BỘ CÔNG AN
CÔNG AN TỈNH CÀ MAU

BÀI DỰ THI

TÌM HIỂU LUẬT DỮ LIỆU TRONG CÔNG AN NHÂN DÂN

NHÓM TÁC GIẢ DỰ THI
"CHIẾN SĨ XANH"

CÀ MAU 2025

BỘ CÔNG AN
CÔNG AN TỈNH CÀ MAU

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

NHÓM TÁC GIẢ DỰ THI
"CHIẾN SĨ XANH"

Trung úy Hồng An Xuyên
Ngày, tháng, năm sinh: 27/6/2001
Giới tính: Nam
Chức vụ: Cán bộ
Đơn vị: Phòng Tham mưu, Công an tỉnh Cà Mau
Số điện thoại: 0981.082.987

Trung tá Ngô Như Phúc
Ngày, tháng, năm sinh: 25/6/1980
Giới tính: Nữ
Chức vụ: Phó Đội trưởng
Đơn vị: Phòng Tham mưu, Công an tỉnh Cà Mau
Số điện thoại: 0916.233.855.

Trung tá Huỳnh Nhật Nam
Ngày, tháng, năm sinh: 14/7/1986
Giới tính: Nam
Chức vụ: Phó Trưởng Công an
Đơn vị: Công an xã Đá Bạc, Công an tỉnh Cà Mau
Số điện thoại: 0913.773.876.

TƯ CÁCH

NGƯỜI CÔNG AN CÁCH MỆNH LÀ:

ĐỐI VỚI TỰ MÌNH, PHẢI	CẦN, KIỆM, LIÊM, CHÍNH.
ĐỐI VỚI ĐỒNG SỰ, PHẢI	THÂN ÁI GIÚP ĐỠ.
ĐỐI VỚI CHÍNH PHỦ, PHẢI	TUYỆT ĐỐI TRUNG THÀNH.
ĐỐI VỚI NHÂN DÂN, PHẢI	KÍNH TRỌNG, LỄ PHÉP.
ĐỐI VỚI CÔNG VIỆC, PHẢI	TẬN TỤY.
ĐỐI VỚI ĐỊCH, PHẢI	CƯƠNG QUYẾT, KHÔN KHÉO.

Trích thư Chủ tịch Hồ Chí Minh
gửi Công an Khu XII, ngày 11 tháng 3 năm 1948

5 LỜI THỀ DANH DỰ

CỦA CÔNG AN NHÂN DÂN VIỆT NAM

1. Tuyệt đối trung thành với Tổ quốc và nhân dân Việt Nam, với Đảng Cộng sản Việt Nam, với Nhà nước Cộng hoà XHCN Việt Nam, suốt đời phấn đấu, hy sinh vì độc lập, tự do, chủ quyền, thống nhất và toàn vẹn lãnh thổ, vì an ninh Tổ quốc.

2. Nghiêm chỉnh chấp hành chủ trương, đường lối, chính sách của Đảng, pháp luật của Nhà nước, nghị quyết, chỉ thị và Điều lệnh CAND; sẵn sàng đi bất cứ đâu, làm bất cứ việc gì khi Tổ quốc, Đảng và nhân dân cần đến.

3. Kính trọng, lễ phép với nhân dân. Sẵn sàng bảo vệ tính mạng, tài sản, quyền và lợi ích hợp pháp của nhân dân. Suốt đời tận tuy phục vụ nhân dân, vì cuộc sống bình yên và hạnh phúc của nhân dân.

4. Đề cao cảnh giác, kiên quyết, mưu trí, dũng cảm đấu tranh phòng, chống các thế lực thù địch, các loại tội phạm và các hành vi vi phạm pháp luật.

5. Ra sức học tập, thực hiện nghiêm túc 6 điều Chủ tịch Hồ Chí Minh dạy CAND, luôn xứng đáng với danh dự và truyền thống của CAND Việt Nam.

10 ĐIỀU KỶ LUẬT

CỦA CÔNG AN NHÂN DÂN VIỆT NAM

ĐIỀU 1: Không có lời nói, hành động xâm hại đến Tổ quốc Việt Nam, đến uy tín của Đảng Cộng sản Việt Nam, đến sự vững mạnh của Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, đến danh dự và truyền thống của CAND Việt Nam.

ĐIỀU 2: Nghiêm chỉnh chấp hành điều lệnh CAND. Sẵn sàng nhận và hoàn thành xuất sắc mọi nhiệm vụ được giao.

ĐIỀU 3: Thực hiện nghiêm chỉnh các qui định về giữ bí mật của Đảng, Nhà nước và CAND.

ĐIỀU 4: Trung thực, thẳng thắn, thấy đúng phải bảo vệ, thấy sai phải đấu tranh. Không che giấu, báo cáo sai sự thật với tổ chức Đảng, Nhà nước và CAND.

ĐIỀU 5: Nêu cao tinh thần phục vụ nhân dân không điều kiện. Có thái độ niềm nở, lịch sự, đúng mực khi tiếp xúc với mọi người; kính trọng người già, yêu mến trẻ em, tôn trọng phụ nữ, giúp đỡ người tàn tật. Không hách dịch, cửa quyền, thô bạo, gây phiền hà, sách nhiễu đối với nhân dân.

ĐIỀU 6: Không ngừng tu dưỡng, rèn luyện phẩm chất đạo đức cách mạng; thực hiện cần, kiệm, liêm, chính, chí công vô tư. Không lợi dụng danh nghĩa, chức trách, nhiệm vụ, quyền hạn để mưu cầu lợi ích cá nhân. Không tham ô, lãng phí, đưa hoặc nhận hối lộ dưới bất kì hình thức nào, gương mẫu thực hiện nếp sống văn hoá.

ĐIỀU 7: Kiên quyết đấu tranh làm thất bại mọi âm mưu, hoạt động xâm hại an ninh, trật tự của Tổ quốc, thiệt hại tài sản Nhà nước, tính mạng, tài sản, quyền và lợi ích hợp pháp của nhân dân. Không làm hại người tốt, không bao che kẻ xấu; không để lọt tội phạm, không làm oan người vô tội.

ĐIỀU 8: Không ngừng học tập để nâng cao nhận thức chính trị, nghiệp vụ, pháp luật và năng lực công tác, góp phần xây dựng lực lượng Công an cách mạng, chính quy, tinh nhuệ và từng bước hiện đại.

ĐIỀU 9: Nghiêm túc tự phê bình và phê bình, giữ gìn đoàn kết, thống nhất trong nội bộ; thương yêu giúp đỡ đồng chí, đồng đội. Chủ động hợp tác với cá nhân và tập thể trong và ngoài lực lượng CAND để hoàn thành xuất sắc nhiệm vụ được giao.

ĐIỀU 10: Thực hiện nghiêm chỉnh các chủ trương, đường lối, chính sách của Đảng, pháp luật của Nhà nước và các qui định của chính quyền địa phương nơi cư trú.

"Chúng ta đang bước vào giai đoạn bình minh của kỷ nguyên số, thời kỳ dữ liệu đã trở thành tài nguyên, tư liệu sản xuất quan trọng, trở thành "năng lượng mới", thậm chí là "máu" của nền kinh tế số. Chuyển đổi số, với dữ liệu là trung tâm, đang làm thay đổi căn bản cách chúng ta sống, làm việc và phát triển"

Tổng Bí thư
TÔ LÂM

"Càng áp lực, thì càng phải nổ lực vươn lên",
"Không nói không, không nói khó, không nói có mà không làm"
"Chỉ bàn làm không bàn lùi",
"Đã nói là phải làm, đã cam kết là phải thực hiện, đã thực hiện là hiệu quả"

Thủ tướng
PHẠM MINH CHÍNH

"Nếu dữ liệu không được thống nhất và tập trung, các nỗ lực chuyển đổi số trong kinh tế và xã hội sẽ khó đạt được thành công. Điều này đặt ra yêu cầu cấp thiết đối với Hiệp hội trong việc xây dựng các cơ chế và chính sách hỗ trợ hiệu quả cho các doanh nghiệp và tổ chức"

Bộ trưởng Bộ Công an

ĐẠI TƯỚNG LƯƠNG TAM QUANG

MỤC LỤC

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 dữ liệu? 10

I. QUY ĐỊNH VỀ SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU 12

II. CÁC GIẢI PHÁP BẢO ĐẢM AN NINH DỮ LIỆU, AN TOÀN DỮ LIỆU TRONG ỨNG DỤNG CÁC SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU 44

Tạm kết câu 7 144

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. 145

PHẦN I. NỘI DUNG QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU 147

I. NỘI DUNG QUẢN LÝ 148

II. 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 192

III. NHIỆM VỤ TRỌNG TÂM CẦN TẬP TRUNG TRONG GIAI ĐOẠN TỪ NAY ĐẾN NĂM 2030 234

IV. ĐỀ XUẤT 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 239

Tạm kết câu 8 327

Lời kết 328

DANH MỤC TÀI LIỆU THAM KHẢO 331

BÀI DỰ THI TÌM HIỂU

LUẬT DỮ LIỆU TRONG CÔNG AN NHÂN DÂN

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 dữ liệu?

Tóm tắt: *Trong bối cảnh dữ liệu trở thành tài sản chiến lược của quốc gia, việc quy định chặt chẽ về sản phẩm, dịch vụ dữ liệu là yêu cầu cấp thiết nhằm tạo lập hành lang pháp lý rõ ràng, thúc đẩy đổi mới sáng tạo, bảo vệ quyền và lợi ích của tổ chức, cá nhân. Các sản phẩm, dịch vụ dữ liệu bao gồm thu thập, xử lý, lưu trữ, phân tích, cung cấp dữ liệu dưới nhiều hình thức và mức độ. Pháp luật cần xác định rõ tiêu chuẩn, điều kiện cấp phép, quyền – nghĩa vụ của các chủ thể cung cấp dịch vụ dữ liệu; đồng thời kiểm soát chất lượng, tính hợp pháp, hợp lệ của dữ liệu được khai thác. Để bảo đảm an ninh, an toàn trong ứng dụng các sản phẩm, dịch vụ về dữ liệu, các giải pháp trọng tâm gồm: hoàn thiện hệ thống pháp luật về dữ liệu và an toàn thông tin; xây dựng cơ chế giám sát, cảnh báo, kiểm định dữ liệu; ứng dụng công nghệ mã hóa, xác thực, kiểm soát truy cập và bảo vệ dữ liệu theo từng cấp độ; phát triển đội ngũ chuyên gia an toàn thông tin; nâng cao nhận thức, kỹ năng số cho cán bộ, người dân và doanh nghiệp; thiết lập cơ chế phối hợp liên ngành nhằm xử lý sự cố, điều tra, truy vết các hành vi vi phạm, đảm bảo chủ quyền số quốc gia trong mọi hoạt động liên quan đến dữ liệu.*

I. QUY ĐỊNH VỀ SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU

1. Khái niệm sản phẩm, dịch vụ về dữ liệu

Ảnh minh họa, Nguồn từ Internet

Dữ liệu đã vượt khỏi vai trò là tài nguyên đầu vào thông thường để trở thành một yếu tố sản xuất mới, ngang hàng với vốn, lao động, đất đai và công nghệ. Cùng với sự phát triển mạnh mẽ của công nghệ thông tin và truyền thông, sự bùng nổ

của Internet, mạng xã hội, thiết bị di động và cảm biến IoT, khối lượng dữ liệu được tạo ra trên toàn cầu đang tăng theo cấp số nhân. Trên nền tảng đó, những sản phẩm và dịch vụ được tạo ra từ dữ liệu đã và đang hình thành một hệ sinh thái mới – được gọi chung là các sản phẩm, dịch vụ về dữ liệu. Việc làm rõ khái niệm này không chỉ có ý nghĩa lý luận mà còn là cơ sở để hoạch định chính sách phát triển kinh tế số và quản lý nhà nước trong giai đoạn hiện nay.

Sản phẩm, dịch vụ về dữ liệu là khái niệm phản ánh những kết quả đầu ra có giá trị, được tạo ra thông qua việc thu thập, lưu trữ, xử lý, phân tích, chia sẻ hoặc khai thác dữ liệu nhằm phục vụ các mục tiêu nhất định như quản trị, kinh doanh, nghiên cứu, giáo dục, cải cách hành chính hay cung cấp dịch vụ công. Khác với sản phẩm vật chất, sản phẩm dữ liệu không mang tính hữu hình mà thường tồn tại dưới dạng số hóa, có thể sao chép không giới hạn với chi phí cận biên gần bằng không. Dịch vụ về dữ liệu là những hoạt động chuyên môn được cung cấp cho tổ chức hoặc cá nhân nhằm hỗ trợ họ trong việc truy cập, phân tích, sử dụng hoặc bảo vệ dữ liệu một cách hiệu quả. Trong kỷ nguyên dữ liệu, việc phát triển các sản phẩm và dịch vụ dữ liệu không chỉ mang lại lợi ích về kinh tế mà còn tạo ra giá trị xã hội to lớn, thúc đẩy minh bạch hóa, ra quyết định dựa trên bằng chứng và đổi mới sáng tạo trên nhiều lĩnh vực.

Phân tích khái niệm trên có thể nhận thấy rằng sản phẩm dữ liệu thường là kết quả của quá trình xử lý dữ liệu thô thành thông tin có cấu trúc và có giá trị sử dụng. Ví dụ điển hình là các bộ dữ liệu mở của cơ quan nhà nước, các báo cáo phân tích dữ liệu lớn *(Big Data analytics)*, các mô hình học máy *(machine learning models)* hay bản đồ số hóa. Trong lĩnh vực tài chính – ngân hàng, sản phẩm dữ liệu có thể là bảng chấm điểm tín dụng dựa trên lịch sử giao dịch và hành vi người tiêu dùng. Trong thương mại điện tử, sản phẩm dữ liệu là hệ thống gợi ý sản phẩm được xây dựng trên hành vi mua sắm và tìm kiếm của người

dùng. Các công ty công nghệ lớn như Google, Facebook, Amazon, Alibaba... đã thành công nhờ vào việc coi dữ liệu là nguyên liệu đầu vào và liên tục phát triển sản phẩm từ đó. Bản thân công cụ tìm kiếm Google là một sản phẩm dữ liệu, được xây dựng từ việc thu thập, lập chỉ mục và phân tích hàng tỷ trang web trên toàn cầu.

Dịch vụ về dữ liệu, về bản chất, là những hình thức phục vụ chuyên biệt giúp người dùng khai thác hoặc bảo vệ dữ liệu hiệu quả hơn. Các dịch vụ này bao gồm: thu thập dữ liệu (dưới dạng khảo sát số, cảm biến, trích xuất từ web), lưu trữ dữ liệu (trên đám mây, máy chủ riêng), chuẩn hóa dữ liệu (làm sạch, gán nhãn, chuyển đổi định dạng), phân tích dữ liệu (dùng công cụ thống kê, học máy), trực quan hóa dữ liệu (báo cáo, dashboard), chia sẻ dữ liệu (qua API, nền tảng mở), và bảo mật dữ liệu (mã hóa, kiểm soát truy cập, tuân thủ pháp lý). Một ví dụ điển hình về dịch vụ dữ liệu là các công ty cung cấp nền tảng DaaS (Data-as-a-Service), cho phép khách hàng truy cập dữ liệu theo yêu cầu thông qua giao diện lập trình ứng dụng. Các doanh nghiệp sử dụng dịch vụ này để lấy dữ liệu thị trường, dữ liệu đối thủ hoặc dữ liệu địa phương hóa mà không cần tự thu thập hoặc xây dựng hạ tầng riêng.

Một số đặc điểm nổi bật của sản phẩm và dịch vụ dữ liệu có thể nhận diện rõ. Thứ nhất, tính phi vật chất – dữ liệu và sản phẩm từ dữ liệu thường tồn tại ở dạng số hóa, có thể sao chép vô hạn với chi phí thấp. Thứ hai, tính chia sẻ – một nguồn dữ liệu có thể được sử dụng đồng thời bởi nhiều người hoặc hệ thống, tạo ra hiệu quả quy mô lớn. Thứ ba, tính tái sử dụng – dữ liệu khi được tổ chức và lưu trữ đúng cách có thể phục vụ nhiều mục đích khác nhau mà không cần tái thu thập. Thứ tư, tính biến động – giá trị của dữ liệu phụ thuộc vào ngữ cảnh, thời gian và công nghệ phân tích; dữ liệu cũ có thể mất giá trị

nhanh nếu không được cập nhật. Cuối cùng là tính bảo mật – dữ liệu là tài sản đặc biệt cần được bảo vệ nghiêm ngặt, nhất là dữ liệu cá nhân, dữ liệu tài chính, dữ liệu an ninh quốc gia.

Xét về phân loại, sản phẩm và dịch vụ dữ liệu có thể được chia theo nhiều tiêu chí. Nếu xét theo đối tượng phục vụ, có thể phân biệt dữ liệu công (do nhà nước cung cấp), dữ liệu doanh nghiệp (phục vụ sản xuất kinh doanh), và dữ liệu cá nhân (phục vụ người tiêu dùng). Nếu xét theo chức năng, có thể phân loại thành dữ liệu mô tả (descriptive), dữ liệu chẩn đoán (diagnostic), dữ liệu dự báo (predictive) và dữ liệu hướng dẫn hành động (prescriptive). Nếu xét theo nguồn gốc, có thể phân biệt dữ liệu do người dùng tạo (user-generated), dữ liệu từ máy móc (machine-generated), và dữ liệu thu thập qua trung gian (third-party data). Sự phân loại này giúp xây dựng các chiến lược phát triển và quản lý dữ liệu phù hợp, tối ưu hóa giá trị tạo ra từ dữ liệu.

