu sẽ giúp doanh nghiệp vừa tăng tốc độ xử lý, vừa giảm chi phí vận hành (do hạn chế được các lỗi đắt đỏ do con người gây ra và tối ưu tài nguyên tính toán).



**Tự động hóa quy trình bằng trí tuệ nhân tạo - Ảnh: VNEconomy**

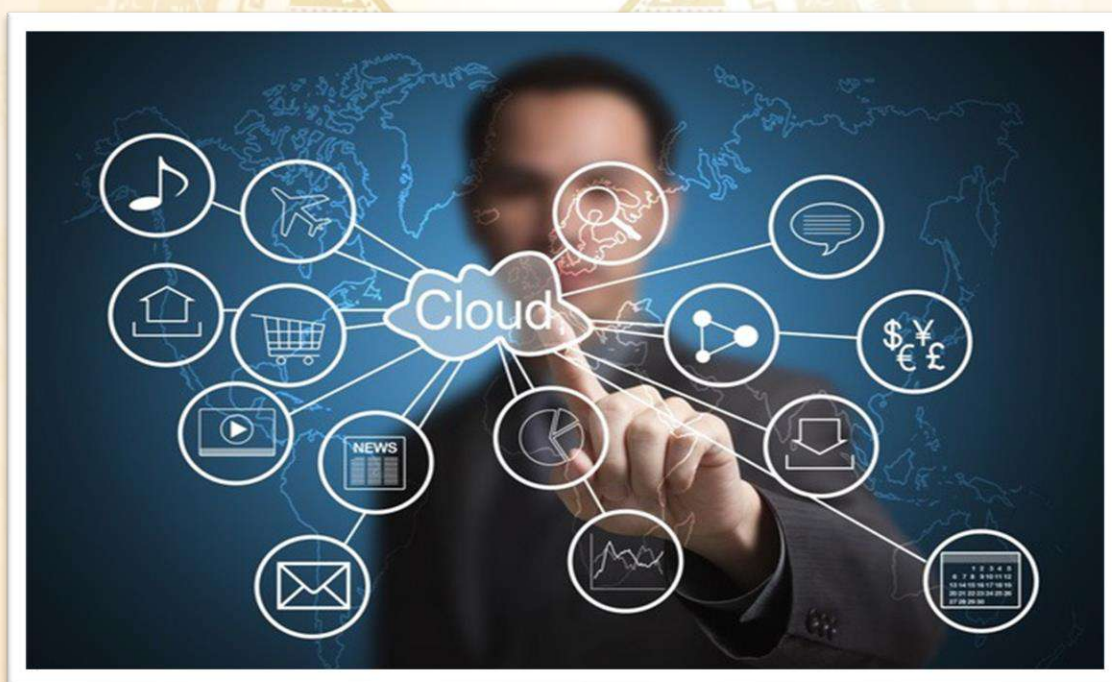
+ **Tận dụng nền tảng điện toán đám mây:** Di chuyển hạ tầng trung gian dữ liệu lên điện toán đám mây (cloud) mang lại nhiều lợi ích về hiệu quả và chi phí. Cloud cho phép doanh nghiệp mở rộng quy mô linh hoạt - tài nguyên





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

máy chủ, bộ nhớ có thể điều chỉnh tăng/giảm nhanh chóng theo lưu lượng dữ liệu thực tế. Điều này đặc biệt hữu ích khi nhu cầu tích hợp dữ liệu tăng đột biến, hệ thống vẫn đáp ứng được mà không bị quá tải. Bên cạnh đó, sử dụng dịch vụ trung gian dữ liệu trên cloud giúp giảm gánh nặng bảo trì hạ tầng, doanh nghiệp không phải đầu tư máy chủ vật lý hay lo lắng về cập nhật phần cứng. Chi phí vận hành cũng theo mô hình trả tiền theo nhu cầu, tối ưu ngân sách công nghệ thông tin. Hơn nữa, cloud tạo điều kiện để tập trung hóa việc quản lý dữ liệu - các kho dữ liệu tập trung trên mây dễ kiểm soát truy cập, sao lưu dự phòng và đảm bảo an toàn hơn. Thực tế, nhiều doanh nghiệp triển khai chiến lược dữ liệu ưu tiên cloud ngay từ đầu đã đạt được hiệu quả cao: hệ thống tích hợp vừa có tính sẵn sàng cao (ít downtime), vừa dễ dàng thích ứng khi quy mô dữ liệu tăng mà không cần tái kiến trúc lớn [65].



**Ứng dụng điện toán đám mây trong phát triển kinh tế - Ảnh: VNEconomy**  
+ **Áp dụng các giải pháp bảo mật tiên tiến (như Blockchain):** Để nâng cao mức độ an toàn của dịch vụ trung gian dữ liệu, doanh nghiệp có thể kết





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

hợp các công nghệ bảo mật hiện đại, điển hình là blockchain. Như đã đề cập, blockchain cung cấp cơ chế sổ cái phân tán bất biến - dữ liệu một khi ghi vào thì không thể chỉnh sửa nếu không có sự đồng thuận của mạng lưới - giúp đảm bảo dữ liệu trao đổi qua trung gian toàn vẹn 100% [57]. Bên cạnh đó, mọi giao dịch dữ liệu trong blockchain đều được gắn dấu thời gian và công khai cho các bên liên quan có quyền, tạo nên sự minh bạch và truy xuất nguồn gốc rõ ràng. Việc tích hợp blockchain vào kiến trúc trung gian dữ liệu (ví dụ: lưu vết giao dịch hoặc quyền truy cập trên blockchain) sẽ giúp ngăn chặn các truy cập trái phép và hành vi gian lận, đồng thời tạo niềm tin cho các bên khi biết rằng dữ liệu luôn được theo dõi chặt chẽ. Ngoài blockchain, doanh nghiệp cũng nên triển khai các biện pháp bảo mật khác như mã hóa dữ liệu mạnh, cơ chế quản lý khóa an toàn, hệ thống phát hiện và ngăn chặn xâm nhập để tạo thành một lớp phòng thủ nhiều tầng cho nền tảng trung gian dữ liệu của mình.



***Tối ưu bảo mật với Blockchain - Ảnh: Internet***





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

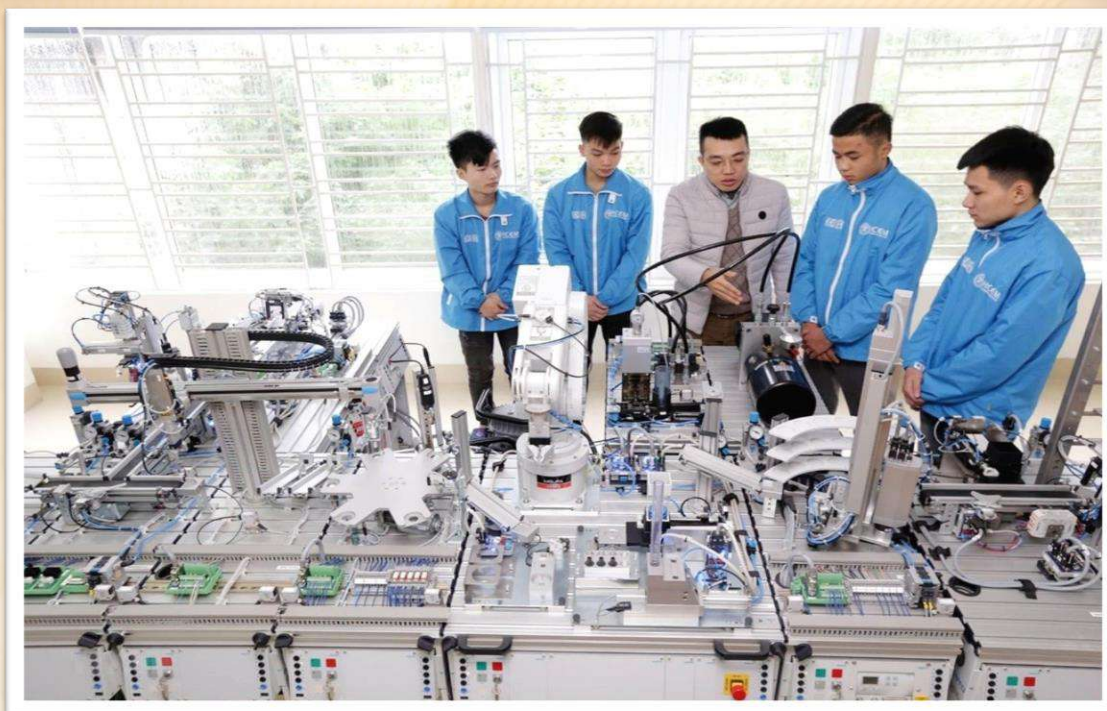
+ **Đào tạo và phát triển kỹ năng cho đội ngũ nhân viên:** Công nghệ chỉ thực sự phát huy hiệu quả khi đi đôi với nguồn nhân lực hiểu biết và thành thạo trong việc vận hành nó. Do đó, doanh nghiệp cần chú trọng đào tạo nhân viên về cách sử dụng, quản trị các sản phẩm, dịch vụ trung gian dữ liệu một cách hiệu quả. Việc bồi dưỡng kỹ năng thông qua các chương trình tập huấn bài bản sẽ giúp đội ngũ phụ trách dữ liệu nâng cao năng lực xử lý và tích hợp dữ liệu. Các khóa đào tạo có thể bao gồm từ kiến thức về làm sạch dữ liệu, mapping dữ liệu, vận hành công cụ ETL đến cập nhật các xu hướng công nghệ mới trong lĩnh vực tích hợp dữ liệu. Khi nhân viên được trang bị kiến thức vững vàng, họ sẽ chủ động hơn trong việc khai thác hệ thống, phát hiện và giải quyết sự cố nhanh chóng, cũng như đề xuất các sáng kiến cải thiện quy trình. Theo khuyến nghị chuyên gia, đưa các chương trình đào tạo có cấu trúc vào chiến lược dữ liệu có thể dẫn đến quy trình làm việc trôi chảy hơn, tăng năng suất và nâng cao chất lượng dữ liệu trong tổ chức. Về lâu dài, một đội ngũ am hiểu về trung gian dữ liệu chính là tài sản quý, giúp doanh nghiệp duy trì lợi thế cạnh tranh trong bối cảnh công nghệ thay đổi nhanh chóng.

Tổng kết lại, để nâng cao hiệu quả của sản phẩm, dịch vụ trung gian dữ liệu, doanh nghiệp cần một cách tiếp cận toàn diện: kết hợp công nghệ phù hợp (AI, cloud, blockchain...) với quy trình tối ưu và con người được đào tạo tốt. Việc lên kế hoạch rõ ràng, đầu tư đúng mức vào những giải pháp tiên tiến và liên tục trau dồi kỹ năng cho đội ngũ sẽ đảm bảo tổ chức khai thác triệt để tiềm năng của dữ liệu, đồng thời duy trì được lợi thế trong thị trường số hóa ngày càng cạnh tranh.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



***Hiện nay có khoảng 70% trên tổng số trường đại học và cao đẳng ở Việt Nam hiện đang đào tạo nhóm ngành phát triển nhân lực công nghệ số -***

***Ảnh: ICT Việt Nam***

***- Quy định về hoạt động trung gian dữ liệu***

Nghị định số 169/2025/NĐ-CP đã bổ sung định nghĩa và khuôn khổ pháp lý chi tiết hơn đối với loại hình sản phẩm và dịch vụ này. Theo đó, “*sản phẩm trung gian dữ liệu*” được hiểu là hệ thống hạ tầng, trang thiết bị, ứng dụng và phần mềm được tổ chức xây dựng nhằm phục vụ các hoạt động kết nối và chia sẻ dữ liệu theo quy định tại Điều 24 của Nghị định này. Trong khi đó, “*dịch vụ trung gian dữ liệu*” được tổ chức cung cấp sản phẩm, dịch vụ cung cấp để phục vụ hoạt động trung gian dữ liệu kết nối, truyền dẫn, truy cập và xử lý dữ liệu điện tử giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng sản phẩm, dịch vụ về dữ liệu bảo đảm an toàn, hiệu quả và đúng định dạng. Điều 24 của Nghị định đã quy định rất rõ ràng các hoạt động trung gian dữ liệu như sau:





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Đại diện cho chủ thể dữ liệu, chủ sở hữu dữ liệu để thực hiện kết nối, chia sẻ, trao đổi, truy cập dữ liệu với bên sử dụng dịch vụ.** Sản phẩm trung gian dữ liệu được phép thay mặt cá nhân, tổ chức (chủ thể dữ liệu, chủ sở hữu dữ liệu) thực hiện kết nối, chia sẻ dữ liệu với bên thứ ba. Điều này tương tự vai trò của một “ủy quyền số” hoặc “đại diện pháp lý kỹ thuật số”. Hay nói cách khác, các tổ chức, cá nhân cung cấp dịch vụ trung gian dữ liệu sẽ đại diện cho chủ thể dữ liệu trong việc thực hiện các quyền và nghĩa vụ liên quan đến dữ liệu, bao gồm: Thiết lập các kênh kết nối, thỏa thuận chia sẻ dữ liệu giữa chủ thể dữ liệu và bên sử dụng dịch vụ; Tạo điều kiện cho việc trao đổi dữ liệu giữa các bên có liên quan; Quản lý việc truy cập dữ liệu, đảm bảo chỉ những bên được phép mới có thể truy cập...

Ví dụ: Công ty A muốn chia sẻ dữ liệu khách hàng với công ty B để phân tích hành vi, nhưng không trực tiếp thực hiện mà ủy quyền cho nền tảng X làm trung gian và kiểm soát hoạt động truy cập.

### MỘT SỐ ĐIỂM KHÁC NHAU GIỮA CHỦ THỂ DỮ LIỆU VÀ CHỦ SỞ HỮU DỮ LIỆU

|                      | <b>Chủ thể dữ liệu<br/>(Data Subject)</b>            | <b>Chủ sở hữu dữ liệu<br/>(Data Owner)</b>                       |
|----------------------|------------------------------------------------------|------------------------------------------------------------------|
| <b>Vai trò chính</b> | Cá nhân mà dữ liệu nói về.                           | Cá nhân hoặc tổ chức chịu trách nhiệm quản lý và bảo vệ dữ liệu. |
| <b>Quyền lợi</b>     | Quyền kiểm soát, truy cập, chỉnh sửa, xóa dữ liệu... | Quyền thiết lập chính sách, quản lý việc sử dụng dữ liệu...      |
| <b>Trách nhiệm</b>   | Không chịu trách nhiệm pháp lý đối với dữ liệu.      | Chịu trách nhiệm pháp lý và hành chính đối với dữ liệu.          |
| <b>Ví dụ</b>         | Một khách hàng của ngân hàng.                        | Ngân hàng chịu trách nhiệm với dữ liệu của khách hàng.           |





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ *Tư vấn, đánh giá tác động việc xử lý dữ liệu, việc cung cấp dịch vụ trung gian dữ liệu giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng dịch vụ dữ liệu.* Trung gian dữ liệu không chỉ đóng vai trò kỹ thuật, mà còn có thể đảm nhiệm chức năng đánh giá rủi ro, đảm bảo xử lý dữ liệu phù hợp với quyền lợi của các bên có liên quan... Hoạt động này có phần tương đồng với quy trình đánh giá tác động quyền riêng tư (Privacy Impact Assessment) trong Quy định Bảo vệ Dữ liệu Chung của EU. Một trong những chức năng trọng yếu của các chủ thể cung cấp dịch vụ trung gian dữ liệu là thực hiện tư vấn và đánh giá tác động việc xử lý dữ liệu, đặc biệt là dữ liệu cá nhân và dữ liệu nhạy cảm. Đây là một quá trình có tính hệ thống nhằm xác định, phân tích và dự báo các rủi ro tiềm ẩn liên quan đến toàn bộ vòng đời của dữ liệu từ khâu thu thập, lưu trữ, chia sẻ đến xử lý và khai thác. Việc đánh giá này được thực hiện trước khi dữ liệu được xử lý, nhằm đảm bảo việc xử lý không gây tổn hại đến quyền, lợi ích hợp pháp của chủ thể dữ liệu và tuân thủ các quy định của pháp luật.



*Minh họa về Bệnh án điện tử - Ảnh: Internet*





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

*Ví dụ:* Một nền tảng trung gian dữ liệu trong lĩnh vực y tế thực hiện đánh giá tác động trước khi chia sẻ hồ sơ bệnh án điện tử từ bệnh viện sang công ty nghiên cứu dược. Trung gian sẽ phân tích xem dữ liệu đó có được ẩn danh hóa chưa, liệu có nguy cơ tái định danh không, và đề xuất giải pháp hạn chế (giới hạn truy cập theo vai trò, kiểm soát nhật ký truy xuất, cảnh báo tự động khi phát hiện hành vi bất thường...).

+ ***Dịch vụ quản trị dữ liệu để ủy thác thay mặt cho chủ thể dữ liệu, chủ sở hữu dữ liệu để kết nối, chia sẻ, trao đổi, truy cập dữ liệu với bên sử dụng dữ liệu.*** Dịch vụ quản trị dữ liệu (Data Stewardship) được ủy thác là một dịch vụ cho phép một bên thứ ba thay mặt chủ thể hoặc chủ sở hữu dữ liệu kết nối, chia sẻ, trao đổi và truy cập dữ liệu với các bên sử dụng dữ liệu khác. Nói cách khác, đây là dịch vụ quản lý dữ liệu, trong đó một tổ chức hoặc cá nhân được ủy quyền để thực hiện các hoạt động liên quan đến dữ liệu thay mặt cho chủ sở hữu dữ liệu, đảm bảo việc sử dụng dữ liệu hiệu quả, an toàn và tuân thủ quy định. Một số tổ chức không có đủ năng lực kỹ thuật hoặc không muốn trực tiếp tham gia vào quá trình quản trị dữ liệu có thể ủy quyền cho trung gian thực hiện thay. Dịch vụ này được gọi là “data stewardship as a service”, trong đó trung gian thực hiện phân loại, lưu trữ, chia sẻ, thiết lập chính sách truy cập dữ liệu... dưới danh nghĩa của bên ủy quyền. Có thể hình dung mô hình như sau: *[Chủ thể dữ liệu] → [Trung gian: kiểm soát, định tuyến, bảo vệ dữ liệu] → [Bên sử dụng dữ liệu]*. Mô hình này giúp tăng cường quản lý tập trung, giảm rủi ro phân mảnh và sai phạm trong khai thác dữ liệu.

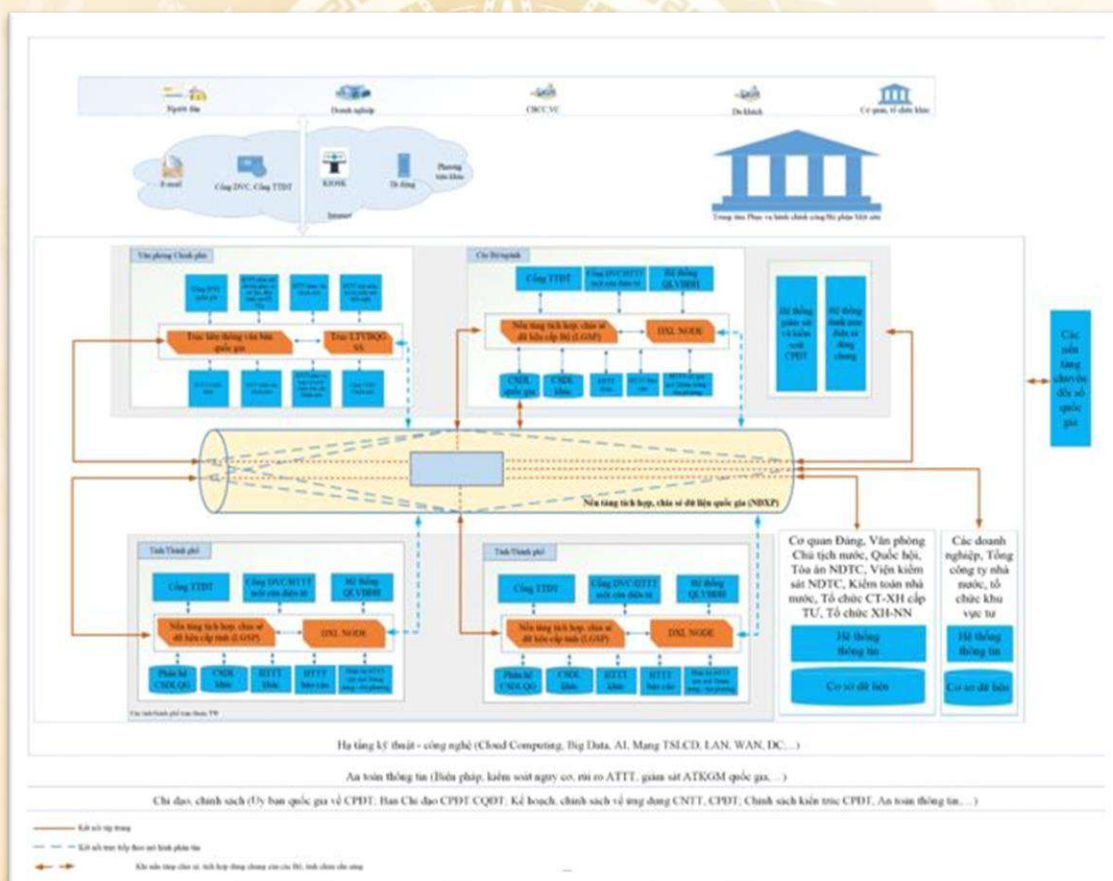
+ ***Đại lý kết nối, chia sẻ, trao đổi, truy cập dữ liệu giữa bên chủ thể dữ liệu, chủ sở hữu dữ liệu với bên sử dụng dữ liệu.*** Đây có thể là một hệ thống trung gian, một nền tảng hoặc một dịch vụ đóng vai trò cầu nối, giúp





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU Trong công an nhân dân

các hệ thống khác nhau kết nối với nhau để chia sẻ, trao đổi, truy cập dữ liệu. Tại Việt Nam, “đại lý kết nối, chia sẻ, trao đổi, truy cập dữ liệu” đang được phát triển mạnh mẽ, đặc biệt trong bối cảnh Chính phủ thúc đẩy chuyển đổi số và phát triển dữ liệu mở. Tuy nhiên, thay vì những “đại lý” chuyên biệt, vai trò này thường được thực hiện bởi các công ty cung cấp dịch vụ công nghệ, viễn thông và giải pháp dữ liệu như Viettel, VNPT, FPT Telecom... Các đơn vị này không chỉ cung cấp hạ tầng Internet mà còn phát triển các trung tâm dữ liệu, dịch vụ điện toán đám mây và các nền tảng tích hợp dữ liệu, giúp các doanh nghiệp và cơ quan nhà nước dễ dàng kết nối, lưu trữ và chia sẻ dữ liệu một cách an toàn.



**Mô hình kết nối quốc gia qua Nền tảng tích hợp, chia sẻ dữ liệu quốc gia**

**NDXP - Ảnh: Bộ Thông tin và Truyền thông (cũ)**





+ ***Dịch vụ cung cấp hạ tầng, trang thiết bị, ứng dụng, phần mềm, dịch vụ truyền đưa và các loại hình khác để phục vụ hoạt động trung gian dữ liệu.*** Chủ thể cung cấp sản phẩm, dịch vụ trung gian dữ liệu cũng có thể là các nhà cung cấp dịch vụ nền tảng, bao gồm các hệ thống lưu trữ, giao thức truyền dẫn, ứng dụng phân tích, nền tảng blockchain... phục vụ việc vận hành hạ tầng chia sẻ dữ liệu.

Chẳng hạn, Amazon Web Services cung cấp nền tảng Data Exchange cho phép các tổ chức mua, bán, chia sẻ dữ liệu qua dịch vụ đám mây. Hay nền tảng tích hợp, chia sẻ dữ liệu quốc gia (National Data Exchange Platform - NDXP) được đưa vào sử dụng, phục vụ việc kết nối, tích hợp, chia sẻ dữ liệu giữa các bộ, ngành, địa phương, giúp tối đa hóa giá trị dữ liệu, nâng cao chất lượng cung cấp dịch vụ công, hiệu quả quản lý chỉ đạo điều hành các cấp, tạo tiền đề thúc đẩy cho quá trình chuyển đổi số quốc gia được nhanh chóng, hiệu quả.

+ ***Dịch vụ hỗ trợ, kiểm soát các thuộc tính của dữ liệu bảo đảm quyền riêng tư, dữ liệu nhạy cảm, dữ liệu cá nhân, đánh giá rủi ro đối với hoạt động chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng theo quy định của pháp luật trong hoạt động trung gian dữ liệu.***

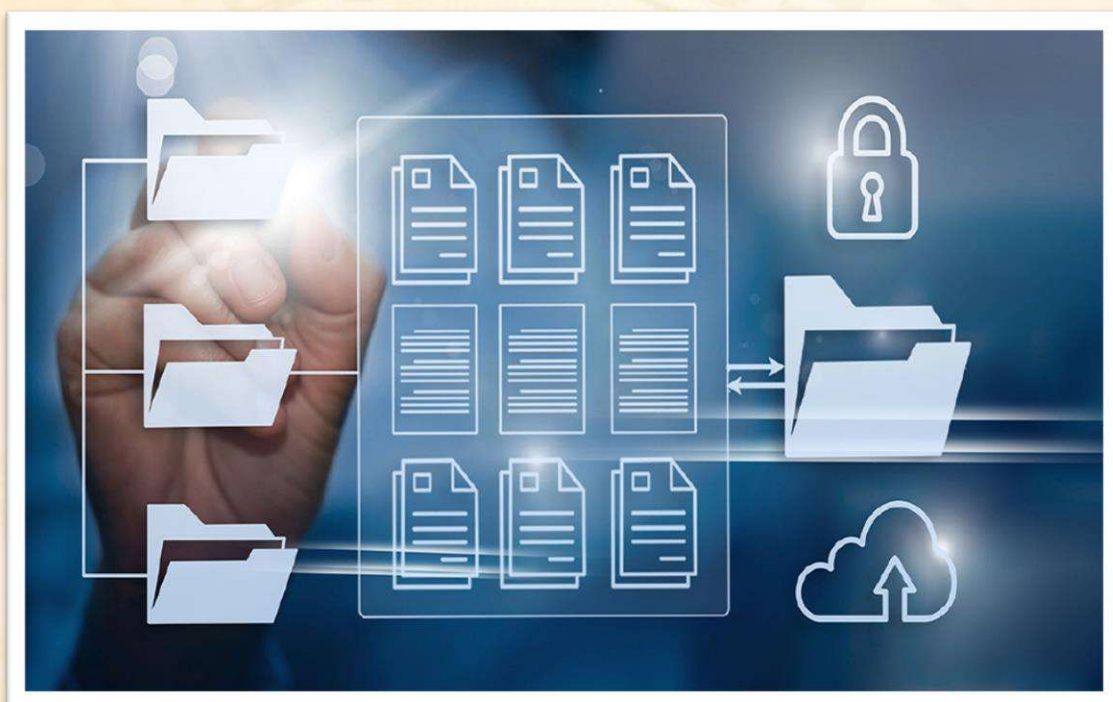
Trong “*hệ sinh thái trung gian dữ liệu*”, một trong những dịch vụ cốt lõi là hỗ trợ và kiểm soát các thuộc tính dữ liệu, nhằm đảm bảo việc xử lý dữ liệu được thực hiện một cách trách nhiệm, minh bạch và phù hợp với quy định bảo vệ quyền riêng tư. Không chỉ giới hạn ở khía cạnh kỹ thuật như bảo mật hay mã hóa, dịch vụ này còn bao gồm các chức năng quản trị việc sử dụng dữ liệu, từ đó ngăn ngừa việc xử lý sai mục đích, hoặc vượt quá phạm vi được cho phép. Đối với dịch vụ này, các kỹ thuật như mã hóa dữ liệu đầu cuối (end-to-end encryption) và mã hóa ở trạng thái nghỉ (at rest encryption)





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

thường được sử dụng trong quá trình lưu trữ và truyền tải. Song song đó, việc thiết lập chế độ kiểm soát truy cập chặt chẽ là cần thiết nhằm bảo đảm chỉ những cá nhân, bộ phận được ủy quyền mới có quyền truy cập dữ liệu. Trong nhiều trường hợp, các nền tảng còn ứng dụng công nghệ ẩn danh hóa (anonymization) hoặc giả danh hóa (pseudonymization) để giảm thiểu rủi ro tái định danh chủ thể dữ liệu.



### ***Phân quyền truy cập dữ liệu để đảm bảo an ninh, an toàn - Ảnh: Internet***

Bên cạnh đó, việc kiểm soát các thuộc tính của dữ liệu là một nội dung quan trọng trong hoạt động trung gian. Các trung gian phải thực hiện phân loại dữ liệu theo từng cấp độ bảo mật (dữ liệu công khai, dữ liệu nội bộ, dữ liệu cá nhân và dữ liệu nhạy cảm...). Việc phân loại này giúp áp dụng các chính sách bảo vệ phù hợp với mức độ nhạy cảm của từng loại dữ liệu, đảm bảo rằng thông tin quan trọng luôn được bảo vệ ở mức cao nhất. Hơn nữa, việc quản lý sự đồng thuận của chủ thể dữ liệu cần được đảm bảo thông qua các cơ chế kỹ thuật minh bạch và thân thiện. Các cơ





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

chế này phải cho phép chủ thể dữ liệu thực hiện đầy đủ các quyền của mình, bao gồm quyền thu hồi, sửa đổi, hoặc từ chối chia sẻ dữ liệu. Đây là yếu tố quyết định để bảo đảm quyền riêng tư và xây dựng sự tin cậy, vốn là giá trị cốt lõi của hoạt động trung gian dữ liệu. Một ví dụ minh họa tại Việt Nam là hệ thống eKYC của Ngân hàng Thương mại cổ phần Quân đội, khi thu thập và xử lý ảnh chân dung, giấy tờ cá nhân, đã tích hợp công nghệ mã hóa, phân quyền truy cập nội bộ và lưu trữ trên hạ tầng đạt tiêu chuẩn ISO 27001. Đồng thời, ngân hàng này cũng cho phép người dùng cập nhật, điều chỉnh hoặc yêu cầu xóa thông tin cá nhân theo cơ chế đồng thuận điện tử, phù hợp quy định về bảo vệ dữ liệu cá nhân trong Luật Bảo vệ dữ liệu cá nhân năm 2025.

Đánh giá rủi ro đối với hoạt động chuyên, xử lý dữ liệu cốt lõi, dữ liệu quan trọng là hoạt động giúp chủ động phát hiện, phân tích và giảm thiểu các nguy cơ có thể xảy ra trong suốt quá trình thu thập, xử lý, truyền đưa hoặc lưu trữ dữ liệu. Quy trình này không chỉ mang tính kỹ thuật, mà còn là yêu cầu pháp lý bắt buộc nhằm bảo vệ cả chủ thể dữ liệu lẫn uy tín của tổ chức trung gian. Các rủi ro cần đánh giá thường bao gồm ba nhóm chính:

**(1) Rủi ro kỹ thuật** như lỗ hổng bảo mật, phần mềm lỗi thời hoặc các cuộc tấn công mạng có thể khiến dữ liệu bị rò rỉ, thất thoát.

**(2) Rủi ro con người** cũng rất phổ biến, bao gồm hành vi sơ suất hoặc cố ý của nhân viên khi thao tác dữ liệu, đặc biệt trong bối cảnh làm việc từ xa ngày càng phổ biến.

**(3) Rủi ro pháp lý**, nếu tổ chức không tuân thủ đầy đủ các quy định của pháp luật có liên quan, có thể dẫn đến chế tài nghiêm khắc, bao gồm phạt hành chính lên đến 5% tổng doanh thu, theo quy định tại khoản 4, Điều 8 của Luật Bảo vệ dữ liệu cá nhân năm 2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Sau khi xác định rủi ro, tổ chức cần phân tích tác động cụ thể lên từng nhóm dữ liệu và nhóm quyền lợi cá nhân liên quan. Ví dụ, nếu xảy ra sự cố rò rỉ dữ liệu y tế của bệnh nhân, tác động không chỉ là vi phạm quyền riêng tư mà còn ảnh hưởng nghiêm trọng đến danh dự và điều trị sức khỏe. Từ đó, trung gian cần đưa ra biện pháp giảm thiểu cụ thể, như tăng cường mã hóa, xây dựng quy trình phân quyền rõ ràng, tổ chức đào tạo định kỳ về an toàn dữ liệu cho nhân viên, hoặc triển khai hệ thống phát hiện truy cập bất thường.

+ ***Dịch vụ hợp tác, chia sẻ dữ liệu để phục vụ kết nối, chia sẻ, khai thác, truy cập dữ liệu theo quy định của pháp luật.*** Trung gian đóng vai trò như một người tạo lập không gian chia sẻ, nơi các bên (có thể là doanh nghiệp, cơ quan nhà nước, tổ chức nghiên cứu hoặc startup) cùng nhau hợp tác, trao đổi, sử dụng dữ liệu để phát triển các sản phẩm, dịch vụ mang giá trị gia tăng. Trung gian bảo đảm mọi hoạt động diễn ra theo nguyên tắc minh bạch, có kiểm soát, có đồng thuận và đặc biệt là tuân thủ các quy định pháp luật về dữ liệu và an ninh mạng.

Tại Singapore, nền tảng Singapore Government Data Platform (SGDP) là một minh chứng điển hình. Đây là nền tảng dữ liệu do chính phủ Singapore xây dựng, cho phép các cơ quan công quyền và doanh nghiệp hợp tác, chia sẻ dữ liệu với nhau trong nhiều lĩnh vực như giao thông, môi trường, năng lượng và đô thị thông minh. Ví dụ, dữ liệu từ cảm biến giao thông do cơ quan quản lý đô thị thu thập có thể được chia sẻ cho các công ty logistics để tối ưu hóa tuyến đường vận chuyển; hoặc dữ liệu thời tiết thời gian thực được tích hợp vào ứng dụng du lịch thông minh cho khách quốc tế. Mọi giao dịch dữ liệu trên SGDP đều được trung gian giám sát chặt chẽ, đảm bảo minh bạch và an toàn.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Tại Việt Nam, dịch vụ này đang được triển khai mạnh mẽ, đặc biệt trong lĩnh vực công. Nổi bật nhất không thể không nhắc đến Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NDXP), là một nền tảng kỹ thuật do Bộ Thông tin và Truyền thông (cũ) xây dựng, đóng vai trò là “trung tâm” kết nối và chia sẻ dữ liệu giữa các bộ, ngành, địa phương và các cơ sở dữ liệu quốc gia khác. Thay vì các cơ quan phải xây dựng kết nối riêng lẻ với nhau, NDXP cung cấp một điểm kết nối duy nhất để trao đổi dữ liệu một cách an toàn và thống nhất. Điều này giúp giảm chi phí, tăng tốc độ triển khai và đảm bảo tính đồng bộ của dữ liệu. Đặc biệt, thông qua NDXP, Bộ Công an có thể chia sẻ dữ liệu về căn cước công dân với Bảo hiểm xã hội Việt Nam để đối chiếu và xác thực thông tin, hoặc với Bộ Tài Chính để đơn giản hóa thủ tục đăng ký doanh nghiệp... Theo thống kê Cục Chuyên đổi số quốc gia, đến tháng 3/2025, có 324 dịch vụ chia sẻ dữ liệu được cung cấp trên NDXP [19].

### **MỘT SỐ DỊCH VỤ CHIA SẺ DỮ LIỆU DO BỘ CÔNG AN CUNG CẤP TRÊN NDXP**

| TT | Mã dịch vụ | Hệ thống/<br>Cơ sở dữ liệu /Dự án | Tên dịch vụ                                                    | Mô tả<br>Nội dung dữ liệu chia sẻ                                                                                                                                                      |
|----|------------|-----------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | G01.01     | Cơ sở dữ liệu quốc gia về dân cư  | Dịch vụ xác thực cấp số Căn cước công dân/ Chứng minh nhân dân | Dịch vụ này cho phép xác thực thông tin cấp số định danh cá nhân/ số căn cước công dân và số chứng minh nhân dân là cùng 01 công dân trong Cơ sở dữ liệu quốc gia về dân cư hay không. |





# BÀI DỰ THI TÌM HIỂU

## LUẬT DỮ LIỆU *Trong công an nhân dân*

| TT | Mã dịch vụ | Hệ thống/<br>Cơ sở dữ liệu /Dự án | Tên dịch vụ                                                       | Mô tả<br>Nội dung dữ liệu chia sẻ                                                                                       |
|----|------------|-----------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| 2  | G01.02     | Cơ sở dữ liệu quốc gia về dân cư  | Dịch vụ tra cứu thông tin công dân                                | Dịch vụ này cho phép chia sẻ các trường thông tin của công dân có trong Cơ sở dữ liệu quốc gia về dân cư.               |
| 3  | G01.03     | Cơ sở dữ liệu quốc gia về dân cư  | Dịch vụ gợi ý số định danh cá nhân                                | Dịch vụ này cho phép cung cấp số định danh công dân có trong Cơ sở dữ liệu quốc gia về dân cư.                          |
| 4  | G01.04     | Cơ sở dữ liệu quốc gia về dân cư  | Dịch vụ đồng bộ thông tin đăng ký doanh nghiệp                    | Dịch vụ này cho phép đồng bộ thông tin đăng ký doanh nghiệp từ Bộ Kế hoạch đầu tư tới Cơ sở dữ liệu quốc gia về dân cư. |
| 5  | G01.05     | Cơ sở dữ liệu quốc gia về dân cư  | Dịch vụ đồng bộ thông tin giấy phép lái xe                        | Dịch vụ này cho phép đồng bộ thông tin giấy phép lái xe từ Bộ Giao thông vận tải tới Cơ sở dữ liệu quốc gia về dân cư.  |
| 6  | G01.06     | Kết nối dữ liệu dân cư            | Dịch vụ cung cấp thông tin công dân và thông tin biến động cư trú | Dịch vụ cung cấp thông tin công dân và thông tin biến động cư trú                                                       |
| 7  | G01.07     | Kết nối dữ liệu dân cư            | Dịch vụ gợi ý số định danh cá nhân                                | Dịch vụ gợi ý số định danh cá nhân (không có số Chứng minh nhân dân)                                                    |





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

| TT | Mã dịch vụ | Hệ thống/<br>Cơ sở dữ liệu /Dự án | Tên dịch vụ                           | Mô tả<br>Nội dung dữ liệu chia sẻ     |
|----|------------|-----------------------------------|---------------------------------------|---------------------------------------|
|    |            |                                   | (không có số Chứng minh nhân dân)     |                                       |
| 8  | G01.08     | Kết nối dữ liệu dân cư            | Xác thực thông tin doanh nghiệp       | Xác thực thông tin doanh nghiệp       |
| 9  | G01.09     | Kết nối dữ liệu dân cư            | Dịch vụ xác nhận thông tin chủ hộ     | Dịch vụ xác nhận thông tin chủ hộ     |
| 10 | G01.10     | Kết nối dữ liệu dân cư            | Dịch vụ đồng bộ thông tin số thuê bao | Dịch vụ đồng bộ thông tin số thuê bao |
| 11 | G01.11     | Kết nối hệ thống VNEID            | Lấy thông tin user                    | Lấy thông tin user                    |

+ Thẩm định điều kiện tham gia sản dữ liệu của các chủ thể có liên quan; tính hợp pháp và việc đáp ứng điều kiện tham gia giao dịch của sản phẩm, dịch vụ dữ liệu; khả năng đáp ứng yêu cầu trong việc bảo đảm an ninh, an toàn khi sử dụng sản phẩm dữ liệu. Ngoài ra, còn có các hoạt động khác thực hiện theo quy định hoạt động thử nghiệm có kiểm soát để đánh giá, phân tích bổ sung vào hoạt động trung gian dữ liệu.

*- Điều kiện đối với tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu giữa bên sử dụng dịch vụ với cơ quan nhà nước:*

Điều 25 của Nghị định số 169/2025/NĐ-CP quy định các điều kiện cụ thể đối với các tổ chức cung cấp sản phẩm và dịch vụ trung gian dữ liệu cho các cơ quan nhà nước. Các tổ chức này phải là đơn vị sự nghiệp hoặc doanh nghiệp được thành lập và hoạt động hợp pháp tại Việt Nam.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

+ **Về nhân sự**, người đứng đầu hoặc người đại diện theo pháp luật phải là công dân Việt Nam, thường trú tại Việt Nam, có trình độ đại học trở lên và ít nhất 3 năm kinh nghiệm trong lĩnh vực quản lý dữ liệu. Ngoài ra, tổ chức cần có ít nhất 5 nhân sự có trình độ đại học trở lên, trong đó có người có các chứng chỉ liên quan đến khoa học dữ liệu, phân tích dữ liệu, quản lý dữ liệu hoặc thẩm định dữ liệu.

+ **Về cơ sở vật chất và kỹ thuật**, tổ chức phải có hạ tầng và trang thiết bị đặt tại Việt Nam, đã được kiểm định an ninh an toàn thông tin theo quy định. Tổ chức cũng phải có một đề án hoạt động chi tiết, bao gồm các phương án về quy trình hoạt động, giải pháp công nghệ, lưu trữ và bảo vệ dữ liệu, an ninh trật tự, thanh toán, thẩm định dữ liệu, định danh và xác thực điện tử, cũng như phòng cháy chữa cháy và dự phòng thảm họa.

+ **Về tài chính**, tổ chức phải ký quỹ không dưới 5 tỷ đồng tại một ngân hàng thương mại Việt Nam. Số tiền này dùng để giải quyết các rủi ro, bồi thường thiệt hại do lỗi của tổ chức và chi trả các chi phí liên quan khi bị thu hồi giấy phép.

### **7.1.4.3. Về sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu**

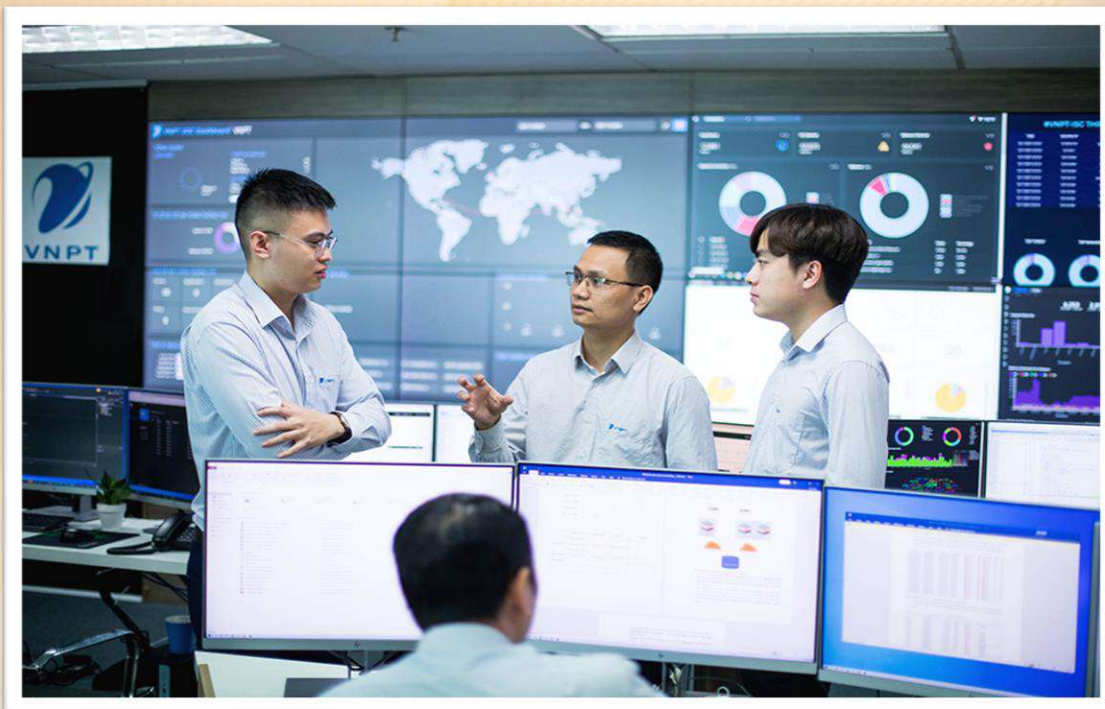
Trong bối cảnh dữ liệu ngày càng trở thành tài nguyên chiến lược của nền kinh tế số, việc phân tích và tổng hợp dữ liệu đóng vai trò ngày càng thiết yếu trong quá trình ra quyết định của doanh nghiệp, cơ quan nhà nước và các tổ chức xã hội. Theo quy định tại Luật Dữ liệu năm 2024, sản phẩm và dịch vụ phân tích, tổng hợp dữ liệu được hiểu như sau:

+ **Sản phẩm phân tích, tổng hợp dữ liệu** là kết quả của quá trình xử lý dữ liệu thô thành các thông tin chuyên sâu, hữu ích ở các cấp độ khác nhau theo yêu cầu của bên sử dụng sản phẩm, phục vụ cho những mục tiêu cụ thể như lập kế hoạch, dự báo hoặc cải tiến vận hành.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



***Minh họa về sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu - Ảnh: Internet***

+ ***Dịch vụ phân tích, tổng hợp dữ liệu*** là hoạt động phân tích, tổng hợp dữ liệu theo yêu cầu cụ thể từ tổ chức hoặc cá nhân có nhu cầu sử dụng dữ liệu.

*Ví dụ:* Một công ty bảo hiểm có thể thuê bên thứ ba thực hiện phân tích dữ liệu hành vi của khách hàng để thiết kế gói bảo hiểm phù hợp. Kết quả phân tích đó chính là “**sản phẩm**”, còn quy trình thực hiện là “**dịch vụ**” phân tích dữ liệu.

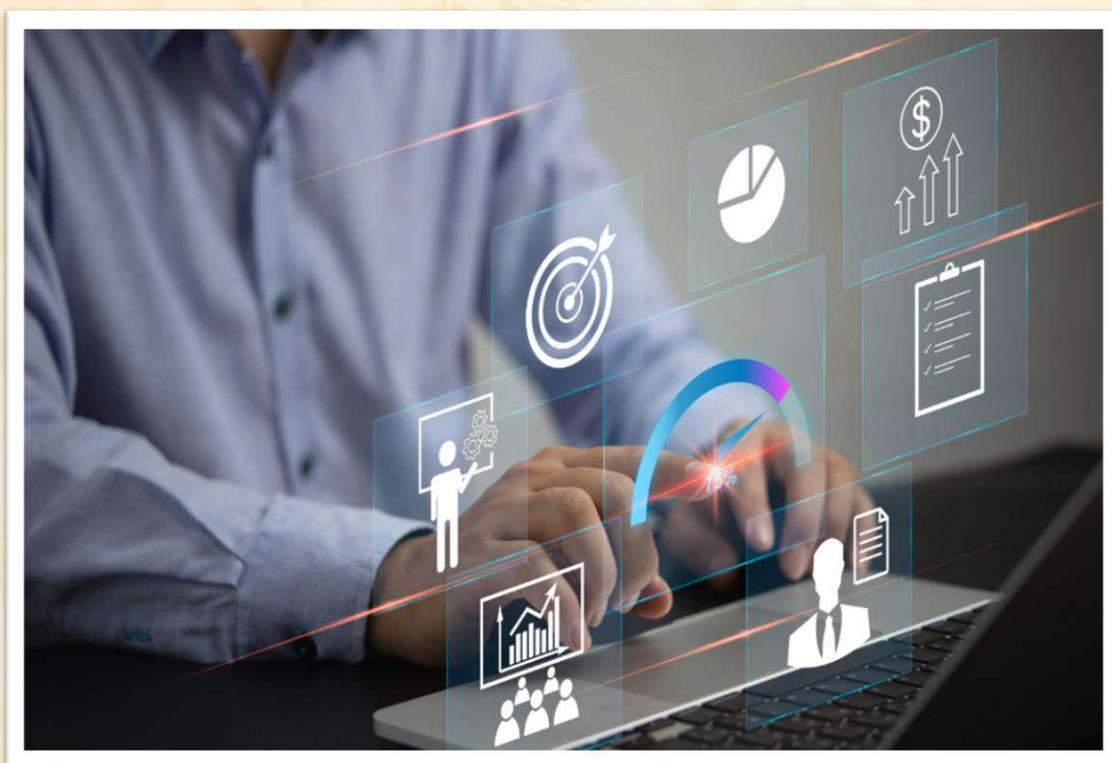
***- Vai trò của sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu trong nền kinh tế số***

Dữ liệu đang được ví như “nguồn tài nguyên mới” hay “dầu mỏ mới” trong nền kinh tế số, đóng vai trò then chốt thúc đẩy đổi mới sáng tạo và tăng trưởng kinh tế. Khác với tài nguyên truyền thống, dữ liệu không bị cạn kiệt khi sử dụng; ngược lại, càng được khai thác và chia sẻ, dữ liệu càng gia tăng giá trị. Một mẫu dữ liệu đơn lẻ có thể ít giá trị, nhưng khi tổng hợp và phân





tích cùng các dữ liệu liên quan, nó sẽ tạo ra tri thức mới, thúc đẩy sáng tạo và nâng cao năng suất. Do đó, tích lũy dữ liệu lớn kết hợp với phân tích chuyên sâu sẽ mở ra cơ hội tăng trưởng dài hạn vượt bậc cho tổ chức và quốc gia. Thực tế cho thấy các công ty có giá trị cao thế giới hiện nay đều lấy dữ liệu làm yếu tố trung tâm trong mô hình kinh doanh<sup>25</sup>.



### ***Phân tích, tổng hợp dữ liệu là khâu đảm bảo hiệu quả hoạt động của cả hệ thống dữ liệu - Ảnh: TACA***

Trong bối cảnh chuyển đổi số, dữ liệu và các dịch vụ phân tích dữ liệu ngày càng trở thành xương sống của mọi hoạt động. Phân tích dữ liệu giúp tổ chức hiểu rõ hơn về hoạt động và khách hàng, từ đó đưa ra quyết định nhanh chóng và chính xác hơn. Báo cáo của IMD khẳng định phân tích dữ liệu là yêu cầu tất yếu để doanh nghiệp hiện đại tồn tại, bởi nó cung cấp

<sup>25</sup> Bích Ngọc (2024), *Giải pháp thúc đẩy phát triển kinh tế dữ liệu tại Việt Nam*, Tạp chí Công Thương, <https://tapchicongthuong.vn/giai-phap-thuc-day-phat-trien-kinh-te-du-lieu-tai-viet-nam-119943.htm>, truy cập ngày 05/8/2025.





những insight (hiểu biết chuyên sâu) có giá trị, giúp ra quyết định dựa trên bằng chứng thay vì cảm tính<sup>26</sup>. Nhờ dữ liệu lớn và công nghệ phân tích, doanh nghiệp có thể tối ưu hóa quy trình, nâng cao hiệu quả vận hành, cũng như phát hiện những cơ hội thị trường mới mà trước đây bị bỏ lỡ. Chẳng hạn, phân tích dữ liệu cho phép ngân hàng đánh giá rủi ro tín dụng và chấm điểm khách hàng chính xác hơn, hỗ trợ phát triển sản phẩm dịch vụ tài chính phù hợp. Tại Việt Nam, các tổ chức tài chính đã ứng dụng thuật toán “*machine learning*” trên tập dữ liệu lớn về doanh nghiệp để xây dựng mô hình chấm điểm tín dụng, dự báo xu hướng rủi ro và tiềm năng tương lai của khách hàng trước khi ra quyết định đầu tư hay cho vay. Đồng thời, dữ liệu giúp sàng lọc đối tác, tinh giản quy trình phục vụ và tiết kiệm chi phí nhân sự (nhất là ở khâu thẩm định, quản lý rủi ro, tiếp thị), qua đó nâng cao năng suất lao động và năng lực cạnh tranh cho doanh nghiệp [32].

Quan trọng hơn, dữ liệu là hạ tầng mềm của nền kinh tế số, là nhiên liệu để vận hành cả bộ máy từ Chính phủ đến doanh nghiệp. Ủy ban Quốc gia về Chuyển đổi số đã chọn năm 2023 là “*Năm Dữ liệu số Quốc gia*”, thể hiện quyết tâm tạo ra giá trị mới từ dữ liệu và coi dữ liệu là động lực thúc đẩy chuyển đổi số quốc gia. Chính phủ Việt Nam nhận định rằng việc khai thác dữ liệu sẽ cải thiện hiệu quả và đổi mới của nền kinh tế, đồng thời giảm bất cân xứng thông tin và chi phí giao dịch, tăng tính minh bạch, hiệu quả, công bằng và cạnh tranh trên thị trường.

Chiến lược dữ liệu quốc gia đến năm 2030 cũng nêu rõ: “*Dữ liệu là yếu tố đột phá; lấy thị trường dữ liệu làm động lực phát triển các hoạt động trong chuỗi giá trị dữ liệu như thu thập, lưu trữ, làm giàu, xử lý, chia sẻ,*

<sup>26</sup> IMD (2024), *Why Data Analytics is Important for Digital Transformation?*, <https://www.imd.org/blog/digital-transformation/the-role-of-data-analytics/>, truy cập ngày 05/8/2025.





*phân tích, phân phối..., qua đó thúc đẩy chuyển đổi số các ngành, lĩnh vực”* [36]. Điều này nhấn mạnh vai trò trung tâm của các sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu trong việc biến dữ liệu thô thành thông tin và tri thức phục vụ phát triển kinh tế số và xã hội số.



### ***Hội thảo Chiến lược dữ liệu quốc gia - Ảnh: VnEconomy***

Trên phạm vi quốc tế, quy mô nền kinh tế dữ liệu đang tăng trưởng ấn tượng, phản ánh tầm quan trọng ngày càng lớn của dữ liệu. Tại Liên minh châu Âu (EU), giá trị nền kinh tế dữ liệu năm 2019 ước tính khoảng 325 tỷ Euro (tương đương 2,6% GDP), dự báo sẽ vượt 550 tỷ Euro vào năm 2025 (khoảng 4% GDP)<sup>27</sup>. Thậm chí một số nghiên cứu cập nhật dự báo con số này có thể đạt 640 tỷ Euro (khoảng 4,8% GDP) vào năm 2025<sup>28</sup>. Nhiều nền

<sup>27</sup> Shaping Europe's digital future (2019), *Building a data economy - Brochure*, <https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure>, truy cập ngày 05/8/2025.

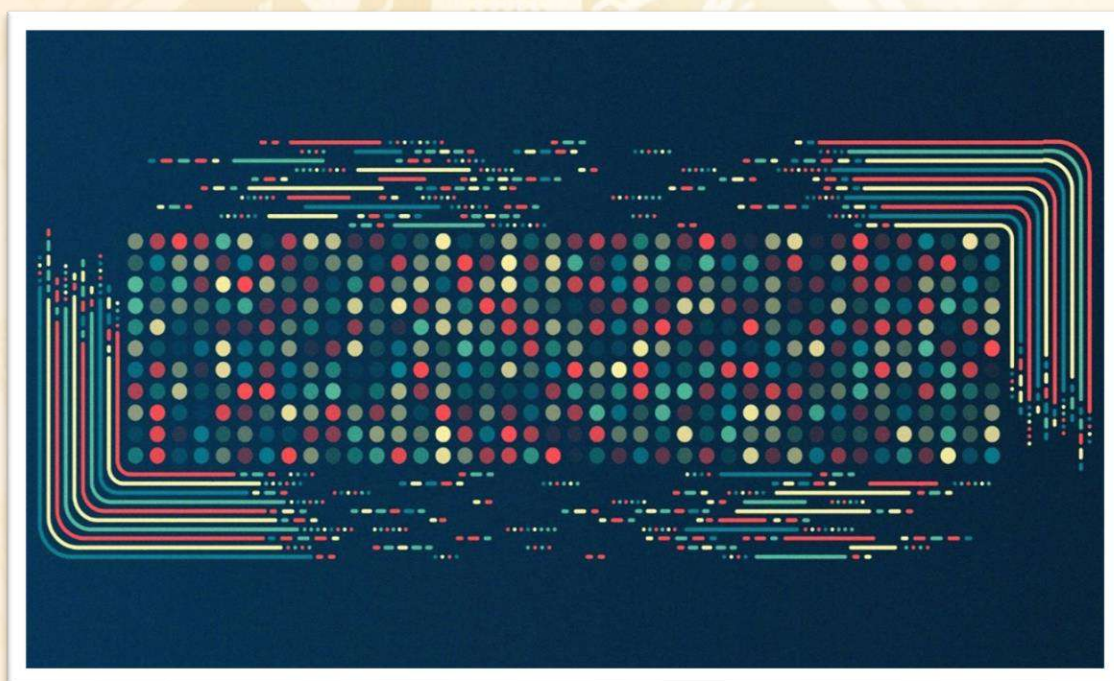
<sup>28</sup> IE Insights (2023), *The Community of Data*, <https://www.ie.edu/insights/articles/the-community-of-data/>, truy cập ngày 05/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

kinh tế phát triển đã coi dữ liệu là lực đẩy quan trọng cho tăng trưởng, đầu tư mạnh vào hạ tầng và nhân lực phân tích dữ liệu nhằm giành lợi thế cạnh tranh. McKinsey nhận định rằng đến năm 2025, đa số nhân viên sẽ sử dụng dữ liệu để tối ưu gần như mọi khía cạnh công việc, tích hợp liền mạch con người và máy móc, đưa quy trình thông minh dựa trên dữ liệu trở thành tiêu chuẩn vận hành doanh nghiệp<sup>29</sup>. Rõ ràng, trong kỷ nguyên số, năng lực khai thác, phân tích và tổng hợp dữ liệu đang là yếu tố cốt lõi quyết định sức mạnh kinh tế của mỗi quốc gia và tổ chức.



### *Ảnh minh họa: Internet*

#### *- Các cấp độ phân tích, tổng hợp dữ liệu*

Theo **Nghị định 169/2025/NĐ-CP**, các hoạt động phân tích, tổng hợp dữ liệu được phân chia theo **04 cấp độ**, tùy theo mức độ ứng dụng trí tuệ nhân tạo (AI):

<sup>29</sup> Fernández-Lasquetty, J. (2023), *The Community of Data*, IE Insights, <https://www.ie.edu/insights/articles/the-community-of-data/>, truy cập ngày 08/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Cấp độ 1:** Việc phân tích, tổng hợp dữ liệu do con người trực tiếp thực hiện, sử dụng thiết bị, phần mềm không tích hợp trí tuệ nhân tạo.

*Ví dụ:* Một nhóm phân tích dữ liệu tại công ty nhỏ sử dụng Microsoft Excel hoặc phần mềm thống kê cơ bản để tính trung bình, xác suất hoặc vẽ biểu đồ, hoàn toàn không có tích hợp AI. Đây là cách tiếp cận truyền thống và phổ biến nhất ở nhiều doanh nghiệp vừa và nhỏ.

+ **Cấp độ 2:** Việc phân tích, tổng hợp dữ liệu do con người trực tiếp thực hiện và có hỗ trợ một phần bởi trí tuệ nhân tạo.

*Ví dụ:* Nền tảng như Hal9 sử dụng Machine Learning (học máy) để “gợi ý” biểu đồ, trực quan dữ liệu và tạo insight ban đầu, nhưng con người vẫn đưa ra quyết định cuối cùng. Hal9 hỗ trợ người dùng truy vấn dữ liệu bằng ngôn ngữ tự nhiên và nhận đề xuất biểu đồ phù hợp<sup>30</sup>. Hoặc một số công ty tiếp thị tại Việt Nam sử dụng công cụ CRM có AI phân tích hành vi khách hàng (ví dụ khách hàng có thể mua lại trong bao lâu), nhưng chuyên viên vẫn đánh giá và chỉnh sửa kết quả trước khi báo cáo cuối cùng.

+ **Cấp độ 3:** Việc phân tích, tổng hợp dữ liệu thực hiện hoàn toàn bởi trí tuệ nhân tạo, có sự giám sát của con người trong quá trình thực hiện.

*Ví dụ:* Các công ty tài chính sử dụng hệ thống phân tích thị trường tự động (AI tự động thu thập, làm sạch và phân tích dữ liệu), sau đó báo cáo được chuyên gia đánh giá trước khi đưa ra quyết định đầu tư. Đây là mô hình AI tự động mà vẫn có chuyên gia bảo đảm độ tin cậy của kết quả. Các nền tảng như AnswerRocket, Athenic AI cho phép xử lý dữ liệu tự phục vụ và con người chỉ giám sát đầu ra<sup>31</sup>.

<sup>30</sup> Hal9 (2024), *Công cụ phân tích dữ liệu AI: Trợ lý thông minh gợi ý biểu đồ và trực quan hóa dữ liệu*, HashDork, <https://www.hashdork.com/vi/cong-cu-phan-tich-du-lieu-ai>, truy cập ngày 05/8/2025.

<sup>31</sup> Unite.AI (2025), *Top AI Tools for Data Analysts in 2025*, <https://www.unite.ai/vi/ai-tools-data-analysts>, truy cập ngày 05/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



### *Ứng dụng trí tuệ nhân tạo - Ảnh: Internet*

+ **Cấp độ 4:** Việc phân tích, tổng hợp dữ liệu thực hiện hoàn toàn bởi trí tuệ nhân tạo, không có sự giám sát của con người.

*Ví dụ:* Các hệ thống chuyên gia AI phân tích dữ liệu và đưa ra quyết định trong thời gian thực, ví dụ trong quản trị kho tự động hoặc điều chỉnh giá sản phẩm theo biến động thị trường tự động mà không cần can thiệp con người. Một trường hợp cụ thể là hệ thống AI như TechRadar Pro và Happy Loop dự báo tồn kho và tự động đặt hàng lại trong ngành bán lẻ tự động hoàn toàn<sup>32</sup>.

*- Trường hợp phải xin cấp Giấy chứng nhận đủ điều kiện kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu*

Theo Nghị định 169/2025/NĐ-CP, doanh nghiệp hoặc tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu cần phải xin cấp phép hoạt động, quản lý theo quy định của pháp luật trong các trường hợp sau:

<sup>32</sup> TechRadar (2024), *Transforming Dark Data into AI-Driven Business Value*, <https://www.techradar.com/pro/transforming-dark-data-into-ai-driven-business-value>, truy cập ngày 05/8/2025.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



## ***Giải pháp trí tuệ nhân tạo - Ảnh: Digitech Solution***

- + Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu thuộc nhóm cấp độ 3 hoặc 4 trong hệ thống thông tin của cơ quan nhà nước;
- + Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có khả năng gây ảnh hưởng đến an ninh quốc gia, quốc phòng, trật tự an toàn xã hội, đạo đức xã hội hoặc sức khỏe cộng đồng (dữ liệu chứa bí mật nhà nước,...);
- + Cung cấp các sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có kết nối, chia sẻ với cơ sở dữ liệu quốc gia hoặc cơ sở dữ liệu chuyên ngành (dữ liệu dân cư, y tế, tài chính công...);
- + Sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu có sử dụng dữ liệu cốt lõi hoặc dữ liệu quan trọng (như dữ liệu định danh, dữ liệu sinh trắc học,...).
- + Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu không thuộc các trường hợp trên gửi thông báo về Bộ Công an khi thực hiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu và được đề nghị Bộ Công an thẩm định, đánh giá để hưởng ưu đãi đối với sản phẩm, dịch vụ đó như các doanh nghiệp hoạt động trong lĩnh vực công nghệ cao, đổi mới sáng tạo, khởi





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

ng nghiệp sáng tạo, công nghiệp công nghệ số; chính sách ưu đãi phát triển hoạt động khoa học, công nghệ và đổi mới sáng tạo về dữ liệu bao gồm:

(1) Trợ lý ảo, hệ thống trí tuệ nhân tạo tạo sinh, hệ thống phân tích các nội dung tự động về video, hình ảnh, tin tức, bài viết và các sản phẩm, dịch vụ tương tự khác có tương tác trực tiếp đến bên sử dụng dịch vụ, có nguy cơ gợi ý, định hướng bên sử dụng dịch vụ đến các nội dung sai lệch;

(2) Các sản phẩm, dịch vụ phân tích, tổng hợp các dữ liệu nhạy cảm của cá nhân có quy mô dữ liệu từ 01 triệu cá nhân trở lên;

(3) Các sản phẩm, dịch vụ phân tích, tổng hợp cấp độ 3, cấp độ 4, thực hiện tự động trong các hệ thống công nghiệp, sản xuất chiếm 20% cơ cấu sử dụng trong ngành công nghiệp, sản xuất đó trở lên;

(4) Đạt quy mô nhất định về dữ liệu phục vụ huấn luyện mô hình phân tích, tổng hợp dữ liệu 10 TB dữ liệu trở lên.

Các quy định này nhằm đảm bảo hoạt động phân tích dữ liệu được kiểm soát chặt chẽ, tránh rủi ro lộ lọt thông tin hoặc lạm dụng dữ liệu nhạy cảm.

*- Điều kiện để được cấp phép kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu*

Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu phải đáp ứng các điều kiện sau để được cấp phép:

- + Là đơn vị sự nghiệp, doanh nghiệp được thành lập hợp pháp tại Việt Nam;
- + Người đứng đầu đơn vị sự nghiệp hoặc đại diện theo pháp luật của doanh nghiệp là công dân Việt Nam, thường trú trong nước, có trình độ đại học trở lên, có ít nhất 3 năm kinh nghiệm trong lĩnh vực quản lý dữ liệu và không thuộc một trong các trường hợp sau:

(1) Đã bị cơ quan tiến hành tố tụng khởi tố bị can;

(2) Đã bị kết án về các tội xâm phạm an ninh quốc gia hoặc các tội khác do lỗi cố ý bị kết án từ 03 năm tù trở lên chưa được xóa án tích; đang trong





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

thời gian được tạm hoãn chấp hành hình phạt tù; đang chấp hành hình phạt cải tạo không giam giữ; đang bị quản chế, cấm cư trú, cấm đảm nhiệm chức vụ, cấm kinh doanh ngành, nghề đầu tư kinh doanh có điều kiện theo quyết định của Tòa án;

**(3)** Đã bị xử phạt vi phạm hành chính trong lĩnh vực dữ liệu, an ninh mạng, công nghệ thông tin, giao dịch điện tử và chưa hết thời hạn được coi là chưa bị xử phạt vi phạm hành chính. Đang bị áp dụng các biện pháp xử lý hành chính hoặc đang trong thời gian chờ áp dụng biện pháp xử lý hành chính; đã bị áp dụng các biện pháp xử lý hành chính nhưng chưa đủ thời hạn để được coi là chưa bị áp dụng biện pháp xử lý hành chính.

+ Có đội ngũ cán bộ kỹ thuật chuyên trách gồm ít nhất 05 người có trình độ đại học trở lên và có một trong những chứng chỉ, chứng nhận về khoa học dữ liệu, phân tích dữ liệu, quản lý, quản trị dữ liệu, tư vấn, môi giới, xúc tiến thương mại; quản trị tài sản; thẩm định dữ liệu.

+ Có cơ sở vật chất, thiết bị công nghệ phù hợp với quy mô và phạm vi hoạt động kinh doanh;

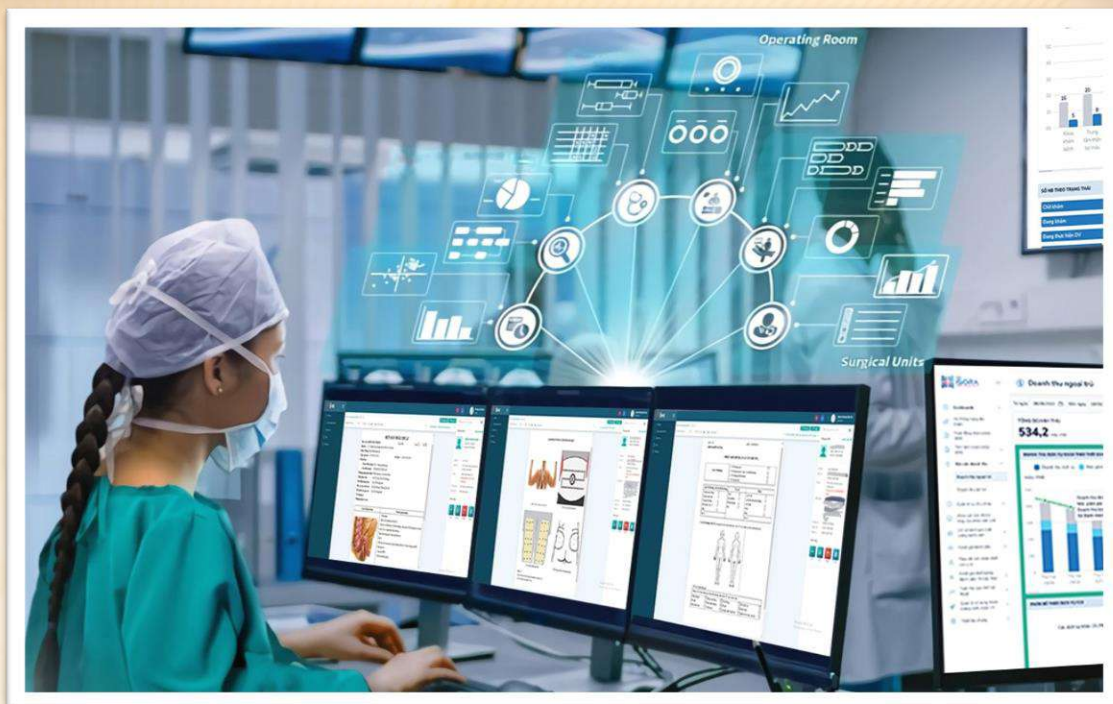
+ Có phương án kinh doanh rõ ràng, nêu rõ loại hình sản phẩm dự kiến cung cấp; phạm vi đối tượng cung cấp sản phẩm, dịch vụ; sự đáp ứng tiêu chuẩn, quy chuẩn kỹ thuật liên quan đối với từng loại sản phẩm, dịch vụ; các tính năng kỹ thuật cơ bản của sản phẩm, dịch vụ.

*Ví dụ:* Một công ty công nghệ tại Thành phố Hồ Chí Minh muốn cung cấp dịch vụ phân tích dữ liệu y tế cho bệnh viện (dữ liệu thuộc nhóm quan trọng, liên quan đến sức khỏe cộng đồng) sẽ cần đăng ký kinh doanh theo quy định, đồng thời đảm bảo các yêu cầu về nhân sự, cơ sở hạ tầng, tài chính và giấy phép kết nối cơ sở dữ liệu ngành y tế.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



## ***Dịch vụ phân tích dữ liệu y tế - Ảnh: Internet***

***- Xu hướng và triển vọng phát triển của công nghệ tổng hợp, phân tích dữ liệu***

***Thứ nhất, về xu hướng.*** Công nghệ tổng hợp, phân tích dữ liệu đang phát triển với tốc độ chưa từng có, mở ra nhiều xu hướng mới định hình tương lai ngành dữ liệu. Nổi bật nhất là sự trỗi dậy của *trí tuệ nhân tạo (AI)* và *học máy (machine learning)* trong mọi khía cạnh của quá trình phân tích từ xử lý, phân tích cho tới trình bày kết quả. Các hệ thống AI hiện đại có khả năng xử lý khối lượng dữ liệu khổng lồ và tìm ra mô thức phức tạp vượt quá khả năng của con người, giúp nâng cao độ chính xác và tính kịp thời của phân tích dữ liệu. Gartner dự báo đến năm 2025, phần lớn quy trình phân tích sẽ được “tăng cường” bởi AI, biến phân tích tăng cường (augmented analytics) thành dòng chủ lưu<sup>33</sup>. Điều này có nghĩa là AI sẽ tự động đảm

<sup>33</sup> Datagalaxy (2024), *Gartner's top 5 data & analytics predictions for 2025*, <https://www.datagalaxy.com/en/blog/gartners-top-data-predictions-for-2025/>, truy cập ngày 05/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

nhiệm nhiều công đoạn như làm sạch, chuẩn bị dữ liệu, phát hiện điểm bất thường, thậm chí tự động tạo ra báo cáo và giải thích kết quả, giúp ngay cả những người dùng không chuyên về dữ liệu cũng có thể khai thác phân tích nâng cao một cách dễ dàng. Xu hướng “*dân chủ hóa*” dữ liệu này sẽ mở rộng phạm vi người hưởng lợi từ phân tích dữ liệu, xây dựng văn hóa ra quyết định dựa trên dữ liệu sâu rộng trong tổ chức.



### ***Trí tuệ nhân tạo tạo sinh (Generative AI) - Ảnh: PACE***

Bên cạnh đó, sự bùng nổ của trí tuệ nhân tạo tạo sinh (Generative AI) và các mô hình ngôn ngữ lớn (LLM) đang tạo ra xu hướng mới trong trải nghiệm phân tích: phân tích hội thoại. Ngày nay đã xuất hiện các trợ lý ảo trả lời truy vấn dữ liệu bằng ngôn ngữ tự nhiên, giúp người dùng tương tác với dữ liệu giống như trò chuyện, thay vì phải biết ngôn ngữ truy vấn kỹ thuật<sup>34</sup>. Chẳng hạn, chatbot phân tích GenAI có thể cho phép người quản lý

<sup>34</sup> Sisense (2025), *Your guide to 2025 data and analytics megatrends*, <https://www.sisense.com/blog/data-analytics-megatrends-guide/>, truy cập ngày 05/8/2025.





doanh nghiệp hỏi đáp về số liệu kinh doanh trực tiếp bằng tiếng Việt và nhận được phân tích, giải thích một cách tức thì, trực quan. Gartner nhận định “làn sóng AI sẽ chạm đến mọi khía cạnh của quy trình phân tích, từ cách chúng ta chuẩn bị dữ liệu đến cách chúng ta tiêu thụ kết quả” [47]. Rõ ràng, AI hóa phân tích dữ liệu chính là xu hướng tất yếu, hứa hẹn nâng tầm chất lượng và hiệu quả của dịch vụ dữ liệu trong vài năm tới.

Song song với AI, xu hướng **điện toán đám mây (cloud computing)** đang định hình lại hạ tầng phân tích dữ liệu. Ngày càng nhiều doanh nghiệp và cơ quan Chính phủ chuyển các hệ thống dữ liệu lên đám mây để tận dụng khả năng lưu trữ linh hoạt và tính toán mở rộng gần như vô hạn. Cloud cho phép triển khai các nền tảng phân tích dữ liệu lớn (Big Data) mà không cần đầu tư hạ tầng máy chủ vật lý đắt đỏ, đồng thời dễ dàng tích hợp các dịch vụ AI/ML sẵn có trên mây. Tại Việt Nam, thị trường hạ tầng dữ liệu và dịch vụ đám mây đang bùng nổ. Quy mô thị trường trung tâm dữ liệu Việt Nam được dự báo đạt 1,04 tỷ USD vào năm 2028 và 1,27 tỷ USD vào năm 2030, với tốc độ tăng trưởng kép cao khoảng 10,8% mỗi năm. Điều này thể hiện nhu cầu mạnh mẽ về hạ tầng lưu trữ, xử lý dữ liệu trong nước, là nền tảng để phát triển các dịch vụ dữ liệu phức tạp hơn<sup>35</sup>. Chính phủ cũng đặt mục tiêu đến năm 2030, các nền tảng điện toán đám mây “*Make in Vietnam*” sẵn sàng đáp ứng 100% nhu cầu lưu trữ, kết nối, chia sẻ dữ liệu trong nước, đảm bảo an toàn, an ninh thông tin cho dữ liệu Việt Nam<sup>36</sup>. Xu hướng chuyển dịch lên cloud còn tạo điều kiện cho mô hình “*Dữ liệu như một dịch vụ*” (Data

<sup>35</sup> Nguyễn Anh Tuấn (2025), *Nghị định 169/2025/NĐ-CP và cơ hội cho các ngân hàng*, Cafef.vn, <https://cafef.vn/ngphi-dinh-169-2025-nd-cp-va-co-hoi-cho-cac-ngan-hang-188250714112857828.chn>, truy cập ngày 05/8/2025.

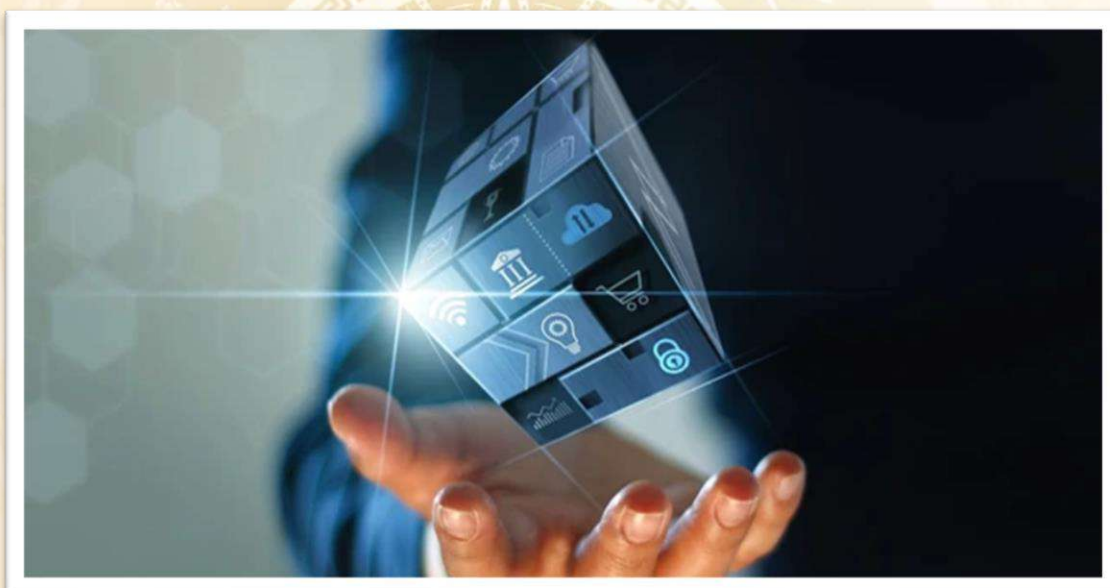
<sup>36</sup> Hoàng Cường (2024), *Chiến lược Dữ liệu quốc gia đến năm 2030 có gì đặc biệt?*, Báo Sức khỏe và Đời sống, <https://suckhoedoisong.vn/chien-luoc-du-lieu-quoc-gia-den-nam-2030-co-gi-dac-biet-169240203080851047.htm>, truy cập ngày 05/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

as a Service - DaaS) phát triển, theo đó các doanh nghiệp có thể thuê ngoài dịch vụ phân tích dữ liệu trên nền tảng đám mây thay vì tự vận hành. Điều này giảm chi phí đầu tư ban đầu, tăng tính linh hoạt và giúp ngay cả doanh nghiệp vừa và nhỏ cũng có thể tiếp cận các công nghệ phân tích hiện đại. Không chỉ hạ tầng, các công cụ phân tích dữ liệu trên mây (cloud analytics) cũng ngày càng phổ biến, cho phép người dùng thực hiện mọi thao tác từ trích xuất dữ liệu, xây dựng mô hình AI cho đến trực quan hóa kết quả ngay trên trình duyệt web. Có thể thấy, điện toán đám mây kết hợp dữ liệu lớn đang mở ra kỷ nguyên phân tích dữ liệu ở quy mô chưa từng có, hỗ trợ đắc lực quá trình chuyển đổi số toàn diện.



***Trí tuệ nhân tạo là xu hướng tất yếu của kỷ nguyên số - Ảnh: Internet***

Một xu hướng quan trọng khác là “**tự động hóa**” dịch vụ dữ liệu và sự ra đời của các nền tảng dữ liệu tự động. “**Tự động hóa**” ở đây bao gồm nhiều khía cạnh: tự động thu thập và cập nhật dữ liệu (nhờ IoT và sensor), tự động quản trị dữ liệu (“data pipeline” tự vận hành, ứng dụng DataOps), và đặc biệt là tự động phân tích, tạo báo cáo (như đã nói về augmented analytics). Các





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

dịch vụ dữ liệu tự động giúp giảm thiểu sự can thiệp thủ công, rút ngắn thời gian từ dữ liệu thô đến thông tin hữu ích. Ví dụ, trong quản trị doanh nghiệp hiện đại, một hệ thống phân tích tự động có thể hàng ngày tự kết nối với các nguồn dữ liệu (bán hàng, sản xuất, thị trường), làm sạch và tổng hợp theo các chỉ số kinh doanh, rồi tự động gửi báo cáo cho nhà quản lý vào mỗi sáng. Xu hướng này đòi hỏi ứng dụng các công nghệ như luồng xử lý dữ liệu thời gian thực (real-time streaming), xử lý ngôn ngữ tự nhiên để diễn giải dữ liệu, cùng các giải pháp tích hợp liên tục. Kết quả là dịch vụ phân tích dữ liệu trở nên tức thời, linh hoạt và sát nhu cầu hơn, hỗ trợ ra quyết định theo thời gian thực thay vì dựa trên báo cáo trễ nhiều ngày.



***Nâng cao hiệu quả ứng dụng công nghệ số trong điều hành,  
quản lý doanh nghiệp - Ảnh: Tạp chí Tài chính***

Ngoài ra, không thể không kể đến các xu hướng công nghệ khác đang và sẽ tác động mạnh đến lĩnh vực dữ liệu, như IoT (Internet vạn vật) tạo ra bùng nổ dữ liệu cảm biến; blockchain hỗ trợ chia sẻ dữ liệu minh bạch, chống giả mạo; điện toán biên (edge computing) giúp xử lý dữ liệu ngay tại nguồn;





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

hay data fabric - “*kiến trúc dữ liệu*” hợp nhất các nguồn dữ liệu rời rạc. Tất cả đều hướng tới mục tiêu chung là khai thác hiệu quả hơn lượng dữ liệu khổng lồ trong mọi lĩnh vực của nền kinh tế.



### ***Phân tích dữ liệu trong doanh nghiệp - Ảnh: Internet***

***Thứ hai, về triển vọng phát triển.*** Ngành dịch vụ phân tích, tổng hợp dữ liệu được dự báo sẽ tăng trưởng mạnh mẽ cả về quy mô thị trường lẫn mức độ trưởng thành. Theo một báo cáo thị trường, quy mô thị trường phân tích dữ liệu lớn toàn cầu năm 2023 khoảng 259,7 tỷ USD, dự kiến sẽ tăng lên 600 tỷ USD vào năm 2032 (tốc độ tăng trưởng trung bình khoảng 9,75%/năm). Đặc biệt, khu vực châu Á - Thái Bình Dương được dự báo là thị trường tăng trưởng nhanh nhất về phân tích dữ liệu lớn, có thể nắm giữ trên 40% dữ liệu toàn cầu vào 2025<sup>37</sup>. Điều này hàm ý các nước đang phát triển (trong đó có Việt Nam) sẽ chứng kiến nhu cầu rất lớn về dịch vụ dữ liệu khi quá trình số hóa diễn ra mạnh mẽ.

<sup>37</sup> Joshna (2025), *Big Data Analytics Adoption Rates by Sector*, Zoe Talent Solutions, <https://zoetalentsolutions.com/big-data-analytics-adoption-rates/>, truy cập ngày 05/8/2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Tại Việt Nam, triển vọng cho ngành dịch vụ dữ liệu cũng rất sáng sủa nhờ sự hỗ trợ từ chính sách và thị trường. Chiến lược dữ liệu quốc gia 2030 đặt mục tiêu phát triển thị trường dữ liệu là yếu tố đột phá, trong đó nhấn mạnh sẽ hoàn thành thí điểm 05 sàn giao dịch dữ liệu để tạo môi trường mua bán, trao đổi dữ liệu an toàn, tuân thủ pháp luật [36]. Những sàn dữ liệu này hứa hẹn thúc đẩy dòng chảy dữ liệu giữa các bên, tạo ra một thị trường mua bán dữ liệu sôi động, tạo tiền đề cho các dịch vụ dữ liệu phát triển. Bên cạnh đó, chiến lược cũng khuyến khích phát triển các dịch vụ dữ liệu mới (tổng hợp, phân tích, gắn nhãn dữ liệu...) nhằm tạo thêm nhiều cơ hội việc làm cho người dân, bao gồm cả người có hoàn cảnh khó khăn, người khuyết tật. Đây là một hướng phát triển mang tính nhân văn: biến dữ liệu thành lĩnh vực kinh tế thu hút nguồn nhân lực rộng rãi, xuất khẩu tri thức của lao động Việt Nam ra thế giới thông qua các công việc số.



***Việt Nam chính thức bước vào cuộc đua phát triển các chương trình  
trí tuệ nhân tạo tạo sinh (AI generative) - Ảnh: Vietnambiz***





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Với sự chuẩn bị kỹ lưỡng về hạ tầng (đầu tư trung tâm dữ liệu quốc gia, mạng 5G), thể chế pháp luật và nhân lực (các chương trình đào tạo chuyển đổi số, khoa học dữ liệu), Việt Nam được kỳ vọng sẽ bắt kịp các xu hướng công nghệ mới và xây dựng thành công ngành công nghiệp dữ liệu có tính cạnh tranh cao. Tóm lại, AI, điện toán đám mây và tự động hóa sẽ tiếp tục là những động lực chính, dẫn dắt sự phát triển của các sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu trong những năm tới, mở ra triển vọng tăng trưởng bùng nổ cho lĩnh vực này trong nền kinh tế số.

### *- Lợi ích của sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu*

Việc ứng dụng rộng rãi các sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu mang lại nhiều lợi ích to lớn về kinh tế và xã hội. Trước hết, **xét về lợi ích kinh tế**, phân tích dữ liệu giúp nâng cao hiệu quả hoạt động và năng lực cạnh tranh của doanh nghiệp, đóng góp trực tiếp vào tăng trưởng kinh tế. Khảo sát của BARC (Business Application Research Center) cho thấy các công ty khai thác dữ liệu lớn đã ghi nhận hàng loạt lợi ích: 69% doanh nghiệp báo cáo quyết định chiến lược tốt hơn, 54% cải thiện kiểm soát quy trình vận hành, 52% hiểu rõ khách hàng hơn và 47% cắt giảm chi phí<sup>38</sup>. Đáng chú ý, những tổ chức đo lường được hiệu quả từ phân tích dữ liệu cho biết doanh thu tăng trung bình 8% và chi phí giảm 10% so với trước [43]. Đây là các con số rất ấn tượng, phản ánh tỷ suất hoàn vốn (ROI) rõ rệt của các dự án phân tích dữ liệu. Ra quyết định dựa trên dữ liệu cũng giúp doanh nghiệp tránh được các sai lầm tốn kém, tối ưu phân bổ nguồn lực và nhanh nhạy nắm bắt cơ hội thị trường. Bên cạnh đó, ngành dịch vụ dữ liệu còn trực tiếp tạo ra doanh thu và việc làm mới trong nền kinh tế.

<sup>38</sup> BARC (2016), *Benefits of Big Data Analytics: Increased Revenues and Reduced Costs*, barc.com, <https://barc.com/big-data-benefits/>, truy cập ngày 06/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Ví dụ, báo cáo của Google 2024 ước tính nếu AI được ứng dụng rộng rãi, nó có thể mang lại lợi ích kinh tế khoảng 79,3 tỷ USD cho các doanh nghiệp Việt Nam vào năm 2030, tương đương gần 12% GDP năm 2030<sup>39</sup>. Đây là lợi ích gián tiếp từ việc nâng cao năng suất và thúc đẩy đổi mới nhờ AI/data, cho thấy tiềm năng đóng góp của phân tích dữ liệu vào tăng trưởng GDP là vô cùng to lớn. Không những vậy, dịch vụ dữ liệu còn mở ra một thị trường kinh doanh mới - thị trường dữ liệu - nơi dữ liệu trở thành hàng hóa có thể mua bán. Điều này tạo thêm nguồn thu cho các tổ chức sở hữu dữ liệu (ví dụ công ty có thể bán dữ liệu ẩn danh về hành vi khách hàng cho bên thứ ba phân tích), đồng thời làm giảm chi phí tiếp cận thông tin cho bên cần dữ liệu (thay vì tự thu thập). Một thị trường dữ liệu phát triển sẽ thúc đẩy cạnh tranh, khuyến khích nhiều doanh nghiệp tham gia cung cấp các dịch vụ giá trị gia tăng từ dữ liệu, từ đó đa dạng hóa nền kinh tế và tạo thêm việc làm chất lượng cao (các chuyên gia dữ liệu, kỹ sư AI,...).