Dữ liệu khách hàng cá nhân. Ảnh minh họa. Nguồn từ Internet.

Vai trò của sản phẩm và dịch vụ dữ liệu ngày càng trở nên trọng yếu trong phát triển kinh tế – xã hội hiện đại. Trong quản trị nhà nước, việc sử dụng các chỉ số dữ liệu, bản đồ số hóa dân cư, phân tích dữ liệu hành chính giúp tăng cường hiệu quả điều hành, cải cách thủ tục hành chính, minh bạch hóa quy trình ra quyết định và nâng cao sự hài lòng của người dân. Trong lĩnh vực kinh tế, dữ liệu là cơ sở để tối ưu hóa chuỗi cung ứng, định giá linh hoạt, phân tích hành vi tiêu dùng và dự báo xu hướng thị trường. Trong lĩnh vực y tế, giáo dục và an sinh xã hội, dữ liệu góp phần quan trọng vào việc phân bổ nguồn

lực, phát hiện sớm vấn đề và xây dựng chính sách dựa trên bằng chứng. Đặc biệt, dữ liệu đóng vai trò nền tảng trong phát triển các mô hình trí tuệ nhân tạo, từ đó mở ra tiềm năng đổi mới sáng tạo đột phá.

Việc phát triển sản phẩm và dịch vụ dữ liệu cũng mở ra một ngành công nghiệp mới – kinh tế dữ liệu (data economy). Nhiều quốc gia đã xác định dữ liệu là yếu tố sản xuất chủ chốt trong nền kinh tế số. Các doanh nghiệp khởi nghiệp trong lĩnh vực dữ liệu đang phát triển mạnh mẽ, từ các công ty phân tích dữ liệu, xây dựng mô hình trí tuệ nhân tạo, cung cấp dịch vụ đám mây, đến các nền tảng dữ liệu mở hoặc dữ liệu chuyên sâu. Thị trường dữ liệu đã hình thành với các hoạt động mua bán dữ liệu, trao đổi dữ liệu liên tổ chức và định giá dữ liệu như một loại tài sản. Điều này đặt ra yêu cầu cấp thiết về khung pháp lý, chuẩn hóa, định nghĩa tài sản dữ liệu và quyền sở hữu dữ liệu, bảo đảm sự phát triển lành mạnh và bền vững của thị trường.

Tuy nhiên, để phát huy giá trị của sản phẩm và dịch vụ dữ liệu, cần đồng thời giải quyết nhiều thách thức. Trước hết là vấn đề phân mảnh dữ liệu – nhiều cơ quan, doanh nghiệp và địa phương sở hữu dữ liệu nhưng không chia sẻ, gây lãng phí và trùng lặp. Thứ hai là vấn đề chất lượng dữ liệu – dữ liệu không đầy đủ, không chuẩn hóa, thiếu cập nhật hoặc sai lệch làm giảm hiệu quả khai thác. Thứ ba là vấn đề năng lực – nhiều tổ chức, đặc biệt ở cấp địa phương, còn thiếu kỹ năng phân tích và quản lý dữ liệu. Thứ tư là vấn đề pháp lý và đạo đức – dữ liệu cá nhân dễ bị xâm phạm, sử dụng sai mục đích nếu không có chế tài và quy định rõ ràng. Do đó, cần có chính sách quốc gia về dữ liệu, trong đó ưu tiên xây dựng hạ tầng dữ liệu, phát triển nhân lực, hoàn thiện thể chế và thúc đẩy hợp tác công – tư trong lĩnh vực dữ liệu.

2. Các loại hình sản phẩm, dịch vụ về dữ liệu

Sự phát triển mạnh mẽ của công nghệ số và dữ liệu lớn đã làm thay đổi căn bản cách thức vận hành của nền kinh tế và bộ máy quản lý nhà nước, đồng thời tạo ra một hệ sinh thái mới – nơi sản phẩm và dịch vụ dữ liệu trở thành một lĩnh vực kinh tế có giá trị gia tăng cao, có khả năng dẫn dắt đổi mới sáng tạo và cạnh tranh toàn cầu. Chính vì vậy, Điều 39 Luật Dữ liệu năm 2024 là một quy định trọng yếu, nhằm xác lập cơ sở pháp lý cho việc hình thành và phát triển thị trường sản phẩm, dịch vụ về dữ liệu tại Việt Nam.

Trước hết, khoản 1 Điều 39 khẳng định rõ: các sản phẩm, dịch vụ về dữ liệu trong các lĩnh vực như trung gian dữ liệu, phân tích dữ liệu, tổng hợp dữ liệu, xác thực điện tử và vận hành sàn dữ liệu đều phải tuân thủ theo Luật Dữ liệu và các quy định pháp luật có liên quan. Điều này cho thấy sự nhận diện đầy đủ các hoạt động có giá trị thương mại từ dữ liệu, đồng thời yêu cầu cao về trách nhiệm pháp lý, minh bạch, chuẩn hóa, đặc biệt trong bối cảnh giao dịch dữ liệu có thể liên quan đến quyền cá nhân, bí mật doanh nghiệp và an ninh quốc gia.

Tiếp theo, khoản 2 quy định cụ thể về dịch vụ xác thực điện tử – đây là một dịch vụ kỹ thuật số quan trọng giúp đảm bảo tính chính xác, tin cậy và hợp pháp của dữ liệu trong các cơ sở dữ liệu quốc gia, chuyên ngành và hệ thống định danh điện tử. Luật yêu cầu dịch vụ này chỉ được thực hiện bởi đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước đáp ứng đủ điều kiện. Điều này nhằm kiểm soát chặt chẽ việc xác thực danh tính, tránh nguy cơ gian lận, giả mạo, và bảo vệ quyền lợi của cá nhân, tổ chức khi dữ liệu được sử dụng trong các giao dịch hành chính, dân sự, tài chính…

Khoản 3 của Điều luật đề cập đến chính sách ưu đãi cho các tổ chức cung cấp dịch vụ trung gian, phân tích, tổng hợp dữ liệu, theo đó các đơn vị này được hưởng ưu đãi như các doanh nghiệp hoạt động trong lĩnh vực công nghệ cao, đổi mới sáng tạo và khởi nghiệp sáng tạo. Đây là điểm nhấn thể hiện chính sách phát triển có chiều sâu, khuyến khích hình thành doanh nghiệp dữ liệu – trụ cột của kinh tế số, đồng thời thúc đẩy hình thành hệ sinh thái sáng tạo dựa trên dữ liệu, tương thích với các xu hướng toàn cầu như dữ liệu mở, dữ liệu theo yêu cầu (Data as a Service – DaaS), trí tuệ nhân tạo và phân tích dự báo.

Khoản 4 mở rộng phạm vi điều chỉnh đối với các sản phẩm, dịch vụ dữ liệu đặc thù trong những lĩnh vực nhạy cảm và quan trọng như giao dịch điện tử, an ninh mạng, công nghiệp quốc phòng, cơ yếu, viễn thông…. Đây là các lĩnh vực có yêu cầu đặc biệt về an ninh, kỹ thuật, tính chính xác và kiểm soát truy cập dữ liệu. Vì vậy, Luật Dữ liệu chỉ xác định nguyên tắc chung và giao cho các luật chuyên ngành điều chỉnh cụ thể để đảm bảo phù hợp với từng lĩnh vực đặc thù.

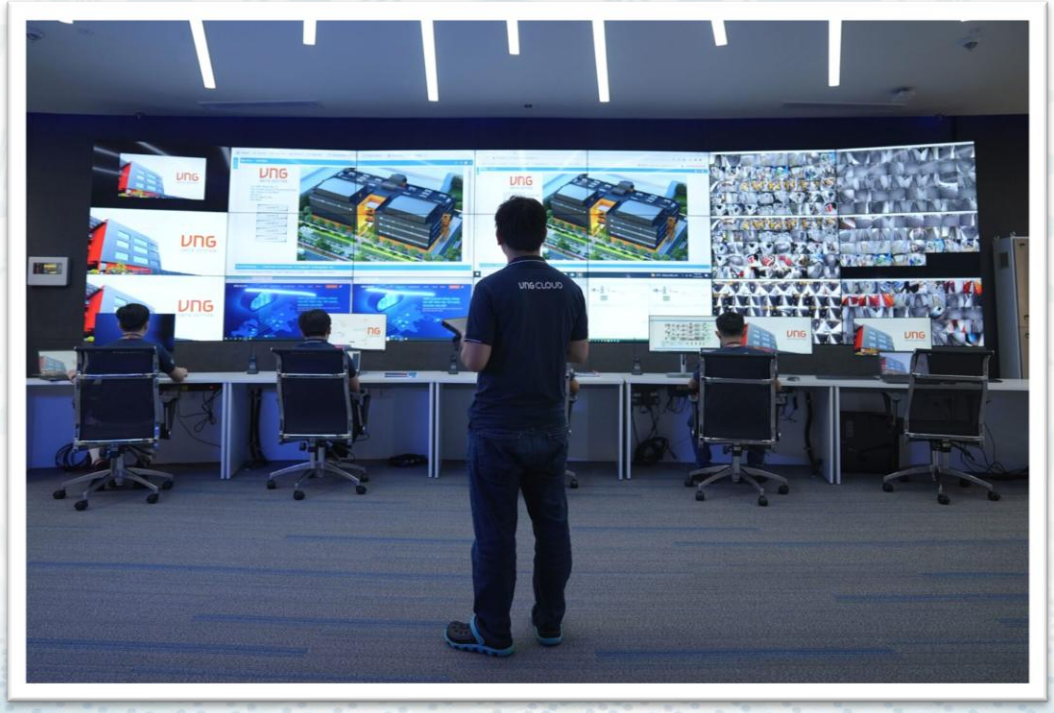
Khoản 5 giao Chính phủ ban hành các quy định chi tiết để hướng dẫn triển khai Điều luật này. Điều đó cho thấy nhận thức rõ ràng của nhà làm luật rằng thị trường sản phẩm, dịch vụ dữ liệu là một lĩnh vực mới mẻ, phức tạp và biến động nhanh, do đó cần có cơ chế điều hành linh hoạt và sự phối hợp giữa nhiều cơ quan quản lý khác nhau.

Điều 39 của Luật Dữ liệu năm 2024 không chỉ mang tính định danh pháp lý cho sản phẩm, dịch vụ dữ liệu, mà còn thiết lập khung thể chế để bảo đảm việc phát triển thị trường dữ liệu minh bạch, an toàn, có kiểm soát và phù hợp với định hướng phát triển kinh tế số của Việt Nam. Đây là cơ sở để hình thành các doanh nghiệp dữ liệu Việt Nam có khả năng cạnh tranh toàn cầu, đồng thời là nền tảng cho việc phát triển các ứng dụng số, dịch vụ công và công nghệ thông minh dựa trên dữ liệu.

Điều 40 của Luật Dữ liệu năm 2024 lần đầu tiên quy định rõ khái niệm pháp lý và hành lang thể chế cho hoạt động cung cấp sản phẩm, dịch vụ trung gian dữ liệu, tạo nền tảng cho việc hình thành một thị trường dữ liệu minh bạch và chuyên nghiệp. Trước hết, khoản 1 của Điều này xác định: sản phẩm, dịch vụ trung gian dữ liệu là những sản phẩm – dịch vụ thiết lập mối quan hệ thương mại giữa chủ thể dữ liệu, chủ sở hữu dữ liệu và bên sử dụng dữ liệu, thông qua các cơ chế thỏa thuận, nhằm phục vụ mục đích chia sẻ, truy cập, trao đổi dữ liệu hoặc thực hiện các quyền liên quan đến dữ liệu. Nói cách khác, đây chính là hoạt động kết nối cung – cầu dữ liệu, đồng thời bảo đảm quyền lợi hợp pháp của các bên tham gia vào chuỗi giá trị dữ liệu. Trung gian dữ liệu giúp "giải mã" các rào cản về ngôn ngữ kỹ thuật, quyền pháp lý, bảo mật và tiêu chuẩn giữa bên nắm giữ dữ liệu và bên có nhu cầu khai thác dữ liệu, từ đó thúc đẩy lưu thông dữ liệu an toàn, hợp pháp. Quan trọng hơn, việc Luật đưa ra định nghĩa chính thức về trung gian dữ liệu mở đường cho sự phát triển của các tổ chức cung cấp dịch vụ dữ liệu độc lập, chẳng hạn như sàn giao dịch dữ liệu, đơn vị phân phối dữ liệu, nền tảng chia sẻ dữ liệu, công ty phân tích – tổng hợp dữ liệu thuê ngoài (data-as-a-service)… Điều này không chỉ tạo ra ngành nghề kinh doanh mới, mà còn giúp định hình chuỗi giá trị dữ liệu – từ thu thập, làm sạch, lưu trữ, phân tích đến phân phối dữ liệu một cách chuyên nghiệp.

Khoản 2 quy định: tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu phải đăng ký hoạt động và chịu sự quản lý theo pháp luật về đầu tư. Điều này giúp Nhà nước kiểm soát, đánh giá được năng lực, trách nhiệm, và mức độ tuân thủ pháp luật của các đơn vị cung cấp dịch vụ dữ liệu. Tuy nhiên, trong trường hợp cung cấp sản phẩm, dịch vụ trung gian dữ liệu trong nội bộ, ví dụ giữa các phòng, ban trong cùng một tập đoàn, bộ ngành hay doanh nghiệp – thì không cần đăng ký riêng, nhằm tạo điều kiện thuận lợi cho hoạt động chia sẻ dữ liệu nội bộ, đồng thời giảm gánh nặng thủ tục hành chính.

Tại khoản 3, Luật giao Chính phủ quy định chi tiết Điều này – cho phép điều chỉnh linh hoạt các loại hình dịch vụ trung gian theo sự phát triển của thị trường dữ liệu trong nước và quốc tế. Trong tương lai, có thể xuất hiện các mô hình trung gian mới như bên ủy thác dữ liệu (data trustee), đại lý dữ liệu (data broker), hạ tầng dữ liệu đáng tin cậy (trusted data space)… – đòi hỏi cơ chế quản lý phải mở, năng động và có tầm nhìn dài hạn.



Trung tâm dữ liệu của VNG. Ảnh minh họa. Nguồn từ Internet.

Quy định tại Điều 40 mang tính đột phá, vì lần đầu tiên tạo ra khung pháp lý riêng cho hoạt động trung gian dữ liệu – một mắt xích không thể thiếu trong nền kinh tế số. Việc kiểm soát hoạt động trung gian không chỉ nhằm đảm bảo quyền lợi hợp pháp của các bên liên quan, mà còn giúp Nhà nước giám sát được dòng chảy dữ liệu, tránh thất thoát thông tin, rủi ro bảo mật và xung đột pháp lý, nhất là trong bối cảnh dữ liệu ngày càng trở thành tài sản mang tính chiến lược của quốc gia.

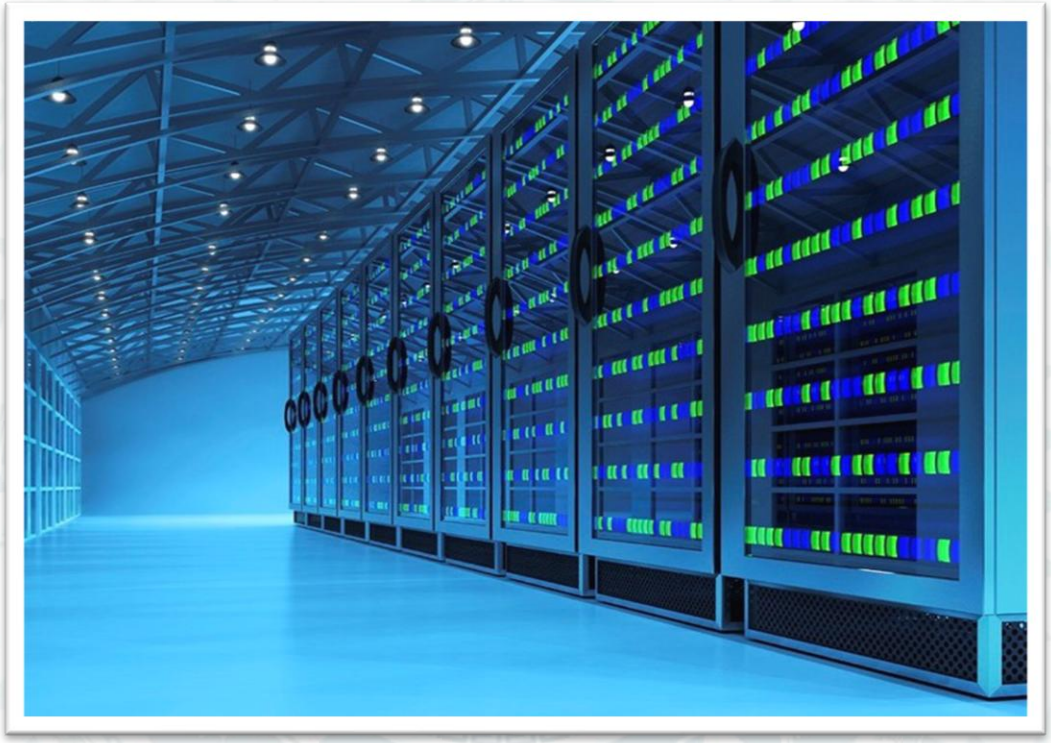
Điều 41 Luật Dữ liệu năm 2024 chính là cơ sở pháp lý quan trọng đầu tiên xác lập khung pháp lý cho sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu tại Việt Nam. Khoản 1 của điều luật này đưa ra khái niệm đầy đủ và chuẩn mực: *sản phẩm phân tích, tổng hợp dữ liệu* là kết quả đầu ra của quá trình xử lý dữ liệu – được tổ chức, sắp xếp lại theo cấu trúc có ý nghĩa và được "chiết xuất" thành thông tin chuyên sâu, hữu ích ở nhiều cấp độ, như: thống kê mô tả, mô hình dự báo, bản đồ dữ liệu, báo cáo phân tích, dashboard tương tác v.v... Trong khi đó, *dịch vụ phân tích, tổng hợp dữ liệu* lại mang tính linh hoạt theo đặt hàng cụ thể từ bên sử dụng, thể hiện xu hướng "dữ liệu như một dịch vụ" (DaaS – Data as a Service).