**Về lợi ích xã hội**, phân tích, tổng hợp dữ liệu là công cụ đắc lực để giải quyết nhiều vấn đề quan trọng của xã hội hiện đại. Y tế và chăm sóc sức khỏe hưởng lợi lớn nhờ phân tích dữ liệu: các hệ thống phân tích hồ sơ bệnh án và dữ liệu dịch tễ giúp phát hiện sớm bệnh tật, nhận diện xu hướng sức khỏe cộng đồng, từ đó hỗ trợ cơ quan y tế đưa ra biện pháp phòng ngừa và điều trị hiệu quả hơn. Chẳng hạn, ứng dụng dữ liệu lớn giúp các nhà khoa học phát triển các mô hình chẩn đoán hình ảnh y khoa chính xác hơn và dự báo sớm diễn biến dịch bệnh như COVID-19 [68]. Quản lý đô thị và giao thông cũng cải thiện đáng kể nhờ dữ liệu: phân tích dữ liệu từ camera giao

<sup>39</sup> Minh Ngọc (2024), *Năm 2030: Lợi ích kinh tế từ AI có thể lên tới 79,3 tỷ USD*, Báo điện tử Chính phủ, <https://baochinhphu.vn/nam-2030-loi-ich-kinh-te-tu-ai-co-the-len-toi-793-ty-usd-102241115164254991.htm>, truy cập ngày 06/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

thông, GPS cho phép tối ưu hóa luồng giao thông, giảm kẹt xe (ví dụ Google Maps phân tích dữ liệu vị trí để chỉ dẫn tránh tắc đường, tiết kiệm hàng triệu giờ di chuyển cho người dân). Trong lĩnh vực môi trường, dữ liệu khí tượng thủy văn và mô hình phân tích giúp dự báo chính xác hơn về biến đổi khí hậu và thiên tai, hỗ trợ chính phủ có kế hoạch ứng phó kịp thời. Phân tích dữ liệu cũng được dùng để phân bổ nguồn lực tối ưu trong các chiến dịch xã hội: ví dụ dự án phân tích dữ liệu phân bổ muối và ký sinh trùng đã giúp một số quốc gia phân bổ nguồn lực phòng chống sốt rét hiệu quả hơn, tiết kiệm chi phí y tế [29].



### ***Hội thảo “Kiến tạo tương lai AI cho Việt Nam”***

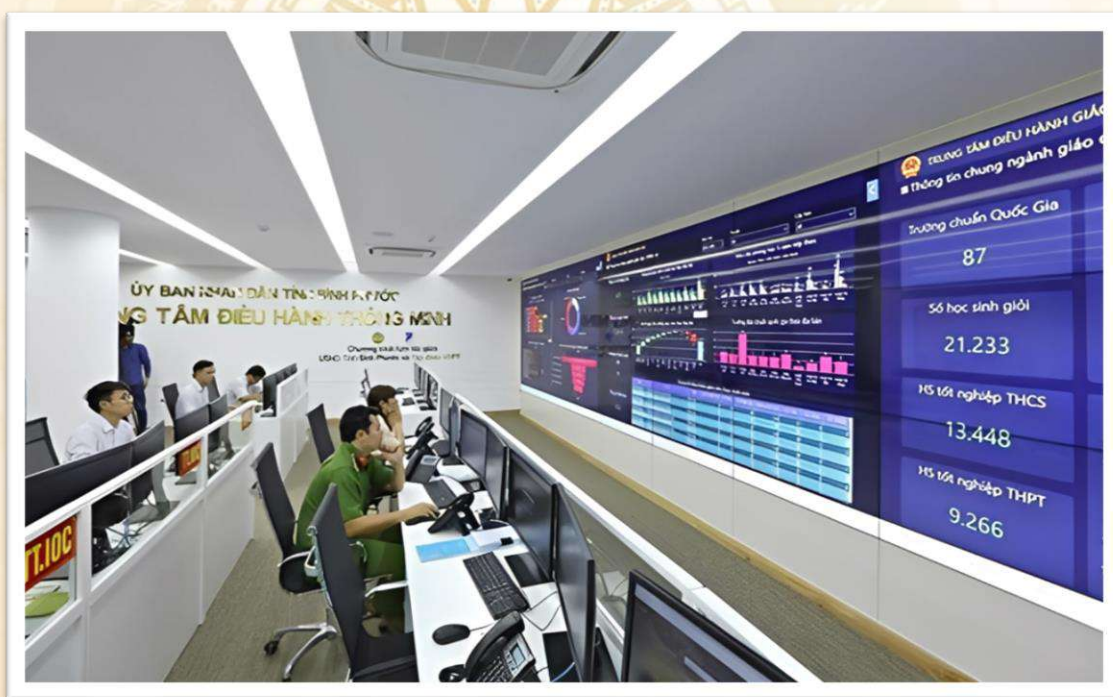
***do NIC phối hợp với Google tổ chức - Ảnh: Báo Điện tử Chính phủ***

Một đóng góp xã hội quan trọng khác của dữ liệu là tăng cường tính minh bạch và hiệu quả trong Quản lý nhà nước. Khi dữ liệu về hoạt động công được công khai và phân tích, chính quyền có thể giám sát và đánh giá chính sách tốt hơn, người dân cũng giám sát được chính quyền, từ đó giảm





tham nhũng và nâng cao niềm tin công chúng. Như phân tích ở trên, dữ liệu giúp giảm bất cân xứng thông tin giữa các chủ thể, làm minh bạch hóa thị trường và hệ thống hành chính [4]. Chương trình Chính phủ điện tử và Chuyển đổi số của Việt Nam đang triển khai mạnh mẽ các cơ sở dữ liệu quốc gia về dân cư, đất đai, bảo hiểm, doanh nghiệp..., khi kết nối liên thông sẽ cắt giảm đáng kể thủ tục hành chính, tiết kiệm thời gian và chi phí cho người dân (ví dụ: người dân, doanh nghiệp chỉ cần cung cấp thông tin một lần khi làm thủ tục, thay vì lặp lại nhiều lần). Dữ liệu mở được cung cấp cho người dân còn tạo điều kiện cho cộng đồng, doanh nghiệp cùng tham gia sáng tạo dịch vụ, đóng góp cho xã hội, chẳng hạn phát triển ứng dụng tra cứu giao thông, bản đồ dịch tễ trên nền dữ liệu mở của Chính phủ.



**Bộ Công an kết nối, ứng dụng dữ liệu trong giải quyết thủ tục hành chính,  
tạo điều kiện thuận lợi cho người dân - Ảnh: cand.com.vn.**

Một khía cạnh xã hội đáng lưu ý là thu hẹp khoảng cách số và tạo cơ hội phát triển đồng đều. Nếu được triển khai hiệu quả, phân tích dữ liệu có





thể giúp các khu vực kém phát triển tiếp cận tri thức và dịch vụ hiện đại mà trước đây chỉ thành thị mới có. Nhận thức được vấn đề này, Chính phủ Việt Nam đã thành lập Quỹ Phát triển Dữ liệu Quốc gia với vốn điều lệ tối thiểu 1.000 tỷ đồng nhằm hỗ trợ nghiên cứu, phát triển hạ tầng dữ liệu, ứng dụng công nghệ mới (AI, Big Data, blockchain) đặc biệt tại các vùng nông thôn, miền núi, hải đảo, kỳ vọng rút ngắn khoảng cách số giữa các vùng miền<sup>40</sup>. Hơn nữa, việc phát triển các dịch vụ dữ liệu như gán nhãn dữ liệu, nhập liệu, kiểm thử AI có thể tạo việc làm trực tuyến cho người lao động ở vùng sâu vùng xa hoặc người khuyết tật - những đối tượng khó tham gia thị trường lao động truyền thống.

Từ những phân tích trên, có thể thấy rằng, sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu mang lại lợi ích kép: kinh tế (tăng hiệu quả, doanh thu, thúc đẩy đổi mới, đóng góp GDP, tạo ngành kinh doanh mới...) và xã hội (cải thiện dịch vụ công, giải quyết vấn đề y tế, môi trường, thu hẹp khoảng cách phát triển...). Những lợi ích này giải thích vì sao cả khu vực công và tư đều đang đầu tư mạnh mẽ vào dữ liệu, coi đó là “*chìa khóa*” để đạt các mục tiêu phát triển kinh tế xã hội trong kỷ nguyên số.

#### **7.1.4.4. Về sản dữ liệu**

*- Sản dữ liệu được quy định như thế nào kể từ ngày 01/7/2025?*

Luật Dữ liệu 2024 đã đưa ra định nghĩa chính thức về “**sản dữ liệu**” (hay sản giao dịch dữ liệu) tại Điều 42, đánh dấu lần đầu tiên khung pháp luật Việt Nam ghi nhận mô hình này. Theo đó, sản dữ liệu được hiểu là môi trường để giao dịch, trao đổi dữ liệu và các sản phẩm, dịch vụ liên quan đến

<sup>40</sup> Hồng Minh (2025), *Luật Dữ liệu xây dựng niềm tin số và thúc đẩy chuyển đổi số toàn diện*, Báo Nhân Dân, <https://nhandan.vn/luat-du-lieu-xay-dung-niem-tin-so-va-thuc-day-chuyen-doi-so-toan-dien-post890961.html>, truy cập ngày 06/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

dữ liệu, cung cấp tài nguyên liên quan đến dữ liệu để phục vụ nghiên cứu, phát triển khởi nghiệp, đổi mới sáng tạo,... qua đó thúc đẩy hình thành thị trường dữ liệu, hỗ trợ phát triển sản phẩm dịch vụ dựa trên dữ liệu, các giao dịch thương mại trên môi trường số được thường xuyên, liên tục, an toàn và minh bạch hơn. Theo Chiến lược dữ liệu quốc gia đến năm 2030, Việt Nam sẽ hoàn thành thí điểm, thử nghiệm 5 sản phẩm dịch vụ dữ liệu nhằm tạo ra thị trường minh bạch để chia sẻ và khai thác dữ liệu. Định nghĩa này tương đồng với khái niệm sản phẩm dịch vụ dữ liệu trên thế giới ở chỗ nhấn mạnh chức năng làm cầu nối giữa bên cung cấp và bên sử dụng dữ liệu, cho phép dữ liệu được lưu thông như một loại hàng hóa đặc biệt trong nền kinh tế số.

Một điểm đáng chú ý trong Luật Dữ liệu 2024 là quy định về chủ thể được phép vận hành sản phẩm dữ liệu. Khác với nhiều lĩnh vực khác có thể do tư nhân đảm nhiệm, luật giới hạn *tổ chức cung cấp dịch vụ sản phẩm dữ liệu* phải là đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước đáp ứng điều kiện và được cấp phép thành lập hợp pháp. Điều này có nghĩa là hiện tại “*khu vực nhà nước*” nắm vai trò chính trong việc tổ chức sản phẩm dịch vụ dữ liệu, phản ánh quan điểm quản lý thận trọng đối với một lĩnh vực mới mẻ và nhạy cảm như dữ liệu. Trên thực tế, đây được coi là ngành nghề kinh doanh có điều kiện, nhằm đảm bảo sản phẩm dữ liệu hoạt động dưới sự giám sát chặt chẽ về an ninh dữ liệu. Một số ý kiến trong quá trình soạn thảo luật từng đề xuất mở rộng cho khu vực tư nhân tham gia nếu đáp ứng các yêu cầu an toàn dữ liệu, thay vì giới hạn chỉ doanh nghiệp nhà nước, đơn vị sự nghiệp công. Tuy nhiên, phương án cuối cùng được thông qua vẫn giữ giới hạn này, chí ít là trong giai đoạn khởi đầu hình thành thị trường dữ liệu.





***Quỹ phát triển dữ liệu quốc gia bảo đảm nguyên tắc không vì mục đích lợi nhuận; quản lý, sử dụng đúng mục đích, đúng pháp luật, kịp thời, hiệu quả, bảo đảm công khai, minh bạch - Ảnh: VGP/LS***

Bên cạnh việc đưa ra khái niệm, Luật Dữ liệu cũng đặt ra giới hạn về loại dữ liệu được phép giao dịch trên sàn nhằm bảo vệ lợi ích công cộng và quyền riêng tư. Cụ thể, những loại dữ liệu bị cấm giao dịch bao gồm:

- (1) Dữ liệu có thể gây nguy hại đến quốc phòng, an ninh, đối ngoại, cơ yếu;
- (2) Dữ liệu cá nhân mà không được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác;
- (3) Các loại dữ liệu khác bị cấm giao dịch theo quy định pháp luật.

Quy định này hướng đến ngăn chặn việc mua bán các dữ liệu nhạy cảm (bí mật nhà nước, thông tin liên quan đến an ninh quốc gia) hoặc dữ liệu cá nhân khi chưa có sự cho phép, qua đó cân bằng giữa mục tiêu thúc đẩy chia sẻ dữ liệu với yêu cầu bảo vệ an ninh và quyền riêng tư của xã hội.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Ngoài ra, trong bối cảnh Luật Dữ liệu phân loại dữ liệu thành các nhóm như dữ liệu cốt lõi, dữ liệu quan trọng (liên quan trực tiếp an ninh quốc gia, lợi ích công cộng), việc cấm giao dịch những dữ liệu này trên sàn là hoàn toàn phù hợp để kiểm soát rủi ro.

### *- Hoạt động của sàn dữ liệu*



Ngay sau khi Luật Dữ liệu được ban hành, Chính phủ đã kịp thời ban hành Nghị định 169/2025/NĐ-CP để quy định chi tiết về sàn dữ liệu cũng như các sản phẩm, dịch vụ dữ liệu khác. Nghị định này quy định cụ thể những hoạt động mà sàn dữ liệu được phép thực hiện, qua đó phác họa rõ hơn mô hình vận hành của sàn dữ liệu trong thực tế. Theo Điều 32 Nghị định 169/2025/NĐ-CP, hoạt động của sàn dữ liệu gồm hai nhóm chính:

**Một là, cung cấp tài nguyên dữ liệu.** Sàn dữ liệu làm nhiệm vụ tập hợp và cung cấp các nguồn dữ liệu số phục vụ cho nghiên cứu khoa học, phát triển sản phẩm khởi nghiệp và hoạt động đổi mới sáng tạo. Các tài nguyên này bao gồm (dữ liệu có trong các cơ sở dữ liệu chuyên ngành và cơ sở dữ liệu quốc gia, và dữ liệu do các cơ quan, tổ chức, cá nhân khác cung cấp).





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Nói cách khác, sản dữ liệu đóng vai trò như một kho dữ liệu tập trung, nơi tích hợp dữ liệu từ nhiều nguồn (cả nhà nước và tư nhân) để người dùng có thể tiếp cận thuận tiện.



***Sản dữ liệu sẽ cung cấp “nhiên liệu”  
để phát triển khoa học, công nghệ - Ảnh: VnEconomy***

**Hai là, cung cấp các dịch vụ liên quan đến dữ liệu.** Bên cạnh việc cung ứng dữ liệu thô, sản dữ liệu còn cung cấp nhiều loại hình dịch vụ trung gian nhằm hỗ trợ quá trình giao dịch dữ liệu hiệu quả và an toàn. Cụ thể, sản có thể cung cấp dịch vụ chào mua, chào bán dữ liệu, dịch vụ môi giới, tư vấn, đại diện, định giá dữ liệu, dịch vụ đấu giá dữ liệu, cũng như dịch vụ đảm bảo môi trường kỹ thuật để các bên thực hiện giao dịch, trao đổi dữ liệu. Đây là các dịch vụ quan trọng giúp kết nối cung cầu dữ liệu, sản có thể hỗ trợ bên bán định giá bộ dữ liệu, hoặc đứng ra tổ chức phiên đấu giá dữ liệu một cách chuyên nghiệp. Việc cung cấp hạ tầng và dịch vụ như vậy giúp giảm chi phí giao dịch và tăng tính minh bạch cho thị trường dữ liệu.

Như vậy, có thể hình dung sản dữ liệu hoạt động tương tự một sàn giao dịch thương mại điện tử nhưng mặt hàng ở đây là dữ liệu và dịch vụ dữ liệu. Sản vừa là nơi niêm yết các “sản phẩm dữ liệu” để bên mua tìm kiếm, vừa





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

có các dịch vụ hỗ trợ giao dịch (môi giới, đấu giá, thanh toán, xác thực...) nhằm tạo thuận lợi cho các bên. Tất cả hoạt động này diễn ra trong môi trường trực tuyến có sự quản lý, giám sát để đảm bảo tuân thủ chính sách pháp luật về dữ liệu.

### *- Quy định về giao dịch dữ liệu trên sàn*

Điều 33 Nghị định 169/2025/NĐ-CP đặt ra một số quy tắc quan trọng về giao dịch trên sàn dữ liệu, định hướng cách thức mà dữ liệu được mua bán, trao đổi qua sàn:

**Một là**, cơ chế giá cả trên sàn dữ liệu tuân theo nguyên tắc thị trường. Tức là giá của các sản phẩm, dịch vụ dữ liệu sẽ được hình thành dựa trên cung - cầu, có cạnh tranh, thương lượng giữa bên mua và bán. Sàn dữ liệu hoặc các tổ chức định giá chuyên nghiệp có thể tham gia hỗ trợ định giá dữ liệu theo nhu cầu, nhưng không áp đặt giá cố định. Quy định này nhằm đảm bảo việc mua bán dữ liệu diễn ra linh hoạt, phản ánh giá trị thực của dữ liệu trên thị trường, thay vì do nhà nước ấn định.

**Hai là**, trách nhiệm xác thực và thẩm định. Các dữ liệu giao dịch qua sàn phải bảo đảm tính xác thực về nguồn gốc, có nghĩa là xuất xứ, độ tin cậy của dữ liệu cần được kiểm chứng trước khi đem ra giao dịch. Tổ chức vận hành sàn hoặc một bên chuyên môn (nếu được chỉ định) có trách nhiệm xác thực nguồn gốc dữ liệu đó. Đồng thời, sàn cũng phải thẩm định các sản phẩm, dịch vụ dữ liệu đưa lên niêm yết nhằm bảo đảm tuân thủ quy định pháp luật như kiểm tra xem dữ liệu có thuộc loại cấm giao dịch hay vi phạm quyền riêng tư không. Những yêu cầu này giúp nâng cao niềm tin của các bên khi tham gia sàn, bởi tính xác thực và hợp pháp của dữ liệu là yếu tố then chốt trong giao dịch dữ liệu - người mua cần tin rằng dữ liệu mua được là đáng tin cậy, còn người bán phải tuân thủ pháp luật khi chia sẻ dữ liệu.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

**Ba là,** yêu cầu bắt buộc giao dịch qua sàn: Nghị định quy định các cơ quan, tổ chức, doanh nghiệp khi cung cấp sản phẩm, dịch vụ về dữ liệu phải thực hiện thông qua sàn dữ liệu đã được cấp phép, trừ trường hợp pháp luật có quy định khác. Quy định này hàm ý rằng sàn dữ liệu được xem là kênh chính thống để mua bán dữ liệu, hạn chế tình trạng giao dịch “chợ đen” tự phát ngoài luồng. Với việc tập trung giao dịch qua sàn, nhà nước có thể theo dõi, quản lý tốt hơn hoạt động mua bán dữ liệu, đảm bảo tuân thủ các tiêu chuẩn an toàn và pháp lý. Tất nhiên, luật vẫn chừa ngoại lệ nếu pháp luật chuyên ngành có quy định khác (ví dụ một số dữ liệu đặc thù có thể trao đổi theo cơ chế riêng), nhưng nhìn chung nguyên tắc là khuyến khích và bắt buộc đưa giao dịch dữ liệu lên sàn tập trung.

**Bốn là,** Nghị định tái khẳng định và cụ thể hóa danh mục dữ liệu cấm giao dịch trên sàn. Tại khoản 6, điều 33 đã liệt kê các loại dữ liệu sau không được phép đưa lên sàn:

- (1) Dữ liệu thuộc danh mục dữ liệu cốt lõi, dữ liệu quan trọng;
- (2) Dữ liệu không được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác;
- (3) Dữ liệu khác bị pháp luật cấm giao dịch.

Danh mục này về cơ bản tương đồng với Luật Dữ liệu 2024 đã nêu, nhưng dùng thuật ngữ “*dữ liệu cốt lõi, dữ liệu quan trọng*” để phù hợp với phân loại chính thức trong luật. Ví dụ, thông tin bí mật quốc phòng hay dữ liệu về an ninh quốc gia sẽ được xếp vào dữ liệu cốt lõi và bị cấm mua bán. Việc nhắc lại điều cấm này trong Nghị định nhằm nhấn mạnh tầm quan trọng và yêu cầu các sàn phải tuân thủ tuyệt đối. Đây chính là những “*lằn ranh đỏ*” để đảm bảo sàn dữ liệu không trở thành nơi tuồn ra những dữ liệu nhạy cảm, trái phép.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Ngoài ra, Nghị định còn đề cập cơ chế đặc thù khi cơ quan nhà nước cung cấp dữ liệu trên sàn: các dữ liệu công nếu giao dịch có thể thu phí theo giá do pháp luật quy định và nếu bán đấu giá thì giá khởi điểm không thấp hơn chi phí đầu vào để có dữ liệu đó. Điều này khuyến khích các “*cơ quan công quyền*” chia sẻ dữ liệu (theo chiến lược dữ liệu mở) nhưng đồng thời đảm bảo giá trị dữ liệu công không bị định giá quá thấp, gây thất thoát tài sản công.

Tóm lại, các quy định giao dịch trên sàn dữ liệu đã thiết lập hàng loạt các quy tắc rõ ràng: giá cả theo thị trường, dữ liệu phải xác thực và hợp pháp, các bên hầu như phải giao dịch qua sàn để được quản lý, và tuyệt đối không mua bán dữ liệu nhạy cảm bị cấm. Khung quy tắc này vừa tạo điều kiện cho thị trường dữ liệu phát triển lành mạnh, vừa bảo vệ lợi ích quốc gia, doanh nghiệp và người dân trong quá trình trao đổi dữ liệu.



***Sàn giao dịch dữ liệu giúp minh bạch***

***và hợp thức hóa mua bán dữ liệu - Ảnh: VnEconomy***

***- Điều kiện cấp Giấy chứng nhận đủ điều kiện kinh doanh sàn dữ liệu***

Do sàn dữ liệu là loại hình kinh doanh mới và tiềm ẩn nhiều yếu tố nhạy cảm, pháp luật đặt ra điều kiện chặt chẽ để một tổ chức có thể được cấp phép





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

hoạt động sản dữ liệu. Điều 34 Nghị định 169/2025/NĐ-CP quy định cụ thể các điều kiện cấp Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sản dữ liệu, tập trung vào bốn nhóm chính: *loại hình tổ chức, nhân sự, cơ sở hạ tầng, kỹ thuật và giấy phép bổ sung* (nếu có hoạt động đặc thù).

## TÓM TẮT CÁC ĐIỀU KIỆN ĐỂ ĐƯỢC CẤP GIẤY CHỨNG NHẬN ĐỦ ĐIỀU KIỆN KINH DOANH SẢN DỮ LIỆU

| Điều kiện về   | Yêu cầu cụ thể                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Chủ thể</b> | Phải là đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước được thành lập và hoạt động hợp pháp tại Việt Nam. <i>(Lưu ý: Hiện chưa cho phép doanh nghiệp tư nhân thuần túy vận hành sản dữ liệu).</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Nhân sự</b> | <ul style="list-style-type: none"><li>- <b>Lãnh đạo:</b> Người đứng đầu tổ chức (hoặc người đại diện pháp luật của doanh nghiệp) phải có trình độ đại học trở lên, trực tiếp tham gia quản lý tại các trung tâm dữ liệu, có ít nhất 3 năm kinh nghiệm liên quan đến quản lý dữ liệu, và không thuộc diện bị cấm (như không có tiền án về an ninh quốc gia, không bị truy cứu hình sự,...).</li><li>- <b>Đội ngũ chuyên môn:</b> Có tối thiểu 05 nhân viên trình độ đại học trở lên, trong đó ít nhất 40% là nhân sự chính thức của tổ chức và ít nhất 30% có chứng chỉ/chứng nhận hoàn thành khóa học về các lĩnh vực liên quan khoa học dữ liệu, phân tích dữ liệu, quản trị dữ liệu, môi giới dữ liệu, thẩm định dữ liệu,...</li></ul> |





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

| Điều kiện về                                                                                             | Yêu cầu cụ thể                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cơ sở hạ tầng, kỹ thuật, quy trình quản lý cung cấp dịch vụ và phương án bảo đảm an ninh, trật tự</b> | <p>- <b>Hạ tầng đặt tại Việt Nam:</b> Hệ thống máy chủ, trung tâm dữ liệu của sản phẩm phải được đặt trên lãnh thổ Việt Nam, đáp ứng các tiêu chuẩn kiểm định về an ninh, an toàn thông tin theo quy định.</p> <p>- <b>Đề án hoạt động:</b> Tổ chức phải xây dựng Đề án hoạt động sản dữ liệu chi tiết, bao gồm các phương án kỹ thuật và quản lý quan trọng: phương án vận hành hệ thống công nghệ thông tin, phương án công nghệ, phương án lưu trữ và đảm bảo tính toàn vẹn, bảo mật dữ liệu, phương án bảo vệ dữ liệu khách hàng, phương án đảm bảo an ninh trật tự, phương án thanh toán, phương án thẩm định dữ liệu, phương án định danh và xác thực điện tử, cũng như phòng cháy và chữa cháy, dự phòng thảm họa và bảo đảm vận hành ổn định, thông suốt; ngoài ra, còn phải thuyết minh về trang thiết bị kỹ thuật được sử dụng.</p> |
| <b>Điều kiện bổ sung (nếu có)</b>                                                                        | Trường hợp có triển khai hoạt động đấu giá dữ liệu, tổ chức vận hành sản phẩm có giấy phép cung cấp dịch vụ đấu giá tài sản do cơ quan có thẩm quyền cấp theo pháp luật về đấu giá tài sản.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Nhìn vào bảng trên có thể thấy, yêu cầu đặt ra khá toàn diện nhằm đảm bảo chỉ những tổ chức có năng lực và uy tín mới được vận hành sản dữ liệu. Việc giới hạn loại hình tổ chức (phải là doanh nghiệp nhà nước hoặc đơn vị sự nghiệp công lập) một lần nữa nhấn mạnh sự thận trọng của nhà làm luật, vì khu





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

vực công thường có tiềm lực và trách nhiệm cao hơn trong việc bảo đảm an ninh, an toàn dữ liệu. Yêu cầu về nhân sự cho thấy sản dữ liệu đòi hỏi chuyên môn liên ngành: không chỉ hiểu biết kỹ thuật dữ liệu mà còn về quản trị, môi giới, thẩm định, qua đó phản ánh tính chất phức tạp của việc kinh doanh dữ liệu: *vừa là dịch vụ công nghệ, vừa liên quan đến pháp lý, thương mại.*

Điều kiện về cơ sở hạ tầng kỹ thuật và đề án hoạt động là điểm nhấn quan trọng khác. Dữ liệu số có thể coi là một dạng “*tài sản số*” đòi hỏi hạ tầng bảo vệ tương xứng, nên pháp luật bắt buộc sản dữ liệu phải có máy chủ đặt trong nước và qua kiểm định an ninh mạng. Điều này nhằm phòng ngừa rủi ro dữ liệu bị đặt ngoài tầm kiểm soát (chẳng hạn đặt máy chủ ở nước ngoài có thể gây khó khăn cho quản lý và an ninh). Đồng thời, việc yêu cầu một đề án hoạt động chi tiết với hàng loạt phương án cho mọi tình huống (từ bảo mật, an toàn, đến phòng cháy chữa cháy, xử lý thảm họa) cho thấy nhà quản lý muốn đảm bảo sản dữ liệu vận hành ổn định, an toàn tuyệt đối trước khi cho phép mở cửa. Thực tế, đây là những tiêu chuẩn thường thấy đối với các sản giao dịch quan trọng như sản chứng khoán, sản tiền tệ,... nay được áp dụng cho sản dữ liệu do tầm quan trọng không kém của nó trong nền kinh tế số.

Cuối cùng, nếu sản dữ liệu có chức năng đấu giá dữ liệu, thì phải đáp ứng thêm yêu cầu về giấy phép đấu giá tài sản. Điều này dễ hiểu vì hoạt động đấu giá đòi hỏi những quy trình minh bạch riêng và thường phải do đơn vị có chức năng đấu giá thực hiện. Quy định này nhằm phòng ngừa, ngăn chặn việc các sản dữ liệu tự ý tổ chức đấu giá khi chưa có kinh nghiệm hoặc giấy phép phù hợp, tránh rủi ro cho người tham gia.

*Về thẩm quyền cấp phép*, Bộ Công an là cơ quan cấp Giấy chứng nhận đủ điều kiện kinh doanh sản dữ liệu. Bộ Công an cũng là đơn vị chủ trì quản lý nhà nước về dữ liệu (trừ lĩnh vực quốc phòng) theo Luật Dữ liệu, cho thấy

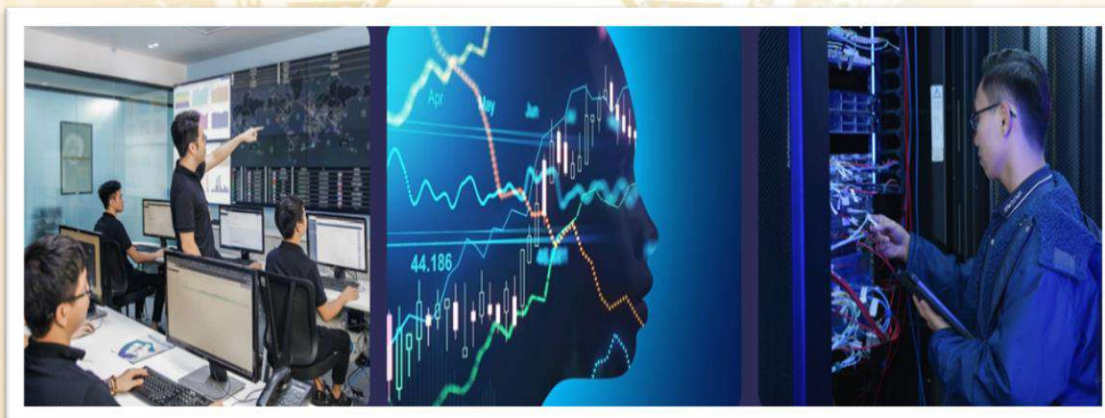




## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

vai trò đặc biệt trong giám sát hoạt động liên quan đến dữ liệu. Sau khi được cấp phép, tổ chức vận hành sàn dữ liệu sẽ phải tuân thủ chế độ báo cáo định kỳ và chịu sự thanh tra, kiểm tra của các cơ quan chức năng nhằm đảm bảo duy trì các điều kiện kinh doanh và xử lý kịp thời vi phạm (nếu có).

*Sự ra đời của sàn dữ liệu trong khung khổ pháp lý Việt Nam* là một bước đi chiến lược nhằm kiến tạo thị trường dữ liệu minh bạch, an toàn. Với định nghĩa và quy chế hoạt động được xác lập trong Luật Dữ liệu 2024 và Nghị định 169/2025/NĐ-CP, sàn dữ liệu được kỳ vọng sẽ trở thành nền tảng kết nối giữa các bên sở hữu dữ liệu và bên có nhu cầu khai thác dữ liệu, từ đó thúc đẩy dòng chảy dữ liệu cho các hoạt động kinh tế số, nghiên cứu khoa học và đổi mới sáng tạo. Những quy định chặt chẽ về điều kiện kinh doanh cho thấy Nhà nước ta đặc biệt coi trọng việc đảm bảo an ninh dữ liệu và quyền riêng tư, cũng như duy trì sự ổn định, tin cậy của môi trường giao dịch dữ liệu ngay từ buổi đầu hình thành.



***Sàn dữ liệu là một bộ phận quan trọng góp phần mở cánh cửa  
“thị trường dữ liệu” tại Việt Nam - Ảnh: VnEconomy***

Trong tương lai gần, Việt Nam đặt mục tiêu thí điểm 5 sàn giao dịch dữ liệu từ nay đến năm 2030 như một phần của Chiến lược dữ liệu quốc gia. Sàn dữ liệu hứa hẹn sẽ mở ra những cơ hội mới cho việc chia sẻ tài nguyên





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

dữ liệu giữa các cơ quan nhà nước với nhau và giữa khu vực công - tư, tối ưu hóa việc khai thác “*dầu mỏ số*” phục vụ phát triển kinh tế, xã hội. Đồng thời, thách thức không nhỏ cũng đặt ra là làm thế nào để vận hành sàn dữ liệu hiệu quả, thu hút được nguồn cung dữ liệu chất lượng và nhu cầu mua dữ liệu thực sự, trong khi vẫn kiểm soát tốt rủi ro về bảo mật và tuân thủ pháp luật.

Kinh nghiệm quốc tế chỉ ra rằng không phải sàn dữ liệu nào ra đời cũng thành công, nhiều mô hình đã thất bại do khó khăn về kỹ thuật, pháp lý và thiếu niềm tin thị trường. Do đó, chặng đường phía trước đòi hỏi sự phối hợp chặt chẽ giữa cơ quan quản lý và các đơn vị vận hành sàn để vừa phát triển thị trường dữ liệu, vừa đảm bảo an ninh, an toàn trong kỷ nguyên số. Với nền móng pháp lý hiện có và quyết tâm từ Chính phủ, hy vọng rằng sàn dữ liệu sẽ sớm đi vào thực tiễn một cách suôn sẻ, trở thành đòn bẩy cho kinh tế số Việt Nam, đúng như tiềm năng mà nó hứa hẹn.

*- Các mô hình sàn giao dịch dữ liệu hiện nay trên thế giới đang vận hành như thế nào?*

Trung Quốc là đất nước tiên phong thiết lập các sàn giao dịch dữ liệu, nhưng họ cũng phải “*vừa làm vừa điều chỉnh*”, chứ chưa thể tạo ra một mô hình chuẩn mực để các quốc gia khác đi theo. Khung pháp lý dù đã khá chặt chẽ, nhưng hiệu quả hoạt động của các sàn này vẫn đang được thử nghiệm để tìm ra công thức tối ưu. Trước năm 2021, sự thiếu vắng các luật về an ninh dữ liệu và quyền riêng tư khiến cả người mua lẫn người bán chưa tin tưởng vào hệ thống, nhiều công ty ngại đưa dữ liệu lên sàn do lo ngại vấn đề định giá và quyền sở hữu. Hệ quả là phần lớn giao dịch dữ liệu diễn ra phi chính thức, trên “*chợ đen*” với quy mô ước tính tới 150 tỷ Nhân Dân Tệ trong năm 2021. Từ năm 2021 trở đi, Trung Quốc ban hành loạt đạo luật nền





tăng (Luật An ninh Dữ liệu, Luật Bảo vệ Thông tin Cá nhân) và thành lập Cục Quản lý Dữ liệu Quốc gia để quản lý tập trung tài nguyên dữ liệu và hoạt động giao dịch. Các sàn giao dịch thể hệ mới được đưa vào khuôn khổ quản lý chặt chẽ hơn - đa số thuộc sở hữu hoặc chịu kiểm soát của nhà nước, vận hành như các đơn vị bán công với vai trò kép vừa là nhà môi giới, vừa là cơ quan giám sát quá trình giao dịch. Chẳng hạn, Sàn Dữ liệu Quý Dương từng thuộc tư nhân đã được cơ cấu lại thành doanh nghiệp 100% nhà nước. Ban quản lý sàn chịu trách nhiệm xác thực người mua, người bán, kiểm tra tuân thủ, đánh giá an ninh và bảo vệ thông tin cá nhân trước khi cho phép giao dịch. Nhiều sàn đã ban hành quy tắc riêng, quy định danh mục dữ liệu cấm giao dịch và tiêu chuẩn kỹ thuật cho quá trình trao đổi<sup>41</sup>.

Đến giữa năm 2023, một số sàn dữ liệu lớn của Trung Quốc bắt đầu ghi nhận kết quả khả quan với doanh số giao dịch vượt 1 tỷ NDT mỗi sàn (như Thâm Quyển, Quý Dương, Quảng Châu) - cải thiện đáng kể so với con số vài triệu trước đây. Tuy vậy, con số này vẫn rất nhỏ bé so với quy mô thị trường dữ liệu tiềm năng của Trung Quốc. Nhiều bài toán thách thức vẫn còn đó: xác định quyền sở hữu và quyền sử dụng dữ liệu (nhất là khi dữ liệu được coi là loại hàng hóa đặc thù, có tính chất công cộng một phần), phương pháp định giá dữ liệu hợp lý, và quan trọng nhất là xây dựng niềm tin giữa các bên. Trung Quốc đang thử nghiệm các giải pháp công nghệ như *chuỗi khối (blockchain)*, *điện toán tin cậy* (kỹ thuật ẩn danh dữ liệu, liên minh) nhằm đảm bảo nguồn gốc và quá trình sử dụng dữ liệu được ghi lại minh bạch theo phương châm “*dữ liệu có thể dùng nhưng không thể nhìn*”. Bên

<sup>41</sup> Alex He và Rebecca Arcesati (2024), *Data Marketplaces and Governance: Lessons from China*, Centre for International Governance Innovation, <https://www.cigionline.org/articles/data-marketplaces-and-governance-lessons-from-china/>, truy cập ngày 06/8/2025.





cạnh đó, chính quyền và hiệp hội ngành nghề cũng đưa ra hướng dẫn định giá dữ liệu: kết hợp cả chi phí tạo lập dữ liệu, giá trị kinh tế tương lai và cung cầu thị trường để hình thành mức giá tham chiếu. Một ví dụ điển hình về nỗ lực tạo niềm tin là Sàn Dữ liệu Thâm Quyển: sàn này đã môi giới thành công khoản vay giữa Ngân hàng Quang Đại Thâm Quyển và công ty hạ tầng AI Thâm Quyển Weiyuan, dựa trên bộ sản phẩm dữ liệu của công ty này được niêm yết trên sàn. Giao dịch được hỗ trợ bởi hệ sinh thái các bên thứ ba (hãng luật, đơn vị thẩm định chất lượng dữ liệu,...) do sàn quy tụ, giúp xác minh quyền dữ liệu và định giá công bằng, từ đó thuyết phục các bên thực hiện giao dịch mà trước đây có thể đã không xảy ra [50].

Có thể thấy rằng, Trung Quốc nhận ra tầm quan trọng của dữ liệu từ rất sớm, xuất phát từ thực tế họ là đất nước tỷ dân nên dữ liệu cũng cực kỳ không lồ. Với nguồn dữ liệu đồ sộ như vậy, Trung Quốc tự đặt ra bài toán là làm thế nào để khai thác hiệu quả nguồn dữ liệu rất lớn đó. Nhất là khi hiện nay dữ liệu được xem như tài sản có giá trị cao trong kỷ nguyên số. Các công nghệ như trí tuệ nhân tạo (AI), phân tích dữ liệu lớn (Big Data Mining) đều cần dữ liệu để vận hành, thúc đẩy tăng trưởng kinh tế, phát triển khoa học và cải thiện đời sống xã hội.

Châu Âu hiện nay cũng vẫn đang tranh cãi về cách quản lý dữ liệu. Điển hình là vụ việc Công ty AVAST bán dữ liệu người dùng cho bên thứ ba. Ban đầu, họ tuyên bố dữ liệu này không định danh, không ảnh hưởng đến quyền riêng tư cá nhân. Nhưng sau đó, các tổ chức độc lập chứng minh được dữ liệu này có thể được truy ngược lại danh tính người dùng, dẫn đến vụ kiện tụng. Kết quả là AVAST bị buộc phải đóng cửa và chịu khoản phạt lên đến 160 triệu USD. Hiện nay, EU đang triển khai một chiến lược dữ liệu chung với trọng tâm xây dựng các “không gian dữ liệu” dùng chung trong những





lĩnh vực quan trọng (y tế, công nghiệp, giao thông,...). Thay vì hình thành các sàn giao dịch dữ liệu công khai như Trung Quốc, châu Âu hướng đến mô hình trung gian dữ liệu tin cậy. Năm 2022, EU ban hành Đạo luật Quản trị Dữ liệu (DGA) nhằm tạo khung pháp lý cho các dịch vụ trung gian dữ liệu (data intermediation services) hoạt động. Các trung gian này có thể là sàn dữ liệu hoặc các “data trust” phải đăng ký và tuân thủ các điều kiện nghiêm ngặt: đóng vai trò bên thứ ba trung lập, minh bạch kết nối bên có dữ liệu với bên muốn sử dụng dữ liệu. Quan trọng là họ không được phép sử dụng dữ liệu mà mình môi giới để thu lợi riêng, và phải tách bạch hoạt động trung gian dữ liệu với mọi dịch vụ khác. DGA cũng thúc đẩy khái niệm “chia sẻ dữ liệu vì lợi ích cộng đồng” (data altruism), khuyến khích các cá nhân, doanh nghiệp tự nguyện đóng góp dữ liệu vì mục đích nghiên cứu, phát triển khoa học - những hoạt động này sẽ do các tổ chức phi lợi nhuận đảm nhiệm theo bộ quy tắc minh bạch của EU<sup>42</sup>.

Song song với DGA, EU đang thảo luận Đạo luật Dữ liệu (DA) để quy định rõ quyền truy cập và sử dụng dữ liệu giữa các chủ thể, ví dụ: dữ liệu do thiết bị IoT tạo ra thì người dùng có quyền yêu cầu nhà sản xuất cung cấp. Tất cả hướng tới mục tiêu cuối cùng là tăng cường lượng dữ liệu được chia sẻ trong nền kinh tế EU một cách có kiểm soát. Thay vì thương mại hóa dữ liệu tràn lan, châu Âu ưu tiên mô hình chia sẻ theo “hệ sinh thái đóng” giữa các bên liên quan, dưới sự bảo trợ của luật pháp về quyền riêng tư và cạnh tranh. Chẳng hạn, các hãng xe hơi châu Âu có thể chia sẻ dữ liệu xe kết nối trong một không gian dữ liệu chung để phát triển dịch vụ thông minh, nhưng

<sup>42</sup> A&O Shearman (2023), *EU – Data Governance Act becomes applicable*, aoshearman.com, <https://www.aoshearman.com/en/insights/ao-shearman-on-data/eu--data-governance-act-becomes-applicable>, truy cập ngày 06/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

việc truy cập dữ liệu đó phải tuân thủ quy tắc chung của ngành và cho phép cơ quan quản lý giám sát.



### ***Các sàn giao dịch dữ liệu trên thế giới - Ảnh: VnEconomy***

***- Hướng đi nào cho Việt Nam trong việc xây dựng và phát triển sàn dữ liệu?***

Tại Việt Nam, khái niệm sàn giao dịch dữ liệu cũng bắt đầu được quan tâm trong vài năm gần đây, nhất là khi dữ liệu được thừa nhận là “*tài nguyên quan trọng*” cho chuyển đổi số quốc gia. Tuy nhiên, đến trước năm 2025, hành lang pháp lý về dữ liệu ở nước ta vẫn chưa đầy đủ, các hoạt động mua bán, trao đổi dữ liệu hầu như bị cấm hoặc diễn ra trong “*vùng xám*”. Do chưa có luật chuyên biệt, một số doanh nghiệp Việt đã linh hoạt tận dụng kẽ hở pháp lý để chia sẻ dữ liệu dưới dạng “*hợp tác*” thay vì mua bán trực tiếp - ví dụ chuyển dữ liệu thông qua công ty liên kết, hoặc đổi dữ liệu để cùng phát triển sản phẩm chung. Dù vậy, những cách làm tạm thời này không thể thay thế cho một thị trường dữ liệu minh bạch, chính thức. Nhận thức được điều đó, Nhà nước đã gấp rút xây dựng Luật Dữ liệu nhằm thống nhất các nguyên tắc quản lý và định hình thị trường dữ liệu hợp pháp. Song song đó, Chiến lược dữ liệu quốc gia được Thủ tướng ban hành cũng đặt mục tiêu *đến năm 2030 hoàn thành thí điểm 5 sàn giao dịch dữ liệu trên cả nước*.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Như vậy, ít nhất đến trước thời điểm 1/7/2025, khi Luật Dữ liệu có hiệu lực, dữ liệu chưa được quản lý và khai thác hiệu quả, cùng với đó là vấn đề bảo vệ dữ liệu. Hiện nay, người dân chủ yếu sử dụng các nền tảng công nghệ từ nước ngoài, trong khi các nền tảng thuần Việt vẫn chiếm thị phần khá nhỏ, ngoại trừ một số cái tên như Zalo. Điều này đặt ra hai vấn đề lớn:

**Một là**, phải xây dựng hành lang pháp lý sao cho các ứng dụng, phần mềm xuyên biên giới phải được kiểm soát chặt chẽ và tuân thủ các quy định tại Việt Nam.

**Hai là**, phải phát triển công nghệ kiểm soát dữ liệu, giám sát ẩn danh đảm bảo dữ liệu được sử dụng, giao dịch đúng quy định.

Dữ liệu để đưa lên các sàn phải là không thể định danh. Nhưng tình hình thực tế chung là các biện pháp kỹ thuật và khung pháp lý vẫn còn chung chung. Tới đây, Luật Dữ liệu của Việt Nam sẽ chính thức có hiệu lực (1/7/2025), tuy nhiên, để Luật đi vào thực tế, cần có các nghị định hướng dẫn chi tiết, đặc biệt là cần thêm các quy chuẩn kỹ thuật, hợp đồng dữ liệu mẫu, cơ chế bảo hiểm dữ liệu và thử nghiệm sandbox. Nếu muốn đi nhanh, cần triển khai các bước một cách khẩn trương để tránh tình trạng “vừa làm vừa run”, gây cản trở sự phát triển. Tất nhiên, chúng ta có thể áp dụng cơ chế sandbox - thử nghiệm, điều chỉnh và sửa sai theo thực tế. Tuy nhiên, khi liên quan đến dữ liệu, đặc biệt là dữ liệu cá nhân, mọi quyết định đều cần cân nhắc kỹ lưỡng. Dữ liệu là tài sản vô giá, để khai thác hiệu quả mà vẫn bảo vệ được quyền lợi của người dân và lợi ích quốc gia là một bài toán khó. Điều này đòi hỏi sự phối hợp chặt chẽ giữa các cơ quan quản lý, doanh nghiệp và các bên liên quan. Nhà nước có thể định hướng chính sách, nhưng việc triển khai cụ thể, đặc biệt là khâu giám sát, vẫn cần các giải pháp công nghệ thực tiễn và khả thi.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Việc xây dựng một sàn giao dịch dữ liệu không phải điều đơn giản, ngay cả các quốc gia phát triển cũng còn nhiều vướng mắc. Dĩ nhiên, Việt Nam cũng không ngoại lệ, với vô vàn thách thức lớn khi xây dựng sàn giao dịch dữ liệu. Bất cập lớn nhất có thể thấy ngay chính là hành lang pháp lý chưa theo kịp tốc độ phát triển của công nghệ. Các quy định về an ninh mạng và an toàn thông tin của Việt Nam đã ra đời cách đây cả chục năm. Luật An ninh mạng mới nhất từ năm 2018, còn Luật An toàn thông tin từ năm 2015. Trong khi đó, công nghệ đã thay đổi rất nhanh, đặc biệt với sự bùng nổ của AI, nhiều quy định cũ trở nên lỗi thời.



***Mình họa về OpenAI và Deepseek - Ảnh: Internet***

Một ví dụ điển hình là tranh cãi gần đây giữa Deepseek và OpenAI về việc Deepseek được cho là đã sử dụng câu trả lời của ChatGPT để huấn luyện mô hình AI của họ. Liệu đây có phải hành vi “đánh cắp” dữ liệu không? Câu hỏi này đến nay vẫn chưa có lời giải thỏa đáng. Ngay cả trên thế giới, vấn đề sở hữu và sử dụng dữ liệu vẫn còn rất mơ hồ, tranh cãi. Điều này cho thấy việc xây dựng một hệ thống quy định chặt chẽ ngay từ đầu là





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

vô cùng khó, đòi hỏi Việt Nam không chỉ phải đưa ra luật phù hợp mà còn cần đảm bảo tuân thủ thông lệ quốc tế. Các nền tảng xuyên biên giới cung cấp dịch vụ trên quy mô hàng trăm quốc gia. Nếu quy định của Việt Nam không phù hợp hoặc quá khắt khe, có thể họ sẽ rời bỏ thị trường.

Thế nhưng, Việt Nam là có một “điểm sáng” về mặt công nghệ. Việt Nam đã có các công ty sở hữu nền tảng xử lý dữ liệu, có năng lực huấn luyện AI và triển khai mô hình AI. Chỉ cần có hướng dẫn pháp lý cụ thể từ cơ quan quản lý, sàn giao dịch dữ liệu hoàn toàn có thể vận hành chính thức. Nhìn chung, ngay cả các nước tiên tiến cũng đang loay hoay trong việc xây dựng luật điều chỉnh thị trường dữ liệu. Đây không chỉ là bài toán riêng của Việt Nam, nhưng nếu chúng ta hoàn thiện khung pháp lý, thậm chí có thể đi trước một bước so với thế giới, thì có thể tạo lợi thế cạnh tranh đáng kể.

Trong nền kinh tế số, dữ liệu được ví như một loại tài sản có giá trị cao, và hiện nay dữ liệu là thứ “không bao giờ đủ” với mọi doanh nghiệp, bất kể lớn hay nhỏ. Các doanh nghiệp lớn thường có lợi thế nhờ sở hữu nguồn dữ liệu dồi dào và tiềm lực tài chính để mua thêm dữ liệu khi cần. Ngược lại, doanh nghiệp nhỏ thường thiếu dữ liệu và hạn chế về ngân sách. Việc có một sàn giao dịch dữ liệu hứa hẹn tạo sân chơi bình đẳng hơn ở chỗ giúp doanh nghiệp nhỏ tiếp cận dữ liệu linh hoạt, theo nhu cầu cụ thể của mình. Mặc dù lợi thế vẫn nghiêng về doanh nghiệp lớn bởi họ có tiền mua dữ liệu và chính họ cũng sở hữu nhiều dữ liệu để gỡ bỏ định danh và bán ra, nhưng sàn dữ liệu sẽ mở ra cơ hội cho doanh nghiệp nhỏ. Thay vì phải bỏ chi phí lớn để mua trọn vẹn cả một tập dữ liệu khổng lồ (mà có thể phần lớn không dùng đến), doanh nghiệp nhỏ có thể mua một phần dữ liệu cụ thể, đúng mục tiêu cần thiết. Cách tiếp cận “chia nhỏ” này giúp họ giảm chi phí và tập trung





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

khai thác giá trị thực sự, đồng thời không phải đầu tư hệ thống công nghệ xử lý dữ liệu quy mô lớn vốn tốn kém.



***Lập sàn giao dịch dữ liệu là đề xuất của Bộ Công an - Ảnh: Báo Đầu tư***

Dữ liệu hiện được coi là nguồn tài nguyên thiết yếu cho đổi mới sáng tạo và chuyển đổi số. Không có dữ liệu, dù công nghệ tiên tiến đến đâu cũng không phát huy được hết giá trị. Một sàn giao dịch dữ liệu hoạt động hiệu quả sẽ cung cấp nguồn dữ liệu phong phú một cách hợp pháp và minh bạch, cho phép các doanh nghiệp, tổ chức khai thác phục vụ nghiên cứu và phát triển công nghệ mới. Nói cách khác, dữ liệu chính là “*nhiên liệu*” cho “*động cơ*” đổi mới sáng tạo, có dữ liệu thì công nghệ AI, Big Data, tự động hóa... mới vận hành trơn tru và tạo ra giá trị. Khi sàn dữ liệu đi vào hoạt động, dự kiến sẽ mở ra nhiều cơ hội để Việt Nam phát triển các lĩnh vực như trí tuệ nhân tạo, phân tích dữ liệu lớn, tự động hóa, và các lĩnh vực công nghệ cao khác.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



## ***Sàn dữ liệu sẽ cung cấp “nhiên liệu” cho phát triển kỷ nguyên số tại Việt Nam - Ảnh: VnEconomy***

Một vấn đề hiện nay không phải là Việt Nam thiếu dữ liệu, mà là dữ liệu bị phân mảnh, rời rạc ở nhiều nơi. Dữ liệu số hóa đã được thu thập từ lâu nhưng nằm rải rác trong các bộ, ngành, địa phương và chưa được liên thông để khai thác hiệu quả. Ngay cả các doanh nghiệp cũng có những “mỏ vàng” dữ liệu riêng nhưng chưa có công cụ để đào lên giá trị, tức chưa khai thác tối ưu được. Việc Bộ Công an thành lập Trung tâm dữ liệu quốc gia được đánh giá là bước đi quan trọng nhằm tập trung hóa những dữ liệu rời rạc này, tạo điều kiện thuận lợi cho việc khai thác và ứng dụng AI trên quy mô quốc gia. Trong bối cảnh đó, sàn giao dịch dữ liệu sẽ đóng vai trò như một hạ tầng kết nối trung tâm giữa các mạng lưới dữ liệu phân tán. Sàn không nhất thiết lưu trữ toàn bộ dữ liệu, nhưng khi cần dữ liệu thì các bên có thể truy vấn để kết nối tới nguồn phù hợp, qua đó giải quyết được bài toán dữ liệu phân tán hiện nay.

Cũng cần lưu ý rằng dữ liệu trong nước dù quan trọng nhưng chỉ đáp ứng khoảng 10% nhu cầu phát triển AI, phần còn lại phụ thuộc vào tri thức toàn cầu. Hiện nhiều hệ thống AI trên thế giới có xu hướng mở (mở mô hình hoặc mã nguồn), chẳng hạn như mô hình Llama của Meta hay dự án





DeepSeek; thậm chí những mô hình thương mại hàng đầu như ChatGPT cũng có thể phải mở hơn trong tương lai. Điều này cho thấy sự hợp tác và chia sẻ dữ liệu, tri thức trên phạm vi quốc tế sẽ ngày càng quan trọng đối với sự phát triển AI của Việt Nam.

Mối quan hệ giữa AI và dữ liệu gắn kết chặt chẽ: không có dữ liệu thì không thể huấn luyện AI, và thiếu AI thì dữ liệu cũng khó phát huy giá trị tối đa. Chuyên gia ví von AI giống như động cơ, còn dữ liệu là nhiên liệu và nếu thiếu một trong hai thì chiếc xe số không thể chạy được. Trong những năm gần đây, dù AI chưa thể vượt con người ở khía cạnh cảm xúc, nhưng về hiệu suất xử lý, tốc độ tính toán và khả năng hoạt động liên tục 24/7, AI vượt trội con người rất nhiều. Chính vì thế, mặc cho đã có những lời kêu gọi tạm dừng phát triển AI, thực tế không ai dừng lại, bởi AI mang đến lợi thế cạnh tranh quá lớn. Tính đến thời điểm này, không một quốc gia hay tổ chức nào trên thế giới nói “*dừng phát triển AI*” nữa - cuộc đua AI đang diễn ra quyết liệt. Việt Nam không thể đứng ngoài cuộc; nếu muốn lọt nhóm dẫn đầu về AI, chúng ta không thể chậm chân.

Về cơ chế vận hành sản giao dịch dữ liệu, **mô hình hợp tác công - tư (Public - Private - Partnership - PPP)** được xem là phù hợp và hiệu quả nhất. Nếu chỉ dựa vào ngân sách nhà nước để xây dựng và vận hành sản, hệ thống có thể thiếu linh hoạt, thiếu động lực phát triển. Việc thu hút sự tham gia của khu vực tư nhân sẽ tận dụng được nguồn lực tài chính, công nghệ và kinh nghiệm thị trường của họ. Theo mô hình PPP, Nhà nước đóng vai trò định hướng, quản lý, giám sát và đảm bảo tuân thủ pháp luật; còn doanh nghiệp tư nhân chịu trách nhiệm khai thác kinh tế, vận hành dịch vụ hiệu quả và liên tục đổi mới để phát triển.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Bài học kinh nghiệm có thể tham khảo từ mô hình của Trung Quốc. Họ triển khai hợp tác công tư rất thành công trong lĩnh vực công nghệ. Huawei là một ví dụ điển hình khi doanh nghiệp công nghệ hàng đầu này nhận được sự hỗ trợ chiến lược từ Nhà nước nhưng vẫn vận hành theo cơ chế thị trường, linh hoạt và cạnh tranh. Cách tiếp cận đó tạo sự cân bằng giữa quản lý của Nhà nước với động lực đổi mới sáng tạo của khu vực tư nhân. Đối với sản phẩm dịch dữ liệu, mô hình PPP sẽ giúp vừa kiểm soát chặt chẽ được dữ liệu (dưới sự giám sát nhà nước), vừa đảm bảo động lực thị trường để sản phẩm phát triển và thu hút người tham gia.

Sự ra đời của sản phẩm dịch dữ liệu sẽ giúp hợp pháp hóa và minh bạch hóa hoạt động mua bán dữ liệu, nhưng không có nghĩa là ngay lập tức loại bỏ được hoàn toàn thị trường “ngầm”. Thực tế, việc mua bán dữ liệu trái phép trên chợ đen sẽ vẫn tiếp diễn ở một mức độ nào đó ngay cả khi sản phẩm chính thức hoạt động. Các tổ chức, cá nhân với mục đích không chính đáng có thể vẫn tìm cách thu thập và trao đổi những dữ liệu định danh (như thông tin cá nhân) một cách bất hợp pháp. Do vậy, bên cạnh việc vận hành sản phẩm dịch, nhà nước cần xây dựng hành lang pháp lý chặt chẽ và cơ chế chế tài nghiêm khắc để kiểm soát và xử lý các vi phạm này. Luật Dữ liệu và các quy định xử phạt sẽ đóng vai trò quan trọng trong việc hạn chế giao dịch dữ liệu trái phép, thay vì kỳ vọng sản phẩm dữ liệu tự thân có thể giải quyết triệt để vấn đề. Nói cách khác, sản phẩm dịch dữ liệu chỉ hiệu quả khi đi kèm với việc thực thi pháp luật mạnh tay nhằm răn đe và giảm thị trường chợ đen.

Về mặt kỹ thuật, để một sản phẩm dịch dữ liệu vận hành thực sự hiệu quả, cần đảm bảo hai điều kiện then chốt: **(1) Năng lực kỹ thuật:** Sản phẩm dịch phải đáp ứng được nhu cầu của người dùng về tốc độ truy vấn dữ liệu, khả năng mua - bán linh hoạt (mua theo lô nhỏ, tùy chọn), cũng như tính





minh bạch và chính xác của giao dịch. Sàn cần có hạ tầng công nghệ mạnh để xử lý khối lượng lớn yêu cầu từ người dùng một cách nhanh chóng, đồng thời cung cấp cơ chế theo dõi, kiểm tra giao dịch rõ ràng nhằm tạo niềm tin cho các bên tham gia. **(2) An ninh và bảo mật:** Đây là yếu tố quan trọng nhất. Nếu sàn giao dịch dữ liệu bị tấn công, hậu quả có thể rất nghiêm trọng. Thực tế cho thấy khi các sàn giao dịch tiền số bị “hack”, thiệt hại thường rất lớn và người dùng gần như không thể dễ dàng lấy lại tài sản đã mất. Với dữ liệu cũng vậy: một khi bị đánh cắp, dữ liệu có thể bị tội phạm mạng bán lại với giá rẻ hơn, khiến bên cung cấp mất kiểm soát hoàn toàn và dữ liệu bị mất giá trị. Do đó, sàn dữ liệu phải có cơ chế bảo mật tối đa, phòng ngừa cả các nguy cơ rò rỉ thông tin lẫn các hành vi sửa đổi, gian lận trong quá trình giao dịch. Nếu an ninh dữ liệu trên sàn không được đảm bảo chặt chẽ, cả bên cung cấp lẫn bên mua sẽ e ngại tham gia. Các tổ chức sở hữu dữ liệu sẽ không muốn đưa dữ liệu của mình lên sàn nếu lo ngại bị đánh cắp. Ngược lại, người mua cũng có tâm lý chờ đợi, vì họ kỳ vọng có thể mua dữ liệu bị rò rỉ với giá rẻ hơn ngoài chợ đen. Khi niềm tin vào sự an toàn của dữ liệu không còn, thị trường dữ liệu hợp pháp sẽ rất khó phát triển bền vững.

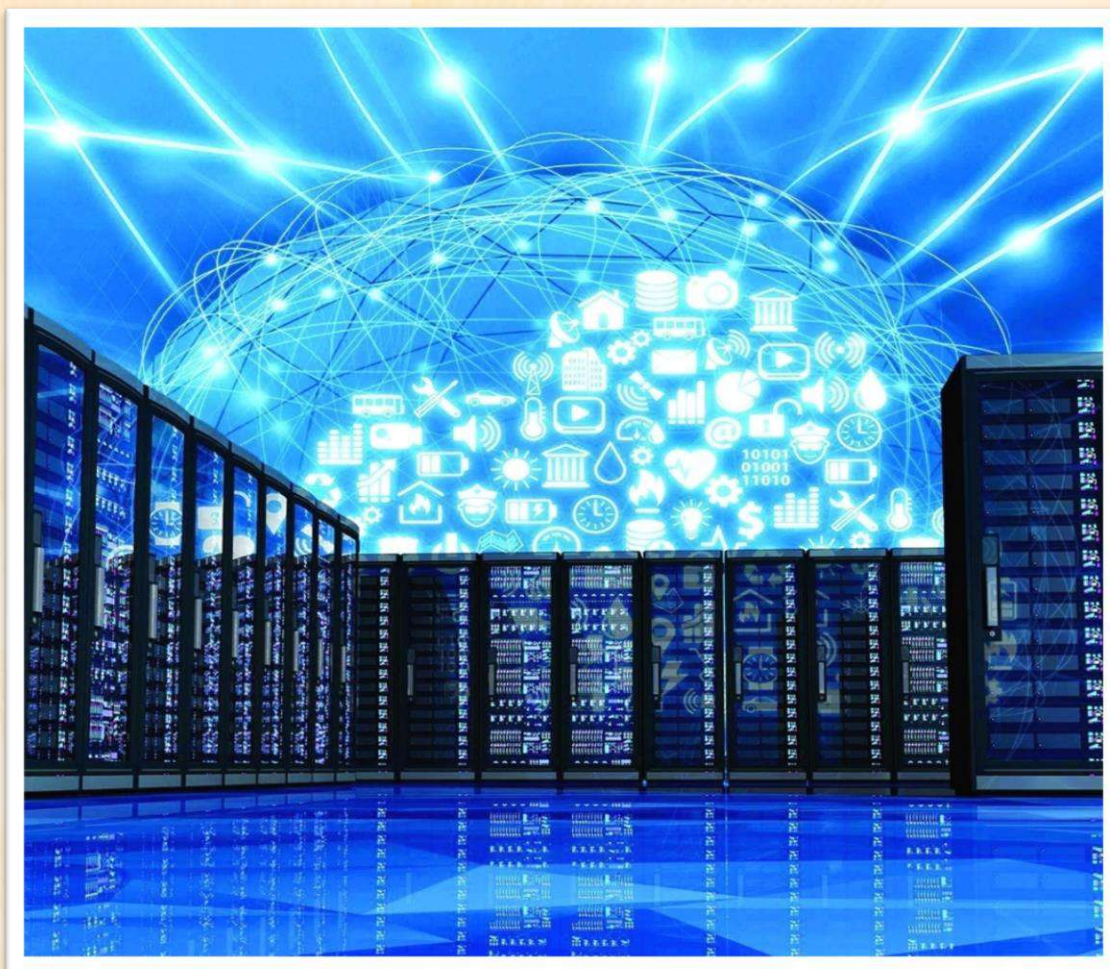
Hiện tại, xét về *năng lực công nghệ*, Việt Nam được đánh giá đã sẵn sàng triển khai sàn giao dịch dữ liệu. Tuy nhiên, về khía cạnh an ninh mạng, việc bảo vệ một sàn giao dịch dữ liệu mở còn khá mới mẻ đối với các đội ngũ an ninh mạng trong nước. Phần lớn chuyên gia bảo mật nội địa đến nay chủ yếu có kinh nghiệm bảo vệ hệ thống nội bộ doanh nghiệp, chứ chưa đối mặt với bài toán bảo mật cho một nền tảng mở, nơi có hàng loạt giao dịch diễn ra liên tục giữa nhiều bên. Bài học từ các cuộc tấn công gần đây cho thấy hacker thường khai thác lỗ hổng logic trong quá trình giao dịch, nghĩa là giao dịch nhìn có vẻ hợp lệ nhưng nội dung đã bị chỉnh sửa để trục lợi.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Điều này đòi hỏi sàn giao dịch dữ liệu không chỉ bảo vệ dữ liệu ở trạng thái tĩnh, mà còn phải bảo vệ chặt chẽ quy trình giao dịch và luồng dữ liệu động trên hệ thống.



### ***Dữ liệu lên sàn, “dễ bàn” nhưng “khó bán”? - Ảnh: McKinsey***

Theo kế hoạch, sàn giao dịch dữ liệu quốc gia sẽ do Bộ Công an chủ trì. Điều này giúp đảm bảo sự tuân thủ pháp luật và yếu tố quản lý nhà nước ngay từ đầu. Tuy nhiên, để vận hành an toàn và hiệu quả, cần có sự phối hợp liên ngành và huy động nguồn lực từ toàn xã hội, đặc biệt là sự tham gia của các doanh nghiệp an ninh mạng tư nhân có năng lực. Một cơ chế linh hoạt nên được thiết lập nhằm kết nối sự hợp tác công - tư trong việc bảo vệ sàn giao dịch dữ liệu: tận dụng kỹ năng, công nghệ và nhân lực từ khu vực tư





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

nhân dưới sự điều phối của cơ quan quản lý nhà nước. Có như vậy, sàn giao dịch dữ liệu mới vừa an toàn bảo mật, vừa phát huy được tối đa tiềm năng thúc đẩy kinh tế số của Việt Nam.

### ***7.1.4.5. Về trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu, sàn dữ liệu***



#### ***- Quy định chung theo Luật Dữ liệu năm 2024***

Luật Dữ liệu 2024 (số 60/2024/QH15) đặt ra các trách nhiệm chung cho mọi tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu và sàn dữ liệu. Cụ thể, Điều 43 của Luật quy định các tổ chức này phải thực hiện các nghĩa vụ sau:

+ ***Cung cấp dịch vụ trên cơ sở hợp đồng:*** Mọi dịch vụ do tổ chức cung cấp phải được thực hiện thông qua thỏa thuận bằng hợp đồng cung cấp dịch vụ với khách hàng. Điều này nhằm đảm bảo các bên thống nhất về phạm vi dịch vụ, quyền và nghĩa vụ trước khi dữ liệu được chia sẻ hay phân tích.

+ ***Đảm bảo dịch vụ thông suốt, liên tục:*** Tổ chức phải bảo đảm có kênh tiếp nhận thông tin và cung cấp dịch vụ thông suốt, liên tục cho khách hàng.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Nói cách khác, hệ thống kỹ thuật và hỗ trợ người dùng phải hoạt động ổn định, sẵn sàng phục vụ 24/7 hoặc ít nhất không bị gián đoạn bất thường.

+ ***Quản lý an toàn dữ liệu và phòng ngừa rủi ro:*** Tổ chức có trách nhiệm quản lý, kiểm tra, giám sát an toàn dữ liệu và bảo mật dữ liệu thường xuyên. Đồng thời phải phòng ngừa, ngăn chặn và xử lý các rủi ro về dữ liệu có thể xảy ra. Điều này đòi hỏi thiết lập các biện pháp kỹ thuật và quy trình nội bộ nhằm bảo vệ dữ liệu khỏi truy cập trái phép, rò rỉ hay mất mát. Tổ chức cũng phải giám sát các hành vi có dấu hiệu xâm phạm hoặc ảnh hưởng đến việc bảo vệ dữ liệu để kịp thời ngăn chặn.

+ ***Tuân thủ pháp luật liên quan:*** Các tổ chức phải tuân thủ đầy đủ quy định pháp luật về an toàn thông tin mạng, an ninh mạng, giao dịch điện tử và các quy định khác có liên quan. Điều này bao gồm việc tuân thủ Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018, Luật Giao dịch điện tử 2023..., các văn bản dưới Luật cũng như các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật dữ liệu. Việc tuân thủ này bảo đảm hoạt động trung gian, phân tích, tổng hợp hay sàn dữ liệu diễn ra trong khuôn khổ pháp luật chung về bảo vệ an ninh và quyền riêng tư.

Những quy định trên tạo nền tảng chung cho trách nhiệm của các tổ chức cung cấp dịch vụ dữ liệu. Trên cơ sở đó, Nghị định số 169/2025/NĐ-CP đã chi tiết hóa trách nhiệm cụ thể cho từng nhóm chủ thể:

- (1) Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu;
- (2) Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu;
- (3) Tổ chức cung cấp dịch vụ sàn dữ liệu (nền tảng giao dịch dữ liệu).

***- Trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu***

Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu là các đơn vị làm cầu nối trung gian giữa bên cung cấp dữ liệu và bên sử dụng dữ liệu.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Nghị định 169/2025/NĐ-CP đã quy định **12 nhóm trách nhiệm** cụ thể đối với các tổ chức trung gian dữ liệu (Điều 26) như sau:

**(1) Chứng minh trách nhiệm thông qua việc kết nối, chia sẻ, trao đổi, truy cập dữ liệu và bảo vệ dữ liệu, bảo vệ dữ liệu cá nhân theo quy định pháp luật:** Tổ chức phải chứng minh được trách nhiệm của mình thông qua việc thiết lập kết nối, chia sẻ, trao đổi, truy cập dữ liệu một cách an toàn, cũng như thực hiện tốt việc bảo vệ dữ liệu (đặc biệt là dữ liệu cá nhân) theo quy định pháp luật. Nói cách khác, họ phải thể hiện được rằng mọi hoạt động trung gian dữ liệu do mình thực hiện đều có kiểm soát và tuân thủ các yêu cầu về an toàn, bảo mật dữ liệu.



**Mình họa về quyền bảo mật dữ liệu cá nhân - Ảnh: Youth and Partners**

**(2) Thông báo cho tổ chức, cá nhân là chủ sở hữu dữ liệu, chủ thể dữ liệu, bên sử dụng dữ liệu về mục đích cung cấp sản phẩm, dịch vụ trung gian dữ liệu và đảm bảo các quyền của cá nhân theo quy định của pháp luật về bảo vệ dữ liệu cá nhân:** Trước khi xử lý hoặc truyền dữ liệu,





bên trung gian phải thông báo cho các bên liên quan bao gồm chủ sở hữu dữ liệu, chủ thể dữ liệu và bên sử dụng dữ liệu về mục đích cung cấp dịch vụ trung gian dữ liệu của mình. Đồng thời, họ phải đảm bảo các quyền của cá nhân theo pháp luật bảo vệ dữ liệu cá nhân. Điều này có nghĩa là người dùng dữ liệu phải được biết dữ liệu của họ được trung gian sử dụng vào mục đích gì, và các quyền như quyền được thông báo, quyền đồng ý..., của cá nhân phải được tôn trọng.

**(3) Việc thu thập, sử dụng hoặc tiết lộ dữ liệu cá nhân cho các mục đích hợp pháp và phải được chủ thể dữ liệu đồng ý:** Mọi việc thu thập, sử dụng hoặc tiết lộ dữ liệu cá nhân thông qua dịch vụ trung gian đều phải phục vụ mục đích hợp pháp và được chủ thể dữ liệu đồng ý trước. Nguyên tắc “*có sự đồng ý của chủ thể dữ liệu*” này hoàn toàn phù hợp với các quy định chung về bảo vệ dữ liệu cá nhân ở Việt Nam, vốn coi sự đồng ý tự nguyện, minh bạch của chủ thể dữ liệu là điều kiện tiên quyết để xử lý dữ liệu cá nhân (trừ một số trường hợp pháp luật cho phép ngoại lệ). *Ví dụ:* Một công ty trung gian dữ liệu kết nối ngân hàng và công ty bảo hiểm để chia sẻ dữ liệu khách hàng bắt buộc phải đảm bảo rằng khách hàng đã đồng ý cho việc chia sẻ dữ liệu cá nhân đó; nếu chưa có, công ty phải thu thập sự đồng ý thích hợp, tránh tình trạng tự ý trao đổi thông tin khách hàng.

**(4) Bảo đảm dữ liệu chính xác, đầy đủ từ chủ thể dữ liệu, chủ sở hữu dữ liệu cung cấp cho bên sử dụng dịch vụ:** Tổ chức trung gian cần đảm bảo tính chính xác và đầy đủ của dữ liệu tiếp nhận từ chủ thể hoặc chủ sở hữu dữ liệu trước khi cung cấp cho bên sử dụng dịch vụ. Nói cách khác, dữ liệu phải được kiểm chứng, đối soát để hạn chế sai sót hoặc thiếu thông tin, tránh gây hiểu lầm cho bên nhận dữ liệu. Trách nhiệm này yêu cầu bên trung gian có cơ chế xác minh, làm sạch dữ liệu trước khi chuyển giao.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

(5) **Bảo đảm việc truy cập dữ liệu đúng mục đích, đúng đối tượng, khai thác đúng theo hợp đồng đã ký kết:** Tổ chức phải bảo đảm việc truy cập và khai thác dữ liệu đúng mục đích, đúng đối tượng như đã thỏa thuận trong hợp đồng. Điều này nghĩa là dữ liệu chỉ được cung cấp cho đúng bên có quyền nhận và chỉ dùng vào mục đích đã cam kết. Bên trung gian phải ngăn ngừa việc dữ liệu bị sử dụng sai mục đích hoặc chia sẻ cho bên thứ ba không được phép. *Chẳng hạn*, nếu hợp đồng trung gian quy định chỉ chia sẻ dữ liệu khách hàng để đánh giá tín dụng, thì trung gian không được để dữ liệu đó bị dùng cho quảng cáo hoặc chuyển tiếp cho đơn vị khác ngoài phạm vi hợp đồng.



**Ảnh: Viettel IDC**

(6) **Thực hiện các biện pháp bảo vệ, bảo mật hợp lý để bảo vệ dữ liệu cá nhân trong quyền sở hữu của tổ chức, bao gồm ngăn chặn truy cập, thu thập, sử dụng, tiết lộ trái phép hoặc các rủi ro tương tự:** Phải thực hiện các biện pháp bảo vệ và bảo mật hợp lý để bảo vệ dữ liệu cá nhân do mình nắm





giữ. Các biện pháp này bao gồm việc ngăn chặn truy cập, thu thập, sử dụng, tiết lộ trái phép cũng như phòng chống các rủi ro tương tự. Tổ chức trung gian cần triển khai những giải pháp kỹ thuật (như mã hóa, tường lửa, kiểm soát truy cập) và quy trình quản lý (như phân quyền, đào tạo nhân viên về an ninh dữ liệu) phù hợp để đảm bảo dữ liệu không bị xâm nhập hay rò rỉ.

**(7) Giới hạn việc lưu trữ dữ liệu cá nhân trong thời gian cần thiết và xử lý thông tin cá nhân đúng cách khi không còn cần thiết cho mục đích kinh doanh hoặc pháp lý:** Dữ liệu cá nhân chỉ nên được lưu trữ trong thời gian cần thiết cho mục đích đã định và phải xóa, hủy hoặc ẩn khi không còn cần thiết cho mục đích kinh doanh hoặc pháp lý. Trách nhiệm này yêu cầu bên trung gian thiết lập chu kỳ xem xét dữ liệu, xóa dữ liệu đúng hạn, tránh việc lưu trữ quá lâu những thông tin nhạy cảm mà không có mục đích rõ ràng. Việc làm này không chỉ giảm thiểu rủi ro lộ lọt dữ liệu mà còn tuân thủ nguyên tắc giới hạn lưu giữ trong bảo vệ dữ liệu cá nhân.

**(8) Bảo đảm giới hạn chuyển giao dữ liệu cá nhân xuyên biên giới theo các yêu cầu của quy định, bảo đảm rằng tiêu chuẩn bảo vệ tương đương với tiêu chuẩn theo yêu cầu pháp luật có liên quan:** Trong trường hợp chuyển dữ liệu cá nhân ra nước ngoài, tổ chức trung gian phải đáp ứng các yêu cầu pháp lý về chuyển dữ liệu xuyên biên giới và bảo đảm dữ liệu được bảo vệ với tiêu chuẩn tương đương khi ở nước ngoài. Điều này phù hợp với xu hướng quản lý chặt chẽ luồng dữ liệu qua biên giới trong luật pháp quốc tế, tức là chỉ cho phép chuyển dữ liệu đi nếu nơi nhận có mức độ bảo vệ dữ liệu tương đương. Bên trung gian có thể phải xin phép cơ quan quản lý hoặc đảm bảo đối tác nước ngoài tuân thủ các tiêu chuẩn bảo mật theo quy định của Việt Nam.





**(9) Thông báo vi phạm dữ liệu tới tổ chức, cá nhân bị ảnh hưởng ngay khi có thể nếu có vi phạm dữ liệu có khả năng gây ra tác hại đáng kể cho cá nhân hoặc có quy mô đáng kể:** Nếu xảy ra vi phạm dữ liệu có khả năng gây tác hại đáng kể cho cá nhân hoặc ảnh hưởng trên quy mô lớn, tổ chức trung gian phải thông báo ngay cho các tổ chức, cá nhân bị ảnh hưởng ngay khi có thể. Thông báo này giúp các cá nhân, đơn vị liên quan kịp thời có biện pháp ứng phó (như đổi mật khẩu, cảnh giác với lừa đảo...). Đây là nghĩa vụ thông báo vi phạm tương tự như quy định tại nhiều quốc gia, nhằm giảm thiểu hậu quả của sự cố mất an toàn dữ liệu.

**(10) chuyển dữ liệu tới đúng bên sử dụng dữ liệu theo đúng thỏa thuận đã ký kết:** Tổ chức trung gian phải đảm bảo khả năng chuyển giao dữ liệu đến đúng bên sử dụng dữ liệu như đã thỏa thuận trong hợp đồng dịch vụ. Nói cách khác, họ phải có hệ thống kỹ thuật và quy trình vận hành đáng tin cậy để dữ liệu đến được đích mong muốn đầy đủ, chính xác và đúng thời điểm. Tránh trường hợp thất lạc dữ liệu hoặc chuyển nhầm đối tượng nhận, gây ảnh hưởng đến quyền lợi các bên.

**(11) Bảo đảm khả năng tư vấn, đánh giá tác động việc xử lý dữ liệu, thẩm định dữ liệu, các hình thức thanh toán linh hoạt, quy định về thuế, phí, giá theo quy định của hoạt động thương mại điện tử:** Tổ chức cần có khả năng tư vấn, đánh giá tác động xử lý dữ liệu, thẩm định dữ liệu, cũng như cung cấp các hình thức thanh toán linh hoạt và tuân thủ quy định về thuế, phí, giá trong hoạt động thương mại điện tử liên quan. Đây là một nhóm trách nhiệm mở rộng, yêu cầu bên trung gian phải hỗ trợ khách hàng trong việc hiểu rõ dữ liệu (đánh giá chất lượng, tác động) và tạo thuận lợi trong giao dịch (thanh toán, hóa đơn, thuế). Ví dụ, nếu trung gian bán dữ liệu trên nền tảng số, họ phải có cơ chế thanh toán trực tuyến an toàn, xuất hóa đơn, kê khai thuế phù hợp.





**(12) Tổ chức tham gia hoạt động trung gian dữ liệu phải thực hiện việc xác thực danh tính theo quy định pháp luật về định danh và xác thực điện tử:** Bất kỳ tổ chức nào tham gia hoạt động trung gian dữ liệu (ví dụ các đối tác kết nối vào nền tảng trung gian) đều phải được xác thực danh tính theo quy định pháp luật về định danh và xác thực điện tử. Điều này nhằm bảo đảm rằng các bên tương tác trên hệ thống trung gian (như người cung cấp dữ liệu, người sử dụng dữ liệu) đều có danh tính rõ ràng, đáng tin cậy, giảm nguy cơ giả mạo hoặc gian lận danh tính khi truy cập dữ liệu.

Nhìn chung, những trách nhiệm trên hướng đến việc bảo vệ dữ liệu cá nhân và bảo đảm an toàn, minh bạch trong hoạt động trung gian dữ liệu. Từ góc độ thực tiễn, các công ty cung cấp dịch vụ trung gian dữ liệu sẽ cần xây dựng hệ thống quản trị dữ liệu chặt chẽ. Để dễ hiểu thì một nền tảng trung gian dữ liệu kết nối bệnh viện với công ty nghiên cứu dược phẩm phải ký hợp đồng quy định rõ mục đích sử dụng dữ liệu bệnh nhân; xin sự đồng ý của bệnh nhân trước khi chia sẻ dữ liệu y tế; mã hóa ẩn danh dữ liệu để bảo mật; chỉ cho phép nhà nghiên cứu truy cập dữ liệu trong phạm vi nghiên cứu đã cam kết và nếu phát hiện dữ liệu bị rò rỉ, phải thông báo ngay cho bệnh nhân và cơ quan chức năng liên quan.

**- Trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu**

Loại hình sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu đề cập đến các dịch vụ xử lý, phân tích dữ liệu ở quy mô lớn để tạo ra thông tin, tri thức phục vụ khách hàng, bao gồm các dịch vụ phân tích dữ liệu thị trường, phân tích hành vi khách hàng, hệ thống AI tổng hợp dữ liệu... Điều 31 Nghị định số 169/2025/NĐ-CP đã quy định các trách nhiệm chủ yếu của tổ chức kinh doanh loại sản phẩm, dịch vụ này, bao gồm:

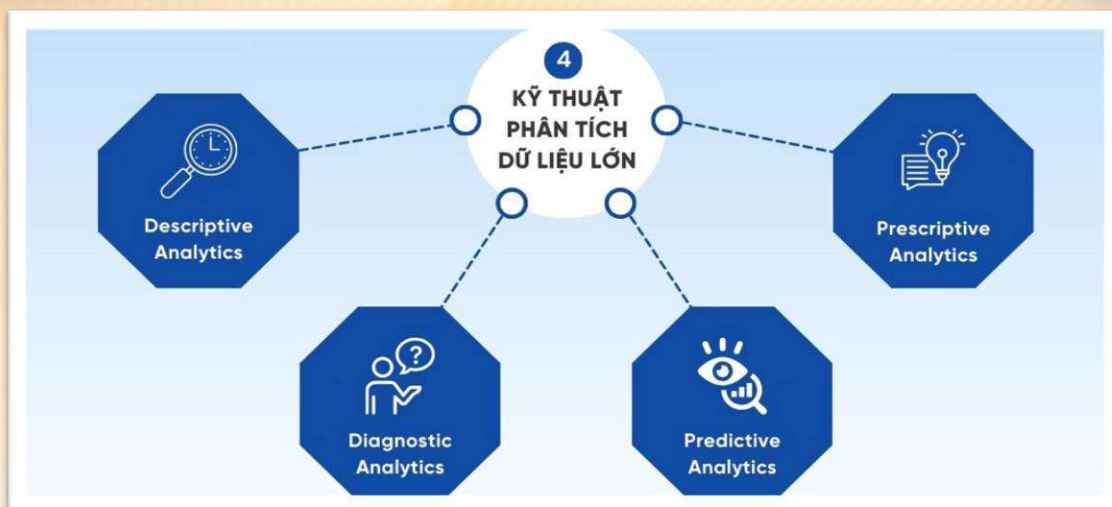




**Thứ nhất, Cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu cho tổ chức, cá nhân trên cơ sở thỏa thuận bằng hợp đồng cung cấp sản phẩm, dịch vụ theo quy định; chịu trách nhiệm về sản phẩm, dịch vụ cung cấp:** Tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu phải ký kết hợp đồng cung cấp dịch vụ với khách hàng (tổ chức, cá nhân sử dụng dịch vụ) và thực hiện trên cơ sở thỏa thuận đó. Đồng thời, họ chịu trách nhiệm về sản phẩm, dịch vụ đã cung cấp, tức là phải đảm bảo kết quả phân tích, báo cáo... đúng như cam kết về chất lượng và phạm vi. Nếu dịch vụ phân tích đưa ra kết quả sai lệch gây thiệt hại cho khách hàng, bên cung cấp có thể phải chịu trách nhiệm bồi thường theo hợp đồng và pháp luật liên quan.

**Thứ hai, Cung cấp đầy đủ thông tin về dịch vụ cho bên sử dụng:** Trong quá trình cung cấp dịch vụ, bên phân tích dữ liệu phải cung cấp đầy đủ và đảm bảo bên sử dụng hiểu rõ các nội dung sau trước khi sử dụng: **(1)** Tên và thông tin liên hệ của đơn vị cung cấp dịch vụ (để khách hàng biết rõ ai chịu trách nhiệm); **(2)** Chức năng, mục đích, phạm vi sử dụng và cơ chế vận hành của sản phẩm/dịch vụ phân tích (tức là dịch vụ sẽ làm gì, sử dụng dữ liệu nào, kết quả ra sao); **(3)** Các tác động, rủi ro có thể ảnh hưởng đến quyền và lợi ích của bên sử dụng (ví dụ: kết quả phân tích có độ chính xác bao nhiêu, rủi ro sai sót/hạn chế của mô hình phân tích, nguy cơ lộ dữ liệu...); **(4)** Thông tin về giấy chứng nhận đủ điều kiện cung cấp dịch vụ (nếu pháp luật yêu cầu phải được cấp phép thì phải nêu rõ số giấy phép, cơ quan cấp...); **(5)** Quyền và nghĩa vụ của bên sử dụng dịch vụ (như quyền yêu cầu giải thích kết quả, nghĩa vụ thanh toán, bảo mật...). Việc minh bạch các thông tin này giúp khách hàng nắm bắt rõ bản chất dịch vụ trước khi đồng ý sử dụng, tránh tình trạng hiểu lầm hay tranh chấp do thiếu thông tin.





## **04 kỹ thuật phân tích dữ liệu lớn quan trọng trong thời đại số - Ảnh: MDA**

**Thứ ba, Tuân thủ pháp luật về dữ liệu và tiêu chuẩn kỹ thuật:** Tổ chức phân tích dữ liệu phải tuân thủ đầy đủ các quy định pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng, an ninh mạng, an ninh dữ liệu, giao dịch điện tử... cũng như tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật liên quan đến dữ liệu và bảo mật thông tin. Họ cũng phải bảo đảm tính chính xác khi cung cấp dịch vụ phân tích. Bên cạnh đó, đơn vị phân tích dữ liệu cần ban hành quy trình hoạt động kinh doanh dịch vụ của mình và phải được cơ quan quản lý nhà nước về dữ liệu đồng ý với quy trình đó. Nói cách khác, quy trình vận hành (bao gồm các bước thu thập dữ liệu, phân tích, kiểm soát chất lượng, bảo mật...) phải được xây dựng rõ ràng và đăng ký hoặc báo cáo với cơ quan quản lý để được phê duyệt.

**Thứ tư, Tuân thủ phương án, quy trình đã phê duyệt:** Sau khi có phương án, quy trình hoạt động được phê duyệt, tổ chức phải tuân thủ nghiêm ngặt các nội dung đã đề ra. Điều này nhằm đảm bảo đơn vị thực hiện đúng cam kết và tiêu chuẩn đã đăng ký, không tự ý thay đổi cách thức hoạt động. Không tự tiện sử dụng dữ liệu khác với phương án đã được duyệt, hoặc không bỏ qua bước kiểm tra an toàn dữ liệu nào đã cam kết.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

**Thứ năm, Báo cáo định kỳ cho cơ quan quản lý:** Tổ chức cung cấp dịch vụ phân tích, tổng hợp dữ liệu thuộc diện quản lý (theo Điều 28 Nghị định 169/2025/NĐ-CP) phải gửi báo cáo định kỳ hàng năm về việc cung cấp dịch vụ. Cụ thể, trước ngày 20 tháng 12 hàng năm, đơn vị phải nộp báo cáo cho Bộ Công an (qua Trung tâm dữ liệu quốc gia) về tình hình cung cấp sản phẩm, dịch vụ phân tích dữ liệu của năm đó, kèm theo các số liệu thống kê từ 15/12 năm trước đến 14/12 năm báo cáo. Ngoài ra, họ phải báo cáo đột xuất khi được yêu cầu (ví dụ khi xảy ra sự cố lớn hoặc phục vụ thanh tra, kiểm tra). Việc báo cáo này giúp cơ quan nhà nước giám sát chặt chẽ hoạt động phân tích dữ liệu, qua đó bảo đảm tuân thủ pháp luật và có căn cứ đánh giá, xử lý nếu có vi phạm.