Tuy nhiên, vì dữ liệu ngày nay gắn liền với nhiều lĩnh vực nhạy cảm như an ninh quốc phòng, tài chính – ngân hàng, y tế, thông tin dân cư…, nên khoản 2 của điều luật này đã thiết lập hành lang pháp lý chặt chẽ đối với hoạt động phân tích, tổng hợp dữ liệu có nguy cơ gây rủi ro cao. Theo đó, mọi tổ chức kinh doanh dịch vụ phân tích dữ liệu có khả năng ảnh hưởng tiêu cực đến quốc phòng, an ninh, đạo đức, sức khỏe cộng đồng… đều phải đăng ký hoạt động và chịu sự quản lý theo pháp luật về đầu tư. Đây là một biện pháp vừa thúc đẩy phát triển thị trường dữ liệu hợp pháp, vừa chủ động kiểm soát các lỗ hổng có thể bị lợi dụng để thao túng thông tin, xâm phạm quyền riêng tư hoặc gây bất ổn xã hội. Trường hợp doanh nghiệp, tổ chức có kết nối và khai thác dữ liệu từ cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành để phục vụ hoạt động phân tích, kinh

doanh, thì sẽ chịu sự điều chỉnh nghiêm ngặt của Luật Dữ liệu và các luật có liên quan. Điều này nhằm tránh tình trạng "trục lợi dữ liệu công" – tức là sử dụng dữ liệu thu thập từ Nhà nước để phục vụ cho mục tiêu lợi nhuận mà không tuân thủ cơ chế quản lý, chia sẻ hoặc không bảo đảm quyền lợi của chủ thể dữ liệu.

Khoản 3 tiếp tục giao Chính phủ quy định chi tiết điều luật để kịp thời điều chỉnh, cập nhật với thực tiễn đổi mới nhanh chóng của công nghệ phân tích dữ liệu, như: trí tuệ nhân tạo (AI), học máy (machine learning), xử lý ngôn ngữ tự nhiên (NLP), khai phá dữ liệu (data mining), phân tích dự đoán (predictive analytics)...

Điều 41 là nền tảng pháp lý tiên phong cho việc phát triển ngành công nghiệp phân tích dữ liệu – vốn là yếu tố quyết định hiệu quả khai thác tài nguyên số trong thời đại mới. Bên cạnh việc mở đường cho các dịch vụ giá trị gia tăng từ dữ liệu, Điều 41 còn thiết lập ranh giới pháp lý cần thiết nhằm bảo đảm rằng mọi hoạt động xử lý – phân tích dữ liệu được kiểm soát, có mục đích chính đáng và tuân thủ nghiêm túc các nguyên tắc an ninh dữ liệu, an toàn thông tin và quyền của người dân. Điều này thể hiện rõ sự thận trọng nhưng linh hoạt của Nhà nước trong quản trị dữ liệu một cách chủ động, kiến tạo và bền vững.



Ảnh minh họa, Nguồn từ Internet

3. Sản phẩm, dịch vụ trung gian dữ liệu

Điều 23 của Nghị định 169/2025/NĐ-CP quy định về sản phẩm và dịch vụ trung gian dữ liệu, trong đó sản phẩm trung gian dữ liệu là các sản phẩm, dịch vụ do tổ chức cung cấp nhằm hỗ trợ hạ tầng, trang thiết bị, ứng dụng, phần mềm phục vụ cho

chủ thể dữ liệu và chủ sở hữu dữ liệu thực hiện các hoạt động theo quy định tại Điều 24 của Nghị định. Dịch vụ trung gian dữ liệu là các sản phẩm, dịch vụ được tổ chức cung cấp nhằm phục vụ hoạt động trung gian 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, đảm bảo các yếu tố an toàn, hiệu quả và đúng định dạng. Tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu khi thực hiện hoạt động trung gian giữa bên sử dụng dịch vụ và cơ quan nhà nước phải được đăng ký quản lý và cấp phép theo quy định tại Nghị định này. Đồng thời, Nghị định cũng nêu rõ sản phẩm, dịch vụ trung gian dữ liệu không bao gồm dịch vụ điện toán đám mây, dịch vụ trung tâm dữ liệu, các sản phẩm, dịch vụ trung gian dữ liệu trong nội bộ tổ chức, cũng như các sản phẩm, dịch vụ đã được quy định tại các văn bản quy phạm pháp luật khác. Quy định này giúp làm rõ phạm vi và đối tượng của sản phẩm, dịch vụ trung gian dữ liệu nhằm tạo cơ sở pháp lý cho hoạt động liên quan trong lĩnh vực khoa học, công nghệ và đổi mới sáng tạo về dữ liệu.

Điều 24 của Nghị định 169/2025/NĐ-CP quy định cụ thể các nội dung hoạt động trung gian dữ liệu nhằm làm rõ phạm vi, chức năng và trách nhiệm của các tổ chức cung cấp dịch vụ trung gian trong lĩnh vực dữ liệu. Theo đó, các tổ chức này có thể đại diện cho chủ thể dữ liệu và chủ sở hữu dữ liệu để thực hiện kết nối, chia sẻ, trao đổi và truy cập dữ liệu với bên sử dụng dịch vụ. Họ cũng thực hiện tư vấn và đánh giá tác động của việc xử lý dữ liệu, đồng thời cung cấp dịch vụ quản trị dữ liệu để ủy thác thay mặt cho chủ thể hoặc chủ sở hữu dữ liệu trong các hoạt động kết nối, chia sẻ, trao đổi và truy cập dữ liệu. Các tổ chức còn có thể làm đại lý kết nối giữa các bên, cung cấp hạ tầng, trang thiết bị, ứng dụng, phần mềm và dịch vụ truyền đưa phục vụ hoạt động trung gian dữ liệu. Họ chịu trách nhiệm hỗ trợ kiểm soát các thuộc tính dữ liệu để bảo đảm quyền riêng tư, bảo vệ dữ liệu nhạy cảm và dữ liệu cá nhân, đồng thời đánh giá rủi ro liên quan đến việc chuyển và xử lý dữ liệu cốt

lõi, dữ liệu quan trọng theo quy định pháp luật. Dịch vụ hợp tác và chia sẻ dữ liệu cũng được cung cấp nhằm phục vụ kết nối, khai thác và truy cập dữ liệu hợp pháp. Tổ chức trung gian còn tham gia thẩm định điều kiện tham gia sàn dữ liệu của các chủ thể liên quan, đánh giá tính hợp pháp và khả năng đáp ứng yêu cầu bảo đảm an ninh, an toàn khi sử dụng sản phẩm dữ liệu. Các hoạt động bổ sung theo quy định của hoạt động thử nghiệm có kiểm soát cũng được thực hiện để đánh giá và phân tích, góp phần hoàn thiện và nâng cao chất lượng hoạt động trung gian dữ liệu. Những quy định này nhằm xây dựng một hệ sinh thái dữ liệu minh bạch, an toàn và hiệu quả, thúc đẩy phát triển khoa học công nghệ và đổi mới sáng tạo tại Việt Nam.

Điều 25 của Nghị định 169/2025/NĐ-CP quy định về 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 nhằm đảm bảo tính chuyên nghiệp, an toàn và hiệu quả trong hoạt động trung gian dữ liệu. Theo đó, tổ chức này có thể là đơn vị sự nghiệp hoặc doanh nghiệp được thành lập và hoạt động hợp pháp tại Việt Nam, đồng thời phải đáp ứng đầy đủ các yêu cầu về nhân sự, cơ sở vật chất kỹ thuật, quy trình quản lý và tài chính. Về nhân sự, người đứng đầu hoặc 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 quản lý dữ liệu, đồng thời không thuộc các trường hợp bị hạn chế theo khoản 1 Điều 9 của Nghị định. Tổ chức cũng cần có ít nhất 5 nhân sự trình độ đại học trở lên, sở hữu các chứng chỉ chuyên môn liên quan đến khoa học dữ liệu, phân tích dữ liệu, quản lý và thẩm định dữ liệu. Về cơ sở vật chất, tổ chức phải có hạ tầng, trang thiết bị kỹ thuật đặt tại Việt Nam, được kiểm định an ninh, an toàn thông tin theo quy định pháp luật, đồng thời xây dựng đề án hoạt động chi tiết bao gồm các phương án vận hành dịch vụ trung gian dữ liệu như: quy trình hoạt động, kỹ thuật công nghệ, lưu trữ và bảo vệ dữ liệu, bảo đảm an ninh trật tự, thanh toán, thẩm định dữ liệu, định danh và xác thực điện tử, phòng

cháy chữa cháy, dự phòng thảm họa, vận hành ổn định và thuyết minh về trang thiết bị kỹ thuật. Về tài chính, tổ chức phải ký quỹ tại ngân hàng thương mại hoạt động tại Việt Nam với số tiền không dưới 5 tỷ đồng nhằm đảm bảo khả năng giải quyết rủi ro và đền bù thiệt hại phát sinh do lỗi của tổ chức trong quá trình cung cấp dịch vụ, cũng như chi trả chi phí duy trì cơ sở dữ liệu nếu bị thu hồi giấy phép. Những điều kiện này nhằm nâng cao chất lượng, độ tin cậy và bảo mật của dịch vụ trung gian dữ liệu, đồng thời góp phần thúc đẩy phát triển hệ sinh thái dữ liệu an toàn và minh bạch tại Việt Nam.

Điều 26 của Nghị định 169/2025/NĐ-CP quy định rõ trách nhiệm của tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu nhằm đảm bảo việc kết nối, chia sẻ, trao đổi và truy cập dữ liệu được thực hiện minh bạch, an toàn và tuân thủ pháp luật. Theo đó, tổ chức cung cấp dịch vụ phải chứng minh trách nhiệm trong việc bảo vệ dữ liệu, đặc biệt là dữ liệu cá nhân, tuân thủ các quy định pháp luật về bảo vệ dữ liệu cá nhân. Họ phải thông báo rõ ràng cho chủ sở hữu dữ liệu, chủ thể dữ liệu và bên sử dụng về mục đích cung cấp dịch vụ, đồng thời đảm bảo việc thu thập, sử dụng hay tiết lộ dữ liệu cá nhân chỉ được thực hiện khi có sự đồng ý hợp pháp của chủ thể dữ liệu. Tổ chức phải bảo đảm dữ liệu được cung cấp đầy đủ, chính xác và việc truy cập dữ liệu diễn ra đúng mục đích, đúng đối tượng và theo đúng hợp đồng đã ký kết. Các biện pháp bảo mật hợp lý cần được thực hiện để ngăn chặn truy cập, sử dụng hay tiết lộ dữ liệu trái phép, đồng thời hạn chế lưu trữ dữ liệu cá nhân trong thời gian cần thiết, xử lý thông tin đúng quy định khi không còn phục vụ mục đích kinh doanh hoặc pháp lý. Việc chuyển giao dữ liệu cá nhân xuyên biên giới phải tuân thủ tiêu chuẩn bảo vệ tương đương quy định pháp luật. Trong trường hợp xảy ra vi phạm dữ liệu gây tác hại đáng kể hoặc có quy mô lớn, tổ chức phải thông báo ngay cho các bên bị ảnh hưởng. Tổ chức cũng phải bảo đảm khả năng chuyển dữ liệu chính xác tới bên sử dụng theo thỏa thuận, cung cấp dịch vụ tư vấn,

đánh giá tác động xử lý dữ liệu, thẩm định dữ liệu cùng với các hình thức thanh toán linh hoạt và tuân thủ quy định về thuế, phí, giá trong thương mại điện tử. Tổ chức tham gia hoạt động trung gian dữ liệu bắt buộc phải thực hiện xác thực danh tính theo quy định pháp luật về định danh và xác thực điện tử, nhằm nâng cao độ tin cậy và bảo mật cho toàn bộ quá trình hoạt động. Những trách nhiệm này là cơ sở để xây dựng môi trường dữ liệu an toàn, minh bạch và bảo vệ quyền lợi của các bên liên quan.

4. Sản phẩm phân tích, tổng hợp dữ liệu

Điều 27 của Nghị định 169/2025/NĐ-CP quy định bốn cấp độ phân tích và tổng hợp dữ liệu, thể hiện mức độ can thiệp và ứng dụng trí tuệ nhân tạo (AI) trong quá trình xử lý dữ liệu. Ở cấp độ 1, toàn bộ quá trình phân tích và tổng hợp dữ liệu do con người trực tiếp thực hiện, sử dụng các thiết bị và phần mềm không tích hợp AI. Cấp độ 2 là sự kết hợp giữa con người và AI, trong đó con người vẫn thực hiện chính công việc phân tích nhưng được hỗ trợ một phần bởi các công cụ trí tuệ nhân tạo. Cấp độ 3 mô tả việc phân tích và tổng hợp dữ liệu hoàn toàn do AI thực hiện, tuy nhiên vẫn có sự giám sát của con người trong suốt quá trình để đảm bảo độ chính xác và an toàn. Cấp độ 4 là mức độ cao nhất, với phân tích và tổng hợp dữ liệu được AI thực hiện hoàn toàn tự động mà không có sự giám sát của con người. Các cấp độ này giúp xác định rõ ràng phạm vi áp dụng công nghệ AI trong hoạt động phân tích dữ liệu, đồng thời làm cơ sở cho việc quản lý, giám sát và phát triển các sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu theo đúng quy định pháp luật.

Điều 28 quy định các trường hợp tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu phải được cấp Giấy chứng nhận đủ điều kiện kinh doanh. Cụ thể, tổ chức cung cấp dịch vụ ở cấp độ 3 và cấp độ 4 trong hệ thống thông tin của cơ

quan nhà nước, có khả năng gây nguy hại đến quốc phòng, an ninh, trật tự xã hội hoặc sức khỏe cộng đồng; các sản phẩm có kết nối hoặc chia sẻ với cơ sở dữ liệu quốc gia, chuyên ngành; hoặc sử dụng dữ liệu cốt lõi, dữ liệu quan trọng đều thuộc phạm vi cấp giấy phép. Đồng thời, các tổ chức không thuộc trường hợp này vẫn phải gửi thông báo cho Bộ Công an khi cung cấp dịch vụ, và có thể được thẩm định để hưởng ưu đãi như các doanh nghiệp hoạt động trong lĩnh vực công nghệ cao, đổi mới sáng tạo hoặc khởi nghiệp. Các sản phẩm dịch vụ thuộc diện ưu đãi gồm trợ lý ảo, hệ thống AI tạo sinh, dịch vụ phân tích nội dung tự động có tương tác trực tiếp, các dịch vụ xử lý dữ liệu nhạy cảm trên quy mô lớn, dịch vụ tự động cấp độ cao trong ngành công nghiệp hoặc dữ liệu huấn luyện mô hình lớn (từ 10 TB trở lên). Nghị định cũng nêu rõ không bao gồm các hoạt động phân tích, tổng hợp dữ liệu nội bộ tổ chức và các sản phẩm dịch vụ đã được quy định trong các văn bản pháp luật khác.

Điều 29 đưa ra các điều kiện kinh doanh mà tổ chức phải đáp ứng, gồm việc phải là đơn vị sự nghiệp hoặc doanh nghiệp thành lập hợp pháp tại Việt Nam; nhân sự quản lý phải là công dân Việt Nam, có trình độ đại học trở lên và kinh nghiệm quản lý dữ liệu theo quy định; đội ngũ kỹ thuật có chứng chỉ hoặc kinh nghiệm chuyên sâu trong các lĩnh vực khoa học dữ liệu, phân tích dữ liệu, quản trị dữ liệu hoặc thẩm định dữ liệu. Tổ chức phải có hệ thống trang thiết bị, cơ sở vật chất và công nghệ phù hợp với phương án kinh doanh. Phương án kinh doanh này cần bao gồm phạm vi, đối tượng cung cấp sản phẩm, loại hình sản phẩm dự kiến, tiêu chuẩn, quy chuẩn kỹ thuật áp dụng và các tính năng kỹ thuật cơ bản của sản phẩm, dịch vụ.

Ảnh minh họa. Nguồn từ Internet.

Điều 30 đưa ra ba tiêu chí cốt lõi để thẩm định sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu. Một là tính hợp pháp của nguồn dữ liệu được sử dụng, bảo đảm dữ liệu được thu thập và khai thác theo đúng quy định pháp luật. Hai là đánh giá mô hình, công thức phân tích, bảo đảm không tạo ra các tác động tiêu cực như thao túng, định hướng người dùng ảnh hưởng đến an ninh, trật tự xã hội, hệ thống công nghiệp trọng yếu hay sức khỏe cộng đồng. Ba là tiêu chí đánh giá độ chính xác, tin cậy của mô hình phân tích – một yêu cầu đặc biệt quan trọng trong bối cảnh dữ liệu được sử dụng để hỗ trợ ra quyết định.