**Ví dụ:** Một công ty khởi nghiệp cung cấp dịch vụ phân tích dữ liệu tiêu dùng sử dụng trí tuệ nhân tạo để dự đoán xu hướng mua sắm sẽ phải:

**(1)** Ký hợp đồng với khách hàng (ví dụ một hãng bán lẻ) quy định rõ sẽ phân tích dữ liệu gì, nhằm mục đích gì;

**(2)** Cung cấp cho khách hàng thông tin về mô hình AI họ dùng, phạm vi dữ liệu đầu vào (ví dụ: dữ liệu hóa đơn mua hàng 5 năm), cảnh báo các rủi ro (như mô hình có thể chưa đo lường được tác động của dịch bệnh chẳng hạn), cũng như quyền của khách hàng được yêu cầu hiệu chỉnh nếu kết quả phân tích có sai sót;

**(3)** Tuân thủ Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (sắp tới là Luật Bảo vệ cá nhân năm 2025) khi xử lý thông tin khách hàng, bảo mật dữ liệu theo tiêu chuẩn ISO liên quan;

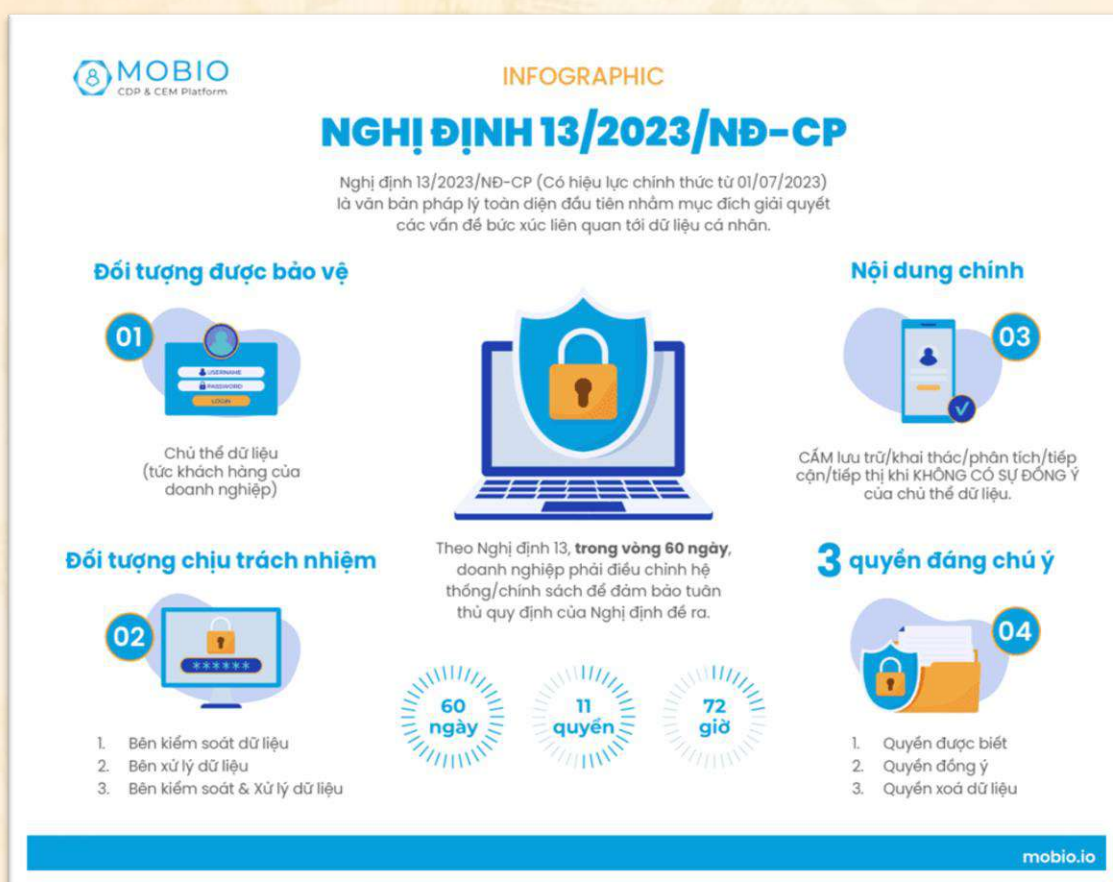
**(4)** Xây dựng quy trình nội bộ về cách thu thập, phân tích, lưu trữ dữ liệu và gửi quy trình này cho Bộ Công an phê duyệt;





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

(5) Định kỳ gửi báo cáo mỗi năm một lần về hoạt động phân tích (số lượng dự án phân tích đã thực hiện, loại dữ liệu đã xử lý, các biện pháp bảo vệ dữ liệu...). Nhờ tuân thủ các trách nhiệm đó, dịch vụ của công ty sẽ vận hành một cách đáng tin cậy, minh bạch, khách hàng có thể yên tâm hơn về kết quả phân tích và dữ liệu của mình được bảo vệ.



## ***Nội dung chính trong Nghị định 13/2023/NĐ-CP Bảo vệ dữ liệu cá nhân***

### ***- Trách nhiệm của tổ chức cung cấp dịch vụ sàn dữ liệu***

Sàn dữ liệu (hay sàn giao dịch dữ liệu) là nền tảng cho phép mua bán, trao đổi dữ liệu giữa các bên theo cơ chế thị trường. Đây có thể xem như “chợ dữ liệu” nơi dữ liệu được coi là hàng hóa đặc thù. Theo Luật Dữ liệu 2024, tổ chức cung cấp dịch vụ sàn dữ liệu thường phải là đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước được cấp phép thành lập hoạt động





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

sản dữ liệu. Nghị định 169/2025/NĐ-CP (Điều 35) quy định nhiều trách nhiệm quan trọng đối với đơn vị vận hành sản dữ liệu, nhằm đảm bảo sản vận hành an toàn, hợp pháp:

**Một là, thẩm định điều kiện của các bên và dữ liệu giao dịch:** Tổ chức cung cấp dịch vụ sản dữ liệu phải kiểm tra, đánh giá việc đáp ứng các điều kiện tham gia sản của mọi chủ thể liên quan, cũng như tính hợp pháp và điều kiện giao dịch của các sản phẩm, dịch vụ dữ liệu được niêm yết. Cụ thể, sản cần xác minh: **(1)** Bên tham gia (người bán, người mua dữ liệu) có đầy đủ năng lực pháp lý theo quy định (cá nhân phải có năng lực hành vi dân sự, tổ chức phải có tư cách pháp nhân hợp lệ); **(2)** Dữ liệu hoặc dịch vụ dữ liệu đưa lên sản có nguồn gốc hợp pháp, nội dung không vi phạm pháp luật, phương thức tạo ra dữ liệu minh bạch, và nếu là loại dữ liệu hạn chế lưu hành thì đã đáp ứng yêu cầu cần thiết; **(3)** Việc sử dụng dữ liệu đó phải đáp ứng yêu cầu an ninh, an toàn, tuân thủ các tiêu chuẩn kỹ thuật về dữ liệu, và cơ chế tiếp nhận, lưu trữ, xử lý dữ liệu trên sản phải bảo đảm an toàn. Việc thẩm định ban đầu này giống như khâu “*kiểm duyệt đầu vào*” nhằm loại trừ dữ liệu bất hợp pháp (thông tin cấm, dữ liệu xâm phạm đời tư chưa được phép...) và đảm bảo các bên giao dịch uy tín.

**Hai là, giám sát hoạt động giao dịch và xử lý vi phạm:** Tổ chức cung cấp dịch vụ sản dữ liệu có trách nhiệm giám sát mọi hoạt động trên sản, bao gồm các giao dịch mua bán dữ liệu, tương tác giữa các bên... nhằm phát hiện kịp thời các vi phạm pháp luật hoặc vi phạm quy chế sản. Sản có quyền quyết định đình chỉ sự tham gia của các bên vi phạm hoặc gỡ bỏ, chấm dứt niêm yết những sản phẩm, dịch vụ dữ liệu vi phạm quy định.

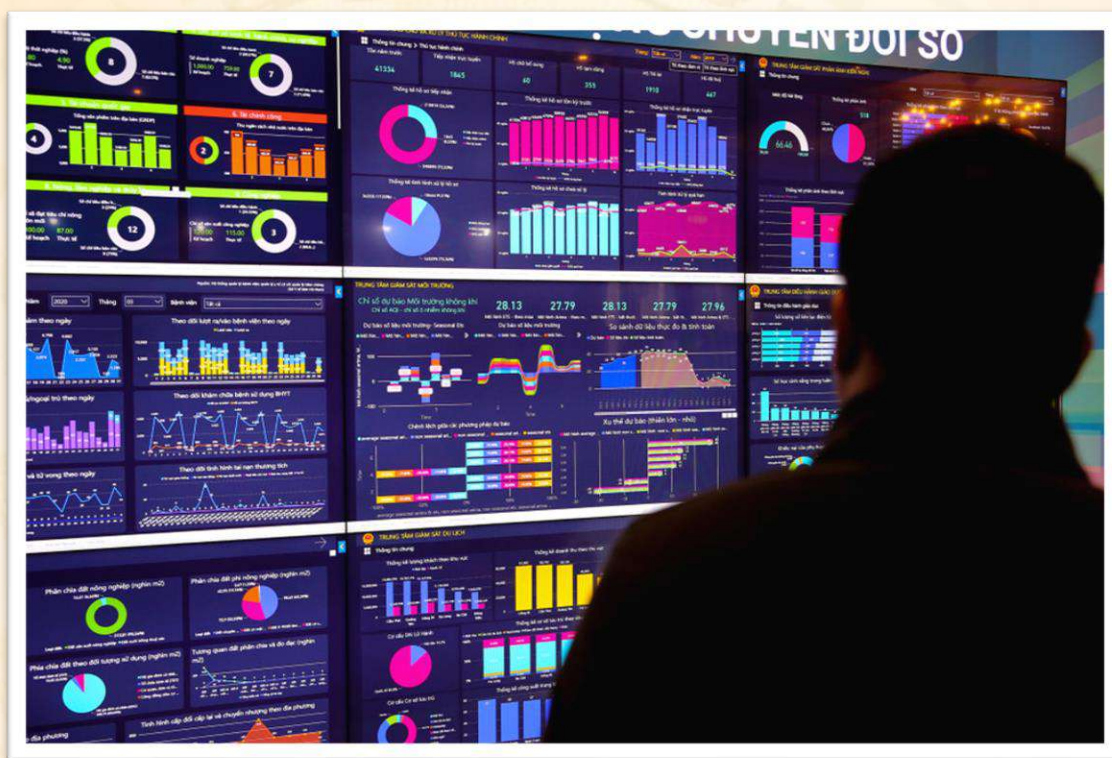
Đồng thời, sản phải thiết lập cơ chế giải quyết tranh chấp giữa các bên một cách kịp thời, hiệu quả. Nếu có hành vi vi phạm pháp luật nghiêm trọng





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

(ví dụ: mua bán dữ liệu trái phép, lừa đảo), sàn cần xử lý, ngăn chặn và báo cáo ngay cho cơ quan nhà nước có thẩm quyền, phối hợp chặt chẽ với các cơ quan này (công an, thanh tra...) trong việc kiểm tra, điều tra và thu thập chứng cứ. Như vậy, sàn dữ liệu hoạt động tương tự một sàn thương mại điện tử, phải vừa tạo môi trường giao dịch tự do, vừa can thiệp khi có dấu hiệu bất thường để bảo vệ người tham gia và trật tự thị trường.



**Ảnh: Thông tấn xã Việt Nam**

**Ba là, ban hành và công khai hoạt động và công khai niêm yết trên trang thông tin điện tử của mình.:** Đơn vị vận hành sàn phải ban hành quy chế hoạt động của sàn và công khai niêm yết quy chế đó trên trang thông tin điện tử của mình. Quy chế hoạt động đóng vai trò tương tự “*điều khoản sử dụng*” của sàn, trong đó phải bao gồm các nội dung chính như: **(1)** Điều kiện tham gia sàn và trách nhiệm của các bên tham gia; **(2)** Quy trình giao dịch (từng bước để thực hiện mua/bán dữ liệu an toàn); **(3)** Yêu cầu bảo mật thông





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

tin và cơ chế chống gian lận; (4) Quản lý rủi ro, xử lý khiếu nại, tranh chấp, bảo vệ dữ liệu cá nhân trên sàn; (5) Điều kiện đối với sản phẩm, dịch vụ dữ liệu được đưa lên sàn (loại dữ liệu nào được phép/cấm giao dịch). Việc niêm yết công khai quy chế giúp mọi người tham gia đều nắm được luật chơi, tạo sự minh bạch và cơ sở để xử lý nếu ai vi phạm quy chế.

**Bốn là, đảm bảo an toàn giao dịch dữ liệu:** Sàn dữ liệu phải thiết lập hệ thống kỹ thuật bảo đảm an toàn giao dịch theo quy định pháp luật. Đồng thời, phải hướng dẫn các bên tham gia sàn về cách bảo vệ dữ liệu, truy xuất nguồn gốc dữ liệu, phát hiện rủi ro; phải có công cụ kiểm tra tuân thủ và sử dụng các biện pháp hiệu quả để bảo vệ dữ liệu cá nhân, quyền riêng tư, bí mật thương mại và dữ liệu quan trọng của các bên liên quan. Nói cách khác, về mặt kỹ thuật, sàn phải xây dựng nền tảng giao dịch bảo mật cao, có kiểm soát như mã hóa dữ liệu khi truyền, xác thực người dùng nhiều lớp, lưu vết giao dịch để truy vết nguồn gốc dữ liệu... nhằm tạo niềm tin cho người mua và người bán dữ liệu rằng giao dịch của họ được bảo vệ tương tự như giao dịch tài chính trực tuyến an toàn.

**Năm là, kế hoạch ứng phó khẩn cấp và đảm bảo dịch vụ 24/7:** Tổ chức vận hành sàn cần xây dựng kế hoạch ứng phó khẩn cấp đối với các sự cố an toàn dữ liệu và định kỳ diễn tập để sẵn sàng xử lý khi xảy ra sự cố. Đồng thời, sàn phải thực hiện việc sao lưu và khôi phục thảm họa cho các hệ thống và cơ sở dữ liệu quan trọng, đảm bảo nếu có sự cố nghiêm trọng (tấn công mạng, mất điện, thiên tai...) thì dữ liệu vẫn được khôi phục, giao dịch sớm trở lại bình thường. Một yêu cầu quan trọng khác là duy trì kênh tiếp nhận thông tin và sử dụng dịch vụ liên tục 24 giờ/ngày, 7 ngày/tuần. Sàn dữ liệu phải luôn sẵn sàng, không có thời gian “đóng cửa” bởi các giao dịch dữ liệu có thể diễn ra bất cứ lúc nào. Chỉ trừ thời gian bảo trì theo lịch (nếu có) cần thông báo trước, còn lại sàn phải hoạt động liên tục.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU Trong công an nhân dân

Sáu là, xây dựng bộ thông số kỹ thuật để đánh giá và quản lý chất lượng sản phẩm, dịch vụ dữ liệu, hệ thống chỉ số đánh giá tài sản dữ liệu, hỗ trợ định giá sản phẩm, dịch vụ dữ liệu:



**Bộ chỉ tiêu đánh giá chất lượng dữ liệu  
thường gặp ở các doanh nghiệp - Ảnh: IPBurger.com**

Một điểm đáng chú ý là sản dữ liệu cần xây dựng bộ thông số kỹ thuật để đánh giá và quản lý chất lượng các sản phẩm, dịch vụ dữ liệu trên sàn, cũng như xây dựng hệ thống chỉ số đánh giá tài sản dữ liệu nhằm hỗ trợ việc định giá tài sản dữ liệu, hỗ trợ định giá sản phẩm, dịch vụ dữ liệu. Việc này có nghĩa sàn phải phát triển tiêu chí để chấm điểm, xếp hạng chất lượng dữ liệu (dựa trên độ đầy đủ, độ cập nhật, tính tin cậy của nguồn dữ liệu,...) và có các chỉ số để định giá dữ liệu một cách công bằng. Đây là trách nhiệm giúp minh bạch hóa giá trị dữ liệu trên thị trường, tránh tình trạng thổi giá hoặc bán dữ liệu chất lượng kém. Chẳng hạn, sàn có thể đưa ra thang điểm chất lượng cho bộ dữ liệu dựa trên nguồn gốc, số lượng bản ghi, tỷ lệ thiếu dữ liệu..., kèm theo khuyến nghị giá tham khảo, giúp người mua lẫn người bán có cơ sở thương thảo giá cả hợp lý.





**Bắt là, báo cáo định kỳ cho cơ quan quản lý:** Tương tự các loại hình trên, tổ chức sàn dữ liệu phải gửi báo cáo định kỳ về hoạt động của sàn. Theo Nghị định, sàn dữ liệu báo cáo 02 lần/năm: báo cáo định kỳ 06 tháng (trước ngày 20/6) và báo cáo định kỳ 01 năm (trước ngày 20/12), gửi Bộ Công an (qua Trung tâm dữ liệu quốc gia). Báo cáo gồm các thông tin thống kê từ ngày 15/12 năm trước đến 14/6 (cho báo cáo định kỳ 06 tháng) hoặc đến 14/12 (cho báo cáo định kỳ 01 năm) về tình hình giao dịch dữ liệu trên sàn, số lượng người tham gia, loại dữ liệu giao dịch, vi phạm phát sinh và cách xử lý... Ngoài ra, sàn cũng phải báo cáo theo yêu cầu đột xuất của cơ quan quản lý khi cần. Quy định này giúp nhà nước theo dõi sự phát triển của thị trường dữ liệu, đồng thời giám sát việc tuân thủ các nghĩa vụ kể trên của sàn.

Như vậy, trách nhiệm của tổ chức cung cấp dịch vụ sàn dữ liệu đòi hỏi khả năng quản trị nền tảng rất cao, tương tự trách nhiệm của chủ sàn thương mại điện tử nhưng ở mức độ khắt khe hơn vì dữ liệu là tài sản đặc biệt. Sàn dữ liệu phải vừa làm “*trọng tài*” công minh, vừa là “*người gác cổng*” đảm bảo *đúng người, đúng dữ liệu, đúng luật*.

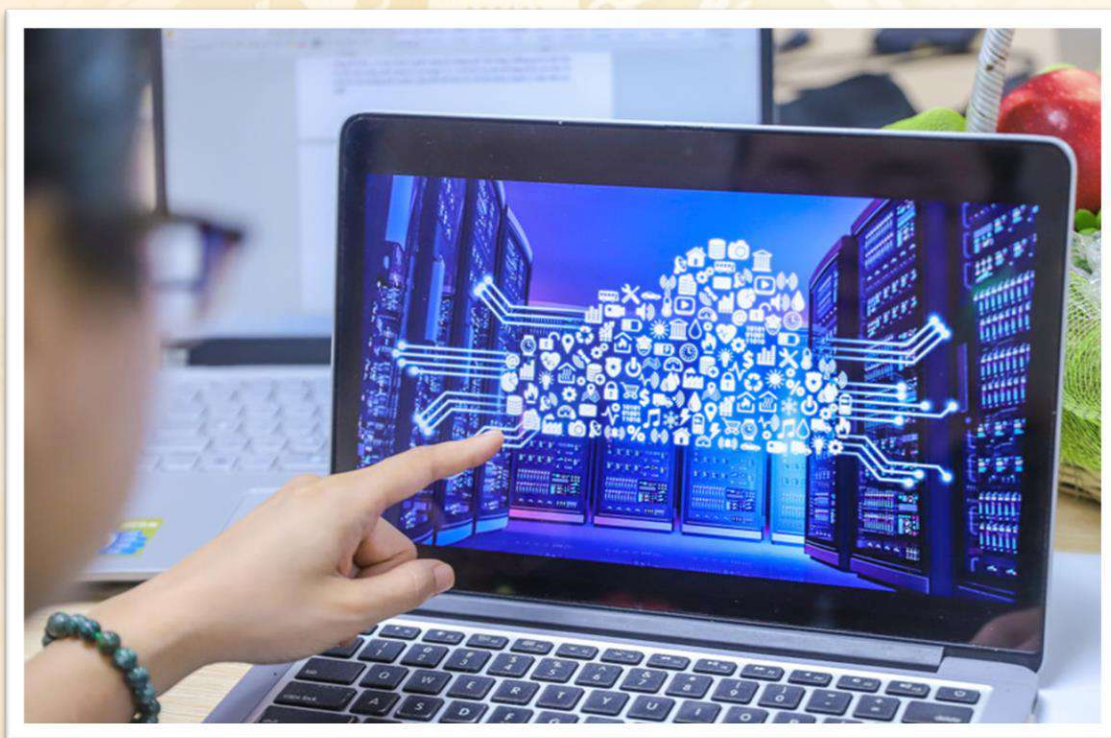
Ví dụ: Giả sử Trung tâm Dữ liệu quốc gia thiết lập một sàn giao dịch dữ liệu quốc gia để các bộ ngành, doanh nghiệp có thể mua bán dữ liệu: Trung tâm này sẽ phải **(1)** Kiểm tra kỹ các cơ quan, doanh nghiệp muốn tham gia sàn (về thẩm quyền chia sẻ dữ liệu, ví dụ một doanh nghiệp phải chứng minh dữ liệu họ bán là do họ thu thập hợp pháp và không thuộc danh mục cấm); **(2)** Xây dựng quy chế sàn quy định rõ cấm giao dịch dữ liệu cá nhân nhạy cảm nếu không có sự đồng ý của cá nhân đó, cấm giao dịch dữ liệu thuộc bí mật nhà nước,..., và công khai cho mọi người tham khảo; **(3)** Liên tục giám sát các giao dịch, nếu thấy một bộ dữ liệu được rao bán có dấu hiệu vi phạm (như chứa thông tin cá nhân công dân mà không có căn cứ pháp lý),





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

sản sẽ tạm đình chỉ giao dịch, thông báo cho Bộ Công an để phối hợp điều tra; (4) Đảm bảo hệ thống sản luôn sẵn sàng, có phương án dự phòng khi lượng giao dịch tăng đột biến, có đội ngũ trực kỹ thuật 24/7 để xử lý nếu hệ thống gặp sự cố; (5) Định kỳ gửi báo cáo cho Bộ Công an về số lượng giao dịch dữ liệu, loại dữ liệu chủ yếu, số vụ vi phạm đã xử lý... Nhờ tuân thủ các trách nhiệm này, sản dữ liệu quốc gia sẽ hoạt động minh bạch, bảo vệ được dữ liệu của các cơ quan, tổ chức, người dân; đồng thời thúc đẩy kinh tế dữ liệu phát triển bền vững và hợp pháp.



***Sản dữ liệu: Đòn bẩy cho nền kinh tế số tại Việt Nam - Ảnh: Minh Sơn***

Trong khuôn khổ bài dự thi, nhóm tác giả đã tiến hành phân tích toàn diện những vấn đề có liên quan đến quy định về sản phẩm, dịch vụ về dữ liệu được quy định tại Luật Dữ liệu năm 2024 và các văn bản có liên quan. Trong đó, nhấn mạnh 03 loại hình then chốt trong hệ sinh thái dữ liệu bao gồm: sản phẩm, dịch vụ trung gian dữ liệu; sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu và dịch vụ sản dữ liệu. Mỗi loại hình đều giữ vai trò khác nhau





nhưng hỗ trợ lẫn nhau trong việc hình thành và phát triển thị trường dữ liệu tại Việt Nam. Bằng cách làm rõ khái niệm, chức năng, vai trò, điều kiện cấp phép và đặc biệt là trách nhiệm pháp lý của từng nhóm chủ thể, nghiên cứu cho thấy rằng pháp luật Việt Nam đang từng bước xây dựng một hệ sinh thái dữ liệu chặt chẽ, minh bạch và có kiểm soát, tạo nền tảng quan trọng để thúc đẩy nền kinh tế dữ liệu phát triển một cách lành mạnh, bền vững và an toàn. Các quy định không chỉ góp phần bảo đảm quyền lợi của tổ chức và cá nhân trong giao dịch dữ liệu, mà còn giúp bảo vệ dữ liệu cá nhân, duy trì an ninh mạng và tạo ra hành lang pháp lý vững chắc cho các mô hình khai thác dữ liệu hiện đại như trí tuệ nhân tạo, phân tích dữ liệu lớn và các nền tảng chia sẻ dữ liệu số.

Với việc xây dựng khuôn khổ pháp lý ngày càng hoàn thiện, cùng với các quy định cụ thể về trách nhiệm của từng chủ thể tham gia, Việt Nam đang dần hội nhập với các chuẩn mực quốc tế trong quản trị dữ liệu và tiến tới hình thành một thị trường dữ liệu số phát triển, an toàn, minh bạch và đáng tin cậy.

## **7.2. ĐỀ XUẤT MỘT SỐ GIẢI PHÁP BẢO ĐẢM AN NINH DỮ LIỆU, AN TOÀN DỮ LIỆU TRONG ỨNG DỤNG CÁC SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU**

*T*rong kỷ nguyên chuyển đổi số, dữ liệu đã trở thành “*tài nguyên chiến lược*” của mỗi quốc gia và doanh nghiệp. Tại Việt Nam vào năm 2022, Bộ trưởng Bộ Công an Tô Lâm từng cho biết dữ liệu cá nhân của hơn 2/3 dân số (khoảng 68 triệu người) đang bị thu thập, chia sẻ trên mạng và thậm chí một khối lượng lớn với khoảng hơn 1.300 GB dữ liệu đã bị khai thác, mua bán trái phép<sup>43</sup>. Nửa đầu

<sup>43</sup> Tony Dang (2023), *Bảo mật dữ liệu trở thành tâm điểm năm 2022*, VNNETWORK, <https://www.vnnetwork.vn/news/bao-mat-du-lieu-tro-thanh-tam-diem-nam-2022/>, truy cập ngày 06/8/2025.





năm 2024, tại Việt Nam đã ghi nhận 46 vụ lộ lọt dữ liệu với khoảng 13 triệu bản ghi thông tin khách hàng bị rò rỉ; các cuộc tấn công bằng mã độc tổng tiền mã hóa 3 TB dữ liệu đã gây thiệt hại ước tính trên 10 triệu USD<sup>44</sup>. Những con số này cho thấy thách thức nghiêm trọng về *an ninh, an toàn dữ liệu* trong thời đại số.

Mặt khác, việc chia sẻ và khai thác dữ liệu đang mở ra cơ hội lớn cho phát triển kinh tế số, từ dịch vụ tài chính, y tế đến thương mại điện tử. Nhiều quốc gia trên thế giới đã ban hành luật và chính sách mạnh mẽ để bảo vệ dữ liệu: Liên minh châu Âu có GDPR, Hoa Kỳ có các đạo luật cấp bang như CCPA, và đặc biệt các nước châu Á có những cách tiếp cận đáng chú ý. Trung Quốc xây dựng “bộ ba” luật dữ liệu gồm Luật An ninh mạng 2017 (CSL), Luật An toàn Dữ liệu 2021 (DSL) và Luật Bảo vệ Thông tin Cá nhân 2021 (PIPL), trong đó yêu cầu doanh nghiệp lưu trữ dữ liệu trong nước, đánh giá an ninh trước khi chuyển dữ liệu ra nước ngoài và cho phép cá nhân có quyền truy cập, chỉnh sửa, rút lại sự đồng ý... đối với dữ liệu của mình. Tương tự, Nhật Bản đã sửa đổi Luật bảo vệ thông tin cá nhân (APPI) tiệm cận GDPR, Hàn Quốc có Đạo luật Bảo vệ Thông tin Cá nhân (PIPA) chặt chẽ hàng đầu châu Á, Singapore có Đạo luật Bảo vệ Dữ liệu Cá nhân (PDPA) cân bằng giữa bảo vệ cá nhân và thúc đẩy đổi mới. Xu thế quốc tế cho thấy muốn hội nhập và giao dịch xuyên biên giới, Việt Nam ***bắt buộc*** phải nâng cao tiêu chuẩn bảo vệ dữ liệu tương đương các chuẩn mực toàn cầu như các Đạo luật kể trên.

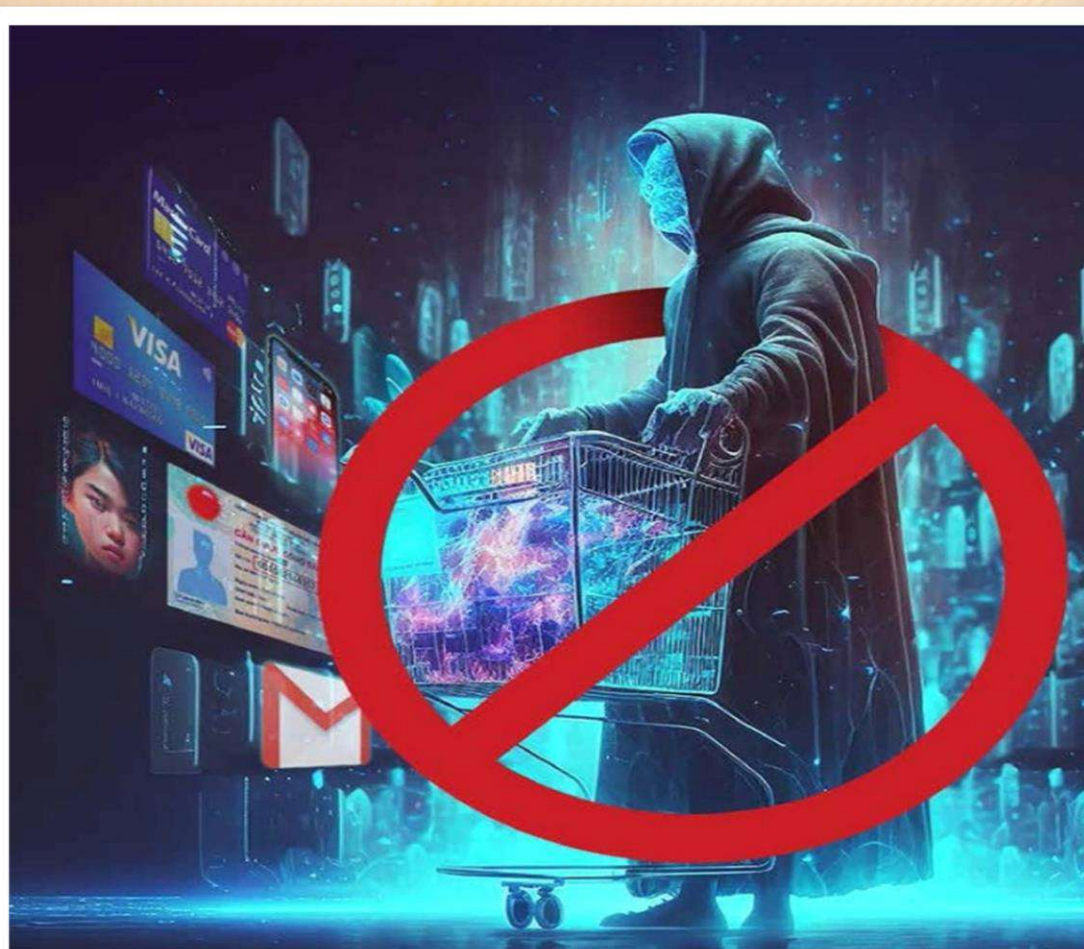
---

<sup>44</sup> Phan Anh (2024), *Hơn 61 triệu tài khoản, bản ghi thông tin cá nhân bị lộ lọt trong nửa đầu năm 2024*, Tạp chí điện tử VnEconomy, <https://vneconomy.vn/hon-61-trieu-tai-khoan-ban-ghi-thong-tin-ca-nhan-bi-lo-lot-trong-nua-dau-nam-2024.htm>, truy cập ngày 06/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



### ***Đảm bảo an ninh, an toàn dữ liệu trong kỷ nguyên số - Ảnh: Internet***

Nhận thức được tầm quan trọng đó, Việt Nam đã ban hành nhiều văn bản pháp luật làm nền tảng cho an ninh, an toàn dữ liệu: từ Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018 đến Nghị định số 53/2022/NĐ-CP hướng dẫn Luật An ninh mạng và Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Đặc biệt, Quốc hội đã thông qua Luật Dữ liệu năm 2024 được xem là luật đầu tiên quy định toàn diện về quản lý, khai thác và bảo vệ dữ liệu số. Luật Dữ liệu 2024 đặt ra các nguyên tắc và yêu cầu nền tảng nhằm phát triển thị trường dữ liệu an toàn, như định nghĩa các loại dữ liệu (mở, quan trọng, cốt lõi) và ràng buộc nghĩa vụ bảo vệ tương ứng. Tuy nhiên, để các quy định pháp luật đi vào cuộc sống và thực sự tạo nên “lá chắn số” bảo vệ dữ





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

liệu, cần một hệ giải pháp đồng bộ từ pháp lý, kỹ thuật, cho tới tổ chức vận hành và ý thức người dùng. Qua quá trình nghiên cứu, nhóm tác giả mạnh dạn đề xuất một số giải pháp trọng tâm nhằm bảo đảm an ninh, an toàn dữ liệu khi ứng dụng các sản phẩm, dịch vụ dữ liệu ở Việt Nam.



### *Quốc hội thông qua Luật Dữ liệu - Ảnh: Báo Chính phủ*

#### **7.2.1. Nguy cơ khi ứng dụng sản phẩm, dịch vụ và dữ liệu gây mất an toàn, trật tự xã hội**

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, dữ liệu và các sản phẩm, dịch vụ dựa trên dữ liệu vừa mở ra cơ hội phát triển to lớn, vừa tiềm ẩn nhiều nguy cơ mất an toàn, trật tự xã hội. Chỉ tính từ đầu năm 2025 đến nay, các cơ quan chức năng đã phát hiện gần 1.500 vụ lừa đảo qua mạng với tổng thiệt hại hơn 1.660 tỷ đồng, đồng thời xử lý hàng nghìn kênh phát tán nội dung độc hại như cờ bạc trực tuyến, quảng bá tiền ảo và buôn bán chất gây nghiện, gây bức xúc trong dư luận và bất ổn trong cộng đồng. Thứ trưởng Bộ Công an Phạm Thế Tùng cũng cảnh báo, không gian mạng vừa là động





lực phát triển kinh tế - xã hội, vừa chứa đựng nhiều rủi ro đe dọa an ninh quốc gia nếu thiếu các biện pháp bảo vệ hữu hiệu. Trên thực tế, sự gia tăng của tin giả, công nghệ deepfake, tấn công mạng vào hạ tầng số, cùng với việc khai thác, mua bán dữ liệu trái phép đã và đang tạo ra những thách thức nghiêm trọng, không chỉ với quản lý nhà nước mà còn đối với niềm tin của nhân dân. Trong bối cảnh đó, việc nhận diện đầy đủ các nguy cơ này là tiền đề để đề xuất những giải pháp toàn diện, đảm bảo an ninh dữ liệu và giữ vững trật tự an toàn xã hội trong kỷ nguyên số.

### ***7.2.1.1. Nguy cơ xâm phạm dữ liệu nhạy cảm và quyền riêng tư của cá nhân từ các sản phẩm, dịch vụ về dữ liệu***

Trong kỷ nguyên số, dữ liệu cá nhân trở thành “tài nguyên chiến lược” không chỉ đối với phát triển kinh tế mà còn gắn chặt với bảo đảm an ninh, trật tự xã hội. Tuy nhiên, thực tiễn cho thấy nguy cơ xâm phạm dữ liệu và quyền riêng tư của cá nhân ngày càng hiện hữu và phức tạp. Nguyên nhân sâu xa xuất phát từ việc thu thập, xử lý dữ liệu cá nhân trên diện rộng nhưng thiếu biện pháp bảo mật tương xứng, trong khi ý thức bảo vệ dữ liệu của nhiều tổ chức, cá nhân còn hạn chế. Ngoài ra, hoạt động tấn công mạng ngày càng tinh vi và có tổ chức, tận dụng lỗ hổng kỹ thuật hoặc sự bất cẩn của người dùng để đánh cắp dữ liệu. Mặc dù hành lang pháp lý tuy đã được hình thành nhưng còn mới mẻ và chưa đồng bộ, trong khi nhiều tổ chức, cá nhân chưa có nhận thức đầy đủ về tầm quan trọng của bảo vệ dữ liệu. Các hệ thống thông tin của cơ quan nhà nước, doanh nghiệp, trường học... thường xuyên trở thành mục tiêu của tin tặc, và khi dữ liệu bị đánh cắp, hậu quả không chỉ ảnh hưởng tới cá nhân mà còn lan rộng, gây bất ổn xã hội.

*Thực tiễn tại Việt Nam* đã ghi nhận nhiều vụ việc nghiêm trọng. Năm 2022, dữ liệu của khoảng 30 triệu học sinh, giáo viên bị rao bán công khai





trên diễn đàn hacker nước ngoài với mức giá chỉ 3.500 USD, trong đó có đầy đủ thông tin cá nhân như họ tên, ngày sinh, địa chỉ, email, số điện thoại<sup>45</sup>. Theo báo cáo do Công ty An ninh mạng Viettel (Viettel Cyber Security) công bố, 14,5 triệu tài khoản tại Việt Nam đã bị rò rỉ dữ liệu trong năm 2024. Báo cáo xây dựng dựa trên dữ liệu từ Hệ thống Tri thức an ninh mạng (Viettel Threat Intelligence). Theo báo cáo, trong năm 2024, hệ thống ghi nhận nguy cơ mất an toàn thông tin tại Việt Nam tiếp tục lan rộng, minh chứng ở các cuộc tấn công mạng gia tăng cả về số lượng, các phương thức và quy mô tấn công ngày càng tinh vi hơn<sup>46</sup>. Đặc biệt, nền tảng ONUS - một ứng dụng giao dịch tiền mã hóa đã bị hacker tấn công, khiến gần 2 triệu hồ sơ khách hàng bị đánh cắp và rao bán trên chợ đen. Những vụ việc này cho thấy khoảng trống lớn trong năng lực bảo mật của cả khu vực công lẫn tư, đồng thời phản ánh mức độ dễ tổn thương của người dân khi dữ liệu bị xâm phạm.

Nguy cơ này không chỉ dừng lại ở việc lộ lọt dữ liệu cá nhân đơn lẻ, mà còn ở khả năng lạm dụng và tái nhận dạng dữ liệu. Với sự phát triển của công nghệ trí tuệ nhân tạo và dữ liệu lớn, kẻ xấu có thể kết hợp các nguồn dữ liệu khác nhau để dựng lại hồ sơ toàn diện về một cá nhân, từ đó tiến hành hành vi mạo danh, lừa đảo tài chính, tống tiền hoặc thậm chí thao túng chính trị - xã hội. Hậu quả là người dân mất quyền kiểm soát dữ liệu suốt đời làm cho uy tín của doanh nghiệp, tổ chức bị suy giảm nghiêm trọng, còn nhà nước đối mặt với nguy cơ mất ổn định xã hội khi niềm tin vào tiến trình chuyển đổi số bị lung lay. Một khi dữ liệu đã bị phát tán trên không gian

<sup>45</sup> Lưu Quý (2022), Hacker rao bán dữ liệu trường học của 30 triệu người Việt, <https://vnexpress.net/hacker-rao-ban-du-lieu-truong-hoc-cua-30-trieu-nguoi-viet-4486789.html>, Truy cập ngày 01/8/2025

<sup>46</sup> Cebid (2024), Năm 2024: Hơn 14 triệu tài khoản tại Việt Nam bị rò rỉ dữ liệu, Cebid.vn, truy cập ngày 01/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

mạng, việc thu hồi là gần như không thể, khiến hậu quả kéo dài nhiều năm và khó lường.



***Bảo vệ dữ liệu cá nhân trên không gian mạng là trách nhiệm của mỗi cá nhân trong kỷ nguyên số - Ảnh: Cổng thông tin điện tử Công an tỉnh Khánh Hòa***

Việc nhận diện đầy đủ nguy cơ xâm phạm dữ liệu cá nhân có ý nghĩa đặc biệt quan trọng. Đối với cơ quan nhà nước, đây là cơ sở để xây dựng và hoàn thiện hành lang pháp lý như Luật Dữ liệu năm 2024, Nghị định 13/2023/NĐ-CP, đồng thời thúc đẩy đầu tư vào hạ tầng bảo mật và quy trình xử lý sự cố. Đối với các bộ, ngành, tổ chức, nhận thức đúng sẽ giúp họ triển khai cơ chế quản trị dữ liệu, nâng cao trách nhiệm bảo vệ thông tin công dân, khách hàng. Đối với doanh nghiệp, đây là động lực để xây dựng niềm tin với người dùng, coi an toàn dữ liệu là lợi thế cạnh tranh. Và đối với người dân, sự nhận thức sẽ giúp họ thận trọng hơn trong việc chia sẻ dữ liệu, đồng thời





chủ động bảo vệ quyền riêng tư của bản thân. Như vậy, nhận thức đúng đắn và kịp thời về nguy cơ này chính là bước đầu tiên để xây dựng một xã hội số an toàn, minh bạch và bền vững.

### ***7.2.1.2. Nguy cơ lợi dụng các sản phẩm, dịch vụ về dữ liệu để thao túng dư luận và lan truyền nội dung sai sự thật***

Nguy cơ này bắt nguồn từ sự phát triển mạnh mẽ của các nền tảng số, mạng xã hội và dịch vụ dữ liệu trực tuyến. Các thuật toán phân tích hành vi, gợi ý nội dung và quảng cáo được thiết kế để tối đa hóa thời gian tương tác của người dùng, vô tình hoặc cố ý tạo điều kiện cho việc lan truyền thông tin sai lệch. Ngoài ra, sự thiếu kiểm chứng trong thu thập và xử lý dữ liệu, cùng với tốc độ lan truyền cực nhanh của thông tin trong môi trường mạng, đã khiến cho tin giả, thông tin xuyên tạc và nội dung sai sự thật dễ dàng được phát tán rộng rãi. Ở Việt Nam, các cơ quan chức năng từng nhiều lần cảnh báo về tình trạng “tin giả”, các đối tượng thường xuyên lợi dụng các sự kiện nóng (dịch bệnh, bầu cử, thiên tai, chính sách mới) để gây nhiễu loạn thông tin và tạo tâm lý hoang mang trong xã hội.

Nguy cơ này thể hiện trên nhiều phương diện của đời sống xã hội. Trên phương diện truyền thông, các trang mạng xã hội như Facebook, TikTok, YouTube... thường xuyên bị lợi dụng để phát tán tin giả về chính sách, dịch bệnh, đời tư lãnh đạo hoặc các sự kiện xã hội. Chẳng hạn, trong đại dịch COVID-19, hàng loạt tin giả về thuốc chữa bệnh, tình hình phong tỏa, hay chính sách tiêm vaccine đã gây ảnh hưởng trực tiếp tới niềm tin của người dân. Trên phương diện chính trị, các thế lực thù địch lợi dụng không gian mạng để tung tin thất thiệt, xuyên tạc đường lối, chính sách của Đảng và Nhà nước, nhằm kích động bất mãn, chia rẽ khối đại đoàn kết dân tộc. Trên phương diện khoa học - công nghệ, sự xuất hiện của công nghệ deepfake và





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

trí tuệ nhân tạo đã làm cho việc tạo ra nội dung giả mạo ngày càng tinh vi. Video, hình ảnh, giọng nói giả khó phân biệt với thật, tạo điều kiện cho kẻ xấu bịa đặt, bôi nhọ hoặc phát tán thông điệp sai lệch với mục đích thao túng dư luận. Ngoài ra, tin giả còn được khai thác để thao túng thị trường, tung tin thất thiệt về giá cổ phiếu, sản phẩm, dịch vụ nhằm trục lợi bất chính.



***Mạng xã hội tiềm ẩn rất nhiều rủi ro - Ảnh: Báo Quân đội nhân dân***

Thao túng dư luận và lan truyền tin giả là hành vi mang tính chất đặc biệt nguy hiểm bởi phạm vi tác động nhanh chóng và rộng lớn. ***Thứ nhất***, nó đe dọa đến sự ổn định xã hội, gây tâm lý hoang mang, mất niềm tin vào thông tin chính thống, thậm chí kích động biểu tình, tụ tập đông người trái phép. ***Thứ hai***, nó xói mòn niềm tin vào thể chế chính trị, ảnh hưởng trực





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

tiếp đến uy tín và năng lực quản lý của Nhà nước. **Thứ ba**, tin giả còn gây thiệt hại kinh tế khi doanh nghiệp, nhà đầu tư hoặc người dân đưa ra quyết định sai lầm dựa trên thông tin không chính xác. Nguy hiểm hơn, trong bối cảnh toàn cầu hóa thông tin, các chiến dịch tung tin giả có thể được tổ chức xuyên biên giới, do các thế lực bên ngoài hậu thuẫn, nhằm can thiệp vào tình hình chính trị - xã hội trong nước.

Việc nhận diện đúng và đầy đủ nguy cơ này có ý nghĩa quan trọng đối với mọi chủ thể trong xã hội. Với các cơ quan quản lý nhà nước, đây là cơ sở để ban hành và hoàn thiện khung pháp lý như Luật An ninh mạng 2018, Luật Dữ liệu 2024 và các nghị định hướng dẫn, nhằm quy định rõ trách nhiệm của nền tảng số và cá nhân trong việc ngăn chặn, gỡ bỏ tin giả. Với các bộ, ngành, tổ chức, nhận thức đúng nguy cơ sẽ thúc đẩy họ triển khai cơ chế giám sát thông tin, phối hợp với cơ quan chức năng và truyền thông chính thống để kịp thời xử lý, định hướng dư luận. Với doanh nghiệp công nghệ, đây là động lực để đầu tư vào các công cụ trí tuệ nhân tạo nhằm phát hiện và gắn nhãn tin giả, đồng thời minh bạch hóa hoạt động của thuật toán gợi ý nội dung. Còn với người dân, việc hiểu được nguy cơ sẽ giúp nâng cao năng lực “*miễn dịch thông tin*”, biết cách kiểm chứng, chọn lọc nguồn tin và không tiếp tay phát tán nội dung sai sự thật.

Như vậy, nhận thức rõ nguy cơ lợi dụng các sản phẩm, dịch vụ dữ liệu để thao túng dư luận và lan truyền tin giả không chỉ là yêu cầu cấp bách để bảo vệ an ninh, trật tự xã hội, mà còn là điều kiện tiên quyết để xây dựng một không gian mạng lành mạnh, an toàn, góp phần giữ vững niềm tin xã hội và tạo nền tảng vững chắc cho quá trình chuyển đổi số quốc gia.





## **7.2.1.3. Nguy cơ tấn công mạng gây gián đoạn hạ tầng số và hệ thống dịch vụ công quốc gia**

Trong bối cảnh hạ tầng số ngày càng trở thành “xương sống” của quản lý nhà nước và cung cấp dịch vụ công, nguy cơ bị tấn công mạng gia tăng cả về tần suất lẫn mức độ. Các hình thức tấn công chủ yếu bắt nguồn từ: **(i)** sự gia tăng các lỗ hổng bảo mật trong hệ thống công nghệ thông tin của các cơ quan, tổ chức khi triển khai dịch vụ công trực tuyến; **(ii)** sự phát triển về âm mưu, thủ đoạn ngày càng tinh vi của tội phạm mạng sử dụng mã độc, tấn công từ chối dịch vụ (DDoS), ransomware để làm tê liệt hệ thống; **(iii)** nguồn lực đảm bảo an ninh mạng chưa đồng bộ, thiếu nhân lực chất lượng cao, thiếu quy trình ứng phó sự cố theo chuẩn quốc tế; **(iv)** yếu tố xung đột địa chính trị và an ninh phi truyền thống cũng là nguyên nhân khiến các cơ sở hạ tầng trọng yếu của quốc gia trở thành mục tiêu bị nhắm tới.



***Nâng cao cảnh giác với các cuộc tấn công mạng  
vào thời điểm nhạy cảm - Ảnh: Internet***





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

*Nguy cơ tấn công mạng gây gián đoạn hạ tầng số và hệ thống dịch vụ công quốc gia thể hiện trên nhiều phương diện đan xen.* Trước hết, ở phương diện kỹ thuật, các cơ sở dữ liệu và hệ thống thông tin trọng yếu như dân cư, đất đai, tài chính, y tế... luôn đứng trước nguy cơ bị tin tặc xâm nhập, đánh cắp hoặc phá hoại, dẫn đến rối loạn hoạt động toàn diện. Tiếp đến, ở phương diện dịch vụ công, các cổng thông tin điện tử, hệ thống khai thuế, hải quan hay đăng ký kinh doanh có thể bị tấn công từ chối dịch vụ, làm gián đoạn quá trình phục vụ người dân và doanh nghiệp. Trên phương diện xã hội, khi những dịch vụ thiết yếu không thể vận hành thông suốt, niềm tin của người dân đối với cơ quan công quyền sẽ suy giảm, dễ dẫn đến tâm lý hoang mang, bất an, thậm chí nảy sinh bất ổn xã hội. Ngoài ra, trên phương diện an ninh quốc gia, các cuộc tấn công mạng không chỉ đơn thuần nhằm mục đích phá hoại kinh tế mà còn có thể mang động cơ chính trị, do các thế lực bên ngoài hậu thuẫn, nhằm làm suy yếu hệ thống hạ tầng trọng yếu, gây rối loạn trật tự và thách thức trực tiếp tới an ninh, chủ quyền quốc gia.

Về hình thức, các hình thức tấn công mạng của số tội phạm công nghệ cao được thực hiện rất đa dạng, sử dụng nhiều công cụ, cách thức tấn công khác nhau. Điển hình như:

+ **Tấn công bằng mã độc (Malware, Ransomware).** Bản chất của phương thức này là cài mã độc vào hệ thống thông tin quốc gia (qua email giả mạo, file đính kèm, USB nhiễm độc), đặc biệt là ransomware mã hóa toàn bộ dữ liệu, buộc nạn nhân phải trả tiền chuộc. Nếu tấn công thành công vào cơ sở dữ liệu quốc gia (dân cư, đất đai, tài chính), hậu quả sẽ đặc biệt nghiêm trọng, có thể làm tê liệt hoạt động hành chính.

+ **Tấn công từ chối dịch vụ (Dos/DDoS).** Tin tặc sử dụng lượng lớn truy cập giả mạo để làm quá tải hệ thống, khiến cổng thông tin điện tử, cổng dịch





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

vụ công hoặc hệ thống khai thuế, hải quan... bị tê liệt nhằm làm gián đoạn dịch vụ công trực tuyến, làm người dân và doanh nghiệp không thể thực hiện thủ tục hành chính, ảnh hưởng tới niềm tin và hiệu quả quản lý nhà nước.

+ **Tấn công khai thác lỗ hổng.** Các đối tượng lợi dụng lỗ hổng trong phần mềm, ứng dụng quản lý nhà nước hoặc nền tảng dịch vụ công (chưa được vá lỗi, sử dụng phiên bản cũ) để có thể chiếm quyền quản trị, đánh cắp dữ liệu, thay đổi thông tin trong hồ sơ, gây rối loạn quản lý.

+ **Tấn công giả mạo (Phishing, Social Engineering).** Đó là đánh lừa cán bộ, công chức hoặc người dân truy cập vào website giả mạo cổng dịch vụ công, hoặc mở email lừa đảo để đánh cắp tài khoản, mật khẩu để chiếm quyền truy cập hệ thống, giả mạo thủ tục hành chính, hoặc đánh cắp dữ liệu định danh cá nhân.

+ **Tấn công hạ tầng trọng yếu về an ninh quốc gia.** Các đối tượng nhắm trực tiếp vào hệ thống điều khiển công nghiệp (SCADA/ICS) của điện lực, viễn thông, giao thông, ngân hàng nhằm làm tê liệt toàn bộ nền kinh tế - xã hội, gây mất ổn định chính trị, an ninh quốc gia.

+ **Tấn công nội gián (Insider Threats).** Người trong nội bộ có thể bị không chế, cưỡng ép hoặc có âm mưu, hoạt động lợi dụng quyền truy cập để đánh cắp, bán dữ liệu hoặc phá hoại hệ thống. Đây là hình thức khó phát hiện nhất vì kẻ tấn công có sẵn quyền truy cập hợp pháp. Nếu xảy ra trong hệ thống dữ liệu quốc gia, hậu quả đặc biệt nghiêm trọng.

+ **SQL Injection:** Kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject và thi hành các câu lệnh SQL bất hợp pháp.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Zero-day:** Dù quản trị viên hệ thống hoặc các nhà phát triển phần mềm có nỗ lực đến đâu, hầu như mọi phần cứng và phần mềm đều tồn tại lỗi. Nếu lỗi đó gây ra rủi ro bảo mật, nó sẽ được gọi là lỗ hổng. Mức độ khai thác của các lỗ hổng này rất khác nhau, có cái gần như không thể bị lợi dụng, có cái có thể bị dùng để gây gián đoạn thiết bị thông qua tấn công từ chối dịch vụ. Nguy hiểm nhất là những lỗ hổng cho phép kẻ tấn công chen và thực thi mã độc của riêng họ mà người dùng hoàn toàn không hay biết. Mặc dù thuật ngữ "zero-day" ban đầu dùng để chỉ khoảng thời gian kể từ khi nhà cung cấp phát hiện ra lỗ hổng, nhưng ngày nay nó cũng được hiểu là những lỗ hổng mà chưa có bản vá hay bất kỳ biện pháp khắc phục nào được đưa ra.

+ **Man-in-the-Middle:** Một cuộc tấn công mà kẻ tấn công bí mật chuyển tiếp và có thể làm thay đổi giao tiếp giữa hai bên mà họ tin rằng họ đang trực tiếp giao tiếp với nhau.



*Mã độc PlugX nghi do nhóm Mustang Panda phát triển là thủ đoạn để khai thác thông tin trái phép từ các hệ thống thông tin thông qua USB - Ảnh: Coro*





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

*Các hành vi tấn công mạng vào hệ thống thông tin quốc gia và nền tảng dịch vụ công thường bắt nguồn từ nhiều động cơ khác nhau: (1) Động cơ kinh tế - tài chính*, khi tin tặc tìm cách chiếm đoạt dữ liệu, lừa đảo hoặc tống tiền bằng mã độc để thu lợi bất chính. (2) *Động cơ chính trị - phản động*, khi các thế lực thù địch muốn gây rối loạn xã hội, làm suy giảm niềm tin của nhân dân vào Nhà nước thông qua việc tê liệt dịch vụ công hay phá hoại cơ sở dữ liệu trọng yếu. (3) *Động cơ tình báo - gián điệp* cũng rất đáng chú ý, khi dữ liệu dân cư, tài chính, y tế bị thu thập lén lút nhằm phân tích cấu trúc xã hội và năng lực quản trị quốc gia. (4) Một số nhóm cực đoan còn mang *động cơ khủng bố*, tấn công để gieo rắc hoang mang, bất ổn xã hội. (5) Có những trường hợp chỉ vì *động cơ cá nhân*, muốn thử nghiệm kỹ năng hoặc khẳng định vị thế trong cộng đồng hacker. Tất cả các động cơ này đều cho thấy mức độ nguy hiểm đa tầng của tấn công mạng, đòi hỏi sự cảnh giác và ứng phó toàn diện của cơ quan nhà nước, tổ chức và công dân.

*Hậu quả của tấn công mạng vào hạ tầng số và dịch vụ công quốc gia mang tính dây chuyền và đặc biệt nghiêm trọng. Thứ nhất*, nó gây gián đoạn hoạt động quản lý và điều hành của Nhà nước, ảnh hưởng trực tiếp tới người dân và doanh nghiệp. *Thứ hai*, thiệt hại kinh tế rất lớn, khi nhiều giao dịch, hợp đồng, dịch vụ bị đình trệ; chi phí khắc phục, khôi phục hệ thống tốn kém. *Thứ ba*, nguy cơ này còn đe dọa đến an ninh quốc phòng, bởi hạ tầng số gắn với năng lượng, giao thông, viễn thông, y tế và tài chính đều là mục tiêu có thể bị lợi dụng để phá hoại. *Thứ tư*, trong bối cảnh xã hội số, một sự cố gián đoạn diện rộng có thể tạo nên khủng hoảng niềm tin, ảnh hưởng tới uy tín của Nhà nước và tác động lâu dài đến an ninh chính trị - xã hội.

*Nhận thức đúng về nguy cơ tấn công mạng gây gián đoạn hạ tầng số có ý nghĩa quyết định đối với việc xây dựng một xã hội số an toàn. (1) Đối*





với cơ quan nhà nước, đây là cơ sở để ưu tiên nguồn lực đầu tư cho bảo mật hạ tầng thông tin trọng yếu, triển khai Chiến lược an ninh mạng quốc gia, đồng thời ban hành cơ chế phối hợp ứng cứu sự cố nhanh chóng, hiệu quả. Việc hiểu rõ nguy cơ giúp nâng cao trách nhiệm trong việc giám sát an ninh mạng, cập nhật thường xuyên các bản vá bảo mật, thực hiện diễn tập định kỳ. **(2) Đối với doanh nghiệp công nghệ**, nhận thức này thúc đẩy họ phát triển các giải pháp phòng thủ tiên tiến, tham gia cung cấp dịch vụ an toàn thông tin. **(3) Đối với công dân**, sự hiểu biết về nguy cơ giúp nâng cao cảnh giác, chủ động phòng tránh các hành vi lừa đảo mạng, đồng thời hợp tác với cơ quan chức năng trong bảo vệ không gian mạng.

Như vậy, nguy cơ tấn công mạng gây gián đoạn hạ tầng số và hệ thống dịch vụ công quốc gia không chỉ là thách thức công nghệ, mà còn là thách thức an ninh phi truyền thống đe dọa trực tiếp đến an toàn xã hội và sự ổn định quốc gia. Nhận thức và hành động kịp thời để phòng ngừa, ứng phó chính là yếu tố then chốt để xây dựng không gian mạng an toàn, bền vững cho tiến trình chuyển đổi số ở Việt Nam.

#### **7.2.1.4. Nguy cơ thao túng và giả mạo thông tin từ trí tuệ nhân tạo và công nghệ deepfake**

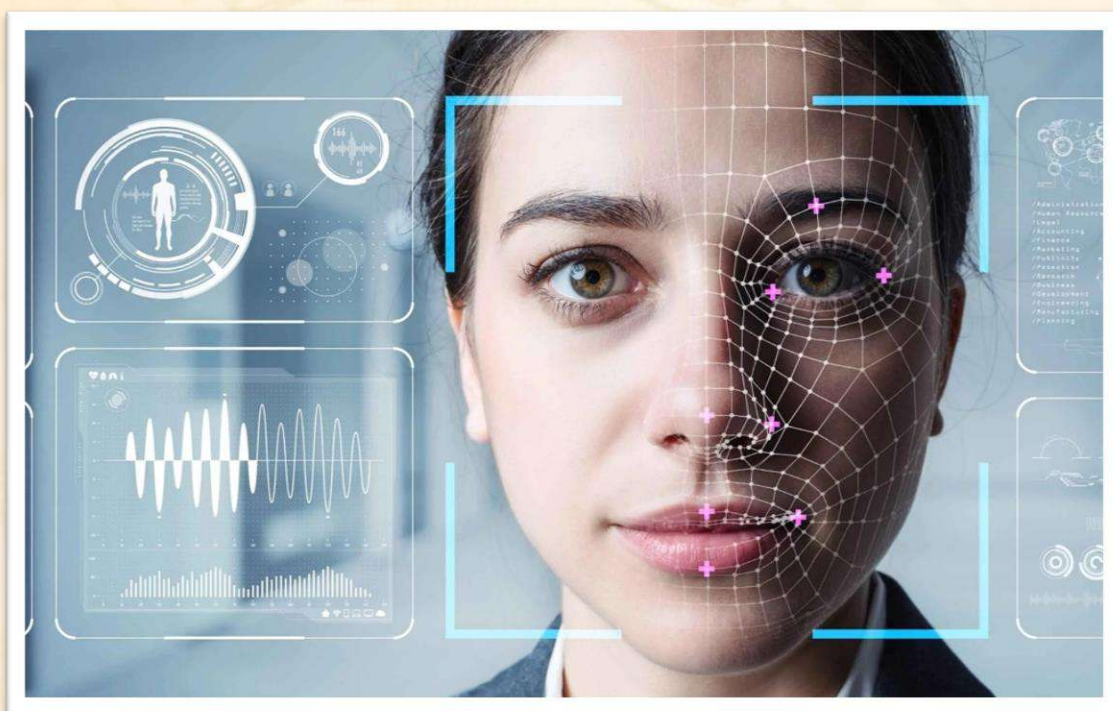
Nguy cơ này xuất phát từ sự phát triển nhanh chóng và mạnh mẽ của công nghệ trí tuệ nhân tạo (AI), đặc biệt là các thuật toán học máy và mô hình sinh dữ liệu. Trên nền tảng dữ liệu khổng lồ được thu thập và xử lý, các hệ thống AI có khả năng tạo ra văn bản, hình ảnh, âm thanh và video có độ chân thực cao, thậm chí khó phân biệt với thông tin thật. Deepfake - công nghệ giả mạo hình ảnh, giọng nói bằng AI là ví dụ điển hình cho thấy khả năng tái hiện con người, sự kiện một cách tinh vi, dễ bị kẻ xấu lợi dụng. Khoảng năm 2017, thuật ngữ “deepfake” xuất hiện lần đầu tiên trên diễn





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

đàn Reddit, khi một số người dùng sử dụng công nghệ học sâu để ghép mặt người nổi tiếng vào video. Từ đó, deepfake nhanh chóng lan rộng và trở thành công cụ phổ biến để giả mạo hình ảnh, giọng nói, video. Ngoài ra, việc các thuật toán được thiết kế chủ yếu để tối ưu hóa hiệu quả kinh tế (như tăng tương tác, thu hút quảng cáo) nhưng thiếu cơ chế kiểm soát chuẩn mực đạo đức và pháp lý cũng góp phần tạo ra nguy cơ lan truyền thông tin độc hại.



### **Tấn công deepfake - mạo danh lãnh đạo là lỗ hổng chí mạng an ninh doanh nghiệp hiện đại - Ảnh: VnEconomy**

Trước hết, ở *phương diện truyền thông*, các sản phẩm deepfake có thể được sử dụng để tạo ra video, hình ảnh giả mạo lãnh đạo, cán bộ hoặc người nổi tiếng, phát tán trên mạng xã hội nhằm bôi nhọ danh dự, gây hoang mang dư luận, hoặc lừa đảo người dân. Tiếp đó, deepfake có thể trở thành công cụ để các thế lực thù địch thực hiện chiến dịch tung tin sai lệch, xuyên tạc đường lối, chính sách của Đảng và Nhà nước, thậm chí can thiệp vào các sự kiện chính trị trọng yếu của quốc gia. Ví dụ, chúng có thể tạo ra các đoạn phát





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

biểu sai sự thật, gán ghép tuyên bố chính trị nhạy cảm nhằm gây hiểu lầm, làm mất uy tín cá nhân, thậm chí kích động sự nghi ngờ, chia rẽ giữa nhân dân với Nhà nước. Không chỉ vậy, khi những sản phẩm “deepfake” với mục đích xấu về chính trị được phát tán rộng rãi trên mạng xã hội, chúng tạo cảm giác như thông tin “*có thật*”, khiến một bộ phận người dân hoang mang và mất niềm tin vào đường lối, chính sách đúng đắn của Đảng và Nhà nước.



***Tập đoàn thiết kế kiến trúc Arup trở thành nạn nhân của vụ lừa đảo deepfake - Ảnh: Bộ Khoa học và Công nghệ***

Ngoài việc xuyên tạc chính sách, deepfake còn có thể bị lợi dụng để “*dựng bằng chứng giả*” về các sự kiện xã hội, chẳng hạn dựng video cảnh sát bạo hành, cán bộ tham nhũng... nhằm kích động bức xúc, lôi kéo người dân xuống đường biểu tình, gây mất an ninh, trật tự. Đây là thủ đoạn tinh vi vì người xem khó phân biệt thật - giả, dễ dẫn tới phản ứng tức thời, vượt ngoài kiểm soát. Trên phương diện kinh tế - tài chính, việc sử dụng AI để giả mạo giọng nói hoặc hình ảnh lãnh đạo doanh nghiệp đã từng được ghi nhận ở nhiều nước, gây ra những vụ lừa đảo tài chính với thiệt hại hàng chục





triệu USD. Điển hình, tại Hồng Kông, một nhân viên tài chính tập đoàn thiết kế và kỹ thuật đa quốc gia Arup của Anh đã bị lừa thực hiện chuyển tiền khoảng 25 triệu USD sau khi tham gia một cuộc gọi video nơi toàn bộ người tham gia đều là deepfake, gồm cả Giám đốc tài chính và đồng nghiệp cấp cao<sup>47</sup>. Cuối cùng, các thuật toán thiên lệch trong xử lý dữ liệu có thể dẫn đến phân biệt đối xử trong tín dụng, tuyển dụng, an sinh xã hội, gây bất công và bất bình trong xã hội.

Rủi ro từ AI và deepfake mang tính chất đặc biệt nguy hiểm bởi khả năng tạo ra khủng hoảng niềm tin sâu sắc. Khi công chúng không thể phân biệt thật - giả, họ dễ rơi vào trạng thái hoài nghi toàn diện, dẫn đến suy giảm niềm tin vào truyền thông chính thống và cơ quan công quyền. Bên cạnh đó, những vụ việc giả mạo có thể gây tổn hại nghiêm trọng tới uy tín của cá nhân, tổ chức, thậm chí kích động bất ổn xã hội. Ở cấp độ quốc gia, việc lan truyền video hoặc thông điệp giả mạo trong bối cảnh nhạy cảm có thể tác động tiêu cực đến an ninh chính trị và quan hệ quốc tế. Nguy hiểm hơn, do đặc tính khó kiểm soát và khó thu hồi, một khi nội dung deepfake được phát tán, hậu quả của nó có thể kéo dài, gây ra thiệt hại khó khắc phục cả về kinh tế lẫn xã hội.

*Nhận diện đúng rủi ro từ ứng dụng AI và deepfake có ý nghĩa then chốt để xây dựng không gian mạng an toàn và đáng tin cậy. (1) Đối với cơ quan nhà nước*, đây là cơ sở để kịp thời ban hành khung pháp lý kiểm soát nội dung do AI tạo ra, ví dụ yêu cầu gắn nhãn hoặc cảnh báo với sản phẩm deepfake, đồng thời xây dựng cơ chế xử phạt nghiêm minh đối với hành vi lợi dụng AI để phạm tội. Việc nhận thức rõ nguy cơ giúp họ chủ động đầu

<sup>47</sup> World Economic Forum (2025), *Deepfake AI “cybercrime” targets multinational firm Arup in \$25 million fraud*, <https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/>, Truy cập ngày 05/08/2025.





tư vào công cụ phát hiện nội dung giả mạo, phối hợp với cơ quan chức năng trong giám sát và xử lý thông tin xấu độc. **(2) Với doanh nghiệp công nghệ**, ý thức được rủi ro này sẽ thúc đẩy họ phát triển công nghệ AI có trách nhiệm, bảo đảm tính minh bạch, công bằng và an toàn. **(3) Đối với người dân**, hiểu biết về nguy cơ từ deepfake và AI sẽ giúp nâng cao cảnh giác, biết cách kiểm chứng nguồn tin, từ đó hạn chế bị lừa đảo hoặc thao túng.

### **7.2.1.5. Nguy cơ lợi dụng sản phẩm, dịch vụ về dữ liệu để thực hiện hành vi vi phạm pháp luật**

Nguy cơ này xuất phát từ tính chất hai mặt của dữ liệu và công nghệ số. Một mặt, dữ liệu và các dịch vụ số là công cụ hỗ trợ quản lý nhà nước, phát triển kinh tế - xã hội. Mặt khác, chúng cũng bị lợi dụng để thực hiện những hành vi vi phạm pháp luật. Sự phát triển nhanh của các nền tảng trực tuyến, thương mại điện tử, ví điện tử, dịch vụ tài chính số và mạng xã hội tạo điều kiện cho tội phạm ẩn danh, che giấu hành vi, đồng thời hoạt động vượt ra ngoài phạm vi lãnh thổ. Hơn nữa, việc chưa có cơ chế kiểm soát đầy đủ đối với dòng chảy dữ liệu, thanh toán điện tử và giao dịch trực tuyến đã tạo lỗ hổng cho các đối tượng phạm tội khai thác.

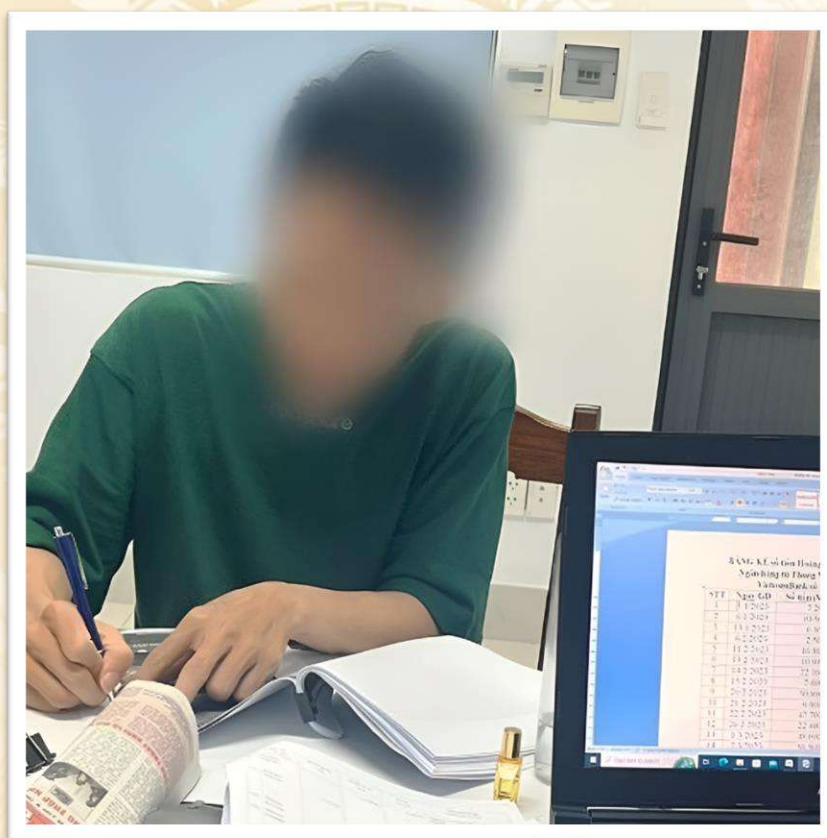
Nguy cơ lợi dụng sản phẩm, dịch vụ từ dữ liệu để vi phạm pháp luật lan tỏa đồng thời trên nhiều bình diện đan xen. **Ở bình diện kinh tế - tài chính**, việc khai thác trái phép dữ liệu định danh, sinh trắc học, giao dịch và hành vi tiêu dùng tạo điều kiện cho hoạt động lừa đảo trực tuyến, tín dụng đen, rửa tiền qua ví điện tử, nền tảng fintech và tiền ảo với mức độ ẩn danh cao, khiến truy vết khó khăn và gây khủng hoảng dây chuyền hoặc một dạng sự cố domino. **Ở bình diện trật tự xã hội**, các nền tảng mạng xã hội và ứng dụng nhắn tin trực tuyến bị biến thành nơi tổ chức cờ bạc, cá độ, mua bán hàng cấm, tuyển dụng trá hình cho đường dây tội phạm, kéo theo gia tăng





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

các tệ nạn, gây hoang mang trong cộng đồng và bào mòn niềm tin xã hội. ***Trên bình diện an ninh quốc gia***, không gian dữ liệu có thể bị các đối tượng trong và ngoài nước lợi dụng để phát tán tài liệu chống phá, kêu gọi tụ tập, biểu tình trái pháp luật hoặc gây chiến tranh tâm lý - chiến tranh thông tin, đe dọa ổn định chính trị và là tiền đề cho một cuộc cách mạng màu tại Việt Nam. Đồng thời, ***trên bình diện pháp lý***, sự lạm dụng dữ liệu xâm phạm quyền riêng tư tạo “vùng xám” trách nhiệm pháp lý giữa các chủ thể nền tảng, bên trung gian và người dùng, khi hành vi phạm pháp diễn ra xuyên biên giới, vượt ngoài thẩm quyền một hệ thống pháp luật đơn lẻ.



***Nhân viên ngân hàng bán thông tin tài khoản chỉ 200.000 đến  
1,9 triệu/trường hợp - Ảnh: Báo Tuổi trẻ***

Về hình thức, thông qua ứng dụng các sản phẩm, dịch vụ về dữ liệu, các đối tượng có thể tiến hành một số hành vi phạm tội như: ***(1) Lừa đảo bằng***





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

**công nghệ Deepfake/Deepvoice** - sử dụng phần mềm giả lập khuôn mặt, giả lập giọng nói, để gọi điện video mạo danh người thân, bạn bè hoặc cấp trên, sau đó yêu cầu chuyển tiền gấp để xử lý công việc hoặc giải quyết tình huống khẩn cấp; **(2) Giả mạo tin nhắn thương hiệu** - Tội phạm gửi tin nhắn giả danh các ngân hàng hoặc tổ chức tài chính uy tín (như TPBank, Sacombank, ZaloPay...), thông báo về việc tài khoản bị khóa, trúng thưởng hoặc cần nâng cấp dịch vụ, kèm theo là đường link giả mạo để lừa người dùng nhập thông tin cá nhân và mã OTP, từ đó chiếm đoạt tiền; **(3) Giả danh “người nước ngoài” để lừa đảo** - Kẻ lừa đảo kết bạn qua mạng xã hội, giả vờ là người nước ngoài giàu có, sau đó thông báo sẽ gửi một món quà giá trị về Việt Nam. Một đối tượng khác sẽ giả danh nhân viên hải quan, sân bay... liên hệ yêu cầu nạn nhân chuyển các khoản phí để nhận quà, rồi chiếm đoạt tiền; **(4) Giả danh là cán bộ, công chức, viên chức nhà nước** - các đối tượng gọi điện thoại mạo danh công an, viện kiểm sát, tòa án, thông báo về các vụ án, yêu cầu nạn nhân phải kê khai tài sản hoặc chuyển tiền vào "tài khoản tạm giữ" để phục vụ điều tra, sau đó chiếm đoạt; **(5) Lừa đảo tuyển mộ nhân viên làm việc online** - Kẻ lừa đảo đăng tin tuyển dụng cộng tác viên bán hàng, làm nhiệm vụ online cho các sàn thương mại điện tử (Shopee, Lazada). Nạn nhân sẽ được yêu cầu chuyển tiền ứng trước cho các đơn hàng “ảo”, và sẽ mất tiền ngay khi thực hiện nhiệm vụ; **(6) Tấn công mạng và đánh cắp dữ liệu** - Tin tặc tấn công vào các hệ thống máy tính của doanh nghiệp và tổ chức, cài mã độc tống tiền (ransomware) để mã hóa dữ liệu, sau đó yêu cầu nạn nhân phải trả tiền chuộc. Ngoài ra, còn có các hình thức tấn công để trộm cắp thông tin cá nhân, chiếm đoạt tài khoản mạng xã hội.

Việc lợi dụng sản phẩm, dịch vụ từ dữ liệu để vi phạm pháp luật có thể gây ra hậu quả lớn trực tiếp và lâu dài. Một mặt, nó gây thiệt hại lớn về tài





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

chính cho người dân và doanh nghiệp thông qua các vụ lừa đảo, chiếm đoạt tài sản. Mặt khác, nó làm gia tăng tỷ lệ tội phạm và các tệ nạn xã hội, như cờ bạc, cá độ, mua bán người, tín dụng đen, ảnh hưởng trực tiếp đến đời sống cộng đồng. Nguy hiểm hơn, nguy cơ này còn đe dọa sự ổn định chính trị - xã hội, khi không gian mạng bị biến thành môi trường cho các hoạt động chống phá Nhà nước như tuyên truyền phá hoại tư tưởng, khủng bố trên không gian mạng... Đặc tính ẩn danh và xuyên biên giới khiến việc điều tra, xử lý trở nên khó khăn, tạo ra thách thức lớn cho các cơ quan bảo vệ pháp luật.



***Đặc tính ẩn danh bị kẻ xấu thường xuyên lợi dụng để xâm phạm  
an ninh dữ liệu - Ảnh: Báo Quân đội nhân dân***

Nhận thức rõ nguy cơ lợi dụng dữ liệu để thực hiện hành vi phạm pháp có ý nghĩa quan trọng đối với mọi chủ thể trong xã hội. **(1) Với cơ quan nhà nước**, đây là căn cứ để hoàn thiện hệ thống pháp luật, tăng cường phối hợp giữa cơ quan chuyên trách lĩnh vực an ninh mạng, cơ quan tư pháp và tài





chính, công nghệ trong quản lý dữ liệu và dịch vụ số. Việc hiểu rõ nguy cơ giúp tăng cường cơ chế kiểm soát nội bộ, triển khai xây dựng các công cụ phát hiện giao dịch bất thường, giám sát chặt chẽ hoạt động trực tuyến. **(2) Với doanh nghiệp công nghệ**, nhận thức này thúc đẩy việc xây dựng nền tảng an toàn, có trách nhiệm xã hội, đồng thời tuân thủ các quy định pháp luật về bảo vệ dữ liệu và phòng chống tội phạm sử dụng công nghệ cao. **(3) Với người dân**, hiểu biết đầy đủ về nguy cơ giúp nâng cao cảnh giác, không cung cấp dữ liệu bừa bãi, đồng thời biết cách hợp tác với cơ quan chức năng khi phát hiện hành vi nghi vấn.

### **7.2.2. Một số giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu**

Trong định hướng chuyển đổi số quốc gia, lãnh đạo Đảng, Nhà nước ta nhiều lần nhấn mạnh yêu cầu đặt an ninh, an toàn dữ liệu ở vị trí then chốt. Tổng Bí thư Tô Lâm khẳng định dữ liệu là **“tài nguyên, tư liệu sản xuất quan trọng”**, là **“máu”** của nền kinh tế số, qua đó đòi hỏi hoàn thiện hành lang pháp lý và cơ chế quản trị dữ liệu hiện đại, theo kịp với xu thế toàn cầu. Cụ thể hóa chủ trương của Bộ Chính trị, Thủ tướng Phạm Minh Chính đã chỉ đạo xây dựng và vận hành Trung tâm Dữ liệu quốc gia như **“trái tim của chuyển đổi số quốc gia”**, yêu cầu bảo đảm an toàn, an ninh hệ thống thông tin của bộ, ngành, địa phương gắn với kết nối - chia sẻ dữ liệu thông suốt. Đồng thời, Thủ tướng nhấn mạnh an ninh mạng **“cần cách tiếp cận toàn cầu và toàn dân”**, huy động vai trò người đứng đầu trong tổ chức triển khai. Trên cơ sở các chỉ đạo này, cần có những giải pháp đồng bộ về thể chế, kỹ thuật, nhân lực và phối hợp liên thông nhằm bảo đảm an ninh dữ liệu, an toàn dữ liệu trong mọi ứng dụng sản phẩm, dịch vụ dữ liệu của quốc gia. Cụ thể như sau:





## **7.2.2.1. Hoàn thiện khung pháp lý và quy chuẩn cho an ninh, an toàn dữ liệu**

Trước tiên, nền tảng pháp lý rõ ràng, đồng bộ và đủ mạnh là điều kiện tiên quyết để bảo đảm an ninh, an toàn dữ liệu. Mặc dù Việt Nam đã có Luật An ninh mạng, Luật An toàn thông tin mạng (đang được đề xuất hợp nhất với Luật An ninh mạng), Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu..., hệ thống pháp luật vẫn cần tiếp tục hoàn thiện để tránh chồng chéo và đáp ứng những thách thức mới, trong đó cần tập trung vào một số nội dung sau:

+ **Cụ thể hóa các khái niệm và phạm vi áp dụng.** Ban hành văn bản hướng dẫn dưới luật để định nghĩa rõ “an ninh dữ liệu” và “an toàn dữ liệu”, từ đó xác định trách nhiệm tương ứng cho từng loại dữ liệu, mức độ nhạy cảm, quan trọng khác nhau. Điều này giúp các cơ quan, doanh nghiệp hiểu rõ nghĩa vụ pháp lý phải tuân thủ cho mỗi loại dữ liệu.

+ **Ban hành tiêu chuẩn quốc gia về an toàn dữ liệu.** Xây dựng bộ tiêu chuẩn, quy chuẩn kỹ thuật cho từng loại sản phẩm, dịch vụ dữ liệu (như dịch vụ trung gian dữ liệu, dịch vụ phân tích dữ liệu, sàn giao dịch dữ liệu...). Bộ tiêu chuẩn này tương đương với các lĩnh vực thiết yếu như tài chính, y tế để áp dụng thống nhất trên toàn quốc. Ví dụ, quy định tối thiểu về mã hóa, sao lưu, quản lý truy cập cho dịch vụ dữ liệu tài chính phải nghiêm ngặt tương tự tiêu chuẩn an ninh thông tin trong ngành ngân hàng.

+ **Sửa đổi, đồng bộ các văn bản pháp luật liên quan.** Rà soát các luật và nghị định hiện hành như Luật An ninh mạng 2018, Luật Giao dịch điện tử 2005 (sửa đổi 2023), Luật Bảo vệ quyền lợi người tiêu dùng 2023... để bảo đảm tính thống nhất, tránh chồng chéo với Luật Dữ liệu mới. Chẳng hạn, Luật An ninh mạng yêu cầu “lưu trữ dữ liệu người dùng trong nước” đối với một số doanh nghiệp nước ngoài, quy định này cần hài hòa với nguyên tắc của





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Luật Dữ liệu về chuyển dữ liệu qua biên giới. Việc đồng bộ pháp luật giúp các bên liên quan **“làm đúng, làm đủ”** và cơ quan quản lý cũng dễ giám sát, xử lý vi phạm.



### ***Khung pháp lý vững chắc tạo đà “bức phá” trong lĩnh vực dữ liệu - Ảnh: Internet***

Một hành lang pháp lý minh bạch và đầy đủ sẽ tạo **điểm tựa vững chắc** cho các giải pháp khác triển khai hiệu quả. Doanh nghiệp có quy tắc rõ ràng để tuân thủ, còn Nhà nước có cơ sở pháp lý để xử lý nghiêm các vi phạm về dữ liệu. Kinh nghiệm quốc tế cho thấy khung pháp luật mạnh sẽ nâng cao niềm tin của người dân và nhà đầu tư vào công tác bảo vệ dữ liệu, đồng thời giúp Việt Nam dễ dàng hợp tác, trao đổi dữ liệu với các nước trong kỷ nguyên số.

#### ***7.2.2.2. Tăng cường các biện pháp kỹ thuật - bảo mật dữ liệu***

Nhiều sự cố rò rỉ dữ liệu xảy ra xuất phát từ lỗ hổng kỹ thuật hoặc thiếu sót bảo mật trong quá trình phát triển sản phẩm, dịch vụ về dữ liệu. Thực tế cho thấy không ít doanh nghiệp chỉ vá lỗi sau khi bị tấn công thay vì phòng



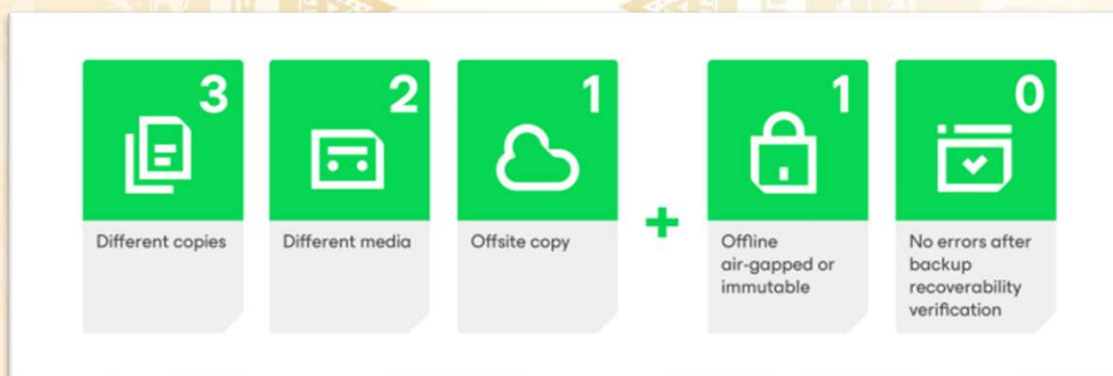


## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

ngừa từ đầu. Do đó, cần áp dụng nguyên tắc **“Secure by Design”**, tích hợp các biện pháp bảo mật ngay từ khâu thiết kế và triển khai dịch vụ. Một số giải pháp kỹ thuật thiết yếu, để triển khai bao gồm:

+ **Xác thực mạnh cho tài khoản:** Áp dụng mật khẩu mạnh (độ dài và độ phức tạp cao) kết hợp xác thực hai lớp (2FA) cho mọi tài khoản quản trị hệ thống và người dùng cuối. Việc này giúp ngăn chặn đăng nhập trái phép ngay cả khi lộ mật khẩu.

+ **Sao lưu dữ liệu định kỳ:** Thiết lập cơ chế sao lưu dữ liệu thường xuyên và lưu trữ bản sao dữ liệu tại một hệ thống độc lập, an toàn. Nguyên tắc 3 - 2 - 1 thường được khuyến nghị: ít nhất 3 bản sao dữ liệu, lưu trên 2 loại phương tiện khác nhau, và 1 bản sao ngoài máy chủ<sup>48</sup>. Điều này đảm bảo dữ liệu có thể phục hồi nhanh khi xảy ra sự cố phần cứng hoặc bị tấn công bởi mã độc tống tiền (ransomware).



**Minh họa nguyên tắc sao lưu 3 - 2 - 1 - Ảnh: Veeam.**

- **Tổ chức thực hiện các biện pháp phòng ngừa và xử lý rủi ro dữ liệu**

**Thứ nhất**, thiết lập hệ thống bảo đảm an toàn giao dịch dữ liệu theo quy định của pháp luật, hướng dẫn các bên tham gia trên sàn thực hiện bảo vệ dữ

<sup>48</sup> Veeam (2025), 3-2-1 Backup Rule Explained: Do I Need One?, <https://www.veeam.com/blog/321-backup-rule.html>, truy cập ngày 06/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

liệu, truy xuất nguồn gốc, xác định rủi ro, kiểm tra tuân thủ và sử dụng các biện pháp hiệu quả để bảo vệ dữ liệu cá nhân, quyền riêng tư cá nhân, bí mật thương mại, và dữ liệu quan trọng theo quy định của Nhà nước (khoản 4 Điều 35 Nghị định số 169/2025/NĐ-CP). Trước hết, các chủ thể tham gia phải thiết lập hệ thống bảo đảm an toàn giao dịch dữ liệu theo đúng chuẩn mực pháp luật, coi đây như “lá chắn” đầu tiên bảo vệ các bên tham gia. Hệ thống này cần có khả năng xác thực giao dịch, lưu vết nhật ký, mã hóa dữ liệu trong quá trình truyền tải, đồng thời phát hiện sớm và ngăn chặn hành vi gian lận.

Song song, tổ chức vận hành sàn dữ liệu phải có trách nhiệm hướng dẫn các bên tham gia thực hiện đúng quy định về bảo vệ dữ liệu, bao gồm bảo đảm quyền riêng tư cá nhân, bí mật thương mại và bảo mật dữ liệu quan trọng do Nhà nước xác định. Việc này gắn liền với yêu cầu truy xuất nguồn gốc của sản phẩm dữ liệu: mỗi tập dữ liệu giao dịch trên sàn cần có thông tin rõ ràng về nguồn gốc, chủ thể sở hữu và phạm vi khai thác hợp pháp. Ngoài ra, cần tiến hành đánh giá và xác định rủi ro tiềm ẩn trong từng giao dịch, chẳng hạn nguy cơ lộ lọt dữ liệu cá nhân, lạm dụng dữ liệu kinh doanh hoặc tấn công vào hệ thống lưu trữ. Trên cơ sở đó, tổ chức sàn phải triển khai cơ chế kiểm tra tuân thủ định kỳ, áp dụng các biện pháp kỹ thuật và quản trị như kiểm thử an ninh, giám sát truy cập, phân quyền chặt chẽ.