Điều 31 xác lập trách nhiệm pháp lý và đạo đức của tổ chức cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu. Các tổ chức này phải ký hợp đồng cung cấp dịch vụ rõ ràng, minh bạch với bên sử dụng; cung cấp thông tin chi tiết về sản phẩm, rủi ro và quyền lợi của người sử dụng; tuân thủ các quy định liên quan đến bảo vệ dữ liệu cá nhân, an toàn thông tin và an ninh mạng. Đơn vị cung cấp còn phải thực hiện báo cáo định kỳ, đặc biệt là báo cáo hằng năm theo mẫu và thời hạn quy định, đồng thời đảm bảo hoạt động kinh doanh đúng với phương án đã được cơ quan có thẩm quyền phê duyệt.

5. Việc cung cấp, mua, bán hoặc các giao dịch liên quan đến sản phẩm, dịch vụ về dữ liệu được thực hiện trên nền tảng Sàn dữ liệu

**** Khái niệm:*** 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 *(Theo Điều 42 Luật Dữ liệu 2024)*.

Sàn dữ liệu là một khái niệm mang tính chiến lược trong bối cảnh chuyển đổi số và phát triển kinh tế dữ liệu tại Việt Nam. Theo Điều 42 Luật Dữ liệu năm 2024, sàn dữ liệu không chỉ là một nền tảng kỹ thuật, mà còn là hạ tầng thị trường – nơi tập trung các nguồn lực, dịch vụ và sản phẩm liên quan đến dữ liệu, góp phần hình thành một "thị trường dữ liệu" đúng nghĩa.

Điều 42 là bước đi mạnh mẽ của Nhà nước Việt Nam trong thể chế hóa thị trường dữ liệu, vừa mở ra cơ hội hình thành các mô hình kinh doanh dữ liệu mới, vừa đảm bảo an toàn, minh bạch và bảo vệ quyền lợi của các chủ thể liên quan. Sàn dữ

liệu trong tương lai không chỉ là trung tâm giao dịch, mà còn là nền tảng thúc đẩy sáng tạo, kết nối dữ liệu công – tư, tạo động lực phát triển kinh tế số dựa trên tài nguyên dữ liệu – một loại tài sản quan trọng của thời đại 4.0.

Ảnh minh họa

**** Nội dung về Sàn dữ liệu:***

- Về hoạt động của sàn dữ liệu: Khoản 1 Điều 32 Nghị định 169/2025/NĐ-CP xác định rõ, sàn dữ liệu hoạt động như sau:

(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 như: Dữ liệu trong cơ sở dữ liệu chuyên ngành, Cơ sở dữ liệu quốc gia; Dữ liệu do cơ quan, tổ chức, cá nhân khác cung cấp.

(2) Cung cấp dịch vụ, gồm:

+ 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;

+ Dịch vụ đấu giá dữ liệu;

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

Như vậy, có thể thấy được rằng sàn dữ liệu có ba chức năng cốt lõi. Thứ nhất, nó là nền tảng cung cấp tài nguyên dữ liệu để phục vụ nghiên cứu, khởi nghiệp và đổi mới sáng tạo, qua đó góp phần nuôi dưỡng hệ sinh thái công nghệ trong nước. Thứ hai, sàn là nơi cung cấp các sản phẩm, dịch vụ từ dữ liệu, bao gồm dịch vụ trung gian, dịch vụ phân tích, tổng hợp, xác thực, nhằm thúc đẩy ứng dụng dữ liệu vào đời sống, sản xuất – kinh doanh, hành chính công. Thứ ba, sàn dữ liệu là môi trường giao dịch, nơi các tổ chức, cá nhân có thể trao đổi, thương mại hóa dữ liệu một cách minh bạch, có kiểm soát – từ đó tạo lập giá trị mới cho dữ liệu, biến dữ liệu thành một loại "hàng hóa số".

- Về cơ chế hoạt động của sàn dữ liệu: Theo khoản 1 Điều 33 Nghị định số 169/2025/NĐ-CP của Chính phủ thì 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.

Như vậy, Điều 33 Nghị định số 169/2025/NĐ-CP quy định về hoạt động cung cấp sản phẩm, dịch vụ dữ liệu lên sàn dữ liệu để giao dịch, trong đó nhấn mạnh nguyên tắc thị trường làm nền tảng cho các giao dịch dữ liệu. Tổ chức, cá nhân có quyền định giá sản phẩm dữ liệu thông qua các tổ chức định giá hợp pháp hoặc tổ chức vận hành sàn. Đối với cơ quan nhà nước, việc cung cấp dữ liệu phải tuân theo quy định về phí, giá của pháp luật, và có thể thực hiện đấu giá với giá khởi điểm không thấp hơn chi phí đầu vào. Các sản phẩm, dịch vụ dữ liệu giao dịch trên sàn phải bảo đảm tính xác thực về nguồn gốc. Việc xác thực này là trách nhiệm của tổ chức cung cấp dịch vụ sàn hoặc đơn vị chuyên môn có chức năng xác thực. Tổ chức, cá nhân đưa sản phẩm lên sàn phải chịu trách nhiệm pháp lý về nội dung dữ liệu; đồng thời, đơn vị vận hành sàn có nghĩa vụ thẩm định sản phẩm để bảo đảm tính tuân thủ pháp luật. Nghị định cũng quy định rõ việc bắt buộc thực hiện giao dịch dữ liệu thông qua sàn đối với các tổ chức, doanh nghiệp, trừ trường hợp có quy định pháp luật khác. Một số loại dữ liệu bị cấm giao dịch trên sàn gồm: dữ liệu cốt lõi, dữ liệu quan trọng; dữ liệu chưa được sự đồng ý của chủ thể; và các loại dữ liệu bị cấm theo quy định pháp luật hiện hành.

Ngoài ra, việc cung cấp, mua, bán hoặc các giao dịch liên quan đến sản phẩm, dịch vụ về dữ liệu được thực hiện trên nền tảng Sàn dữ liệu cũng được quy định rất chi tiết trong Nghị định 169/2025/NĐ-CP, cụ thể như sau:

- Về các điều kiện cần thiết để tổ chức được cấp giấy chứng nhận đủ điều kiện kinh doanh hoạt động dữ liệu:

Điều 34 Nghị định 169/2025/NĐ-CP nêu các điều kiện cần thiết để tổ chức được cấp giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn dữ liệu. Tổ chức này phải là đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước được thành lập và hoạt động hợp pháp tại Việt Nam. Người đứng đầu tổ chức phải có bằng đại học, có ít nhất ba năm kinh nghiệm trong lĩnh vực quản lý dữ liệu và không vi phạm các điều kiện loại trừ theo quy định. Về nhân sự, tổ chức cần có tối thiểu năm người có trình độ đại học, trong đó ít nhất 40% làm việc chính thức và 30% có chứng chỉ chuyên ngành liên quan đến dữ liệu, thẩm định, xúc tiến thương mại hoặc quản trị tài sản. Đây là yêu cầu nhằm bảo đảm đội ngũ có đủ năng lực chuyên môn trong hoạt động vận hành sàn dữ liệu. Tổ chức cần có cơ sở vật chất, thiết bị kỹ thuật đặt tại Việt Nam, được kiểm định an toàn thông tin, cùng với một đề án hoạt động chi tiết. Đề án này bao gồm các nội dung về hệ thống công nghệ thông tin, bảo mật, quy trình thanh toán, thẩm định dữ liệu, định danh điện tử, phòng cháy chữa cháy và đảm bảo vận hành ổn định. Trường hợp tổ chức có hoạt động đấu giá dữ liệu thì cần có giấy phép đấu giá tài sản theo quy định của pháp luật.

- Về trách nhiệm của tổ chức cung cấp dịch vụ sàn dữ liệu:

Điều 35 Nghị định 169/2025/NĐ-CP quy định rõ trách nhiệm của tổ chức cung cấp dịch vụ sàn dữ liệu nhằm đảm bảo hoạt động sàn được thực hiện minh bạch, an toàn và tuân thủ pháp luật. Trước hết, tổ chức này có trách nhiệm kiểm tra và đánh giá điều kiện tham gia sàn của các chủ thể liên quan, bao gồm năng lực pháp lý của cá nhân và tổ chức, tính hợp pháp và điều kiện lưu hành của sản phẩm, dịch vụ dữ liệu cũng như khả năng đáp ứng yêu cầu an ninh, an toàn trong quá trình sử dụng. Tổ chức vận hành sàn phải giám sát hoạt động trên sàn, có quyền đình chỉ hoặc chấm dứt niêm yết sản phẩm, xử lý vi

phạm, giải quyết tranh chấp và phối hợp với cơ quan nhà nước trong công tác thanh tra, điều tra khi cần thiết. Họ còn phải ban hành quy chế hoạt động của sàn, công khai trên trang thông tin điện tử và quy định rõ quy trình giao dịch, trách nhiệm của các bên, điều kiện bảo mật thông tin và cơ chế xử lý rủi ro. Để đảm bảo an toàn giao dịch, sàn dữ liệu phải xây dựng hệ thống kỹ thuật đáp ứng các yêu cầu pháp luật, đồng thời hướng dẫn người dùng thực hiện bảo vệ dữ liệu, quyền riêng tư và bí mật thương mại. Cùng với đó, tổ chức này phải xây dựng phương án ứng phó khẩn cấp đối với sự cố an toàn dữ liệu, thực hiện sao lưu và diễn tập định kỳ để tăng cường khả năng phục hồi hệ thống. Họ cũng phải đảm bảo duy trì dịch vụ liên tục 24/7 và tuân thủ các quy trình hoạt động đã được phê duyệt. Đơn vị cung cấp dịch vụ sàn dữ liệu cần xây dựng bộ tiêu chí kỹ thuật đánh giá chất lượng sản phẩm, hệ thống chỉ số tài sản dữ liệu và công cụ hỗ trợ định giá dữ liệu. Họ có trách nhiệm báo cáo định kỳ 6 tháng và 1 năm về tình hình cung cấp dịch vụ sàn dữ liệu theo mẫu quy định, gửi về Bộ Công an *(qua Trung tâm dữ liệu quốc gia)* đúng thời hạn hoặc khi có yêu cầu.

6. Các hành vi bị nghiêm cấm

- Khoản 3 của Điều 42 Luật Dữ liệu 2024 liệt kê những loại dữ liệu không được phép giao dịch trên sàn, nhằm thiết lập ranh giới pháp lý, đạo đức và an ninh. Đó là:

+ Dữ liệu gây nguy hại đến quốc phòng, an ninh, đối ngoại, cơ yếu, bởi đây là những loại dữ liệu có khả năng làm lộ bí mật quốc gia hoặc bị lợi dụng gây mất ổn định chính trị – xã hội;

+ Dữ liệu chưa được sự đồng ý của chủ thể dữ liệu, trừ khi pháp luật có quy định đặc biệt khác;

+ Dữ liệu khác bị cấm giao dịch theo quy định của pháp luật.

Quy định này nhằm bảo vệ quyền riêng tư, quyền kiểm soát thông tin cá nhân của công dân, phù hợp với xu thế bảo vệ dữ liệu cá nhân toàn cầu; Các loại dữ liệu bị cấm giao dịch theo pháp luật, bao gồm dữ liệu liên quan đến hoạt động tội phạm, dữ liệu giả mạo, sai sự thật, dữ liệu vi phạm đạo đức xã hội...

- Khoản 6 Điều 33 Nghị định 169/2025/NĐ-CP bổ sung thêm quy định dữ liệu không được phép giao dịch, gồm:

+ Dữ liệu thuộc danh mục dữ liệu cốt lõi, dữ liệu quan trọng;

+ Dữ liệu không được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác;

+ Dữ liệu khác bị cấm giao dịch theo quy định của pháp luật.

7. Thẩm quyền, trình tự, thủ tục, hồ sơ hoạt động liên quan đến sản phẩm, dịch vụ dữ liệu

Theo quy định tại Điều 36, Bộ Công an là cơ quan có thẩm quyền cấp các loại Giấy chứng nhận liên quan đến hoạt động dữ liệu, bao gồm: Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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; và Giấy chứng nhận đủ điều kiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu. Ngoài ra, Bộ trưởng Bộ Công an có thể giao trách nhiệm cho cơ quan, đơn vị trực thuộc để thực hiện việc cấp các loại giấy chứng nhận này theo đúng quy định của pháp luật, nhằm bảo đảm hiệu lực quản lý nhà nước đối với các hoạt động dữ liệu có ảnh hưởng lớn đến an ninh, trật tự và phát triển kinh tế số.

Trung tâm dữ liệu quốc gia về dân cư. Ảnh: Hải Dương

Theo quy định tại Điều 37, tổ chức có nhu cầu cấp Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn dữ liệu, sản phẩm, dịch vụ trung gian dữ liệu, phân tích – tổng hợp dữ liệu hoặc cung cấp sản phẩm, dịch vụ phân tích – tổng hợp dữ liệu phải nộp một bộ hồ sơ gồm tờ khai theo mẫu tương ứng (TK01 đến TK04 tại Phụ lục kèm theo Nghị định) và các tài liệu chứng minh đáp ứng điều kiện quy định tại các Điều 25, 29 và 34 của Nghị định, trừ trường hợp đề nghị cấp Giấy chứng nhận cung cấp sản phẩm, dịch vụ phân tích – tổng hợp dữ liệu thì không cần chứng minh điều kiện như trên. Hồ sơ

được nộp trực tiếp, trực tuyến hoặc qua dịch vụ bưu chính đến cơ quan có thẩm quyền. Trong vòng 5 ngày làm việc kể từ ngày nhận được đầy đủ hồ sơ hợp lệ, cơ quan này sẽ lấy ý kiến của các đơn vị, tổ chức, cá nhân liên quan; sau đó, trong vòng 10 ngày, các đơn vị được lấy ý kiến có trách nhiệm phản hồi bằng văn bản. Kể từ thời điểm nhận đầy đủ các ý kiến này, trong vòng 5 ngày làm việc tiếp theo, cơ quan có thẩm quyền được quy định tại Điều 36 Nghị định sẽ xem xét và quyết định cấp Giấy chứng nhận dưới dạng bản giấy và bản điện tử theo mẫu GCN01 đến GCN04 tương ứng, hoặc ra văn bản từ chối nêu rõ lý do không cấp nếu không đủ điều kiện.

Theo Điều 38 về việc cấp lại, cấp đổi Giấy chứng nhận đủ điều kiện kinh doanh trong các lĩnh vực dữ liệu được quy định tại Nghị định: Trong trường hợp bị mất hoặc bị hỏng bản giấy của Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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; hoặc Giấy chứng nhận đủ điều kiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu, tổ chức có nhu cầu được phép nộp tờ khai theo mẫu tương ứng (TK05 đến TK08 theo từng loại Giấy chứng nhận) và gửi đến cơ quan có thẩm quyền thông qua một trong các phương thức: nộp trực tiếp, trực tuyến hoặc qua dịch vụ bưu chính. Trong vòng 5 ngày làm việc kể từ khi nhận đủ hồ sơ hợp lệ, cơ quan có thẩm quyền phải xem xét, quyết định cấp lại Giấy chứng nhận theo đúng mẫu đã được ban hành kèm theo Nghị định; nếu từ chối cấp lại thì phải nêu rõ lý do bằng văn bản gửi cho tổ chức đề nghị. Trường hợp cấp đổi Giấy chứng nhận được thực hiện khi có sai thông tin hoặc có sự thay đổi nội dung trên Giấy chứng nhận đã cấp (bao gồm phương án, quy trình hoạt động của sàn dữ liệu hoặc kinh doanh sản phẩm, dịch vụ dữ liệu theo Điều 25, 29, 34 của Nghị định), tổ chức phải nộp 01 bộ hồ sơ bao gồm: Tờ khai

đề nghị cấp đổi theo đúng mẫu TK tương ứng, kèm theo các giấy tờ, tài liệu chứng minh nội dung sai sót hoặc thay đổi. Sau khi tiếp nhận hồ sơ theo một trong ba phương thức nói trên, cơ quan có thẩm quyền sẽ lấy ý kiến các đơn vị có liên quan trong thời hạn 5 ngày làm việc. Các đơn vị được lấy ý kiến có trách nhiệm trả lời bằng văn bản trong vòng 10 ngày kể từ ngày nhận được văn bản đề nghị. Sau khi nhận đầy đủ ý kiến từ các đơn vị có liên quan, người có thẩm quyền được quy định tại Điều 36 của Nghị định có trách nhiệm xem xét, quyết định cấp đổi bản giấy và bản điện tử Giấy chứng nhận trong thời hạn 5 ngày làm việc, với mẫu tương ứng theo từng loại hình hoạt động dữ liệu. Trường hợp không cấp đổi thì cũng phải có văn bản thông báo rõ lý do từ chối. Việc cấp lại hoặc cấp đổi bảo đảm nguyên tắc công khai, minh bạch, đúng quy trình, tạo thuận lợi cho tổ chức hoạt động trong lĩnh vực dữ liệu, đồng thời tuân thủ các yêu cầu về an ninh, an toàn và bảo mật thông tin theo quy định pháp luật.