**Thứ hai,** thực hiện các biện pháp bảo vệ, bảo mật hợp lý để bảo vệ dữ liệu cá nhân trong truyền sở hữu của tổ chức, bao gồm ngăn chặn truy cập, thu thập, sử dụng, tiết lộ trái phép hoặc các rủi ro tương tự. Trước hết, các tổ chức cần xây dựng cơ chế kiểm soát truy cập chặt chẽ, bảo đảm chỉ những cá nhân có thẩm quyền mới được phép tiếp cận dữ liệu. Cùng với đó, hệ thống phải triển khai giải pháp kỹ thuật phòng ngừa như mã hóa dữ liệu khi





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

lưu trữ và truyền tải, sử dụng tường lửa và phần mềm giám sát an ninh mạng để phát hiện sớm hành vi bất thường. Bên cạnh khía cạnh kỹ thuật, cần thực hiện các biện pháp quản trị và tuân thủ pháp luật, bao gồm việc rà soát quy trình thu thập, xử lý, chia sẻ dữ liệu để ngăn chặn tình trạng truy cập, sử dụng, tiết lộ dữ liệu trái phép. Mọi hoạt động xử lý phải gắn với sự đồng ý của chủ thể dữ liệu và phù hợp với Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, cũng như Luật Dữ liệu 2024. Ngoài ra, tổ chức phải có kế hoạch ứng phó sự cố nhằm kịp thời ngăn chặn và khắc phục khi xảy ra rủi ro như tấn công mạng hoặc rò rỉ dữ liệu.

**Thứ ba**, xây dựng hệ thống sao lưu dữ liệu tự động và thường xuyên; kiểm tra khả năng khôi phục dữ liệu. Đây là giải pháp quan trọng nhằm đảm bảo tính liên tục và ổn định cho mọi hoạt động quản lý dữ liệu trong tổ chức. Về mặt kỹ thuật, hệ thống cần được thiết kế để sao lưu theo lịch trình định kỳ (hàng ngày, hàng tuần hoặc theo thời gian thực đối với dữ liệu nhạy cảm), lưu trữ bản sao tại nhiều địa điểm khác nhau, trong đó có cả máy chủ nội bộ và dịch vụ lưu trữ đám mây bảo mật. Việc này giúp hạn chế tối đa rủi ro mất dữ liệu do sự cố phần cứng, lỗi hệ thống, tấn công mạng hoặc thiên tai. Bên cạnh việc sao lưu, tổ chức cần thường xuyên kiểm tra khả năng khôi phục dữ liệu thông qua các bài kiểm thử thực tế. Việc khôi phục thử không chỉ chứng minh tính khả dụng của bản sao lưu mà còn giúp phát hiện sớm các lỗi kỹ thuật trong quá trình lưu trữ, từ đó kịp thời điều chỉnh. Đặc biệt, dữ liệu được sao lưu phải được mã hóa và kiểm soát truy cập nghiêm ngặt, tránh nguy cơ bị lộ lọt trong quá trình lưu trữ hoặc vận hành.

**Thứ tư**, cập nhật phần mềm, hệ điều hành và vá các loại lỗ hổng bảo mật kịp thời. Cập nhật phần mềm, hệ điều hành và vá các loại lỗ hổng bảo mật kịp thời là một trong những biện pháp cơ bản nhưng mang tính sống còn





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

trong việc bảo đảm an toàn dữ liệu và hệ thống thông tin. Các phần mềm và hệ điều hành, sau một thời gian vận hành, thường bộc lộ lỗ hổng bảo mật mà tin tặc có thể lợi dụng để tấn công, xâm nhập và chiếm quyền kiểm soát. Nếu không kịp thời vá lỗi, tổ chức sẽ phải đối mặt với nguy cơ rò rỉ dữ liệu, gián đoạn dịch vụ và thiệt hại tài chính.

Vì vậy, việc cập nhật định kỳ và theo dõi sát sao các bản vá bảo mật do nhà sản xuất phát hành cần được đưa vào quy trình quản trị an ninh thông tin chuẩn hóa. Các bản vá này phải được kiểm thử trên môi trường giả lập (sandbox) trước khi áp dụng rộng rãi, nhằm tránh xung đột phần mềm hoặc ảnh hưởng đến vận hành hệ thống. Song song, tổ chức cũng cần thiết lập cơ chế cảnh báo và quản lý bản vá tự động, đảm bảo mọi máy trạm, máy chủ và thiết bị đầu cuối đều được cập nhật đồng bộ, tránh tình trạng bỏ sót.



***Cần ban hành cụ thể phương án xử lý đối với từng trường hợp  
cơ sở dữ liệu bị xâm phạm - Ảnh: Internet***





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Ngoài khía cạnh kỹ thuật, việc cập nhật phần mềm còn gắn với yêu cầu pháp lý: Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (sắp tới là Luật Bảo vệ dữ liệu cá nhân năm 2025) và Nghị định 169/2025/NĐ-CP đều nhấn mạnh trách nhiệm của tổ chức trong việc bảo đảm an toàn hệ thống thông tin. Như vậy, cập nhật và vá lỗ hổng không chỉ giúp giảm thiểu nguy cơ bị tấn công, mà còn thể hiện sự tuân thủ pháp luật, góp phần xây dựng môi trường số an toàn, tin cậy, bảo vệ dữ liệu công dân cũng như duy trì uy tín của tổ chức.

**Thứ năm**, đào tạo nhân sự về an toàn dữ liệu và các tình huống rủi ro phổ biến (phishing, ransomware...). Đào tạo nhân sự về an toàn dữ liệu và các tình huống rủi ro phổ biến là một trong những giải pháp trọng yếu, vì yếu tố con người thường được coi là “*mắt xích yếu*” trong chuỗi an ninh mạng. *Trước hết*, các tổ chức cần xây dựng chương trình đào tạo bài bản và định kỳ cho toàn bộ nhân viên, từ lãnh đạo đến cán bộ kỹ thuật, tập trung vào nhận diện các mối đe dọa thường gặp như tấn công giả mạo (phishing), lừa đảo qua email, mã độc tống tiền (ransomware), rò rỉ dữ liệu do sử dụng thiết bị cá nhân hoặc chia sẻ tài liệu không đúng quy trình. Nội dung đào tạo nên bao gồm cả phần lý thuyết (quy định pháp luật, chính sách nội bộ, quy trình ứng cứu sự cố) và phần thực hành (mô phỏng email lừa đảo, bài tập xử lý tình huống, hướng dẫn cách sử dụng công cụ bảo mật).

*Thêm vào đó*, tổ chức cần triển khai các chiến dịch nâng cao nhận thức liên tục, chẳng hạn gửi bản tin cảnh báo về thủ đoạn mới, dán poster nhắc nhở tại nơi làm việc, tổ chức “*tháng an toàn thông tin*” hoặc các cuộc thi nhỏ về nhận diện rủi ro mạng. Việc này không chỉ giúp nhân viên có khả năng tự bảo vệ mình, mà còn hình thành văn hóa an toàn dữ liệu trong toàn tổ chức. *Về mặt quản lý*, các cơ quan, doanh nghiệp phải gắn đào tạo với





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

trách nhiệm cá nhân, quy định rõ hình thức xử lý khi vi phạm quy trình an toàn dữ liệu, đồng thời khuyến khích khen thưởng những cá nhân phát hiện sớm rủi ro hoặc đề xuất giải pháp hiệu quả.

**Thứ sáu,** áp dụng các biện pháp xác thực đa yếu tố (MFA) để tăng cường độ tin cậy. Áp dụng các biện pháp xác thực đa yếu tố (MFA - Multi-Factor Authentication) là một trong những giải pháp quan trọng nhằm nâng cao mức độ an toàn trong quản trị dữ liệu và hệ thống thông tin. MFA yêu cầu người dùng phải vượt qua ít nhất hai lớp xác thực khác nhau, thay vì chỉ sử dụng mật khẩu truyền thống, từ đó giảm thiểu nguy cơ bị chiếm đoạt tài khoản khi thông tin đăng nhập bị lộ.

Cụ thể, ngoài mật khẩu, người dùng có thể phải cung cấp thêm mã OTP qua tin nhắn hoặc ứng dụng xác thực, sử dụng vân tay, nhận diện khuôn mặt, thẻ thông minh hoặc thiết bị bảo mật chuyên dụng (token). Cách tiếp cận này giúp hạn chế đáng kể các rủi ro từ tấn công giả mạo (phishing), đánh cắp mật khẩu hay tấn công brute force. Việc triển khai MFA cần được thực hiện trước hết đối với hệ thống dữ liệu nhạy cảm và tài khoản quản trị cấp cao, sau đó mở rộng ra toàn bộ dịch vụ công trực tuyến, tài khoản nội bộ của cán bộ, nhân viên và cả đối tác tham gia hệ thống. Đồng thời, để đảm bảo hiệu quả, cần kết hợp MFA với chính sách quản lý danh tính và truy cập (IAM), phân quyền chặt chẽ và theo dõi nhật ký truy cập nhằm phát hiện sớm hành vi bất thường.

**Thứ bảy,** thiết lập quy trình phản ứng sự cố (incident response plan) rõ ràng, có người phụ trách cụ thể. Thiết lập quy trình phản ứng sự cố (IRP) rõ ràng, cần có người phụ trách cụ thể là yêu cầu thiết yếu trong chiến lược bảo vệ dữ liệu và an ninh mạng của tổ chức. Quy trình này cần được xây dựng theo các bước chặt chẽ, bảo đảm khi xảy ra sự cố, hệ thống có thể phản ứng nhanh chóng, hạn chế tối đa thiệt hại. Trước hết, tổ chức phải xác định rõ vai





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

trò, trách nhiệm và người chịu trách nhiệm chính trong xử lý sự cố, từ khâu tiếp nhận thông tin, đánh giá rủi ro, cô lập hệ thống bị tấn công cho đến khắc phục và khôi phục dịch vụ. Một đội phản ứng sự cố (Incident Response Team) nên được thành lập, bao gồm chuyên gia an ninh mạng, cán bộ pháp chế và người đại diện lãnh đạo để bảo đảm phối hợp đa chiều. Quy trình này cần được thiết kế theo vòng đời sự cố, bao gồm: phát hiện - phân tích - ứng phó - khắc phục - phục hồi - rút kinh nghiệm. Mỗi giai đoạn phải có hướng dẫn cụ thể, thời gian xử lý tối đa và kênh liên lạc khẩn cấp. Đặc biệt, sau mỗi sự cố, tổ chức cần tiến hành đánh giá lại toàn bộ quy trình, cập nhật bài học kinh nghiệm và bổ sung biện pháp phòng ngừa.

Bên cạnh đó, quy trình phản ứng sự cố phải được kiểm thử định kỳ thông qua các buổi diễn tập mô phỏng, giúp nhân viên quen với quy trình và giảm thiểu lúng túng khi sự cố thực sự xảy ra. Song song, cần thiết lập cơ chế báo cáo kịp thời cho cơ quan quản lý nhà nước có thẩm quyền, phù hợp với khung pháp lý về bảo vệ an ninh dữ liệu tại Việt Nam.

*- Tiến hành các biện pháp giám sát hành vi có thể ảnh hưởng đến công tác bảo vệ an ninh, an toàn dữ liệu.*

**Thứ nhất**, giám sát hoạt động trên sàn dữ liệu, quyết định đình chỉ tham gia các bên, tiếp tục niêm yết và chấm dứt niêm yết các sản phẩm, dịch vụ dữ liệu; giải quyết tranh chấp; giám sát, kịp thời phát hiện, xử lý, ngăn chặn báo cáo các vi phạm pháp luật; phối hợp với cơ quan quản lý nhà nước có liên quan trong việc kiểm tra, điều tra, thu thập chứng cứ (khoản 2 Điều 35 Nghị định số 169/2025/NĐ-CP). Theo khoản 2 Điều 35 Nghị định số 169/2025/NĐ-CP, tổ chức vận hành sàn không chỉ theo dõi các giao dịch thường xuyên mà còn có trách nhiệm giải quyết tranh chấp giữa các bên, kịp thời phát hiện và xử lý vi phạm, đồng thời báo cáo, ngăn chặn hành vi trái





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

pháp luật. Trong quá trình này, sàn dữ liệu có quyền chủ động quyết định việc duy trì hay loại bỏ các sản phẩm, dịch vụ không đáp ứng yêu cầu, qua đó bảo vệ lợi ích chính đáng của các bên tham gia. Bên cạnh đó, cơ chế phối hợp chặt chẽ với cơ quan quản lý nhà nước trong kiểm tra, điều tra và thu thập chứng cứ giúp tăng cường tính pháp lý, bảo đảm rằng mọi hành vi vi phạm đều được xử lý nghiêm minh. Đây không chỉ là biện pháp quản trị kỹ thuật mà còn là công cụ quản lý nhà nước quan trọng, góp phần duy trì kỷ cương pháp luật, ngăn chặn các hoạt động lợi dụng dữ liệu để trục lợi hoặc gây bất ổn xã hội, đồng thời tạo dựng niềm tin cho tổ chức, cá nhân khi tham gia thị trường dữ liệu.



**Ảnh minh họa - Ảnh: Internet**

**Thứ hai,** thông báo vi phạm dữ liệu tới tổ chức, cá nhân bị ảnh hưởng ngay khi có thể nếu có vi phạm dữ liệu có khả năng gây tác hại đáng kể cho cá nhân hoặc có quy mô đáng kể. Khi xảy ra sự cố vi phạm dữ liệu có khả năng gây tác hại đáng kể cho cá nhân hoặc ảnh hưởng diện rộng, tổ chức quản lý dữ liệu phải nhanh chóng thông tin cho các bên liên quan để họ kịp





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

thời áp dụng biện pháp phòng ngừa, như thay đổi mật khẩu, khóa tài khoản, giám sát giao dịch hoặc báo cho cơ quan chức năng. Nghĩa vụ thông báo này không chỉ thể hiện trách nhiệm minh bạch và tuân thủ pháp luật của tổ chức, mà còn góp phần giảm thiểu hậu quả dây chuyền từ rò rỉ dữ liệu, như nguy cơ lừa đảo, tống tiền, xâm phạm quyền riêng tư hay mất uy tín.

Thực tiễn quốc tế cũng cho thấy yêu cầu này đã trở thành chuẩn mực: Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR) bắt buộc các tổ chức phải thông báo sự cố vi phạm dữ liệu cá nhân cho cơ quan giám sát trong vòng 72 giờ và thông báo cho cá nhân nếu rủi ro cao đối với quyền và tự do của họ. Việt Nam, qua Luật Dữ liệu 2024 và Nghị định 169/2025/NĐ-CP, cũng đã tiếp cận theo hướng tương tự, yêu cầu cơ quan, tổ chức quản lý dữ liệu phải nhanh chóng báo cáo và thông tin cho các chủ thể bị ảnh hưởng. Nhờ đó, người dân và tổ chức có thể chủ động bảo vệ mình, còn cơ quan quản lý có cơ sở để xử lý sự cố, ngăn chặn hành vi vi phạm tiếp tục diễn ra.

**Thứ ba**, triển khai công nghệ theo dõi, phân tích thành viên người dùng (UEBA - User and Entity Behavior Analytics). Triển khai công nghệ UEBA là một giải pháp tiên tiến giúp các tổ chức nâng cao năng lực giám sát và bảo vệ an ninh, an toàn dữ liệu trong bối cảnh các mối đe dọa mạng ngày càng tinh vi. UEBA hoạt động bằng cách phân tích hành vi của người dùng và các thực thể trong hệ thống (như tài khoản, thiết bị, ứng dụng), từ đó xây dựng “hồ sơ hành vi chuẩn” cho từng đối tượng.

Khi phát hiện những hành vi bất thường so với chuẩn mực, ví dụ đăng nhập vào giờ không thông thường, truy cập khối lượng dữ liệu lớn bất thường, hay kết nối từ vị trí địa lý lạ, hệ thống sẽ tự động cảnh báo cho đội ngũ an ninh mạng. Khác với các công cụ giám sát truyền thống vốn chủ yếu





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

dựa trên các quy tắc tĩnh, UEBA tận dụng trí tuệ nhân tạo và máy học để liên tục học hỏi và phát hiện hành vi bất thường tiềm ẩn, kể cả khi chưa có “*dấu hiệu tấn công*” rõ ràng.

Việc triển khai UEBA mang lại nhiều lợi ích: nó giúp phát hiện sớm nguy cơ rò rỉ dữ liệu từ nội bộ, ngăn chặn kịp thời các hành vi xâm nhập trá hình (insider threats), đồng thời hỗ trợ điều tra sau sự cố nhờ khả năng ghi lại và phân tích chi tiết toàn bộ hành vi người dùng. Với Việt Nam, áp dụng công nghệ này là phù hợp trong bối cảnh các hệ thống dữ liệu quốc gia, đặc biệt là dữ liệu dân cư, tài chính, y tế, ngày càng trở thành mục tiêu tấn công.

**Thứ tư**, thiết lập cảnh báo tự động khi có hoạt động bất thường như tại dữ liệu hàng loạt, truy cập ngoài giờ... Thiết lập cảnh báo tự động khi có hoạt động bất thường là một biện pháp kỹ thuật quan trọng nhằm phát hiện sớm rủi ro an ninh dữ liệu và ngăn chặn sự cố trước khi gây hậu quả nghiêm trọng. Các hệ thống giám sát cần được cấu hình để nhận diện những dấu hiệu bất thường như việc truy xuất dữ liệu hàng loạt ngoài phạm vi công việc, đăng nhập từ nhiều địa chỉ IP cùng lúc, hoặc truy cập hệ thống vào khung giờ không bình thường. Khi các hành vi này xuất hiện, hệ thống sẽ lập tức phát tín hiệu cảnh báo tới bộ phận an ninh mạng để xử lý kịp thời.

Việc thiết lập cảnh báo tự động có ý nghĩa đặc biệt trong bối cảnh dữ liệu ngày càng trở thành mục tiêu của cả tội phạm mạng lẫn nguy cơ rò rỉ từ bên trong. Đây không chỉ là công cụ phát hiện kỹ thuật, mà còn giúp nâng cao khả năng phản ứng nhanh của tổ chức, giảm thiểu thiệt hại tiềm ẩn và tăng cường tính chủ động trong quản lý rủi ro. Hơn nữa, cơ chế này cũng thể hiện sự tuân thủ các quy định pháp luật về bảo mật dữ liệu trong quy định pháp luật, góp phần khẳng định trách nhiệm của tổ chức trong việc bảo vệ quyền lợi hợp pháp của công dân, doanh nghiệp và cơ quan nhà nước.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

**Thứ năm**, giám sát truy cập dữ liệu nhạy cảm, ghi nhật ký (log) và lưu trữ để truy cập khi cần thiết. Việc này yêu cầu mọi hành động truy cập vào dữ liệu quan trọng (như dữ liệu cá nhân, tài chính, y tế hay an ninh quốc gia) đều phải được hệ thống ghi nhận chi tiết, bao gồm thời gian, địa chỉ IP, người dùng, thao tác thực hiện và khối lượng dữ liệu truy xuất. Các bản ghi nhật ký này cần được lưu trữ an toàn trong khoảng thời gian đủ dài theo quy định của pháp luật, đồng thời bảo đảm tính toàn vẹn để có thể sử dụng làm chứng cứ khi cần thiết. Bên cạnh chức năng giám sát, nhật ký còn là công cụ hữu hiệu để phát hiện hành vi bất thường, hỗ trợ công tác điều tra khi xảy ra sự cố an ninh, và chứng minh mức độ tuân thủ của tổ chức với các chuẩn mực pháp lý và kỹ thuật.

Trên thực tế, nhiều vụ rò rỉ dữ liệu lớn trên thế giới đã chỉ ra rằng thiếu cơ chế log và giám sát đã khiến tổ chức mất nhiều tuần, thậm chí nhiều tháng, mới phát hiện sự cố. Đối với Việt Nam, quy định này phù hợp với yêu cầu của Luật An ninh mạng 2018, Luật Dữ liệu 2024 và Nghị định 169/2025/NĐ-CP, trong đó nhấn mạnh nghĩa vụ quản trị dữ liệu an toàn và minh bạch.

|       | Case ID | Activity                    | Time Stamp          | Event Attributes |       |
|-------|---------|-----------------------------|---------------------|------------------|-------|
|       | Case ID | Activity                    | Time Stamp          | User             | Cost  |
| Event | 1       | Incident logging            | 2022/02/20 12:09:00 | edmund.price     | 20.00 |
|       | 1       | Incident classification     | 2022/02/20 12:10:20 | edmund.price     | 20.00 |
|       | 2       | Incident logging            | 2022/02/20 12:33:01 | angela.lewis     | 20.00 |
|       | 1       | Initial diagnosis           | 2022/02/20 12:33:03 | phillip.sanchez  | 20.00 |
|       | 2       | Incident classification     | 2022/02/20 12:34:11 | angela.lewis     | 40.00 |
|       | 2       | Initial diagnosis           | 2022/02/20 12:41:08 | chris.watkins    | 30.00 |
|       | 1       | Functional escalation       | 2022/02/20 15:50:27 | christine.chenal | 10.00 |
|       | 1       | Investigation and diagnosis | 2022/02/20 9:24:43  | christine.chenal | 10.00 |
|       | 1       | Resolution and recovery     | 2022/02/20 10:44:01 | christine.chenal | 10.00 |
|       | 1       | Incident closure            | 2022/02/20 11:57:21 | karen.anderson   | 10.00 |

**Nhật ký (log) ghi nhận mọi hoạt động của từng người dùng cũng như thời lượng truy cập - Ảnh: Appian Documentation**





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

**Thứ sáu**, thực hiện kiểm tra định kỳ tài khoản người dùng, đặc biệt là tài khoản có quyền cao. Đây là một trong những biện pháp then chốt để phòng ngừa nguy cơ rò rỉ dữ liệu và xâm nhập trái phép. Trong quản trị hệ thống, các tài khoản quản trị viên hay người dùng có quyền truy cập sâu thường được tin cậy nhất, bởi khi chiếm được chúng, kẻ tấn công có thể dễ dàng kiểm soát, sửa đổi hoặc đánh cắp dữ liệu quy mô lớn.

Do đó, việc kiểm tra định kỳ bao gồm nhiều nội dung: rà soát số lượng tài khoản đang hoạt động, đối chiếu quyền hạn được cấp với chức năng thực tế của người dùng, phát hiện những tài khoản không còn sử dụng nhưng chưa được vô hiệu hóa, hoặc các trường hợp cấp quyền vượt quá phạm vi công việc. Song song, cần thường xuyên đánh giá các nhật ký truy cập để nhận diện hành vi bất thường, như truy cập vào ngoài giờ hành chính, từ vị trí địa lý lạ, hoặc khối lượng dữ liệu truy xuất quá lớn.

Bên cạnh kiểm tra kỹ thuật, tổ chức cần thiết lập quy trình quản trị vòng đời tài khoản rõ ràng: từ khâu cấp quyền ban đầu, thay đổi quyền khi nhân sự luân chuyển công tác, đến việc thu hồi ngay khi nghỉ việc. Các biện pháp hỗ trợ như xác thực đa yếu tố (MFA) và chính sách mật khẩu mạnh cũng cần được áp dụng bắt buộc cho nhóm tài khoản đặc biệt này.

**Thứ bảy**, xây dựng văn hóa bảo mật trong tổ chức: nêu rõ trách nhiệm cá nhân và khuyến khích phát hiện rủi ro. Xây dựng văn hóa bảo mật trong tổ chức trước hết đòi hỏi làm rõ trách nhiệm cá nhân ở từng vị trí công việc, coi việc bảo vệ dữ liệu là nghĩa vụ nghề nghiệp bắt buộc như quy trình chuyên môn. Trong đó, mỗi cán bộ, nhân viên phải ký cam kết bảo mật, nắm rõ phạm vi dữ liệu được phép xử lý, chịu trách nhiệm về mọi hành vi truy cập dưới tài khoản của mình và bị xử lý khi vi phạm. Cùng với đó, tổ chức cần thiết lập cơ chế khuyến khích phát hiện rủi ro: kênh phản ánh ẩn danh,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

cơ chế “không trừng phạt” đối với báo cáo thiện chí, chính sách khen thưởng cho cá nhân phát hiện lỗi hổng hoặc hành vi bất thường; đồng thời phổ biến bản tin cảnh báo định kỳ, diễn tập tình huống sự cố để củng cố “tính dịch tễ” và khả năng ứng phó sự cố. Văn hóa này phải được dẫn dắt từ người đứng đầu, gắn chỉ tiêu an toàn dữ liệu vào đánh giá thi đua, lồng ghép nội dung bảo mật trong đào tạo hội nhập và bồi dưỡng hằng năm. Qua đó biến bảo mật dữ liệu thành thói quen tổ chức, giảm thiểu rủi ro nội bộ, tăng năng lực tự phòng vệ và củng cố niềm tin của người dân, doanh nghiệp đối với dịch vụ số.

Nhìn chung, nhóm giải pháp này nhằm tạo ra “**vành đai an toàn**” bảo vệ những tài sản dữ liệu chiến lược của quốc gia và doanh nghiệp. Sai sót nhỏ đối với dữ liệu cốt lõi có thể dẫn tới hậu quả khôn lường, vậy nên đầu tư bảo vệ nhiều lớp là hoàn toàn cần thiết. Đây không chỉ là vấn đề kỹ thuật mà còn mang ý nghĩa bảo vệ chủ quyền số và an ninh quốc gia trong thời gian tới.



***Secure Sockets Layer là tiêu chuẩn của công nghệ bảo mật, truyền thông mã hoá giữa máy chủ Web server và trình duyệt - Ảnh: Internet***





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Những biện pháp trên không đòi hỏi công nghệ quá phức tạp và *phù hợp với cả các doanh nghiệp vừa và nhỏ* hoặc cơ quan địa phương nơi nguồn lực về công nghệ còn hạn chế. Việc nâng cao “*sức đề kháng*” kỹ thuật cơ bản sẽ giảm đáng kể rủi ro phổ biến như lộ mật khẩu, lộ dữ liệu khách hàng, bị mã độc tống tiền..., tạo môi trường số an toàn hơn cho cả người dân lẫn tổ chức.

### **7.2.2.3. Thiết lập tổ chức bảo mật chuyên trách và nâng cao năng lực nhân sự**

Yếu tố con người và tổ chức giữ vai trò then chốt trong bảo đảm an toàn dữ liệu. Nhiều vụ lộ lọt xảy ra không chỉ do lỗi kỹ thuật mà còn từ sự bất cẩn hoặc cố ý của nội bộ nhân viên. Vì vậy, cùng với công nghệ, các tổ chức cung cấp sản phẩm, dịch vụ dữ liệu cần xây dựng cơ chế quản trị bảo mật chặt chẽ và chuyên nghiệp hóa đội ngũ nhân sự liên quan:



### **Hội thảo “Tăng cường hệ miễn dịch cho tổ chức, doanh nghiệp trên không gian số” - Ảnh: Báo Nhân dân**

+ **Phân công trách nhiệm rõ ràng:** Mỗi cơ quan, doanh nghiệp nên cử một cán bộ phụ trách về dữ liệu (*Data Protection Officer - DPO* theo mô





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

hình quốc tế). Người này chịu trách nhiệm chính trong việc giám sát tuân thủ quy định bảo vệ dữ liệu, phối hợp xử lý khi có sự cố, và làm đầu mối làm việc với cơ quan chức năng. Ngay cả khi kiêm nhiệm, vị trí này cần có tiếng nói và hiểu biết đủ sâu về pháp luật và công nghệ thông tin.

+ **Nâng cao nhận thức bảo mật cho nhân viên:** Thường xuyên tổ chức các khóa đào tạo kỹ năng an toàn thông tin cho toàn bộ nhân viên, đặc biệt là những người trực tiếp vận hành hệ thống và xử lý dữ liệu. Nội dung đào tạo tập trung vào các thực hành cơ bản: không sử dụng email cá nhân để gửi dữ liệu nhạy cảm, không cài phần mềm lạ, cảnh giác với email lừa đảo, cách xử lý khi phát hiện sự cố... Theo Cục An toàn thông tin, khoảng 80% sự cố lộ lọt dữ liệu cá nhân là do người dùng bất cẩn trong các thao tác hàng ngày, nên nâng cao ý thức, nhận thức cho đội ngũ nhân sự sẽ giảm thiểu đáng kể rủi ro [49].



**Kiểm soát quyền truy cập dữ liệu - Ảnh: Whitehat**

+ **Xây dựng quy trình và chuẩn bị giải pháp ứng phó sự cố:** Xây dựng quy trình báo cáo và xử lý sự cố dữ liệu rõ ràng. Nhân viên cần biết





phải thông báo cho ai, trong thời gian bao lâu khi phát hiện dữ liệu bị mất, bị truy cập trái phép hoặc hệ thống bị tấn công. Song song đó, đội ứng cứu cần có kịch bản hành động để cô lập hệ thống, thu thập bằng chứng, khôi phục dữ liệu từ bản sao lưu và thông báo cho khách hàng hoặc cơ quan quản lý khi cần. Sự chuẩn bị trước sẽ giúp giảm thiểu thiệt hại và thời gian gián đoạn khi xảy ra sự cố.

+ **Chính sách quản lý nhân sự chặt chẽ:** Thực hiện nguyên tắc “*phân tách nhiệm vụ*” và “*kiểm soát quyền truy cập*”, tức là không một cá nhân nào được quyền truy cập tất cả dữ liệu hoặc hệ thống trừ trường hợp thật cần thiết. Kiểm tra tiền sử và sàng lọc nhân sự làm việc ở các vị trí nhạy cảm. Đồng thời, có thể áp dụng quy chế luân chuyển vị trí sau một thời gian để hạn chế nguy cơ nhân viên lợi dụng sự quen thuộc để lấy cắp dữ liệu. Những biện pháp quản lý con người này, cùng với chế tài kỷ luật nghiêm khắc (sa thải, truy cứu hình sự nếu có ý vi phạm), sẽ tạo tính răn đe và ý thức tuân thủ cao hơn trong nội bộ tổ chức.

Tóm lại, xây dựng văn hóa an toàn dữ liệu trong tổ chức cũng quan trọng không kém gì đầu tư công nghệ. Con người là phòng tuyến cuối cùng; một đội ngũ nhân sự có kiến thức, trách nhiệm và quy trình bài bản sẽ giúp bảo vệ dữ liệu hiệu quả “*từ bên trong*”.

#### **7.2.2.4. Bảo vệ quyền lợi của người dùng dữ liệu - đặt con người làm trung tâm trong bảo đảm an ninh, an toàn dữ liệu**

Mọi sản phẩm, dịch vụ dữ liệu suy cho cùng đều phục vụ con người, do đó việc bảo vệ quyền và lợi ích của cá nhân - người mà dữ liệu đề cập đến - phải là trọng tâm. Nếu dữ liệu cá nhân bị thu thập và sử dụng thiếu kiểm soát, hậu quả có thể rất nghiêm trọng: cá nhân bị xâm phạm đời tư, quấy rối, lừa đảo hoặc phân biệt đối xử. Vì vậy, các giải pháp hướng đến minh bạch





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

và tôn trọng quyền riêng tư của người dùng cần được triển khai đồng bộ, phù hợp với các chuẩn mực quốc tế như GDPR hay PIPL:

+ ***Minh bạch trong thu thập dữ liệu cá nhân:*** Ứng dụng, dịch vụ khi muốn thu thập thông tin cá nhân phải thông báo và xin ý kiến đồng ý rõ ràng từ người dùng. Không được mặc định tích sẵn ô “Tôi đồng ý” hoặc “chôn” điều khoản trong nội dung khó hiểu. Người dùng cần được biết dữ liệu nào của họ sẽ được thu thập, nhằm mục đích gì, chia sẻ cho ai. Nguyên tắc minh bạch này cũng là yêu cầu đầu tiên trong 07 nguyên tắc xử lý dữ liệu cá nhân tại Nghị định số 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân.

+ ***Cho phép người dùng kiểm soát dữ liệu của mình:*** Cá nhân có quyền truy cập, xem lại các thông tin mà dịch vụ lưu trữ về mình và được chỉnh sửa nếu sai. Đặc biệt, phải cung cấp cơ chế để người dùng rút lại dữ liệu hoặc yêu cầu xóa bỏ dữ liệu khi không còn sử dụng dịch vụ nữa. Quyền “*được lãng quên*” này đã được quy định trong GDPR của EU và nhiều luật quốc gia khác, giúp cá nhân bảo vệ đời tư của mình.



***Quyền được lãng quên trên không gian mạng - Ảnh: Luật Bạch Tuyết***





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Hạn chế chia sẻ cho bên thứ ba:** Dữ liệu người dùng thu thập được không chia sẻ cho bên thứ ba (đối tác quảng cáo, phân tích) nếu chưa có sự chấp thuận của người dùng. Mọi trường hợp mua bán, trao đổi dữ liệu cá nhân không có căn cứ pháp luật đều bị nghiêm cấm theo Nghị định 13/2023/NĐ-CP. Doanh nghiệp cần tuân thủ chặt chẽ nguyên tắc giới hạn mục đích sử dụng: dữ liệu thu thập được chỉ được dùng cho mục đích đã thông báo, không tự ý mở rộng.

+ **Áp dụng phương pháp “Quyền riêng tư theo thiết kế” (Privacy by Design),** nghĩa là từ khi xây dựng sản phẩm phải tính đến các tính năng bảo vệ riêng tư. Chú ý đặt mặc định chế độ hồ sơ ở mức riêng tư, chỉ thu thập những dữ liệu tối thiểu cần thiết, ẩn giấu thông tin nhạy cảm trên giao diện nếu không cần thiết,... Những thiết kế này giúp người dùng ít bị lộ thông tin hơn nếu họ không có kiến thức chuyên môn về công nghệ, kỹ thuật.

Giải pháp lấy con người làm trung tâm này phản ánh đúng tinh thần của Luật Dữ liệu 2024 cũng như thông lệ quốc tế: *coi trọng quyền của chủ thể dữ liệu*. Luật PIPL của Trung Quốc hay GDPR của EU đều liệt kê đầy đủ các quyền như được đồng ý rõ ràng, quyền truy cập, chỉnh sửa, hạn chế xử lý, khiếu nại... cho cá nhân. Nghị định 13/2023/NĐ-CP của Việt Nam cũng đã bước đầu công nhận các quyền tương tự (quyền được biết, quyền đồng ý, quyền rút “consent”, quyền xóa dữ liệu...). Khi các dịch vụ tuân thủ tốt các nguyên tắc này, người dân sẽ không còn cảm giác bị “giám sát” trước công nghệ, từ đó họ tin tưởng sử dụng sản phẩm, dịch vụ dữ liệu hơn. Niềm tin người dùng chính là nền tảng để kinh tế dữ liệu phát triển bền vững.





## **7.2.2.5. Xác định chính xác và xây dựng phương án bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng**

Không phải mọi dữ liệu đều có mức độ rủi ro như nhau, sẽ có những tập dữ liệu mà nếu bị lộ lọt hoặc can thiệp sẽ gây hậu quả đặc biệt nghiêm trọng cho quốc gia và cộng đồng. Luật Dữ liệu 2024 đã đưa ra khái niệm **“dữ liệu quan trọng”** và **“dữ liệu cốt lõi”** để chỉ các dữ liệu có tầm ảnh hưởng lớn đến lợi ích quốc gia (quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, trật tự xã hội, sức khỏe cộng đồng...). Ngày 30/6/2025, Phó Thủ tướng Nguyễn Chí Dũng đã ký Quyết định số 20/2025/QĐ-TTg của Thủ tướng Chính phủ ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi. Theo đó, Quyết định số 20/2025/QĐ-TTg chỉ ra 26 dữ liệu cốt lõi và 43 dữ liệu quan trọng<sup>49</sup>. Để bảo đảm an ninh quốc gia trên không gian dữ liệu, cần áp dụng các giải pháp sau đối với nhóm dữ liệu đặc biệt này:

+ **Phân loại dữ liệu và áp dụng biện pháp phù hợp theo mức độ nhạy cảm:** Tất cả tổ chức, doanh nghiệp phải thực hiện **“phân loại dữ liệu”** mình quản lý. Các nhóm cơ bản gồm: dữ liệu cốt lõi, dữ liệu quan trọng, dữ liệu dùng chung nội bộ, dữ liệu công khai... Mỗi mức cần có chính sách bảo vệ tương ứng. Ví dụ, dữ liệu cốt lõi (như Dữ liệu về biên giới quốc gia, chủ quyền lãnh thổ do cơ quan nhà nước thu thập, quản lý chưa công khai) phải bảo mật tối đa, trong khi dữ liệu mở có thể công bố rộng rãi. Chủ quản dữ liệu phải xác định rõ danh mục dữ liệu cốt lõi, quan trọng thuộc phạm vi mình quản lý và báo cáo cơ quan có thẩm quyền.

+ **Lưu trữ trong lãnh thổ đối với dữ liệu trọng yếu:** Các dữ liệu thuộc lĩnh vực nhạy cảm cao (quốc phòng, an ninh, tài chính, y tế, thông tin cá

<sup>49</sup> Bạch Dương (2025), *Chính phủ ban hành danh mục 26 dữ liệu cốt lõi và 43 dữ liệu quan trọng*, [vneconomy.vn](https://vneconomy.vn/chinh-phu-ban-hanh-danh-muc-26-du-lieu-cot-loi-va-43-du-lieu-quan-trong.htm), <https://vneconomy.vn/chinh-phu-ban-hanh-danh-muc-26-du-lieu-cot-loi-va-43-du-lieu-quan-trong.htm>, truy cập ngày 06/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

nhân quy mô lớn,...) nên được lưu trữ trên các máy chủ đặt tại Việt Nam. Đây là biện pháp đảm bảo chủ quyền số đang được nhiều nước áp dụng, chẳng hạn Luật An ninh mạng 2017 của Trung Quốc yêu cầu dữ liệu cá nhân và dữ liệu quan trọng của công dân Trung Quốc phải lưu trữ nội địa. Việc lưu trữ trong nước giúp Nhà nước dễ dàng kiểm soát, thanh tra, kiểm tra và tránh nguy cơ bị nước ngoài cản trở truy cập khi cần điều tra sự cố.



***Dữ liệu cốt lõi và dữ liệu quan trọng gây tác động trực tiếp  
đến an ninh quốc gia, độc lập, chủ quyền - Ảnh: VNEconomy.***

+ ***Kiểm soát chặt việc chuyển dữ liệu ra nước ngoài:*** Thiết lập cơ chế đánh giá an ninh dữ liệu xuyên biên giới. Chỉ cho phép chuyển dữ liệu quan trọng, cốt lõi ra ngoài lãnh thổ sau khi đã được cơ quan có thẩm quyền thẩm định và cấp phép. Tiêu chí thẩm định bao gồm: quốc gia nhận dữ liệu có luật bảo vệ dữ liệu tương đương không, mục đích chuyển có chính đáng không, bên nhận có đủ khả năng bảo vệ không... Chẳng hạn, Luật An toàn Dữ liệu 2021 của Trung Quốc quy định doanh nghiệp sở hữu lượng dữ liệu lớn phải xin đánh giá an ninh trước khi xuất khẩu dữ liệu. Việt Nam cũng có thể học





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

hỏi mô hình này để quản lý luồng dữ liệu ra nước ngoài, ngăn chặn nguy cơ bị lộ dữ liệu chiến lược.

+ ***Áp dụng công nghệ cao bảo vệ dữ liệu nhạy cảm***: Đối với các dữ liệu quan trọng hay dữ liệu cốt lõi, nên nghiên cứu sử dụng các giải pháp công nghệ như “Blockchain” hoặc “tính toán đa bên” (MPC). Blockchain có ưu điểm tạo sổ cái phân tán minh bạch, không thể bị sửa đổi trái phép, phù hợp để đảm bảo tính toàn vẹn cho dữ liệu gốc. Còn MPC cho phép nhiều bên xử lý dữ liệu chung mà không ai thấy toàn bộ dữ liệu, giảm nguy cơ lộ thông tin nhạy cảm khi chia sẻ. Những công nghệ tiên tiến này sẽ tạo thêm một lớp phòng thủ cho dữ liệu trọng yếu, tuy nhiên cần đầu tư và đánh giá kỹ trước khi triển khai trên quy mô lớn.

### ***- Tổ chức thực hiện các biện pháp phòng ngừa và xử lý rủi ro dữ liệu***

***Thứ nhất***, thiết lập hệ thống bảo đảm an toàn giao dịch dữ liệu theo quy định của pháp luật, hướng dẫn các bên tham gia trên sàn thực hiện bảo vệ dữ liệu, truy xuất nguồn gốc, xác định rủi ro, kiểm tra tuân thủ và sử dụng các biện pháp hiệu quả để bảo vệ dữ liệu cá nhân, quyền riêng tư cá nhân, bí mật thương mại, và dữ liệu quan trọng theo quy định của Nhà nước (khoản 4 Điều 35 Nghị định số 169/2025/NĐ-CP).

+ Các chủ thể tham gia phải thiết lập hệ thống bảo đảm an toàn giao dịch dữ liệu theo đúng chuẩn mực pháp luật, coi đây như “lá chắn” đầu tiên bảo vệ các bên tham gia. Hệ thống này cần có khả năng xác thực giao dịch, lưu vết nhật ký, mã hóa dữ liệu trong quá trình truyền tải, đồng thời phát hiện sớm và ngăn chặn hành vi gian lận.

+ Tổ chức vận hành sàn dữ liệu phải có trách nhiệm hướng dẫn các bên tham gia thực hiện đúng quy định về bảo vệ dữ liệu, bao gồm bảo đảm quyền riêng tư cá nhân, bí mật thương mại và bảo mật dữ liệu quan trọng do Nhà





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

nước xác định. Việc này gắn liền với yêu cầu truy xuất nguồn gốc của sản phẩm dữ liệu: mỗi tập dữ liệu giao dịch trên sàn cần có thông tin rõ ràng về nguồn gốc, chủ thể sở hữu và phạm vi khai thác hợp pháp. Ngoài ra, cần tiến hành đánh giá và xác định rủi ro tiềm ẩn trong từng giao dịch, chẳng hạn nguy cơ lộ lọt dữ liệu cá nhân, lạm dụng dữ liệu kinh doanh hoặc tấn công vào hệ thống lưu trữ. Trên cơ sở đó, tổ chức sàn phải triển khai cơ chế kiểm tra tuân thủ định kỳ, áp dụng các biện pháp kỹ thuật và quản trị như kiểm thử an ninh, giám sát truy cập, phân quyền chặt chẽ.

**Thứ hai,** thực hiện các biện pháp bảo vệ, bảo mật hợp lý để bảo vệ dữ liệu cá nhân trong truyền sở hữu của tổ chức, bao gồm ngăn chặn truy cập, thu thập, sử dụng, tiết lộ trái phép hoặc các rủi ro tương tự. Các tổ chức cần xây dựng cơ chế kiểm soát truy cập chặt chẽ, bảo đảm chỉ những cá nhân có thẩm quyền mới được phép tiếp cận dữ liệu. Cùng với đó, hệ thống phải triển khai giải pháp kỹ thuật phòng ngừa như mã hóa dữ liệu khi lưu trữ và truyền tải, sử dụng tường lửa và phần mềm giám sát an ninh mạng để phát hiện sớm hành vi bất thường. Bên cạnh khía cạnh kỹ thuật, cần thực hiện các biện pháp quản trị và tuân thủ pháp luật, bao gồm việc rà soát quy trình thu thập, xử lý, chia sẻ dữ liệu để ngăn chặn tình trạng truy cập, sử dụng, tiết lộ dữ liệu trái phép. Mọi hoạt động xử lý phải gắn với sự đồng ý của chủ thể dữ liệu và phù hợp với Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, cũng như Luật Dữ liệu 2024. Ngoài ra, tổ chức phải có kế hoạch ứng phó sự cố nhằm kịp thời ngăn chặn và khắc phục khi xảy ra rủi ro như tấn công mạng hoặc rò rỉ dữ liệu.

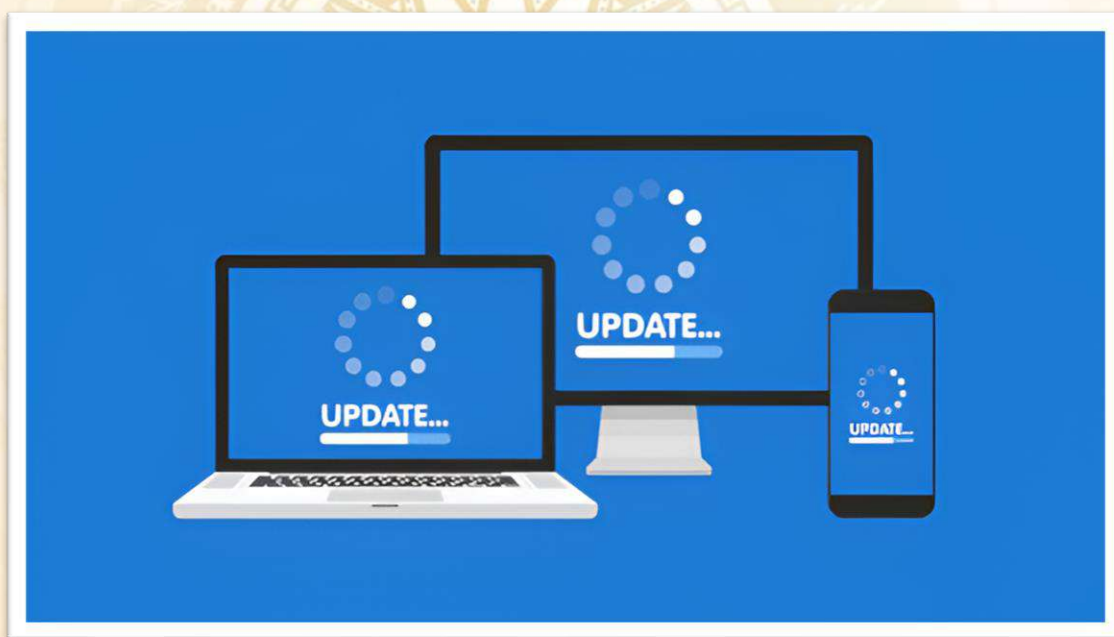
**Thứ ba,** xây dựng hệ thống sao lưu dữ liệu tự động và thường xuyên; kiểm tra khả năng khôi phục dữ liệu. Đây là giải pháp quan trọng nhằm bảo đảm tính liên tục và ổn định cho mọi hoạt động quản lý dữ liệu trong tổ chức.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Về mặt kỹ thuật, hệ thống cần được thiết kế để sao lưu theo lịch trình định kỳ (hàng ngày, hàng tuần hoặc theo thời gian thực đối với dữ liệu nhạy cảm), lưu trữ bản sao tại nhiều địa điểm khác nhau, trong đó có cả máy chủ nội bộ và dịch vụ lưu trữ đám mây bảo mật. Việc này giúp hạn chế tối đa rủi ro mất dữ liệu do sự cố phần cứng, lỗi hệ thống, tấn công mạng hoặc thiên tai. Bên cạnh việc sao lưu, tổ chức cần thường xuyên kiểm tra khả năng khôi phục dữ liệu thông qua các bài kiểm thử thực tế. Việc khôi phục thử không chỉ chứng minh tính khả dụng của bản sao lưu mà còn giúp phát hiện sớm các lỗi kỹ thuật trong quá trình lưu trữ, từ đó kịp thời điều chỉnh. Đặc biệt, dữ liệu được sao lưu phải được mã hóa và kiểm soát truy cập nghiêm ngặt, tránh nguy cơ bị lộ lọt trong quá trình lưu trữ hoặc vận hành.



***Việc update định kỳ đảm bảo giảm thiểu  
sự cố ngoài mong muốn - Ảnh: TCI Technologies***

**Thứ tư**, cập nhật phần mềm, hệ điều hành và vá các loại lỗ hổng bảo mật kịp thời. Cập nhật phần mềm, hệ điều hành và vá các loại lỗ hổng bảo mật kịp thời là một trong những biện pháp cơ bản nhưng mang tính sống còn





trong việc bảo đảm an toàn dữ liệu và hệ thống thông tin. Các phần mềm và hệ điều hành, sau một thời gian vận hành, thường bộc lộ lỗ hổng bảo mật mà tin tặc có thể lợi dụng để tấn công, xâm nhập và chiếm quyền kiểm soát. Nếu không kịp thời vá lỗi, tổ chức sẽ phải đối mặt với nguy cơ rò rỉ dữ liệu, gián đoạn dịch vụ và thiệt hại tài chính.

Vì vậy, việc cập nhật định kỳ và theo dõi sát sao các bản vá bảo mật do nhà sản xuất phát hành cần được đưa vào quy trình quản trị an ninh thông tin chuẩn hóa. Các bản vá này phải được kiểm thử trên môi trường giả lập (sandbox) trước khi áp dụng rộng rãi, nhằm tránh xung đột phần mềm hoặc ảnh hưởng đến vận hành hệ thống. Song song, tổ chức cũng cần thiết lập cơ chế cảnh báo và quản lý bản vá tự động, đảm bảo mọi máy trạm, máy chủ và thiết bị đầu cuối đều được cập nhật đồng bộ, tránh tình trạng bỏ sót.

Ngoài khía cạnh kỹ thuật, việc cập nhật phần mềm còn gắn với yêu cầu pháp lý: Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân và Nghị định 169/2025/NĐ-CP đều nhấn mạnh trách nhiệm của tổ chức trong việc bảo đảm an toàn hệ thống thông tin. Như vậy, cập nhật và vá lỗ hổng không chỉ giúp giảm thiểu nguy cơ bị tấn công, mà còn thể hiện sự tuân thủ pháp luật, góp phần xây dựng môi trường số an toàn, tin cậy, bảo vệ dữ liệu công dân cũng như duy trì uy tín của tổ chức.

**Thứ năm,** đào tạo nhân sự về an toàn dữ liệu và các tình huống rủi ro phổ biến (phishing, ransomware...). Đào tạo nhân sự về an toàn dữ liệu và các tình huống rủi ro phổ biến là một trong những giải pháp trọng yếu, vì yếu tố con người thường được coi là “*mắt xích yếu*” trong chuỗi an ninh mạng.

+ Các tổ chức cần xây dựng chương trình đào tạo bài bản và định kỳ cho toàn bộ nhân viên, từ lãnh đạo đến cán bộ kỹ thuật, tập trung vào nhận diện các mối đe dọa thường gặp như tấn công giả mạo (phishing), lừa đảo



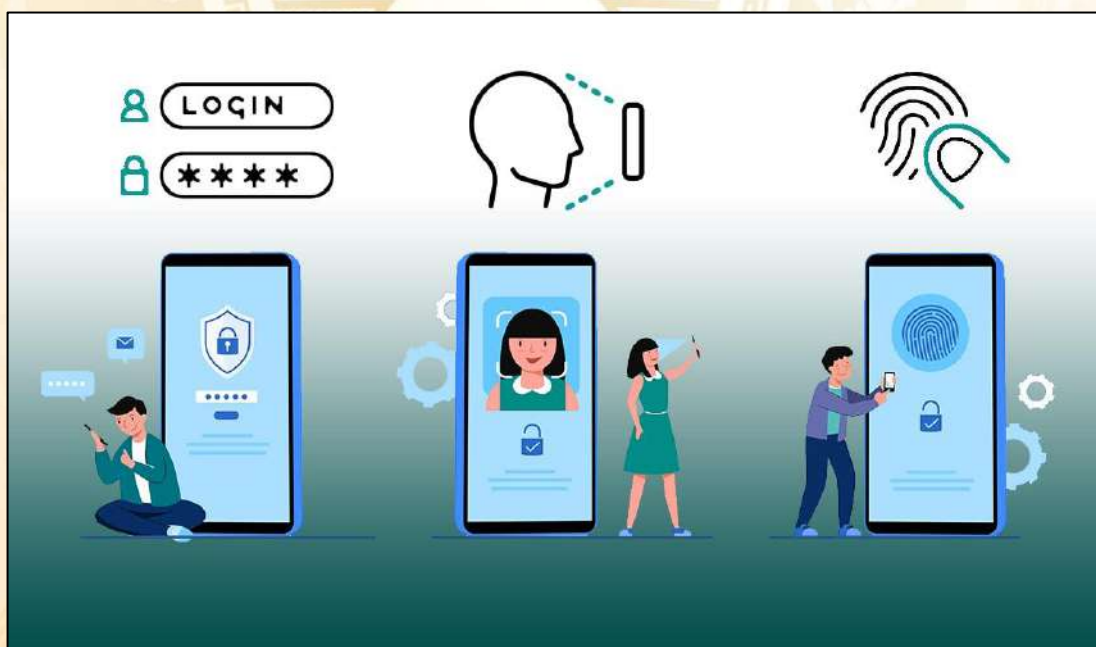


## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

qua email, mã độc tống tiền (ransomware), rò rỉ dữ liệu do sử dụng thiết bị cá nhân hoặc chia sẻ tài liệu không đúng quy trình. Nội dung đào tạo nên bao gồm cả phần lý thuyết (quy định pháp luật, chính sách nội bộ, quy trình ứng cứu sự cố) và phần thực hành (mô phỏng email lừa đảo, bài tập xử lý tình huống, hướng dẫn cách sử dụng công cụ bảo mật).

+ Tổ chức cần triển khai các chiến dịch nâng cao nhận thức liên tục, chẳng hạn gửi bản tin cảnh báo về thủ đoạn mới, dán poster nhắc nhở tại nơi làm việc, tổ chức “*tháng an toàn thông tin*” hoặc các cuộc thi nhỏ về nhận diện rủi ro mạng. Việc này không chỉ giúp nhân viên có khả năng tự bảo vệ mình, mà còn hình thành văn hóa an toàn dữ liệu trong toàn tổ chức.

+ *Về mặt quản lý*, các cơ quan, doanh nghiệp phải gắn đào tạo với trách nhiệm cá nhân, quy định rõ hình thức xử lý khi vi phạm quy trình an toàn dữ liệu, đồng thời khuyến khích khen thưởng những cá nhân phát hiện sớm rủi ro hoặc đề xuất giải pháp hiệu quả.



***Biện pháp xác thực đa yếu tố  
(MFA - Multi-Factor Authentication) - Ảnh: ARATEK***





**Thứ sáu,** áp dụng các biện pháp xác thực đa yếu tố (MFA) để tăng cường độ tin cậy. Áp dụng các biện pháp xác thực đa yếu tố (MFA - Multi-Factor Authentication) là một trong những giải pháp quan trọng nhằm nâng cao mức độ an toàn trong quản trị dữ liệu và hệ thống thông tin. MFA yêu cầu người dùng phải vượt qua ít nhất hai lớp xác thực khác nhau, thay vì chỉ sử dụng mật khẩu truyền thống, từ đó giảm thiểu nguy cơ bị chiếm đoạt tài khoản khi thông tin đăng nhập bị lộ.

Cụ thể, ngoài mật khẩu, người dùng có thể phải cung cấp thêm mã OTP qua tin nhắn hoặc ứng dụng xác thực, sử dụng vân tay, nhận diện khuôn mặt, thẻ thông minh hoặc thiết bị bảo mật chuyên dụng (token). Cách tiếp cận này giúp hạn chế đáng kể các rủi ro từ tấn công giả mạo (phishing), đánh cắp mật khẩu hay tấn công “brute force”. Việc triển khai MFA cần được thực hiện trước hết đối với hệ thống dữ liệu nhạy cảm và tài khoản quản trị cấp cao, sau đó mở rộng ra toàn bộ dịch vụ công trực tuyến, tài khoản nội bộ của cán bộ, nhân viên và cả đối tác tham gia hệ thống. Đồng thời, để đảm bảo hiệu quả, cần kết hợp MFA với chính sách quản lý danh tính và truy cập (IAM), phân quyền chặt chẽ và theo dõi nhật ký truy cập nhằm phát hiện sớm hành vi bất thường.

**Thứ bảy,** thiết lập quy trình phản ứng sự cố (incident response plan) rõ ràng, có người phụ trách cụ thể. Thiết lập quy trình phản ứng sự cố (IRP) rõ ràng, cần có người phụ trách cụ thể là yêu cầu thiết yếu trong chiến lược bảo vệ dữ liệu và an ninh mạng của tổ chức. Quy trình này cần được xây dựng theo các bước chặt chẽ, bảo đảm khi xảy ra sự cố, hệ thống có thể phản ứng nhanh chóng, hạn chế tối đa thiệt hại.

+ Tổ chức phải xác định rõ vai trò, trách nhiệm và người chịu trách nhiệm chính trong xử lý sự cố, từ khâu tiếp nhận thông tin, đánh giá rủi ro,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

cô lập hệ thống bị tấn công cho đến khắc phục và khôi phục dịch vụ. Một đội phản ứng sự cố (Incident Response Team) nên được thành lập, bao gồm chuyên gia an ninh mạng, cán bộ pháp chế và người đại diện lãnh đạo để đảm bảo phối hợp đa chiều. Quy trình này cần được thiết kế theo vòng đời sự cố, bao gồm: *phát hiện - phân tích - ứng phó - khắc phục - phục hồi - rút kinh nghiệm*. Mỗi giai đoạn phải có hướng dẫn cụ thể, thời gian xử lý tối đa và kênh liên lạc khẩn cấp. Đặc biệt, sau mỗi sự cố, tổ chức cần tiến hành đánh giá lại toàn bộ quy trình, cập nhật bài học kinh nghiệm và bổ sung biện pháp phòng ngừa.



### ***Minh họa về IRP - Ảnh: Hà Phương***

+ Bên cạnh đó, quy trình phản ứng sự cố phải được kiểm thử định kỳ thông qua các buổi diễn tập mô phỏng, giúp nhân viên quen với quy trình và giảm thiểu lúng túng khi sự cố thực sự xảy ra. Song song, cần thiết lập cơ chế báo cáo kịp thời cho cơ quan quản lý nhà nước có thẩm quyền, phù hợp với khung pháp lý về bảo vệ an ninh dữ liệu tại Việt Nam.





## **7.2.2.6. Tăng cường giám sát, kiểm tra và xử lý vi phạm**

Dù có biện pháp phòng ngừa tốt đến đâu, rủi ro mất an toàn dữ liệu vẫn có thể xảy ra. Do vậy, việc thiết lập một cơ chế giám sát chủ động và xử lý vi phạm nghiêm minh, minh bạch sẽ giúp phát hiện sớm sự cố và răn đe các hành vi vi phạm. Một số giải pháp chủ chốt trong nhóm này gồm:

**- Đối với Nhà nước:**

**+ Chính phủ cần quan tâm, chỉ đạo các cơ quan, ban, ngành có liên quan tăng cường công tác giám sát, kiểm tra và xử lý phạm:** các Bộ, ban, ngành chủ động nghiên cứu, xây dựng và ban hành quy trình nghiêm ngặt trong cấp phép hoạt động kinh doanh sản phẩm, dịch vụ, dữ liệu theo thẩm quyền, lĩnh vực quản lý theo Nghị định số 169/2025/NĐ-CP. Điều này nhằm tạo hành lang pháp lý minh bạch, bảo đảm thị trường dữ liệu phát triển lành mạnh và có kiểm soát. Bên cạnh đó, Bộ Công an giữ vai trò chủ trì, phối hợp với các bộ, ngành khác và Ủy ban nhân dân các cấp để thực hiện công tác kiểm tra, giám sát, tiếp nhận và giải quyết khiếu nại, tố cáo, cũng như phòng ngừa, phát hiện và xử lý vi phạm trong các hoạt động thử nghiệm có kiểm soát, kinh doanh dữ liệu, sản dữ liệu và các dịch vụ phân tích, tổng hợp dữ liệu. Đây là giải pháp then chốt để bảo đảm an ninh dữ liệu quốc gia, ngăn ngừa tình trạng lạm dụng dữ liệu gây mất an toàn, trật tự xã hội. Riêng đối với Bộ Quốc phòng, cơ quan này được giao trách nhiệm kiểm tra, giám sát và xử lý các vấn đề liên quan đến hoạt động thử nghiệm dữ liệu trong lĩnh vực quốc phòng, cơ yếu, nhằm bảo đảm tuyệt đối an toàn thông tin, tránh mọi nguy cơ xâm nhập hoặc lợi dụng từ bên ngoài. Sự phân công rõ ràng này không chỉ nâng cao hiệu lực quản lý nhà nước mà còn khẳng định quyết tâm bảo vệ dữ liệu - một tài nguyên chiến lược của quốc gia - khỏi mọi nguy cơ vi phạm, góp phần củng cố an ninh, trật tự trong kỷ nguyên số.

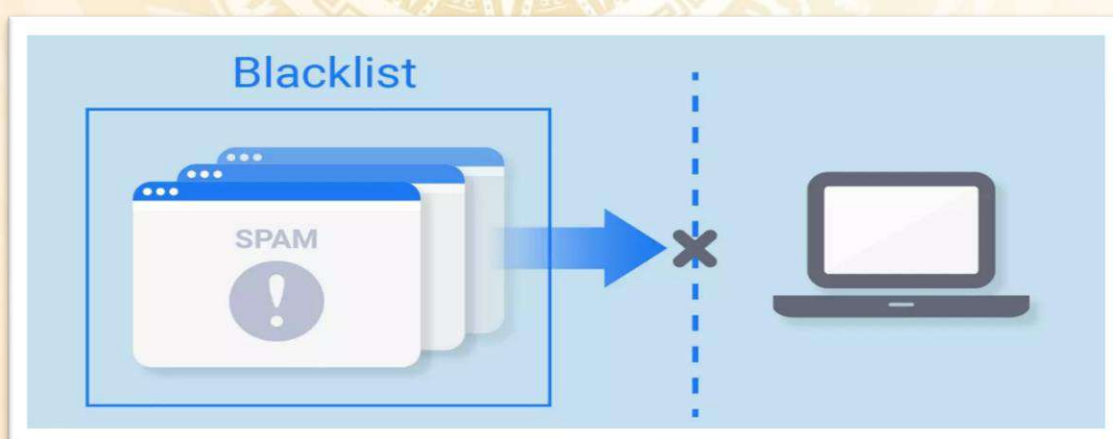




## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Thành lập cơ quan chuyên trách về bảo vệ dữ liệu:** Nhà nước cần phát triển hệ thống thanh tra, giám sát chuyên ngành về an ninh, an toàn dữ liệu (có thể trong Bộ Công an). Cơ quan này được trang bị công cụ kỹ thuật hiện đại để giám sát dịch vụ dữ liệu thời gian thực và tiến hành thanh tra định kỳ hoặc đột xuất các đơn vị quản lý dữ liệu. Ở Trung Quốc, Cục Quản lý Không gian mạng (CAC) có quyền yêu cầu kiểm tra tại chỗ, đình chỉ dịch vụ hoặc xử phạt doanh nghiệp vi phạm về bảo đảm an ninh, an toàn dữ liệu, kể cả công ty nước ngoài [77].

+ **Công khai vi phạm để cảnh báo:** Xây dựng “danh sách đen” công khai các tổ chức, doanh nghiệp vi phạm nghiêm trọng quy định bảo vệ dữ liệu, đăng tải trên Cổng Dữ liệu Quốc gia hoặc phương tiện thông tin đại chúng. Ví dụ, nếu một công ty tài chính để lộ dữ liệu khách hàng nhiều lần, tên công ty đó sẽ được công bố, cảnh báo người dân thận trọng khi sử dụng dịch vụ. Sự minh bạch này tạo áp lực mạnh buộc doanh nghiệp phải coi trọng an ninh, an toàn dữ liệu, bởi không ai muốn bị nêu tên trước công luận, ảnh hưởng uy tín và kinh doanh.



**Ảnh minh họa - Ảnh: ezCloud**

+ **Xử lý nghiêm và đủ sức răn đe:** Hoàn thiện chế tài xử phạt vi phạm dữ liệu theo hướng tăng mức phạt đủ sức răn đe, đặc biệt cho các hành vi cố





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

ý nghiêm trọng như: thu thập/mua bán dữ liệu cá nhân trái phép quy mô lớn, tái phạm nhiều lần, che giấu sự cố không báo cáo. Biện pháp có thể bao gồm phạt tiền nặng (tham khảo GDPR có thể phạt đến 4% doanh thu toàn cầu của công ty), tước giấy phép hoạt động công nghệ thông tin, hoặc truy cứu trách nhiệm hình sự những trường hợp gây hậu quả rất nghiêm trọng, đặc biệt nghiêm trọng. Song song đó, cần bảo vệ và khuyến khích tố giác vi phạm dữ liệu, tạo cơ chế để nhân viên nội bộ hay người dùng có thể báo cáo sai phạm mà không sợ bị “trả thù”.

Sự vận hành an toàn của một hệ thống quản lý dữ liệu phụ thuộc vào việc giám sát và thực thi pháp luật một cách nghiêm minh. Hoạt động thanh tra, kiểm tra định kỳ hoặc đột xuất, cùng với việc áp dụng chế độ xử phạt công khai và minh bạch, tạo áp lực tuân thủ lên các bên liên quan. Điều này buộc các tổ chức phải chủ động nâng cao năng lực bảo vệ dữ liệu của mình. Khi nhận thức được rằng sẽ có hậu kiểm chặt chẽ, các doanh nghiệp sẽ xem việc đầu tư vào an ninh dữ liệu là một yêu cầu sống còn, không chỉ là tuân thủ quy định một cách hình thức.

***- Đối với doanh nghiệp, tổ chức, cá nhân:***

Doanh nghiệp, tổ chức, cá nhân khi kinh doanh, sử dụng sản phẩm, dịch vụ về dữ liệu cần chú ý một số vấn đề như sau:

***+ Tuân thủ các quy định của pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng, an ninh mạng, an ninh dữ liệu, giao dịch điện tử, tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu, bảo mật thông tin, bảo đảm tính chính xác của việc cung cấp dịch vụ; ban hành quy trình hoạt động kinh doanh sản phẩm, dịch vụ, phân tích, tổng hợp dữ liệu và được sự đồng ý của cơ quan quản lý nhà nước về dữ liệu.*** Tuân thủ các quy định của pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng, an ninh mạng, an





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

ninh dữ liệu và giao dịch điện tử là yêu cầu bắt buộc đối với mọi tổ chức, cá nhân tham gia kinh doanh sản phẩm, dịch vụ dữ liệu. Việc này không chỉ nhằm đảm bảo quyền riêng tư của công dân và tính toàn vẹn của dữ liệu, mà còn là điều kiện để các hoạt động kinh doanh gắn với dữ liệu được công nhận là hợp pháp. Các chủ thể phải vận hành hệ thống trên cơ sở tuân thủ các tiêu chuẩn và quy chuẩn kỹ thuật quốc gia về dữ liệu, từ đó bảo đảm tính chính xác, minh bạch trong quá trình cung cấp dịch vụ. Đồng thời, tổ chức, cá nhân phải ban hành quy trình hoạt động rõ ràng đối với việc thu thập, phân tích, tổng hợp và kinh doanh dữ liệu, trong đó quy định cụ thể trách nhiệm bảo mật, cơ chế giám sát và xử lý rủi ro. Mọi hoạt động này chỉ được phép triển khai sau khi có sự đồng ý và phê duyệt của cơ quan quản lý nhà nước có thẩm quyền về dữ liệu. Đây là điều kiện pháp lý nền tảng để bảo vệ lợi ích quốc gia, quyền lợi người dân, đồng thời duy trì sự ổn định và niềm tin xã hội trong tiến trình phát triển kinh tế số và xã hội số.

+ ***Kiểm tra, đánh giá việc đáp ứng điều kiện tham gia sản dữ liệu của các chủ thể có liên quan; tính hợp pháp và việc đáp ứng các điều kiện tham gia giao dịch của sản phẩm, dịch vụ dữ liệu, khả năng đáp ứng yêu cầu trong bảo đảm an ninh, an toàn khi sử dụng sản phẩm dữ liệu.*** Theo khoản 1 Điều 35 Nghị định số 169/2025/NĐ-CP, các tổ chức, cá nhân khi cung cấp sản phẩm, dịch vụ dữ liệu hoặc tham gia sản dữ liệu cần được thẩm định toàn diện trên ba phương diện chính.

Trước hết là *tính hợp pháp*, tức là sản phẩm, dịch vụ dữ liệu phải có nguồn gốc rõ ràng, không vi phạm quyền riêng tư cá nhân, không khai thác trái phép dữ liệu thuộc phạm vi quản lý của Nhà nước, đồng thời tuân thủ đầy đủ quy định pháp luật về an ninh mạng, an toàn thông tin và bảo vệ dữ liệu cá nhân. Tiếp theo là *điều kiện tham gia giao dịch*, trong đó chủ thể cần





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

chứng minh năng lực kỹ thuật, nhân sự và tài chính để cung cấp dịch vụ dữ liệu ổn định, không gây gián đoạn hoặc rủi ro cho người sử dụng. Cuối cùng là *khả năng bảo đảm an ninh, an toàn*, đòi hỏi có chính sách bảo mật rõ ràng, áp dụng công nghệ mã hóa, phân quyền truy cập chặt chẽ, thường xuyên kiểm tra hệ thống và có phương án ứng cứu sự cố khi bị tấn công.

Quy trình kiểm tra, đánh giá này giúp ngăn chặn từ sớm tình trạng lợi dụng sản dữ liệu để rao bán dữ liệu trái phép, cung cấp dịch vụ kém chất lượng hoặc phát tán sản phẩm tiềm ẩn nguy cơ an ninh. Đồng thời, nó cũng khẳng định vai trò của cơ quan quản lý trong việc thiết lập “chuẩn mực thị trường dữ liệu”, tạo môi trường cạnh tranh lành mạnh, bảo vệ quyền lợi của tổ chức, cá nhân tham gia và củng cố niềm tin xã hội vào quá trình phát triển kinh tế số, xã hội số.

**+ Xây dựng chính sách và quy trình bảo mật dữ liệu chặt chẽ, chiến lược bảo vệ toàn diện, bao gồm việc ban hành các chính sách bảo vệ dữ liệu rõ ràng, phân loại dữ liệu theo mức độ nhạy cảm để áp dụng vào biện pháp bảo vệ phù hợp, và kiểm soát truy cập chặt chẽ.** Trước hết, tổ chức, cá nhân cần xây dựng các chính sách, phương án cụ thể, minh bạch về bảo vệ dữ liệu, xác định rõ trách nhiệm và quyền hạn trong từng khâu thu thập, lưu trữ, xử lý, chia sẻ và hủy dữ liệu. Đi liền với đó là việc phân loại dữ liệu theo mức độ nhạy cảm để áp dụng biện pháp bảo vệ phù hợp: dữ liệu công khai có thể chia sẻ rộng rãi, dữ liệu nội bộ yêu cầu bảo mật trong phạm vi tổ chức, còn dữ liệu mật và tuyệt mật phải được mã hóa, kiểm soát nghiêm ngặt và hạn chế tối đa quyền truy cập. Một chính sách bảo mật bài bản như vậy không chỉ giúp phòng ngừa nguy cơ rò rỉ từ cả bên ngoài lẫn nội bộ, mà còn bảo đảm sự tuân thủ pháp luật hiện hành như Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP, Luật Dữ liệu 2024





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

và Nghị định 169/2025/NĐ-CP, đồng thời tạo tiền đề để cơ quan, tổ chức đạt được các chuẩn mực quốc tế, nâng cao uy tín và củng cố niềm tin của xã hội đối với hệ thống dữ liệu quốc gia.



### ***Minh họa quy trình mã hóa dữ liệu - Ảnh: Onetel***

+ ***Áp dụng các công nghệ mã hóa dữ liệu trong quá trình lưu trữ và truyền tải, mã hóa dữ liệu nhạy cảm, thường xuyên cập nhật phần mềm, vá các lỗ hổng bảo mật và tổ chức đào tạo nâng cao nhận thức cho nhân viên là những yếu tố cốt lõi để duy trì một môi trường dữ liệu an toàn và tuân thủ pháp luật.*** Trước hết, dữ liệu nhạy cảm cần được mã hóa toàn diện cả khi lưu trữ trên máy chủ lẫn khi truyền qua mạng, nhằm ngăn chặn việc bị đánh cắp hoặc nghe lén trong quá trình trao đổi. Việc sử dụng các chuẩn mã hóa tiên tiến như AES-256 hay TLS 1.3 không chỉ tăng cường khả năng bảo mật mà còn đáp ứng yêu cầu pháp lý trong Luật An ninh mạng 2018 và Luật Dữ liệu 2024. Song song với đó, các tổ chức phải duy trì cơ chế cập nhật phần mềm và vá lỗ hổng bảo mật thường xuyên, bởi đa số các vụ tấn công mạng đều xuất phát từ việc khai thác hệ thống chưa được vá lỗi. Bên cạnh biện pháp kỹ thuật, yếu tố con người cũng giữ vai trò quyết định: việc





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

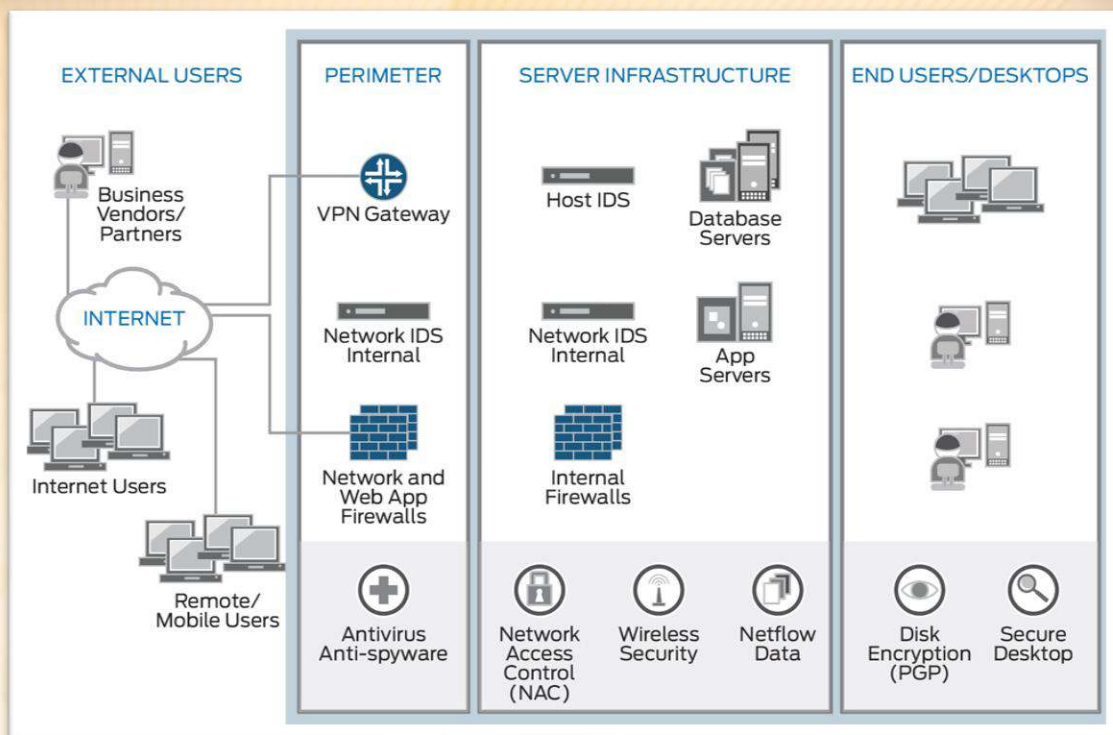
đào tạo, nâng cao nhận thức an ninh mạng cho nhân viên sẽ giúp giảm thiểu nguy cơ từ bên trong, hạn chế những hành vi vô ý hoặc thiếu hiểu biết dẫn đến rò rỉ dữ liệu. Sự kết hợp đồng bộ giữa mã hóa dữ liệu, quản trị lỗ hổng và đào tạo nhân lực chính là nền tảng để duy trì một môi trường dữ liệu an toàn, bền vững, đồng thời bảo đảm tuân thủ pháp luật và chuẩn mực quốc tế trong kỷ nguyên số.

+ ***Sử dụng phần mềm giám sát an ninh mạng (SIEM, IDS/IPS) để phát hiện sớm các hành vi bất thường.*** Việc sử dụng phần mềm giám sát an ninh mạng như SIEM (Security Information and Event Management) hay IDS/IPS (Intrusion Detection/Prevention System) cần được triển khai đồng bộ và xem như một lớp phòng thủ chủ động trong quản trị dữ liệu. Cụ thể, SIEM có chức năng thu thập nhật ký từ nhiều hệ thống, phân tích và tương quan dữ liệu để phát hiện hành vi bất thường, từ đó gửi cảnh báo thời gian thực đến đội ngũ quản trị. IDS/IPS lại tập trung giám sát trực tiếp lưu lượng mạng, nhận diện các sự tấn công hoặc hành vi bất thường, đồng thời có khả năng ngăn chặn tự động các gói tin độc hại, bảo vệ hệ thống trước nguy cơ xâm nhập. Khi được tích hợp, hai công cụ này giúp cơ quan, tổ chức vừa có bức tranh toàn cảnh về an ninh mạng, vừa có khả năng ngăn chặn tức thì các mối đe dọa. Để phát huy hiệu quả, cần xác định rõ phạm vi giám sát (ưu tiên các cơ sở dữ liệu và dịch vụ công trọng yếu), thường xuyên cập nhật quy tắc nhận diện, phân quyền xử lý sự cố, đồng thời tổ chức đào tạo nhân lực để phân tích và phản ứng kịp thời. Nhờ đó, SIEM và IDS/IPS trở thành công cụ then chốt giúp phát hiện sớm, ứng phó nhanh và giảm thiểu tối đa rủi ro mất an ninh, an toàn dữ liệu trong bối cảnh hiện nay.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



## ***Phần mềm giám sát an ninh mạng SIEM (Security Information and Event Management) - Ảnh: Juniper Networks***

+ ***Thực hiện đánh giá an ninh hệ thống định kỳ (audit) và kiểm thử xâm nhập (penetration testing).*** Việc thực hiện đánh giá an ninh hệ thống định kỳ kết hợp với kiểm thử xâm nhập là giải pháp quan trọng để chủ động phát hiện và xử lý lỗ hổng bảo mật trước khi bị tin tặc lợi dụng. Thông qua audit, các tổ chức tiến hành rà soát toàn diện hạ tầng công nghệ thông tin như máy chủ, mạng, cơ sở dữ liệu và ứng dụng, đối chiếu với quy định pháp luật (Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP, Nghị định 169/2025/NĐ-CP...) cũng như các chuẩn quốc tế (ISO/IEC 27001, NIST). Nhờ đó, có thể sớm phát hiện các sai sót trong cấu hình, điểm yếu kỹ thuật và thiếu sót trong việc tuân thủ quy định pháp lý để kịp thời khắc phục.

Song song, ***kiểm thử xâm nhập*** mô phỏng các phương thức tấn công thực tế dưới góc nhìn của tin tặc, sử dụng các kỹ thuật như quét lỗ hổng, tấn





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

công thử SQL Injection, Cross-Site Scripting hoặc kiểm thử mật khẩu yếu nhằm đánh giá khả năng phòng thủ của hệ thống. Sự kết hợp này tạo ra cơ chế phòng thủ nhiều lớp, audit đảm bảo sự tuân thủ và chuẩn hóa, trong khi penetration testing giúp xác định những điểm yếu tiềm ẩn trong thực tế. Khi được triển khai nghiêm túc và định kỳ, hai biện pháp này không chỉ tăng cường mức độ an toàn dữ liệu, mà còn góp phần duy trì niềm tin của người dân, doanh nghiệp vào dịch vụ công trực tuyến và năng lực quản lý của cơ quan nhà nước trong kỷ nguyên số.



*05 bước kiểm thử xâm nhập được nhiều doanh nghiệp thực hiện - Ảnh: Akto*

+ **Phân quyền truy cập dữ liệu nghiêm ngặt.** Phân quyền truy cập dữ liệu nghiêm ngặt là một giải pháp quản trị thiết yếu nhằm bảo đảm rằng chỉ những cá nhân, bộ phận có thẩm quyền mới được tiếp cận đúng loại dữ liệu





cần thiết cho công việc. Trên thực tế, việc triển khai cần tuân thủ nguyên tắc “ít quyền nhất”, nghĩa là mỗi người dùng chỉ được cấp quyền trong phạm vi tối thiểu cần thiết. Dữ liệu cần được phân loại theo cấp độ nhạy cảm, từ công khai đến mật, tối mật, tuyệt mật, với cơ chế cấp quyền và bảo mật tương ứng. Để tăng cường an toàn, các tổ chức phải áp dụng xác thực đa yếu tố, quản lý vòng đời tài khoản, thu hồi quyền ngay khi nhân sự chuyển vị trí hoặc nghỉ việc. Đồng thời, việc giám sát và ghi nhật ký truy cập phải được thực hiện liên tục để bảo đảm mọi hoạt động đều có dấu vết, dễ dàng kiểm soát và điều tra khi cần thiết. Giải pháp này không chỉ giúp ngăn ngừa rò rỉ dữ liệu từ bên trong mà còn đáp ứng yêu cầu pháp lý của Luật An ninh mạng 2018, Luật Dữ liệu 2024 và Nghị định 169/2025/NĐ-CP, qua đó bảo vệ dữ liệu nhạy cảm, nâng cao trách nhiệm giải trình và củng cố niềm tin xã hội vào dịch vụ công cũng như năng lực quản lý nhà nước trong kỷ nguyên số.

+ ***Đảm bảo chế độ báo cáo định kỳ.*** Các tổ chức, doanh nghiệp cung cấp sản phẩm, dịch vụ dữ liệu phải báo cáo định kỳ về thực trạng an toàn dữ liệu. Báo cáo bao gồm các chỉ số về sự cố đã xảy ra, điểm yếu đã phát hiện, số yêu cầu của chủ thể dữ liệu được xử lý... Việc này nhằm tạo thói quen tự đánh giá và sớm phát hiện nguy cơ tiềm ẩn trước khi biến thành vi phạm nghiêm trọng.

#### ***7.2.2.7. Nâng cao năng lực quốc gia về an ninh, an toàn dữ liệu***

Cuối cùng nhưng không kém phần quan trọng, bảo đảm an ninh, an toàn dữ liệu cần được đặt trong chiến lược tổng thể nâng cao năng lực quốc gia về khoa học, công nghệ và nguồn nhân lực. Trong bối cảnh cạnh tranh số, quốc gia nào làm chủ tốt dữ liệu và an toàn dữ liệu sẽ có lợi thế vượt

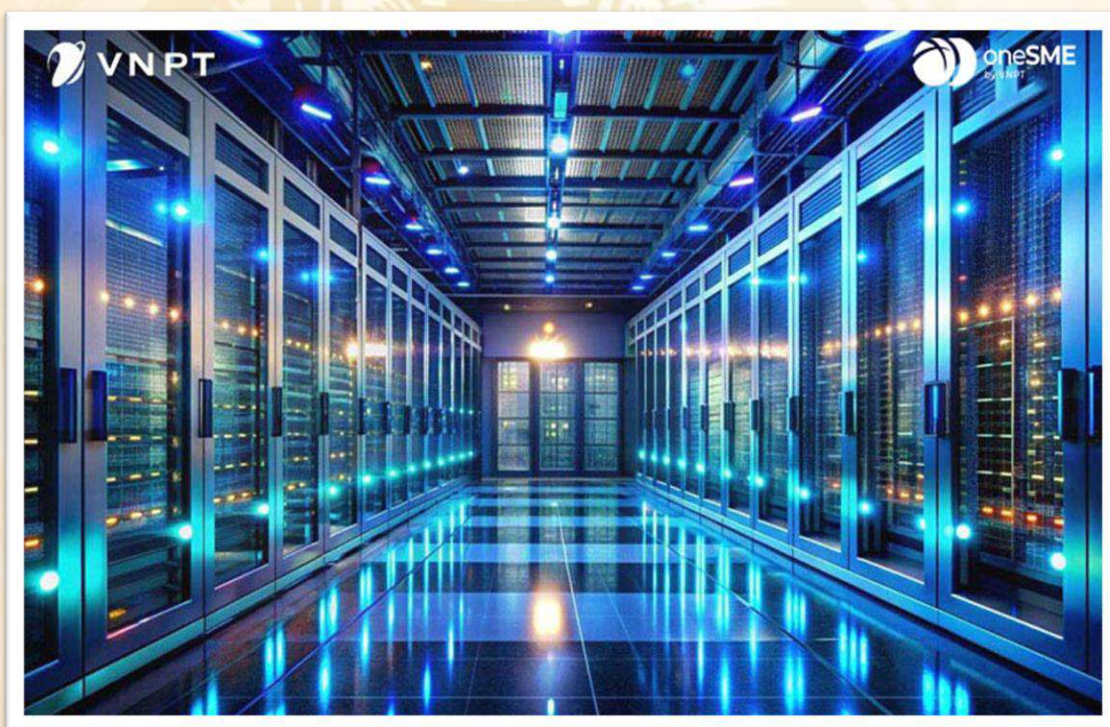




## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

trội. Để đạt được mục tiêu dài hạn này, cần triển khai các hiệu quả, đồng bộ **04 giải pháp** sau:

+ **Đầu tư hạ tầng kỹ thuật đạt chuẩn quốc tế:** Xây dựng các Trung tâm Dữ liệu quốc gia với quy mô và tiêu chuẩn an toàn cao, có cơ chế dự phòng thảm họa và năng lực xử lý lớn phục vụ nhu cầu lưu trữ, phân tích dữ liệu trong nước. Hạ tầng này nên do các doanh nghiệp Việt Nam làm chủ để đảm bảo chủ quyền. Nhà nước có thể hỗ trợ vốn, ưu đãi thuế để khuyến khích phát triển ngành công nghiệp trung tâm dữ liệu và điện toán đám mây nội địa.



**Làn sóng đầu tư vào trung tâm dữ liệu tại Việt Nam - Ảnh: VnEconomy**

+ **Thúc đẩy nghiên cứu và làm chủ công nghệ bảo mật:** Tập trung nguồn lực cho các chương trình nghiên cứu quốc gia về an toàn thông tin, mật mã. Tập trung vào các lĩnh vực mới nổi như mật mã hậu lượng tử, AI trong an ninh mạng, công nghệ phòng thủ tự động... Mục tiêu là Việt Nam có thể tự chủ được các giải pháp bảo mật cốt lõi thay vì phụ thuộc hoàn toàn





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

vào giải pháp ngoại nhập. Bên cạnh đó, khuyến khích khu vực tư nhân, các “start-up” tham gia sáng tạo sản phẩm dịch vụ an ninh dữ liệu (ví dụ giải pháp giám sát anomalies bằng AI, nền tảng chia sẻ dữ liệu an toàn...). Nhà nước có thể hỗ trợ thông qua các quỹ đổi mới sáng tạo, chương trình “sandbox” thí điểm.

+ **Tăng cường hợp tác quốc tế:** An ninh dữ liệu là “vấn đề xuyên biên giới”, do đó việc hợp tác với cộng đồng quốc tế rất quan trọng. Việt Nam cần chủ động tham gia các mạng lưới chia sẻ thông tin sự cố an ninh mạng, ký kết thỏa thuận tương trợ điều tra tội phạm mạng với các nước, và học hỏi kinh nghiệm xây dựng thể chế bảo vệ dữ liệu từ các đối tác tiềm năng. Ví dụ, phối hợp với INTERPOL và các nước ASEAN trong việc truy vết, xử lý tội phạm công nghệ cao xuyên quốc gia; có cơ chế trao đổi chuyên gia với các Trung tâm an ninh mạng hàng đầu thế giới. Qua đó cũng giúp Việt Nam nâng cao vị thế, uy tín trong mắt nhà đầu tư nước ngoài, từ đó thu hút thêm nguồn lực phát triển kinh tế số.

+ **Nâng cao nhận thức cộng đồng về bảo vệ dữ liệu:** Phát động các chiến dịch truyền thông, tuyên truyền pháp luật, giáo dục về an ninh, an toàn dữ liệu. Đưa chủ đề “quyền dữ liệu cá nhân” vào chương trình giáo dục phổ thông và đại học để thế hệ trẻ hiểu biết và cẩn trọng hơn khi chia sẻ thông tin trên mạng. Tổ chức các cuộc thi, hội thảo, tọa đàm, trao đổi về an ninh mạng để thu hút sự quan tâm của xã hội. Khi toàn dân có ý thức bảo vệ dữ liệu, ví dụ như biết cách đặt mật khẩu mạnh, cảnh giác với các hình thức lừa đảo trực tuyến (phishing) và tôn trọng quyền riêng tư của người khác, thì mức độ an toàn thông tin chung của quốc gia sẽ được nâng cao.