Điều 39 về Thu hồi Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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 quy định như sau: Việc thu hồi Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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 được thực hiện trong các trường hợp cụ thể sau: tổ chức cung cấp dịch vụ không hoạt động liên tục trong thời gian từ 6 tháng trở lên; bị giải thể hoặc phá sản theo quy định của pháp luật; hoặc không khắc phục các vi phạm liên quan đến bảo vệ dữ liệu cá nhân, an toàn thông

tin, an ninh mạng, an ninh dữ liệu theo yêu cầu của cơ quan nhà nước có thẩm quyền. Người có thẩm quyền theo quy định tại Điều 36 của Nghị định sẽ ban hành Quyết định thu hồi Giấy chứng nhận theo các mẫu QĐ01 đến QĐ04 tại Phụ lục kèm theo. Sau khi có quyết định thu hồi, tổ chức bị thu hồi Giấy chứng nhận có trách nhiệm nộp lại bản giấy Giấy chứng nhận đã được cấp cho cơ quan có thẩm quyền trong vòng 5 ngày làm việc kể từ ngày nhận được quyết định. Đồng thời, cơ quan có thẩm quyền cũng sẽ thực hiện thu hồi bản điện tử của Giấy chứng nhận và công bố thông tin thu hồi trên Hệ thống thông tin hoặc Trang thông tin điện tử của cơ quan mình, bảo đảm công khai, minh bạch, kịp thời, tránh các hoạt động kinh doanh trái phép tiếp diễn sau thu hồi.

8. Trách nhiệm quản lý nhà nước về sản phẩm, dịch vụ về dữ liệu

Theo Điều 40 Nghị định 169/2025/NĐ-CP, Bộ Công an chịu trách nhiệm quản lý nhà nước đối với sản phẩm, dịch vụ về dữ liệu thông qua các nhiệm vụ chủ yếu sau: chủ trì phối hợp với các bộ, ngành tổ chức thực hiện hoạt động quản lý, hợp tác quốc tế, hỗ trợ hệ sinh thái khởi nghiệp đổi mới sáng tạo trong lĩnh vực dữ liệu; phổ biến, tuyên truyền pháp luật liên quan; tổ chức cấp, cấp đổi, cấp lại và thu hồi Giấy chứng nhận đủ điều kiện kinh doanh các loại sản phẩm, dịch vụ về dữ liệu; kiểm tra, giám sát, xử lý vi phạm và kiến nghị hoàn thiện chính sách, pháp luật trong lĩnh vực sản phẩm, dịch vụ về dữ liệu.

Xây dựng Trung tâm dữ liệu quốc gia theo các tiêu chuẩn quốc gia và quốc tế, phù hợp với xu thế và xứng tầm thế giới.

Ảnh minh họa. Nguồn: TTXVN

Theo Điều 41 Nghị định 169/2025/NĐ-CP, trách nhiệm quản lý nhà nước về *sản phẩm, dịch vụ về dữ liệu* được phân công cho các bộ ngành như sau:

Bộ Quốc phòng chịu trách nhiệm phổ biến pháp luật, cấp và giám sát các Giấy chứng nhận thử nghiệm có kiểm soát trong lĩnh vực dữ liệu quốc phòng, kiểm tra và phối hợp với Bộ Công an trong việc quản lý hoạt động kinh doanh, cung cấp sản phẩm, dịch vụ dữ liệu, bao gồm trung gian, phân tích, tổng hợp và sàn dữ liệu; đồng thời đề xuất hoàn thiện chính sách pháp luật liên quan.

Bộ Khoa học và Công nghệ phối hợp với các bộ ngành khác đào tạo nhân lực dữ liệu, kiểm tra và giám sát các hoạt động thử nghiệm có kiểm soát cũng như hoạt động kinh doanh sản phẩm, dịch vụ dữ liệu. Bộ này cũng có trách nhiệm kiến nghị sửa đổi chính sách về khoa học, công nghệ và đổi mới sáng tạo liên quan đến dữ liệu.

Bộ Tài chính thực hiện hợp tác quốc tế, phối hợp kiểm tra, giám sát và đề xuất hoàn thiện khung pháp lý về sản phẩm, dịch vụ dữ liệu trong phạm vi chức năng được giao, nhất là trong hoạt động kinh doanh và thử nghiệm có kiểm soát.

Bộ Giáo dục và Đào tạo chủ trì xây dựng đề án đào tạo nhân lực chất lượng cao về dữ liệu, triển khai chính sách hỗ trợ học sinh – sinh viên trong các ngành công nghệ thông tin, khoa học dữ liệu, trí tuệ nhân tạo; đồng thời phối hợp giám sát và kiến nghị hoàn thiện chính sách pháp luật trong lĩnh vực giáo dục liên quan đến sản phẩm, dịch vụ về dữ liệu.

Theo Điều 42 Nghị định 169/2025/NĐ-CP, các bộ khác, cơ quan ngang bộ, cơ quan thuộc Chính phủ và UBND các tỉnh, thành phố trực thuộc Trung ương có trách nhiệm quản lý nhà nước về sản phẩm, dịch vụ về dữ liệu trong phạm vi thẩm quyền. Cụ thể, các cơ quan này thực hiện hợp tác quốc tế, phổ biến pháp luật, hướng dẫn và cấp các giấy chứng nhận liên quan đến hoạt động thử nghiệm có kiểm soát, kiểm tra và giám sát hoạt động nghiên cứu, ứng dụng dữ liệu tại địa bàn quản lý. Đồng thời, họ phối hợp với Bộ Công an trong việc thanh tra, giải quyết vi phạm trong hoạt động kinh doanh sản phẩm,

dịch vụ dữ liệu (gồm trung gian, phân tích, tổng hợp và sàn dữ liệu). Các đơn vị có trách nhiệm kiến nghị sửa đổi, bổ sung văn bản pháp luật liên quan và tổ chức tiếp nhận, chuyển hồ sơ cấp giấy chứng nhận đủ điều kiện kinh doanh sản phẩm, dịch vụ dữ liệu đến cơ quan có thẩm quyền để xem xét cấp phép.

II. CÁC GIẢI PHÁP BẢO ĐẢM AN NINH DỮ LIỆU, AN TOÀN DỮ LIỆU TRONG ỨNG DỤNG CÁC SẢN PHẨM, DỊCH VỤ VỀ DỮ LIỆU

1. Nguy cơ khi ứng dụng các sản phẩm, dịch vụ về dữ liệu gây mất an toàn, trật tự xã hội

Hiện nay, trong quá trình ứng dụng các sản phẩm, dịch vụ về dữ liệu vào hoạt động của cơ quan nhà nước, doanh nghiệp và đời sống xã hội, vẫn còn tồn tại nhiều lỗ hổng nghiêm trọng trong công tác bảo đảm an ninh, an toàn dữ liệu. Trước hết, hệ thống pháp luật liên quan đến an ninh dữ liệu còn chưa hoàn thiện, thiếu tính thống nhất, đồng bộ và chưa bao quát hết các tình huống, rủi ro có thể xảy ra. Việc phân tán các quy định trong nhiều văn bản, cũng như thiếu một đạo luật chuyên biệt về bảo vệ dữ liệu cá nhân, khiến cho việc áp dụng thực tiễn gặp nhiều khó khăn, đặc biệt là trong xác định trách nhiệm khi xảy ra vi phạm hoặc sự cố lộ lọt dữ liệu. Một số quy định hiện hành vẫn còn mang tính nguyên tắc chung, chưa có hướng dẫn chi tiết, chưa xác định rõ cơ chế kiểm soát nội bộ và trách nhiệm của từng chủ thể trong chuỗi cung ứng dữ liệu.

Cơ quan An ninh điều tra Công an thành phố Huế tống đạt quyết định khởi tố vụ án, khởi tố bị can và bắt tạm giam các đối tượng trong đường dây mua bán gần 56 triệu thông tin dữ liệu cá nhân. Ảnh minh họa. Nguồn từ Internet.

Bên cạnh đó, hạ tầng kỹ thuật phục vụ bảo đảm an toàn, an ninh dữ liệu còn yếu, thiếu đầu tư bài bản và chưa theo kịp tốc độ phát triển của công nghệ số. Nhiều hệ thống thông tin trọng yếu chưa được thiết lập hệ thống bảo mật đa tầng, chưa có khả năng tự động phát hiện, phản ứng hoặc phục hồi sau sự cố. Các cơ sở dữ liệu quốc gia, chuyên ngành mặc dù đã được triển khai nhưng việc kết nối, chia sẻ, khai thác còn rời rạc, chưa có cơ chế xác thực và kiểm soát truy cập hiệu quả, dẫn đến nguy cơ rò rỉ

dữ liệu từ bên trong. Hơn nữa, hiện tượng sử dụng phần mềm mã nguồn mở không rõ nguồn gốc hoặc hệ thống chưa được cập nhật bản vá lỗ hổng bảo mật kịp thời vẫn diễn ra ở nhiều đơn vị, trở thành điểm yếu để tin tặc tấn công khai thác.

Một trong những vấn đề đáng lo ngại khác là nhận thức và năng lực bảo vệ dữ liệu của một bộ phận cán bộ, công chức, viên chức, người lao động và người dùng còn hạn chế. Nhiều người chưa được đào tạo bài bản về kỹ năng nhận diện rủi ro và xử lý các tình huống liên quan đến an toàn thông tin, dẫn đến sơ suất trong sử dụng mật khẩu yếu, chia sẻ dữ liệu không kiểm soát, truy cập trái phép vào hệ thống. Thậm chí, có trường hợp cán bộ trong cơ quan nhà nước vô tình hoặc cố ý chia sẻ thông tin nội bộ ra bên ngoài mà không bị phát hiện và xử lý kịp thời. Đáng chú ý, trong khi trình độ tấn công mạng của tội phạm ngày càng tinh vi, thì biện pháp phòng thủ của nhiều tổ chức, cá nhân lại lạc hậu, thiếu cập nhật.

Cuối cùng, sự thiếu hụt trong hợp tác quốc tế về bảo vệ dữ liệu cũng là một khoảng trống cần được lấp đầy. Trong bối cảnh dữ liệu xuyên biên giới trở thành xu thế tất yếu, Việt Nam chưa có đủ thỏa thuận song phương, đa phương để chia sẻ thông tin, đồng bộ quy chuẩn bảo mật hay phối hợp xử lý sự cố mạng. Điều này làm giảm khả năng chủ động trong ứng phó với các cuộc tấn công mạng quy mô lớn, có yếu tố nước ngoài. Vì vậy, việc nhận diện đầy đủ và kịp thời các lỗ hổng trong bảo đảm an toàn, an ninh dữ liệu chính là tiền đề để hoàn thiện hành lang pháp lý, nâng cao năng lực tổ chức và ứng dụng công nghệ bảo mật, qua đó bảo vệ lợi ích của Nhà nước, tổ chức, doanh nghiệp và cá nhân trong thời đại số.

Để khắc phục những tồn tại, hạn chế trong bảo đảm an ninh, an toàn dữ liệu khi ứng dụng các sản phẩm, dịch vụ dữ liệu, cần tiếp tục hoàn thiện khuôn khổ pháp lý theo hướng đồng bộ, thống nhất, phù hợp với tốc độ phát triển của công nghệ số và yêu cầu bảo vệ dữ liệu cá nhân, dữ liệu quan trọng quốc gia. Trước hết, cần rà soát, sửa đổi, bổ sung và ban hành mới

các văn bản quy phạm pháp luật liên quan đến an ninh mạng, an toàn thông tin, bảo vệ dữ liệu cá nhân và dữ liệu chuyên ngành, đảm bảo không chồng chéo, mâu thuẫn và tạo hành lang pháp lý rõ ràng, minh bạch cho các hoạt động thu thập, xử lý, khai thác và cung cấp sản phẩm, dịch vụ dữ liệu. Đồng thời, cần tăng cường năng lực của các cơ quan quản lý nhà nước trong việc kiểm tra, giám sát, đánh giá rủi ro an ninh dữ liệu và xử lý nghiêm các hành vi vi phạm.

Cùng với đó, việc đầu tư, phát triển hạ tầng kỹ thuật bảo mật hiện đại, áp dụng các công nghệ mới như blockchain, trí tuệ nhân tạo, điện toán đám mây… để mã hóa, giám sát, phát hiện sớm và ngăn chặn các cuộc tấn công mạng, rò rỉ thông tin cũng là yêu cầu cấp thiết. Các cơ quan, tổ chức cung cấp sản phẩm, dịch vụ dữ liệu cần xây dựng quy trình bảo mật nội bộ chặt chẽ, phân quyền truy cập rõ ràng, thường xuyên đánh giá, kiểm tra hệ thống bảo mật. Người dùng cũng cần được tuyên truyền, phổ biến kiến thức về an toàn dữ liệu, nâng cao nhận thức và kỹ năng phòng vệ trên môi trường số.

Bên cạnh đó, cần có chính sách đào tạo, phát triển nguồn nhân lực chất lượng cao trong lĩnh vực an ninh mạng và bảo mật dữ liệu, đáp ứng yêu cầu thực tiễn trong quản lý và vận hành các hệ thống dữ liệu lớn, đặc biệt là các cơ sở dữ liệu quốc gia. Việc tăng cường hợp tác quốc tế trong chia sẻ thông tin, kinh nghiệm và công nghệ về bảo mật dữ liệu cũng cần được quan tâm nhằm thích ứng với các thách thức xuyên biên giới. Chỉ khi kết hợp đồng bộ giữa thể chế, công nghệ, tổ chức và con người thì mới có thể từng bước khắc phục những lỗ hổng còn tồn tại và bảo đảm an toàn, an ninh dữ liệu một cách hiệu quả, bền vững trong kỷ nguyên số.

2. Các giải pháp bảo đảm an ninh dữ liệu, an toàn dữ liệu

2.1. Nhóm 1: Biện pháp kiểm tra giám sát an toàn dữ liệu, bảo mật dữ liệu và biện pháp giám sát hành vi có thể gây ảnh hưởng đến việc bảo vệ dữ liệu

2.1.1. Biện pháp kiểm tra giám sát an toàn dữ liệu, bảo mật dữ liệu

2.1.1.1. Nhà nước

(1) Xây dựng 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 quy định tại Nghị định 169/2025/NĐ-CP các cá nhân, tổ chức hoạt động kinh doanh sản phẩm, dịch vụ dữ liệu phải thực hiện đầy đủ trình tự thủ tục, hồ sơ, như sau:

Theo quy định tại Điều 37 Nghị định 169/2025/NĐ-CP, tổ chức có nhu cầu cấp Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn dữ liệu, sản phẩm, dịch vụ trung gian dữ liệu, phân tích – tổng hợp dữ liệu hoặc cung cấp sản phẩm, dịch vụ phân tích – tổng hợp dữ liệu phải nộp một bộ hồ sơ gồm tờ khai theo mẫu tương ứng *(TK01 đến TK04 tại Phụ lục kèm theo Nghị định)* và các tài liệu chứng minh đáp ứng điều kiện quy định tại các Điều 25, 29 và 34 của Nghị định, trừ trường hợp đề nghị cấp Giấy chứng nhận cung cấp sản phẩm, dịch vụ phân tích – tổng hợp dữ liệu thì không cần chứng minh điều kiện như trên. Hồ sơ được nộp trực tiếp, trực tuyến hoặc qua dịch vụ bưu chính đến cơ quan có thẩm quyền. Trong vòng 5 ngày làm việc kể từ ngày nhận được đầy đủ hồ sơ hợp lệ, cơ quan này sẽ lấy ý kiến của các đơn vị, tổ chức, cá nhân liên quan; sau đó, trong vòng 10 ngày, các đơn vị được lấy ý kiến có trách nhiệm phản hồi bằng văn bản. Kể từ thời điểm nhận đầy đủ

các ý kiến này, trong vòng 5 ngày làm việc tiếp theo, cơ quan có thẩm quyền được quy định tại Điều 36 Nghị định sẽ xem xét và quyết định cấp Giấy chứng nhận dưới dạng bản giấy và bản điện tử theo mẫu GCN01 đến GCN04 tương ứng, hoặc ra văn bản từ chối nêu rõ lý do không cấp nếu không đủ điều kiện.

Theo Điều 38 Nghị định 169/2025/NĐ-CP về việc cấp lại, cấp đổi Giấy chứng nhận đủ điều kiện kinh doanh trong các lĩnh vực dữ liệu được quy định tại Nghị định: Trong trường hợp bị mất hoặc bị hỏng bản giấy của Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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; hoặc Giấy chứng nhận đủ điều kiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu, tổ chức có nhu cầu được phép nộp tờ khai theo mẫu tương ứng *(TK05 đến TK08 theo từng loại Giấy chứng nhận)* và gửi đến cơ quan có thẩm quyền thông qua một trong các phương thức: nộp trực tiếp, trực tuyến hoặc qua dịch vụ bưu chính. Trong vòng 5 ngày làm việc kể từ khi nhận đủ hồ sơ hợp lệ, cơ quan có thẩm quyền phải xem xét, quyết định cấp lại Giấy chứng nhận theo đúng mẫu đã được ban hành kèm theo Nghị định; nếu từ chối cấp lại thì phải nêu rõ lý do bằng văn bản gửi cho tổ chức đề nghị. Trường hợp cấp đổi Giấy chứng nhận được thực hiện khi có sai thông tin hoặc có sự thay đổi nội dung trên Giấy chứng nhận đã cấp *(bao gồm phương án, quy trình hoạt động của sàn dữ liệu hoặc kinh doanh sản phẩm, dịch vụ dữ liệu theo Điều 25, 29, 34 của Nghị định 169/2025/NĐ-CP)*, tổ chức phải nộp 01 bộ hồ sơ bao gồm: Tờ khai đề nghị cấp đổi theo đúng mẫu TK tương ứng, kèm theo các giấy tờ, tài liệu chứng minh nội dung sai sót hoặc thay đổi. Sau khi tiếp nhận hồ sơ theo một trong ba phương thức nói trên, cơ quan có thẩm quyền sẽ lấy ý kiến các đơn vị có liên quan trong thời hạn 5 ngày làm việc. Các đơn vị được lấy ý kiến có trách nhiệm trả lời bằng văn bản

trong vòng 10 ngày kể từ ngày nhận được văn bản đề nghị. Sau khi nhận đầy đủ ý kiến từ các đơn vị có liên quan, người có thẩm quyền được quy định tại Điều 36 của Nghị định có trách nhiệm xem xét, quyết định cấp đổi bản giấy và bản điện tử Giấy chứng nhận trong thời hạn 5 ngày làm việc, với mẫu tương ứng theo từng loại hình hoạt động dữ liệu. Trường hợp không cấp đổi thì cũng phải có văn bản thông báo rõ lý do từ chối. Việc cấp lại hoặc cấp đổi bảo đảm nguyên tắc công khai, minh bạch, đúng quy trình, tạo thuận lợi cho tổ chức hoạt động trong lĩnh vực dữ liệu, đồng thời tuân thủ các yêu cầu về an ninh, an toàn và bảo mật thông tin theo quy định pháp luật.