Trên đây là các nhóm giải pháp cơ bản, chủ yếu góp phần đảm bảo an ninh, an toàn dữ liệu trong sử dụng các sản phẩm, dịch vụ dữ liệu trong thời gian tới. Mặc dù các nguyên tắc chung đều cần được tuân thủ, mỗi sản phẩm, dịch vụ dữ liệu (trung gian dữ liệu, tổng hợp, phân tích dữ liệu và sàn dữ liệu) sẽ có những đặc thù riêng. Nhóm tác giả cũng đã cố gắng lồng ghép các giải pháp phát triển, nâng cao hiệu quả sử dụng nói chung và giải pháp đảm bảo an ninh, an toàn dữ liệu cho từng nhóm sản phẩm, dịch vụ dữ liệu nói riêng xuyên suốt quá trình trình bày bài dự thi; xin phép không nhắc lại trong phần “7.2. Giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu”.

Như vậy, an ninh, an toàn dữ liệu trong các sản phẩm, dịch vụ dữ liệu không chỉ là câu chuyện kỹ thuật mà đã trở thành một phần cốt lõi của chiến lược phát triển quốc gia trong kỷ nguyên số. Luật Dữ liệu 2024 ra đời đánh dấu bước tiến quan trọng, đặt nền móng pháp lý hiện đại cho việc quản lý và bảo vệ dữ liệu ở Việt Nam. Tuy nhiên, chặng đường phía trước đòi hỏi nỗ lực đồng bộ từ hoàn thiện pháp luật, triển khai công nghệ, tổ chức nhân sự đến giáo dục cộng đồng. Bảy nhóm giải pháp nêu trên tựa như những mắt xích liên kết chặt chẽ với nhau; khi được thực thi một cách hài hòa, chúng sẽ tạo nên một “lá chắn số” vững chắc bảo vệ dữ liệu quốc gia. Nhờ đó, Việt Nam có thể tự tin khai thác hiệu quả “mỏ dầu dữ liệu” để phát triển kinh tế, xã hội, đồng thời bảo đảm an toàn cho người dân, tổ chức và giữ vững chủ quyền số của đất nước trước bất kỳ tình huống nào./.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

## Cách bảo vệ dữ liệu thông tin cá nhân

Trong xã hội hiện đại, việc giao tiếp qua mạng xã hội cũng như giao dịch trực tuyến là phổ biến nhưng cũng rất dễ để lộ thông tin riêng tư. Dưới đây là những lời khuyên hữu ích nhằm bảo vệ các dữ liệu thông tin cá nhân.



### Chia sẻ thông tin trên phương tiện truyền thông xã hội càng ít càng tốt

Mỗi trang web truyền thông xã hội cho phép cá nhân thay đổi cài đặt bảo mật nhằm bảo vệ quyền riêng tư, vì vậy nên sử dụng chúng bất cứ khi nào chia sẻ thông tin.



### Sử dụng trình duyệt web riêng tư hoặc bảo mật

Cách này xóa tệp Internet tạm thời và lịch sử trình duyệt web khi người sử dụng đóng cửa sổ. Đó là mức độ bảo vệ cao nhất mà người sử dụng có thể nhận được.



### Tránh sử dụng Wifi công cộng và tại các điểm nóng

Những kết nối này không an toàn. Nếu phải sử dụng Wifi công cộng, hãy đảm bảo sử dụng ứng dụng mã hóa dữ liệu hoặc sử dụng VPN\*.



### Sử dụng mật khẩu mạnh và độc đáo

Kết hợp các ký tự ngẫu nhiên, số và ký hiệu đặc biệt sẽ là một mật khẩu tốt nhất. Không bao giờ sử dụng cùng một mật khẩu cho 2 hoặc nhiều tài khoản.



### Sử dụng xác thực 2 yếu tố

Phải sử dụng mã mà trang web gửi tới điện thoại cá nhân tại thời điểm đăng nhập. Tin tặc dù biết mật khẩu nhưng không thể truy cập tài khoản của cá nhân vì không có điện thoại di động.



### Kiểm tra https

Hãy đảm bảo rằng trang web khi tham gia trình duyệt bắt đầu bằng https, có nghĩa là dữ liệu chia sẻ với trang web này chỉ hiển thị với những người có quyền truy cập được phép đọc.

Nguồn: TTXVN; Jakarta Post

<http://infographics.vn>

© TTXVN  
Vietnam News Agency

**Infographic về bảo vệ dữ liệu cá nhân - Ảnh: TTXVN**



## *Câu 8*

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

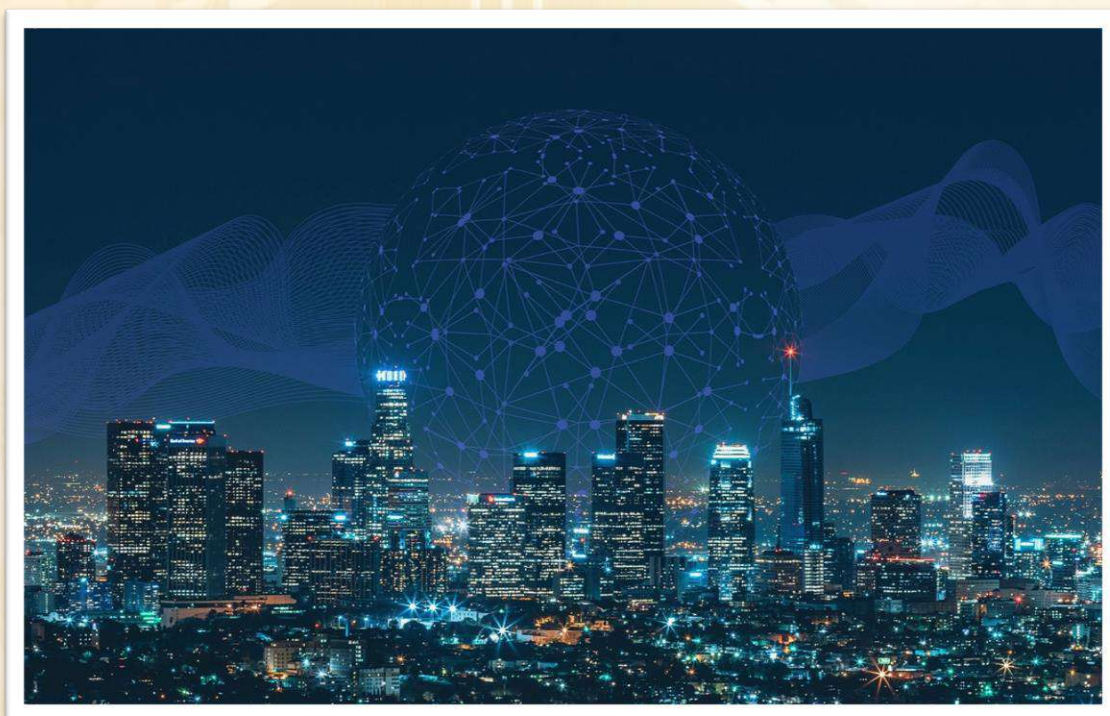






## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

*“Dữ liệu được nhìn nhận sẽ góp phần chuyển đổi cơ cấu nền kinh tế Việt Nam, giúp đất nước vượt qua mức thu nhập trung bình thấp vào năm 2030 và đạt mức thu nhập cao vào năm 2045”<sup>50</sup>. Với tầm quan trọng chiến lược của dữ liệu trong kỷ nguyên số, Việt Nam đã thể hiện sự chủ động trong việc thiết lập một khung pháp lý vững chắc qua Điều 8 của Luật Dữ liệu năm 2024. Qua đó cho thấy đây là một bước tiến quan trọng, tạo nền tảng toàn diện cho công tác quản lý nhà nước về dữ liệu.*



***Kết nối dữ liệu trong kỷ nguyên mới - Ảnh: VnEconomy***

### ***Điều 8. Quản lý nhà nước về dữ liệu***

#### ***1. Nội dung quản lý nhà nước về dữ liệu bao gồm:***

<sup>50</sup> Bạch Dương (2025), *Bốn mục tiêu cho Chiến lược dữ liệu quốc gia đến năm 2030*, [vneconomy.vn](https://vneconomy.vn/bon-muc-tieu-cho-chien-luoc-du-lieu-quoc-gia-den-nam-2030.htm), <https://vneconomy.vn/bon-muc-tieu-cho-chien-luoc-du-lieu-quoc-gia-den-nam-2030.htm>, truy cập ngày 06/8/2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

a) Xây dựng, ban hành, tổ chức thực hiện Chiến lược dữ liệu quốc gia; văn bản quy phạm pháp luật về dữ liệu; tiêu chuẩn, quy chuẩn kỹ thuật, định mức kinh tế - kỹ thuật, chất lượng dữ liệu;

b) Tuyên truyền, phổ biến chính sách, pháp luật về dữ liệu; hướng dẫn cơ quan quản lý cơ sở dữ liệu, hệ thống thông tin trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu;

c) Quản lý, giám sát các hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu, bảo đảm an ninh, an toàn dữ liệu;

d) Báo cáo, thống kê về dữ liệu; nghiên cứu, ứng dụng khoa học và công nghệ về dữ liệu; sản phẩm, dịch vụ về dữ liệu; quản lý, giám sát, phát triển thị trường dữ liệu;

đ) Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về dữ liệu;

e) Đào tạo, bồi dưỡng, phát triển nguồn nhân lực và hợp tác quốc tế về dữ liệu.

2. Trách nhiệm quản lý nhà nước về dữ liệu được quy định như sau:

a) Chính phủ thống nhất quản lý nhà nước về dữ liệu;

b) Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về dữ liệu, trừ quy định tại điểm c khoản này;

c) Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về dữ liệu thuộc phạm vi quản lý.

Bộ trưởng Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về dữ liệu cơ yếu thuộc phạm vi quản lý theo quy định của pháp luật về cơ yếu;





d) Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình xây dựng, phát triển cơ sở dữ liệu; phối hợp với Bộ Công an thực hiện quản lý nhà nước về dữ liệu;

đ) Ủy ban nhân dân cấp tỉnh xây dựng, phát triển cơ sở dữ liệu; thực hiện quản lý nhà nước về dữ liệu tại địa phương.

## 8.1. NỘI DUNG QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU

### 8.1.1. Nội dung quản lý nhà nước về dữ liệu

Theo Điều 8 của Luật Dữ liệu năm 2024, công tác quản lý nhà nước về dữ liệu bao gồm các nội dung cốt lõi sau:

**8.1.1.1. Xây dựng, ban hành và tổ chức thực hiện Chiến lược dữ liệu quốc gia; văn bản pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật, định mức kinh tế - kỹ thuật, chất lượng dữ liệu**

**Thứ nhất**, một trong những nội dung nền tảng của quản lý nhà nước về dữ liệu là xây dựng, ban hành Chiến lược dữ liệu quốc gia và tổ chức thực hiện chiến lược này. Chiến lược dữ liệu quốc gia đặt tầm nhìn dài hạn cho việc phát triển và khai thác dữ liệu trên phạm vi quốc gia. Thủ tướng Chính phủ đã phê duyệt Chiến lược dữ liệu quốc gia đến năm 2030 tại Quyết định số 142/QĐ-TTg ngày 02/02/2024. Chiến lược đã xác định dữ liệu là nền tảng mở ra không gian phát triển mới cho chính phủ số, kinh tế số và xã hội số, đồng thời đảm bảo quá trình chuyển đổi số thành công, đưa Việt Nam trở thành quốc gia số an toàn<sup>51</sup>.

Chiến lược dữ liệu quốc gia 2030 đề ra các mục tiêu chính, bao gồm: hoàn thiện thể chế (nghiên cứu xây dựng Luật về công nghiệp công nghệ số

<sup>51</sup> Bộ Khoa học và Công nghệ (2025), *Chiến lược dữ liệu quốc gia - Tầm nhìn đến năm 2030*, Mst.gov.vn, <https://mst.gov.vn/chien-luoc-du-lieu-quoc-gia-tam-nhin-den-nam-2030-197250220222423434.htm>, truy cập ngày 07/8/2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

nhằm xác lập quyền sở hữu dữ liệu và thị trường dữ liệu), phát triển hạ tầng dữ liệu quốc gia (xây dựng các trung tâm dữ liệu quốc gia, bảo đảm kết nối đồng bộ trên toàn quốc), phát triển các cơ sở dữ liệu quốc gia trọng điểm (như Cơ sở dữ liệu quốc gia về dân cư, đất đai, đăng ký doanh nghiệp, tài chính, bảo hiểm,...) và thúc đẩy kết nối, chia sẻ dữ liệu giữa các cơ quan thông qua các nền tảng tích hợp, chia sẻ dữ liệu quốc gia. Việc ban hành chiến lược giúp định hướng cho các bộ, ngành và địa phương trong việc phát triển dữ liệu, đảm bảo rằng mọi hoạt động quản lý nhà nước về dữ liệu đều thống nhất theo một tầm nhìn chung.



***Thủ tướng Chính phủ Phạm Minh Chính yêu cầu các Bộ, ngành, địa phương tăng cường kết nối, chia sẻ dữ liệu giữa các Cơ sở dữ liệu quốc gia, chuyên ngành, bảo đảm thông suốt, hiệu quả - Ảnh: VGP***

***Thứ hai***, cùng với chiến lược, Nhà nước có trách nhiệm xây dựng và ban hành hệ thống văn bản quy phạm pháp luật về dữ liệu, cũng như các tiêu





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

chuẩn, quy chuẩn kỹ thuật, định mức kinh tế - kỹ thuật, quy định về chất lượng dữ liệu. Điều này tạo khung pháp lý và kỹ thuật cho mọi hoạt động về dữ liệu. Trên thực tế, Quốc hội đã ban hành Luật Dữ liệu 2024 để thiết lập nền tảng pháp lý chung. Bên cạnh luật này, Chính phủ và các bộ ngành cũng ban hành các nghị định, thông tư liên quan như Nghị định số 47/2020/NĐ-CP về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước đã quy định chi tiết việc quản trị dữ liệu, chia sẻ dữ liệu giữa các cơ quan. Ngoài ra, Chính phủ cũng ban hành Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân - văn bản quy phạm pháp luật đầu tiên quy định toàn diện về bảo vệ dữ liệu cá nhân tại Việt Nam (hiện nay đã có Luật Bảo vệ dữ liệu cá nhân 2025) qua đó hoàn thiện hành lang pháp lý bảo vệ quyền riêng tư và an toàn thông tin.

**Thứ ba**, song song với việc hoàn thiện pháp luật, Nhà nước xây dựng các tiêu chuẩn và quy chuẩn kỹ thuật về dữ liệu. Điều 28 Luật Dữ liệu 2024 dành riêng để quy định về tiêu chuẩn, quy chuẩn kỹ thuật trong quản lý dữ liệu. Các tiêu chuẩn này bao gồm chuẩn về hạ tầng hệ thống, định dạng dữ liệu, quy trình đảm bảo chất lượng dữ liệu, an toàn dữ liệu..., nhằm đảm bảo dữ liệu của các cơ quan được thống nhất, đồng bộ, chính xác và an toàn. Chẳng hạn, đã có hướng dẫn về cấu trúc mã định danh và định dạng dữ liệu dùng chung trong cơ quan nhà nước. Việc ban hành tiêu chuẩn giúp các cơ sở dữ liệu và hệ thống thông tin của các bộ, ngành có khả năng kết nối, chia sẻ dễ dàng, tránh tình trạng “cát cứ” dữ liệu cục bộ.

Có thể thấy rằng, nội dung này đóng vai trò là “xương sống”, là nền móng pháp lý và chiến lược cho toàn bộ hệ sinh thái dữ liệu quốc gia. Việc xây dựng một Chiến lược dữ liệu quốc gia không chỉ là một văn bản hành chính mà còn là việc hoạch định chính sách, thể hiện tầm nhìn tương lai, xác định rõ con đường mà nước ta sẽ đi trong cuộc cách mạng số. Song hành với





đó, việc ban hành văn bản quy phạm pháp luật tạo ra một khuôn khổ pháp lý bình đẳng, minh bạch, xác định rõ quyền và nghĩa vụ của nhà nước, doanh nghiệp và người dân. Điều này góp phần tạo dựng niềm tin để người dân sẵn sàng chia sẻ dữ liệu và doanh nghiệp yên tâm đầu tư. Cuối cùng, tiêu chuẩn và quy chuẩn kỹ thuật chính là “ngôn ngữ chung” cho phép các hệ thống khác nhau có thể “nói chuyện” và trao đổi dữ liệu một cách thông suốt, phá vỡ tình trạng “cát cứ dữ liệu” từ đó tối ưu hóa nguồn lực và tạo ra giá trị mới từ dữ liệu.

### ***8.1.1.2. Tuyên truyền, phổ biến chính sách, pháp luật về dữ liệu; hướng dẫn cơ quan quản lý cơ sở dữ liệu, hệ thống thông tin trong xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu***

**Thứ nhất**, tuyên truyền, phổ biến pháp luật về dữ liệu là nội dung quan trọng để đưa các quy định của Nhà nước vào cuộc sống. Điều này bao gồm việc nâng cao nhận thức cho các cơ quan, tổ chức và người dân về giá trị của dữ liệu cũng như các quyền, nghĩa vụ liên quan. Ngay sau khi Luật Dữ liệu được thông qua cuối năm 2024, Bộ Công an (cơ quan đầu mối quản lý nhà nước về dữ liệu) đã xây dựng tài liệu giới thiệu, tuyên truyền về nội dung của luật. Các địa phương cũng tích cực vào cuộc: nhiều tỉnh, thành đã ban hành kế hoạch triển khai thi hành Luật Dữ liệu, trong đó nhấn mạnh công tác tuyên truyền trên các phương tiện thông tin đại chúng và tổ chức tập huấn cho cán bộ phụ trách dữ liệu ở cơ sở.

*Ví dụ*, Ủy ban nhân dân tỉnh Phú Yên (cũ) đã ban hành kế hoạch triển khai Luật Dữ liệu trên địa bàn, yêu cầu tổ chức tuyên truyền sâu rộng Luật Dữ liệu đến các cơ quan, doanh nghiệp và người dân, đồng thời chuẩn bị hạ tầng kỹ thuật cho việc thi hành luật. Tương tự, Bộ Công an đã phổ biến “*Đề cương tuyên truyền Luật Dữ liệu 2024*” để các bộ, ngành, địa phương sử





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

dùng làm tài liệu truyền thông thống nhất. Nhờ các hoạt động này, các quy định về quản lý, chia sẻ, bảo vệ dữ liệu dần được hiểu rõ và ủng hộ, tạo thuận lợi cho việc thực thi luật trên thực tế.



### ***Hội nghị tuyên truyền phổ biến, giáo dục phát luật - Ảnh: HANU***

**Thứ hai,** Nhà nước giữ vai trò hướng dẫn chuyên môn cho các bộ, ngành, địa phương trong quản lý dữ liệu. Điều này có nghĩa là các cơ quan quản lý nhà nước cấp trên (như các bộ chuyên ngành, cơ quan đầu mối) sẽ ban hành văn bản hướng dẫn, tiêu chí, quy trình để giúp các đơn vị xây dựng và vận hành cơ sở dữ liệu (CSDL) và hệ thống thông tin một cách hiệu quả, đúng pháp luật.

Chẳng hạn, Bộ Thông tin và Truyền thông (cũ) đã ban hành Khung Kiến trúc Chính phủ điện tử Việt Nam (phiên bản 2.0) trong đó có hướng dẫn về tích hợp, chia sẻ dữ liệu giữa các hệ thống thông tin quốc gia và cấp tỉnh, giúp các địa phương xây dựng CSDL đồng bộ, liên thông. Bộ Công an và Bộ Nội vụ cũng đã có các thông tư hướng dẫn về quản lý CSDL chuyên





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

ngành (như CSDL quốc gia về dân cư, CSDL cán bộ, công chức, viên chức...), trong đó quy định cụ thể về quy trình thu thập, cập nhật, khai thác dữ liệu để bảo đảm tính chính xác, đầy đủ và kịp thời.



***Tập huấn công tác đảm bảo an toàn, an ninh mạng và bảo vệ  
dữ liệu cá nhân - Ảnh: Trang thông tin điện tử Công an tỉnh Sơn La***

**Thứ ba**, đối với công tác bảo vệ và quản trị dữ liệu, các cơ quan chuyên trách cũng ban hành hướng dẫn nhằm nâng cao năng lực cho các đơn vị cơ sở. Ví dụ, Bộ Công an định kỳ tổ chức tập huấn về an ninh mạng và an toàn thông tin cho cán bộ quản trị hệ thống dữ liệu tại các bộ, ngành, địa phương, nhằm hướng dẫn cách phòng chống tấn công mạng, sao lưu dữ liệu và xử lý sự cố. Những hướng dẫn này giúp chuẩn hóa hoạt động quản trị dữ liệu trên toàn quốc, bảo đảm mọi cơ quan hiểu và thực hiện đúng các quy định kỹ thuật và pháp lý trong vận hành dữ liệu.

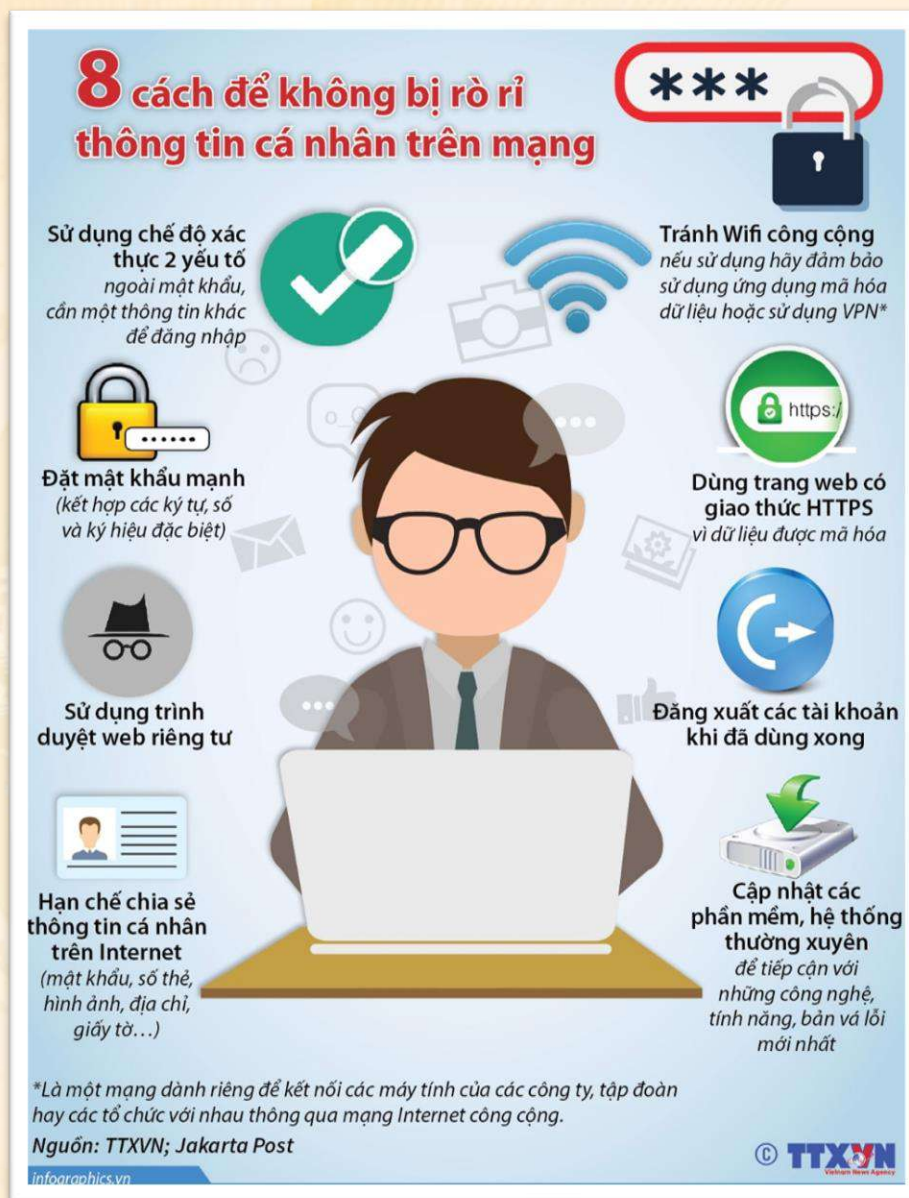
Nhìn chung, một chính sách dù tốt đến đâu cũng sẽ thất bại nếu không được thấu hiểu và thực thi đúng đắn. Tuyên truyền, phổ biến không chỉ là thông báo, mà là một quá trình thay đổi nhận thức sâu sắc trong toàn xã hội,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

đặc biệt là trong bộ máy hệ thống chính trị, đó là cần chuyển đổi tư duy từ việc xem dữ liệu là gánh nặng hành chính sang coi nó là một tài sản chiến lược cần được khai thác.



Quan trọng hơn, việc hướng dẫn chuyên môn đóng vai trò là cầu nối giữa chính sách vĩ mô và thực hiện vi mô. Nhiều cơ quan, địa phương có thể còn lúng túng về mặt kỹ thuật, thiếu nhân lực và kinh nghiệm để quản trị dữ liệu hiệu quả. Sự hướng dẫn từ cơ quan quản lý nhà nước sẽ đảm bảo việc





triển khai được đồng bộ, đúng chuẩn, tránh tình trạng “mạnh ai nấy làm” gây lãng phí nguồn lực và tạo ra các rủi ro về an ninh, an toàn thông tin. Đây là nhiệm vụ bảo đảm chiến lược quốc gia được lan tỏa và bén rễ sâu rộng trong thực tế.

### ***8.1.1.3. Quản lý, giám sát các hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu, bảo đảm an ninh, an toàn dữ liệu***

Trong bối cảnh các mối đe dọa an ninh mạng ngày càng tinh vi và nguy hiểm, việc bảo đảm an ninh, an toàn dữ liệu không còn là một lựa chọn mà là một yêu cầu bắt buộc. Bất kỳ sự cố rò rỉ, mất mát dữ liệu nào, đặc biệt là dữ liệu cá nhân của công dân hay dữ liệu cốt lõi, dữ liệu quan trọng của Nhà nước đều có thể gây ra những hậu quả khôn lường và kinh tế, xã hội và thậm chí là an ninh quốc gia, trật tự an toàn xã hội. Vì vậy, để dữ liệu được sử dụng hiệu quả và không bị lạm dụng, Nhà nước phải quản lý, giám sát chặt chẽ các hoạt động xây dựng, phát triển, khai thác, sử dụng dữ liệu; đồng thời đảm bảo an ninh, an toàn cho dữ liệu. Nội dung này đòi hỏi sự tham gia tích cực của các cơ quan quản lý chuyên ngành về an toàn thông tin và an ninh mạng.

**Thứ nhất**, việc giám sát thể hiện ở chỗ nhà nước thiết lập các quy định và cơ chế kiểm soát đối với hoạt động dữ liệu. Hoạt động quản lý giám sát phải được thực hiện một cách chủ động, liên tục thay, thay vì chỉ phản ứng khi có sự cố xảy ra. Điều này đòi hỏi phải có các trung tâm giám sát hiện đại, bộ phận phản ứng nhanh và một cơ chế theo dõi chặt chẽ việc tuân thủ các quy định về an toàn thông tin của mọi tổ chức, cá nhân. Chỉ khi người dân và doanh nghiệp tin rằng dữ liệu của mình được bảo vệ một cách nghiêm ngặt thì mới sẵn lòng tham gia vào các hoạt động của Chính phủ số và kinh tế số.

Luật Dữ liệu 2024 quy định các nguyên tắc và hành vi bị nghiêm cấm, ví dụ: nghiêm cấm giả mạo, làm sai lệch, phá hoại dữ liệu trong CSDL của





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

cơ quan nhà nước hoặc cố ý không cung cấp dữ liệu theo quy định. Các hành vi xâm phạm dữ liệu quan trọng có thể bị xử lý hình sự hoặc xử phạt hành chính tùy theo mức độ. Bên cạnh đó, các tổ chức cung cấp dịch vụ về dữ liệu (như các nền tảng trung gian phân tích dữ liệu, sàn giao dịch dữ liệu) phải tuân thủ pháp luật về an toàn thông tin mạng, an ninh mạng và có trách nhiệm giám sát, ngăn chặn rủi ro, hành vi vi phạm trên nền tảng của mình.



Từ góc nhìn của một doanh nghiệp công nghệ, tôi cho rằng mô hình “nhà nước kiến tạo - tư nhân đồng hành” sẽ phù hợp để hướng tới mục tiêu trên. Theo đó, Nhà nước đóng vai trò dẫn dắt đường lối, ban hành tiêu chuẩn, giám sát pháp lý và bảo vệ quyền lợi; trong khi doanh nghiệp công nghệ nội địa cung cấp nền tảng kỹ thuật, hệ thống phân tích và cơ chế vận hành chuyên môn hóa.

### **Bà MAI THỊ THANH OANH**

Phó Tổng giám đốc,  
Công ty TNHH Cốc Cốc

**Ảnh: VnEconomy**

**Thứ hai**, về an ninh, an toàn dữ liệu, Nhà nước ban hành nhiều chính sách để bảo vệ dữ liệu ở các cấp độ. Luật An ninh mạng 2018 và các văn bản dưới luật yêu cầu bảo vệ hệ thống thông tin quan trọng, ngăn chặn tấn công mạng, đánh cắp dữ liệu. Gần đây, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân đặt ra yêu cầu rất cao về bảo mật thông tin cá nhân, áp dụng cho mọi tổ chức, cá nhân xử lý dữ liệu cá nhân tại Việt Nam. Nghị định này coi dữ liệu cá nhân là tài sản số quan trọng, yêu cầu các doanh nghiệp phải có chính sách bảo vệ dữ liệu minh bạch và có thể bị phạt hàng trăm triệu đồng





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

nếu vi phạm, chẳng hạn như không thông báo về xử lý dữ liệu hay không đánh giá tác động đến dữ liệu cá nhân. Đặc biệt, mọi hình thức mua bán dữ liệu cá nhân đều bị nghiêm cấm, thể hiện quyết tâm của Nhà nước trong việc ngăn chặn tình trạng mua bán dữ liệu trái phép.

**Thứ ba,** Nhà nước cũng thiết lập các cơ chế giám sát thường xuyên. Bộ Công an với vai trò cơ quan đầu mối sẽ phối hợp với các cơ quan liên quan kiểm tra định kỳ việc đảm bảo an toàn dữ liệu tại các bộ, ngành, địa phương. Các hệ thống giám sát an toàn không gian mạng quốc gia cũng được triển khai để phát hiện sớm và cảnh báo các nguy cơ đối với các cơ sở dữ liệu lớn. Nhờ đó, hoạt động về dữ liệu được giám sát toàn diện, giảm thiểu rủi ro mất mát, lộ lọt thông tin.



***Tam giác bảo mật CIA Triad - Ảnh: IDStrong***

Có thể thấy rằng, hoạt động quản lý và giám sát là tiền đề để tiến tới bảo đảm an ninh dữ liệu. Có thể nói an ninh dữ liệu là quá trình bảo vệ dữ liệu số khỏi sự truy cập trái phép, sử dụng sai mục đích, phá hủy hoặc thay đổi không mong muốn; trong đó, bảo đảm ba nguyên tắc cốt lõi là *tính bảo*





*mật (Confidentiality), tính toàn vẹn (Integrity) và tính sẵn sàng (Availability). An ninh dữ liệu không chỉ là các biện pháp kỹ thuật như mã hóa, tường lửa hay là kiểm soát truy cập mà còn bao gồm các chính sách, quy trình và ý thức của người dân nhằm bảo đảm dữ liệu được an toàn trong suốt vòng đời của nó, từ khi tạo ra, lưu trữ, truyền tải cho đến khi hủy bỏ. Việc thực thi an ninh dữ liệu hiệu quả giúp bảo vệ vững chắc an ninh quốc gia, đề cao tinh thần thượng tôn pháp luật và duy trì lợi thế cạnh tranh của quốc gia trong chuyển đổi số.*

#### ***8.1.1.4. Báo cáo, thống kê về dữ liệu; nghiên cứu, ứng dụng khoa học công nghệ về dữ liệu; sản phẩm, dịch vụ về dữ liệu; quản lý, giám sát, phát triển thị trường dữ liệu***

Nhà nước có trách nhiệm tổ chức báo cáo, thống kê định kỳ về tình hình dữ liệu; đồng thời thúc đẩy nghiên cứu khoa học, ứng dụng công nghệ trong lĩnh vực dữ liệu và phát triển thị trường dữ liệu.

***Thứ nhất***, công tác báo cáo, thống kê về dữ liệu giúp Chính phủ nắm được bức tranh toàn cảnh về tài sản dữ liệu quốc gia. Các bộ, ngành hàng năm sẽ báo cáo lên Chính phủ về hiện trạng các cơ sở dữ liệu (quy mô, mức độ cập nhật, tỷ lệ kết nối chia sẻ) và tình hình khai thác dữ liệu trong quản lý nhà nước. Thông qua đó, Nhà nước có cơ sở để đánh giá hiệu quả chính sách và điều chỉnh kịp thời. Chẳng hạn, báo cáo có thể cho thấy tỷ lệ dịch vụ công sử dụng dữ liệu dùng chung tăng theo từng năm, hay số lượng cơ sở dữ liệu quốc gia đã hoàn thành kết nối liên thông. Việc thống kê cũng giúp nhận diện các khó khăn vướng mắc (như thiếu nhân lực dữ liệu, hạ tầng chưa đồng bộ) để có giải pháp hỗ trợ. Nội dung này thể hiện một tầm nhìn kinh tế rất rõ ràng, xem dữ liệu là “*động cơ tăng trưởng*” mới. Hoạt động báo cáo, thống kê là cơ sở để đo lường, đánh giá hiệu quả của chính sách, giúp các nhà quản





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

lý đưa ra các quyết định dựa trên bằng chứng thay vì cảm tính. Việc thúc đẩy nghiên cứu, ứng dụng khoa học công nghệ như AI, Big Data là chìa khóa để “mở khóa” những giá trị tiềm ẩn trong các kho dữ liệu khổng lồ, tạo ra những đột phá trong y tế giao thông, nông nghiệp,...

**Thứ hai**, Nhà nước khuyến khích nghiên cứu và ứng dụng khoa học - công nghệ về dữ liệu. Điều này thể hiện qua việc đầu tư cho các chương trình nghiên cứu phát triển công nghệ dữ liệu lớn (Big Data), trí tuệ nhân tạo (AI), học máy (ML), nhằm phục vụ việc phân tích, khai thác dữ liệu hiệu quả hơn. Các trường đại học, viện nghiên cứu được khuyến khích tham gia đề tài về quản trị dữ liệu, bảo mật dữ liệu. Chính phủ cũng thúc đẩy ứng dụng công nghệ mới trong quản lý dữ liệu nhà nước như sử dụng công nghệ blockchain để đảm bảo tính toàn vẹn dữ liệu, hay ứng dụng AI để tự động phân loại và làm sạch dữ liệu. Những ứng dụng này giúp nâng cao chất lượng và giá trị của dữ liệu được thu thập, đồng thời tạo ra sản phẩm, dịch vụ dữ liệu mới phục vụ người dân và doanh nghiệp. Theo Luật Dữ liệu, phát triển sản phẩm, dịch vụ về dữ liệu (như dịch vụ phân tích dữ liệu, dịch vụ lưu trữ đám mây, dịch vụ tư vấn dữ liệu) cũng là một nội dung quản lý nhà nước. Do đó, Nhà nước sẽ xây dựng cơ chế để các dịch vụ này được quản lý chặt chẽ nhưng vẫn khuyến khích sáng tạo.

Đặc biệt, *phát triển thị trường dữ liệu* là điểm mới đáng chú ý. Luật Dữ liệu 2024 lần đầu tiên đề cập đến việc hình thành sàn dữ liệu tại Việt Nam. Theo Điều 42 Luật Dữ liệu, *sàn dữ liệu* được định nghĩa là nền tảng cung cấp tài nguyên dữ liệu để phục vụ nghiên cứu, đổi mới sáng tạo, cung cấp sản phẩm dịch vụ dữ liệu cho phát triển kinh tế - xã hội, đồng thời là môi trường để giao dịch, trao đổi dữ liệu một cách hợp pháp. Nhà nước quản lý chặt chẽ loại hình thị trường mới mẻ này: chỉ các đơn vị sự nghiệp công lập





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

hoặc doanh nghiệp nhà nước đủ điều kiện mới được phép cung cấp dịch vụ sản dữ liệu. Những dữ liệu thuộc danh mục cấm (như dữ liệu ảnh hưởng đến an ninh quốc gia, dữ liệu cá nhân nhạy cảm chưa được đồng ý) sẽ không được phép giao dịch trên sàn. Như vậy, Nhà nước vừa tạo cơ hội cho dữ liệu trở thành hàng hóa trao đổi hợp pháp, vừa bảo vệ lợi ích công và quyền riêng tư trong thị trường dữ liệu.



### ***Thị trường dữ liệu đang dần được “mở cửa” tại Việt Nam***

Song song, Chiến lược dữ liệu quốc gia cũng đặt mục tiêu “đưa dữ liệu trở thành một loại tài sản được pháp luật bảo vệ và tạo lập thị trường dữ liệu”, cho thấy định hướng rõ ràng của Việt Nam trong việc phát triển thị trường giao dịch dữ liệu minh bạch, an toàn. Một thị trường dữ liệu sôi động, nơi dữ liệu (sau khi được ẩn danh và bảo đảm tuân thủ quy định pháp luật) có thể được chia sẻ, mua bán sẽ tạo ra một ngành công nghiệp hoàn toàn mới, thúc đẩy đổi mới sáng tạo trong doanh nghiệp và tạo ra một số việc làm chất lượng cao; tuy nhiên, thách thức lớn nhất là xây dựng được một cơ chế quản lý cân bằng giữa việc thúc đẩy thị trường và bảo vệ quyền riêng tư, an ninh dữ liệu.





## **8.1.1.5. Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về dữ liệu**

Hoạt động này chính là “*thanh gươm công lý*” bảo đảm tính thực thi, tính nghiêm minh của pháp luật về dữ liệu. Mỗi chiến lược, quy định pháp luật sẽ chỉ mang tính hình thức nếu không có một cơ chế, chế tài đủ mạnh để đảm bảo thi hành hiệu quả. Hoạt động thanh tra, kiểm tra không chỉ nhằm phát hiện sai phạm mà còn có tác dụng răn đe, phòng ngừa, buộc các tổ chức, cá nhân phải có ý thức tuân thủ ngay từ đầu; quy định này đã tạo ra một thông điệp rõ ràng là vi phạm các quy định về dữ liệu sẽ phải đối mặt với những chế tài xử lý của Nhà nước. Nội dung này nhấn mạnh vai trò cưỡng chế thi hành pháp luật, đảm bảo tính “*thượng tôn pháp luật*” trong quản trị dữ liệu.

Cơ quan thanh tra chuyên ngành (như Thanh tra Bộ Công an) sẽ được giao nhiệm vụ kiểm tra việc chấp hành các quy định về xây dựng, kết nối, chia sẻ dữ liệu tại các bộ, ngành, doanh nghiệp. Thanh tra có thể kiểm tra một doanh nghiệp cung cấp dịch vụ dữ liệu xem họ có tuân thủ quy định về bảo mật thông tin khách hàng hay không; hoặc kiểm tra một địa phương trong việc vận hành CSDL dân cư xem đã bảo đảm an toàn, đúng quy trình chưa. Nếu phát hiện vi phạm, các cơ quan này có quyền xử phạt hành chính theo quy định (cảnh cáo, phạt tiền, tịch thu tang vật, đình chỉ hoạt động liên quan đến dữ liệu...). Hiện nay, chế tài xử phạt vi phạm về dữ liệu nằm rải rác ở nhiều văn bản (ví dụ: vi phạm bảo vệ dữ liệu cá nhân bị phạt đến 80 triệu đồng theo Nghị định 13/2023/NĐ-CP; vi phạm về cung cấp, sử dụng thông tin trên mạng bị phạt theo Nghị định 15/2020/NĐ-CP...). Dự kiến, để thi hành Luật Dữ liệu 2024, Chính phủ sẽ ban hành nghị định xử phạt vi phạm hành chính riêng trong lĩnh vực dữ liệu nhằm hợp nhất và bổ sung các chế tài đủ sức răn đe, trước mắt là Nghị định số 190/2025/NĐ-CP ngày





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

01/7/2025 của Chính phủ, có nội dung bổ sung quy định về xử lý vi phạm hành chính trên môi trường điện tử.



### ***Dữ liệu cá nhân đang phải đối mặt với nhiều nguy cơ - Ảnh: VnEconomy***

Song song, người dân và tổ chức có quyền khiếu nại, tố cáo nếu phát hiện cơ quan hay cá nhân vi phạm pháp luật về dữ liệu (chẳng hạn làm lộ dữ liệu cá nhân, lạm dụng dữ liệu vì mục đích không phép). Việc giải quyết khiếu nại, tố cáo là cơ chế bảo vệ quyền lợi hợp pháp cho người dân và doanh nghiệp. Khi một cá nhân phát hiện dữ liệu của mình bị lạm dụng, hoặc một công ty đối thủ cạnh tranh không lành mạnh bằng dữ liệu, họ phải có một địa chỉ tin cậy để tìm đến sự bảo vệ. Việc xử lý nghiêm minh các hành vi vi phạm sẽ củng cố niềm tin vào pháp luật, tạo ra một môi trường số công bằng và an toàn, nơi quyền về dữ liệu của mỗi thực thể được tôn trọng và bảo vệ một cách hiệu quả. Các cơ quan nhà nước có trách nhiệm giải quyết những khiếu nại, tố cáo này một cách khách quan, đúng luật. Thực tế, thời gian qua





đã có những vụ việc người dùng khiếu nại về việc thông tin cá nhân bị rò rỉ hoặc bị công ty thu thập trái phép; các cơ quan quản lý đã tiếp nhận và xử lý nghiêm, tạo niềm tin cho công chúng. Quá trình thanh tra, giải quyết khiếu nại, tố cáo không chỉ nhằm trừng trị vi phạm mà còn giúp phát hiện những bất cập trong chính sách để Nhà nước điều chỉnh cho phù hợp.

### **8.1.1.6. Đào tạo, bồi dưỡng, phát triển nguồn nhân lực và hợp tác quốc tế về dữ liệu**

Cuối cùng nhưng không kém phần quan trọng, quản lý nhà nước về dữ liệu bao gồm việc đào tạo, bồi dưỡng nguồn nhân lực chuyên trách về dữ liệu và đẩy mạnh hợp tác quốc tế trong lĩnh vực này. Nhân lực và hợp tác quốc tế là hai yếu tố hỗ trợ để các nội dung quản lý dữ liệu nêu trên được thực thi hiệu quả và bắt kịp xu hướng thế giới.

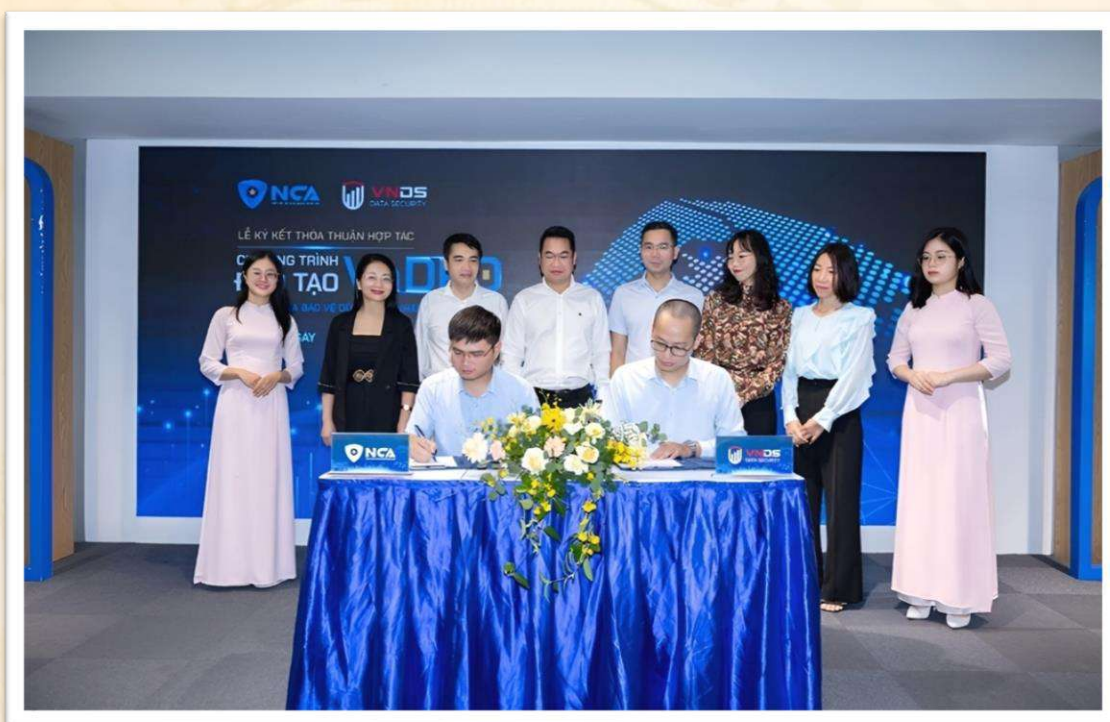
**Thứ nhất**, về đào tạo nguồn nhân lực, Nhà nước chú trọng phát triển đội ngũ cán bộ có kiến thức và kỹ năng về quản trị dữ liệu. Đây là nhiệm vụ có tầm nhìn xa nhất, đầu tư vào yếu tố quyết định sự thành bại của mọi chiến lược là con người và sự hội nhập. Công nghệ có thể mua, chiến lược có thể tham khảo kinh nghiệm quốc tế, nhưng nguồn nhân lực chất lượng cao phải do chính chúng ta đào tạo. Một quốc gia không thể khai thác được “mỏ vàng” dữ liệu nếu thiếu đi những “người thợ mỏ” lành nghề, đó là các nhà khoa học dữ liệu, kỹ sư dữ liệu, chuyên gia phân tích và cả những nhà quản lý am hiểu về dữ liệu. Do đó, đầu tư vào đào tạo, bồi dưỡng là đầu tư cho tương lai bền vững, tạo ra năng lực cạnh tranh cốt lõi của mỗi quốc gia trong dài hạn. Các chương trình đào tạo, bồi dưỡng về *khoa học dữ liệu, phân tích dữ liệu, an toàn thông tin* được tổ chức cho cán bộ công chức trong bộ máy nhà nước. Nhiều bộ, ngành đã cử cán bộ đi học các khóa nâng cao về quản lý dữ liệu hoặc hợp tác với các trường đại học để mở lớp chuyên sâu. Chẳng





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

hạn, Bộ Khoa học và Công nghệ phối hợp với một số trường đại học chuyên đào tạo về lĩnh vực công nghệ để đào tạo chuyên gia phân tích dữ liệu phục vụ cho Chính phủ số. Bên cạnh đó, trong khuôn khổ Đề án phát triển nguồn nhân lực chuyển đổi số, Chính phủ cũng yêu cầu lồng ghép nội dung quản lý và khai thác dữ liệu vào chương trình bồi dưỡng cán bộ các cấp, nhằm tạo ra một lớp cán bộ am hiểu về dữ liệu ở mọi ngành, lĩnh vực.



***Hiệp hội An ninh mạng Quốc gia và Công ty An ninh Dữ liệu Việt Nam (VNDS) ký kết phối hợp đào tạo chuyên gia DPO - Ảnh: vov.vn***

**Thứ hai**, về hợp tác quốc tế, Việt Nam tích cực tham gia các sáng kiến và tuân thủ các thông lệ quốc tế về dữ liệu. Hợp tác quốc tế trong lĩnh vực dữ liệu là xu thế tất yếu, Điều 7 Luật Dữ liệu nêu rõ hợp tác quốc tế về dữ liệu phải tuân thủ điều ước quốc tế mà Việt Nam là thành viên, trên nguyên tắc bình đẳng và cùng có lợi. Nội dung hợp tác quốc tế rất đa dạng, bao gồm: đào tạo nhân lực với nước ngoài, hợp tác nghiên cứu khoa học về dữ liệu,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

chuyển giao công nghệ tiên tiến (đặc biệt là công nghệ hạ tầng dữ liệu, bảo mật), thu hút đầu tư phát triển các trung tâm dữ liệu tại Việt Nam và tham gia xây dựng các quy tắc, tiêu chuẩn quốc tế về dữ liệu. Ví dụ, Việt Nam đã cử chuyên gia tham gia các diễn đàn quốc tế về dữ liệu mở và dữ liệu lớn; hợp tác với Liên minh châu Âu trong Dự án “EVFTA - Hỗ trợ pháp lý về bảo vệ dữ liệu” để học hỏi kinh nghiệm bảo vệ dữ liệu cá nhân theo tiêu chuẩn GDPR. Trong ASEAN, Việt Nam cũng đóng góp vào việc xây dựng Khung quản trị dữ liệu số ASEAN, hướng tới chia sẻ dữ liệu xuyên biên giới một cách hài hòa. Những hoạt động này giúp Việt Nam cập nhật xu hướng quản lý dữ liệu tiên tiến, đồng thời quảng bá chính sách dữ liệu quốc gia, thu hút các nguồn lực quốc tế.



***Tăng cường hợp tác Việt Nam - Nhật Bản trong đổi mới công nghệ, chuyển đổi số và đa dạng hóa chuỗi cung ứng - Ảnh: Bộ Công Thương Việt Nam***





Có thể thấy rằng, việc hợp tác quốc tế giúp nước ta học hỏi kinh nghiệm thành công và cả thất bại từ các nước đi trước, tiếp cận các công nghệ tiên tiến. Quan trọng hơn, nó giúp chúng ta hài hòa hóa các quy định của mình với chuẩn mực chung của thế giới, tạo điều kiện thuận lợi cho thương mại điện tử, thu hút đầu tư nước ngoài và nâng cao vị thế, tiếng nói của nước ta trên trường quốc tế trong việc định hình thị trường toàn cầu về dữ liệu.

Tóm lại, quản lý nhà nước về dữ liệu ở Việt Nam hiện nay là một lĩnh vực rộng và phức tạp, bao quát từ tầm hoạch định chiến lược đến triển khai kỹ thuật, pháp lý, cũng như giám sát thực thi. Luật Dữ liệu 2024 và các văn bản liên quan đã xác định rõ *06 nhóm nội dung* quản lý chủ yếu, tạo thành một chu trình toàn diện để dữ liệu được quản trị hiệu quả, an toàn và phát huy giá trị trong phát triển kinh tế, xã hội. Trong bối cảnh chuyển đổi số mạnh mẽ, việc thực hiện đồng bộ các nội dung này sẽ giúp Việt Nam xây dựng được nền kinh tế dữ liệu vững chắc, khai thác nguồn “*dầu mỏ số*” một cách bền vững, đồng thời bảo vệ chủ quyền dữ liệu quốc gia và quyền lợi của người dân. Các thách thức vẫn còn, như hoàn thiện khung pháp lý thứ cấp, nâng cao năng lực thực thi tại địa phương, nhưng với quyết tâm của Nhà nước thể hiện qua Chiến lược Dữ liệu Quốc gia và Luật Dữ liệu, Việt Nam đang từng bước tiến tới mục tiêu trở thành quốc gia số an toàn, thịnh vượng dựa trên nền tảng dữ liệu.

### **8.1.2. Ý nghĩa của việc quy định nội dung quản lý nhà nước về dữ liệu**

Việc Luật Dữ liệu năm 2024 xác định rõ nội dung quản lý nhà nước về dữ liệu có ý nghĩa đặc biệt quan trọng và mang tính thiết thực trên nhiều phương diện trong bối cảnh chuyển đổi số hiện nay.

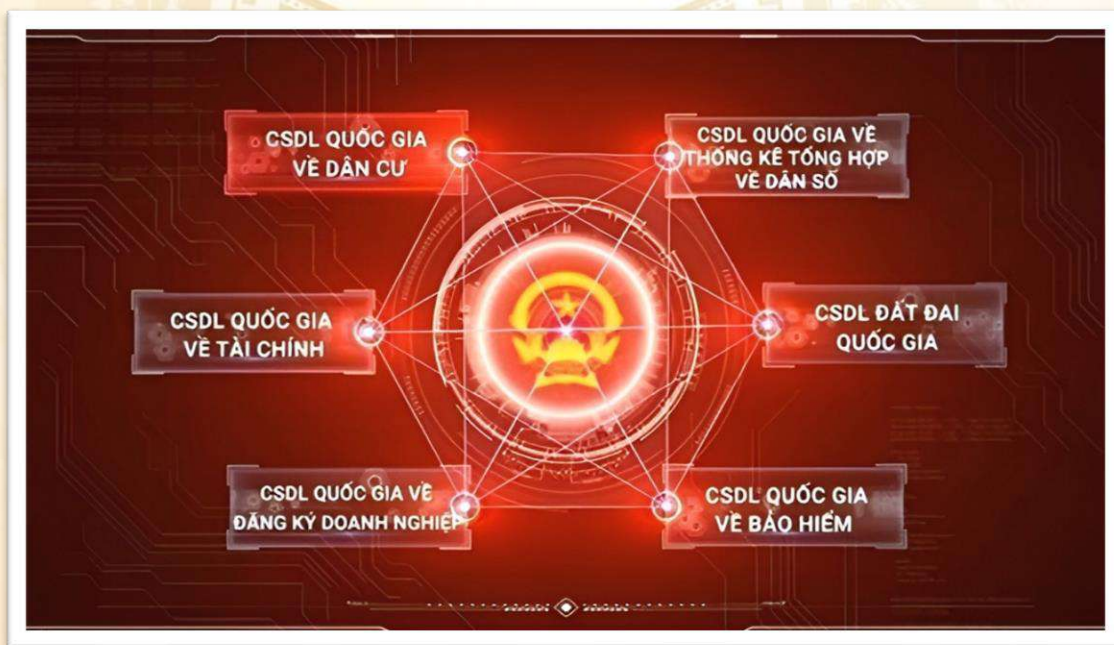
**Một là**, quy định này xác lập rõ vai trò lãnh đạo, điều hành của Nhà nước trong xây dựng hệ sinh thái dữ liệu quốc gia *an toàn, đồng bộ, hiệu quả*, bảo đảm sự thống nhất trong phát triển và sử dụng dữ liệu giữa mọi





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

ngành, mọi cấp. Điều này khắc phục tình trạng phân tán, cát cứ dữ liệu trước đây: nhiều bộ ngành từng triển khai cơ sở dữ liệu riêng lẻ với hạ tầng chưa đồng bộ, trùng lặp dữ liệu và thiếu tiêu chuẩn kỹ thuật chung, gây khó khăn cho kết nối, chia sẻ thông tin và tiềm ẩn rủi ro về an ninh. Việc pháp luật hóa nội dung quản lý nhà nước giúp thiết lập một khuôn khổ tập trung, qua đó hợp nhất các hệ thống dữ liệu hiện có và định hướng phát triển Cơ sở dữ liệu tổng hợp quốc gia như trụ cột dữ liệu chung. Đây là nền tảng cho Chính phủ điện tử, tạo điều kiện tích hợp dữ liệu liên ngành thông suốt, tránh trùng lặp, tiết kiệm chi phí và nâng cao hiệu quả khai thác dữ liệu trong quản lý nhà nước. Nhờ vậy, Nhà nước có thể phối hợp đồng bộ các nguồn lực thông tin, xây dựng các hệ thống dữ liệu *tin cậy, ổn định*, sẵn sàng cho những ứng dụng phân tích chuyên sâu nhằm tạo ra các *giá trị mới và sản phẩm, dịch vụ* dữ liệu mới cho xã hội trong giai đoạn chuyển đổi số.



***Hoàn thiện hệ sinh thái phục vụ kết nối, khai thác, bổ sung làm giàu dữ liệu dân cư là một trong 5 nhóm tiện ích của Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 - Ảnh: VGP***





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

**Hai là**, Luật Dữ liệu 2024 đã thiết lập cơ sở pháp lý đầy đủ để Nhà nước giám sát và quản lý mọi hoạt động về dữ liệu trong xã hội. Thông qua việc tổ chức tuyên truyền, hướng dẫn cũng như kiểm tra, thanh tra và giám sát toàn bộ quá trình thu thập, xử lý, sử dụng dữ liệu, nhận thức pháp luật của các tổ chức, cá nhân về dữ liệu được nâng cao, góp phần bảo đảm mọi chủ thể tuân thủ đúng quy định. Nhà nước có thể chủ động phòng ngừa và ngăn chặn các hành vi vi phạm (như đánh cắp, mua bán dữ liệu trái phép, sử dụng dữ liệu sai mục đích) ngay từ sớm, qua đó tăng cường an ninh dữ liệu, an toàn thông tin và bảo vệ *lợi ích quốc gia* trong kỷ nguyên số.



***Quyền và lợi ích của người dân trong môi trường số vừa là động lực vừa là mục tiêu thúc đẩy Việt Nam nâng cao năng lực quản trị số - Ảnh: Internet***

Có thể nói, Điều 8 Luật Dữ liệu với nội dung quản lý nhà nước về dữ liệu không chỉ đơn thuần là một danh mục trách nhiệm, mà còn là công cụ pháp lý quan trọng giúp Nhà nước điều tiết thực tiễn hiệu quả. Đây là nền





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

tăng để xử lý nghiêm các vi phạm, tránh tình trạng khoảng trống pháp lý trước đây khi chưa có luật thống nhất về dữ liệu, đảm bảo mỗi cơ quan, doanh nghiệp khi tham gia vào hoạt động dữ liệu đều chịu sự quản lý và chế tài rõ ràng. Nhờ khung pháp lý này, Việt Nam có thể nâng cao năng lực quản trị quốc gia trong thời đại số hóa mạnh mẽ, khi dữ liệu trở thành nhân tố cốt lõi của quản lý và phát triển. Bên cạnh đó, luật cũng gián tiếp bảo vệ quyền và lợi ích của người dân trong môi trường số: Nhà nước có thẩm quyền yêu cầu cung cấp dữ liệu vì mục đích công cộng trong những trường hợp cần thiết, đồng thời thắt chặt quản lý cả “*dữ liệu cá nhân*” lẫn “*dữ liệu phi cá nhân*” nhằm ngăn chặn lạm dụng, bảo đảm quyền riêng tư và an ninh thông tin cho cộng đồng.

**Ba là**, việc quy định rõ nội dung quản lý nhà nước còn phân định minh bạch vai trò, trách nhiệm của từng cấp, từng ngành trong công tác quản lý dữ liệu, từ trung ương đến địa phương. Luật đã giao Chính phủ thống nhất quản lý, Bộ Công an là cơ quan đầu mối chịu trách nhiệm chính về dữ liệu quốc gia (trừ lĩnh vực quốc phòng), các bộ ngành khác phối hợp với Bộ Công an, và Ủy ban nhân dân cấp tỉnh quản lý dữ liệu tại địa phương. Cách phân công, phân cấp này phản ánh tầm nhìn chính trị: Nhà nước coi dữ liệu là lĩnh vực cần sự chỉ đạo tập trung, tương tự như bảo đảm quốc phòng - an ninh. Quản lý nhà nước về dữ liệu được đặt dưới sự điều hành thống nhất sẽ tránh tình trạng chồng chéo trách nhiệm, đồng thời tạo ra cơ chế liên kết liên ngành chặt chẽ. Mỗi bộ, ngành và địa phương vừa xây dựng, phát triển cơ sở dữ liệu thuộc phạm vi mình, vừa tuân theo chuẩn mực chung và phối hợp với cơ quan trung ương, đảm bảo “*dữ liệu thông chạy, quản lý thông suốt*” trên toàn hệ thống. Điều này đặc biệt quan trọng để phát huy tối đa nguồn lực dữ liệu sẵn có, đẩy mạnh chia sẻ dữ liệu dùng chung và nâng cao tính liên thông





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

giữa các hệ thống thông tin. Hệ quả trực tiếp là thúc đẩy quá trình chuyển đổi số quốc gia theo đúng định hướng chiến lược đã đề ra.

Dữ liệu trước đây phân tán nay được kết nối, cho phép triển khai các “dịch vụ số liên thông” và “quy trình ra quyết định” dựa trên dữ liệu ở tầm vĩ mô. Như Luật nhân mạnh, tăng cường phối hợp quản lý dữ liệu sẽ góp phần xây dựng thành công Chính phủ số, kinh tế số và xã hội số ở Việt Nam. Điều này hoàn toàn phù hợp với các nghị quyết của Đảng và Nhà nước về chuyển đổi số toàn diện, giúp hiện thực hóa mục tiêu cải cách hành chính và cung cấp dịch vụ công trực tuyến hiệu quả. Trên thực tế, thời gian qua, việc kết nối một số Cơ sở dữ liệu quốc gia như Cơ sở dữ liệu quốc gia về dân cư với các bộ, ngành đã cho thấy lợi ích to lớn: quy trình xác thực, chia sẻ thông tin công dân trở nên nhanh chóng, minh bạch, giảm bớt giấy tờ và tiết kiệm thời gian cho người dân và doanh nghiệp. Với khuôn khổ pháp lý mới, các sáng kiến tương tự sẽ được nhân rộng, từ đó cải thiện đáng kể chất lượng dịch vụ công và năng lực quản lý xã hội dựa trên dữ liệu.

**Bốn là,** Luật Dữ liệu 2024 khẳng định dữ liệu là một tài nguyên quan trọng của quốc gia, cần được quản lý, khai thác để tạo ra giá trị kinh tế. Nhà nước có chính sách huy động mọi nguồn lực nhằm làm giàu dữ liệu, phát triển dữ liệu trở thành tài sản. Điều này nhấn mạnh khía cạnh kinh tế của quản lý dữ liệu: dưới sự điều phối của Nhà nước, dữ liệu không còn là nguồn lực tiềm tàng bị phân mảnh, mà trở thành yếu tố sản xuất thiết yếu trong nền kinh tế số. Việc luật hóa nội dung quản lý nhà nước về dữ liệu sẽ tạo môi trường thuận lợi để phát triển thị trường dữ liệu tại Việt Nam. Cụ thể, các quy định về sản phẩm, dịch vụ dữ liệu giúp hình thành khung pháp lý cho những lĩnh vực kinh doanh mới mẻ này, vốn trước đây chưa được luật khác đề cập đầy đủ.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Nhà nước thống nhất quản lý nhưng đồng thời khuyến khích, tạo điều kiện cho khu vực tư nhân đầu tư, sáng tạo trong lĩnh vực dữ liệu từ xây dựng các trung tâm lưu trữ, xử lý dữ liệu đặt tại Việt Nam cho đến phát triển các sản phẩm, dịch vụ đổi mới sáng tạo dựa trên dữ liệu. Điều đó sẽ thu hút nguồn lực xã hội vào công cuộc chuyển đổi số, thúc đẩy hình thành hệ sinh thái doanh nghiệp dữ liệu nội địa. Bản thân thị trường dữ liệu được xem là động lực đột phá giúp kích thích chuyển đổi số trong mọi ngành, lĩnh vực và nâng cao năng lực cạnh tranh quốc gia. Chẳng hạn, khi cơ sở pháp lý về chia sẻ và giao dịch dữ liệu rõ ràng, các doanh nghiệp có thể yên tâm hơn trong việc trao đổi dữ liệu (theo đúng chuẩn mực về chất lượng, bảo mật) để tạo ra dịch vụ mới, từ đó trực tiếp đóng góp cho tăng trưởng kinh tế số. Bên cạnh đó, việc Nhà nước quản lý chặt chẽ hoạt động chuyển dữ liệu ra nước ngoài đối với “*dữ liệu cốt lõi, dữ liệu quan trọng*” cũng là một nội dung đáng chú ý. Nó bảo đảm rằng những tài sản dữ liệu quý giá cho kinh tế và an ninh quốc gia không bị thất thoát, sử dụng trái phép ngoài phạm vi lãnh thổ. Tất cả những yếu tố này góp phần định hình một nền kinh tế dữ liệu lành mạnh, có trật tự dưới sự giám sát của Nhà nước, đồng thời mở đường cho sáng tạo và phát triển bền vững.

**Năm là,** ý nghĩa của việc quy định nội dung quản lý nhà nước về dữ liệu còn thể hiện ở tầm nhìn chiến lược trong bối cảnh quốc tế. Việt Nam đã kịp thời ban hành Luật Dữ liệu đầu tiên, tạo nền tảng pháp lý cho kỷ nguyên dữ liệu tương tự cách nhiều quốc gia khác đang làm. Trên thế giới, nhiều nước đã sớm xây dựng luật về dữ liệu để quản trị việc vận hành, khai thác dữ liệu trong cả khu vực công lẫn tư: Hàn Quốc có Luật Dữ liệu mở, Liên minh Châu Âu có Đạo Luật Quản trị dữ liệu và Đạo luật Dữ liệu chung áp dụng cho 27 nước thành viên... Những đạo luật này đều nhằm tạo cơ chế,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

chính sách thúc đẩy ứng dụng dữ liệu vào quản lý nhà nước và phát triển kinh tế - xã hội, đồng thời bảo vệ quyền lợi người dân.



***Ảnh dựng khu trung tâm dữ liệu 140 MW  
của Viettel tại Tân Phú Trung - Ảnh: Viettel***

Việt Nam với Luật Dữ liệu 2024 đã chính thức tham gia vào xu thế đó, khẳng định cam kết của Nhà nước trong việc quản lý và phát triển tài nguyên dữ liệu một cách bài bản. Đặc biệt, trong bối cảnh các cường quốc công nghệ coi trọng “*chủ quyền dữ liệu*”, luật của ta cũng nhấn mạnh yếu tố an ninh quốc gia và chủ quyền số. Chẳng hạn, Trung Quốc ban hành Luật An toàn dữ liệu năm 2021 và xác định dữ liệu là tài nguyên mang tính chiến lược, việc bảo vệ an toàn dữ liệu thông qua luật pháp được xem là yếu tố then chốt để giữ vững lợi ích cốt lõi quốc gia trong kỷ nguyên số<sup>52</sup>. Tinh thần tương

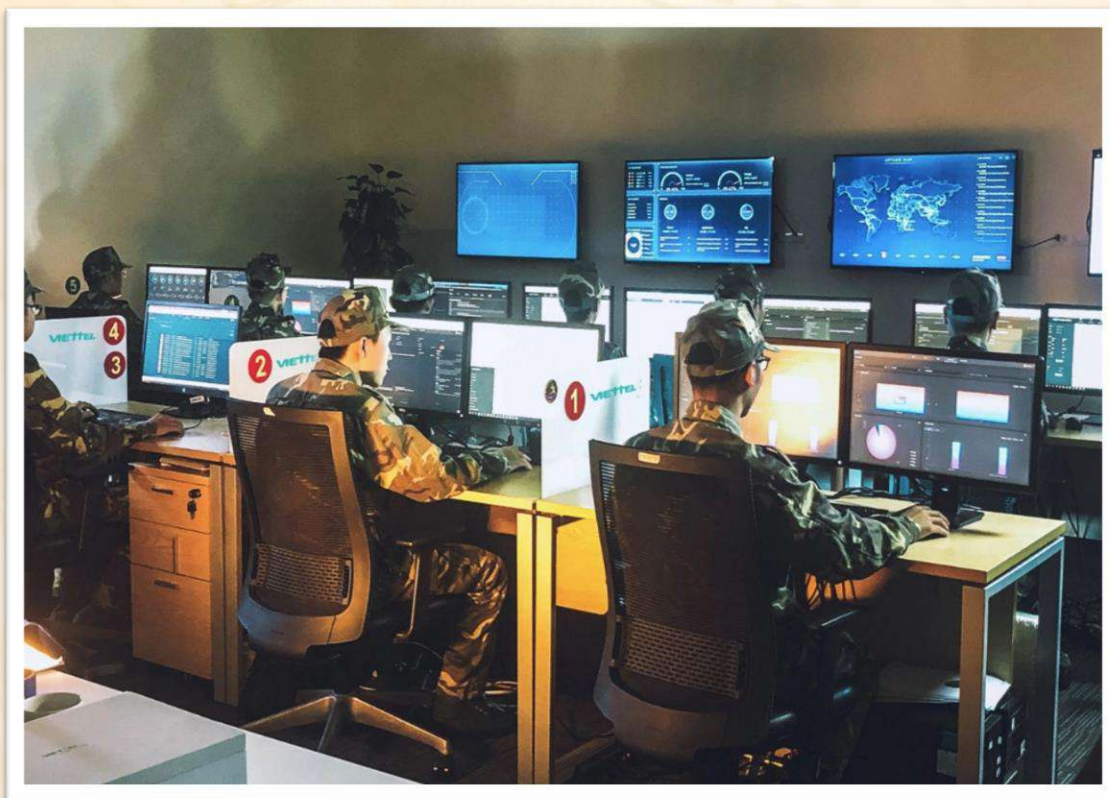
<sup>52</sup> Chen, A. (2021), *China's Data Security Law in Effect Sept. 1, 2021: Prepare for Compliance*, China Briefing News, <https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/>, truy cập ngày 10/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

tự thể hiện trong Luật Dữ liệu: Việt Nam khẳng định quyền kiểm soát đối với dữ liệu quan trọng, coi đó là nhiệm vụ gắn liền với bảo đảm an ninh, quốc phòng. Như vậy, việc quy định nội dung quản lý nhà nước về dữ liệu đã mang lại ý nghĩa pháp lý - chính trị to lớn: nó đặt dữ liệu dưới sự quản lý của Nhà nước pháp quyền xã hội chủ nghĩa, phục vụ các mục tiêu phát triển đất nước, đồng thời hài hòa với thông lệ quốc tế tiên bộ.



***Giám sát, phản ứng sự cố an toàn thông tin 24/7  
của Viettel Security - Ảnh: VGP***

Về tổng thể, Luật Dữ liệu 2024 cùng các nội dung quản lý nhà nước được quy định trong đó sẽ là bước đệm quan trọng để Việt Nam chuyển mình thành quốc gia số, quản trị và khai thác hiệu quả “nguồn dầu mỏ mới” của nền kinh tế, nhưng vẫn bảo vệ vững chắc chủ quyền, an ninh và lợi ích của quốc gia, tổ chức và từng người dân trong kỷ nguyên số hóa.





### **8.1.3. Chủ thể, đầu mối quản lý nhà nước về dữ liệu**

Theo khoản 2 Điều 8 Luật Dữ liệu và các Điều 27, 28, 29, 30, 31, 32 Nghị định số 165/2025/NĐ-CP quy định các đầu mối quản lý dữ liệu hiện nay như sau:

- a) Chính phủ thống nhất quản lý nhà nước và dữ liệu;
- b) Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước và dữ liệu, trừ quy định tại điểm c khoản này;
- c) Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về dữ liệu thuộc phạm vi quản lý;  
Bộ trưởng Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về dữ liệu cơ yếu thuộc phạm vi quản lý theo quy định của pháp luật về cơ yếu;
- d) Bộ và cơ quan ngang Bộ, cơ quan thuộc Chính phủ trong phạm vi, chức năng, nhiệm vụ, quyền hạn của mình xây dựng, phát triển cơ sở dữ liệu; phối hợp với Bộ Công an thực hiện quản lý nhà nước và dữ liệu;
- đ) Ủy ban nhân dân cấp tỉnh xây dựng, phát triển cơ sở dữ liệu; thực hiện quản lý nhà nước về dữ liệu tại địa phương.

Có thể thấy rằng, cơ chế đầu mối quản lý dữ liệu của Việt Nam được thiết kế theo mô hình phân tầng, kết hợp “thống nhất quản lý” ở tầm Chính phủ với “phân công - phân quyền” ở cấp bộ, ngành và địa phương. Mục tiêu là bảo đảm định hướng chiến lược nhất quán, nhưng vẫn tận dụng chuyên môn nghiệp vụ của từng lĩnh vực, đồng thời đặt an ninh, an toàn dữ liệu làm trọng tâm xuyên suốt.

Về cấu trúc, Chính phủ giữ vai trò thống nhất quản lý nhà nước về dữ liệu, chịu trách nhiệm hoạch định tầm nhìn, ban hành chính sách, chuẩn mực, kiến trúc tổng thể và cơ chế phối hợp liên ngành. Bộ Công an là cơ quan đầu





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

mỗi chịu trách nhiệm trước Chính phủ trong quản lý nhà nước về dữ liệu (trừ phần thuộc quốc phòng), do đó cần thực thi các nhiệm vụ then chốt như chuẩn hóa quy trình bảo vệ dữ liệu, điều phối kết nối - chia sẻ, giám sát, thẩm định an ninh đối với cơ sở dữ liệu dùng chung, và tổ chức kiểm tra, thanh tra, xử lý vi phạm. Bộ Quốc phòng chịu trách nhiệm quản lý dữ liệu thuộc phạm vi quốc phòng và cơ yếu, xác lập “*vùng bảo vệ đặc biệt*” đối với thông tin bí mật nhà nước, tiêu chuẩn mật mã và kiểm soát nghiêm việc chuyển dữ liệu nhạy cảm. Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ là chủ thể “*sở hữu nghiệp vụ*” dữ liệu chuyên ngành: xây dựng, vận hành cơ sở dữ liệu, chuẩn hóa siêu dữ liệu (metadata), bảo đảm tính đúng - đủ - kịp thời, liên thông với các hệ thống dùng chung, và phối hợp với Bộ Công an về an ninh dữ liệu. Ủy ban nhân dân cấp tỉnh tổ chức phát triển cơ sở dữ liệu địa phương, kết nối - chia sẻ với trung ương, thực thi quản lý nhà nước về dữ liệu tại chỗ, bảo đảm tính liên tục của dịch vụ công trên nền tảng số.



**Chính phủ là cơ quan cấp cao nhất trong quản lý nhà nước và dữ liệu -**

**Ảnh: Báo Điện tử Chính phủ**





Về ưu điểm, cách bố trí các lực lượng trong công tác quản lý nhà nước về dữ liệu này có một số điểm mạnh như: **(i)** Phân vai rõ ràng giữa Trung ương - bộ, ngành - địa phương, giúp tránh “khoảng trống quản trị”; **(ii)** Đặt đầu mối bảo đảm an ninh dữ liệu tại một cơ quan có năng lực điều tra, giám sát (Bộ Công an), qua đó tăng cường tính răn đe và hiệu quả thực thi; **(iii)** Tách bạch dữ liệu quốc phòng, cơ yếu dưới sự quản lý chuyên trách của Bộ Quốc phòng, phù hợp yêu cầu bảo mật cấp cao; **(iv)** Trao trách nhiệm “chủ sở hữu nghiệp vụ” cho từng bộ, ngành và địa phương, giúp dữ liệu sát thực tiễn, cập nhật và có người chịu trách nhiệm.

Tuy nhiên, nguy cơ chồng chéo về thẩm quyền giữa Bộ Công an và các cơ quan, ban, ngành chuyên môn khác là khó tránh khỏi, đặc biệt là trong việc thẩm định, chia sẻ và xử lý dữ liệu liên ngành. Cùng với đó, sự chênh lệch về nguồn lực và năng lực công nghệ giữa trung ương và địa phương khiến cho chất lượng cơ sở dữ liệu không đồng bộ, khó bảo đảm tính chính xác, kịp thời và liên thông. Việc chuẩn hóa quy trình, tiêu chuẩn kỹ thuật và phân loại dữ liệu vẫn còn hạn chế, dẫn đến nguy cơ thiếu thống nhất trong vận hành và bảo mật và nguy cơ đe dọa an ninh mạng từ tội phạm công nghệ cao ngày càng gia tăng, trong khi cơ chế giám sát, ứng cứu sự cố chưa thực sự đồng bộ. Những hạn chế trên đòi hỏi các cấp, các ngành cần sớm rà soát những sơ hở, thiếu sót để kịp thời tham mưu Chính phủ, các Bộ, ngành nhanh chóng xử lý, khắc phục triệt để các hạn chế này.

Tóm lại, việc xác định rõ chủ thể và đầu mối quản lý dữ liệu theo Luật Dữ liệu 2024 và Nghị định số 165/2025/NĐ-CP đã tạo dựng một khung khổ pháp lý quan trọng, bảo đảm sự lãnh đạo thống nhất của Chính phủ, đồng thời phân công trách nhiệm cụ thể cho Bộ Công an, Bộ Quốc phòng, các bộ, ngành và chính quyền địa phương. Mô hình này vừa phát huy được vai trò trung tâm của cơ quan đầu mối, vừa khuyến khích sự chủ động của từng lĩnh vực.





vực, địa bàn trong xây dựng và khai thác dữ liệu. Tuy nhiên, những thách thức về chồng chéo thẩm quyền, chênh lệch năng lực, thiếu chuẩn hóa kỹ thuật và áp lực từ các nguy cơ an ninh mạng vẫn hiện hữu, đòi hỏi phải tiếp tục hoàn thiện cơ chế phối hợp, nâng cao năng lực hạ tầng, củng cố văn hóa chia sẻ dữ liệu và tăng cường giám sát. Nếu làm tốt, cơ chế phân định đầu mối này sẽ trở thành nền tảng vững chắc cho việc hình thành một hệ sinh thái dữ liệu quốc gia an toàn, minh bạch và hiệu quả, phục vụ đồng thời cho phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh và khẳng định chủ quyền số quốc gia trong kỷ nguyên mới.

## **8.2. VAI TRÒ, TRÁCH NHIỆM CỦA BỘ CÔNG AN VÀ CÔNG AN CÁC ĐƠN VỊ, ĐỊA PHƯƠNG TRONG CÔNG TÁC QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU**

**T**rong bối cảnh an ninh dữ liệu được xem là một bộ phận quan trọng của an ninh quốc gia, việc tổ chức quản lý, khai thác và bảo vệ dữ liệu mang ý nghĩa đặc biệt quan trọng, nhất là đối với lực lượng Công an nhân dân. Sự giao thoa giữa an ninh quốc gia và an ninh, an toàn dữ liệu là một điểm nhấn quan trọng. Dữ liệu không chỉ là một yếu tố thúc đẩy kinh tế hay cải cách hành chính, mà còn là một thành phần thiết yếu của an ninh quốc gia. Lực lượng Công an nhân dân, với vai trò là lực lượng nòng cốt trong bảo đảm an ninh quốc gia và giữ gìn trật tự, an toàn xã hội, có trách nhiệm đặc biệt trong công tác quản lý nhà nước về dữ liệu cũng như bảo vệ dữ liệu khỏi các mối đe dọa, cả từ bên trong lẫn bên ngoài.

### **8.2.1. Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu**

Điều 26 Nghị định số 165/2025/NĐ-CP quy định vai trò, trách nhiệm chung của Bộ Công an trong công tác quản lý nhà nước về dữ liệu như sau:





- Chủ trì, phối hợp với các cơ quan có liên quan tổ chức triển khai, hướng dẫn, kiểm tra, đôn đốc việc thực hiện nghị định này.

- Chủ trì, phối hợp với các cơ quan có liên quan quản lý hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; bảo đảm an ninh dữ liệu, đấu tranh phòng, chống tội phạm và các hành vi vi phạm pháp luật trong lĩnh vực dữ liệu; quản lý, theo dõi, giám sát đối với hoạt động kinh doanh các sản phẩm, dịch vụ về dữ liệu theo quy định của Nghị định này.

- Chủ trì, phối hợp với các cơ quan có liên quan triển khai xây dựng Trung tâm dữ liệu quốc gia, đáp ứng các quy định, tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu.

- Chủ trì xây dựng, ban hành và trình cơ quan quản nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật hướng dẫn thực hiện các quy định pháp luật về dữ liệu.

- Chủ trì phối hợp với Bộ Tư pháp, Văn phòng Chính phủ, Bộ Khoa học và Công nghệ và các cơ quan liên quan rà soát, tổng hợp, đề xuất Chính phủ chỉ đạo các bộ, cơ quan, địa phương xây dựng, bổ sung, sửa đổi, bổ sung các văn bản liên quan đến việc triển khai, quản trị, vận hành của Trung tâm dữ liệu quốc gia.

- Tổ chức thực hiện kết nối, chia sẻ, điều phối dữ liệu giữa hệ thống thông tin, cơ sở dữ liệu của cơ quan, tổ chức, cá nhân với Cơ sở dữ liệu tổng hợp quốc gia thông qua Nền tảng chia sẻ, điều phối dữ liệu với Trung tâm dữ liệu quốc gia.

- Bảo đảm hạ tầng công nghệ thông tin cho cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội phục vụ việc quản lý, quản trị, xử lý dữ liệu thuộc phạm vi quản lý tại Trung tâm dữ liệu quốc gia.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

- Chủ trì, phối hợp với Bộ Khoa học và Công nghệ thẩm định, đánh giá, kiểm tra, hỗ trợ, giám sát và điều phối ứng phó với sự cố an ninh mạng, an toàn thông tin trong quá trình xây dựng, triển khai, vận hành các hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu quốc gia.

- Chủ trì, phối hợp với Bộ Khoa học và Công nghệ xây dựng tiêu chuẩn, quy chuẩn kỹ thuật hoặc hướng dẫn kỹ thuật về tổ chức, kết nối, chia sẻ, đồng bộ dữ liệu với Trung tâm dữ liệu quốc gia

- Xây dựng tiêu chuẩn kiến trúc hệ thống phần mềm tại Trung tâm dữ liệu quốc gia.

- Hướng dẫn tổ chức phân loại dữ liệu của cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội; tổ chức, chỉ đạo công tác đào tạo, bồi dưỡng về chuyên môn, nghiệp vụ về dữ liệu trên phạm vi cả nước.

- Xây dựng và vận hành Cổng dữ liệu quốc gia.

- Bộ trưởng Bộ Công an quyết định mức chi cho hoạt động hỗ trợ kinh phí, đảm bảo kết nối, chia sẻ; hỗ trợ bù đắp chi phí tạo lập, thu thập dữ liệu trên cơ sở thống nhất với Bộ trưởng Bộ tài chính, Bộ trưởng Bộ Khoa học và Công nghệ.

Trên cơ sở quy định trên, cùng với các quy định trong Luật Dữ liệu 2024 và Nghị định số 169/2025/NĐ-CP, nhóm tác giả phân tích, khái quát thành một số vai trò, trách nhiệm chính như sau:

**Thứ nhất**, là cơ quan đầu mối chịu trách nhiệm trước Chính phủ trong quản lý nhà nước về dữ liệu.

Luật Dữ liệu năm 2024 đã xác định Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ trong quản lý nhà nước về dữ liệu (ngoại trừ lĩnh vực cơ yếu do Bộ Quốc phòng quản lý). Cụ thể, Chính phủ thống nhất quản lý nhà nước về dữ liệu; Bộ Công an chịu trách nhiệm chính trước





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Chính phủ trong tổ chức thực hiện quản lý nhà nước về dữ liệu; Bộ Quốc phòng chịu trách nhiệm quản lý dữ liệu thuộc phạm vi quốc phòng, cơ yếu; còn các bộ, ngành và địa phương phối hợp với Bộ Công an trong phạm vi chức năng của mình. Điều này có nghĩa Bộ Công an đóng vai trò dẫn dắt, điều phối hoạt động của các bộ, ngành và Ủy ban nhân dân các tỉnh, thành phố trong mọi mặt công tác quản lý, xây dựng, khai thác, chia sẻ và bảo vệ dữ liệu trên phạm vi cả nước một cách thống nhất.



*Trang phục Khố nam sĩ quan An ninh mạng và Phòng chống tội phạm công nghệ cao trong lễ kỷ niệm, diễu binh, diễu hành kỷ niệm 80 năm Cách mạng Tháng Tám thành công (19/8/1945 - 19/8/2025) và Quốc khánh nước Cộng hòa xã hội chủ nghĩa Việt Nam (2/9/1945 - 2/9/2025) - Ảnh: Báo Phụ nữ số*

Là cơ quan đầu mối về quản lý nhà nước trong lĩnh vực dữ liệu, Bộ Công an không chỉ có vai trò hoạch định chính sách và tổ chức triển khai các cơ sở dữ liệu quốc gia, mà còn được giao trọng trách tổ chức triển khai





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

thực thi pháp luật trong toàn hệ thống. Điều này được thể hiện cụ thể tại khoản 1, Điều 26 Nghị định số 165/2025/NĐ-CP, theo đó, Bộ Công an “*chủ trì, phối hợp với các cơ quan có liên quan tổ chức triển khai, hướng dẫn, kiểm tra, đôn đốc việc thực hiện Nghị định này*”. Trên thực tế, đây là trách nhiệm pháp lý đóng vai trò cầu nối giữa quy phạm pháp luật và thực tiễn, nhằm bảo đảm Luật Dữ liệu và các văn bản hướng dẫn thi hành được quán triệt và thực thi nghiêm túc, đồng bộ trên phạm vi toàn quốc.

Việc triển khai này không chỉ đơn thuần là phổ biến văn bản pháp luật, mà bao gồm cả việc xây dựng kế hoạch tổ chức thực hiện, phân công rõ trách nhiệm cho các đơn vị trực thuộc, tổ chức tập huấn, hướng dẫn kỹ thuật, tổ chức kiểm tra liên ngành, thanh tra chuyên đề, và báo cáo tiến độ định kỳ cho Chính phủ. Trong giai đoạn đầu thi hành, Bộ Công an đã tập trung xây dựng, hoàn thiện Trung tâm Dữ liệu quốc gia và tổ chức nhiều hội nghị tập huấn, hướng dẫn các cơ quan, địa phương triển khai Nghị định 165/2025/NĐ-CP, qua đó bảo đảm sự thống nhất, đồng bộ trong công tác quản lý nhà nước về dữ liệu. Trong giai đoạn 2025 - 2026 sắp tới, Bộ Công an nên chủ động xây dựng hệ thống chỉ tiêu đánh giá kết quả triển khai Nghị định 165, ban hành các biểu mẫu báo cáo định kỳ về kết nối dữ liệu, tình trạng tuân thủ chia sẻ thông tin, và chất lượng dữ liệu đầu vào tại các địa phương, bộ ngành. Chính những hoạt động này sẽ góp phần nâng cao hiệu lực, hiệu quả quản lý nhà nước về dữ liệu, khắc phục tình trạng triển khai hình thức hoặc không đồng bộ giữa các cấp, các ngành.

Một điểm đặc thù có thể thấy trong mô hình Việt Nam khi lực lượng Công an được giao vai trò “*chủ đạo*” trong quản lý nhà nước về dữ liệu. Ở nhiều quốc gia khác, việc điều phối và giám sát tuân thủ pháp luật về dữ liệu thường do các cơ quan độc lập hoặc dân sự đảm nhiệm hơn là cơ quan Công





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

an. Ví dụ, trong Liên minh Châu Âu, việc thực thi Quy định Bảo vệ Dữ liệu Chung (GDPR) được giao cho các Cơ quan bảo vệ dữ liệu (Data Protection Authorities - DPA) độc lập ở mỗi quốc gia, chứ không phải cho lực lượng Cảnh sát hay An ninh. Mỗi nước EU có một “DPA” chịu trách nhiệm giám sát việc áp dụng GDPR, xử lý khiếu nại và có quyền điều tra, xử phạt các vi phạm về dữ liệu [53]. Chức năng của các DPA này thiên về bảo vệ quyền riêng tư và hướng dẫn tuân thủ cho doanh nghiệp, người dân, còn vai trò của cảnh sát chỉ giới hạn khi dữ liệu bị lợi dụng cho hành vi tội phạm như lừa đảo, đánh cắp danh tính... Ngược lại, tại Việt Nam, Luật Dữ liệu lại đặt trọng tâm quản lý vào Bộ Công an xuất phát từ quan điểm coi dữ liệu (đặc biệt dữ liệu cá nhân, dữ liệu quan trọng) là tài sản chiến lược gắn với an ninh quốc gia. Việc huy động lực lượng Công an tham gia sâu vào quá trình xây dựng, khai thác, bảo vệ dữ liệu nhằm đảm bảo an ninh ngay từ khâu thiết kế hệ thống.



*Bộ Công an là cơ quan đầu mối quản lý nhà nước về dữ liệu - Ảnh: Vietnamplus*





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Tùy bối cảnh mỗi nước, mô hình tổ chức thực thi pháp luật về dữ liệu có thể khác nhau. Việt Nam lựa chọn cách tiếp cận “*an ninh dữ liệu*” một cách chủ động, với lực lượng Công an nhân dân làm nòng cốt quản lý, khai thác, bảo vệ dữ liệu và phòng ngừa vi phạm. Mô hình này giúp thống nhất chỉ huy, phản ứng nhanh với nguy cơ an ninh, nhưng cũng đặt ra thách thức về đào tạo nhân lực - lực lượng Công an cần trang bị kiến thức sâu về công nghệ và pháp lý dữ liệu. Đồng thời, đòi hỏi sự kết hợp hài hòa giữa mục tiêu bảo vệ an ninh và quyền riêng tư, phát triển kinh tế số. Nhìn rộng hơn, trong bối cảnh chuyển đổi số toàn cầu, Việt Nam đang nỗ lực hoàn thiện hành lang pháp lý về dữ liệu song song với việc xây dựng hạ tầng dữ liệu quốc gia. Sự tham gia tích cực của Công an các đơn vị, địa phương vào quá trình này là một điểm sáng, góp phần đảm bảo rằng quá trình chuyển đổi số diễn ra an toàn, bền vững. Đây cũng là kinh nghiệm để các quốc gia khác tham khảo về vai trò của lực lượng thực thi pháp luật trong quản trị dữ liệu thời đại mới, khi mà dữ liệu “*vừa là động lực phát triển kinh tế, vừa tiềm ẩn nhiều nguy cơ an ninh phi truyền thống*”.