Điều 39 về Thu hồi Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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 quy định như sau: Việc thu hồi Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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 được thực hiện trong các trường hợp cụ thể sau: tổ chức cung cấp dịch vụ không hoạt động liên tục trong thời gian từ 6 tháng trở lên; bị giải thể hoặc phá sản theo quy định của pháp luật; hoặc không khắc phục các vi phạm liên quan đến bảo vệ dữ liệu cá nhân, an toàn thông tin, an ninh mạng, an ninh dữ liệu theo yêu cầu của cơ quan nhà nước có thẩm quyền. Người có thẩm quyền theo quy định tại Điều 36 của Nghị định sẽ ban hành Quyết định thu hồi Giấy chứng nhận theo các mẫu QĐ01 đến QĐ04 tại Phụ lục kèm theo. Sau khi có quyết định thu hồi, tổ chức bị thu hồi Giấy chứng nhận có trách nhiệm nộp lại bản giấy Giấy chứng nhận

đã được cấp cho cơ quan có thẩm quyền trong vòng 5 ngày làm việc kể từ ngày nhận được quyết định. Đồng thời, cơ quan có thẩm quyền cũng sẽ thực hiện thu hồi bản điện tử của Giấy chứng nhận và công bố thông tin thu hồi trên Hệ thống thông tin hoặc Trang thông tin điện tử của cơ quan mình, bảo đảm công khai, minh bạch, kịp thời, tránh các hoạt động kinh doanh trái phép tiếp diễn sau thu hồi.

* Về thẩm quyền cấp các loại Giấy chứng nhận liên quan đến hoạt động dữ liệu:

Theo quy định tại Điều 36 Nghị định 169/2025/NĐ-CP, Bộ Công an là cơ quan có thẩm quyền cấp các loại Giấy chứng nhận liên quan đến hoạt động dữ liệu, bao gồm: Giấy chứng nhận đủ điều kiện kinh doanh hoạt động sàn 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; và Giấy chứng nhận đủ điều kiện cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu. Ngoài ra, Bộ trưởng Bộ Công an có thể giao trách nhiệm cho cơ quan, đơn vị trực thuộc để thực hiện việc cấp các loại giấy chứng nhận này theo đúng quy định của pháp luật, nhằm bảo đảm hiệu lực quản lý nhà nước đối với các hoạt động dữ liệu có ảnh hưởng lớn đến an ninh, trật tự và phát triển kinh tế số.

Trung tâm dữ liệu quốc gia về dân cư. Ảnh: Hải Dương

(2) Bộ Công an chủ trì, phối hợp với các bộ, ngành thực hiện công tác kiểm tra, giám sát, giải quyết khiếu nại, tố cáo, phòng ngừa, phát hiện, xử lý vi phạm liên quan đến hoạt động thử nghiệm có kiểm soát, kinh doanh hoạt động sàn dữ liệu, kinh doanh sản phẩm, dịch vụ trung gian dữ liệu, kinh doanh, cung cấp sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu, cụ thể:

Khoản 4 Điều 40 Nghị định số 169/2025/NĐ-CP của Chính phủ quy định về trách nhiệm của Bộ Công an như sau: Bộ Công an có trách nhiệm chủ trì phối hợp với các bộ, ngành kiểm tra, giám sát, giải quyết khiếu nại, tố cáo, phòng ngừa, phát hiện và xử lý vi phạm liên quan đến hoạt động thử nghiệm có kiểm soát, hoạt động sàn dữ liệu, kinh doanh, cung cấp dịch vụ trung gian, phân tích, tổng hợp dữ liệu theo đúng thẩm quyền. Bộ ban hành hoặc kiến nghị sửa đổi, bổ sung, hoàn thiện văn bản pháp luật trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ dữ liệu theo phạm vi được giao.

Tại Điều 41 Nghị định 169/2025/NĐ-CP của Chính phủ quy định về trách nhiệm của Bộ Quốc phòng, Bộ Khoa học và Công nghệ, Bộ Tài chính, Bộ Giáo dục và Đào tạo, nêu rõ: **Bộ Quốc phòng** thực hiện hợp tác quốc tế, tuyên truyền pháp luật, hướng dẫn và tổ chức cấp Giấy chứng nhận thử nghiệm có kiểm soát, **kiểm tra giám sát hoạt động nghiên cứu, sử dụng dữ liệu trong lĩnh vực quốc phòng**, đồng thời phối hợp với Bộ Công an trong xử lý vi phạm liên quan đến kinh doanh, cung cấp dịch vụ dữ liệu, ban hành và kiến nghị hoàn thiện văn bản pháp luật chuyên ngành. **Bộ Khoa học và Công nghệ** thực hiện hợp tác quốc tế về khoa học, công nghệ và đổi mới sáng tạo về dữ liệu; phối hợp với Bộ Công an, Bộ Giáo dục và Đào tạo xây dựng chương trình đào tạo, đào tạo nguồn nhân lực; **phối hợp kiểm tra, giám sát và xử lý vi phạm trong các hoạt động liên quan đến thử nghiệm, sàn dữ liệu và dịch vụ dữ liệu**; đề xuất hoàn thiện văn bản quy phạm pháp luật. **Bộ Tài chính** thực hiện hợp tác quốc tế trong phạm vi được giao; **phối hợp kiểm tra, xử lý vi phạm các hoạt động dữ liệu**; đề xuất sửa đổi, bổ sung văn bản pháp luật liên quan đến khoa học, công nghệ và dịch vụ dữ liệu. **Bộ Giáo dục và Đào tạo** thực hiện hợp tác quốc tế về giáo dục, đào tạo trong lĩnh vực dữ liệu; chủ trì phối hợp xây dựng đề án đào tạo nguồn nhân lực chất lượng cao phục vụ phát triển khoa học, công nghệ và đổi mới sáng tạo về dữ liệu; chủ trì phối hợp xây dựng chính sách học bổng, học phí và hợp tác công tư trong đào tạo lĩnh vực công nghệ thông tin, an ninh mạng, khoa học dữ liệu và trí tuệ nhân tạo;

phối hợp kiểm tra, giám sát các hoạt động thử nghiệm và kinh doanh dữ liệu; đề xuất hoàn thiện văn bản quy phạm pháp luật trong giáo dục và lĩnh vực liên quan đến dữ liệu.

Điều 42 Nghị định số 169/2025/NĐ-CP quy định về trách nhiệm của các bộ khác, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương tiếp tục nêu: Các cơ quan này thực hiện hợp tác quốc tế về khoa học, công nghệ và đổi mới sáng tạo về dữ liệu trong phạm vi chức năng, nhiệm vụ, địa bàn được phân công. Các cơ quan có trách nhiệm tuyên truyền, phổ biến pháp luật chuyên ngành liên quan đến hoạt động khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ dữ liệu. Các cơ quan tổ chức cấp Giấy chứng nhận tham gia và kết thúc hoạt động thử nghiệm có kiểm soát, điều chỉnh, gia hạn thời gian thử nghiệm; kiểm tra giám sát hoạt động nghiên cứu, sử dụng dữ liệu trong phạm vi mình quản lý. ***Các cơ quan phối hợp với Bộ Công an thực hiện kiểm tra, giám sát, xử lý vi phạm liên quan đến hoạt động thử nghiệm, kinh doanh, cung cấp dữ liệu theo thẩm quyền. Các cơ quan đề xuất sửa đổi, bổ sung văn bản pháp luật trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ dữ liệu***. Các cơ quan chỉ đạo đơn vị trực thuộc lập biên bản tiếp nhận và chuyển hồ sơ cấp Giấy chứng nhận các loại gồm tham gia thử nghiệm, hoạt động sàn dữ liệu, dịch vụ trung gian dữ liệu, dịch vụ phân tích và tổng hợp dữ liệu đến cơ quan có thẩm quyền cấp phép.

(3) Bộ Quốc phòng thực hiện công tác kiểm tra, giám sát, giải quyết khiếu nại, tố cáo, phòng ngừa, phát hiện, xử lý vi phạm liên quan đến hoạt động thử nghiệm có kiểm soát về dữ liệu thuộc lĩnh vực quốc phòng, cơ yếu *(Điều 41 Nghị định số 169/2025/NĐ-CP)*.

(4) Quy định trách nhiệm, hành vi vi phạm và biện pháp xử lý đối với hành vi vi phạm an toàn dữ liệu, bảo mật dữ liệu

Trong kỷ nguyên số, dữ liệu cá nhân được coi là tài sản phi truyền thống và có liên quan chặt chẽ tới quyền con người, quyền công dân, an toàn, an ninh mạng, an ninh thông tin, an ninh dữ liệu, công nghệ thông tin… Thảo luận về dự án Luật Bảo vệ dữ liệu cá nhân, các đại biểu Quốc hội đề nghị, dự thảo Luật cần tăng cường quyền kiểm soát của người dân đối với dữ liệu cá nhân và quy định chế tài có tính răn đe cao đối với những hành vi xâm phạm.

Song song với thiết lập kỹ thuật, cần phát triển chính sách và quy trình giám sát rõ ràng, bao gồm quyền truy cập, quy định về bảo mật, phân quyền trách nhiệm và các hình thức xử lý vi phạm. Quy trình này phải bảo đảm tuân thủ pháp luật, tôn trọng quyền riêng tư cá nhân nhưng vẫn đủ khả năng phát hiện và ngăn chặn hành vi gây hại cho tổ chức. Cần thiết lập các bảng phân tích rủi ro, ma trận quyền truy cập, định nghĩa các hành vi bất thường cụ thể và cơ chế phản ứng thích hợp cho từng mức độ đe dọa.

Một yêu cầu quan trọng là xây dựng cơ chế kiểm tra định kỳ, kiểm toán và đánh giá hiệu quả hoạt động của hệ thống giám sát. Việc thực hiện các bài kiểm tra thâm nhập (penetration testing), mô phỏng tấn công có kiểm soát (red team/blue team), đánh giá bảo mật định kỳ sẽ giúp phát hiện sớm các lỗ hổng, điểm yếu trong hệ thống và nâng cao tính sẵn sàng đối phó với các cuộc tấn công thực tế. Các kết quả đánh giá cần được lưu trữ có hệ thống, phân tích xu hướng và dùng để cải tiến hoạt động giám sát theo thời gian.

Trong bối cảnh các mối đe dọa an ninh mạng không ngừng gia tăng cả về quy mô lẫn mức độ tinh vi, việc thiết lập hệ thống giám sát liên tục là yêu cầu bắt buộc trong mọi tổ chức hiện đại. Ngoài các yếu tố kỹ thuật, hệ thống giám sát cần gắn kết với chiến lược quản trị tổng thể của tổ chức, bảo đảm sự phối hợp giữa các bộ phận chức năng, từ công nghệ thông tin đến quản lý rủi ro và pháp chế, để tạo thành một hệ sinh thái phòng thủ chặt chẽ, chủ động và linh hoạt.

Đối với lực lượng Công an nhân dân, nhiệm vụ thiết lập hệ thống giám sát an ninh mạng có vai trò đặc biệt quan trọng trong công tác bảo vệ an ninh quốc gia, trật tự an toàn xã hội trong không gian mạng. Lực lượng Công an cần chủ động triển khai hệ thống giám sát tại các đơn vị chuyên trách về an ninh mạng, thu thập và phân tích thông tin từ nhiều nguồn, từ đó phát hiện và ngăn chặn kịp thời các hoạt động gián điệp mạng, phá hoại cơ sở hạ tầng trọng yếu, truyền bá thông tin xấu độc hoặc xâm phạm chủ quyền số quốc gia. Ngoài ra, lực lượng Công an cần tăng cường phối hợp với các cơ quan quản lý nhà nước, doanh nghiệp cung cấp dịch vụ số và cộng đồng nghiên cứu để hoàn thiện năng lực giám sát, đồng thời xây dựng các Trung tâm điều hành an ninh mạng cấp bộ, cấp tỉnh nhằm phát hiện sớm các mối nguy và tổ chức phản ứng nhanh, góp phần giữ vững ổn định chính trị, bảo vệ quyền và lợi ích chính đáng của người dân trong thời đại số.

Ngày 26/6/2025, tại Kỳ họp thứ 9, Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam đã chính thức thông qua Luật Bảo vệ dữ liệu cá nhân *(Luật số 91/2025/QH15)*. Trong đó, có một số quy định đáng chú ý như nghiêm cấm mua bán dữ liệu cá nhân; doanh nghiệp phải xóa dữ liệu cá nhân người lao động sau khi chấm dứt hợp đồng; mạng xã hội không được yêu cầu cung cấp hình ảnh, video chứa nội dung về giấy tờ tùy thân làm yếu tố xác thực..., theo đó:

*** Nghiêm cấm hành vi mua bán dữ liệu cá nhân:** Theo Điều 7 Luật Bảo vệ dữ liệu cá nhân quy định thì có 07 hành vi bị nghiêm cấm liên quan đến dữ liệu cá nhân, gồm:

- Xử lý dữ liệu cá nhân nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây ảnh hưởng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- Cản trở hoạt động bảo vệ dữ liệu cá nhân.

- Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để thực hiện hành vi vi phạm pháp luật.

- Xử lý dữ liệu cá nhân trái quy định của pháp luật.

- Sử dụng dữ liệu cá nhân của người khác, cho người khác sử dụng dữ liệu cá nhân của mình để thực hiện hành vi trái quy định của pháp luật.

- Mua, bán dữ liệu cá nhân, trừ trường hợp luật có quy định khác.

- Chiếm đoạt, cố ý làm lộ, làm mất dữ liệu cá nhân.

*** Phạt tối đa đến 5% doanh thu năm liền kề đối với hành vi xâm phạm dữ liệu cá nhân:** Theo khoản 4 Điều 8 của Luật quy định thì mức phạt tiền tối đa trong xử phạt vi phạm hành chính đối với tổ chức có hành vi vi phạm quy định chuyển dữ liệu cá nhân xuyên biên giới là 5% doanh thu của năm trước liền kề của tổ chức đó.

Trường hợp không có doanh thu của năm trước liền kề hoặc mức phạt tính theo doanh thu thấp hơn mức phạt tiền tối đa theo quy định tại khoản 5 Điều 8 thì áp dụng mức phạt tiền theo quy định tại khoản 5 Điều 8.

*** Doanh nghiệp phải xóa dữ liệu cá nhân người lao động sau khi chấm dứt hợp đồng:** Khoản 2 Điều 25 quy định về trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân trong quản lý, sử dụng người lao động. Theo đó, doanh nghiệp sau khi chấm dứt hợp đồng phải có trách nhiệm:

- Tuân thủ quy định của Luật này, pháp luật về lao động, việc làm, pháp luật về dữ liệu và quy định khác của pháp luật có liên quan;

- Dữ liệu cá nhân của người lao động phải lưu trữ trong thời hạn theo quy định của pháp luật hoặc theo thỏa thuận;

- Phải xóa, hủy dữ liệu cá nhân của người lao động khi chấm dứt hợp đồng, trừ trường hợp theo thỏa thuận hoặc pháp luật có quy định khác.

*** Mạng xã hội không được yêu cầu cung cấp hình ảnh, video chứa nội dung về giấy tờ tùy thân làm yếu tố xác thực:** Theo Điều 29 Luật Bảo vệ dữ liệu cá nhân thì tổ chức, cá nhân cung cấp dịch vụ mạng xã hội, dịch vụ truyền thông trực tuyến phải có trách nhiệm:

- Thông báo rõ ràng nội dung dữ liệu cá nhân thu thập khi chủ thể dữ liệu cá nhân cài đặt và sử dụng mạng xã hội, dịch vụ truyền thông trực tuyến; không thu thập trái phép dữ liệu cá nhân và ngoài phạm vi theo thỏa thuận với khách hàng.

- Không được yêu cầu cung cấp hình ảnh, video chứa nội dung đầy đủ hoặc một phần giấy tờ tùy thân làm yếu tố xác thực tài khoản.

- Cung cấp lựa chọn cho phép người dùng từ chối thu thập và chia sẻ tệp dữ liệu (gọi là cookies).

- Cung cấp lựa chọn "không theo dõi" hoặc chỉ được theo dõi hoạt động sử dụng mạng xã hội, dịch vụ truyền thông trực tuyến khi có sự đồng ý của người sử dụng.

- Không nghe lén, nghe trộm hoặc ghi âm cuộc gọi và đọc tin nhắn văn bản khi không có sự đồng ý của chủ thể dữ liệu cá nhân, trừ trường hợp pháp luật có quy định khác.

- Công khai chính sách bảo mật, giải thích rõ cách thức thu thập, sử dụng và chia sẻ dữ liệu cá nhân; cung cấp cho người dùng cơ chế truy cập, chỉnh sửa, xóa dữ liệu và thiết lập quyền riêng tư cho dữ liệu cá nhân, báo cáo các vi phạm về bảo mật và quyền riêng tư; bảo vệ dữ liệu cá nhân của công dân Việt Nam khi chuyển dữ liệu xuyên biên giới; xây dựng quy trình xử lý vi phạm về bảo vệ dữ liệu cá nhân nhanh chóng và hiệu quả.

2.1.1.2. Tổ chức, cá nhân

Để bảo đảm an ninh, an toàn dữ liệu trong ứng dụng các sản phẩm, dịch vụ dữ liệu, các tổ chức, cá nhân cần tập trung thực hiện các giải pháp sau:

(1) 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

Việc quy định rõ trách nhiệm pháp lý, kỹ thuật và đạo đức của tổ chức, cá nhân trong thu thập, xử lý, chia sẻ và lưu trữ dữ liệu là yêu cầu cấp thiết trong bối cảnh dữ liệu số trở thành tài sản chiến lược của quốc gia. Trách nhiệm pháp lý phải được thiết lập thành hệ thống văn bản quy phạm pháp luật đồng bộ, chặt chẽ, bảo đảm tính răn đe, minh bạch, khả thi và phù hợp

với thực tiễn quản lý dữ liệu hiện đại. Mỗi tổ chức, cá nhân khi tham gia vào quá trình xử lý dữ liệu cần chịu sự điều chỉnh bởi các khung quy định cụ thể, phân định rõ vai trò, quyền hạn và nghĩa vụ để tránh tình trạng né tránh trách nhiệm, làm phát sinh các rủi ro và hành vi lợi dụng dữ liệu vì mục đích trục lợi, vi phạm quyền riêng tư hay an ninh quốc gia.

Trung tâm dữ liệu quốc gia được kỳ vọng trở thành công cụ giải quyết, tháo gỡ các điểm nghẽn, tạo đột phá trong phát triển cơ sở dữ liệu quốc gia (Ảnh minh họa: Bộ Công an)

Trách nhiệm kỹ thuật là một trụ cột quan trọng, yêu cầu các chủ thể thực hiện đầy đủ các biện pháp bảo mật, bảo đảm toàn vẹn, chính xác và sẵn sàng của dữ liệu trong suốt vòng đời khai thác. Tổ chức, cá nhân có trách nhiệm xây dựng hệ thống kỹ thuật đáp ứng các tiêu chuẩn về an ninh mạng, bảo vệ dữ liệu cá nhân và dữ liệu nhạy cảm, đồng thời phải tiến hành kiểm tra, đánh giá bảo mật định kỳ, ghi nhật ký hoạt động, đảm bảo khả năng phát hiện và ứng phó với sự cố. Các hành vi cấu hình sai, bỏ qua quy trình kỹ thuật, sử dụng hệ thống lạc hậu hoặc cố tình tạo lỗ hổng sẽ bị truy cứu trách nhiệm kỹ thuật, gắn với trách nhiệm hành chính hoặc hình sự tùy theo mức độ nghiêm trọng.

Trách nhiệm đạo đức cần được nâng lên ngang tầm với trách nhiệm pháp lý và kỹ thuật, bởi lẽ nhiều hành vi vi phạm về dữ liệu xuất phát từ động cơ chủ quan, lợi ích cá nhân hoặc sự thờ ơ trong nhận thức về hậu quả. Đạo đức số, đạo đức nghề nghiệp trong lĩnh vực dữ liệu cần được đưa vào chương trình đào tạo, tập huấn bắt buộc, trong đó nhấn mạnh các nguyên tắc: tôn trọng quyền riêng tư của người dùng, minh bạch trong xử lý, tránh thiên vị thuật toán, không sử dụng dữ liệu vào các mục đích trái với đạo lý xã hội, không khai thác dữ liệu vượt quá phạm vi cho phép. Việc vi phạm đạo đức trong lĩnh vực dữ liệu tuy khó định lượng hơn các lỗi kỹ thuật nhưng cần được nhận diện rõ, kết hợp với cơ chế xử phạt và điều chỉnh kịp thời để xây dựng nền văn hóa dữ liệu có trách nhiệm.

Cơ chế xử lý vi phạm cần được thiết lập với tính nghiêm minh, rõ ràng và thống nhất, thể hiện qua các hình thức xử phạt hành chính, truy cứu trách nhiệm hình sự, xử lý nội bộ hoặc cấm hành nghề đối với các vi phạm nghiêm trọng. Hệ thống chế tài phải phân loại rõ ràng các mức độ vi phạm: vô ý, thiếu sót kỹ thuật, cố tình vi phạm, hành vi mang tính tổ chức; đồng thời có quy trình điều tra, thu thập bằng chứng, giám định dữ liệu rõ ràng nhằm đảm bảo công bằng trong xử lý. Cần đặc biệt

lưu ý đến các hành vi cố tình chia sẻ, bán dữ liệu cá nhân trái phép, thu thập dữ liệu mà không có sự đồng ý, hoặc vi phạm các giới hạn sử dụng dữ liệu công, phải được xem là hành vi xâm phạm quyền con người và bị trừng phạt nghiêm khắc.

Bên cạnh xử lý sau vi phạm, cần thiết lập cơ chế phòng ngừa chủ động bằng cách yêu cầu tổ chức, cá nhân xây dựng quy trình quản trị dữ liệu rõ ràng, đăng ký trách nhiệm pháp lý, ký cam kết đạo đức nghề nghiệp và chịu kiểm tra định kỳ. Hệ thống giám sát cần kết hợp giữa công nghệ và giám sát thủ công, trong đó áp dụng các công nghệ phân tích hành vi, AI kiểm soát truy cập, blockchain theo dõi lịch sử chỉnh sửa dữ liệu, từ đó sớm phát hiện các bất thường và hành vi gian lận tiềm ẩn. Đồng thời, việc công khai hóa trách nhiệm của từng vai trò trong hệ sinh thái dữ liệu như nhà cung cấp dịch vụ, quản trị viên, người lập trình, bên thứ ba, người sử dụng cũng góp phần nâng cao tính minh bạch và giảm thiểu vi phạm.

Cơ sở pháp lý để thực hiện những yêu cầu nêu trên cần được hoàn thiện và đồng bộ, bảo đảm tính bao quát cả dữ liệu công và dữ liệu tư, cả dữ liệu truyền thống và dữ liệu phi cấu trúc, dữ liệu được xử lý bằng công nghệ AI. Luật cần phân loại dữ liệu theo mức độ nhạy cảm, quy định nghĩa vụ thông báo vi phạm dữ liệu, trách nhiệm báo cáo định kỳ, quy trình phối hợp giữa các cơ quan chức năng và doanh nghiệp. Cơ chế giải quyết tranh chấp dữ liệu, xử lý yêu cầu xóa bỏ dữ liệu cá nhân, khôi phục quyền truy cập hoặc quyền phản đối xử lý dữ liệu cũng phải rõ ràng, giúp bảo vệ công dân và duy trì sự tin cậy vào hệ thống số quốc gia.

Một nhiệm vụ quan trọng khác là tuyên truyền và nâng cao nhận thức cộng đồng về trách nhiệm pháp lý, kỹ thuật và đạo đức liên quan đến dữ liệu. Các chiến dịch phổ biến pháp luật, các chương trình đào tạo công dân số, các lớp bồi dưỡng cho cán bộ quản lý, chuyên gia công nghệ, sinh viên ngành công nghệ thông tin cần được tổ chức thường xuyên, linh hoạt,

gắn liền với tình huống thực tế và chuẩn mực hành xử mới trong không gian số. Việc tích hợp nội dung về đạo đức dữ liệu, trách nhiệm pháp lý trong giáo dục phổ thông và đại học sẽ góp phần xây dựng lớp công dân số có năng lực và ý thức bảo vệ dữ liệu ngay từ khi bước vào thế giới mạng.

Trong lĩnh vực đặc thù như y tế, tài chính, giao thông, giáo dục, dữ liệu thường chứa thông tin nhạy cảm hoặc ảnh hưởng đến tính mạng, tài sản và quyền lợi của hàng triệu người, vì vậy việc quy định trách nhiệm và xử lý vi phạm càng phải cụ thể hóa hơn nữa. Mỗi ngành cần có quy chuẩn đạo đức dữ liệu riêng, hướng dẫn kỹ thuật xử lý phù hợp, cơ chế kiểm tra chéo giữa các đơn vị, cũng như bộ công cụ kiểm toán dữ liệu độc lập để đảm bảo mọi hoạt động khai thác dữ liệu đều nằm trong tầm kiểm soát và được lưu vết đầy đủ. Sự phối hợp giữa các bộ ngành cần được thể chế hóa qua các văn bản liên ngành, tránh chồng chéo, đùn đẩy trách nhiệm, nhất là khi xảy ra sự cố dữ liệu lớn hoặc tấn công mạng quy mô lớn.

Để giải pháp này đi vào thực tiễn, cần xây dựng cơ quan chuyên trách giám sát đạo đức và pháp lý dữ liệu, có thẩm quyền thanh tra, điều tra, xử phạt và kiến nghị chính sách. Cơ quan này hoạt động độc lập hoặc trực thuộc cơ quan quản lý dữ liệu quốc gia, có sự tham gia của các chuyên gia pháp lý, công nghệ, xã hội học và đạo đức học, từ đó đảm bảo quyết định xử lý vi phạm mang tính khách quan, khoa học và công bằng. Việc công khai danh sách tổ chức, cá nhân vi phạm, mức độ vi phạm và hình thức xử lý cũng là một biện pháp nâng cao tính răn đe, khuyến khích các đơn vị tự giác tuân thủ quy định.

Trong bối cảnh lực lượng Công an nhân dân thực hiện vai trò nòng cốt trong bảo vệ an ninh quốc gia, trật tự an toàn xã hội, giải pháp quy định trách nhiệm và xử lý vi phạm trong lĩnh vực dữ liệu càng trở nên đặc biệt quan trọng. Lực lượng Công an cần tăng cường năng lực điều tra tội phạm mạng, xây dựng đội ngũ chuyên gia giỏi về pháp lý và kỹ thuật dữ liệu, thiết lập

quy trình điều tra số rõ ràng, minh bạch, có thể truy vết và chứng minh được vi phạm trong không gian số. Công an cũng cần chủ động phối hợp với các cơ quan quản lý dữ liệu để chia sẻ thông tin, cảnh báo sớm rủi ro, xử lý các hành vi vi phạm có tổ chức như đánh cắp dữ liệu cá nhân, bán thông tin nội bộ, thao túng dữ liệu xã hội. Đặc biệt, trong công tác đảm bảo an ninh mạng, an ninh thông tin, Công an nhân dân giữ vai trò kiểm tra, giám sát tính tuân thủ của các hệ thống dữ liệu trọng yếu quốc gia, đồng thời phát hiện, ngăn chặn và xử lý nghiêm các hành vi vi phạm đạo đức, pháp luật trong lĩnh vực dữ liệu theo đúng tinh thần "nghiêm từ gốc, chặt từ đầu", góp phần xây dựng không gian mạng an toàn, tin cậy và văn minh.

(2) Thiết lập cơ chế cấp phép hoạt động đối với các tổ chức cung cấp sản phẩm, dịch vụ dữ liệu và thực hiện kiểm định an toàn định kỳ theo khung pháp lý hiện hành

Thiết lập cơ chế cấp phép hoạt động đối với các tổ chức cung cấp sản phẩm, dịch vụ dữ liệu và thực hiện kiểm định an toàn định kỳ theo khung pháp lý hiện hành là một trong những giải pháp trọng yếu nhằm bảo đảm môi trường dữ liệu minh bạch, tin cậy và an toàn trong thời đại chuyển đổi số. Việc cấp phép phải dựa trên các tiêu chí rõ ràng, thống nhất và được luật hóa nhằm đảm bảo sự kiểm soát hiệu quả của Nhà nước đối với hoạt động dữ liệu. Cơ quan quản lý cần xây dựng quy trình cấp phép với các bước như: đánh giá năng lực tổ chức, xác minh nguồn gốc và tính hợp pháp của dữ liệu, kiểm tra công nghệ xử lý và lưu trữ dữ liệu, đánh giá phương án bảo mật, khả năng ứng phó với sự cố và trách nhiệm pháp lý trong trường hợp xảy ra vi phạm. Các tiêu chí đánh giá cần bám sát các quy định pháp luật về bảo vệ dữ liệu cá nhân, an ninh mạng, sở hữu trí tuệ và các luật chuyên ngành liên quan, đồng thời có khả năng cập nhật phù hợp với thực tiễn phát triển nhanh chóng của công nghệ.

Trong quá trình thiết lập cơ chế cấp phép, cần phân loại các tổ chức cung cấp dịch vụ dữ liệu thành các nhóm theo phạm vi hoạt động (nội địa hoặc xuyên biên giới), lĩnh vực chuyên môn (tài chính, y tế, giáo dục, hạ tầng…) và mức độ nhạy cảm của dữ liệu mà họ xử lý. Từ đó, khung pháp lý cấp phép cần xác định rõ những yêu cầu đặc thù cho từng loại hình hoạt động. Các tổ chức hoạt động trong các lĩnh vực trọng yếu liên quan đến dữ liệu cá nhân, dữ liệu mật, dữ liệu nhà nước phải chịu sự giám sát và yêu cầu nghiêm ngặt hơn về kiểm soát nội bộ, công nghệ mã hóa, phương án sao lưu, phục hồi dữ liệu và hệ thống giám sát an ninh mạng. Ngoài ra, cần có quy định cụ thể về thời hạn hiệu lực của giấy phép, điều kiện gia hạn, tạm đình chỉ hoặc thu hồi giấy phép trong trường hợp tổ chức vi phạm các điều khoản đã cam kết hoặc không đáp ứng được tiêu chuẩn an toàn thông tin tối thiểu.

Một nội dung quan trọng không thể thiếu là xây dựng quy trình kiểm định an toàn định kỳ, nhằm bảo đảm rằng các tổ chức cung cấp dịch vụ dữ liệu luôn duy trì năng lực bảo vệ dữ liệu và vận hành an toàn trong suốt thời gian được cấp phép. Việc kiểm định phải được thực hiện bởi các đơn vị có đủ tư cách pháp lý và năng lực chuyên môn, có thể là các tổ chức kiểm định độc lập hoặc cơ quan chuyên trách của Nhà nước. Hoạt động kiểm định cần dựa trên các tiêu chuẩn quốc gia và quốc tế đã được công nhận như ISO/IEC 27001 về quản lý an toàn thông tin, ISO/IEC 27701 về quản lý quyền riêng tư dữ liệu, cũng như các quy chuẩn kỹ thuật được ban hành bởi Bộ Thông tin và Truyền thông. Kiểm định phải bao gồm cả đánh giá kỹ thuật (kiểm tra mã hóa, bảo vệ truy cập, hệ thống giám sát an ninh mạng, năng lực phục hồi sau sự cố) và đánh giá quy trình tổ chức (chính sách nội bộ, đào tạo nhân viên, quản lý rủi ro, ứng phó vi phạm dữ liệu).

Cần quy định rõ tần suất kiểm định theo mức độ rủi ro của từng loại hình dịch vụ, ví dụ như đối với các tổ chức xử lý dữ liệu cá nhân quy mô lớn, hoạt động xuyên biên giới, kiểm định có thể tiến hành hàng năm, trong khi các tổ chức cung cấp

dịch vụ dữ liệu không nhạy cảm có thể kiểm định theo chu kỳ hai hoặc ba năm. Kết quả kiểm định phải được công khai một phần để cộng đồng người dùng có cơ sở đánh giá mức độ tin cậy của các tổ chức cung cấp dịch vụ, đồng thời làm căn cứ cho cơ quan quản lý Nhà nước quyết định việc tiếp tục, đình chỉ hoặc thu hồi giấy phép hoạt động. Trường hợp kiểm định phát hiện tổ chức không đáp ứng yêu cầu về bảo mật, cần có quy trình xử lý nghiêm túc, yêu cầu khắc phục trong thời hạn cụ thể, nếu không đạt sẽ đình chỉ hoạt động tạm thời hoặc vĩnh viễn.

Việc triển khai cơ chế cấp phép và kiểm định định kỳ phải đi kèm với xây dựng cơ sở dữ liệu quốc gia về tổ chức cung cấp sản phẩm, dịch vụ dữ liệu, bao gồm thông tin về loại hình dịch vụ, thời hạn giấy phép, kết quả kiểm định, vi phạm (nếu có), tình trạng khắc phục và mức độ tuân thủ pháp luật. Cơ sở dữ liệu này vừa giúp tăng cường tính minh bạch trong thị trường dữ liệu, vừa hỗ trợ cơ quan quản lý trong việc ra quyết định chính sách, phát hiện sớm các dấu hiệu rủi ro và điều phối các hoạt động kiểm tra, giám sát một cách khoa học. Để bảo đảm hiệu lực thực thi, các quy định về cấp phép và kiểm định cần được ban hành dưới hình thức pháp lý đủ mạnh, có thể là nghị định của Chính phủ hoặc thông tư hướng dẫn thi hành luật dữ liệu, đồng thời phải được lồng ghép trong các văn bản pháp luật liên quan khác như luật an ninh mạng, luật bảo vệ dữ liệu cá nhân, luật giao dịch điện tử.