**Thứ hai**, phát triển hạ tầng và nền tảng dữ liệu quốc gia.

Theo định hướng của Chính phủ, Bộ Công an được giao thành lập Trung tâm dữ liệu quốc gia - một đơn vị sự nghiệp công lập tương đương cấp Cục trực thuộc Bộ Công an. Trung tâm Dữ liệu quốc gia là hạ tầng trọng điểm để tích hợp, đồng bộ, lưu trữ, chia sẻ, phân tích và điều phối dữ liệu của các cơ quan nhà nước, từ đó hình thành kho dữ liệu về con người và kho dữ liệu tổng hợp từ các cơ sở dữ liệu quốc gia. Dữ liệu tại Trung tâm sẽ là nền tảng cốt lõi cung cấp các dịch vụ liên quan đến dữ liệu, hỗ trợ hoạch định chính sách, kiến tạo phát triển, xây dựng Chính phủ số, kinh tế số và xã hội số; đồng thời cung cấp hạ tầng công nghệ cho các tổ chức chính trị -





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

xã hội và các hệ thống dữ liệu quốc gia, bảo đảm hiệu quả khai thác và an ninh mạng.



***Các tiện ích đã và đang được triển khai, xây dựng trên ứng dụng VNEID - Ảnh: Báo Công an Nhân dân.***

Hiện nay, Bộ Công an đang gấp rút hoàn thiện việc xây dựng Trung tâm dữ liệu quốc gia để kịp đưa vào vận hành từ ngày 19/8/2025, bảo đảm các điều kiện hạ tầng kỹ thuật cho thi hành Luật Dữ liệu<sup>53</sup>. Song song đó, Bộ Công an triển khai thu thập, cập nhật dữ liệu từ các bộ, ngành để đưa vào “Cơ sở dữ liệu tổng hợp quốc gia” (một cơ sở dữ liệu tích hợp dùng chung cho Chính phủ) trực thuộc Trung tâm này. Có thể thấy rằng, Trung tâm Dữ liệu quốc gia không chỉ phục vụ lưu trữ dữ liệu dùng chung và dữ liệu mở cho Chính phủ cũng như cộng đồng, mà còn cung cấp các dịch vụ hạ tầng như điện toán đám mây, chỗ đặt máy chủ, lưu trữ, cũng như các nền tảng

<sup>53</sup> Mekong, A. (2025), *Xây dựng quy chuẩn kết nối, chia sẻ dữ liệu từ địa phương lên trung ương*, Mekong ASEAN, <https://mekongasean.vn/xay-dung-quy-chuan-ket-noi-chia-se-du-lieu-tu-dia-phuong-len-trung-uong-43297.html>, truy cập ngày 07/8/2025.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

phân tích dữ liệu lớn nhằm hỗ trợ công tác dự báo, quản lý và xây dựng chính sách quốc gia. Chẳng hạn, Trung tâm đang phát triển hệ thống tính toán hiệu năng cao (HPC) và hệ thống phân tích dữ liệu để phục vụ phân tích dự báo kinh tế, xã hội, đồng thời hỗ trợ nghiên cứu khoa học và phát triển sản phẩm, dịch vụ về dữ liệu. Bên cạnh đó, Trung tâm sẽ vận hành Công Dữ liệu quốc gia - điểm truy cập tập trung để các cơ quan nhà nước công bố thông tin về dữ liệu đang quản lý và cung cấp dữ liệu mở. Việc công khai dữ liệu này không chỉ tăng tính minh bạch trong hoạt động của Chính phủ mà còn khuyến khích các sáng kiến đổi mới dựa trên dữ liệu, nâng cao chất lượng dịch vụ công và hỗ trợ hoạch định chính sách dựa trên dữ liệu.

Một nội dung then chốt khác là theo khoản 5 Điều 26 Nghị định 165/2025/NĐ-CP, Bộ Công an được giao nhiệm vụ chủ trì phối hợp với Bộ Tư pháp, Văn phòng Chính phủ, Bộ Khoa học và Công nghệ và các cơ quan liên quan trong rà soát, tổng hợp, đề xuất sửa đổi, bổ sung các văn bản pháp luật liên quan đến việc triển khai, quản trị, vận hành Trung tâm Dữ liệu quốc gia. Đặc biệt là về các quy định về phân cấp quản lý, chia sẻ dữ liệu, bảo đảm an toàn thông tin và tiêu chuẩn kỹ thuật... Đây là một nhiệm vụ mang tính chiến lược, bởi Trung tâm Dữ liệu quốc gia là hạ tầng trọng yếu phục vụ Chính phủ số và nền kinh tế số, do đó cần được vận hành trong một hành lang pháp lý hoàn chỉnh, linh hoạt và bắt kịp với tốc độ phát triển công nghệ. Có thể thấy rằng, trách nhiệm này thể hiện vai trò chủ động của Bộ Công an trong việc hoàn thiện hành lang pháp lý đồng bộ, thống nhất, phù hợp với mô hình điều phối dữ liệu tập trung mà Trung tâm đảm nhận.

Thực tiễn cho thấy, nhiều văn bản pháp luật hiện hành vẫn tồn tại những khoảng trống hoặc mâu thuẫn, chưa kịp cập nhật với mô hình điều phối dữ liệu tập trung do Trung tâm Dữ liệu quốc gia đảm nhiệm. Thời gian tới, Bộ Công an cần kiến nghị, tham mưu Chính phủ ban hành các quy định điều





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

chính, trong đó có việc sửa đổi Luật An ninh mạng, đồng bộ với Luật Dữ liệu; xây dựng nghị định về khai thác, sử dụng dữ liệu số; và ban hành các thông tư hướng dẫn vận hành kho dữ liệu dùng chung.

Như vậy, với vai trò chủ trì, Bộ Công an đã và đang hiện thực hóa các trụ cột hạ tầng dữ liệu quan trọng, tạo nền tảng cho việc khai thác dữ liệu hiệu quả và an toàn ở cấp độ quốc gia. Bộ Chính trị đã khẳng định Trung tâm dữ liệu quốc gia chính là “*lõi trụ cột*” của quá trình chuyển đổi số quốc gia, khi dữ liệu được coi là tư liệu sản xuất chính của kỷ nguyên mới và hạ tầng dữ liệu là một trong bốn trụ cột của kỷ nguyên số<sup>54</sup>. Vai trò tiên phong của Bộ Công an trong phát triển hạ tầng dữ liệu cho thấy quyết tâm của Việt Nam trong việc xây dựng “*chủ quyền số*” vững chắc dựa trên tài nguyên dữ liệu quốc gia.



***Đại tướng Lương Tam Quang, Bộ trưởng Bộ Công an phát biểu chỉ đạo, giao nhiệm vụ đối với Trung tâm Dữ liệu quốc gia - Ảnh: cand.com.vn***

<sup>54</sup> Baochinhpvu.vn (2025), *Bộ Công an tổ chức lễ ra mắt Trung tâm Dữ liệu quốc gia*, <https://baochinhphu.vn/ra-mat-trung-tam-du-lieu-quoc-gia-don-vi-cap-cuc-thuoc-bo-cong-an-102250225161046985.htm>, truy cập ngày 07/8/2025.

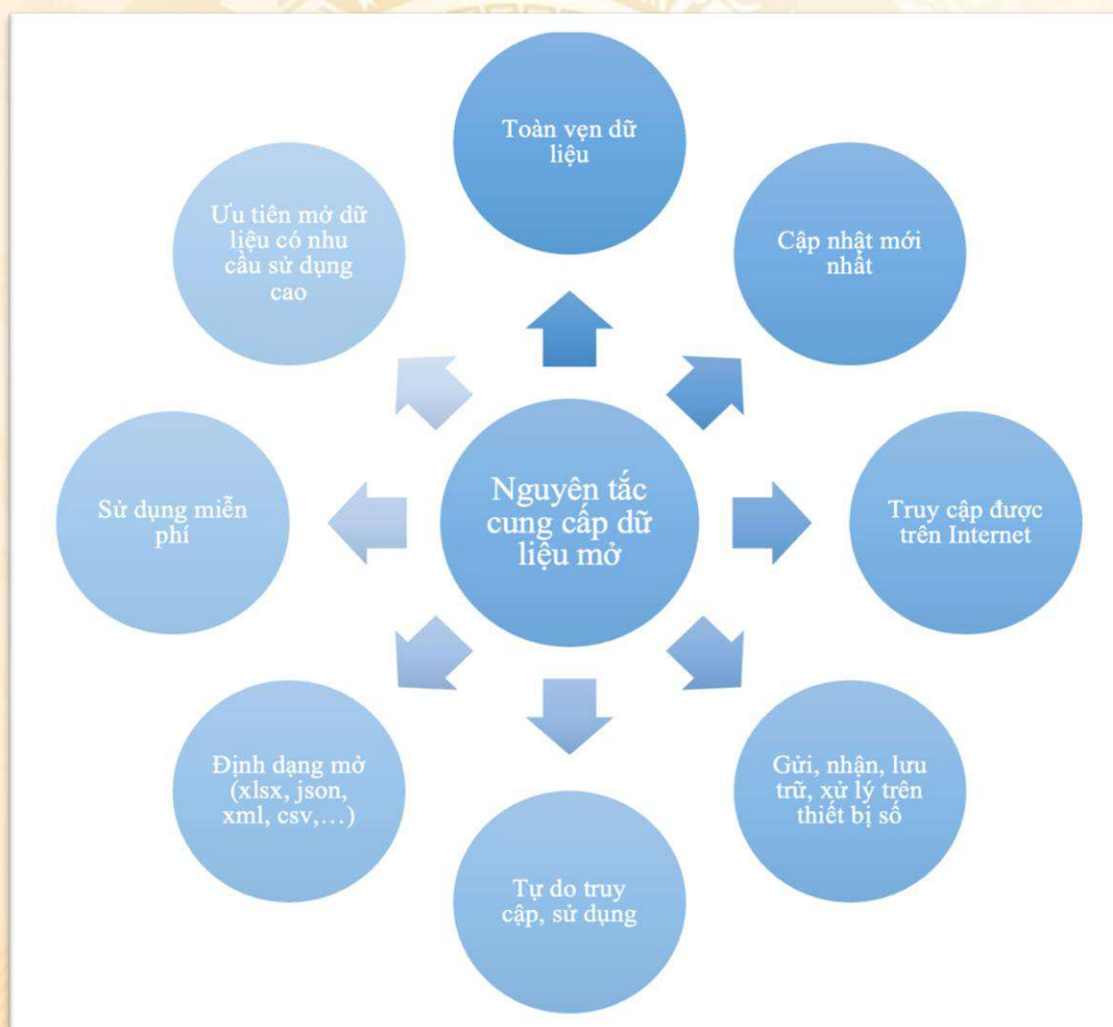




## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

**Thứ ba**, hướng dẫn và điều phối quản lý dữ liệu liên ngành, địa phương.

Bộ Công an không những xây dựng hạ tầng trung tâm, mà còn chịu trách nhiệm hướng dẫn và điều phối các bộ, ngành, địa phương trong quản lý, kết nối và chia sẻ dữ liệu. Luật Dữ liệu quy định rõ: các bộ, cơ quan ngang bộ và cơ quan thuộc Chính phủ trong phạm vi chức năng, nhiệm vụ của mình phải xây dựng, phát triển các cơ sở dữ liệu chuyên ngành và phối hợp với Bộ Công an trong thực hiện quản lý nhà nước về dữ liệu. Tương tự, Ủy ban nhân dân cấp tỉnh có trách nhiệm phát triển cơ sở dữ liệu và thực hiện quản lý nhà nước về dữ liệu tại địa phương mình, dưới sự hướng dẫn chung của Bộ Công an.



**Ảnh: Cổng thông tin chuyển đổi số quốc gia**





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Trên thực tế, Bộ Công an đóng vai trò đầu mối kết nối, chia sẻ dữ liệu giữa Trung tâm dữ liệu quốc gia với các bộ, ngành và địa phương. Bộ Công an có trách nhiệm “*Hướng dẫn, thực hiện các biện pháp bảo đảm an ninh mạng trong quá trình kết nối, chia sẻ dữ liệu số*” qua Cổng Dữ liệu quốc gia. Qua đó, không những biến Cổng Dữ liệu quốc gia thành điểm truy cập tập trung để các cơ quan công khai thông tin dữ liệu và cung cấp dữ liệu mở như đã nêu, mà còn bảo đảm sự minh bạch và thúc đẩy các sáng kiến sử dụng dữ liệu tại địa phương.

Bên cạnh đó, Bộ Công an đang phối hợp với Bộ Khoa học và Công nghệ cũng như các cơ quan liên quan xây dựng các quy chuẩn kết nối dữ liệu từ cấp tỉnh lên Trung ương, bảo đảm mọi địa phương tuân thủ thống nhất một kiến trúc chia sẻ dữ liệu chung. Theo chỉ đạo của Chính phủ, các bộ, ngành, địa phương phải ban hành tiêu chuẩn kỹ thuật về kết nối dữ liệu từ hệ thống của mình lên Trung tâm Dữ liệu quốc gia, hoàn thiện cơ chế chia sẻ, liên thông dữ liệu với trung tâm này trước khi Luật Dữ liệu có hiệu lực đầy đủ. Đồng thời, Bộ Công an được giao phối hợp rà soát hiện trạng các cơ sở dữ liệu hiện có, tiếp tục xây dựng các hệ thống dữ liệu ở từng cấp để bảo đảm đồng bộ, thống nhất về cấu trúc, tiêu chuẩn, phục vụ kết nối dữ liệu toàn quốc. Nhờ vai trò “*nhạc trưởng*” của Bộ Công an, Việt Nam đang nỗ lực và tiến gần hơn đến việc thiết lập được một “*kiến trúc dữ liệu quốc gia thống nhất*” từ trung ương tới địa phương, khắc phục tình trạng dữ liệu cát cứ, phân tán giữa các bộ ngành và địa phương.

**Thứ tư**, xây dựng chiến lược, chính sách và tiêu chuẩn kỹ thuật dữ liệu.

Khoản 3, Điều 28 Luật Dữ liệu có quy định: “*Bộ Công an chủ trì, phối hợp với cơ quan có liên quan ban hành danh mục tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu; trừ danh mục tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu*





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

*thuộc lĩnh vực quốc phòng, cơ yếu”. Theo đó, một trong những nhiệm vụ trọng tâm của Bộ Công an theo Luật Dữ liệu là tham mưu xây dựng chiến lược, chính sách và ban hành tiêu chuẩn, quy chuẩn kỹ thuật cho lĩnh vực dữ liệu. Bộ Công an được giao chủ trì ban hành danh mục tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu (phối hợp với các cơ quan liên quan), ngoại trừ các tiêu chuẩn, quy chuẩn thuộc lĩnh vực quốc phòng, cơ yếu do Bộ Quốc phòng ban hành. Đây là cơ sở để đảm bảo sự đồng bộ, liên thông và an toàn cho hệ thống hạ tầng dữ liệu quốc gia, khắc phục tình trạng manh mún, thiếu thống nhất trước đây về tiêu chuẩn dữ liệu giữa các bộ, ngành và địa phương. Thực tế, trước khi có Luật Dữ liệu, nhiều bộ, ngành xây dựng cơ sở dữ liệu theo các tiêu chuẩn khác nhau, gây trùng lặp và khó khăn khi kết nối, chia sẻ. Nay với vai trò đầu mối, Bộ Công an đang thiết lập bộ khung tiêu chuẩn chung, làm “ngôn ngữ chung” cho dữ liệu giữa các hệ thống. Ví dụ, Bộ Công an hiện chủ trì xây dựng các quy chuẩn kỹ thuật kết nối, chia sẻ dữ liệu giữa các cơ sở dữ liệu từ trung ương đến địa phương, nhằm đảm bảo các hệ thống dữ liệu vận hành thông suốt, liên thông từ cấp trung ương xuống cơ sở. Thủ tướng Chính phủ cũng đã chỉ đạo Bộ Công an phối hợp với các bộ liên quan ban hành quy định bắt buộc về kết nối, chia sẻ dữ liệu, xác định rõ danh mục dữ liệu cần chia sẻ, tiêu chuẩn kỹ thuật và trách nhiệm của từng cơ quan, hoàn thành trong tháng 8/2025 [27]. Những động thái này nhằm tạo nên hạ tầng pháp lý và kỹ thuật đồng bộ, thống nhất cho dữ liệu, tránh tình trạng “cát cứ” dữ liệu cản trở cuộc cách mạng chuyển đổi số toàn diện của nước ta hiện nay.*

Bên cạnh đó, một trong những nhiệm vụ chuyên biệt được quy định tại khoản 10, Điều 26 Nghị định số 165/2025/NĐ-CP là Bộ Công an “*xây dựng tiêu chuẩn kiến trúc hệ thống phần mềm tại Trung tâm dữ liệu quốc gia*”.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Đây là nhiệm vụ có tính nền tảng, bởi kiến trúc phần mềm chính là “*khung xương*” quy định cách thức các ứng dụng, cơ sở dữ liệu và dịch vụ số được thiết kế, triển khai, kết nối và vận hành trong một hệ thống tập trung. Nếu coi Trung tâm Dữ liệu quốc gia là “*trái tim*” của hạ tầng số, thì kiến trúc phần mềm chính là “*mạch máu công nghệ*”, quyết định khả năng liên thông, mở rộng và bảo đảm an ninh của toàn bộ hệ sinh thái dữ liệu.



***Thủ tướng Phạm Minh Chính và các đại biểu khai trương  
Trung tâm Dữ liệu quốc gia số 1 - Ảnh: Dương Giang/TTXVN***

Về phương diện kỹ thuật, việc xây dựng kiến trúc phần mềm hướng tới ba yêu cầu cơ bản: **(1) Đồng bộ và tương thích:** Bảo đảm các phần mềm, dịch vụ dữ liệu do các bộ, ngành, địa phương phát triển khi kết nối về Trung tâm phải tuân thủ cùng một khung chuẩn; tránh tình trạng “*cát cứ dữ liệu*” và trùng lặp hệ thống. **(2) An toàn và linh hoạt:** Áp dụng nguyên tắc “*an toàn theo thiết kế*” (security by design), tích hợp các lớp bảo mật, kiểm soát



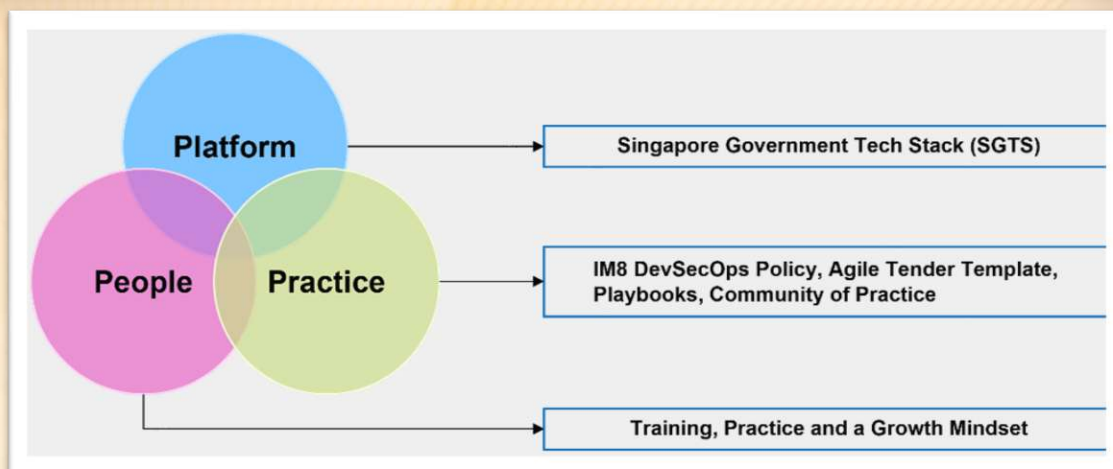


truy cập, mã hóa dữ liệu ngay từ giai đoạn thiết kế. Đồng thời, kiến trúc phải đủ linh hoạt để mở rộng quy mô, tích hợp công nghệ mới như trí tuệ nhân tạo, phân tích dữ liệu lớn hay blockchain. **(3) Hiệu quả và tối ưu:** Hướng tới sử dụng nền tảng điện toán đám mây quốc gia, khai thác lợi thế của kiến trúc vi dịch vụ (microservices) nhằm tiết kiệm tài nguyên, tăng khả năng tái sử dụng và giảm chi phí vận hành.

Về phương diện quản trị, Bộ Công an không chỉ là cơ quan xây dựng bộ tiêu chuẩn kiến trúc mà còn có trách nhiệm ban hành các hướng dẫn kỹ thuật, kiểm tra việc tuân thủ của các cơ quan khi đưa hệ thống dữ liệu lên Trung tâm. Đây là cơ chế quan trọng bảo đảm một ngôn ngữ kỹ thuật thống nhất, tạo điều kiện cho các bộ, ngành dễ dàng tích hợp và chia sẻ dữ liệu. Đồng thời, kiến trúc phần mềm chuẩn còn giúp Chính phủ kiểm soát chặt chẽ an ninh mạng và chất lượng dữ liệu, từ đó giảm rủi ro trong khai thác, sử dụng.

Kinh nghiệm quốc tế cho thấy nhiều quốc gia đã coi việc xây dựng kiến trúc phần mềm cho hạ tầng dữ liệu là nhiệm vụ chiến lược. Chẳng hạn, Liên minh châu Âu đã ban hành *Khung kiến trúc dữ liệu liên châu Âu (European Interoperability Framework)* nhằm thống nhất các tiêu chuẩn kỹ thuật trong chia sẻ dữ liệu công. Tại Singapore, GovTech xây dựng kiến trúc nền tảng “SG Tech Stack” để đảm bảo mọi dịch vụ và ứng dụng của Chính phủ kết nối trên cùng chuẩn kỹ thuật, đồng thời được CSA giám sát về an ninh mạng. Những mô hình này cho thấy, nếu không có kiến trúc phần mềm chuẩn, các nền tảng dữ liệu quốc gia sẽ khó đạt được sự tương thích, dẫn đến lãng phí và mất an toàn. Việt Nam, với việc giao cho Bộ Công an nhiệm vụ xây dựng kiến trúc phần mềm cho Trung tâm Dữ liệu quốc gia, đang đi theo xu hướng chung, đồng thời khẳng định *quyết tâm xây dựng một hạ tầng dữ liệu hiện đại, an toàn và liên thông*.





### ***Singapore Government Tech Stack - Ảnh: SGDP***

Có thể khẳng định, việc Bộ Công an chủ trì xây dựng kiến trúc phần mềm tại Trung tâm dữ liệu quốc gia không chỉ là yêu cầu kỹ thuật, mà còn mang ý nghĩa chính trị - pháp lý. Đây là điều kiện tiên quyết để vận hành hệ sinh thái dữ liệu quốc gia một cách đồng bộ, bảo mật và hiệu quả, tạo nền móng vững chắc cho Chính phủ số, kinh tế số và xã hội số.

**Thứ năm**, hợp tác quốc tế và phát triển hệ sinh thái đổi mới, sáng tạo về dữ liệu, thị trường dữ liệu.

Trong lĩnh vực khoa học, công nghệ và đổi mới sáng tạo liên quan đến dữ liệu, Điều 40 của Nghị định 169/2025/NĐ-CP “giao” Bộ Công an một loạt trách nhiệm quan trọng. Trước hết, Bộ Công an là đầu mối quản lý hoạt động hợp tác quốc tế về khoa học, công nghệ và đổi mới sáng tạo trong lĩnh vực dữ liệu. Điều này có nghĩa mọi hoạt động hợp tác với nước ngoài về nghiên cứu phát triển công nghệ dữ liệu, trao đổi kinh nghiệm quản trị dữ liệu, bảo vệ dữ liệu xuyên biên giới... đều do Bộ Công an chủ trì thống nhất. Thời gian qua, Bộ Công an đã thiết lập nhiều kênh hợp tác với các tổ chức quốc tế về bảo vệ dữ liệu, chuyển giao công nghệ và đào tạo nhân lực. Chẳng hạn, Trung tâm Dữ liệu quốc gia được trao quyền ký kết các thỏa thuận, biên





bản ghi nhớ với tổ chức quốc tế nhằm thúc đẩy hợp tác về bảo vệ dữ liệu, đào tạo, chuyển giao công nghệ và khai thác dữ liệu xuyên biên giới. Đây là nền tảng để Việt Nam tranh thủ nguồn lực và kinh nghiệm quốc tế, đồng thời nâng cao vị thế trong các vấn đề quản trị dữ liệu toàn cầu.

Bộ Công an cũng đóng vai trò hỗ trợ ươm tạo và phát triển hệ sinh thái khởi nghiệp về dữ liệu. Nghị định 169/2025/NĐ-CP (khoản 1, Điều 40) quy định Bộ Công an chủ trì, phối hợp với các bộ, ngành, cơ quan liên quan để hỗ trợ các doanh nghiệp khởi nghiệp, các dự án đổi mới sáng tạo dựa trên dữ liệu. Mục tiêu là tạo môi trường thuận lợi cho doanh nghiệp cung cấp các sản phẩm, dịch vụ mới dựa trên dữ liệu, từ đó hình thành một thị trường dữ liệu sôi động. Ví dụ điển hình cho vai trò này là việc Chính phủ thành lập “*Quỹ Phát triển Dữ liệu Quốc gia*” (một quỹ tài chính nhà nước ngoài ngân sách) và giao Bộ Công an quản lý<sup>55</sup>. Quỹ Phát triển Dữ liệu Quốc gia có vốn điều lệ ban đầu 1.000 tỷ đồng từ ngân sách nhà nước, hoạt động không vì lợi nhuận, nhằm hỗ trợ các hoạt động phát triển, ứng dụng công nghệ dữ liệu phục vụ quản lý nhà nước, lợi ích quốc gia và cộng đồng. Mục tiêu của quỹ là thúc đẩy những lĩnh vực công nghệ mới trong xử lý dữ liệu như trí tuệ nhân tạo, dữ liệu lớn, học máy, điện toán đám mây, chuỗi khối, Internet vạn vật...; hỗ trợ chuyển đổi số quốc gia, đặc biệt ở các địa bàn kinh tế, xã hội khó khăn; đồng thời ươm tạo các doanh nghiệp khởi nghiệp dữ liệu, phát triển hệ sinh thái đổi mới sáng tạo và thị trường dữ liệu Việt Nam. Quỹ này do Bộ Công an trực tiếp quản lý và điều hành, thể hiện vai trò “*nhạc trưởng*” của Bộ trong việc huy động nguồn lực thúc đẩy đổi mới sáng tạo dựa trên dữ liệu ở Việt Nam.

<sup>55</sup> Phạm Dự (2025), *Bộ Công an quản lý quỹ nghìn tỷ phát triển dữ liệu quốc gia*, Vnexpress.net, <https://vnexpress.net/bo-cong-an-quan-ly-quy-nghin-ty-phat-trien-du-lieu-quoc-gia-4908788.html>, truy cập ngày 07/8/2025.





***Ảnh: Quỹ phát triển dữ liệu quốc gia***

Bên cạnh đó, Bộ Công an còn được giao trách nhiệm đào tạo, bồi dưỡng nguồn nhân lực khoa học, công nghệ về dữ liệu trên phạm vi cả nước. Cụ thể, Bộ Công an chủ trì phối hợp với Bộ Giáo dục và Đào tạo, Bộ Khoa học và Công nghệ và các bộ ngành liên quan xây dựng và thực hiện chương trình đào tạo, bồi dưỡng nâng cao trình độ chuyên môn, nghiệp vụ cho đội ngũ nhân lực khoa học, công nghệ và đổi mới sáng tạo về dữ liệu (theo Nghị định 169/2025/NĐ-CP). Thực hiện nhiệm vụ này, Bộ Công an đã triển khai nhiều hoạt động phối hợp với ngành giáo dục và các viện nghiên cứu để đào tạo chuyên sâu về lĩnh vực dữ liệu. Bộ Công an đã cử cán bộ tham gia các khóa học thạc sĩ về khoa học dữ liệu, an toàn thông tin, trí tuệ nhân tạo...; đồng thời mở các lớp bồi dưỡng kỹ năng quản trị dữ liệu cho cán bộ trong và ngoài ngành Công an. Những chương trình đào tạo nhân lực chất lượng cao về khoa học dữ liệu, an ninh mạng, trí tuệ nhân tạo như vậy nhằm đáp ứng yêu cầu chuyển đổi số và quản trị dữ liệu quốc gia trong giai đoạn mới.

***Thứ sáu***, cấp phép và quản lý hoạt động kinh doanh sản phẩm, dịch vụ dữ liệu. Để phát triển một thị trường dữ liệu minh bạch, đáng tin cậy, Bộ





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Công an được trao thẩm quyền quản lý chặt chẽ hoạt động kinh doanh các dịch vụ liên quan đến dữ liệu. Nghị định 169/2025/NĐ-CP (khoản 3, Điều 40) quy định Bộ Công an hướng dẫn và tổ chức cấp các loại giấy chứng nhận đủ điều kiện kinh doanh trong lĩnh vực dữ liệu. Cụ thể, Bộ Công an có thẩm quyền cấp, cấp đổi và thu hồi giấy chứng nhận cho các loại hình hoạt động sau: **(1)** Thử nghiệm có kiểm soát về dữ liệu; **(2)** Kinh doanh sàn dữ liệu; **(3)** Kinh doanh sản phẩm, dịch vụ trung gian dữ liệu; **(4)** Kinh doanh (hoặc cung cấp) sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu. Các giấy chứng nhận này đóng vai trò như “*giấy phép con*” đảm bảo doanh nghiệp đáp ứng đầy đủ các yêu cầu kỹ thuật, tổ chức về an ninh, an toàn và chất lượng dữ liệu trước khi tham gia thị trường dữ liệu.

Quy trình cấp phép các hoạt động nêu trên được thiết kế chặt chẽ, bảo đảm sàng lọc các chủ thể tham gia thị trường dữ liệu. Chẳng hạn, doanh nghiệp muốn vận hành sàn dữ liệu phải lập hồ sơ đề nghị Bộ Công an thẩm định và cấp giấy chứng nhận đủ điều kiện kinh doanh. Hồ sơ gồm tờ khai theo mẫu do Bộ Công an ban hành, gửi tới Bộ (qua Trung tâm Dữ liệu quốc gia) để được xem xét cấp phép. Mẫu tờ khai đề nghị cấp phép hoạt động sàn dữ liệu quy định rõ các thông tin doanh nghiệp phải cung cấp (tên, địa chỉ, năng lực nhân sự, hạ tầng kỹ thuật, phương án bảo đảm an toàn dữ liệu...) và cam kết tuân thủ pháp luật.

Thời gian qua, Bộ Công an đã xây dựng sẵn các biểu mẫu hồ sơ điện tử và quy trình hướng dẫn để doanh nghiệp nộp hồ sơ cấp phép một cách thuận tiện, có thể thông qua cổng dịch vụ công trực tuyến. Việc Bộ Công an thống nhất quản lý khâu cấp phép này nhằm bảo đảm các chủ thể tham gia thị trường dữ liệu đáp ứng các tiêu chuẩn kỹ thuật và yêu cầu an ninh, tránh tình trạng dữ liệu bị mua bán, trao đổi trái phép gây rủi ro cho xã hội.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

**Thứ bảy**, giám sát, bảo đảm an ninh và xử lý vi phạm trong lĩnh vực dữ liệu. Một trong những trách nhiệm trọng tâm của Bộ Công an theo khoản 2, Điều 26 Nghị định 165/2025/NĐ-CP là “*chủ trì, phối hợp với các cơ quan có liên quan quản lý hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; bảo đảm an ninh dữ liệu, đấu tranh phòng, chống tội phạm và các hành vi vi phạm pháp luật trong lĩnh vực dữ liệu; quản lý, theo dõi, giám sát đối với hoạt động kinh doanh các sản phẩm, dịch vụ về dữ liệu*”. Quy định này thể hiện rõ vai trò *giám sát và bảo vệ* của Bộ Công an, đồng thời nhấn mạnh trách nhiệm xử lý các vi phạm phát sinh trong quá trình xây dựng và vận hành hệ sinh thái dữ liệu quốc gia.

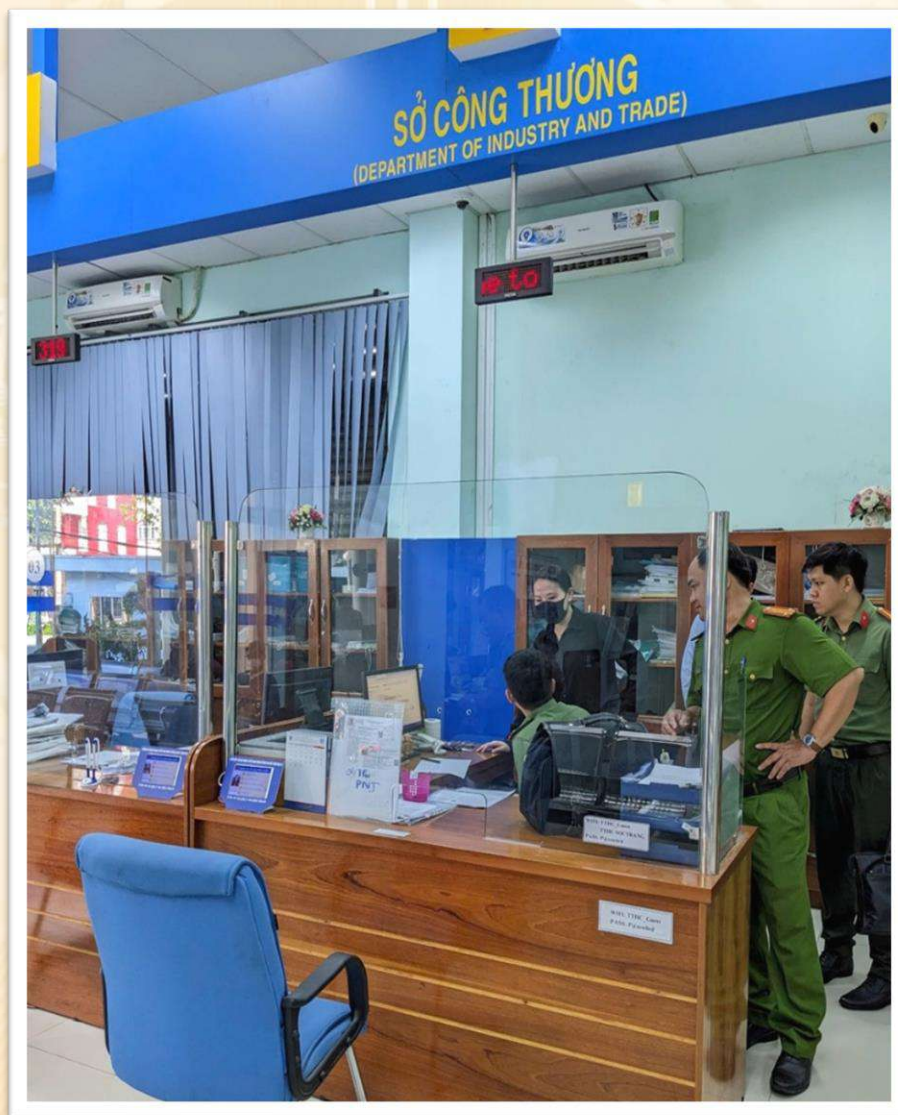
Trước hết, Bộ Công an được giao trách nhiệm *giám sát toàn diện* các hoạt động dữ liệu: từ khâu tạo lập, quản trị, khai thác đến kinh doanh sản phẩm, dịch vụ liên quan đến dữ liệu. Việc giám sát không chỉ nhằm bảo đảm tính hợp pháp và minh bạch trong hoạt động dữ liệu, mà còn tạo ra cơ chế cảnh báo sớm, kịp thời phát hiện những bất cập, sai phạm để xử lý ngay từ giai đoạn đầu. Đây chính là nền tảng để ngăn chặn tình trạng lạm dụng dữ liệu, mua bán dữ liệu trái phép, hay các hành vi xâm phạm quyền lợi người dân và doanh nghiệp. Bên cạnh đó, Bộ Công an là lực lượng nòng cốt trong bảo đảm an ninh dữ liệu quốc gia. Trong bối cảnh các mối đe dọa từ tội phạm mạng ngày càng gia tăng, quy định này khẳng định trách nhiệm của Bộ không chỉ dừng ở quản lý hành chính mà còn trực tiếp đấu tranh, trấn áp các hành vi tấn công, xâm nhập, phá hoại hệ thống dữ liệu. Thực tiễn triển khai Trung tâm dữ liệu quốc gia cho thấy, Bộ Công an đã chủ động xây dựng các đơn vị chuyên trách giám sát an toàn thông tin 24/7, đồng thời thiết lập cơ chế phối hợp với công an các địa phương để cùng theo dõi, phát hiện và xử lý sự cố. Cuối cùng, vai trò “*theo dõi, giám sát đối với hoạt động kinh doanh*





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

*sản phẩm, dịch vụ về dữ liệu” cho thấy Bộ Công an có quyền quản lý và kiểm soát thị trường dịch vụ dữ liệu, bảo đảm rằng các chủ thể tham gia phải tuân thủ pháp luật, tôn trọng quy chuẩn về bảo mật, quyền riêng tư và an ninh quốc gia. Đây là một cơ chế phòng ngừa quan trọng, đặt hoạt động kinh doanh dữ liệu dưới sự giám sát chặt chẽ của cơ quan quản lý nhà nước, qua đó tạo niềm tin cho xã hội và khuyến khích phát triển thị trường dữ liệu minh bạch, an toàn.*



***Tổ Công tác triển khai Đề án 06 kiểm tra máy tính quay Sở Công thương -  
Ảnh: Cổng thông tin điện tử Văn phòng UBND tỉnh Sóc Trăng***





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Có thể khẳng định rằng, thông qua trách nhiệm giám sát, bảo đảm an ninh và xử lý vi phạm theo Điều 26 Nghị định 165/2025/NĐ-CP, Bộ Công an giữ vai trò “*người gác cổng*” cho hệ sinh thái dữ liệu quốc gia. Đây chính là điều kiện tiên quyết để thúc đẩy chia sẻ, khai thác dữ liệu một cách an toàn, hiệu quả, đồng thời củng cố nền tảng pháp lý và kỹ thuật cho tiến trình chuyển đổi số quốc gia.

**Thứ tám**, điều phối ứng phó sự cố an ninh mạng, an toàn thông tin tại Trung tâm dữ liệu quốc gia.

Trong bối cảnh dữ liệu đã trở thành hạ tầng thiết yếu của quốc gia, việc bảo đảm an ninh mạng và an toàn thông tin cho các hệ thống dữ liệu tập trung mang ý nghĩa sống còn. Nghị định số 165/2025/NĐ-CP, tại khoản 8 Điều 26, quy định rõ trách nhiệm của Bộ Công an là “*chủ trì, phối hợp với Bộ Khoa học và Công nghệ thẩm định, đánh giá, kiểm tra, hỗ trợ, giám sát và điều phối ứng phó với sự cố an ninh mạng, an toàn thông tin trong quá trình xây dựng, triển khai, vận hành các hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu quốc gia*”. Quy định này cho thấy, bên cạnh chức năng quản lý nhà nước về dữ liệu, Bộ Công an còn có trách nhiệm bảo vệ an toàn hạ tầng trọng yếu (Trung tâm dữ liệu quốc gia) trước mọi nguy cơ tấn công từ không gian mạng.

Vai trò “*điều phối ứng phó sự cố*” được hiểu theo nghĩa rộng, bao gồm cả phòng ngừa, phát hiện và xử lý các rủi ro an ninh mạng có thể xảy ra. Trước hết, Bộ Công an chủ trì thẩm định, đánh giá an toàn của các hệ thống thông tin và phần mềm khi đưa vào vận hành tại Trung tâm, nhằm kịp thời phát hiện lỗ hổng, nguy cơ mất an toàn. Trong quá trình vận hành, Bộ thực hiện giám sát liên tục, xây dựng cơ chế cảnh báo sớm, phân tích nhật ký hệ thống, triển khai các công cụ trí tuệ nhân tạo để phát hiện hành vi bất thường.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Đặc biệt, khi xảy ra sự cố, chẳng hạn như tấn công từ chối dịch vụ, đánh cắp dữ liệu, hoặc cài cắm mã độc, Bộ Công an sẽ là cơ quan đầu mối điều phối lực lượng, huy động chuyên gia, phối hợp với Bộ Khoa học và Công nghệ cùng các đơn vị liên quan để cô lập, khắc phục, đồng thời điều tra, truy vết thủ phạm.

Nhiệm vụ này thể hiện rõ bản chất *hai tầng trách nhiệm* của Bộ Công an: vừa là cơ quan quản lý nhà nước, vừa là lực lượng nòng cốt trong bảo vệ an ninh quốc gia trên không gian mạng. Việc trực tiếp tham gia ứng phó sự cố không chỉ bảo đảm hoạt động liên tục của Trung tâm dữ liệu quốc gia mà còn củng cố niềm tin của các bộ, ngành, địa phương và doanh nghiệp khi chia sẻ, kết nối dữ liệu về Trung tâm. Có thể khẳng định rằng, với năng lực và kinh nghiệm của lực lượng an ninh mạng, Bộ Công an đang giữ vai trò “lá chắn thép” bảo vệ dữ liệu quốc gia, bảo đảm tính toàn vẹn, sẵn sàng và bí mật của hệ thống dữ liệu trong kỷ nguyên số.



*Quang cảnh buổi Diễn tập thực chiến đảm bảo an toàn thông tin mạng, ứng cứu sự cố tỉnh Ninh Bình năm 2025 - Ảnh: Đỗ Hùng*





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

*Kinh nghiệm quốc tế cho thấy, các nước đều đặt nhiệm vụ ứng phó sự cố dữ liệu ở vị trí trung tâm. Tại Liên minh châu Âu, Cơ quan An ninh mạng EU (ENISA) giữ vai trò điều phối ứng phó sự cố xuyên biên giới và ban hành chuẩn an ninh cho hạ tầng dữ liệu trọng yếu, thông qua công cụ pháp lý chung như “Chỉ thị NIS2”. Ở Mỹ, Cơ quan An ninh mạng và an ninh hạ tầng (CISA) là cơ quan trung tâm bảo đảm an ninh mạng, trực tiếp điều phối các đội US-CERT ứng cứu sự cố đối với hạ tầng dữ liệu và thông tin trọng yếu. Singapore cũng xây dựng Cơ quan An ninh mạng quốc gia (CSA) để điều phối và bảo đảm an ninh cho các hạ tầng thông tin trọng yếu, trong đó có các nền tảng dữ liệu Chính phủ như Government Data Hub do GovTech vận hành. CSA vừa ban hành chuẩn an ninh mạng, vừa phối hợp điều phối ứng phó sự cố, qua đó bảo đảm tính an toàn và liên tục cho việc chia sẻ, khai thác dữ liệu công. Việc Bộ Công an Việt Nam được giao vai trò điều phối ứng phó sự cố tại Trung tâm Dữ liệu quốc gia thể hiện sự tiệm cận xu hướng quốc tế, đồng thời khẳng định quyết tâm xây dựng “lá chắn số” bảo vệ chủ quyền dữ liệu.*

**Thứ chín,** phổ biến pháp luật và hoàn thiện thể chế quản trị dữ liệu.

Ngoài các nhiệm vụ chuyên môn, Bộ Công an còn có trách nhiệm tuyên truyền, phổ biến pháp luật và tham mưu hoàn thiện thể chế trong lĩnh vực dữ liệu. Khoản 2, Điều 40 Nghị định 169/2025/NĐ-CP quy định Bộ Công an có trách nhiệm: “*Phổ biến, tuyên truyền, giáo dục pháp luật trong lĩnh vực quản lý chuyên ngành có liên quan đến hoạt động khoa học, công nghệ và đổi mới sáng tạo và sản phẩm, dịch vụ về dữ liệu thuộc phạm vi quản lý*”. Cũng tại khoản 5 điều này, Bộ Công an có trách nhiệm ban hành theo thẩm quyền và kiến nghị, đề xuất sửa đổi, bổ sung, hoàn thiện các văn bản quy phạm pháp luật trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ về dữ liệu.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



***Minh họa về tuyên truyền, phổ biến pháp luật -  
Ảnh: Cổng thông tin điện tử Công an tỉnh Hà Tĩnh***

Ngay sau khi Luật Dữ liệu được ban hành, Bộ Công an đã chỉ đạo các đơn vị chức năng tổ chức phổ biến rộng rãi nội dung luật và các văn bản hướng dẫn đến cán bộ, chiến sĩ trong toàn lực lượng cũng như các cơ quan, tổ chức và người dân. Nhiều hội nghị, hội thảo đã được Bộ tổ chức, chẳng hạn Hội nghị triển khai thi hành Luật Dữ liệu tại Công an Thành phố Hà Nội vào tháng 7 năm 2025, nhằm quán triệt quy định mới cho đội ngũ cán bộ và thực hiện công tác tuyên truyền, phổ biến pháp luật ra toàn xã hội.

Song song đó, Bộ Công an chủ động rà soát, đề xuất xây dựng mới hoặc sửa đổi, bổ sung các văn bản quy phạm pháp luật để hoàn thiện khung pháp lý về dữ liệu. Thực tế cho thấy Bộ Công an đã thể hiện sự chủ động trong lĩnh vực này qua việc soạn thảo Luật Dữ liệu năm 2024. Dự án luật do Bộ Công an chủ trì xây dựng đã được Quốc hội thông qua với đa số phiếu tán thành, đánh dấu lần đầu tiên Việt Nam ban hành một đạo luật toàn diện về





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

dữ liệu. Không dừng ở đó, sau khi Luật Dữ liệu được thông qua, Bộ Công an tiếp tục soạn thảo các nghị định hướng dẫn thi hành luật, trình Chính phủ ban hành đồng bộ vào giữa năm 2025. Tiêu biểu, là Nghị định số 165/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu; Nghị định số 169/2025/NĐ-CP về hoạt động khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ về dữ liệu; Nghị định số 160/2025/NĐ-CP về Quỹ phát triển Dữ liệu quốc gia... Việc kịp thời ban hành đồng loạt các văn bản dưới luật này (đều có dấu ấn chủ trì, soạn thảo của Bộ Công an) đã đảm bảo Luật Dữ liệu được triển khai *thống nhất, đồng bộ, sát với thực tiễn* ngay từ khi có hiệu lực vào 01/07/2025.

Như vậy, với vị trí là cơ quan đầu mối, Bộ Công an giữ vai trò chủ quản toàn diện đối với công tác quản lý nhà nước trên lĩnh vực dữ liệu: từ hoạch định chiến lược, xây dựng hạ tầng, ban hành tiêu chuẩn kỹ thuật, cấp phép kinh doanh, thanh tra, giám sát cho đến hợp tác quốc tế và phát triển nhân lực về dữ liệu. Tất cả các nỗ lực này đều nhằm hướng tới mục tiêu xây dựng một nền kinh tế số, xã hội số an toàn, lành mạnh dựa trên khai thác dữ liệu hiệu quả. Luật Dữ liệu được ban hành đã đặt nền móng cho niềm tin số - yếu tố cốt lõi để phát triển Chính phủ số và xã hội số an toàn. Người dân và doanh nghiệp có thể an tâm khi tham gia các hoạt động chuyển đổi số, vì dữ liệu, thứ được ví như “*dòng máu*” của nền kinh tế số, đã có hành lang pháp lý bảo vệ và cơ quan chuyên trách đủ mạnh để quản lý. Có thể khẳng định rằng, Việt Nam đang dần hình thành một hệ sinh thái dữ liệu quốc gia vừa mở và sáng tạo, vừa an ninh và bền vững, tạo động lực cho chuyển đổi số và phát triển kinh tế, xã hội trong kỷ nguyên mới.

**Thứ mười**, quyết định mức chi hỗ trợ kinh phí cho hoạt động kết nối, chia sẻ và tạo lập dữ liệu.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Một điểm mới và quan trọng của Nghị định số 165/2025/NĐ-CP là trao cho Bộ trưởng Bộ Công an thẩm quyền “*quyết định mức chi cho hoạt động hỗ trợ kinh phí, bảo đảm kết nối, chia sẻ; hỗ trợ bù đắp chi phí tạo lập, thu thập dữ liệu trên cơ sở thống nhất với Bộ trưởng Bộ Tài chính, Bộ trưởng Bộ Khoa học và Công nghệ* (Điều 26, khoản 13). Đây là cơ chế tài chính đặc thù, phản ánh nhận thức rằng xây dựng và vận hành Trung tâm Dữ liệu quốc gia không thể chỉ dựa vào hạ tầng kỹ thuật, mà cần đi kèm một cơ chế *phân bổ nguồn lực công bằng, minh bạch và bền vững*.

Quy định này xác lập Bộ Công an vừa là cơ quan điều phối dữ liệu, vừa là *đầu mối phân bổ hỗ trợ tài chính* cho các bộ, ngành, địa phương khi tham gia kết nối dữ liệu về Trung tâm Dữ liệu quốc gia. Việc gắn thẩm quyền tài chính với thẩm quyền quản lý dữ liệu giúp tránh tình trạng “*quyền quản lý một nơi, quyền chi một nơi*”, qua đó tăng tính hiệu lực của chính sách. Đồng thời, yêu cầu thống nhất với Bộ Tài chính và Bộ Khoa học và Công nghệ thể hiện nguyên tắc phối hợp liên ngành, bảo đảm vừa cân đối ngân sách, vừa gắn với mục tiêu phát triển khoa học - công nghệ.

*Tại Việt Nam*, trong bối cảnh nhiều địa phương, bộ ngành còn hạn chế về nguồn lực cho số hóa dữ liệu, việc Bộ Công an được giao quyền quyết định hỗ trợ kinh phí có ý nghĩa tháo gỡ khó khăn, khuyến khích các đơn vị mạnh dạn kết nối, chia sẻ dữ liệu. Cơ chế này cũng gắn với định hướng hình thành Quỹ Phát triển dữ liệu quốc gia theo Nghị định 160/2025/NĐ-CP - một quỹ tài chính nhà nước ngoài ngân sách nhằm bổ sung nguồn lực cho phát triển dữ liệu. Như vậy, Bộ Công an có thể sử dụng cả ngân sách thường xuyên và nguồn quỹ chuyên biệt để bảo đảm kinh phí vận hành hệ sinh thái dữ liệu quốc gia.





Về kinh nghiệm quốc tế, nhiều quốc gia đã triển khai cơ chế hỗ trợ tài chính cho hoạt động dữ liệu. Tại Liên minh châu Âu, Chương trình “Digital Europe 2021 - 2027” phân bổ hàng tỷ euro để hỗ trợ các nước thành viên xây dựng hạ tầng dữ liệu chung và trung tâm siêu máy tính. Hàn Quốc thành lập *Quỹ dữ liệu lớn (Big Data Fund)*, hỗ trợ doanh nghiệp và cơ quan công trong việc thu thập, chuẩn hóa và khai thác dữ liệu. Những mô hình này cho thấy việc thiết lập cơ chế tài chính bền vững là điều kiện tiên quyết để dữ liệu trở thành động lực phát triển kinh tế - xã hội.

Có thể khẳng định, trao thẩm quyền quyết định mức chi cho Bộ trưởng Bộ Công an không chỉ là một quy định kỹ thuật, mà còn là cam kết chính trị trong việc bảo đảm nguồn lực cho hạ tầng dữ liệu quốc gia. Đây là bước đi quan trọng nhằm hình thành một chu trình khép kín: *xây dựng - kết nối - vận hành - tài chính*, giúp hệ sinh thái dữ liệu quốc gia không chỉ bền vững về mặt công nghệ mà còn vững chắc về mặt tài chính. Qua đó góp phần xây dựng niềm tin số, thúc đẩy Chính phủ số, kinh tế số và xã hội số phát triển ổn định, an toàn.

### **8.2.2. Vai trò, trách nhiệm của Trung tâm dữ liệu quốc gia trong quản lý nhà nước về dữ liệu**

Với vai trò là một đơn vị cấp Cục trực thuộc Bộ Công an, Trung tâm dữ liệu quốc gia cũng có những vai trò, trách nhiệm nhất định (quy định tại Điều 21 Nghị định số 165/2025/NĐ-CP), cụ thể như sau:

- *Hướng dẫn cơ quan, tổ chức, cá nhân trong việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu thuộc phạm vi đồng bộ về Trung tâm dữ liệu quốc gia.*
- *Thực hiện các biện pháp giám sát, đánh giá chất lượng dữ liệu được chia sẻ, đồng bộ về Trung tâm dữ liệu quốc gia.*





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



***Thiếu tướng Nguyễn Ngọc Cương, Giám đốc Trung tâm Dữ liệu quốc gia phát biểu tại lễ phát động - Ảnh: Báo điện tử Công an nhân dân***

- Điều phối dữ liệu của Cơ sở dữ liệu tổng hợp quốc gia.
- Thực hiện các biện pháp bảo vệ dữ liệu được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu theo quy định tại khoản 6 Điều 16 Nghị định này.
- Thực hiện ký kết các thỏa thuận, biên bản ghi nhớ với các cơ quan, tổ chức quốc tế để thúc đẩy hợp tác quốc tế trong quản lý, bảo vệ dữ liệu, nghiên cứu khoa học, chuyển giao dữ liệu xuyên biên giới, đào tạo, nâng cao năng lực, trình độ về các nội dung liên quan đến dữ liệu nhằm thúc đẩy các hoạt động đổi mới sáng tạo, chuyển giao công nghệ phục vụ phát triển kinh tế - xã hội.
- Giúp Bộ Công an thực hiện quản lý nhà nước về dữ liệu.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Từ quy định trên, có thể thấy rằng, Trung tâm dữ liệu quốc gia là đơn vị giữ vai trò then chốt trong quản lý, điều phối và bảo vệ dữ liệu quốc gia. Đây không chỉ là cơ quan kỹ thuật thuần túy, mà còn là “trụ cột” tham mưu và triển khai chiến lược về dữ liệu trong phạm vi cả nước.

Trung tâm Dữ liệu quốc gia có trách nhiệm hướng dẫn các cơ quan, tổ chức, cá nhân áp dụng thống nhất tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu, bảo đảm dữ liệu được đồng bộ, liên thông, dễ dàng tích hợp vào hệ thống quốc gia. Đây là cơ sở để khắc phục tình trạng phân tán, manh mún trong quản lý dữ liệu và thúc đẩy hình thành hạ tầng dữ liệu thống nhất.

Bên cạnh đó, Trung tâm trực tiếp giám sát và đánh giá chất lượng dữ liệu được chia sẻ, đồng bộ về hệ thống, nhằm bảo đảm tính chính xác, toàn vẹn và kịp thời của dữ liệu. Chức năng này giúp nâng cao độ tin cậy của các cơ sở dữ liệu quốc gia, phục vụ hiệu quả cho công tác quản lý nhà nước, hoạch định chính sách cũng như cung cấp dịch vụ công trực tuyến.



***Khu vực “Khám phá Trái tim số” của Trung tâm Dữ liệu Quốc gia tại  
Triển lãm 80 năm thành tựu đất nước - Ảnh: Báo Nhân dân***





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Một nhiệm vụ trọng tâm khác là điều phối dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia, đóng vai trò “*cầu nối*” giữa các bộ, ngành, địa phương trong việc chia sẻ, khai thác dữ liệu, đồng thời bảo đảm nguyên tắc minh bạch, công bằng và an toàn. Song song, Trung tâm còn có trách nhiệm áp dụng các biện pháp bảo vệ dữ liệu ngay từ giai đoạn thiết kế và trong suốt vòng đời xử lý dữ liệu, từ khâu thu thập đến khai thác, phù hợp với yêu cầu tại khoản 6 Điều 16 Nghị định số 165/2025/NĐ-CP.

*Ở tầm quốc tế*, Trung tâm là đầu mối ký kết các thỏa thuận, biên bản ghi nhớ với cơ quan, tổ chức nước ngoài nhằm thúc đẩy hợp tác trong quản lý, bảo vệ dữ liệu, chuyển giao công nghệ, nghiên cứu khoa học và đào tạo nhân lực. Qua đó, Việt Nam vừa tranh thủ được nguồn lực quốc tế cho phát triển kinh tế - xã hội, vừa nâng cao năng lực bảo vệ an ninh dữ liệu quốc gia.

Ngoài ra, Trung tâm còn có vai trò giúp Bộ Công an thực hiện quản lý nhà nước về dữ liệu, từ xây dựng thể chế, giám sát thực thi, đến điều phối hoạt động dữ liệu trên phạm vi toàn quốc. Như vậy, Trung tâm dữ liệu quốc gia không chỉ là cơ quan kỹ thuật thuần túy, mà còn là công cụ quản lý chiến lược, góp phần xây dựng hệ sinh thái dữ liệu thống nhất, an toàn, minh bạch, phục vụ phát triển đất nước và bảo đảm quốc phòng - an ninh trong kỷ nguyên số.

Mặc dù được xác định là đơn vị đầu mối chiến lược trong quản lý nhà nước về dữ liệu, Trung tâm dữ liệu quốc gia vẫn đối diện với nhiều thách thức lớn trong quá trình triển khai nhiệm vụ.

**Thứ nhất**, nguy cơ chồng chéo thẩm quyền. Với vai trò điều phối, giám sát và bảo vệ dữ liệu, Trung tâm có thể gặp khó khăn khi phối hợp với các bộ,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

ngành, địa phương vốn đang trực tiếp quản lý các cơ sở dữ liệu chuyên ngành. Nếu không có cơ chế phối hợp chặt chẽ, minh bạch, tình trạng “cát cứ dữ liệu” hoặc mâu thuẫn về quyền quản lý, chia sẻ thông tin rất dễ xảy ra.



***Thiếu tướng Nguyễn Ngọc Cương,***

***Giám đốc Trung tâm Dữ liệu quốc gia - Ảnh: VOV***

***Thứ hai,*** thách thức từ hạ tầng kỹ thuật. Khối lượng dữ liệu quốc gia ngày càng lớn, đa dạng và phức tạp, đòi hỏi hạ tầng lưu trữ, xử lý, kết nối phải hiện đại, bảo mật nhiều lớp và có khả năng mở rộng linh hoạt. Trong khi đó, việc đầu tư đồng bộ, chuẩn hóa kiến trúc dữ liệu quốc gia vẫn còn hạn chế, đặc biệt là sự khác biệt giữa các bộ, ngành và địa phương.

***Thứ ba,*** áp lực từ an ninh mạng và tội phạm công nghệ cao. Trung tâm dữ liệu quốc gia chắc chắn sẽ là mục tiêu tấn công của tin tặc và các thế lực





thù địch. Các hình thức tấn công mạng hiện nay ngày càng tinh vi, từ tấn công DDoS, mã độc tống tiền (ransomware), cho tới cài cắm gián điệp mạng, đòi hỏi Trung tâm phải liên tục nâng cấp công nghệ phòng thủ và duy trì khả năng ứng cứu khẩn cấp.

**Thứ tư,** vấn đề nhân lực chất lượng cao. Quản trị và bảo vệ dữ liệu quốc gia không chỉ cần cán bộ có trình độ công nghệ thông tin mà còn đòi hỏi kiến thức liên ngành về pháp luật, an ninh, kinh tế - xã hội và hợp tác quốc tế. Tuy nhiên, đội ngũ nhân sự chuyên sâu trong lĩnh vực này ở Việt Nam hiện vẫn còn mỏng và phân tán, khó đáp ứng kịp yêu cầu thực tiễn.

**Thứ năm,** thách thức từ hợp tác quốc tế. Trong bối cảnh toàn cầu hóa dữ liệu, Trung tâm cần ký kết, triển khai nhiều thỏa thuận hợp tác quốc tế. Tuy nhiên, vấn đề đặt ra là phải vừa tranh thủ công nghệ và kinh nghiệm tiên tiến, vừa bảo đảm chủ quyền số, bí mật nhà nước, không để các yếu tố bên ngoài chi phối. Đây là bài toán khó đòi hỏi cơ chế sàng lọc, lựa chọn đối tác hết sức cẩn trọng.

Tóm lại, Trung tâm dữ liệu quốc gia là đơn vị đầu mối chiến lược, giữ vai trò trung tâm trong việc bảo đảm an ninh, an toàn dữ liệu, điều phối Cơ sở dữ liệu tổng hợp quốc gia, kết nối và liên thông dữ liệu giữa các chủ thể, đồng thời mở rộng hợp tác quốc tế để nâng cao năng lực quản trị dữ liệu quốc gia. Đây chính là nền tảng để xây dựng một hệ sinh thái dữ liệu thống nhất, an toàn, phục vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh và khẳng định chủ quyền số của Việt Nam.





### **8.3. NHIỆM VỤ TRỌNG TÂM CẦN TẬP TRUNG TRONG GIAI ĐOẠN TỪ NAY ĐẾN NĂM 2030 ĐỂ NÂNG CAO HIỆU QUẢ CÔNG TÁC QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU**

#### **8.3.1. Bối cảnh và sự cần thiết nâng cao hiệu quả quản lý nhà nước về dữ liệu đến năm 2030**

##### **8.3.1.1. Bối cảnh chuyển đổi số toàn cầu và trong nước**

*T*rong những thập kỷ gần đây, thế giới chứng kiến sự bùng nổ của cách mạng số và sự lan tỏa mạnh mẽ của dữ liệu số trong mọi lĩnh vực. Dữ liệu đã được ví như “*dầu mỏ mới*” của nền kinh tế số toàn cầu - một loại tài nguyên đầu vào không thể thiếu cho hoạt động của mọi chủ thể từ Chính phủ đến doanh nghiệp.

Theo *MIT Technology Review*, tổng lượng dữ liệu được tạo ra toàn cầu dự báo đạt khoảng 175 zettabyte vào năm 2025 (1 zettabyte tương đương  $10^{21}$  byte), với dữ liệu doanh nghiệp tăng trung bình 42% mỗi năm. Song song đó, các công nghệ tiên tiến như trí tuệ nhân tạo (AI), Internet vạn vật (IoT) đang ngày càng tối ưu hóa việc khai thác dữ liệu, tạo ra những đột phá trong sản xuất và quản lý trên thế giới. Nhiều quốc gia đã sớm ban hành khung pháp lý để quản lý và khai thác dữ liệu hiệu quả, coi dữ liệu là tài sản chiến lược của quốc gia. Chẳng hạn, Liên minh châu Âu (EU) đã ban hành Chỉ thị về dữ liệu mở, yêu cầu công bố miễn phí các tập dữ liệu có giá trị cao để phục vụ phát triển trí tuệ nhân tạo, và một số nước như Mexico, Hàn Quốc đã có luật riêng về dữ liệu mở; các nước khác như Pháp, Estonia, Anh cũng đã đưa quy định về dữ liệu mở vào pháp luật của chính phủ. Những động thái này cho thấy xu thế tất yếu: *quản trị và khai thác dữ liệu hiệu quả đã trở thành một yêu cầu khách quan để tăng cường năng lực cạnh tranh quốc gia trong bối cảnh chuyển đổi số toàn cầu.*





## ***Chuyển đổi số tác động mạnh mẽ đến kinh tế toàn cầu - Ảnh: Internet***

Tại Việt Nam, chuyển đổi số được Đảng và Nhà nước xác định là yêu cầu chiến lược, vừa cấp bách vừa lâu dài để phát triển đất nước. Bộ Chính trị đã ban hành Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư, nhấn mạnh cần tận dụng hiệu quả cơ hội của chuyển đổi số nhằm nâng cao năng suất, hiệu quả, sức cạnh tranh của nền kinh tế, đồng thời nâng cao hiệu lực, hiệu quả quản lý xã hội. Trên cơ sở đó, Chính phủ đã triển khai Chương trình Chuyển đổi số quốc gia đến 2025, định hướng 2030 (Quyết định 749/QĐ-TTg ngày 03/6/2020) và Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số 2021 - 2025, định hướng 2030 (Quyết định 942/QĐ-TTg ngày 15/6/2021). Những chương trình chiến lược này đặt ra mục tiêu đưa Việt Nam nằm trong nhóm dẫn đầu khu vực về chính phủ điện tử, hoàn thành nền tảng Chính phủ số vào năm 2030, coi chuyển đổi số là động lực phát triển mới. Đáng chú ý, năm 2023 được Ủy ban Quốc gia về Chuyển đổi số chọn là “Năm Dữ liệu số quốc gia”, tập trung vào các sáng kiến về dữ liệu:





bảo vệ dữ liệu cá nhân, xây dựng và kết nối các cơ sở dữ liệu, mở dữ liệu để chia sẻ, bảo đảm an toàn dữ liệu và xây dựng các trung tâm dữ liệu lớn quốc gia. Việc lựa chọn dữ liệu số làm trọng tâm cho thấy quyết tâm của Việt Nam trong việc tận dụng dữ liệu phục vụ phát triển kinh tế, xã hội và hiện đại hóa quản trị quốc gia trong kỷ nguyên số.

### **8.3.1.2. Vai trò của dữ liệu trong phát triển kinh tế - xã hội và quản lý nhà nước**

Dữ liệu ngày nay được coi là yếu tố cốt lõi quyết định thành công của phát triển kinh tế số và nâng cao năng lực quản trị quốc gia. Từ góc độ kinh tế, dữ liệu mở ra những cơ hội to lớn để đổi mới sáng tạo, nâng cao năng suất lao động và hình thành nên các mô hình kinh doanh hoàn toàn mới. Báo cáo của Ngân hàng Thế giới chỉ ra rằng dữ liệu mở có thể đóng góp 0,4 - 1,4% GDP toàn cầu (năm 2021) và dự kiến mang lại giá trị từ 2,8 nghìn tỷ USD (năm 2019) lên đến 10 nghìn tỷ USD vào năm 2025 cho kinh tế thế giới [38].

Dữ liệu không còn chỉ là công cụ hỗ trợ ra quyết định, mà đã trở thành tư liệu sản xuất quan trọng của thời đại số. Đảng và Nhà nước ta luôn nhấn mạnh quan điểm “*dữ liệu là tài nguyên chiến lược*”, là “*khoáng sản quý*” của thế kỷ 21, có thể khai thác để tạo ra tri thức và của cải mới cho xã hội. Chẳng hạn, dữ liệu về “thị trường, khách hàng” khi được phân tích sẽ giúp doanh nghiệp dự báo xu hướng và tối ưu hóa hoạt động sản xuất kinh doanh; dữ liệu lớn khi được xử lý có thể nhân lên nhiều lần giá trị, hình thành nên “*kinh tế dữ liệu*” như một lĩnh vực kinh tế mới song hành cùng kinh tế số.

Đối với quản lý nhà nước, dữ liệu đóng vai trò nền tảng để xây dựng chính phủ điện tử, chính phủ số hướng tới quản lý dựa trên bằng chứng (evidence-based policymaking). Việc ra quyết định dựa trên dữ liệu giúp các cơ quan công quyền phân tích toàn diện, khách quan các vấn đề kinh tế - xã





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

hội, từ đó hoạch định chính sách hiệu quả hơn. Những người lãnh đạo ở cả khu vực công và tư hiện nay đều dựa nhiều vào phân tích dữ liệu để đưa ra quyết định. Chính phủ có thể phân bổ nguồn lực hợp lý dựa trên số liệu thống kê dân số, kinh tế; đánh giá chính sách bằng phân tích chi phí - lợi ích dựa trên dữ liệu; đồng thời theo dõi kịp thời hiệu quả cung cấp dịch vụ công thông qua các hệ thống dữ liệu phản hồi từ người dân.



***Hình ảnh mô phỏng dữ liệu truyền trong cáp quang - Ảnh: Internet***

Ngoài ra, dữ liệu mở do các cơ quan nhà nước cung cấp cũng trở thành đòn bẩy cho phát triển kinh tế và cải thiện quản trị. Theo Ngân hàng Thế giới, dữ liệu mở không chỉ thúc đẩy tăng trưởng kinh tế mà còn nâng cao hiệu quả điều hành của chính phủ, cho phép chính quyền minh bạch hơn và người dân tham gia giám sát tốt hơn. Thực tiễn quốc tế cho thấy, nhiều quốc gia đã ứng dụng dữ liệu mở để cải thiện dịch vụ công và tạo cơ hội kinh doanh mới. Ví dụ, một nửa số doanh nghiệp tại Hoa Kỳ (đặc biệt là doanh nghiệp vừa và nhỏ) hiện đang sử dụng dữ liệu mở của chính phủ, qua đó tiết kiệm chi phí và tìm kiếm cơ hội thị trường mới [38]. Kết luận rằng dữ liệu không chỉ là nguồn





lực cho phát triển kinh tế - xã hội, mà còn là công cụ để Nhà nước quản lý hiệu quả hơn, hướng tới một nền quản trị thông minh và minh bạch.

### **8.3.1.3. Thực trạng công tác quản lý nhà nước về dữ liệu ở Việt Nam**

Nhận thức được vai trò quan trọng của dữ liệu, Việt Nam đã bước đầu xây dựng các Cơ sở dữ liệu quốc gia làm nền tảng cho Chính phủ điện tử. Theo Nghị định số 47/2024/NĐ-CP ngày 09/5/2024 về danh mục cơ sở dữ liệu quốc gia; việc xây dựng, cập nhật, duy trì, khai thác và sử dụng cơ sở dữ liệu quốc gia, hiện nay Việt Nam có 10 cơ sở dữ liệu quốc gia bao gồm:

- (1) Cơ sở dữ liệu quốc gia về dân cư;
- (2) Cơ sở dữ liệu quốc gia về đất đai;
- (3) Cơ sở dữ liệu quốc gia về đăng ký doanh nghiệp;
- (4) Cơ sở dữ liệu quốc gia về tài chính;
- (5) Cơ sở dữ liệu quốc gia về bảo hiểm;
- (6) Cơ sở dữ liệu quốc gia về cán bộ, công chức, viên chức trong các cơ quan nhà nước;
- (7) Cơ sở dữ liệu quốc gia về thủ tục hành chính;
- (8) Cơ sở dữ liệu tổng hợp quốc gia;
- (9) Cơ sở dữ liệu quốc gia về hoạt động xây dựng;
- (10) Cơ sở dữ liệu quốc gia về xuất nhập cảnh.

Hạ tầng công nghệ cho dữ liệu như các trung tâm dữ liệu cũng bắt đầu được quan tâm đầu tư, chẳng hạn như Trung tâm Dữ liệu quốc gia do Bộ Công an xây dựng, quản lý, khai thác và vận hành nhằm thực hiện việc tích hợp, đồng bộ, lưu trữ, chia sẻ, phân tích, khai thác, điều phối dữ liệu của các cơ quan nhà nước theo quy định của pháp luật nhằm hình thành kho dữ liệu về con người và kho dữ liệu tổng hợp từ các cơ sở dữ liệu





quốc gia. Tuy nhiên, nhìn chung hiệu quả quản lý và khai thác dữ liệu của nước ta còn nhiều hạn chế, chưa đáp ứng yêu cầu của chuyển đổi số. Thực tế cho thấy tình trạng phân tán, cục bộ trong quản lý dữ liệu: nhiều bộ, ngành và địa phương tự xây dựng cơ sở dữ liệu riêng nhưng chưa kết nối liên thông, dẫn đến dữ liệu trùng lặp, chồng chéo và thiếu đồng bộ về tiêu chuẩn kỹ thuật. Chẳng hạn, có hiện tượng cùng một loại dữ liệu nhưng do nhiều cơ quan thu thập riêng rẽ, gây lãng phí nguồn lực và khó khăn khi tổng hợp phục vụ ra quyết định. Chất lượng dữ liệu tại không ít hệ thống còn chưa được chuẩn hóa, làm sạch, gây cản trở cho việc khai thác phân tích chuyên sâu.

Bên cạnh đó, vấn đề an ninh, an toàn dữ liệu đang nổi lên như một thách thức lớn. Khi chuyển đổi hoạt động lên môi trường số, các nguy cơ tấn công mạng, rò rỉ dữ liệu cá nhân ngày càng gia tăng, trong khi nhiều cơ quan, tổ chức ở Việt Nam chưa có hệ thống bảo mật đủ mạnh. Công tác quản trị dữ liệu tại nhiều nơi còn yếu, minh chứng qua việc một lượng lớn dữ liệu của người Việt Nam đang nằm trên các nền tảng công nghệ nước ngoài. Theo Hiệp hội Internet Việt Nam, có tới 80% tài nguyên dữ liệu số của Việt Nam “đang ở nước ngoài” trên các hệ thống của doanh nghiệp ngoại quốc. Điều này đặt ra lo ngại về chủ quyền số và khả năng tự chủ trong khai thác tài nguyên dữ liệu quốc gia. Ngoài ra, chuyên gia về phân tích, quản trị dữ liệu chất lượng cao còn thiếu hụt trầm trọng, dẫn đến nhiều cơ quan dù có hệ thống thông tin hiện đại nhưng vận hành chưa hiệu quả. Tất cả những hạn chế, thách thức này đòi hỏi Việt Nam phải sớm có giải pháp đồng bộ để kiện toàn quản lý nhà nước về dữ liệu, phát huy tối đa giá trị của dữ liệu trong phát triển đất nước.





## **8.3.1.4. Một số mục tiêu chính đến năm 2030 trong các chiến lược, văn kiện quốc gia về dữ liệu**

Nhằm khắc phục những hạn chế và tận dụng cơ hội từ chuyển đổi số, Chính phủ đã ban hành **Chiến lược dữ liệu quốc gia đến năm 2030** (Quyết định số 142/QĐ-TTg ngày 02/02/2024) với tầm nhìn xây dựng hệ sinh thái dữ liệu số đồng bộ, kết nối thông suốt trên phạm vi toàn quốc. Chiến lược đã đề ra hàng loạt mục tiêu cụ thể đến năm 2030 nhằm nâng cao hạ tầng và quản trị dữ liệu quốc gia. Về hạ tầng dữ liệu, phấn đấu 100% các Trung tâm dữ liệu quốc gia, vùng và các trung tâm dữ liệu lớn được kết nối thành mạng lưới thống nhất, chia sẻ năng lực tính toán và lưu trữ phục vụ phát triển kinh tế - xã hội. Nền tảng điện toán đám mây Chính phủ và các nền tảng số “*Make in Vietnam*” sẽ đáp ứng **100% nhu cầu** lưu trữ, kết nối, chia sẻ dữ liệu trong các cơ quan nhà nước, đồng thời bảo đảm an toàn, an ninh mạng cho hệ thống dữ liệu quốc gia.

Về phát triển dữ liệu cho Chính phủ số, mục tiêu đến 2030 hoàn thành số hóa và vận hành hiệu quả tất cả các cơ sở dữ liệu quốc gia thuộc danh mục ưu tiên; bảo đảm các cơ sở dữ liệu này kết nối thông suốt với Trung tâm Dữ liệu quốc gia và chia sẻ trên phạm vi toàn quốc. Đặc biệt, chiến lược nhấn mạnh yêu cầu mở dữ liệu để phục vụ xã hội: 100% các bộ, ngành ở trung ương và Ủy ban nhân dân cấp tỉnh phải mở và cung cấp dữ liệu mở đảm bảo chất lượng, được khai thác sử dụng hiệu quả. Dữ liệu mở từ các cơ quan nhà nước phải sẵn sàng hỗ trợ cho điều hành, hoạch định chính sách cũng như phát triển các ứng dụng trí tuệ nhân tạo phục vụ kinh tế số, xã hội số. Song song, 100% hồ sơ và kết quả giải quyết thủ tục hành chính sẽ được số hóa; tối thiểu 80% dữ liệu từ quá trình xử lý thủ tục hành chính được **tái sử dụng, chia sẻ**, bảo đảm người dân và doanh nghiệp “chỉ cung cấp thông





tin một lần” khi thực hiện dịch vụ công trực tuyến. Những mục tiêu này thể hiện quyết tâm rất cao của Việt Nam trong việc hiện đại hóa quản lý nhà nước về dữ liệu vào năm 2030.



*Bộ Thông tin và Truyền thông (cũ) trao chứng nhận cho đại diện 5 doanh nghiệp có nền tảng đám mây Make in Vietnam đạt tiêu chuẩn - Ảnh: VnEconomy*

Bên cạnh Chiến lược dữ liệu quốc gia, nhiều chiến lược khác của Việt Nam cũng đề ra các mục tiêu liên quan đến dữ liệu và chuyển đổi số cho giai đoạn đến 2030. Chiến lược quốc gia phát triển kinh tế số và xã hội số (Quyết định 411/QĐ-TTg ngày 31/3/2022) xác định các chỉ tiêu như: tỷ trọng kinh tế số đạt 30% GDP vào năm 2030; tỷ lệ doanh nghiệp sử dụng dữ liệu số và tham gia thị trường dữ liệu tăng mạnh; hạ tầng số phủ khắp phục vụ kết nối và xử lý dữ liệu ở mọi vùng miền. Nghị quyết Đại hội Đảng XIII (2021) cũng nhấn mạnh mục tiêu đến 2030 hoàn thành xây dựng Chính phủ số, hình thành các đô thị thông minh kết nối với khu vực và thế giới. Để hỗ trợ cho những mục tiêu này, các văn kiện đặt trọng tâm vào việc phát triển nguồn nhân lực số, đảm bảo an ninh dữ liệu, và xây dựng thị trường dữ





liệu an toàn, lành mạnh. Chẳng hạn, Nghị quyết 52-NQ/TW yêu cầu xây dựng cơ chế thử nghiệm có kiểm soát (sandbox) để tạo điều kiện cho các công nghệ và dịch vụ dữ liệu mới phát triển, đồng thời tăng cường hợp tác quốc tế, học hỏi kinh nghiệm các nước trong quản trị dữ liệu. Gần đây nhất, Luật Dữ liệu năm 2024 (số 60/2024/QH15, có hiệu lực từ 1/7/2025) đã được Quốc hội thông qua nhằm tạo hành lang pháp lý cao nhất, thống nhất cho quản lý, phát triển, chia sẻ và bảo vệ dữ liệu. Luật Dữ liệu 2024 đặt nền móng cho việc thiết lập Trung tâm Dữ liệu Quốc gia, xác định rõ quyền sở hữu dữ liệu, quyền và trách nhiệm của các chủ thể dữ liệu, cũng như thúc đẩy hình thành thị trường dữ liệu tại Việt Nam. Có thể nói, đến năm 2030, Việt Nam hướng tới một nền quản trị dữ liệu tiên tiến, nơi dữ liệu được quản lý tập trung, đồng bộ, khai thác hiệu quả để đạt các mục tiêu phát triển kinh tế - xã hội và bảo đảm an ninh quốc gia trong kỷ nguyên số.

#### ***8.3.1.5. Vì sao phải nâng cao hiệu quả quản lý nhà nước về dữ liệu?***

Từ bối cảnh và hiện trạng phân tích ở trên, việc nâng cao hiệu lực, hiệu quả quản lý nhà nước về dữ liệu ở Việt Nam không chỉ là cần thiết mà còn hết sức cấp bách trong giai đoạn hiện nay.

**Thứ nhất**, dữ liệu đã và đang trở thành tài nguyên đặc biệt quý giá của quốc gia trong thời đại số. Nếu không được quản lý tốt, tài nguyên này sẽ bị lãng phí, thậm chí thất thoát ra nước ngoài, khiến Việt Nam mất đi lợi thế cạnh tranh về dữ liệu. Như Thủ tướng Chính phủ Phạm Minh Chính nhấn mạnh, “dữ liệu là tài nguyên quý của quốc gia cần khai thác, phát huy để trở thành nguồn lực, động lực phát triển trong kỷ nguyên số”. Theo Luật Dữ liệu 2024, Nhà nước có trách nhiệm xây dựng và ban hành chính sách, tiêu chuẩn, quy chuẩn kỹ thuật để quản lý, khai thác dữ liệu một cách hợp pháp, tối ưu giá trị và phục vụ phát triển kinh tế - xã hội. Do đó, công tác quản lý





nhà nước về dữ liệu khi được triển khai hiệu quả sẽ đảm bảo dữ liệu được khai thác một cách đúng hướng, hợp pháp và tối ưu giá trị, phục vụ thiết thực cho người dân, doanh nghiệp và nền kinh tế.

**Thứ hai**, việc quản lý nhà nước về dữ liệu hiệu quả là điều kiện tiên quyết để thực hiện thành công các mục tiêu chuyển đổi số quốc gia đến 2030. Mục tiêu xây dựng Chính phủ số, phát triển kinh tế số 30% GDP hay cung cấp 100% dịch vụ công trực tuyến đều phụ thuộc lớn vào việc Nhà nước thiết lập khung pháp lý và cơ chế chia sẻ dữ liệu thống nhất. Thực tiễn cho thấy, nếu công tác quản lý nhà nước không bảo đảm tính kết nối và liên thông, các hệ thống thông tin sẽ hoạt động rời rạc, gây lãng phí nguồn lực. Ngược lại, khi Nhà nước áp dụng mô hình quản lý tập trung, ban hành quy chuẩn kỹ thuật và yêu cầu kết nối dữ liệu giữa các bộ, ngành, địa phương, sẽ hình thành hạ tầng dữ liệu quốc gia đồng bộ, đáp ứng yêu cầu ra quyết định nhanh và chính xác. Một báo cáo của Bộ Công an tại phiên họp thẩm định Luật Dữ liệu đã chỉ rõ: hiện nay nhiều trung tâm dữ liệu của các bộ ngành “*đầu tư thiếu đồng bộ, không bảo đảm tiêu chuẩn an ninh, an toàn, không được bảo trì nâng cấp thường xuyên*”, dẫn đến hiệu quả thấp. Do vậy, cần sớm kiện toàn thể chế và hạ tầng để khắc phục tình trạng này, tạo nền tảng dữ liệu quốc gia vững chắc đạt chuẩn, làm xương sống cho Chính phủ số.

**Thứ ba**, tăng cường hiệu quả quản lý nhà nước về dữ liệu là cần thiết để bảo vệ người dân và chủ quyền quốc gia trong không gian số. Khi dữ liệu ngày càng gắn bó với mọi mặt đời sống, chính phủ cần có năng lực quản lý tốt để bảo vệ dữ liệu cá nhân, ngăn chặn việc sử dụng dữ liệu sai mục đích, đồng thời đảm bảo an ninh mạng trước các mối đe dọa mới. Thực tế những năm qua, đã có nhiều vụ lộ lọt thông tin cá nhân và tấn công vào hệ thống thông tin quan trọng. Điều này đòi hỏi Nhà nước phải quản lý chặt chẽ quá





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

trình thu thập, lưu trữ, xử lý dữ liệu của các tổ chức, doanh nghiệp, cũng như ban hành các quy định pháp luật đủ mạnh để răn đe và xử lý vi phạm. Việc Quốc hội ban hành Luật dữ liệu trong bối cảnh hiện nay không chỉ cần thiết mà còn rất cấp bách để tạo hành lang pháp lý đồng bộ, thống nhất cho quản lý, khai thác, chia sẻ và kinh doanh dữ liệu. Nhờ đó, quyền lợi của người dân sẽ được bảo vệ tốt hơn trong môi trường số, đồng thời chủ quyền dữ liệu của Việt Nam được giữ vững trước sức ép từ các nền tảng công nghệ nước ngoài.

**Thứ tư**, quản lý nhà nước hiệu quả sẽ thúc đẩy việc hình thành thị trường dữ liệu và các ngành công nghiệp dữ liệu mới ở Việt Nam. Nhà nước đóng vai trò điều tiết, ban hành khung pháp lý và cơ chế giám sát để dữ liệu được lưu thông hợp pháp. Đồng thời, khi khung khổ quản lý rõ ràng, các doanh nghiệp sẽ mạnh dạn đầu tư vào các dịch vụ dữ liệu như môi giới, phân tích, lưu trữ dữ liệu, qua đó tạo công ăn việc làm và giá trị gia tăng mới cho nền kinh tế. Ngược lại, nếu không quản lý tốt, thị trường dữ liệu tự phát có thể dẫn đến lạm dụng dữ liệu, vi phạm quyền riêng tư và làm xói mòn niềm tin của công chúng. Những quốc gia có khung quản trị dữ liệu minh bạch, thuận lợi như Liên minh châu Âu với Data Governance Act đã thu hút nhiều doanh nghiệp công nghệ tham gia và thúc đẩy đổi mới sáng tạo. Kinh nghiệm quốc tế cho thấy quốc gia nào sớm xây dựng được khung quản trị dữ liệu minh bạch, thuận lợi sẽ thu hút được nhiều doanh nghiệp công nghệ và khởi nghiệp đổi mới sáng tạo tham gia phát triển kinh tế số. Do đó, Việt Nam cần tận dụng “*cơ hội vàng*” thập kỷ 2020 - 2030 để nâng cao hiệu quả quản lý dữ liệu, tạo đột phá chiến lược nhằm thúc đẩy nền kinh tế số tăng trưởng nhanh và bền vững.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Tóm lại, nâng cao hiệu quả quản lý nhà nước về dữ liệu đến năm 2030 là một đòi hỏi tất yếu để Việt Nam *bắt kịp xu thế chuyển đổi số, phát huy tối đa nguồn lực dữ liệu* cho phát triển kinh tế - xã hội, đồng thời *đảm bảo an toàn, chủ quyền* trong kỷ nguyên số. Việc này phù hợp với chủ trương, định hướng lớn của Đảng và Nhà nước ta, thể hiện qua hàng loạt văn kiện, chính sách từ Nghị quyết 52-NQ/TW (2019) đến Chiến lược dữ liệu quốc gia (2024) và Luật Dữ liệu (2024). Có thể khẳng định, Đây là chìa khóa để khai thác tối đa giá trị dữ liệu, phục vụ phát triển bền vững, bảo đảm an ninh, an toàn và chủ quyền quốc gia trong kỷ nguyên số, đưa nước ta vươn lên trong nền kinh tế số toàn cầu và phục vụ tốt hơn mọi nhu cầu của người dân, doanh nghiệp trong tương lai.



***Mình họa quản lý nhà nước về dữ liệu - Ảnh: Youth and Partners***

### **8.3.2. Định hướng chiến lược phát triển dữ liệu đến năm 2030**

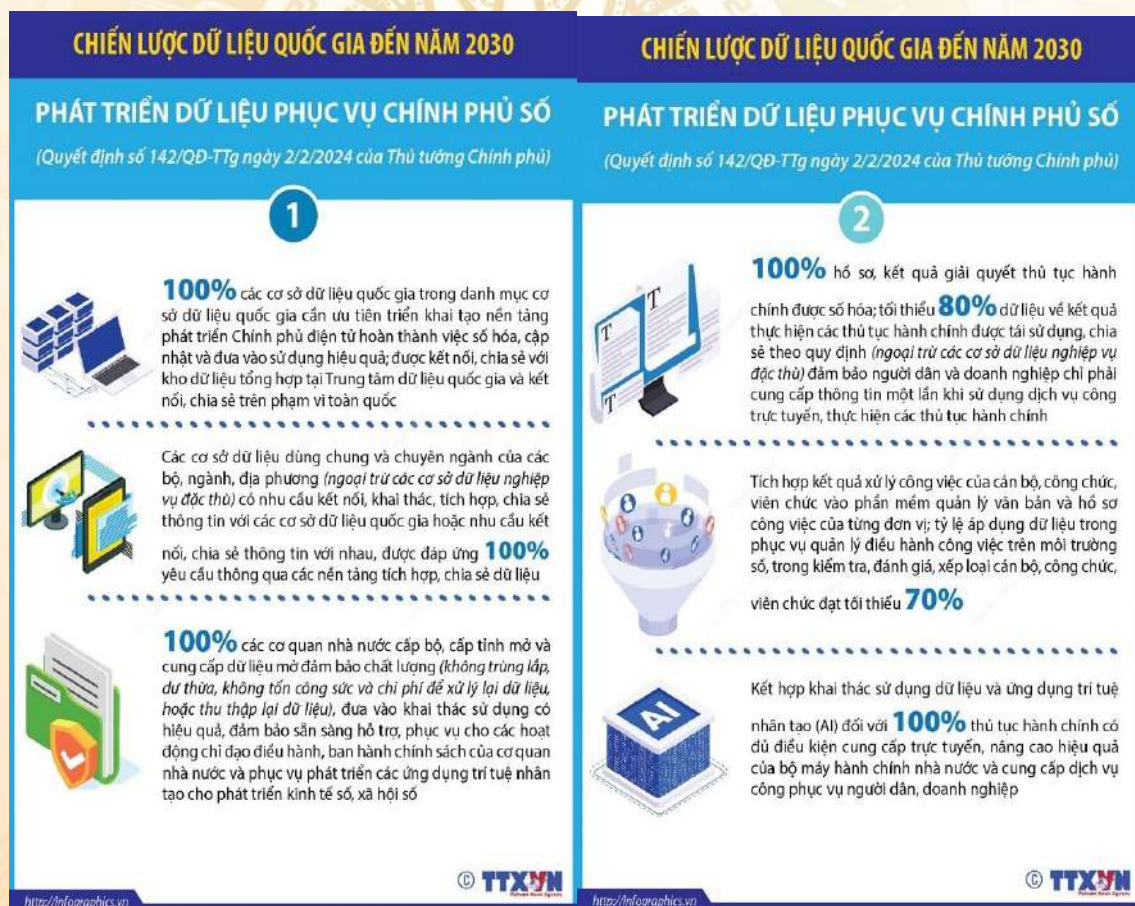
Trong bối cảnh chuyển đổi số toàn diện, Nhà nước Việt Nam coi dữ liệu là tài nguyên chiến lược của quốc gia và đặt mục tiêu biến dữ liệu thành “*tài sản số*” phục vụ Chính phủ số, kinh tế số và xã hội số. Luật Dữ liệu năm 2024 (có hiệu lực từ 1/7/2025) quy định rõ: “*Dữ liệu là tài nguyên, Nhà*





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

nước có chính sách huy động mọi nguồn lực để làm giàu dữ liệu, phát triển dữ liệu trở thành tài sản”. Trên nền tảng này, Quyết định 142/QĐ-TTg (ngày 02/02/2024) đã phê duyệt Chiến lược Dữ liệu Quốc gia đến năm 2030 với tầm nhìn: dữ liệu mở ra không gian phát triển mới cho Chính phủ số, kinh tế số và xã hội số, thúc đẩy năng lực cạnh tranh, đảm bảo chuyển đổi số thành công và đưa Việt Nam trở thành “quốc gia số an toàn” vào năm 2030. Kế hoạch này đặt mục tiêu Việt Nam lọt vào nhóm 50 quốc gia dẫn đầu thế giới về chuyển đổi số và đứng thứ 3 trong ASEAN về kinh tế số vào năm 2030. Từ đó, *định hướng của Chính phủ là xây dựng một hệ sinh thái dữ liệu thống nhất, an toàn, minh bạch - làm nền tảng cho một nền kinh tế, xã hội số năng động, hội nhập quốc tế và cạnh tranh cao.*



**Phát triển dữ liệu phục vụ Chính phủ số - Ảnh: TTXVN**





### 8.3.2.1. Quan điểm và nguyên tắc chỉ đạo

Chiến lược dữ liệu quốc gia của Việt Nam được định hướng theo các nguyên tắc chỉ đạo quan trọng sau:

+ **An toàn, bảo mật:** Nhà nước coi dữ liệu là tài nguyên quan trọng của quốc gia, do đó Luật Dữ liệu yêu cầu các cơ quan chức năng phải bảo vệ nghiêm ngặt dữ liệu, đặc biệt là dữ liệu công và dữ liệu quan trọng quốc gia. Nghị định 169/2025/NĐ-CP quy định hoạt động khoa học, công nghệ về dữ liệu có nguyên tắc thử nghiệm có kiểm soát, trong đó “*bảo đảm tuân thủ theo quy định của Hiến pháp, Luật Dữ liệu và các quy định pháp luật liên quan*” và “*đảm bảo minh bạch trong quá trình đánh giá, lựa chọn, xét duyệt tổ chức, cá nhân tham gia thử nghiệm*”. Các quy định này nhằm ngăn ngừa lạm dụng dữ liệu, phá hoại lợi ích quốc gia và tạo hành lang pháp lý bảo mật cho dữ liệu công.

+ **Minh bạch, thống kê:** Quản lý nhà nước về dữ liệu phải minh bạch trong ban hành chính sách và cũng như các báo cáo. Luật Dữ liệu quy định công bố công khai tiêu chuẩn kỹ thuật, quy chuẩn dữ liệu và yêu cầu thường xuyên công bố báo cáo thống kê, đánh giá về dữ liệu quốc gia. Các cơ quan quản lý cần xây dựng và công khai Chiến lược dữ liệu quốc gia, văn bản pháp luật, tiêu chuẩn kỹ thuật và phổ biến chính sách về dữ liệu. Đồng thời, Nhà nước giám sát việc thực hiện, công bố kết quả kiểm tra định kỳ, góp phần minh bạch hóa quản trị dữ liệu. Ví dụ, Điều 8 của Luật Dữ liệu liệt kê nội dung quản lý nhà nước về dữ liệu bao gồm cả việc công bố tiêu chuẩn, quy chuẩn kỹ thuật, quy chuẩn chất lượng dữ liệu và thực hiện báo cáo, thống kê dữ liệu.

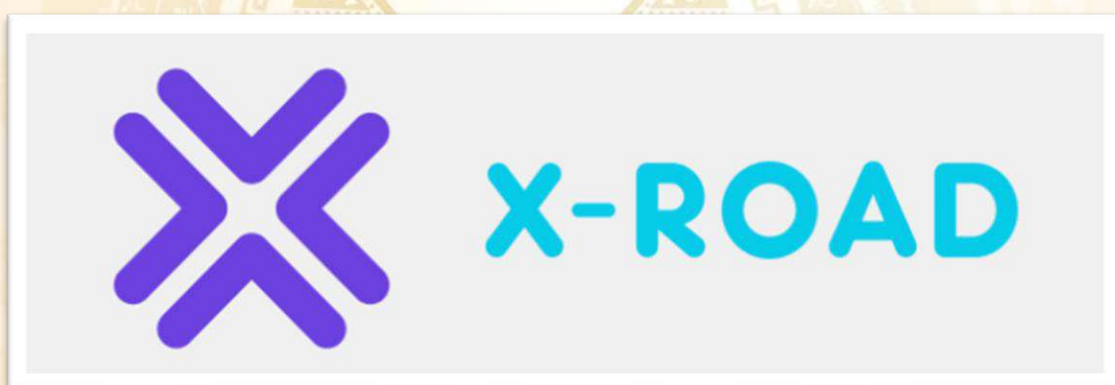
+ **Chia sẻ, kết nối dữ liệu:** Nhà nước thúc đẩy liên thông dữ liệu giữa các cơ quan, tổ chức. Chiến lược nhấn mạnh phát triển nền tảng tích hợp,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

chia sẻ dữ liệu quốc gia (NDXP), kết nối với Trục liên thông văn bản quốc gia và nền tảng IoT để dữ liệu của các bộ, ngành, địa phương được kết nối xuyên suốt. Hiện nay NDXP đã thiết lập hàng trăm điểm kết nối giữa cơ sở dữ liệu các cơ quan nhà nước: theo báo cáo tháng 4/2024, NDXP đã có 388 điểm kết nối giữa 95 cơ quan, bình quân hơn 2,8 triệu giao dịch mỗi ngày. Ví dụ quốc tế như Singapore với Kiến trúc Dữ liệu Chính phủ (GDA) đã xây dựng “*Nguồn dữ liệu duy nhất*” (Single Source of Truth) và “*Trung tâm tin cậy*” (Trusted Centres) cho mỗi loại dữ liệu, cho phép chia sẻ dữ liệu công an toàn và hiệu quả. Tại Estonia, hạ tầng X-Road hỗ trợ nguyên tắc “*một lần hỏi*” (once-only): công dân chỉ cần cung cấp dữ liệu một lần, các cơ quan tự động tái sử dụng, đồng thời Estonia đã liên thông X-Road với Phần Lan để trao đổi dữ liệu dân cư xuyên biên giới [50].



***Mô hình X-Road trong Chính phủ điện tử tại Estonia - Ảnh:***

***Antoanthongtin.vn***

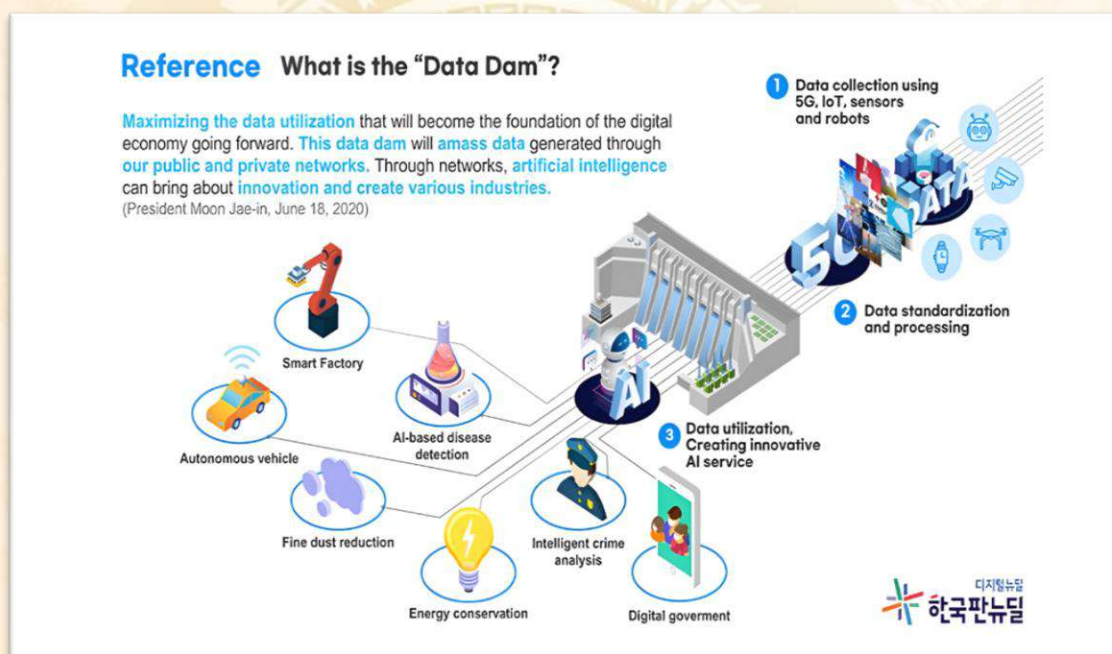
+ ***Đổi mới, sáng tạo:*** Phát triển công nghệ và dịch vụ mới về dữ liệu là động lực cải cách. Luật Dữ liệu khuyến khích các tổ chức, cá nhân trong và ngoài nước đầu tư, nghiên cứu, ứng dụng công nghệ mới trong lĩnh vực dữ liệu. Chính sách “thử nghiệm có kiểm soát” theo Nghị định 169/2025/NĐ-CP cho phép triển khai các mô hình dữ liệu mới trong phạm vi giới hạn để đánh giá và hoàn thiện trước khi áp dụng đại trà. Sáng kiến như “Data Dam”





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

(Siêu đập Dữ liệu) của Hàn Quốc cho thấy xu hướng tích hợp dữ liệu quy mô lớn để hỗ trợ phát triển AI. Theo Bộ Khoa học và Công nghệ thông tin Hàn Quốc, Data Dam là dự án tập trung “thu thập dữ liệu từ cả mạng công cộng và tư nhân, chuẩn hóa, xử lý và khai thác để tạo ra các hệ thống trí tuệ nhân tạo thông minh hơn”. Hàn Quốc cũng thiết lập Cổng Dữ liệu Mở quốc gia (data.go.kr) và nền tảng AI Hub cung cấp hàng trăm tập dữ liệu phục vụ nghiên cứu và phát triển<sup>56</sup>. Việt Nam sẽ khuyến khích phát triển các nền tảng tương tự (AI Hub, dữ liệu mở) và tổ chức hackathon, diễn đàn để thúc đẩy đổi mới trên dữ liệu.



### **Mô hình Data Dam của Hàn Quốc - Ảnh: KoreaTechToday**

+ **Hội nhập quốc tế:** Chiến lược hướng tới hợp tác, liên thông dữ liệu xuyên biên giới. Luật Dữ liệu và Chiến lược nêu rõ tuân thủ quy định quốc tế và khuyến khích hợp tác song phương, đa phương. Chẳng hạn, Trung tâm

<sup>56</sup> Business Wire (2021), *Korea Kicks Off “Data Dam”*, PR Newswire, <https://www.prnewswire.com/news-releases/korea-kicks-off-data-dam-301325717.html>, truy cập ngày 07/8/2025.

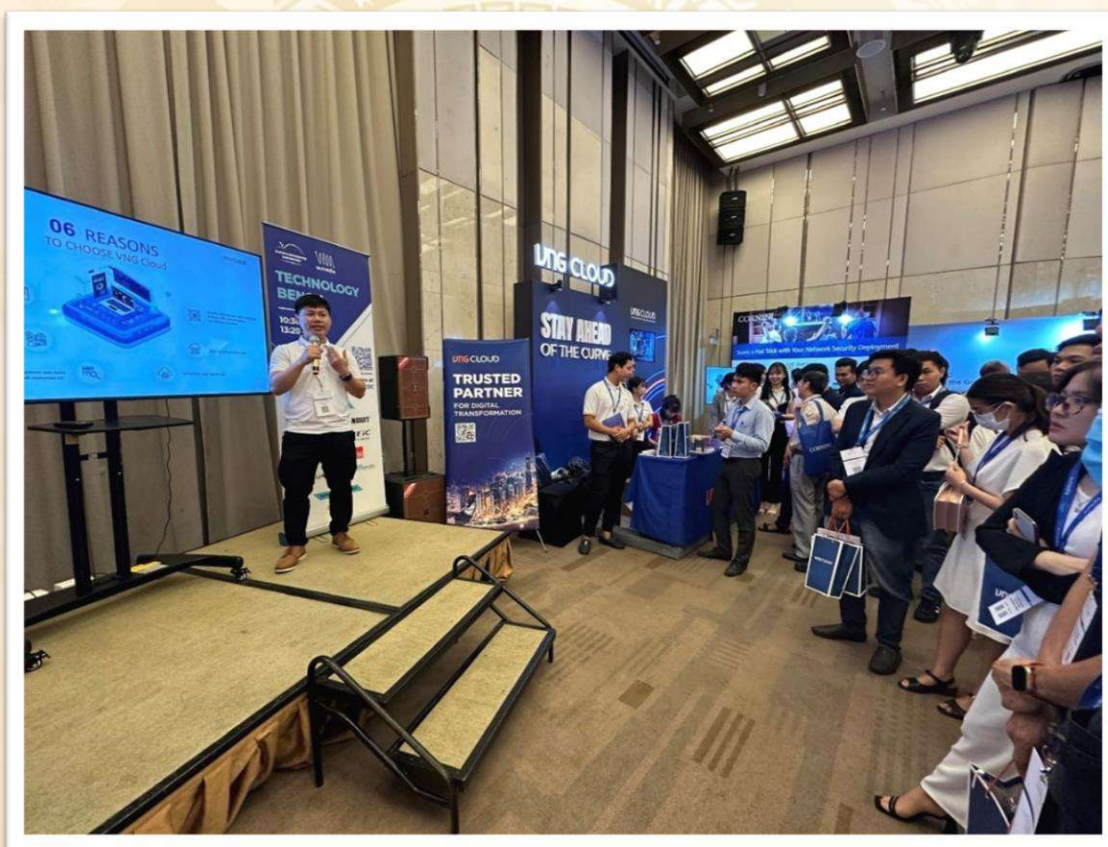




## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Dữ liệu Quốc gia tương lai có thể học hỏi mô hình liên thông dữ liệu khu vực như Estonia và Phần Lan, và hướng tới tham gia “không gian dữ liệu chung” của EU. EU đã đề xuất “không gian dữ liệu chung” ngành/ngành (Data Spaces) để tiêu chuẩn hóa chia sẻ dữ liệu an toàn xuyên biên giới. Tiếp theo, chiến lược “Data Union” của EU đang được xây dựng nhằm hỗ trợ phát triển AI qua chia sẻ dữ liệu chất lượng cao xuyên quốc gia. Việt Nam sẽ học hỏi các chuẩn mực quốc tế này, đồng thời phát huy tiềm lực trong nước và bảo vệ chủ quyền dữ liệu.

### **8.3.2.2. Tầm nhìn và mục tiêu đến năm 2030**



**Đại diện VNG giới thiệu giải pháp VNG cloud tại Hội thảo Điện toán đám mây và Trung tâm dữ liệu Việt Nam 2023 ở TP.HCM - Ảnh: VnEconomy**

Chiến lược đặt ra tầm nhìn đến 2030 là hình thành một hệ sinh thái dữ liệu thống nhất, an toàn, minh bạch và hiệu quả, trong đó dữ liệu là xương





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

sống của Chính phủ số và kinh tế số. Theo nội dung phê duyệt, Việt Nam nỗ lực trở thành quốc gia số an toàn, đồng thời phấn đấu lọt top 50 thế giới về chuyển đổi số và thứ 3 ASEAN về kinh tế số. Các mục tiêu cụ thể đến 2030 bao gồm:

+ ***Hoàn thiện hạ tầng dữ liệu quy mô lớn:*** Xây dựng Trung tâm Dữ liệu Quốc gia và các Trung tâm dữ liệu vùng (theo tiêu chuẩn xanh), kết nối với Trạm trung chuyển Internet quốc gia (VNIX) để đảm bảo dữ liệu liên thông, dự phòng lẫn nhau, không gián đoạn ngay cả khi mất kết nối quốc tế.

+ ***Số hóa toàn diện dữ liệu quan trọng:*** Đưa 90 - 100% dữ liệu quan trọng thuộc các lĩnh vực ưu tiên (như dân cư, đất đai, đăng ký doanh nghiệp, tài chính, bảo hiểm xã hội, hồ sơ cán bộ) vào dạng số và liên thông giữa các hệ thống. Chiến lược đặt mục tiêu số hóa 100% cơ sở dữ liệu quốc gia về lao động - bảo hiểm xã hội và số hóa 90% di sản văn hóa phi vật thể để phục vụ quản lý và du lịch.

+ ***Kết nối, chia sẻ dữ liệu liên ngành:*** Đảm bảo mọi cơ sở dữ liệu chuyên ngành được nối vào NDXP và Trục liên thông quốc gia. Khi đó, dữ liệu từ trung ương đến địa phương sẽ cập nhật tự động, hỗ trợ quản trị minh chứng (evidence-based policy) và nâng cao chất lượng dịch vụ công.

+ ***An toàn, chủ quyền và cạnh tranh:*** Hệ sinh thái dữ liệu phải đạt chuẩn an ninh cao, bảo vệ chủ quyền số, tạo lợi thế cạnh tranh quốc tế. Ví dụ, EU nhấn mạnh bảo vệ chủ quyền dữ liệu kết hợp với năng lực cạnh tranh của khối. Việt Nam định hướng tham gia các tiêu chuẩn quốc tế, đồng thời phát huy nguồn lực nội sinh để đảm bảo an toàn và hội nhập.

### ***8.3.2.3. Giải pháp tổ chức thực hiện***

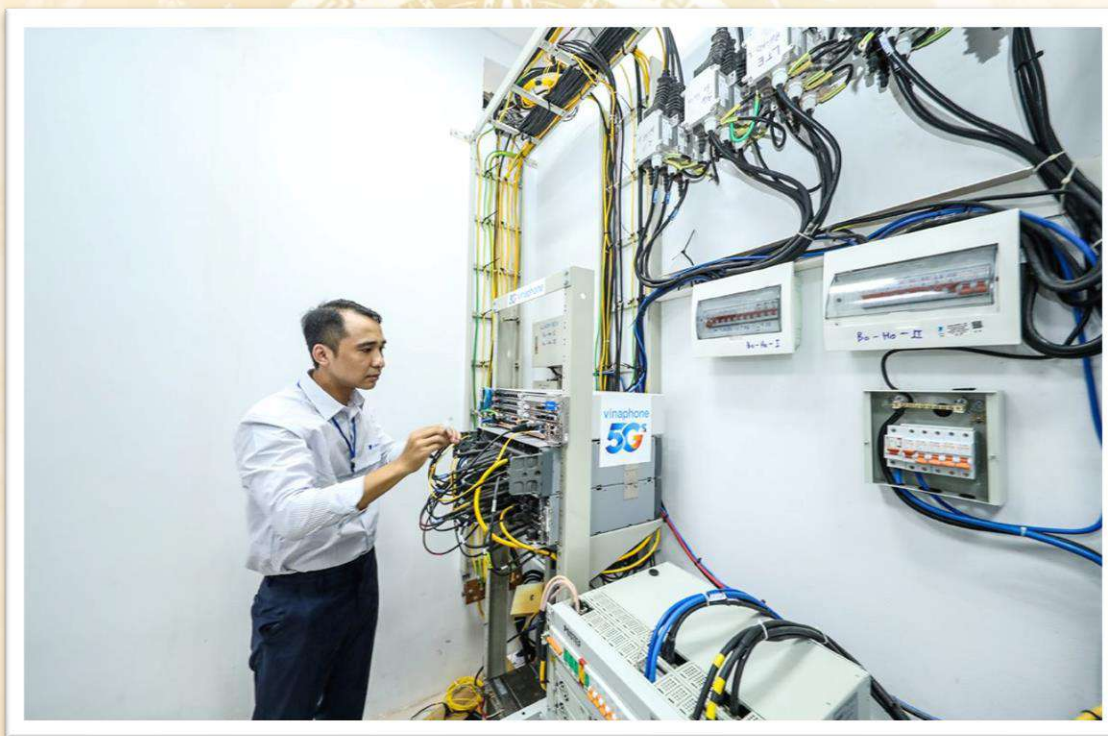
Để hiện thực hóa chiến lược, Việt Nam dự kiến triển khai đồng bộ các giải pháp sau:





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ ***Hoàn thiện thể chế, chính sách pháp luật:*** Hoàn thiện khung pháp lý là nền tảng. Việt Nam đã ban hành Luật Dữ liệu 2024, các văn bản hướng dẫn (các Nghị định 165/2024/NĐ-CP, 169/2025/NĐ-CP, 160/2025/NĐ-CP, 102/2025/NĐ-CP, Quyết định 20/2025/QĐ-TTg...). Đặc biệt là Luật Công nghiệp Công nghệ số, trong đó quy định rõ “*các hình thức sở hữu dữ liệu, quyền tài sản dữ liệu, chính sách mua bán dữ liệu*”, nhằm đưa dữ liệu trở thành tài sản được pháp luật bảo vệ và hình thành thị trường dữ liệu. Đồng thời hoàn thiện quy định về bảo mật, quyền riêng tư, phân loại dữ liệu theo mức độ nhạy cảm. Tham khảo kinh nghiệm quốc tế như EU (GDPR, Data Act) để nâng cao niềm tin và khuyến khích chia sẻ dữ liệu công - tư.



***Kỹ sư VNPT kiểm tra trạm thu phát sóng 5G tại Hà Nội - Ảnh: Báo Tuyên Quang***

+ ***Đầu tư hạ tầng và nền tảng dữ liệu:*** Xây dựng hệ thống Trung tâm Dữ liệu Quốc gia và vùng quy mô lớn (theo tiêu chuẩn xanh) và phát triển các nền tảng tích hợp, chia sẻ dữ liệu quốc gia đảm bảo thông tin liên thông





giữa các cơ quan. Ví dụ, Singapore đã áp dụng GDA với các “*nguồn dữ liệu duy nhất*” giúp chia sẻ dữ liệu công hiệu quả và an toàn. Việt Nam cũng đã triển khai Nền tảng Tích hợp, Chia sẻ Dữ liệu Quốc gia (NDXP) để kết nối các cơ sở dữ liệu chuyên ngành, tạo điều kiện thuận lợi cho trao đổi dữ liệu liên bộ, liên ngành.

+ ***Xây dựng cơ sở dữ liệu nền tảng:*** Ưu tiên phát triển cơ sở dữ liệu quốc gia cốt lõi (dân cư, đất đai, doanh nghiệp, tài chính, bảo hiểm xã hội, cán bộ, công chức, viên chức) làm “khung xương” cho Chính phủ số. Ví dụ, Việt Nam đã số hóa hồ sơ dân cư và bảo hiểm xã hội, liên thông với Cổng Dịch vụ công quốc gia, từng bước đạt “*một cửa một lần*” cho người dân. Các nước tiên tiến như Estonia cũng triển khai cơ sở dữ liệu chỉ số cá nhân để tự động hóa cấp phép dịch vụ dựa trên thông tin đã có.

+ ***Khuyến khích đổi mới và phát triển thị trường dữ liệu:*** Xây dựng thị trường dữ liệu nội địa, phát triển dịch vụ phân tích và trung gian dữ liệu. Luật Dữ liệu khuyến khích các tổ chức, cá nhân trong và ngoài nước đầu tư xây dựng công nghệ, sản phẩm, dịch vụ dữ liệu. Việt Nam có thể học hỏi Hàn Quốc với Cổng Dữ liệu Mở quốc gia (data.go.kr) cung cấp hàng chục nghìn tập dữ liệu và API công khai, cùng dự án Data Dam chuẩn hóa dữ liệu lớn cho AI [44]. Tương tự, Việt Nam đã lập AI Hub (cấp phép truy cập dữ liệu phục vụ AI) và thường xuyên tổ chức “*Hackathon*” - một sự kiện thi đua lập trình - để thúc đẩy đổi mới.

+ ***Đào tạo nhân lực và nâng cao năng lực quản trị:*** Đào tạo chuyên gia dữ liệu, nhà khoa học dữ liệu là yêu cầu bắt buộc. Nhà nước ưu tiên bồi dưỡng chuyên viên dữ liệu và có chính sách thu hút chuyên gia cấp cao. Đồng thời, cần tổ chức cơ quan chuyên trách quản lý dữ liệu quốc gia (đang nghiên cứu thành lập Ủy ban Chiến lược Dữ liệu, tương tự vai trò của Bộ





Công an trong Luật Dữ liệu) để đảm bảo thống nhất chính sách, giám sát chặt chẽ và hỗ trợ ứng dụng dữ liệu ở địa phương, ngành.

Tóm lại, có thể khẳng định rằng định hướng quản lý nhà nước về dữ liệu đến 2030 của Việt Nam là xây dựng một hệ sinh thái dữ liệu kết nối - an toàn - minh bạch, phục vụ mục tiêu Chính phủ số, kinh tế số và xã hội số. Chính phủ đã đặt nền tảng pháp luật, đang đầu tư hạ tầng và phát triển cơ sở dữ liệu nền tảng, đồng thời khuyến khích đổi mới trên dữ liệu và hợp tác toàn cầu. Kinh nghiệm quốc tế cho thấy một chiến lược dữ liệu hiệu quả cần minh bạch trong quy định, tổ chức quản trị rõ ràng và tuân thủ các tiêu chuẩn toàn cầu, đó là điều mà chiến lược Việt Nam đang hướng tới.

### ***8.3.3. Các nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030 để nâng cao hiệu quả công tác quản lý nhà nước về dữ liệu***

Quản lý nhà nước về dữ liệu là một chức năng “vĩ mô” của Nhà nước, bao quát việc xây dựng thể chế, chính sách, tiêu chuẩn kỹ thuật, giám sát, thanh tra và định hướng thị trường dữ liệu. Theo Khoản 1, Điều 8 Luật Dữ liệu 2024, khái quát nội dung quản lý nhà nước về dữ liệu bao gồm xây dựng, ban hành chiến lược, pháp luật, tiêu chuẩn (điểm a); tuyên truyền, hướng dẫn chính sách pháp luật (điểm b); giám sát, bảo vệ dữ liệu, bảo đảm an ninh, an toàn (điểm c); điều phối báo cáo, thống kê, phát triển thị trường dữ liệu (điểm d); thanh tra, kiểm tra, xử lý vi phạm (điểm đ); và đào tạo, phát triển nguồn nhân lực, hợp tác quốc tế (điểm e). Như vậy, quản lý nhà nước về dữ liệu vừa có tính vĩ mô, mang tính quyền lực công, vừa gắn liền điều tiết thể chế, chính sách, kỹ thuật và xúc tiến phát triển kinh tế số. Trong thời gian tới, cụ thể là giai đoạn 2025 - 2030, Việt Nam cần tập trung triển khai có hiệu quả một số nhiệm vụ trọng tâm sau đây:





## ***8.3.3.1. Các nhiệm vụ trọng tâm cần tập trung trong giai đoạn 2025 - 2030 trong công tác quản lý nhà nước về dữ liệu***

### ***- Về dữ liệu***

Trong giai đoạn 2025 - 2030, nhiệm vụ trọng tâm đặt ra là xây dựng và khai thác hiệu quả kho dữ liệu tổng hợp quốc gia, coi đây là nền tảng để hình thành hệ sinh thái dữ liệu đồng bộ, minh bạch và an toàn.

Trước hết, *đến năm 2025*, cần hoàn thành việc xây dựng và đưa vào khai thác kho dữ liệu tổng hợp, trong đó triển khai ngay công tác tổng hợp dữ liệu liên quan đến công dân Việt Nam và người nước ngoài sinh sống, hoạt động tại nước ta. Đây sẽ là tiền đề cho sự phát triển các cơ sở dữ liệu quốc gia, đồng thời bảo đảm dữ liệu phục vụ an ninh quốc gia, quản lý xã hội và phát triển kinh tế. Yêu cầu đặt ra là dữ liệu phải “*đúng - đủ - sạch - sống*”, được tổng hợp, đối sánh từ nhiều nguồn khác nhau, nhằm giảm thiểu các bước trung gian trong quá trình kết nối và chia sẻ. Kho dữ liệu về con người phải bao quát nhiều lĩnh vực: dân cư, sinh trắc học, di biến động cư trú, bảo hiểm, y tế, an sinh xã hội, giáo dục - đào tạo, lao động - việc làm, hộ tịch, thu nhập cá nhân, thuế và cả vi phạm hành chính.

Cùng thời hạn đến hết năm 2025, cần hoàn thành kho dữ liệu tổng hợp được đồng bộ từ các cơ sở dữ liệu quốc gia và phối hợp chặt chẽ với kho dữ liệu về con người. *Từ năm 2026*, định hướng là triển khai phân tích dữ liệu chuyên sâu, phục vụ xây dựng cơ chế, chính sách và quy hoạch chiến lược phát triển quốc gia. Đồng thời, kho dữ liệu này cũng sẽ là nền tảng để phát triển sản phẩm, dịch vụ số mới, dựa trên dữ liệu dùng chung và dữ liệu mở, góp phần trực tiếp vào tăng trưởng kinh tế - xã hội.





# **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Đặc biệt, từ năm 2025, Trung tâm dữ liệu quốc gia phải trở thành đầu mối trao đổi và kết nối quốc tế, qua đó chia sẻ thông tin, nghiên cứu và phát triển các chiến lược quốc gia, đồng thời đặt nền tảng cho việc khai thác và phát triển khoa học - công nghệ của đất nước.

Đến năm 2030, mục tiêu là hoàn thành triển khai Trung tâm dữ liệu quốc gia trở thành hạ tầng lưu trữ và điều phối dữ liệu quốc gia, bao gồm các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và hệ thống thông tin của các bộ, ngành, địa phương. Đồng thời, Trung tâm phải có khả năng kết nối, liên thông dữ liệu với các tổ chức quốc tế và chính phủ các nước, phục vụ trao đổi, hợp tác trên môi trường số, bảo đảm lợi ích hợp pháp và chủ quyền số của Việt Nam.

## ***- Về quy hoạch kiến trúc dữ liệu của Trung tâm dữ liệu quốc gia***

Trong giai đoạn đầu, đến hết năm 2025, nhiệm vụ trọng tâm là hoàn thiện Bộ tiêu chuẩn về quy hoạch kiến trúc dữ liệu quốc gia tại Trung tâm dữ liệu quốc gia. Bộ tiêu chuẩn này phải quy định rõ cơ chế phân cấp và phân loại dữ liệu theo nhiều cấp độ: dữ liệu mở, dữ liệu mật, tối mật, tuyệt mật, cũng như theo mức độ ảnh hưởng đối với an ninh quốc gia, quyền lợi của công dân và hoạt động của doanh nghiệp. Trên cơ sở đó, cần xây dựng quy hoạch cụ thể cho các kho lưu trữ dữ liệu, bảo đảm việc bố trí lưu giữ hợp lý, tách bạch từng loại dữ liệu theo chuẩn mực bảo mật. Song song, phải ban hành các chính sách an ninh, an toàn thông tin phù hợp với từng đối tượng sử dụng, từng phương thức truy cập và từng cấp độ khai thác, nhằm vừa tạo điều kiện khai thác hiệu quả, vừa bảo đảm kiểm soát chặt chẽ và hạn chế rủi ro.





## BÀI DỰ THI TÌM HIỂU

## LUẬT DỮ LIỆU *Trong công an nhân dân*

| SỐ TT | ĐỐI TƯỢNG   | TỔ CHỨC XÂY DỰNG VÀ BIÊN SOẠN                                                           | TỔ CHỨC THẨM ĐỊNH VÀ CÔNG BỐ                           |
|-------|-------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------|
| 1     | <b>QCVN</b> | Bộ và cơ quan ngang Bộ thuộc Chính phủ                                                  | Các Bộ, Ngành thẩm định. Bộ có QCVN công bố            |
| 2     | <b>QCĐP</b> | Các sở, ban ngành thuộc các Tỉnh, TP trực thuộc Trung ương                              | UBND Tỉnh, thành phố trực thuộc Trung ương công bố     |
| 3     | <b>TCVN</b> | Các Bộ, cơ quan ngang Bộ                                                                | Bộ KHCN thẩm định và công bố                           |
| 4     | <b>TCCS</b> | Tổ chức kinh tế<br>Cơ quan nhà nước<br>Đơn vị sự nghiệp<br>Tổ chức xã hội - nghề nghiệp | Sở KHCN hoặc Bộ KHCN thẩm định. Các tổ chức tự công bố |

***Quy chuẩn kỹ thuật địa phương về quy hoạch và kiến trúc của Viện Kiến trúc Quốc gia là hình mẫu để tham khảo - Ảnh: Viện Kiến trúc Quốc gia***

Bước sang năm 2030, yêu cầu đặt ra là phải hoàn thiện toàn bộ quy hoạch, tiêu chuẩn và kiến trúc dữ liệu quốc gia, không chỉ tại Trung tâm dữ liệu quốc gia mà còn được mở rộng, đồng bộ đến các cơ sở dữ liệu của bộ, ngành, địa phương. Đây là giai đoạn bảo đảm sự thống nhất về kiến trúc dữ liệu trên phạm vi toàn quốc, tạo nên một hệ sinh thái dữ liệu chuẩn hóa, liên thông, đồng bộ, vừa đáp ứng nhu cầu quản lý, vừa phục vụ phát triển kinh tế - xã hội. Khi hoàn thành, hệ thống này sẽ đóng vai trò nền tảng cho việc xây dựng Chính phủ số, xã hội số, kinh tế số, đồng thời bảo đảm an ninh, an toàn dữ liệu quốc gia trong dài hạn.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

## *- Về phân tích và khai thác dữ liệu*

Trong giai đoạn *đến hết năm 2025*, trọng tâm là xây dựng năng lực lõi về phân tích dữ liệu: triển khai đồng bộ các công nghệ và giải pháp hiện đại (nền tảng phân tích thời gian thực, kho dữ liệu dùng chung, hồ dữ liệu/lakehouse, công cụ trực quan hóa và khai phá dữ liệu), đồng thời đào tạo đội ngũ chuyên gia khoa học dữ liệu, đặc biệt là các chuyên gia phân tích có trình độ cao. Mục tiêu là hình thành quy trình chuẩn cho toàn bộ vòng đời dữ liệu gồm: thu thập, làm sạch, đối sánh, tổng hợp đến phân tích tổng thể, đa chiều, khách quan, bảo đảm dữ liệu “*đúng - đủ - sạch - sống*”, có thể tái sử dụng ngay cho nghiệp vụ và hoạch định chính sách. Cùng với đó, thiết lập cơ chế quản trị dữ liệu (data governance), danh mục siêu dữ liệu (metadata catalog), quản lý chất lượng (DQM) và đánh giá tác động bảo vệ dữ liệu (DPIA) để mọi phân tích đều tuân thủ pháp luật, an ninh, an toàn.

*Từ năm 2026*, chuyển trọng tâm sang khai thác giá trị dữ liệu ở quy mô quốc gia: định kỳ lập báo cáo dự báo, cảnh báo sớm tham mưu cho Chính phủ, các bộ, ngành, địa phương trong điều hành vĩ mô và quản trị chuyên ngành (y tế, giáo dục, an sinh, giao thông, môi trường...). Song song, cung cấp có chọn lọc dữ liệu dùng chung và dữ liệu mở quan trọng qua API tiêu chuẩn, phục vụ người dân, doanh nghiệp và đối tác quốc tế; qua đó thúc đẩy hệ sinh thái đổi mới sáng tạo, hình thành các sản phẩm - dịch vụ mới dựa trên dữ liệu số. Toàn bộ quá trình phải gắn với cơ chế phân loại dữ liệu, kiểm soát truy cập theo nguyên tắc “*ít quyền nhất*”, mã hóa đầu cuối, giám sát - nhật ký truy cập, bảo đảm quyền riêng tư và bí mật nhà nước.

*Đến năm 2030*, phần đầu trên 90% hoạt động hành chính, trao đổi, phối hợp, cung cấp thông tin giữa các cơ quan nhà nước được thay thế bằng chia sẻ dữ liệu số qua các kho dữ liệu tổng hợp tại Trung tâm dữ liệu quốc gia,





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

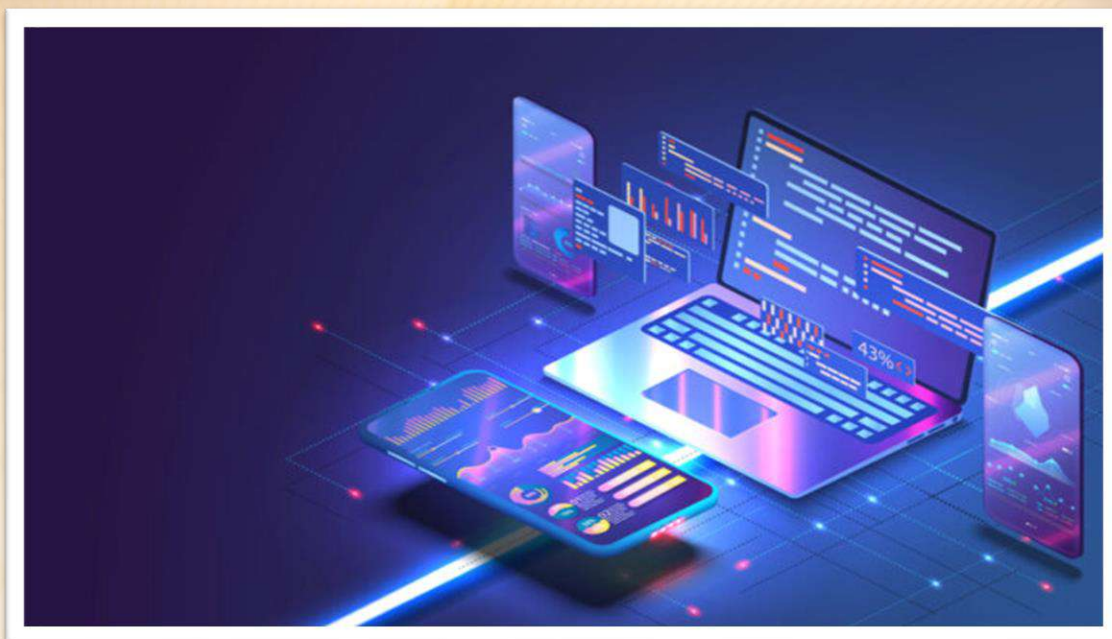
bảo đảm liên thông - thời gian thực - truy xuất nguồn gốc. Khi đó, phân tích dữ liệu trở thành quy trình tác nghiệp mặc định của quản trị công, giúp rút ngắn thời gian ra quyết định, nâng cao chất lượng chính sách dựa trên bằng chứng, giảm chi phí tuân thủ cho người dân và doanh nghiệp, đồng thời củng cố niềm tin xã hội vào nền quản trị số minh bạch, hiệu quả và an toàn.

### ***- Về hạ tầng, thiết bị công nghệ thông tin***

*Đến hết năm 2025*, hoàn thành cơ bản việc xây dựng hạ tầng nhà trạm của Trung tâm dữ liệu quốc gia tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật của quốc tế về trung tâm dữ liệu, về an toàn thông tin, đảm bảo độ sẵn sàng của hệ thống hạ tầng công nghệ hiện đại, đồng bộ. Chủ động triển khai nền tảng điện toán đám mây trong Trung tâm dữ liệu quốc gia. Liên tục cập nhật theo xu thế công nghệ mới nhất, tránh lãng phí, đáp ứng nhu cầu đúng mục tiêu của cách mạng 4.0.

*Từ năm 2026*, thực hiện cung cấp hạ tầng nhà trạm (nguồn điện, điều hòa bảo đảm phòng cháy chữa cháy...) và chỗ đặt trang thiết bị công nghệ thông tin theo tiêu chuẩn Trung tâm dữ liệu ANSI/TIA-942 tối thiểu Tier 3 hoặc tương đương cho cán bộ, ngành, địa phương có nhu cầu nhằm đảm bảo tính đồng bộ trong bảo đảm an toàn, an ninh thông tin. Đồng thời, tăng cường các yếu tố về an ninh, quốc phòng trong việc bảo đảm tính bí mật, an ninh trật tự trong cả trong và xung quanh khu vực Trung tâm dữ liệu quốc gia; bảo đảm cung cấp hạ tầng công nghệ thông tin (tài nguyên hệ thống) cho các cơ sở dữ liệu quốc gia; các bộ, ngành, địa phương (có nhu cầu) và 100% tổ chức chính trị - xã hội sử dụng; tích hợp với hạ tầng công nghệ thông tin có sẵn của các đơn vị để thống nhất, đồng bộ trong công tác vận hành, quản trị và đảm bảo an ninh, an toàn, tiết kiệm, hiệu quả.





## ***Hạ tầng công nghệ thông tin đảm bảo cho dữ liệu được khai thác có hiệu quả - Ảnh: Cti Supply***

Đến năm 2030, cơ bản các hệ thống thông tin của bộ, ngành, địa phương (có nhu cầu) được quản lý, lưu trữ tại Trung tâm dữ liệu quốc gia (trừ các hệ thống phục vụ quốc phòng, an ninh và các hệ thống chuyên ngành đặc thù khác do Thủ tướng

### ***- Về cải cách, cắt giảm thủ tục hành chính***

Tham gia và đóng góp quan trọng vào việc thực hiện các mục tiêu cải cách hành chính và phát triển Chính phủ số như: đảm bảo 100% kết quả giải quyết thủ tục hành chính, giấy tờ do cơ quan nhà nước ban hành được lưu trữ trong kho dữ liệu số của cơ quan nhà nước, được chia sẻ và sử dụng lại trong các thủ tục hành chính, hoạt động hành chính và sử dụng thay thế hoàn toàn văn bản giấy. 100% người dân và doanh nghiệp sử dụng dịch vụ công trực tuyến được định danh và xác thực thông suốt, hợp nhất trên tất cả hệ thống của các cấp chính quyền từ trung ương đến địa phương. Đến năm 2025, tối thiểu 80% hồ sơ thủ tục hành chính được xử lý hoàn toàn trực





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

tuyển, người dân, tổ chức và đơn vị chỉ phải nhập dữ liệu một lần. Cắt giảm tối thiểu 20% thành phần hồ sơ thủ tục hành chính của cơ quan nhà nước so với hiện nay. Mức độ hài lòng của người dân, doanh nghiệp về giải quyết thủ tục hành chính đạt tối thiểu 90%. Đến năm 2030, 90% số lượng người dân, doanh nghiệp tham gia hệ thống Chính phủ điện tử được xác định danh điện tử thông suốt và hợp nhất trên tất cả các hệ thống thông tin của các cấp chính quyền từ trung ương đến địa phương. Mức độ hài lòng của người dân, doanh nghiệp về giải quyết thủ tục hành chính đạt tối thiểu 95%.

### *- Về phát triển Chính phủ điện tử*

Trong giai đoạn 2025 - 2030, xây dựng và phát triển Chính phủ điện tử tiếp tục được xác định là một trong những trụ cột chiến lược của tiến trình chuyển đổi số quốc gia. Mục tiêu trọng tâm là nâng cao hiệu lực, hiệu quả quản lý nhà nước, tăng cường minh bạch, giảm thiểu thủ tục hành chính, đồng thời nâng cao mức độ hài lòng của người dân và doanh nghiệp khi tiếp cận dịch vụ công trực tuyến.

Theo lộ trình, đến năm 2025, Việt Nam phấn đấu thuộc nhóm 70 quốc gia dẫn đầu về Chính phủ điện tử (EGDI), 50 nước đứng đầu về công nghệ thông tin (IDI) và 40 nước dẫn đầu về an toàn, an ninh mạng (GCI). Đây là những chỉ tiêu có ý nghĩa then chốt, khẳng định vị thế của Việt Nam trên bản đồ số toàn cầu, đồng thời phản ánh quyết tâm chính trị trong việc cải cách hành chính và xây dựng hạ tầng số hiện đại.

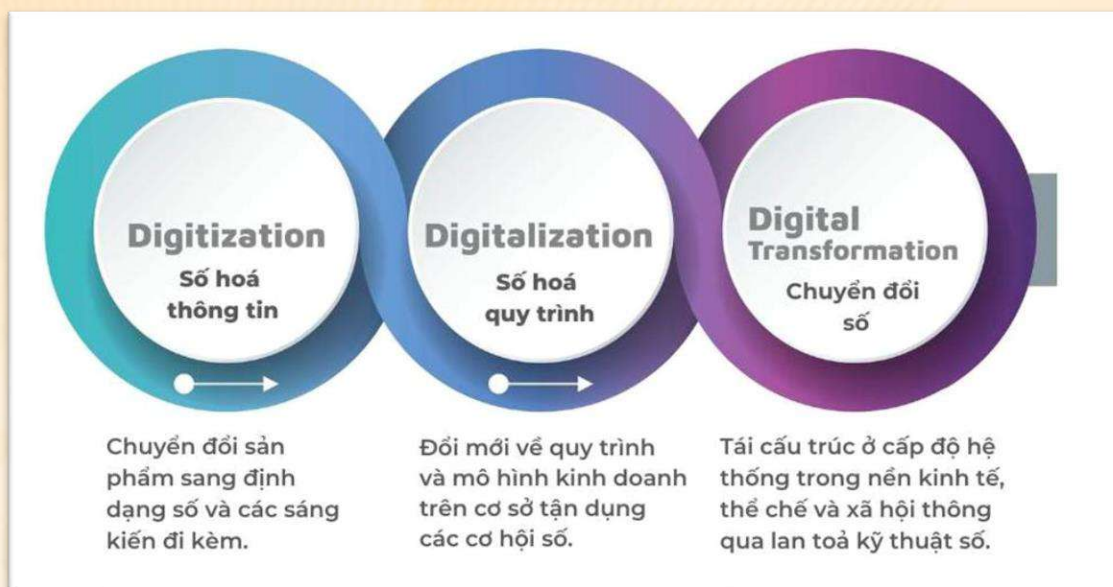
Đến năm 2030, các chỉ số này tiếp tục được nâng cao: Việt Nam đạt mục tiêu vào top 50 thế giới về EGDI, top 30 về IDI và top 30 về GCI. Đây là bước tiến quan trọng, thể hiện sự vươn lên mạnh mẽ cả về hạ tầng công nghệ, năng lực bảo mật, cũng như chất lượng dịch vụ công trực tuyến. Việc đạt được những mục tiêu này không chỉ giúp củng cố niềm tin xã hội, mà





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

còn góp phần tăng cường năng lực cạnh tranh quốc gia, tạo môi trường thuận lợi để phát triển kinh tế số và hội nhập quốc tế sâu rộng.



### ***Chương trình chuyển đổi số Việt Nam - Ảnh: Open Development Vietnam***

Có thể khẳng định, phát triển Chính phủ điện tử gắn với các chỉ số EGDI, IDI và GCI chính là thước đo cụ thể của thành công trong công tác quản lý nhà nước bằng dữ liệu số, qua đó góp phần xây dựng Nhà nước pháp quyền xã hội chủ nghĩa hiện đại, kiến tạo phát triển, phục vụ nhân dân.

#### ***- Về phát triển kinh tế - xã hội***

Trong giai đoạn 2025 - 2030, phát triển kinh tế - xã hội dựa trên nền tảng dữ liệu được coi là một trong những định hướng chiến lược nhằm tạo động lực tăng trưởng mới cho đất nước. Dữ liệu sẽ trở thành yếu tố cốt lõi để hình thành các lĩnh vực, ngành nghề kinh tế mới như kinh tế dữ liệu, kinh tế trí tuệ nhân tạo, thương mại điện tử thế hệ mới, tài chính số, y tế số, giáo dục số và các dịch vụ sáng tạo dựa trên phân tích dữ liệu lớn. Đây không chỉ là xu thế toàn cầu mà còn là yêu cầu tất yếu để Việt Nam bắt kịp tiến trình chuyển đổi số quốc tế.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Theo mục tiêu quốc gia, *đến năm 2025*, kinh tế số Việt Nam dự kiến chiếm khoảng 20% GDP, đưa Việt Nam vươn lên vị trí thứ hai về quy mô kinh tế số trong khu vực Đông Nam Á. Đến năm 2030, tỷ trọng kinh tế số được đặt mục tiêu đạt 30% GDP, khẳng định vai trò trung tâm của dữ liệu trong cấu trúc nền kinh tế quốc dân. Để hiện thực hóa mục tiêu này, việc khai thác, phân tích và ứng dụng dữ liệu trong mọi lĩnh vực - từ quản lý nhà nước, quy hoạch phát triển, đến hoạt động sản xuất, kinh doanh - phải được tiến hành một cách đồng bộ, minh bạch và an toàn.

Đặc biệt, phát triển nền kinh tế dữ liệu không chỉ nhằm nâng cao hiệu quả tăng trưởng, mà còn góp phần bảo đảm tính tự chủ chiến lược của quốc gia trong không gian số. Việc dữ liệu được quản lý, khai thác hợp lý sẽ giúp giảm thiểu lệ thuộc vào công nghệ và nền tảng nước ngoài, đồng thời tạo điều kiện thúc đẩy đổi mới sáng tạo trong nước. Như vậy, phát triển kinh tế dựa trên dữ liệu không chỉ mang ý nghĩa kinh tế, mà còn mang tầm vóc chính trị - an ninh - xã hội, gắn trực tiếp với mục tiêu xây dựng nền kinh tế số, xã hội số và chính phủ số của Việt Nam trong kỷ nguyên 4.0.

***8.3.3.2. Các nhiệm vụ khác liên quan đến trách nhiệm được Chính phủ giao và chức năng quản lý nhà nước về an ninh trật tự, an toàn xã hội của Bộ Công an và các cơ quan, ban, ngành có liên quan***

***- Hoàn thiện thể chế pháp luật về dữ liệu***

Đây là nhiệm vụ nền tảng nhất. Hiện Việt Nam đã có Luật Dữ liệu 2024 quy định khung pháp lý chung về dữ liệu, Luật Bảo vệ dữ liệu cá nhân 2025 quy định về việc bảo vệ dữ liệu cá nhân của công dân và Chiến lược Dữ liệu Quốc gia đến 2030 (Quyết định 142/QĐ-TTg ngày 02/02/2024) đề ra tầm nhìn, mục tiêu cụ thể cho hệ thống chính sách dữ liệu. Nghị định 165/2025/NĐ-CP hướng dẫn thi hành Luật Dữ liệu đã quy định chi tiết các





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

biện pháp bảo vệ và đánh giá rủi ro dữ liệu quan trọng, xuyên biên giới. Bên cạnh đó, Nghị định 169/2025/NĐ-CP quy định hoạt động khoa học, công nghệ, đổi mới sáng tạo về dữ liệu tạo khung hỗ trợ nghiên cứu và phát triển trong lĩnh vực dữ liệu.



***Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương tạo điều kiện thuận lợi cho nền kinh tế số Việt Nam phát triển - Ảnh: Internet***

Tuy nhiên, hệ thống pháp luật vẫn cần được hoàn thiện. Ví dụ, cần đẩy nhanh ban hành Nghị định và thông tư hướng dẫn, như các quy định về “sandbox” dữ liệu, điều kiện kinh doanh nền tảng dữ liệu, chuẩn hóa tính minh bạch của các giao dịch dữ liệu. Cũng cần sớm ban hành và điều chỉnh Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018 để đồng bộ với Luật Dữ liệu. Chiến lược dữ liệu đã nhấn mạnh mục tiêu biến dữ liệu thành tài sản được pháp luật bảo vệ, xây dựng chính sách ưu đãi cho doanh nghiệp dữ liệu và chống thao túng thị trường bởi các tổ chức lớn. Các nước phát





triển cũng ưu tiên hoàn thiện thể chế: EU có GDPR (2016) bảo hộ dữ liệu cá nhân và mới đây là Data Act (2023) quy định chia sẻ dữ liệu công nghiệp một cách công bằng. Học hỏi kinh nghiệm đó, Việt Nam cần tiếp tục cập nhật khung pháp lý, bảo đảm tiêu chuẩn quốc tế (như tuân thủ nghị định thư Hiệp định Đối tác Toàn diện và Tiên bộ xuyên Thái Bình Dương (CPTPP) về dữ liệu), đồng thời mở rộng pháp lý cho các mô hình dữ liệu mới (đám mây, trí tuệ nhân tạo...).

Bên cạnh đó, cần tiếp tục thực hiện các giải pháp sau:

**Một là**, tiếp tục rà soát, phân loại, đánh giá tổng kết thi hành văn bản pháp luật quy định về dữ liệu nói chung và triển khai áp dụng quy định liên quan đến dữ liệu cốt lõi, dữ liệu quan trọng nói riêng theo Luật Dữ liệu, Quyết định số 20/2025/QĐ-TTg ngày 01/7/2025 của Thủ tướng Chính phủ sẽ quy định danh mục dữ liệu cốt lõi, dữ liệu quan trọng. Theo đó, cần nghiên cứu, xác định cụ thể hơn các loại dữ liệu về hạ tầng thông tin quan trọng, quốc phòng, an ninh, cơ sở dữ liệu quốc gia về dân cư, đất đai, tài chính và các ngành kinh tế then chốt khác cần được bảo vệ cao hơn, liên quan trực tiếp đến an ninh quốc gia: cần quy định chặt chẽ, lưu trữ, xử lý và nghiêm cấm chuyển giao ra khỏi “*biên giới số*” của nước ta nếu chưa có sự cho phép của cơ quan có thẩm quyền.

**Hai là**, nghiên cứu, hoàn thiện văn bản quy phạm pháp luật về dữ liệu, bảo vệ dữ liệu cá nhân: trong đó, định nghĩa rõ nghĩa vụ của mọi tổ chức, doanh nghiệp (kể cả nền tảng xuyên biên giới) phải lưu trữ dữ liệu quan trọng của người dùng Việt Nam tại nước ta và cung cấp dữ liệu cho lực lượng an ninh khi có yêu cầu hợp pháp để phục vụ điều tra, phòng chống khủng bố, tội phạm. Đây là điều kiện tiên quyết để đảm bảo thực thi chủ quyền và pháp luật Việt Nam trên không gian mạng.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

**Ba là**, xây dựng, ban hành các văn bản pháp luật về quy trình, quy chuẩn kỹ thuật liên quan an ninh dữ liệu: áp dụng bắt buộc cho các hệ thống thông tin, đặc biệt là các hệ thống trong cơ quan nhà nước và hạ tầng quan trọng; bảo đảm việc tuân thủ không phải là khuyến khích mà là yêu cầu, nghĩa vụ pháp lý bắt buộc, là điều kiện để được phép hoạt động quản lý, xử lý dữ liệu

### ***- Xây dựng và phát triển hạ tầng dữ liệu quốc gia***

Hạ tầng dữ liệu quốc gia là xương sống để lưu trữ, kết nối và xử lý dữ liệu trên quy mô quốc gia. Luật Dữ liệu 2024 quy định Trung tâm dữ liệu quốc gia phải đảm bảo tiêu chuẩn kỹ thuật cao, an toàn thông tin, khả năng phục hồi và sẵn sàng mở rộng khi cần. Cơ sở hạ tầng này bao gồm các thành phần chính: cơ sở dữ liệu tổng hợp quốc gia; nền tảng chia sẻ, điều phối dữ liệu; cổng dịch vụ công quốc gia; cổng dữ liệu mở; và các hệ thống phân tích, phân tích dữ liệu phục vụ chỉ đạo điều hành; hệ thống, phần mềm quản lý, khai thác, cung cấp dịch vụ dữ liệu, cổng dữ liệu mở, cổng dịch vụ dữ liệu; các nền tảng, phần mềm, hệ thống nghiệp vụ khác do Chính phủ, Thủ tướng Chính phủ quyết định. Chiến lược dữ liệu 2030 cũng đề ra xây dựng mạng lưới trung tâm dữ liệu quốc gia và vùng, kết nối với Trạm trung chuyển internet quốc gia (VNIX) để đảm bảo dữ liệu đồng bộ, thông suốt, chịu được sự cố quốc tế.

Thực trạng hiện nay cho thấy Việt Nam đã triển khai một số bước: dự án Trung tâm dữ liệu quốc gia giai đoạn 1 đã hoàn thành, các cơ sở dữ liệu quốc gia về dân cư, đất đai, doanh nghiệp... được số hóa ban đầu. Tuy nhiên, tính liên kết và đồng bộ dữ liệu còn thấp, nhiều hệ thống vẫn nằm độc lập, dẫn đến chồng chéo. Các ví dụ quốc tế có thể làm gương: Estonia xây dựng nền tảng chia sẻ dữ liệu *X-Road* theo mô hình phi tập trung, cho phép hơn 450 cơ quan công và tư phối hợp chia sẻ an toàn, thúc đẩy trên 3.000 dịch





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

vụ số<sup>57</sup>. X-Road đặt dữ liệu “*tại nơi phát sinh*” (Ask-once-only); các bộ tự quản lý cơ sở dữ liệu của mình nhưng chia sẻ qua cầu nối an toàn. Tương tự, Singapore phát triển kiến trúc dữ liệu quốc gia (GDA) với các “nguồn dữ liệu thật” chung (SSOT) và trung tâm tin cậy để đảm bảo dữ liệu lỗi dùng chung cho nhiều cơ quan<sup>58</sup>. Hàn Quốc xây dựng dự án “Data Dam”, một kho dữ liệu liên ngành kết nối công - tư, chuẩn hóa và cho AI học tập.



***Trung tâm dữ liệu quốc gia được xây dựng  
theo tiêu chuẩn quốc tế - Ảnh: Báo Chính phủ***

<sup>57</sup> Govinsider.asia (2024), *Estonia's X-Road: data exchange in the world's most digital society*, Govinsider.asia, <https://govinsider.asia/intl-en/article/estonias-x-road-data-exchange-in-the-worlds-most-digital-society>, truy cập ngày 07/8/2025.

<sup>58</sup> NCS and Talend (2020), *Compliance considerations for public agencies: an introduction to Singapore's data governance and protection frameworks*, ncs.co, <https://www.ncs.co/dam/jcr:1018c9ab-44f0-4cda-aeb5-7b9fffd45a0/a-compliance-introduction-to-singapore-dgp-framework-for-public-agencies-talend-ncs-17Nov2020.pdf>, truy cập ngày 07/8/2025.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Trong giai đoạn tới, Việt Nam cần tiếp tục hoàn thiện kết nối liên thông các hệ thống thông tin nhà nước thông qua Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NDXP) và đẩy mạnh dữ liệu mở; đầu tư nâng cấp hạ tầng trung tâm dữ liệu về công nghệ mới (đám mây, ảo hóa, phần cứng an toàn); quy hoạch dự phòng chống thiên tai, tấn công mạng; và mở rộng liên kết với các mạng lưới dữ liệu khu vực (ví dụ tham gia sáng kiến *Gaia-X* của EU). Việc chuẩn hóa dữ liệu, áp dụng kiến trúc mở (như X-Road, GAIA-X) sẽ giúp tối ưu hiệu quả hạ tầng và kết nối thị trường dữ liệu quốc tế.

### *- Nâng cao năng lực bảo đảm an ninh, an toàn dữ liệu*

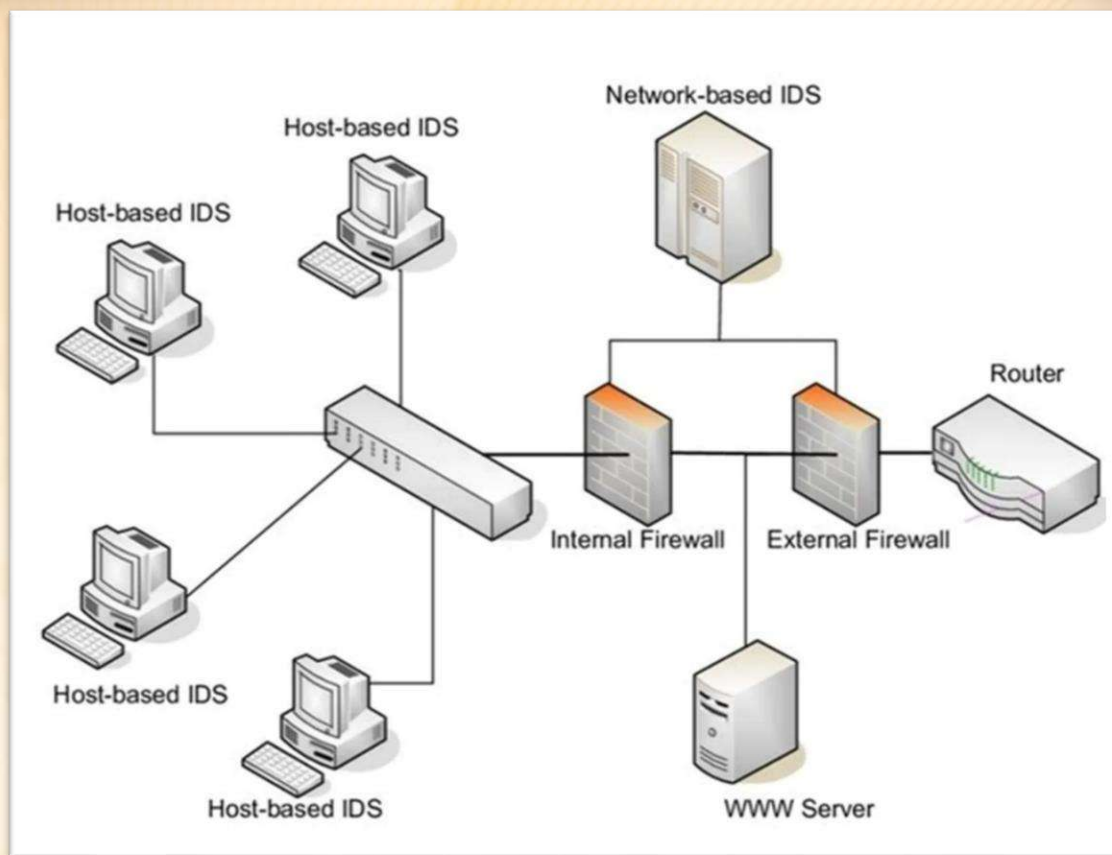
Dữ liệu là tài nguyên then chốt của quốc gia, vì vậy an toàn, an ninh dữ liệu là trọng tâm trong quản lý nhà nước. Luật An toàn thông tin mạng 2015 định nghĩa an toàn mạng là việc bảo vệ thông tin và hệ thống trên mạng tránh truy nhập, sử dụng, tiết lộ trái phép, bảo đảm tính toàn vẹn và khả dụng. Luật Dữ liệu 2024 yêu cầu các biện pháp bảo vệ dữ liệu phải được áp dụng xuyên suốt vòng đời xử lý (Điều 27) và quy định chi tiết việc mã hóa, kiểm soát truy cập, giám sát dữ liệu cốt lõi. Nghị định 165/2025/NĐ-CP cũng yêu cầu đánh giá tác động khi chuyển dữ liệu cốt lõi, quan trọng ra nước ngoài, tập trung vào tính hợp pháp, rủi ro an ninh quốc gia và quyền lợi cá nhân (Điều 12).

Hiện nay, Việt Nam đã triển khai các hệ thống bảo vệ như tường lửa, IDS/IPS, mã hóa dữ liệu và khung pháp lý tương đối đầy đủ. Tuy nhiên, với khối lượng dữ liệu lớn và công nghệ cao, thách thức về an ninh tăng lên. Các vi phạm quốc tế cũng gia tăng như tấn công ransomware vào hạ tầng trọng yếu. Ngoài ra, dữ liệu cá nhân đang lan truyền rộng khắp, đòi hỏi tuân thủ Luật Bảo vệ dữ liệu cá nhân mới ban hành (có hiệu lực từ ngày 01/01/2026) về quyền của người sở hữu dữ liệu.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



## *Mình họa cách thức tường lửa hoạt động - Ảnh: FPT Shop*

Trong giai đoạn 2025 - 2030, Việt Nam cần tập trung vào một số nhiệm vụ cụ thể sau:

(1) Hoàn thiện luật pháp liên quan (thông tư hướng dẫn bảo mật dữ liệu, chính sách sử dụng mã hoá mạnh theo chuẩn quốc tế) và tăng cường phối hợp liên ngành (Công an, Quốc phòng, An ninh mạng) để bảo vệ dữ liệu trọng yếu.

(2) Áp dụng các tiêu chuẩn khắt khe cho trung tâm dữ liệu (độ sẵn sàng cao, chống xâm nhập).

(3) Triển khai thường xuyên đánh giá, kiểm thử an toàn (penetration test) cho toàn bộ hệ thống.





(4) Đào tạo chiến lược ứng cứu khẩn cấp và xây dựng kho dự phòng dữ liệu (disaster recovery) để đảm bảo tính liên tục ngay cả khi mất kết nối quốc tế. Ví dụ như Singapore luôn rà soát định kỳ và nâng cấp bảo mật sau những sự cố an ninh nghiêm trọng năm 2018 - 2019.

Để hiện thực hóa các nội dung trên, cần xác định công tác nghiệp vụ cốt lõi, chuyển trạng thái bị động, ứng phó sang chủ động nắm bắt, phân tích, dự báo và triệt tiêu các nguy cơ đe dọa an ninh quốc gia, trật tự, an toàn xã hội trong hoạt động xây dựng, quản trị, quản lý, xử lý, bảo vệ dữ liệu; giải pháp để thực hiện nhiệm vụ này cần: (i) Xây dựng lực lượng chuyên trách về bảo vệ nền dữ liệu; bên cạnh việc phát huy vai trò của Trung tâm dữ liệu quốc gia (C12) của Bộ Công an, có thể nghiên cứu, bố trí cán bộ tại Công an các đơn vị, địa phương đảm nhiệm công tác bảo đảm an ninh dữ liệu, có nhiệm vụ trực tiếp quản lý, giám sát, hỗ trợ các cơ quan, đơn vị, tổ chức, cá nhân tại địa bàn trong quản lý trong hoạt động xây dựng, quản trị, quản lý, xử lý, bảo vệ dữ liệu; (ii) Tăng cường năng lực hệ thống giám sát, ứng dụng trí tuệ nhân tạo vào công tác quản lý; nhất là 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; (iii) Đẩy mạnh quản lý danh tính số qua VNeID, thúc đẩy VNeID trở thành nền tảng định danh xác thực điện tử duy nhất, bắt buộc cho các dịch vụ công và các giao dịch quan trọng khác như tài chính, ngân hàng, thuế, hải quan, thương mại điện tử sản phẩm dữ liệu... Việc quản lý chặt chẽ danh tính số sẽ hạn chế tối đa tình trạng nặc danh, mạo danh để thực hiện các hành vi vi phạm pháp luật, nâng cao trách nhiệm, khả năng truy vết khi cần thiết.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

### *- Phát triển nguồn nhân lực và trình độ khoa học, công nghệ về dữ liệu*

Nguồn nhân lực dữ liệu là “chìa khóa” để triển khai các nhiệm vụ trên. Luật Dữ liệu và Nghị định 169/2025/NĐ-CP đều nhấn mạnh ưu tiên phát triển nhân lực chất lượng cao trong lĩnh vực dữ liệu và công nghệ liên quan. Chẳng hạn, Điều 6 Nghị định 169/2025/NĐ-CP quy định Bộ Công an, Bộ Giáo dục và đào tạo, Bộ Khoa học và Công nghệ phối hợp đào tạo, bồi dưỡng chuyên sâu cho cán bộ thuộc lĩnh vực công nghệ thông tin, khoa học dữ liệu, trí tuệ nhân tạo, an ninh mạng. Đồng thời, Điều 5 khuyến khích phát triển mạng lưới chuyên gia, nhà khoa học, các tổ chức khoa học công nghệ về dữ liệu trong và ngoài nước trung tâm nghiên cứu về khoa học dữ liệu, đổi mới sáng tạo ứng dụng trí tuệ nhân tạo, điện toán đám mây, chuỗi khối, truyền thông dữ liệu, Internet vạn vật, dữ liệu lớn.

Tuy nhiên, Việt Nam vẫn đang thiếu hụt nhân lực chuyên môn cao: chưa đủ giáo sư, tiến sĩ trong khoa học dữ liệu, kỹ sư phân tích dữ liệu... so với quy mô thị trường dữ liệu hiện nay. Số Học viện, trường Đại học có chương trình đào tạo về “khoa học dữ liệu” vẫn còn khiêm tốn, và các trường đại học chủ yếu tập trung công nghệ thông tin, toán tin. Việc hợp tác nước ngoài còn hạn chế do hệ sinh thái học thuật ít kết nối.

Như vậy, nhiệm vụ cấp bách đặt ra là cần mở rộng quy mô, nghiên cứu đổi mới chương trình đào tạo theo chuẩn quốc tế; chẳng hạn như Singapore đã khuyến khích liên kết các đại học với đối tác toàn cầu để giảng dạy “Data Science” theo mô hình quốc tế. Nghị định 169/2025/NĐ-CP khuyến khích đặc thù thu hút chuyên gia tài năng từ nước ngoài và Việt kiều về làm việc trong lĩnh vực dữ liệu. Việt Nam có thể thiết kế chương trình học bổng, xây dựng các trung tâm xuất sắc về AI, Big Data và tăng cường đầu tư nghiên cứu cơ bản liên ngành. Các doanh nghiệp công nghệ





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

lớn cũng cần được hưởng ưu đãi để tham gia đào tạo nhân lực (cơ chế GPDG), tạo hệ sinh thái hạt nhân phát triển kỹ năng (start-up, vườn ươm, bootcamp). Ngoài ra, chương trình “My Data” của Hàn Quốc cho phép công dân tự quản lý dữ liệu của mình, cho thấy tầm quan trọng của đào tạo nhận thức cộng đồng về dữ liệu.



**Hợp tác đào tạo, kết nối nhân tài công nghệ thông tin - Ảnh: VnEconomy**

Có thể thấy rằng, trong chuyển đổi số, yếu tố con người đóng vai trò quyết định thành công; do vậy, cần xây dựng đội ngũ cán bộ, chiến sĩ vừa có bản lĩnh chính trị vững vàng, lòng trung thành tuyệt đối, vừa có trình độ chuyên môn, nghiệp vụ, vừa có trình độ khoa học, công nghệ, nhất là công nghệ thông tin. Theo đó, giải pháp thực hiện nhiệm vụ này cần:

**Một là**, hiện đại hóa các cơ sở đào tạo trong Công an nhân dân; trong đó, đầu tư trọng điểm, nâng cấp các học viện, nhà trường Công an nhân dân thành các trung tâm đào tạo, nghiên cứu hàng đầu về khoa học dữ liệu, chuyển đổi số. Việc hiện đại hóa các cơ sở đào tạo trong Công an nhân dân là giải pháp mang tính chiến lược, có ý nghĩa quyết định trong việc chuẩn





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

bị nguồn nhân lực chất lượng cao phục vụ chuyển đổi số và quản lý dữ liệu quốc gia.

Trước hết, trong bối cảnh dữ liệu được xác định là tài nguyên chiến lược của đất nước, các học viện, trường đại học Công an nhân dân không chỉ đơn thuần đào tạo nghiệp vụ truyền thống, mà cần trở thành những trung tâm nghiên cứu - đào tạo hàng đầu về khoa học dữ liệu, công nghệ thông tin và chuyển đổi số. Điều này đòi hỏi sự đầu tư trọng điểm về hạ tầng công nghệ, phòng thí nghiệm an ninh mạng, trung tâm dữ liệu thực hành, cũng như các hệ thống mô phỏng để học viên có điều kiện rèn luyện kỹ năng xử lý tình huống sát thực tế.

Bên cạnh yêu tố hạ tầng, đổi mới chương trình và phương pháp giảng dạy là yêu cầu cấp bách. Các cơ sở đào tạo cần tích hợp các môn học về trí tuệ nhân tạo, phân tích dữ liệu lớn, an ninh mạng, quản trị dữ liệu, điện toán đám mây, đồng thời cập nhật các chuẩn mực quốc tế và thực tiễn quản lý dữ liệu của Việt Nam. Sự gắn kết chặt chẽ giữa đào tạo lý thuyết và thực hành sẽ giúp học viên có khả năng ứng dụng trực tiếp vào thực tiễn công tác.

Đặc biệt, hiện đại hóa cơ sở đào tạo cũng cần đi liền với hợp tác quốc tế và liên kết với các viện nghiên cứu, doanh nghiệp công nghệ hàng đầu. Thông qua các chương trình trao đổi, chuyển giao công nghệ và đồng nghiên cứu, đội ngũ cán bộ, giảng viên và học viên sẽ có cơ hội tiếp cận tri thức tiên tiến, nâng cao năng lực cạnh tranh trong môi trường số toàn cầu.

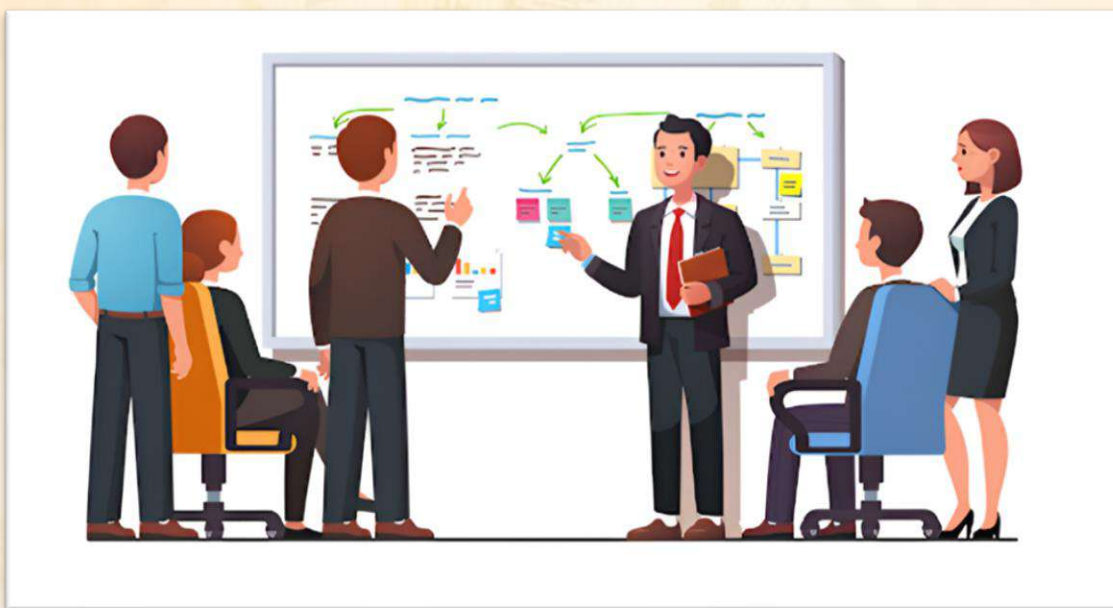
**Hai là**, triển khai chương trình đào tạo nguồn cán bộ phục vụ công tác chuyển đổi số trong lực lượng Công an nhân dân; bảo đảm có cơ chế đặc thù để phát hiện, tuyển chọn và đào tạo các học sinh, sinh viên xuất sắc trong các lĩnh vực công nghệ thông tin để tạo nguồn cán bộ kế cận chất lượng cao phục vụ lâu dài cho công tác quản lý nhà nước về dữ liệu, bảo đảm an ninh





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

quốc gia, trật tự, an toàn xã hội. Việc triển khai chương trình đào tạo nguồn cán bộ phục vụ công tác chuyển đổi số trong lực lượng Công an nhân dân mang ý nghĩa chiến lược lâu dài, bởi con người chính là nhân tố quyết định thành bại của quá trình hiện đại hóa quản lý dữ liệu và bảo đảm an ninh quốc gia trong kỷ nguyên số.



***Chú trọng công tác đào tạo, bồi dưỡng góp phần nâng cao chất lượng đội ngũ cán bộ phục vụ công tác chuyển đổi số trong lực lượng Công an nhân dân - Ảnh: Chi cục Quản lý thị trường Hà Tĩnh***

Trước hết, cần thiết lập một chương trình đào tạo toàn diện, chuyên sâu dành riêng cho cán bộ, chiến sĩ Công an nhân dân, với nội dung gắn chặt vào thực tiễn quản lý nhà nước về dữ liệu và nhiệm vụ bảo vệ an ninh mạng. Chương trình này không chỉ trang bị kiến thức nền tảng về công nghệ thông tin, an toàn thông tin, trí tuệ nhân tạo, phân tích dữ liệu lớn mà còn phải rèn luyện kỹ năng xử lý tình huống, ứng cứu sự cố và tư duy phản biện trước các thách thức an ninh phi truyền thống.

Đi đôi với đó, cần có cơ chế đặc thù để phát hiện, tuyển chọn và đào tạo nhân lực xuất sắc. Việc ưu tiên phát hiện các học sinh, sinh viên có thành





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

tích vượt trội trong lĩnh vực công nghệ thông tin và khoa học dữ liệu, sau đó đưa vào quy hoạch đào tạo chuyên biệt, sẽ tạo ra một thế hệ cán bộ kế cận có chất lượng cao, am hiểu công nghệ, gắn bó lâu dài với sự nghiệp bảo đảm an ninh dữ liệu quốc gia. Cơ chế đặc thù này phải bảo đảm tính cạnh tranh, minh bạch và khuyến khích tài năng trẻ cống hiến.

Đồng thời, chương trình đào tạo cũng cần gắn với mô hình huấn luyện thực tế và liên thông quốc tế, kết hợp giữa *lý thuyết - thực hành - nghiên cứu*, đồng thời tham khảo chuẩn mực tiên tiến trên thế giới. Thông qua hợp tác với các trường đại học, viện nghiên cứu và doanh nghiệp công nghệ trong và ngoài nước, lực lượng Công an nhân dân có thể tiếp cận công nghệ nguồn, phương pháp đào tạo hiện đại, từ đó nâng cao trình độ đội ngũ cán bộ.

**Ba là**, thực hiện hợp tác quốc tế phục vụ lợi ích bảo đảm an ninh dữ liệu quốc gia; chủ động và lựa chọn đối tác quốc tế để hợp tác, ưu tiên các quốc gia có công nghệ nguồn tiên tiến và có thiện chí trong việc chuyển giao công nghệ về xử lý dữ liệu, đào tạo chuyên gia, chia sẻ kinh nghiệm về quản trị, quản lý, bảo vệ dữ liệu, phòng, chống tội phạm mạng, nhất là tội phạm xuyên quốc gia. Mọi hoạt động hợp tác đều phải được tiến hành trên nguyên tắc bảo đảm an ninh, giữ bí mật nhà nước và không để các thể lực bên ngoài can thiệp vào công việc nội bộ.

Về *mục tiêu hợp tác*, hợp tác quốc tế phải hướng đến phục vụ trực tiếp lợi ích an ninh dữ liệu quốc gia. Điều này bao gồm tiếp thu công nghệ nguồn tiên tiến, nâng cao năng lực phân tích, xử lý dữ liệu, đồng thời tận dụng cơ hội đào tạo đội ngũ chuyên gia chất lượng cao.

Về *lựa chọn đối tác*, Việt Nam cần chủ động, có chọn lọc, ưu tiên hợp tác với các quốc gia và tổ chức uy tín, có thiện chí trong việc chuyển giao công nghệ, hỗ trợ kỹ thuật, chia sẻ kinh nghiệm. Trọng tâm là các





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

nước phát triển trong lĩnh vực an ninh mạng, trí tuệ nhân tạo, phân tích dữ liệu lớn.

*Về nội dung hợp tác*, tập trung vào các mảng thiết thực như chuyển giao công nghệ xử lý dữ liệu, hợp tác đào tạo chuyên gia an ninh mạng - dữ liệu, chia sẻ kinh nghiệm quản trị - quản lý dữ liệu, và phối hợp phòng chống tội phạm mạng, đặc biệt là tội phạm xuyên quốc gia.

*Về nguyên tắc hợp tác*: Mọi hoạt động hợp tác phải đặt dưới sự giám sát chặt chẽ, tuân thủ nguyên tắc bảo đảm an ninh, giữ vững bí mật nhà nước, không để các thế lực bên ngoài can thiệp vào công việc nội bộ. Nghĩa là, hợp tác chỉ có giá trị khi vừa đem lại lợi ích thực chất cho quốc gia, vừa bảo đảm tuyệt đối an toàn chủ quyền dữ liệu.

### ***- Tăng cường hợp tác quốc tế về dữ liệu***

Dữ liệu là nguồn tài nguyên không biên giới, vì vậy hợp tác quốc tế là xu hướng tất yếu. Luật Dữ liệu đã xác định nguyên tắc chủ quyền dữ liệu và yêu cầu phối hợp quốc tế. Theo điểm e, Khoản 1, Điều 8 Luật Dữ liệu, hợp tác quốc tế về khoa học, công nghệ, giáo dục và nguồn lực liên quan đến dữ liệu là một nội dung quản lý nhà nước. Điều 4 Nghị định 169/2025/NĐ-CP quy định rõ vai trò của Bộ Công an làm đầu mối quản lý hợp tác quốc tế về dữ liệu quan trọng, Bộ Quốc phòng phụ trách lĩnh vực quân sự, còn các bộ ngành, địa phương thực hiện trong phạm vi chức năng. Chiến lược Dữ liệu Quốc gia đến năm 2030 nhấn mạnh Việt Nam cần tận dụng năng lực của các nước phát triển, đồng thời đảm bảo an ninh, chủ quyền dữ liệu quốc gia.

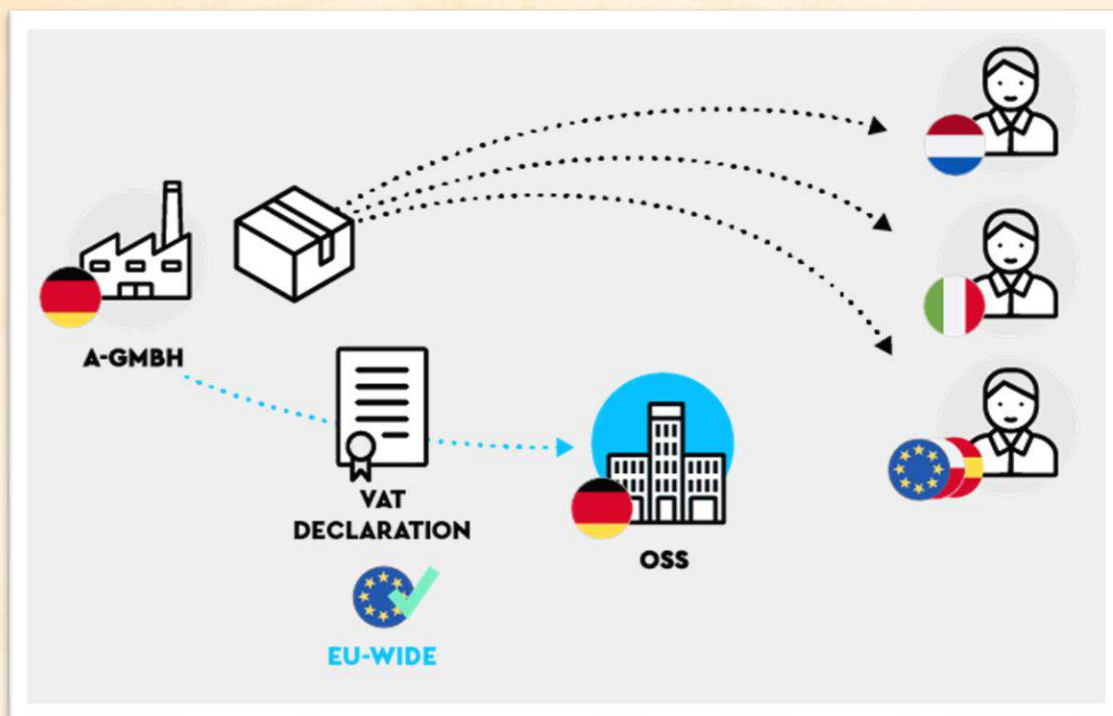
Thực tế, Việt Nam đã tham gia một số diễn đàn toàn cầu về dữ liệu, nhưng còn thiếu cơ chế hiệp định song phương/quốc tế về chia sẻ dữ liệu an toàn (mặc dù có cam kết ASEAN về Thương mại điện tử). Trong ASEAN,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Việt Nam cần bắt kịp các quy tắc chung như “*One Stop Shop*” (một cửa) của ASEAN về bảo vệ dữ liệu cá nhân. Về đối tác chiến lược, liên kết với EU, Mỹ trong các khuôn khổ số hóa (AIPA, EVFTA) sẽ giúp áp dụng tiêu chuẩn cao (ví dụ EU yêu cầu nghiêm ngặt trong GDPR và Data Act).



### ***Mô tả cách thức vận hành của One Stop Shop (OSS) - Ảnh: Taxdoo***

Không dừng lại ở đó, Việt Nam phải đẩy mạnh xây dựng chính sách ngoại giao dữ liệu gồm thương thảo thỏa thuận chia sẻ dữ liệu công - tư, công song phương cho dữ liệu quan trọng, dữ liệu cốt lõi. Tăng cường tham gia vào sáng kiến *Digital Economy Partnership Agreement* (DEPA) và chấp nhận chuẩn chung như GAIA-X là một sáng kiến nhằm phát triển một kế hoạch có khả năng phát triển một cơ sở hạ tầng dữ liệu an toàn liên bang cho Châu Âu. Việt Nam cũng cần hợp tác nghiên cứu quốc tế thông qua các dự án AI toàn cầu và sớm chuẩn bị ứng phó với quy định của các nền kinh tế lớn (như CCPA của Mỹ, hay IP5) để đảm bảo doanh nghiệp nội địa không bị mất cơ hội đầu tư, xuất khẩu dịch vụ.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

### *- Tăng cường giám sát, thanh tra, kiểm tra và xử lý vi phạm về dữ liệu*

Đây là nhiệm vụ trọng yếu, là công cụ bảo đảm công tác quản lý nhà nước về dữ liệu được thực thi có hiệu quả. Luật Dữ liệu quy định rõ các hành vi bị cấm và chế tài xử phạt. Ngay trong điểm đ, Khoản 1, Điều 8 Luật Dữ liệu buộc cơ quan chức năng phải thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm về dữ liệu. Điều 10 cấm lợi dụng dữ liệu để xâm phạm lợi ích quốc gia, dân tộc, quốc phòng, an ninh... Cơ chế ủy quyền quản lý cho Bộ Công an, Bộ Quốc phòng và các địa phương tại Khoản 2, Điều 8 cũng phân định rõ trách nhiệm giám sát, phối hợp. Ngoài ra, Luật An toàn thông tin mạng 2015 trao quyền cho các cơ quan chuyên trách như Cục An toàn Thông tin trực thuộc Bộ Thông tin và Truyền thông xử phạt vi phạm an ninh mạng (trước khi Bộ Thông tin và Truyền thông bàn giao nhiệm vụ bảo đảm an toàn thông tin mạng về Bộ Công an).

Tuy nhiên, lực lượng thanh tra dữ liệu hiện chưa thành lập chuyên biệt (như đội ngũ Cục Dữ liệu Quốc gia trong tương lai), và quy trình thanh tra chéo giữa các bộ, ban, ngành còn rời rạc. Chưa có quy định cụ thể về mức phạt hay cơ chế phối hợp với cơ quan điều tra khi vi phạm dữ liệu xuyên tỉnh, xuyên biên giới. Một số vi phạm mới phát sinh như buôn bán dữ liệu cá nhân trái phép qua mạng xã hội chưa được khắc phục kịp thời do pháp luật chưa bắt kịp.

Những tồn tại đó đòi hỏi Việt Nam phải có biện pháp nâng cấp hệ thống giám sát như thiết lập “*Trung tâm giám sát an ninh dữ liệu quốc gia*” để phối hợp theo thời gian thực (tương tự Trung tâm Giám sát an toàn không gian mạng quốc gia trước kia, nay đã chính thức dừng hoạt động vào ngày 28/2/2025 do các hoạt động chuyển giao nhiệm vụ). Mở rộng thẩm quyền thanh tra liên bộ (Bộ Công an chủ trì) đối với dữ liệu cốt lõi, dữ liệu quan





trọng; kết hợp thanh tra đột xuất, định kỳ với gắn trách nhiệm của người đứng đầu đơn vị khi vi phạm. Đặc biệt, tăng cường xử lý vi phạm trong lĩnh vực dữ liệu cá nhân theo Luật mới. Học hỏi theo EU, nên bổ nhiệm cơ quan giám sát cấp quốc gia (như Ủy ban bảo vệ dữ liệu) và buộc các cơ quan, tổ chức, doanh nghiệp dữ liệu phải công bố báo cáo theo định kỳ.

Trên cơ sở các phân tích trên, cần thực hiện trọng tâm một số nhiệm vụ sau:

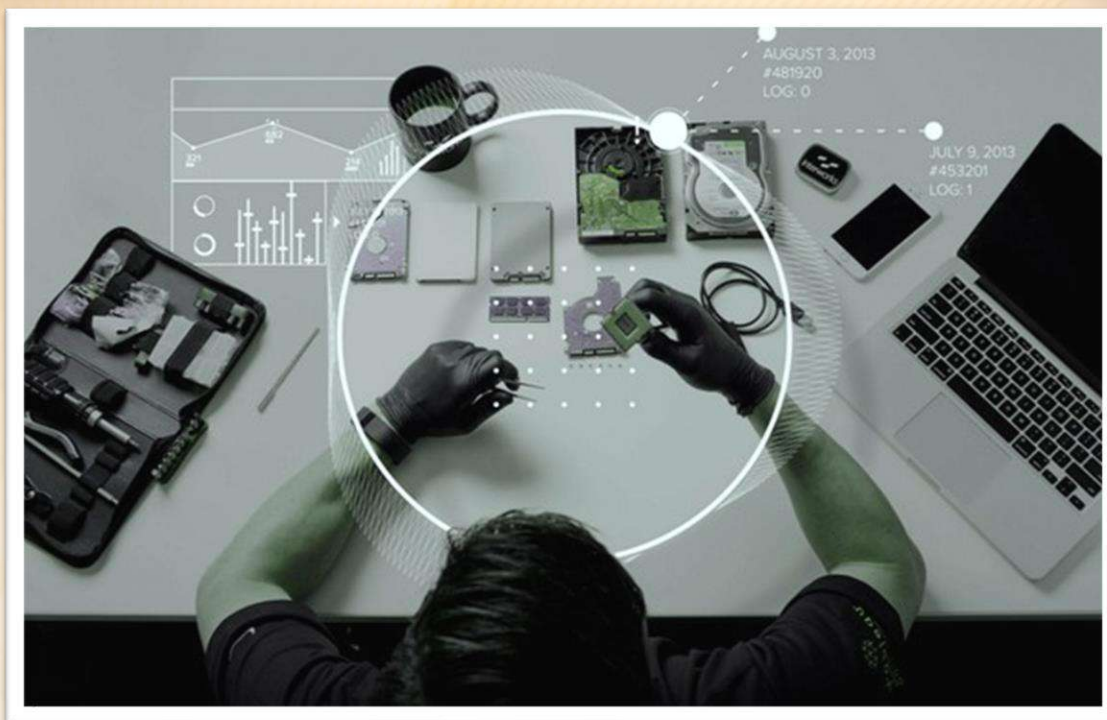
**Một là**, xây dựng đội ngũ tham mưu, hoàn thiện thể chế, pháp luật về dữ liệu; quản trị, quản lý, vận hành cơ sở dữ liệu, hạ tầng công nghệ thông tin một cách chuyên nghiệp, chính quy; đồng thời, nghiên cứu xây dựng, hoàn thiện một bộ phận chuyên biệt tại Công an các đơn vị, địa phương chịu trách nhiệm về điều tra, xử lý tội phạm trong lĩnh vực dữ liệu; tăng cường bồi dưỡng, đào tạo lực lượng chuyên trách có khả năng điều tra các vụ án công nghệ cao phức tạp, phòng, chống mua bán, đánh cắp dữ liệu, gián điệp dữ liệu... và trang bị các công cụ phòng thí nghiệm “pháp y số” hiện đại.

Một trong những giải pháp mang tính đột phá hiện nay là xây dựng lực lượng chuyên trách về dữ liệu trong Công an nhân dân theo hướng chính quy, hiện đại và chuyên biệt. Trước hết, cần hình thành đội ngũ tham mưu có đủ năng lực nghiên cứu, đề xuất và hoàn thiện thể chế, pháp luật về dữ liệu, bảo đảm khung khổ pháp lý luôn theo kịp thực tiễn chuyên đổi số. Song song, cần nghiên cứu thành lập một bộ phận chuyên biệt tại Công an các đơn vị, địa phương để trực tiếp phụ trách điều tra, xử lý tội phạm trong lĩnh vực dữ liệu - một loại hình tội phạm đang ngày càng gia tăng, tinh vi và mang tính xuyên quốc gia. Bộ phận này phải được trang bị các phòng thí nghiệm “pháp y số” hiện đại, có khả năng phục hồi, giám định và phân tích chứng cứ điện tử, qua đó nâng cao chất lượng điều tra, truy tố và xét xử.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



### *Pháp y số, nhiệm vụ đầy thử thách của lực lượng Công an Nhân dân - Ảnh: CIO Vietnam*

Đồng thời, cần có chính sách phát triển nguồn nhân lực chuyên sâu: tăng cường bồi dưỡng, đào tạo lực lượng cán bộ, chiến sĩ có khả năng điều tra các vụ án công nghệ cao, nắm vững kỹ năng phòng, chống mua bán dữ liệu, đánh cắp thông tin, gián điệp mạng. Việc đào tạo phải gắn với mô hình huấn luyện thực tế, cập nhật công nghệ mới và tham khảo chuẩn mực quốc tế, tạo ra một đội ngũ tinh nhuệ, có khả năng xử lý các vụ việc phức tạp cả trong nước lẫn xuyên biên giới.

*Điểm mới của giải pháp này* không chỉ nằm ở việc hiện đại hóa cơ sở hạ tầng kỹ thuật, mà còn ở tư duy quản trị dữ liệu theo hướng chuyên nghiệp, chính quy và chuyên biệt, biến dữ liệu thành một lĩnh vực nghiệp vụ trọng điểm trong Công an nhân dân. Qua đó, lực lượng không chỉ hoàn thành tốt nhiệm vụ quản lý nhà nước về dữ liệu, mà còn chủ động, hiệu quả trong phát





hiện, phòng ngừa và đấu tranh với các loại tội phạm công nghệ cao, góp phần giữ vững an ninh quốc gia, trật tự an toàn xã hội trong kỷ nguyên số.

**Hai là**, tiếp tục hoàn thiện quy định về thu thập và sử dụng chứng cứ là dữ liệu điện tử như ban hành các quy định, quy trình chuẩn hóa, chặt chẽ về việc thu thập, phục hồi, phân tích và trình bày chứng cứ là dữ liệu điện tử, bảo đảm tính hợp pháp, khách quan và toàn vẹn của chứng cứ, đáp ứng yêu cầu của công tác tổ tụng hình sự trong bối cảnh mới. Giải pháp hoàn thiện quy định về thu thập và sử dụng chứng cứ là dữ liệu điện tử có ý nghĩa then chốt trong bảo đảm hiệu quả đấu tranh phòng, chống tội phạm công nghệ cao, đồng thời đáp ứng yêu cầu tổ tụng hình sự trong bối cảnh chuyển đổi số.

Trước hết, cần ban hành các quy định và quy trình chuẩn hóa, chặt chẽ về thu thập, phục hồi, phân tích và trình bày chứng cứ điện tử. Quy trình này phải quy định rõ thẩm quyền, trách nhiệm, phương pháp nghiệp vụ và chuẩn mực kỹ thuật, bảo đảm rằng mọi dữ liệu thu thập được đều có nguồn gốc hợp pháp, không bị sai lệch, và có thể được chấp nhận trước tòa án. Điều này đòi hỏi sự phối hợp giữa các cơ quan tổ tụng và lực lượng chuyên trách trong Công an nhân dân, từ giai đoạn khám nghiệm hiện trường số, phục hồi dữ liệu bị xóa, đến việc lập biên bản và bảo quản chứng cứ.

Tiếp theo, phải xây dựng chuẩn mực pháp lý và kỹ thuật về bảo đảm tính toàn vẹn và khách quan của chứng cứ điện tử. Các biện pháp như mã hóa, băm dữ liệu (hashing), chữ ký số, niêm phong điện tử cần được áp dụng để bảo vệ dữ liệu khỏi bị thay đổi trong quá trình thu thập, lưu trữ và phân tích. Đồng thời, việc phân tích và trình bày chứng cứ trước tòa phải tuân thủ nguyên tắc khách quan, minh bạch, dễ kiểm chứng, bảo đảm quyền lợi của bị can, bị cáo và những người liên quan.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Ngoài ra, cần tiếp tục đồng bộ hóa pháp luật trong nước với chuẩn mực quốc tế về chứng cứ điện tử, nhất là các công ước và hiệp định mà Việt Nam tham gia, như Công ước Budapest về tội phạm mạng. Điều này giúp nâng cao giá trị pháp lý của chứng cứ điện tử trong hợp tác điều tra quốc tế, đặc biệt là các vụ án xuyên biên giới.

**Ba là,** đẩy mạnh hợp tác quốc tế trong đấu tranh tội phạm; tăng cường ký kết và thực thi các hiệp định tương trợ tư pháp về hình sự, các thỏa thuận hợp tác với cơ quan thực thi pháp luật các nước và các tổ chức quốc tế (như INTERPOL) để phối hợp điều tra, truy bắt và dẫn độ các đối tượng tội phạm trong lĩnh vực dữ liệu đang lẫn trốn ở nước ngoài. Giải pháp đẩy mạnh hợp tác quốc tế trong đấu tranh tội phạm dữ liệu mang ý nghĩa đặc biệt quan trọng trong bối cảnh tính chất xuyên biên giới của tội phạm công nghệ cao ngày càng gia tăng.

Trước hết, cần tăng cường ký kết và thực thi các hiệp định tương trợ tư pháp về hình sự, coi đây là công cụ pháp lý nền tảng để tạo hành lang hợp tác trong thu thập chứng cứ, dẫn độ, chuyển giao người phạm tội và hỗ trợ điều tra xuyên quốc gia. Những hiệp định này giúp các cơ quan tiến hành tố tụng của Việt Nam có cơ sở vững chắc khi phối hợp với đối tác nước ngoài, bảo đảm việc xử lý tội phạm không bị gián đoạn do khác biệt về pháp luật và thủ tục.

Tiếp theo, Việt Nam cần mở rộng các thỏa thuận hợp tác song phương và đa phương với cơ quan thực thi pháp luật các nước, nhất là những quốc gia có thể mạnh về điều tra tội phạm mạng và quản trị dữ liệu. Thông qua các kênh hợp tác này, các bên có thể chia sẻ thông tin tình báo về tội phạm, phối hợp điều tra đồng thời, truy bắt nhanh chóng và xử lý hiệu quả các đường dây tội phạm dữ liệu.





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

Đặc biệt, việc hợp tác với các tổ chức quốc tế như INTERPOL, ASEANAPOL, UNODC có vai trò then chốt trong việc thiết lập mạng lưới toàn cầu phòng, chống tội phạm dữ liệu. Đây là kênh để Việt Nam tham gia trao đổi thông tin, cập nhật cảnh báo sớm, phối hợp điều tra và truy bắt các đối tượng tội phạm công nghệ cao đang lẩn trốn ở nước ngoài.

### *- Phát triển thị trường và hệ sinh thái dữ liệu*

Thị trường dữ liệu là động lực tạo giá trị từ nguồn tài nguyên này. Theo Luật Dữ liệu, Nhà nước thành lập Quỹ Phát triển dữ liệu quốc gia nhằm tài trợ không lợi nhuận cho các hoạt động xây dựng, ứng dụng dữ liệu. Luật cũng nhấn mạnh phát triển sản phẩm, dịch vụ dữ liệu (điểm d khoản 1 Điều 8) để hình thành thị trường dữ liệu. Chiến lược dữ liệu quốc gia đến năm 2030 đề cập tới mục tiêu bảo vệ người yếu thế và chống độc quyền dữ liệu khi xây dựng thị trường số.



*Sáu doanh nghiệp trụ cột đang cách mạng  
ngành công nghệ Việt Nam - Ảnh: VnEconomy*





Hiện nay, thị trường dữ liệu Việt Nam đang ở giai đoạn đầu. Một số công ty về Công nghệ Thông tin và Truyền thông (ICT) lớn bắt đầu cung cấp dịch vụ “cloud” và phân tích dữ liệu, song các sản phẩm dịch dữ liệu, nền tảng dữ liệu mở còn rất ít. Khung chính sách ưu đãi còn hạn chế, thủ tục cấp phép trung gian dữ liệu mới được quy định trong Nghị định 169/2025/NĐ-CP (cấp giấy chứng nhận sản dữ liệu, dịch vụ trung gian).

Trong khi đó, khối lượng dữ liệu thô còn phân tán, chưa được thương mại hóa rộng rãi. Do đó, một trong những nhiệm vụ trọng tâm là phải xây dựng cơ chế khuyến khích như giảm thuế, hỗ trợ vốn cho “start-up” dữ liệu; đơn giản hóa thủ tục cấp phép sản dữ liệu, dịch vụ trung gian, phân tích, tổng hợp dữ liệu và sớm ban hành nghị định cho phép hình thành các nền tảng dữ liệu công (public data spaces). Nhà nước có thể ban hành quy chế ưu đãi cho “người chia sẻ dữ liệu” (ví dụ giảm thuế cho tổ chức chia sẻ dữ liệu ít nhất 70% cho cộng đồng). Để phát triển hệ sinh thái, cần khuyến khích hợp tác công - tư trong Trung tâm sáng tạo, khai thác dữ liệu, hỗ trợ nghiên cứu liên kết trong đào tạo nguồn nhân lực tương tự như chính sách Singapore ưu đãi đặc thù cho công tác nghiên cứu và phát triển dữ liệu...

Bên cạnh đó, công tác quản lý cần công bằng, minh bạch để thị trường cạnh tranh lành mạnh. Nghị định 165/2025/NĐ-CP yêu cầu đánh giá tác động chuyển dữ liệu xuyên biên giới để đảm bảo lợi ích quốc gia và quyền cá nhân. Các ví dụ quốc tế như EU Data Act cũng đặt ra quy định rõ ràng về chia sẻ và truy xuất dữ liệu giữa doanh nghiệp và nhà nước. Việc học hỏi mô hình này sẽ giúp Việt Nam phát triển thị trường dữ liệu dựa trên khung pháp lý chặt chẽ và minh bạch.

Bên cạnh việc phát triển, cần nhận thức được việc quản lý thị trường dữ liệu cũng rất quan trọng, cần phải được thực hiện một cách chặt chẽ, không





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

để các hoạt động kinh tế này tác động xấu đến an ninh quốc gia, trật tự an toàn xã hội; giải pháp để thực hiện nhiệm vụ này cần: **(1)** Triển khai thiết lập các sản dữ liệu, bảo đảm cơ chế thẩm định trước khi giao dịch, cơ chế chứng nhận sở hữu, quản lý dữ liệu sau giao dịch; theo đó, cần định hướng bất kỳ hoạt động nào liên quan đến việc mua bán, trao đổi các bộ dữ liệu lớn, nhạy cảm hoặc có sự tham gia của yếu tố nước ngoài đều phải trải qua một quy trình thẩm định an ninh do cơ quan chức năng thực hiện. Việc này nhằm ngăn chặn nguy cơ dữ liệu trọng yếu quốc gia bị bán ra nước ngoài hoặc bị các thế lực thù địch thu gom; **(2)** Thúc đẩy phát triển công nghệ an ninh “*make in Vietnam*”: Nhà nước cần có chương trình đầu tư chiến lược, đặt hàng các doanh nghiệp công nghệ trong nước nghiên cứu, phát triển và làm chủ công nghệ cốt lõi về an ninh, bảo mật, mã hóa, giám sát an ninh, các phần mềm phân tích, tổng hợp dữ liệu của nước ta... Việc tự chủ công nghệ sẽ giúp loại bỏ rủi ro từ các sản phẩm nước ngoài có thể chứa mã độc, bảo vệ nền tảng công nghiệp dữ liệu, thị trường dữ liệu của quốc gia; **(3)** Tiếp tục tăng cường quản lý các nền tảng xuyên biên giới: trong đó, tập trung xây dựng quy trình thẩm định các sản phẩm trí tuệ nhân tạo, sản phẩm trung gian, phân tích, tổng hợp dữ liệu để “*sàng lọc*” kỹ trước khi đưa vào ứng dụng, khai thác, kinh doanh, phục vụ nhu cầu của cơ quan, tổ chức, cá nhân; giảm thiểu nguy cơ mất an ninh, an toàn dữ liệu, thu thập, khai thác, sử dụng dữ liệu trái phép.

*Tổng kết lại*, để thực hiện có hiệu quả công tác quản lý nhà nước về dữ liệu, Việt Nam cần tiếp tục hoàn thiện thể chế, đẩy mạnh đầu tư hạ tầng, tăng cường an ninh, ưu tiên đào tạo nhân lực, đẩy mạnh hợp tác quốc tế và phát triển thị trường dữ liệu. Mỗi nhóm nhiệm vụ trên đều mối quan hệ biện chứng, tác động lẫn nhau: khung pháp lý và cơ chế là nền tảng; hạ tầng và công nghệ là điều kiện; an ninh và pháp chế bảo đảm hoạt động bền





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

vững; nhân lực và hợp tác quốc tế đảm bảo nguồn lực; giám sát và thị trường thúc đẩy hiệu quả triển khai. Quá trình này sẽ được dẫn dắt bởi các quy định cụ thể trong Luật Dữ liệu 2024 và các văn bản hướng dẫn, đồng thời học hỏi, tiếp thu, sáng tạo từ những kinh nghiệm quốc tế như GDPR, X-Road, GDA, Data Dam, để tạo nên một hệ sinh thái dữ liệu quốc gia phù hợp thực tiễn Việt Nam và hội nhập sâu rộng trong khu vực cũng như toàn cầu.

*- Tuyên truyền, phổ biến nhằm xây dựng thể trận An ninh nhân dân trong công tác xây dựng, quản trị, quản lý, xử lý, bảo vệ dữ liệu.*

Đây là nhiệm vụ chuyên hóa nhận thức của mỗi người dân thành ý thức cảnh giác của toàn xã hội, để chủ động phát hiện và đấu tranh với các thông tin sai trái, thù địch, xâm phạm an ninh dữ liệu của quốc gia; giải pháp để thực hiện nhiệm vụ này cần:

**Một là**, triển khai các chiến dịch tuyên truyền, phổ biến, nâng cao cảnh giác trong công tác bảo vệ dữ liệu sâu rộng đến tổ chức, cá nhân, tăng cường phối hợp đồng bộ với các bộ, ban, ngành, đoàn thể triển khai các chiến dịch truyền thông nhằm nâng cao khả năng nhận diện âm mưu, phương thức, thủ đoạn hoạt động của thế lực thù địch, tội phạm trong hoạt động quản lý, quản trị, xử lý, bảo vệ dữ liệu. Tích hợp nội dung giáo dục về bảo vệ dữ liệu, bảo đảm an ninh, an toàn thông tin, an ninh mạng, kỹ năng nhận diện tin giả, dữ liệu xấu, độc vào chương trình giáo dục phổ thông. Qua đó, xây dựng “lá chắn”, tăng cường “sức đề kháng” mạnh mẽ trong toàn xã hội trước các cuộc tấn công xâm phạm đến quyền, lợi ích hợp pháp của chủ thể dữ liệu, chủ sở hữu dữ liệu.

**Hai là**, thiết lập và phổ biến các kênh tương tác với quần chúng nhân dân trong việc đảm bảo an ninh dữ liệu: Công an các đơn vị, địa phương cần





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

xây dựng và quảng bá rộng rãi các kênh chính thức, an toàn (qua ứng dụng VneID, mạng xã hội, đường dây nóng...) để người dân có thể dễ dàng, bí mật tố giác tội phạm, báo tin về các hoạt động khả nghi liên quan đến thu thập, mua bán dữ liệu trái phép, góp phần vào công tác phòng ngừa, đấu tranh, chống tội phạm từ sớm, từ xa.

**Ba là**, bồi dưỡng lớp nghiệp vụ bảo vệ dữ liệu cho lực lượng Công an tại cơ sở; tổ chức lớp tập huấn chuyên sâu cho lực lượng Công an cấp xã về kỹ năng trong công tác thu thập, khai thác, sử dụng, bảo vệ dữ liệu; nhất là trong thu thập chứng cứ số và hướng dẫn người dân các biện pháp tự bảo vệ, biến mỗi cán bộ cơ sở thành một điểm tựa an ninh tin cậy. Tiếp tục đẩy mạnh phong trào “*Bình dân học vụ số*”, mở rộng các nền tảng số khác trong bồi dưỡng, tập huấn kiến thức về công nghệ số cho cán bộ, chiến sĩ Công an nhân dân.

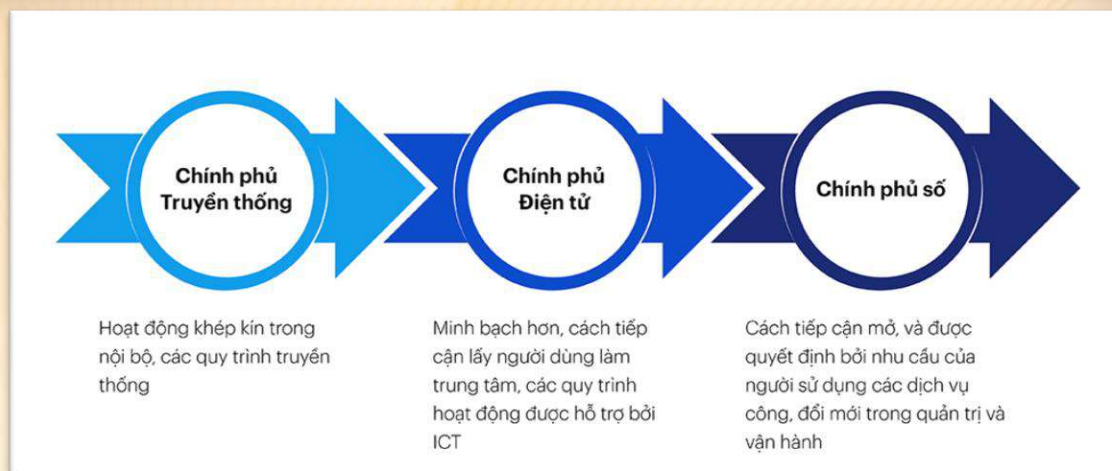
### **8.3.4. Đề xuất lộ trình triển khai trong giai đoạn 2025 - 2030 nhằm nâng cao hiệu quả quản lý nhà nước về dữ liệu**

Để nâng cao hiệu quả quản lý nhà nước về dữ liệu trong thời gian tới, Việt Nam sẽ triển khai một lộ trình đồng bộ từ nay đến năm 2030 với ba giai đoạn chính: **(1)** giai đoạn 2025 - 2026, **(2)** giai đoạn 2027 - 2028 và **(3)** giai đoạn 2029 - 2030. Lộ trình này bám sát các định hướng trong Luật Dữ liệu 2024 (được Quốc hội thông qua ngày 30/11/2024, có hiệu lực từ ngày 01/7/2025) và các văn bản liên quan như Nghị định 165/2025/NĐ-CP (ban hành 30/6/2025) quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu. Bên cạnh đó, lộ trình cũng đảm bảo sự nhất quán với các luật hiện hành về an toàn thông tin mạng và bảo vệ dữ liệu cá nhân, tuân thủ tinh thần chỉ đạo của Đảng và Nhà nước về chuyển đổi số và quản trị dữ liệu.





# BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*



## ***Xây dựng Chính phủ số bắt đầu từ đâu? - Ảnh: FPT Digital***

Cụ thể, *trong giai đoạn 2025 - 2026*, trọng tâm là hoàn thiện thể chế pháp lý và xây dựng hạ tầng dữ liệu quốc gia cơ bản. *Giai đoạn 2027 - 2028* tập trung liên thông dữ liệu trên phạm vi toàn quốc và tăng cường bảo mật, giám sát. Và cuối cùng, *giai đoạn 2029 - 2030* hướng đến hoàn thiện hệ sinh thái dữ liệu và hội nhập quốc tế về dữ liệu. Các mục tiêu này nhằm xây dựng Chính phủ số dựa trên dữ liệu, nơi dữ liệu trở thành “*tài nguyên mới*”, được chia sẻ liên thông và khai thác hiệu quả phục vụ quản lý nhà nước, kinh tế số và xã hội số.

### ***8.3.4.1. Giai đoạn 2025 - 2026: Hoàn thiện thể chế pháp lý và xây dựng hạ tầng dữ liệu quốc gia cơ bản***

**Mục tiêu chính:** Hoàn thiện khung pháp lý về quản lý dữ liệu và xây dựng hạ tầng dữ liệu quốc gia nền tảng, kết nối các cơ sở dữ liệu trọng yếu, với các nhiệm vụ trọng tâm như sau:

+ ***Hoàn thiện khung pháp lý và chính sách:*** Tiếp tục ban hành các văn bản hướng dẫn Luật Dữ liệu 2024, bao gồm các nghị định và thông tư chi tiết. Ngay trong năm 2025, Chính phủ đã ban hành Nghị định 165/2025/NĐ-CP hướng dẫn thi hành Luật Dữ liệu, Nghị định 169/2025/NĐ-CP quy định





hoạt động khoa học, công nghệ và đổi mới sáng tạo trong quản trị, xử lý, sử dụng dữ liệu, cũng như điều kiện kinh doanh các dịch vụ dữ liệu (trung gian dữ liệu, phân tích, tổng hợp dữ liệu, sàn dữ liệu). Đồng thời, cần rà soát, cập nhật các quy định pháp luật liên quan về an toàn thông tin mạng và bảo vệ dữ liệu cá nhân để đồng bộ với Luật Dữ liệu. Việc thống nhất pháp lý đảm bảo rằng Luật Dữ liệu mới không chồng chéo với Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018 và các luật khác; nếu có mâu thuẫn thì xác định rõ áp dụng Luật Dữ liệu hay luật chuyên ngành nhằm tạo hành lang pháp lý đầy đủ cho quản lý, chia sẻ dữ liệu và bảo vệ quyền riêng tư trong môi trường số.

**+ Xây dựng, phát triển hạ tầng dữ liệu quốc gia:** Triển khai xây dựng, hoàn thiện và vận hành Trung tâm Dữ liệu Quốc gia và các trung tâm dữ liệu vùng, đảm bảo năng lực lưu trữ, tính liên thông và dự phòng. Thực tế, Chính phủ đã phê duyệt Đề án Trung tâm Dữ liệu quốc gia, giao Bộ Công an thành lập Trung tâm này như một đơn vị cấp Cục thuộc Bộ. Ngày 25/02/2025, Bộ Công an tổ chức lễ công bố thành lập Trung tâm Dữ liệu quốc gia, với nhiệm vụ tích hợp, đồng bộ, lưu trữ và chia sẻ dữ liệu từ các cơ sở dữ liệu quốc gia và chuyên ngành. Đồng thời, Thủ tướng Chính phủ đặt mục tiêu đưa Trung tâm Dữ liệu quốc gia vào vận hành từ ngày 19/8/2025, coi đây là “trái tim” của hạ tầng dữ liệu quốc gia. Cùng với trung tâm trung ương, các cơ sở dữ liệu quốc gia quan trọng (dân cư, đất đai, doanh nghiệp, tài chính, bảo hiểm, giáo dục, y tế,...) phải được hoàn thiện và kết nối liên thông trên phạm vi cả nước. Tất cả các bộ, ngành, địa phương cần kết nối cơ sở dữ liệu của mình với Cổng dữ liệu quốc gia (data.gov.vn) - cổng này đã được Bộ Thông tin và Truyền thông (cũ) khởi động từ 31/8/2020 làm đầu mối công bố dữ liệu mở và thông tin chia sẻ dữ liệu của





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

các cơ quan nhà nước. Cổng dữ liệu quốc gia vừa là nơi các cơ quan đăng tải dữ liệu dùng chung, vừa là nơi người dân, doanh nghiệp tiếp cận dữ liệu mở phục vụ nghiên cứu, đổi mới sáng tạo. Việc kết nối liên thông tuân thủ Khung Kiến trúc Chính phủ điện tử Việt Nam và triển khai qua Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NDXP). NDXP đóng vai trò “*xương sống*” cho kết nối dữ liệu toàn quốc, đã liên thông hệ thống của hơn 90 cơ quan và xử lý trung bình 500.000 giao dịch chia sẻ dữ liệu mỗi ngày. Các hệ thống thông tin, cơ sở dữ liệu mới khi xây dựng đều phải sẵn sàng kết nối vào NDXP theo quy định tại Nghị định 47/2020/NĐ-CP. Về tiêu chuẩn kỹ thuật, hạ tầng dữ liệu quốc gia được thiết kế đáp ứng các chuẩn mực quốc tế về an toàn thông tin (như ISO/IEC 27001) để đảm bảo an ninh, bảo mật và khả năng khôi phục dữ liệu sau sự cố.

+ **Đào tạo và phát triển nhân lực:** Tổ chức các khóa đào tạo chuyên sâu về quản trị dữ liệu, phân tích dữ liệu và an ninh dữ liệu cho đội ngũ cán bộ, công chức, viên chức. Đặc biệt, đội ngũ quản lý tại Bộ Công an, Cơ quan chủ trì Trung tâm Dữ liệu quốc gia, và các đơn vị phụ trách cơ sở dữ liệu ở bộ, ngành cần được bồi dưỡng kỹ năng mới để vận hành hệ thống dữ liệu lớn an toàn, hiệu quả. Song song, thúc đẩy hợp tác với các cơ sở đào tạo trong nước và quốc tế nhằm phát triển nguồn nhân lực chất lượng cao về khoa học dữ liệu và quản lý dữ liệu. Việc hình thành các chương trình liên kết đào tạo, học bổng, trao đổi chuyên gia sẽ giúp Việt Nam xây dựng đội ngũ chuyên gia đáp ứng yêu cầu của kỷ nguyên dữ liệu. Ngoài ra, tập trung phát triển Quỹ đổi mới sáng tạo về khoa học dữ liệu để hỗ trợ cá nhân, doanh nghiệp khởi nghiệp trong lĩnh vực dữ liệu, qua đó nuôi dưỡng nhân tài và ý tưởng mới phục vụ chuyển đổi số quốc gia.





## CHIẾN LƯỢC DỮ LIỆU QUỐC GIA ĐẾN NĂM 2030

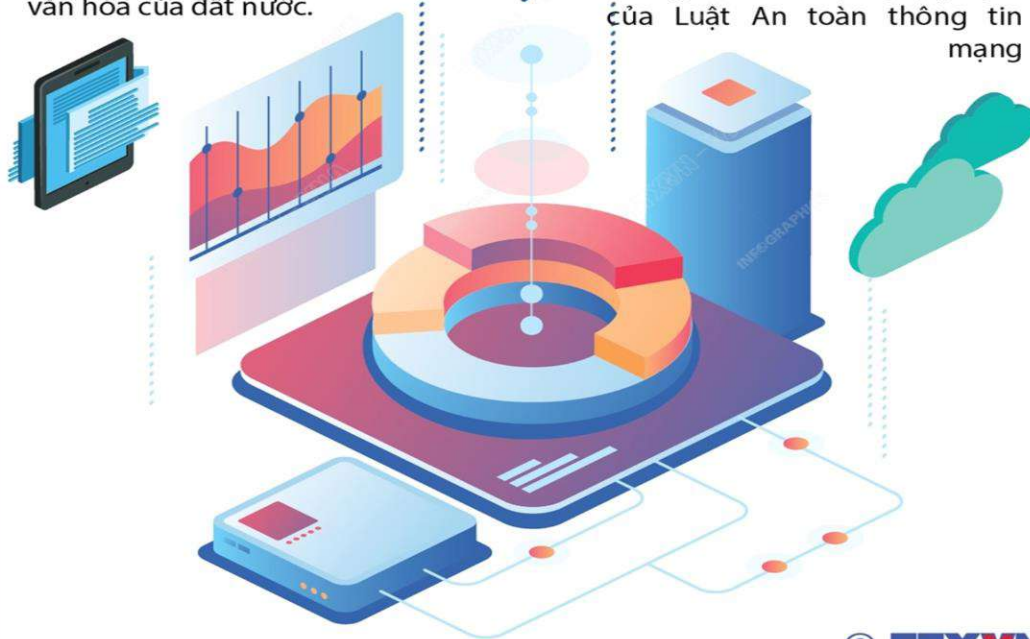
# PHÁT TRIỂN HẠ TẦNG DỮ LIỆU

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

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

Các Nền tảng điện toán đám mây Chính phủ và các Nền tảng ứng dụng trên thiết bị di động Make in Viet Nam đảm bảo sẵn

sàng đáp ứng **100%** nhu cầu lưu trữ, thu thập, kết nối, chia sẻ dữ liệu của Việt Nam, nhu cầu đảm bảo an toàn thông tin, an ninh mạng và bảo mật thông tin theo cấp độ quy định của Luật An toàn thông tin mạng



<http://infographics.vn>

© **TTXVN**  
Vietnam News Agency

### **Ảnh: Smart Nation and Digital Government Office**

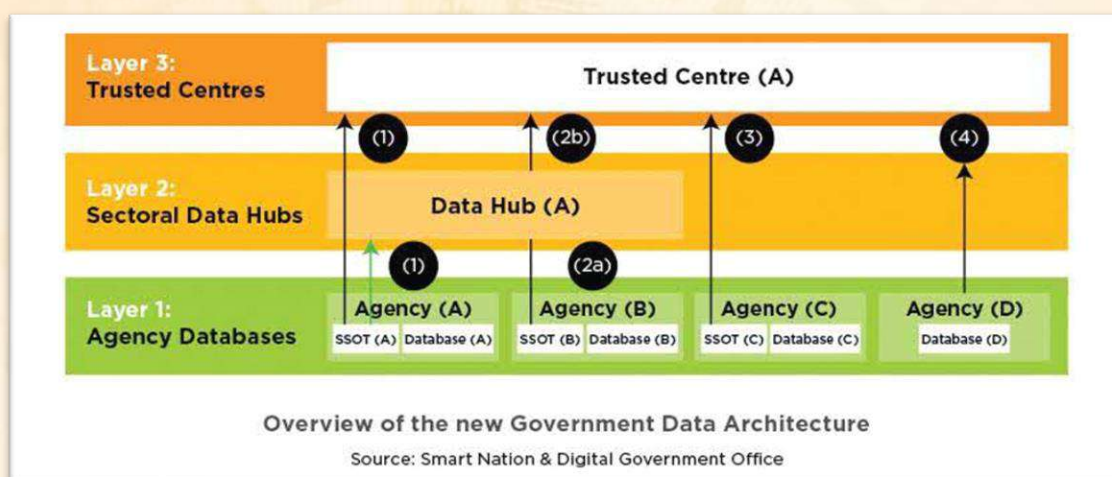
+ **Kinh nghiệm từ thực tiễn:** Singapore là quốc gia đi đầu trong xây dựng hạ tầng dữ liệu Chính phủ. Năm 2019, Singapore triển khai Government Data Architecture (GDA) là kiến trúc dữ liệu Chính phủ cho phép các cơ quan công quyền chia sẻ dữ liệu một cách an toàn và hiệu





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

quả. GDA thiết lập các “*nguồn dữ liệu tin cậy duy nhất*” và các trung tâm dữ liệu tin cậy, giúp bảo đảm dữ liệu chia sẻ giữa các cơ quan luôn sạch và đáng tin cậy. Nhờ đó, Singapore tạo nền tảng hạ tầng dữ liệu đồng bộ trên toàn chính phủ, hỗ trợ ra quyết định và cung cấp dịch vụ công nhanh chóng, minh bạch.



### **Mô hình hoạt động của Government Data Architecture -**

#### **8.3.4.2. Giai đoạn 2027 - 2028: Liên thông dữ liệu toàn quốc và tăng cường bảo mật, giám sát, đảm bảo an ninh, an toàn dữ liệu**

**Mục tiêu chính:** Hoàn thiện liên thông dữ liệu giữa các cấp, các ngành trên quy mô toàn quốc; đồng thời nâng cao năng lực giám sát, bảo mật dữ liệu, đảm bảo an toàn thông tin trong mọi hoạt động số của chính phủ; với các nhiệm vụ trọng tâm như sau

+ **Liên thông và chia sẻ dữ liệu:** Phát triển toàn diện mạng lưới kết nối dữ liệu quốc gia. Trong giai đoạn này, Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NDXP) sẽ được nâng cấp để liên thông tất cả các bộ, ngành và địa phương. Mục tiêu là mọi cơ sở dữ liệu quốc gia và chuyên ngành (dân cư, đất đai, doanh nghiệp, thuế, bảo hiểm xã hội, giáo dục, y tế,...) đều tích hợp vào một hệ thống chung, cho phép trao đổi dữ liệu thông suốt từ trung ương





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

đến địa phương. Các cơ quan nhà nước thực hiện kết nối theo mô hình phân tán thông qua NDXP và các nền tảng chia sẻ cấp bộ, tỉnh (chẳng hạn như LGSP), bảo đảm dữ liệu được liên thông theo thời gian thực phục vụ công tác nghiệp vụ. Một nguyên tắc quan trọng là thực hiện triệt để cơ chế “*một lần khai báo*” - người dân, doanh nghiệp chỉ cần cung cấp dữ liệu một lần, các cơ quan sẽ chia sẻ cho nhau thay vì yêu cầu lặp lại. Để đạt được điều này, giai đoạn 2027 - 2028 sẽ hoàn thiện tính tương thích liên thông giữa các hệ thống: chuẩn hóa định dạng dữ liệu, danh mục dùng chung, API kết nối, cũng như mở rộng các dịch vụ nền tảng (như dịch vụ định danh và xác thực điện tử, chữ ký số) hỗ trợ cho việc chia sẻ dữ liệu xuyên suốt. Đặc biệt, tập trung tích hợp các cơ sở dữ liệu lõi (dữ liệu “gốc” về dân cư, doanh nghiệp, đất đai...) vào Kho dữ liệu tổng hợp quốc gia đặt tại Trung tâm Dữ liệu quốc gia. Kho dữ liệu tổng hợp này sẽ đóng vai trò cung cấp dữ liệu tập trung, thống nhất cho các cơ quan khai thác, vừa tránh trùng lặp vừa hỗ trợ phân tích chuyên sâu phục vụ hoạch định chính sách.



*Minh họa về tích hợp dữ liệu - Ảnh: ELCOM*





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

+ **Tăng cường bảo mật và giám sát dữ liệu:** Cùng với mở rộng kết nối, giai đoạn này đặt trọng tâm vào an ninh dữ liệu. Triển khai hệ thống giám sát an toàn thông tin hiện đại, ứng dụng trí tuệ nhân tạo (AI) và học máy (ML) để phát hiện sớm các hành vi bất thường hoặc truy cập trái phép vào hệ thống dữ liệu nhà nước. Hệ thống này sẽ theo dõi lưu lượng và nhật ký truy cập trên NDXP cũng như các cơ sở dữ liệu trọng yếu, tự động cảnh báo và ngăn chặn các cuộc tấn công mạng hoặc rò rỉ dữ liệu. Song song đó, hoàn thiện các cơ chế bảo vệ dữ liệu cá nhân và dữ liệu nhạy cảm. Ngày 01/01/2026, Việt Nam sẽ chính thức thi hành Luật Bảo vệ dữ liệu cá nhân năm 2025, với các quy định chặt chẽ hơn về xử lý, lưu trữ và chuyển dữ liệu cá nhân ra nước ngoài. Việc xử lý vi phạm dữ liệu xuyên biên giới cũng được chú trọng thông qua hợp tác quốc tế. Đặc biệt, trong bối cảnh Quy định chung về bảo vệ dữ liệu của EU (GDPR) đã thiết lập các tiêu chuẩn cao về quyền riêng tư, Việt Nam cần học hỏi và tiệm cận các chuẩn mực này để bảo vệ công dân của mình khi dữ liệu được truyền qua biên giới. Các cơ quan sẽ xây dựng cơ chế phối hợp với đối tác quốc tế nhằm điều tra và xử lý triệt để, hiệu quả các vụ vi phạm dữ liệu có yếu tố nước ngoài, đảm bảo “không vùng cấm” trong bảo vệ dữ liệu cá nhân.

+ **Kinh nghiệm từ thực tiễn:** Estonia là hình mẫu về liên thông dữ liệu và an ninh dữ liệu cấp quốc gia. Quốc gia này vận hành hệ thống “X-Road”, một lớp trao đổi dữ liệu an toàn kết nối hơn 450 cơ quan công và tư, cung cấp trên 3.000 dịch vụ số cho người dân [56]. X-Road cho phép các bộ, ngành chia sẻ dữ liệu an toàn, nhanh chóng mà không cần tập trung dữ liệu vào một kho chung (tránh rủi ro điểm lỗi duy nhất). Mỗi cơ quan giữ cơ sở dữ liệu riêng nhưng có thể kết nối qua X-Road để trao đổi thông tin theo thời gian thực. Nhờ đó, công dân Estonia chỉ cần nhập dữ liệu một lần, các cơ quan sẽ





tự động khai thác dùng lại, đúng với nguyên tắc “*một lần duy nhất*”. X-Road cũng tích hợp các cơ chế mã hóa, chữ ký số và sao lưu lịch sử đầy đủ cho mọi giao dịch, đảm bảo tính riêng tư và toàn vẹn dữ liệu. Kết quả là Estonia xây dựng được Chính phủ số liên thông và tiết kiệm mỗi năm hàng ngàn giờ công (ước tính X-Road giúp tiết kiệm hơn 1.300 năm công lao động trong năm 2018), đồng thời giữ vững an ninh cho hệ thống dữ liệu quốc gia.

### **8.3.4.3. Giai đoạn 2029 - 2030: Hoàn thiện hệ sinh thái dữ liệu và hội nhập quốc tế về dữ liệu**

**Mục tiêu chính:** Phát triển mạnh mẽ thị trường dữ liệu quốc gia và các ngành công nghiệp liên quan đến dữ liệu; nâng cao mức độ hội nhập quốc tế về dữ liệu, đưa Việt Nam thành một thành viên tích cực trong nền kinh tế dữ liệu toàn cầu; với các nhiệm vụ trọng tâm như sau:

+ **Phát triển thị trường dữ liệu:** Xây dựng một hệ sinh thái dữ liệu hoàn chỉnh, nơi dữ liệu trở thành hàng hóa, tài sản được khai thác hợp pháp và minh bạch. Nhà nước sẽ khuyến khích hình thành các sàn dữ liệu được cấp phép, nơi các tổ chức, doanh nghiệp có thể mua bán, trao đổi dữ liệu dưới sự giám sát để đảm bảo tuân thủ pháp luật. Nghị định 169/2025/NĐ-CP đã đặt nền móng cho lĩnh vực này khi quy định chi tiết điều kiện kinh doanh đối với dịch vụ sàn dữ liệu và dịch vụ trung gian dữ liệu. Đến giai đoạn 2029 - 2030, Việt Nam kỳ vọng có một số sàn dữ liệu vận hành hiệu quả, thu hút sự tham gia của cả khu vực công và tư, qua đó thúc đẩy kinh tế dữ liệu phát triển. Ngoài ra, đẩy mạnh hỗ trợ doanh nghiệp khởi nghiệp và doanh nghiệp công nghệ trong lĩnh vực dữ liệu. Các doanh nghiệp cung cấp dịch vụ phân tích dữ liệu, dịch vụ điện toán đám mây, dịch vụ bảo mật dữ liệu... sẽ được hưởng các chính sách ưu đãi về thuế, vốn hoặc cơ sở hạ tầng để mở rộng hoạt động. Nhà nước cũng tăng cường quan tâm vào Quỹ đổi





mới sáng tạo về dữ liệu nhằm đầu tư cho các ý tưởng, giải pháp sử dụng dữ liệu đột phá. Mục tiêu là hình thành một thị trường dữ liệu sôi động nhưng được quản lý chặt chẽ, vừa tạo nguồn lực cho nền kinh tế, vừa không vi phạm quyền riêng tư và lợi ích công cộng.

+ **Hợp tác quốc tế và hội nhập về dữ liệu:** Tăng cường vị thế của Việt Nam trong lĩnh vực quản trị dữ liệu toàn cầu thông qua việc chủ động tham gia các sáng kiến và mạng lưới quốc tế. Trước hết, Việt Nam sẽ xây dựng các hiệp định song phương và đa phương về trao đổi dữ liệu với các quốc gia đối tác, đặc biệt trong ASEAN. Những hiệp định này nhằm tạo hành lang pháp lý cho việc chia sẻ dữ liệu xuyên biên giới an toàn, hợp pháp, ví dụ chia sẻ dữ liệu phòng chống tội phạm, y tế, nghiên cứu khoa học... Tiếp đó, Việt Nam tích cực tham gia các diễn đàn về dữ liệu của Liên Hợp Quốc, APEC, OECD nhằm học hỏi kinh nghiệm và đóng góp tiếng nói vào việc xây dựng chuẩn mực dữ liệu quốc tế. Về mặt luật pháp, Việt Nam sẽ tiệm cận các chuẩn mực tiên tiến như của Liên minh Châu Âu. Ngoài GDPR đã đề cập, Việt Nam theo dõi và nghiên cứu Đạo luật Quản trị dữ liệu (Data Governance Act - DGA) của EU - đạo luật mới thúc đẩy chia sẻ dữ liệu an toàn, tạo lập không gian dữ liệu chung châu Âu. DGA đề ra cơ chế khuyến khích trung gian dữ liệu tin cậy và cho phép dữ liệu được sử dụng xuyên biên giới một cách linh hoạt nhưng vẫn đảm bảo tuân thủ luật pháp. Thông qua việc tham gia các sáng kiến như vậy, Việt Nam có thể đồng bộ hóa tiêu chuẩn quản trị dữ liệu của mình với thế giới, tạo niềm tin cho các doanh nghiệp và đối tác quốc tế. Một ví dụ tiêu biểu trong khu vực là Nhật Bản và Hàn Quốc đã tham gia Mạng lưới luân chuyển dữ liệu tự do tin cậy (DFFT) và thúc đẩy quy tắc CBPR của APEC về bảo vệ dữ liệu cá nhân xuyên biên giới. Việt Nam cũng đặt mục tiêu gia nhập các cơ chế tương tự để vừa bảo





vệ chủ quyền dữ liệu quốc gia, vừa thuận lợi hóa dòng chảy dữ liệu cho phát triển kinh tế số.

+ **Kinh nghiệm từ thực tiễn:** Hàn Quốc đã xây dựng một thị trường dữ liệu mở năng động nhờ chính sách chính phủ mở dữ liệu từ sớm. Cổng Dữ liệu Mở quốc gia của Hàn Quốc (data.go.kr) ra mắt năm 2013, đóng vai trò như một “một cửa” trung tâm cho người dân và doanh nghiệp truy cập dữ liệu công khai. Tính đến năm 2024, cổng này đã cung cấp khoảng 87.000 tập dữ liệu công khai thuộc nhiều lĩnh vực khác nhau - một con số khổng lồ hàng đầu thế giới. Chính phủ Hàn Quốc xếp hạng nhất nhiều năm liền về “Chỉ số dữ liệu mở” do OECD đánh giá, nhờ việc không ngừng mở rộng danh mục dữ liệu có thể cung cấp cho công chúng. Kho dữ liệu khổng lồ này vừa giúp người dân, doanh nghiệp dễ dàng tiếp cận thông tin để nghiên cứu, phát triển dịch vụ, vừa tạo nền tảng cho các doanh nghiệp khởi nghiệp về dữ liệu ra đời. Thị trường dữ liệu mở của Hàn Quốc đã chứng minh rằng dữ liệu công nếu được khai thác đúng cách sẽ trở thành tài sản chung quý giá, thúc đẩy đổi mới sáng tạo và tăng trưởng kinh tế. Việt Nam có thể học hỏi kinh nghiệm này để phát triển thị trường dữ liệu của riêng mình, gắn với lộ trình hoàn thiện khung pháp lý và hạ tầng kỹ thuật tương ứng.

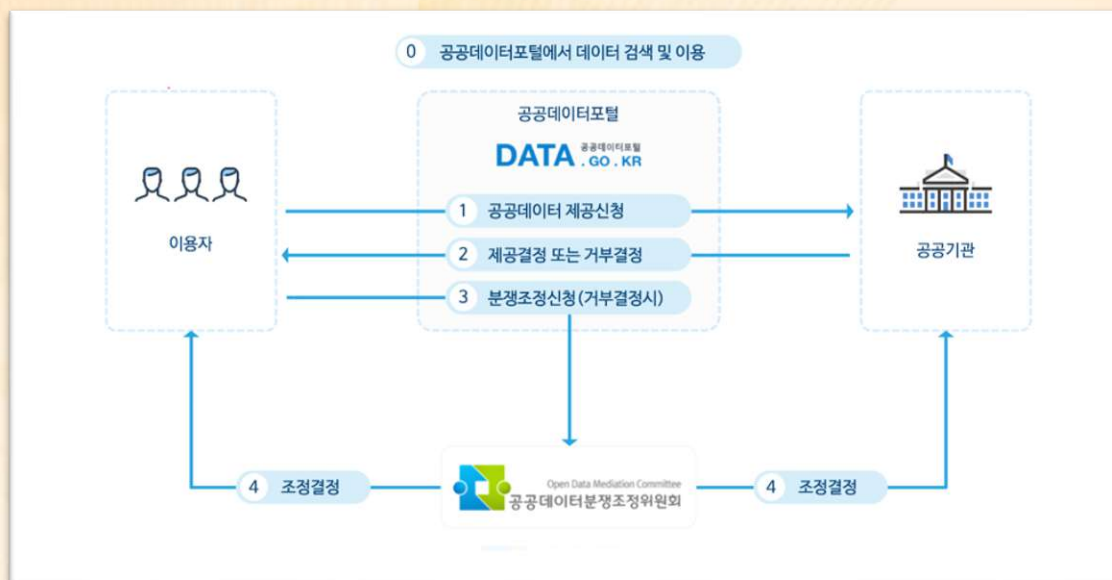
Lộ trình triển khai quản lý nhà nước về dữ liệu giai đoạn 2025 - 2030 đề ra một cách tiếp cận toàn diện, từ hoàn thiện thể chế, đầu tư hạ tầng, đến phát triển nhân lực và hợp tác quốc tế. Việc thực hiện nghiêm túc các bước đi này sẽ giúp Việt Nam thiết lập nền tảng dữ liệu quốc gia an toàn, hiện đại và hiệu quả, phục vụ đắc lực cho Chính phủ số, kinh tế số và xã hội số. Dữ liệu sẽ trở thành “nguồn tài nguyên quý giá, tư liệu sản xuất mới”, là động lực thúc đẩy đổi mới sáng tạo, nâng cao năng suất lao động và năng lực cạnh tranh quốc gia. Đồng thời, một hệ sinh thái dữ liệu minh bạch, có sự quản





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU Trong công an nhân dân

lý của Nhà nước sẽ bảo đảm quyền lợi của người dân được tôn trọng (về quyền riêng tư, bảo vệ dữ liệu cá nhân) và an ninh quốc gia được giữ vững trong kỷ nguyên số.



### **Mô hình hoạt động của Cổng Dữ liệu Mở quốc gia của Hàn Quốc - Ảnh: data.go.kr**

Nếu lộ trình được triển khai đúng định hướng và đạt các mục tiêu đề ra, đến năm 2030 Việt Nam sẽ cơ bản có một thị trường dữ liệu phát triển song hành cùng một khung khổ quản trị dữ liệu tiên tiến. Khi đó, Việt Nam không chỉ đáp ứng tốt các nhu cầu trong nước về khai thác dữ liệu mà còn đủ năng lực hội nhập sâu rộng với khu vực và thế giới trong lĩnh vực dữ liệu. Quản lý nhà nước về dữ liệu hiệu quả sẽ là bộ phận đưa Việt Nam tiến vào kỷ nguyên số một cách tự tin và vững chắc, đóng góp vào sự thịnh vượng chung của đất nước trong kỷ nguyên vươn mình của dân tộc.

Việc phát triển dữ liệu số một cách bền vững, an toàn, hiệu quả đòi hỏi một kế hoạch hành động tổng thể, đồng bộ với sự tham gia của cả trung ương và địa phương. Thực tiễn cho thấy, nếu thiếu sự phối hợp chặt chẽ giữa các cấp, việc triển khai các cơ sở dữ liệu và hạ tầng số dễ dẫn đến tình trạng





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

phân mảnh, cục bộ, gây lãng phí nguồn lực. Do đó, một kế hoạch hành động thống nhất xuyên suốt từ Trung ương đến địa phương là rất cần thiết, nhằm bảo đảm kết nối, liên thông, chia sẻ dữ liệu thông suốt trên phạm vi cả nước. Chính phủ Việt Nam đã nhận thức rõ điều này khi ban hành Nghị quyết số 214/NQ-CP ngày 23/7/2025 Ban hành Kế hoạch hành động của Chính phủ về thúc đẩy tạo lập dữ liệu phục vụ chuyển đổi số toàn diện với mục tiêu xây dựng kiến trúc dữ liệu đồng bộ toàn hệ thống chính trị, kết nối từ các bộ, ngành đến các tỉnh, thành phố. Kế hoạch này đặt ra những mục tiêu cụ thể như 100% cơ sở dữ liệu quốc gia và chuyên ngành được chuẩn hóa theo tiêu chuẩn chung, liên thông và tích hợp phục vụ hiệu quả công tác quản lý, cung cấp dịch vụ. Đây là bước quan trọng để bảo đảm sự đồng bộ, thống nhất giữa trung ương và địa phương trong phát triển dữ liệu, tạo nền tảng cho chuyển đổi số trên quy mô toàn quốc.



***Chương trình hành động của Chính phủ về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số - Ảnh: Báo Điện tử Chính phủ***





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Bên cạnh yếu tố trong nước, việc học hỏi một cách sáng tạo những kinh nghiệm quốc tế và áp dụng vào thực tiễn Việt Nam đóng vai trò quyết định để bảo đảm quá trình phát triển dữ liệu diễn ra bền vững, an toàn, hiệu quả. Nhiều quốc gia trên thế giới đã sớm xây dựng khung pháp lý và chiến lược về dữ liệu, từ đó rút ra những bài học quý cho Việt Nam, không những chúng ta phải đẩy nhanh tiến độ hoàn thiện luật pháp, mà còn phải nghiên cứu, điều chỉnh sao cho phù hợp với môi trường, thị trường ở Việt Nam. Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia của Bộ Chính trị đã nhấn mạnh yêu cầu phát triển hạ tầng số và dữ liệu trên nguyên tắc “hiện đại, đồng bộ, an ninh, an toàn, hiệu quả”, đưa dữ liệu trở thành tư liệu sản xuất chính để thúc đẩy nhanh phát triển kinh tế dữ liệu. Đồng thời, Nghị quyết này đặt mục tiêu đến năm 2030 Việt Nam thuộc nhóm các nước dẫn đầu về an ninh mạng và bảo vệ dữ liệu, coi bảo đảm an ninh dữ liệu, an toàn thông tin là yêu cầu xuyên suốt, không tách rời trong phát triển kinh tế số. Để hiện thực hóa tầm nhìn đó, Việt Nam đã và đang xây dựng một hệ thống chính sách, pháp luật khá toàn diện về dữ liệu. Lần đầu tiên, một Luật Dữ liệu chuyên biệt đã được ban hành, tạo cơ sở pháp lý thống nhất cho quản lý, chia sẻ và khai thác dữ liệu trong nền kinh tế số và xã hội số. Cùng với đó, Chính phủ đã phê duyệt Chiến lược dữ liệu quốc gia đến năm 2030, ban hành các văn bản quan trọng như Luật Giao dịch điện tử 2023, Luật An ninh mạng 2018, Luật Bảo vệ dữ liệu cá nhân 2025..., nhằm hoàn thiện hành lang pháp lý cho lĩnh vực dữ liệu. Những nỗ lực này thể hiện quyết tâm của Việt Nam trong việc học hỏi và áp dụng các chuẩn mực quốc tế về dữ liệu, đồng thời điều chỉnh cho phù hợp với điều kiện thực tiễn trong nước.





## **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

Thực tiễn quốc tế cung cấp nhiều ví dụ điển hình giúp Việt Nam định hướng chiến lược phát triển dữ liệu. Chẳng hạn, Trung Quốc đã xây dựng khung pháp lý tương đối hoàn chỉnh với Luật An toàn Dữ liệu (2021), Luật Bảo vệ Thông tin Cá nhân (2021) và Luật An ninh mạng (2017), qua đó phân loại dữ liệu theo mức độ quan trọng và bảo vệ quyền riêng tư tương tự GDPR của EU. Nước này mạnh dạn thí điểm các sàn giao dịch dữ liệu tại nhiều địa phương nhằm thúc đẩy thị trường dữ liệu, cho phép chia sẻ và thương mại hóa dữ liệu trong khuôn khổ pháp lý dần được hoàn thiện. Singapore từ năm 2012 đã có Luật PDPA bảo vệ dữ liệu cá nhân, đồng thời phát triển các nền tảng dữ liệu mở và các sàn dữ liệu chuyên ngành như SGFinDex (tài chính), SGTraDex (thương mại) để khai thác hiệu quả nguồn dữ liệu trong nền kinh tế. Ở Hoa Kỳ, dù chưa có luật dữ liệu chung ở cấp liên bang, hệ thống luật lệ phân tán (với hàng trăm luật liên bang và bang) cùng sự giám sát của Ủy ban Thương mại Liên bang đã tạo nên môi trường dữ liệu cạnh tranh, cởi mở, khuyến khích khu vực tư nhân phát triển các nền tảng dữ liệu lớn như AWS Data Exchange với hàng nghìn bộ dữ liệu sẵn có phục vụ nhiều lĩnh vực. Những kinh nghiệm quốc tế đó cho thấy tầm quan trọng của hành lang pháp lý rõ ràng, đồng bộ, cũng như việc thúc đẩy hạ tầng dữ liệu hiện đại và sự tham gia của cả khu vực công lẫn tư trong phát triển dữ liệu.

Đối chiếu với Việt Nam, việc kết hợp hài hòa kinh nghiệm quốc tế với điều kiện thực tiễn trong nước là chìa khóa để đạt được mục tiêu phát triển dữ liệu bền vững, an toàn, hiệu quả. Việt Nam cần tiếp tục nắm bắt cơ hội, học hỏi kinh nghiệm các nước trong việc xây dựng thị trường và hệ sinh thái dữ liệu. Trước mắt, một nhiệm vụ trọng tâm là hoàn thiện các văn bản hướng dẫn thi hành Luật Dữ liệu và các quy định liên quan, qua đó thiết lập hành





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

lang pháp lý minh bạch, thống nhất về quyền sở hữu, quyền truy cập và bảo vệ dữ liệu. Điều này sẽ tạo dựng niềm tin cho các bên tham gia khai thác dữ liệu, đồng thời bảo đảm tuân thủ các chuẩn mực quốc tế về an toàn, quyền riêng tư. Song song, cần đẩy mạnh đầu tư vào hạ tầng lưu trữ, bảo mật và quản trị dữ liệu theo chuẩn mực quốc tế, cũng như phát triển nhân lực số chất lượng cao về an toàn thông tin và quản lý dữ liệu. Sự hợp tác giữa Việt Nam và các tập đoàn công nghệ hàng đầu thế giới đang cho thấy hiệu quả tích cực trong chuyển giao công nghệ và tri thức về dữ liệu - đây là nền tảng để chúng ta vừa tiếp thu kinh nghiệm quốc tế, vừa triển khai phù hợp với bối cảnh Việt Nam.



***Bộ trưởng Nguyễn Mạnh Hùng chia sẻ những câu chuyện và kinh nghiệm từ chuyển công tác tại Phần Lan về đổi mới, sáng tạo tại Hội nghị giao ban quản lý nhà nước tháng 9/2024 - Ảnh: Bộ Khoa học và Công nghệ***

Tổng kết lại, một kế hoạch hành động tổng thể, đồng bộ từ trung ương đến địa phương kết hợp với việc học hỏi kinh nghiệm quốc tế một cách chọn lọc sẽ là nhân tố quyết định cho thành công của Việt Nam trong “*kỷ nguyên dữ liệu*”. Sự nhất quán trong chỉ đạo và phối hợp sẽ giúp tránh chồng chéo giữa các bộ, ngành và địa phương, tối ưu hóa nguồn lực quốc gia. Đồng thời,





## BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU *Trong công an nhân dân*

vận dụng sáng tạo những bài học kinh nghiệm trên thế giới từ khung pháp lý đến phát triển hạ tầng và thị trường dữ liệu sẽ giúp Việt Nam đảm bảo phát triển dữ liệu một cách bền vững, an toàn về an ninh, bảo mật và hiệu quả về kinh tế, xã hội. Kết hợp những yếu tố đó, Việt Nam có thể tự tin tiến bước, biến dữ liệu thực sự trở thành tài nguyên chiến lược cho phát triển quốc gia trong tương lai, đồng thời đóng góp tích cực vào công cuộc chuyển đổi số và tăng trưởng bền vững của đất nước trong kỷ nguyên vươn mình của dân tộc.

Nhóm chúng tôi - **Những chiến sĩ An ninh “Dữ liệu số”** - thật vinh dự khi được tham gia vào dòng chảy mạnh mẽ của công cuộc chuyển đổi số quốc gia, đặc biệt là trong lực lượng Công an nhân dân. Sự ra đời của Luật Dữ liệu năm 2024 không chỉ là cơ sở pháp lý, mà còn là kim chỉ nam để mỗi người chiến sĩ chúng tôi hành động đúng đắn, chính xác và hiệu quả. Với mỗi cán bộ, chiến sĩ, dữ liệu không còn là những con số, văn bản khô khan mà đã trở thành “*dòng máu*” nuôi dưỡng trí tuệ nghiệp vụ, là “*mắt xích*” quan trọng để bảo vệ Tổ quốc trên không gian số.

Với vai trò, trách nhiệm của người chiến sĩ An ninh, chúng tôi quyết tâm không ngừng tìm tòi, ứng dụng khoa học, công nghệ và đổi mới sáng tạo; làm chủ công nghệ, làm chủ dữ liệu và các nền tảng số, biến dữ liệu thành công cụ sắc bén để phục vụ công tác nghiệp vụ, nâng cao hiệu quả công tác. Chúng tôi tin rằng, với tinh thần đổi mới, sáng tạo, dám nghĩ, dám làm, không ngại khó khăn và sự đồng lòng của toàn thể cán bộ, chiến sĩ, lực lượng Công an nhân dân sẽ là một trong những đơn vị tiên phong, đi đầu trong công cuộc chuyển đổi số. Chúng ta hãy cùng nhau làm chủ dữ liệu, làm chủ công nghệ để xây dựng một đất nước Việt Nam giàu mạnh, hùng cường, một dân tộc Việt Nam vươn mình mạnh mẽ trong kỷ nguyên mới./.





## *Danh mục tài liệu tham khảo*

### **I. Tiếng Việt**

1. Bạch Dương (2025), *Bốn mục tiêu cho chiến lược dữ liệu quốc gia đến năm 2030*, [vneconomy.vn](https://vneconomy.vn/bon-muc-tieu-cho-chien-luoc-du-lieu-quoc-gia-den-nam-2030.htm), <https://vneconomy.vn/bon-muc-tieu-cho-chien-luoc-du-lieu-quoc-gia-den-nam-2030.htm>, truy cập ngày 06/8/2025.
2. Bạch Dương (2025), *Chính phủ ban hành danh mục 26 dữ liệu cốt lõi và 43 dữ liệu quan trọng*, [vneconomy.vn](https://vneconomy.vn/ chinh-phu-ban-hanh-danh-muc-26-du-lieu-cot-loi-va-43-du-lieu-quan-trong.htm), <https://vneconomy.vn/ chinh-phu-ban-hanh-danh-muc-26-du-lieu-cot-loi-va-43-du-lieu-quan-trong.htm>, truy cập ngày 06/8/2025.
3. Baohinhphu.vn (2025), *Bộ Công an tổ chức lễ ra mắt Trung tâm Dữ liệu quốc gia*, <https://baohinhphu.vn/ra-mat-trung-tam-du-lieu-quoc-gia-don-vi-cap-cuc-thuoc-bo-cong-an-102250225161046985.htm>, truy cập ngày 07/8/2025.
4. Bích Ngọc (2024), *Giải pháp thúc đẩy phát triển kinh tế dữ liệu tại Việt Nam*, Tạp chí Công Thương, <https://tapchicongthuong.vn/giai-phap-thuc-day-phat-trien-kinh-te-du-lieu-tai-viet-nam-119943.htm>, truy cập ngày 05/8/2025.
5. Bộ Chính trị (2019), *Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư*, Hà Nội.
6. Bộ Chính trị (2024), *Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia*, Hà Nội.
7. Bộ Khoa học và Công nghệ (2025), *Chiến lược dữ liệu quốc gia - Tầm nhìn đến năm 2030*, [Mst.gov.vn](https://mst.gov.vn), <https://mst.gov.vn/chien-luoc-du-lieu-quoc-gia-den-nam-2030>.





# **BÀI DỰ THI TÌM HIỂU LUẬT DỮ LIỆU** *Trong công an nhân dân*

[lieu-quoc-gia-tam-nhin-den-nam-2030-197250220222423434.htm](http://lieu-quoc-gia-tam-nhin-den-nam-2030-197250220222423434.htm),  
truy cập ngày 07/8/2025.

8. Bộ Y tế (2022), *Kế hoạch phòng chống dịch bệnh truyền nhiễm năm 2022*, Ban hành kèm theo Quyết định số 165/QĐ-BYT ngày tháng năm 2022 của Bộ trưởng Bộ Y tế.
9. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2020), *Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước*, Hà Nội.
10. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2022), *Nghị định số 53/2022/NĐ-CP ngày 15/08/2022 hướng dẫn Luật An ninh mạng*, Hà Nội.
11. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023), *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về Bảo vệ dữ liệu cá nhân*, Hà Nội.
12. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2024), *Nghị định số 47/2024/NĐ-CP ngày 09/5/2024 Quy định về danh mục cơ sở dữ liệu quốc gia*, Hà Nội.
13. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị định số 160/2025/NĐ-CP ngày 29/06/2025 về Quỹ phát triển Dữ liệu quốc gia*, Hà Nội.
14. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu*, Hà Nội.
15. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị định 169/2025/NĐ-CP ngày 30/6/2025 quy định hoạt động khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ về dữ liệu*, Hà Nội.
16. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị định số 190/2025/NĐ-CP ngày 01/7/2025 Sửa đổi, bổ sung một số điều của*





*Nghị định số 118/2021/NĐ-CP ngày 23 tháng 12 năm 2021 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Xử lý vi phạm hành chính được sửa đổi, bổ sung theo Nghị định số 68/2025/NĐ-CP ngày 18 tháng 3 năm 2025 của Chính phủ và Nghị định số 120/2021/NĐ-CP ngày 24 tháng 12 năm 2021 của Chính phủ quy định chế độ áp dụng biện pháp xử lý hành chính giáo dục tại xã, phường, thị trấn, Hà Nội.*

17. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị quyết số 214/NQ-CP ngày 23/7/2025 kế hoạch hành động của Chính phủ về thúc đẩy tạo lập dữ liệu phục vụ chuyển đổi số toàn diện*, Hà Nội.
18. Chu Anh (2023), *Nền tảng truyền hình số quốc gia VTVgo - Vươn mình cạnh tranh OTT quốc tế*, vtv.vn, <https://vtv.vn/truyen-hinh/nen-tang-truyen-hinh-so-quoc-gia-vtvgo-vuon-minh-canh-tranh-ott-quoc-te-20230608033031842.htm>, truy cập ngày 31/07/2025.
19. Dx.gov.vn (2025), *Danh mục các dịch vụ chia sẻ dữ liệu được cung cấp trên nền tảng tích hợp chia sẻ dữ liệu NDXP*, <https://dx.gov.vn/danh-muc-cac-doch-vu-chia-se-du-lieu-duoc-cung-cap-tren-nen-tang-tich-hop-chia-se-du-lieu-ndxp-1742293458268.htm>, truy cập ngày 05/8/2025.
20. Đảng Cộng sản Việt Nam (2021), *Nghị quyết Đại hội đại biểu toàn quốc lần thứ XIII của Đảng*, Hà Nội.
21. Đỗ Hùng (2025), *Công an tỉnh tổ chức Diễn tập thực chiến đảm bảo an toàn thông tin mạng, ứng cứu sự cố tỉnh Ninh Bình năm 2025*, Trang thông tin điện tử Công an tỉnh Ninh Bình, <https://congan.ninhbinh.gov.vn/cong-an-tinh-to-chuc-dien-tap-thuc-chien-dam-bao-an-toan-thong-tin-mang-ung-cuu-su-co-tinh-ninh-binh-nam-2025>, truy cập ngày 07/8/2025.





22. Hà Văn (2023), *Thủ tướng: Dữ liệu là tài nguyên quốc gia, là nguồn lực, động lực phát triển trong kỷ nguyên số*, Báo Điện tử Chính phủ, <https://baochinhphu.vn/thu-tuong-du-lieu-la-tai-nguyen-quoc-gia-la-nguon-luc-dong-luc-phat-trien-trong-ky-nguyen-so-1022302251236115.htm>, truy cập ngày 31/7/2025.
23. Hải Lan (2025), *Triệt phá đường dây mua bán gần 56 triệu dữ liệu cá nhân*, Báo Công an Nhân dân điện tử, <https://cand.com.vn/Ho-so-Interpol/triet-pha-duong-day-mua-ban-gan-56-trieu-du-lieu-ca-nhan-i759592/>, truy cập ngày 07/8/2025.
24. Hal9 (2024), *Công cụ phân tích dữ liệu AI: Trợ lý thông minh gợi ý biểu đồ và trực quan hóa dữ liệu*, HashDork, <https://www.hashdork.com/vi/cong-cu-phan-tich-du-lieu-ai>, truy cập ngày 05/8/2025.
25. Hoàng Cường (2024), *Chiến lược dữ liệu quốc gia đến năm 2030 có gì đặc biệt?*, Báo Sức khỏe và Đời sống, <https://suckhoedoisong.vn/chien-luoc-du-lieu-quoc-gia-den-nam-2030-co-gi-dac-biet-169240203080851047.htm>, truy cập ngày 05/8/2025.
26. Hồng Minh (2025), *Luật Dữ liệu xây dựng niềm tin số và thúc đẩy chuyển đổi số toàn diện*, Báo Nhân Dân, <https://nhandan.vn/luat-du-lieu-xay-dung-niem-tin-so-va-thuc-day-chuyen-doi-so-toan-dien-post890961.html>, truy cập ngày 06/8/2025.
27. Mekong, A. (2025), *Xây dựng quy chuẩn kết nối, chia sẻ dữ liệu từ địa phương lên trung ương*, Mekong ASEAN, <https://mekongasean.vn/xay-dung-quy-chuan-ket-noi-chia-se-du-lieu-tu-dia-phuong-len-trung-uong-43297.html>, truy cập ngày 07/8/2025.
28. Minh Hiền (2025), *Luật Dữ liệu có hiệu lực thi hành từ ngày 1/7*, Báo Công an Nhân dân điện tử, <https://cand.com.vn/su-kien-binh-luan->





thoi-su/luat-du-lieu-co-hieu-luc-thi-hanh-tu-ngay-1-7-i773416/, truy cập ngày 07/8/2025.

29. Minh Ngọc (2024), *Năm 2030: Lợi ích kinh tế từ AI có thể lên tới 79,3 tỷ USD*, Báo điện tử Chính phủ, <https://baochinhphu.vn/nam-2030-loi-ich-kinh-te-tu-ai-co-the-len-toi-793-ty-usd-102241115164254991.htm>, truy cập ngày 06/8/2025.
30. Nguyễn Anh Tuấn (2025), *Nghị định 169/2025/NĐ-CP và cơ hội cho các ngân hàng*, Cafef.vn, <https://cafef.vn/ngphi-dinh-169-2025-nd-cp-va-co-hoi-cho-cac-ngan-hang-188250714112857828.chn>, truy cập ngày 05/8/2025.
31. Phạm Dự (2025), *Bộ Công an quản lý quỹ nghìn tỷ phát triển dữ liệu quốc gia*, Vnexpress.net, <https://vnexpress.net/bo-cong-an-quan-ly-quy-nghin-ty-phat-trien-du-lieu-quoc-gia-4908788.html>, truy cập ngày 07/8/2025.
32. Phan Anh (2024), *Hơn 61 triệu tài khoản, bản ghi thông tin cá nhân bị lộ lọt trong nửa đầu năm 2024*, Tạp chí điện tử VnEconomy, <https://vneconomy.vn/hon-61-trieu-tai-khoan-ban-ghi-thong-tin-ca-nhan-bi-lo-lot-trong-nua-dau-nam-2024.htm>, truy cập ngày 06/8/2025.
33. Tiểu Minh (2020), *Ứng dụng nghe nhạc Việt được tích hợp trí tuệ nhân tạo*, Báo Pháp Luật TP.HCM, <https://plo.vn/ky-nguyen-so/ung-dung-nghe-nhac-viet-duoc-tich-hop-tri-tue-nhan-cao-post594743.html>, truy cập ngày 31/7/2025.
34. Tony Dang (2023), *Bảo mật dữ liệu trở thành tâm điểm năm 2022*, VNNETWORK, <https://www.vnetwork.vn/news/bao-mat-du-lieu-tro-thanh-tam-diem-nam-2022/>, truy cập ngày 06/8/2025.
35. Thanh Hà (2025), *Khám phá hệ thống camera AI tự động phát hiện vi phạm giao thông, hành vi gây rối và đối tượng truy nã*, Báo Điện Tử Tiền Phong, <https://tienphong.vn/kham-pha-he-thong-camera-ai-tu>





dong-phat-hien-vi-pham-giao-thong-hanh-vi-gay-roi-va-doi-tuong-truy-na-post1760924.tpo, truy cập ngày 31/07/2025.

36. Thủ tướng Chính phủ (2024), *Quyết định số 142/QĐ-TTg Phê duyệt Chiến lược dữ liệu quốc gia đến năm 2030*, Hà Nội.
37. Trang (2025), *Ngành Ngân hàng tiếp tục tiên phong trong chuyển đổi số, cùng đất nước bước vào kỷ nguyên mới*, Tạp Chí Ngân Hàng, <https://tapchinganhang.gov.vn/nganh-ngan-hang-tiep-tuc-tien-phong-trong-chuyen-doi-so-cung-dat-nuoc-buoc-vao-ky-nguyen-moi-16085.html>, truy cập ngày 31/07/2025.
38. Trọng Đạt (2021), *Xếp hạng dữ liệu mở Việt Nam chỉ tốt hơn Thái, Lào, Campuchia*, Báo VietNamNet, <https://vietnamnet.vn/xep-hang-du-lieu-mo-viet-nam-tot-hon-thai-lan-lao-campuchia-794027.html>, truy cập ngày 06/8/2025.
39. Viettel (n.d.), *Nền tảng dữ liệu lớn Viettel Data Platform (VDP)*, solutions.viettel.vn, <https://solutions.viettel.vn/vi/vi/cong-nghe-thong-tin/nen-tang-du-lieu-lon-viettel-data-platform-vdp.html>, truy cập ngày 31/07/2025.

## **II. Tiếng Anh**

40. A&O Shearman (2023), *EU - Data Governance Act becomes applicable*, <https://www.aoshearman.com/en/insights/ao-shearman-on-data/eu--data-governance-act-becomes-applicable>, truy cập ngày 06/8/2025.
41. Alex He và Rebecca Arcesati (2024), *Data Marketplaces and Governance: Lessons from China*, Centre for International Governance Innovation, <https://www.cigionline.org/articles/data-marketplaces-and-governance-lessons-from-china/>, truy cập ngày 06/8/2025.
42. Amazon Web Services, Inc. (n.d.), *Natively use third-party data within your AWS environment*, <https://aws.amazon.com/data-exchange/why-aws-data-exchange/>, truy cập ngày 31/7/2025.





43. BARC (2016), *Benefits of Big Data Analytics: Increased Revenues and Reduced Costs*, barc.com, <https://barc.com/big-data-benefits/>, truy cập ngày 06/8/2025.
44. Business Wire (2021), *Korea Kicks Off “Data Dam”*, PR Newswire, <https://www.prnewswire.com/news-releases/korea-kicks-off-data-dam-301325717.html>, truy cập ngày 07/8/2025.
45. CRMVIET (2024), *Tích hợp CRM ERP: Hướng dẫn chi tiết*, <https://crmviet.vn/tich-hop-crm-erp-huong-dan-chi-tiet/>, truy cập ngày 10/8/2025.
46. Chen, A. (2021), *China’s Data Security Law in Effect Sept. 1, 2021: Prepare for Compliance*, China Briefing News, <https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/>, truy cập ngày 10/8/2025.
47. Datagalaxy (2024), *Gartner's top 5 data & analytics predictions for 2025*, <https://www.datagalaxy.com/en/blog/gartners-top-data-predictions-for-2025/>, truy cập ngày 05/8/2025.
48. DevX (2023), *Data Services - Glossary*, <https://www.devx.com>, truy cập ngày 31/07/2025.
49. DevX (n.d.), *Data Services*, <https://www.devx.com/terms/data-services/>, truy cập ngày 31/7/2025.
50. E-Estonia (2017), *X-Road*, <https://e-estonia.com/solutions/interoperability-services/x-road/>, truy cập ngày 07/8/2025.
51. EUR-Lex (2018), *Protecting personal data that is used by police and criminal justice authorities (from 2018)*, EUR-Lex, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:310401\\_3](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:310401_3), truy cập ngày 10/8/2025.





52. EUR-Lex (n.d.), *Regulation - 2022/868 - EN - EUR-Lex*, EUR-Lex.europa.eu, <https://eur-lex.europa.eu/eli/reg/2022/868/oj>, truy cập ngày 10/8/2025.
53. European Data Protection Board (n.d.), *Data Protection Authority and you*, [https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you\\_en](https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en), truy cập ngày 06/8/2025.
54. Federal Trade Commission (2023), *Data privacy enforcement actions*, <https://www.ftc.gov>, truy cập ngày 01/8/2025.
55. Google Cloud (2024), *What is BigQuery Data Transfer Service?*, <https://cloud.google.com/bigquery/docs/dts-introduction>, truy cập ngày 31/7/2025.
56. Govinsider.asia (2024), *Estonia's X-Road: data exchange in the world's most digital society*, Govinsider.asia, <https://govinsider.asia/intl-en/article/estonias-x-road-data-exchange-in-the-worlds-most-digital-society>, truy cập ngày 07/8/2025.
57. IBM (2022), *What is Blockchain Technology?*, <https://www.ibm.com/topics/what-is-blockchain>, truy cập ngày 5/8/2025.
58. IE Insights (2023), *The Community of Data*, <https://www.ie.edu/insights/articles/the-community-of-data/>, truy cập ngày 05/8/2025.
59. IMD (2024), *Why Data Analytics is Important for Digital Transformation?*, <https://www.imd.org/blog/digital-transformation/the-role-of-data-analytics/>, truy cập ngày 05/8/2025.
60. Informatica (n.d.), *Cloud Data Integration Overview*, <https://www.informatica.com/products/cloud-integration/cloud-data-integration.html>, truy cập ngày 03/08/2025.
61. Informatica (n.d.), *What is Data Services: Definition*, Informatica.com, <https://www.informatica.com/services-and-training/glossary-of-terms/data-services-definition.html>, truy cập ngày 01/8/2025.





62. Joshna (2025), *Big Data Analytics Adoption Rates by Sector*, Zoe Talent Solutions, <https://zoetalentsolutions.com/big-data-analytics-adoption-rates/>, truy cập ngày 05/8/2025.
63. NCS and Talend (2020), *Compliance considerations for public agencies: an introduction to Singapore's data governance and protection frameworks*, ncs.co, <https://www.ncs.co/dam/jcr:1018c9ab-44f0-4cda-aeb5-7b9fffd45a0/a-compliance-introduction-to-singapore-dgp-framework-for-public-agencies-talend-ncs-17Nov2020.pdf>, truy cập ngày 07/8/2025.
64. OECD (2019), *Data in the Digital Age*, OECD Going Digital Policy Note, <https://www.oecd.org/going-digital/data-in-the-digital-age.pdf>, truy cập ngày 29/7/2025.
65. Perfect Data Entry (2024), *“Benefits of Cloud-Based Data Integration Tools”*, <https://www.perfectdataentry.com/cloud-data-integration>, truy cập ngày 05/08/2025.
66. Pykes, K. (2024), *What Is a Data Product? Concepts and Best Practices*, DataCamp.com, <https://www.datacamp.com/blog/data-product>, truy cập ngày 01/8/2025.
67. Querio Blog (2023), *“Using AI to Improve Data Integration Efficiency”*, <https://querio.ai/blog/ai-in-data-integration>, truy cập ngày 5/8/2025.
68. Shaping Europe's digital future (2019), *Building a data economy - Brochure*, <https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure>, truy cập ngày 05/8/2025.
69. Sisense (2025), *Your guide to 2025 data and analytics megatrends*, <https://www.sisense.com/blog/data-analytics-megatrends-guide/>, truy cập ngày 05/8/2025.





70. Snowflake Inc (2025), *About Snowflake Marketplace*, Snowflake Documentation, <https://docs.snowflake.com/en/>, truy cập ngày 03/08/2025.
71. TechRadar (2024), *Transforming Dark Data into AI-Driven Business Value*, <https://www.techradar.com/pro/transforming-dark-data-into-ai-driven-business-value>, truy cập ngày 05/08/2025.
72. Unite AI (2025), *Top AI Tools for Data Analysts in 2025*, <https://www.unite.ai/vi/ai-tools-data-analysts>, truy cập ngày 05/08/2025.
73. Veeam (2025), *3-2-1 Backup Rule Explained: Do I Need One?*, <https://www.veeam.com/blog/321-backup-rule.html>, truy cập ngày 06/8/2025.
74. Wikipedia (2025), *Data Product*, [https://en.wikipedia.org/wiki/Data\\_product](https://en.wikipedia.org/wiki/Data_product), truy cập ngày 31/07/2025.
75. Zimmergren (2025), *Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework*, Microsoft.com, <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework>, truy cập ngày 31/7/2025.

### **III. Tiếng Trung**

76. State Council of the People's Republic of China (2020), *Opinions on Building a More Complete Factor Market System (关于构建更加完善的要素市场化配置体制机制的意见)*, Gov.cn, [https://www.gov.cn/zhengce/2020-04/09/content\\_5500622.htm](https://www.gov.cn/zhengce/2020-04/09/content_5500622.htm), truy cập ngày 31/7/2025.
77. 国家互联网信息办公室 (2023), 《国家互联网信息办公室令 (第14) 网信部门行政执法程序规定》, 中国政府网, [https://www.gov.cn/gongbao/2023/issue\\_10506/202306/content\\_6885255.html](https://www.gov.cn/gongbao/2023/issue_10506/202306/content_6885255.html), truy cập ngày 07/08/2025.





# BÀI DỰ THI TÌM HIỂU

# LUẬT DỮ LIỆU *Trong công an nhân dân*

|                                                                                                                                                                                                                                            |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Mục lục .....                                                                                                                                                                                                                              | 3          |
| Lời mở đầu .....                                                                                                                                                                                                                           | 5          |
| Tóm tắt nội dung .....                                                                                                                                                                                                                     | 7          |
| Câu 7. Quy định về sản phẩm, dịch vụ về dữ liệu? Các giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu? .....                                                                             | 12         |
| <b>7.1. QUY ĐỊNH VỀ SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU .....</b>                                                                                                                                                                                 | <b>13</b>  |
| 7.1.1. Vì sao phải quy định về sản phẩm, dịch vụ về dữ liệu? .....                                                                                                                                                                         | 13         |
| 7.1.2. Sản phẩm, dịch vụ về dữ liệu là gì? .....                                                                                                                                                                                           | 22         |
| 7.1.3. Quy định của pháp luật Việt Nam về sản phẩm, dịch vụ về dữ liệu .....                                                                                                                                                               | 45         |
| 7.1.4. Một số điểm đáng chú ý trong các quy định của pháp luật Việt Nam về sản phẩm, dịch vụ về dữ liệu .....                                                                                                                              | 63         |
| <b>7.2. ĐỀ XUẤT MỘT SỐ GIẢI PHÁP BẢO ĐẢM AN NINH DỮ LIỆU, AN TOÀN DỮ LIỆU TRONG ỨNG DỤNG CÁC SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU .....</b>                                                                                                        | <b>157</b> |
| 7.2.1. Nguy cơ khi ứng dụng sản phẩm, dịch vụ và dữ liệu gây mất an toàn, trật tự xã hội .....                                                                                                                                             | 160        |
| 7.2.2. Một số giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ về dữ liệu .....                                                                                                                     | 180        |
| Câu 8. Nội dung quản lý nhà nước về dữ liệu? Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu? Nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030? ..... | 224        |
| <b>8.1. NỘI DUNG QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU .....</b>                                                                                                                                                                                     | <b>227</b> |
| 8.1.1. Nội dung quản lý nhà nước về dữ liệu .....                                                                                                                                                                                          | 227        |
| 8.1.2. Ý nghĩa của việc quy định nội dung quản lý nhà nước về dữ liệu .....                                                                                                                                                                | 245        |
| 8.1.3. Chủ thể, đầu mối quản lý nhà nước về dữ liệu .....                                                                                                                                                                                  | 253        |
| <b>8.2. VAI TRÒ, TRÁCH NHIỆM CỦA BỘ CÔNG AN VÀ CÔNG AN CÁC ĐƠN VỊ, ĐỊA PHƯƠNG TRONG CÔNG TÁC QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU .....</b>                                                                                                         | <b>256</b> |
| 8.2.1. Vai trò, trách nhiệm của Bộ Công an và Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu .....                                                                                                              | 256        |
| 8.2.2. Vai trò, trách nhiệm của Trung tâm dữ liệu quốc gia trong quản lý nhà nước về dữ liệu .....                                                                                                                                         | 283        |
| <b>8.3. NHIỆM VỤ TRỌNG TÂM CẦN TẬP TRUNG TRONG GIAI ĐOẠN TỪ NAY ĐẾN NĂM 2030 ĐỂ NÂNG CAO HIỆU QUẢ CÔNG TÁC QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU .....</b>                                                                                           | <b>289</b> |
| 8.3.1. Bối cảnh và sự cần thiết nâng cao hiệu quả quản lý nhà nước về dữ liệu đến năm 2030 .....                                                                                                                                           | 289        |
| 8.3.2. Định hướng chiến lược phát triển dữ liệu đến năm 2030 .....                                                                                                                                                                         | 300        |
| 8.3.3. Các nhiệm vụ trọng tâm cần tập trung trong giai đoạn từ nay đến năm 2030 để nâng cao hiệu quả công tác quản lý nhà nước về dữ liệu .....                                                                                            | 309        |
| 8.3.4. Đề xuất lộ trình triển khai trong giai đoạn 2025 - 2030 nhằm nâng cao hiệu quả quản lý nhà nước về dữ liệu .....                                                                                                                    | 342        |
| Danh mục tài liệu tham khảo .....                                                                                                                                                                                                          | 359        |