Bên cạnh cơ chế hành chính, cần thúc đẩy sự tham gia của thị trường và cộng đồng chuyên gia vào hoạt động kiểm định, thông qua việc công nhận các tổ chức kiểm định độc lập, cho phép họ cung cấp dịch vụ kiểm định và đánh giá cho các tổ chức dữ liệu theo cơ chế cạnh tranh công khai, minh bạch. Điều này không chỉ giảm tải cho cơ quan Nhà nước mà còn giúp nâng cao chất lượng kiểm định nhờ sự tham gia của lực lượng chuyên gia đa dạng. Tuy nhiên, để bảo đảm tính thống nhất, các tổ chức kiểm định độc lập phải được cấp chứng chỉ hành nghề, chịu giám sát chặt chẽ và có trách nhiệm pháp lý nếu thực

hiện kiểm định sai lệch hoặc không khách quan. Cần phát triển khung năng lực kiểm định, tiêu chuẩn hóa quy trình và công cụ đánh giá, đồng thời đào tạo lực lượng nhân sự có trình độ cao đáp ứng yêu cầu thực tiễn.

Hoạt động cấp phép và kiểm định an toàn dữ liệu cũng cần tính đến yếu tố quốc tế, nhất là trong bối cảnh dữ liệu xuyên biên giới và dịch vụ đám mây phát triển mạnh mẽ. Việt Nam cần tích cực học hỏi các mô hình quản lý dữ liệu hiệu quả từ các quốc gia có nền tảng công nghệ phát triển như EU, Mỹ, Nhật Bản, đồng thời chủ động tham gia các hiệp định đa phương về bảo vệ dữ liệu, tiêu chuẩn hóa hoạt động kiểm định. Việc công nhận lẫn nhau về kiểm định giữa các quốc gia hoặc tổ chức khu vực cũng là một xu hướng tất yếu, tạo điều kiện thuận lợi cho doanh nghiệp Việt Nam tham gia chuỗi giá trị toàn cầu, đồng thời giảm gánh nặng kiểm định trùng lặp. Trong tương lai, cần phát triển hệ thống kiểm định thông minh tích hợp công nghệ AI, blockchain và điện toán đám mây để tăng hiệu quả, độ chính xác và tính minh bạch trong đánh giá.

Cuối cùng, trong bối cảnh tội phạm mạng lợi dụng không gian số để thực hiện các hành vi xâm phạm dữ liệu ngày càng tinh vi, việc thiết lập cơ chế cấp phép và kiểm định an toàn dữ liệu không chỉ là yêu cầu quản lý nhà nước mà còn là công cụ hỗ trợ đắc lực cho lực lượng Công an trong việc phát hiện, điều tra, ngăn chặn các hoạt động phạm pháp liên quan đến dữ liệu. Các cơ sở dữ liệu về tổ chức dịch vụ dữ liệu, kết quả kiểm định và mức độ tuân thủ sẽ trở thành nguồn thông tin quan trọng giúp lực lượng Công an phân tích rủi ro, xây dựng hồ sơ nghiệp vụ, xác định mục tiêu giám sát trọng điểm. Việc kiểm định định kỳ cũng có vai trò như một biện pháp ngăn ngừa tội phạm từ sớm, phát hiện kẽ hở trong hệ thống bảo mật để kịp thời cảnh báo và phối hợp xử lý. Trong quá trình điều tra tội phạm sử dụng công nghệ cao, thông tin về giấy phép, lịch sử hoạt động và kết quả kiểm định của các tổ chức liên quan là bằng chứng quan trọng giúp truy vết dòng dữ liệu, làm rõ trách nhiệm pháp lý của các bên. Do vậy, lực lượng Công an cần được tham gia từ sớm vào quá trình xây dựng khung pháp lý cấp

phép và kiểm định, đồng thời phối hợp chặt chẽ với các cơ quan quản lý và tổ chức kiểm định để tăng cường hiệu quả bảo vệ an ninh mạng, bảo vệ dữ liệu và bảo vệ chủ quyền quốc gia trên không gian mạng.

- 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.

- 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 biện pháp bảo vệ phù hợp, và kiêm soát truy cập chặt chẽ.

- 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.

(3) Tích hợp các giải pháp mã hóa mạnh trong quá trình lưu trữ, truyền dẫn và xử lý dữ liệu để phòng ngừa truy cập trái phép và đánh cắp thông tin

Tích hợp các giải pháp mã hóa mạnh trong quá trình lưu trữ, truyền dẫn và xử lý dữ liệu là một trong những yêu cầu sống còn để bảo đảm an toàn thông tin, phòng ngừa truy cập trái phép và đánh cắp dữ liệu trong thời đại số. Với sự phát triển nhanh chóng của các công nghệ số, dữ liệu đã trở thành tài sản cốt lõi trong hoạt động của các cơ quan, tổ chức và doanh nghiệp. Tuy nhiên, song hành với giá trị của dữ liệu là nguy cơ bị xâm phạm ngày càng gia tăng cả về tần suất lẫn mức độ

tinh vi. Do đó, việc mã hóa dữ liệu không chỉ là một giải pháp kỹ thuật đơn thuần mà đã trở thành trụ cột trong chiến lược an ninh mạng và bảo vệ thông tin quốc gia.

Trước hết, cần xây dựng khuôn khổ pháp lý và tiêu chuẩn kỹ thuật rõ ràng, thống nhất để hướng dẫn việc áp dụng các giải pháp mã hóa mạnh trên phạm vi toàn quốc. Bộ Thông tin và Truyền thông, phối hợp với Bộ Quốc phòng, Bộ Công an và các cơ quan chuyên trách, cần ban hành hệ thống quy chuẩn, tiêu chuẩn kỹ thuật về mã hóa dữ liệu, đảm bảo phù hợp với thông lệ quốc tế nhưng vẫn đáp ứng yêu cầu bảo mật của quốc gia. Các tiêu chuẩn này cần quy định cụ thể về thuật toán mã hóa được phép sử dụng, độ dài khóa mã, quy trình quản lý khóa mã, cơ chế kiểm tra và đánh giá định kỳ mức độ an toàn của hệ thống mã hóa. Đặc biệt, cần phân loại dữ liệu theo mức độ nhạy cảm và yêu cầu bảo vệ khác nhau để áp dụng giải pháp mã hóa tương ứng, tránh lãng phí tài nguyên và đảm bảo hiệu quả trong thực tiễn triển khai.

Song song với đó, cần tổ chức đánh giá hiện trạng hệ thống dữ liệu đang lưu trữ, truyền dẫn và xử lý tại các cơ quan nhà nước và doanh nghiệp, đặc biệt là những hệ thống liên quan đến dữ liệu cá nhân, dữ liệu hành chính công, dữ liệu y tế, tài chính, an ninh quốc phòng. Việc rà soát và phân tích rủi ro bảo mật sẽ giúp nhận diện các điểm yếu hiện hữu, từ đó xây dựng lộ trình tích hợp mã hóa dữ liệu một cách có trọng tâm, trọng điểm. Các hệ thống có nguy cơ cao bị tấn công hoặc rò rỉ thông tin phải được ưu tiên mã hóa đầu tiên, đồng thời cần có phương án cập nhật, nâng cấp hạ tầng kỹ thuật phù hợp với công nghệ mã hóa mới.

Một nhiệm vụ quan trọng là tích hợp giải pháp mã hóa ngay từ khâu thiết kế hệ thống thông tin và phần mềm (security by design), thay vì áp dụng bổ sung sau khi hệ thống đã vận hành (add-on). Điều này đòi hỏi các đơn vị phát triển phần mềm, các nhà cung cấp dịch vụ công nghệ thông tin cần thay đổi tư duy thiết kế, lấy an toàn dữ liệu làm trung tâm. Các nền tảng

công nghệ mới như điện toán đám mây, trí tuệ nhân tạo, chuỗi khối (blockchain) hay internet vạn vật (IoT) cũng phải được thiết kế để hỗ trợ mã hóa dữ liệu ở nhiều lớp, từ dữ liệu gốc, dữ liệu sao lưu đến dữ liệu trong quá trình truyền tải giữa các thiết bị. Việc này giúp ngăn chặn hiệu quả các hình thức nghe lén, tấn công trung gian, can thiệp bất hợp pháp trong toàn bộ vòng đời của dữ liệu.

Tổng bí thư Tô Lâm đề nghị Tổ công tác bám sát lộ trình thực hiện Đề án, quyết tâm hoàn thành các nội dung công việc theo đúng tiến độ đề ra. Ảnh minh họa. Nguồn từ Internet.

Công tác đào tạo, nâng cao nhận thức và năng lực kỹ thuật về mã hóa dữ liệu cho đội ngũ cán bộ, nhân viên kỹ thuật và quản lý thông tin là yếu tố then chốt đảm bảo khả năng triển khai thực tế các giải pháp mã hóa mạnh. Các chương trình đào tạo cần được thiết kế sát thực tiễn, cập nhật các xu hướng mã hóa hiện đại như mã hóa đồng hình (homomorphic encryption), mã hóa dựa trên định danh (attribute-based encryption), mã hóa định hướng quyền (role-based encryption) hoặc các mô hình mã hóa hậu lượng tử (post-quantum cryptography) trong bối cảnh máy tính lượng tử dần trở thành hiện thực. Bên cạnh đào tạo kỹ thuật, cũng cần nâng cao nhận thức cho cán bộ, công chức về tầm quan trọng của bảo mật dữ liệu, tránh chủ quan trong thao tác hằng ngày như chia sẻ tập tin, sử dụng thiết bị lưu trữ di động hay truy cập từ xa.

Các cơ quan chức năng cần xây dựng và vận hành hệ thống kiểm tra, giám sát việc triển khai và duy trì các giải pháp mã hóa dữ liệu trên diện rộng, tránh tình trạng hình thức hoặc không tuân thủ các quy định kỹ thuật. Các công cụ giám sát cần đảm bảo khả năng phát hiện sớm lỗ hổng mã hóa, tình trạng sử dụng thuật toán lạc hậu hoặc khóa mã yếu, từ đó đưa ra cảnh báo và hướng dẫn xử lý phù hợp. Việc đánh giá định kỳ mức độ an toàn mã hóa cần được lồng ghép vào các cuộc thanh tra an toàn thông tin, đồng thời thúc đẩy trách nhiệm của người đứng đầu cơ quan, tổ chức trong bảo đảm mã hóa dữ liệu mà đơn vị mình quản lý.

Tích cực ứng dụng các giải pháp mã hóa dữ liệu trong các dịch vụ hành chính công, như cổng dịch vụ công trực tuyến, hệ thống quản lý văn bản, hệ thống hộ tịch điện tử, y tế, giáo dục, tài chính công để đảm bảo quyền riêng tư và lợi ích của công dân. Đặc biệt, các dịch vụ có xử lý dữ liệu cá nhân cần có cơ chế mã hóa ở cả phía máy chủ và phía người dùng đầu cuối (end-to-end encryption), bảo đảm không ai – kể cả nhà cung cấp dịch vụ – có thể truy cập được nội dung dữ liệu nếu không

có quyền hợp pháp. Điều này sẽ tạo dựng niềm tin của người dân, thúc đẩy chuyển đổi số trong lĩnh vực công một cách an toàn và bền vững.

Các doanh nghiệp cung cấp dịch vụ số, đặc biệt là những nền tảng thương mại điện tử, tài chính – ngân hàng, logistics, cần được yêu cầu bắt buộc áp dụng mã hóa mạnh cho toàn bộ quá trình giao dịch, thanh toán, lưu trữ thông tin khách hàng và đối tác. Nhà nước có thể thiết lập các yêu cầu pháp lý tối thiểu về mã hóa trong các lĩnh vực này, đồng thời khuyến khích doanh nghiệp áp dụng các chứng chỉ bảo mật quốc tế như ISO/IEC 27001, PCI DSS, SOC 2. Đối với các tổ chức có năng lực công nghệ hạn chế, Nhà nước cần có chính sách hỗ trợ về hạ tầng, chuyên gia tư vấn và công cụ kỹ thuật mã nguồn mở, giảm thiểu khoảng cách số và tăng khả năng tự bảo vệ dữ liệu.

Nghiên cứu, phát triển và làm chủ công nghệ mã hóa nội địa là chiến lược dài hạn cần được quan tâm đặc biệt. Các viện nghiên cứu, trường đại học và doanh nghiệp công nghệ trong nước cần được đầu tư để xây dựng các bộ mã hóa độc quyền, phù hợp với đặc điểm tiếng Việt, luật pháp và môi trường mạng trong nước. Việc này không chỉ đảm bảo khả năng ứng phó với các lệnh cấm vận công nghệ từ nước ngoài mà còn bảo vệ chủ quyền số quốc gia. Hệ sinh thái các công nghệ mã hóa nội địa cần được tích hợp vào hệ điều hành, phần mềm văn phòng, trình duyệt web, thiết bị IoT, điện thoại thông minh và các thiết bị mạng khác.

Trong lĩnh vực quốc phòng, an ninh, cần ưu tiên ứng dụng các giải pháp mã hóa cấp độ cao, đa tầng, được chứng nhận bởi cơ quan có thẩm quyền, đặc biệt là đối với dữ liệu tuyệt mật, tối mật hoặc phục vụ công tác điều tra, trinh sát, phản gián. Mỗi đơn vị phải có đội ngũ chuyên gia mã hóa có trình độ, được trang bị đầy đủ công cụ và được đào tạo thường xuyên về

các mối đe dọa mới nổi cũng như kỹ thuật mã hóa tiên tiến. Ngoài ra, cần tăng cường hợp tác quốc tế để cập nhật các tiêu chuẩn mã hóa tiên tiến nhất, đồng thời thiết lập các kênh trao đổi thông tin về mã hóa an toàn với các quốc gia có trình độ bảo mật cao.

Đối với lực lượng Công an nhân dân, việc tích hợp các giải pháp mã hóa mạnh trong quá trình lưu trữ, truyền dẫn và xử lý dữ liệu là yêu cầu bắt buộc để bảo vệ an toàn hệ thống dữ liệu nghiệp vụ, thông tin tình báo, hồ sơ vụ án và dữ liệu dân cư. Trong quá trình điều tra, lực lượng công an thường xuyên phải thu thập, phân tích và lưu trữ khối lượng lớn dữ liệu nhạy cảm, nếu không được bảo vệ bằng mã hóa phù hợp sẽ dễ bị xâm nhập, khai thác hoặc làm sai lệch, ảnh hưởng nghiêm trọng đến hiệu quả công tác nghiệp vụ. Vì vậy, Bộ Công an cần ban hành quy định nội bộ về tiêu chuẩn mã hóa trong từng cấp độ bảo mật nghiệp vụ; đồng thời xây dựng đội ngũ kỹ thuật chuyên trách về an toàn mã hóa, đảm bảo khả năng triển khai nhanh, xử lý sự cố và chủ động tấn công ngăn chặn các âm mưu phá hoại, xâm nhập dữ liệu. Việc tích hợp mã hóa còn góp phần nâng cao uy tín, niềm tin của nhân dân vào hệ thống quản lý dữ liệu của lực lượng Công an, từ đó hỗ trợ đắc lực cho công cuộc xây dựng xã hội an toàn, công bằng và văn minh.

(4) Thực hiện đánh giá an ninh hệ thống định kỳ (audit) và kiểm thử xâm nhập (penetration testing).

Thực hiện kiểm tra, đánh giá và kiểm toán định kỳ an toàn thông tin.

Ảnh minh họa. Nguồn từ Internet.

Việc thực hiện kiểm tra, đánh giá và kiểm toán định kỳ an toàn thông tin đối với hạ tầng dữ liệu, dịch vụ dữ liệu và các nền tảng tích hợp – chia sẻ là một nội dung then chốt nhằm duy trì sự bền vững, tin cậy và khả năng phục hồi của hệ thống thông tin trong bối cảnh dữ liệu ngày càng trở thành tài sản chiến lược của các cơ quan, tổ chức và quốc gia. Hoạt động này cần được triển khai đồng bộ, có hệ thống, gắn liền với chu trình quản trị an toàn thông tin, phù hợp với các tiêu chuẩn quốc tế như ISO/IEC 27001, ISO/IEC 27701 hoặc NIST SP 800. Trước hết, cần thiết lập quy trình kiểm tra và kiểm toán định kỳ

một cách khoa học, minh bạch và có khả năng cập nhật liên tục theo thay đổi công nghệ, mô hình tấn công mạng và hành vi sử dụng dữ liệu. Các quy trình này phải xác định rõ vai trò, trách nhiệm của các bên liên quan từ bộ phận công nghệ thông tin, an ninh mạng, quản trị dữ liệu đến cấp lãnh đạo ra quyết định, đảm bảo rằng kết quả kiểm toán có thể dẫn tới các hành động cải thiện cụ thể thay vì chỉ dừng ở mức ghi nhận.

Hệ thống hạ tầng dữ liệu cần được kiểm tra toàn diện từ các lớp vật lý như máy chủ, hệ thống lưu trữ, thiết bị mạng đến các lớp logic như hệ điều hành, phần mềm trung gian, cơ sở dữ liệu và dịch vụ dữ liệu. Trong mỗi chu kỳ kiểm tra, cần đánh giá các lỗ hổng tiềm tàng, cấu hình sai, điểm yếu bảo mật và khả năng chống chịu trước các tình huống bất thường như tấn công DDoS, rò rỉ dữ liệu, truy cập trái phép hoặc lỗi vận hành nội bộ. Việc kiểm tra này không thể tách rời các biện pháp phát hiện và phản ứng sự cố, mà cần tích hợp vào quy trình giám sát liên tục, để có thể kích hoạt các cảnh báo sớm và biện pháp khắc phục kịp thời. Hơn nữa, các bài kiểm thử xâm nhập (penetration testing) và đánh giá kỹ thuật (vulnerability assessment) cần được tiến hành một cách chuyên sâu, có sự tham gia của đội ngũ chuyên gia độc lập để đảm bảo tính khách quan và phát hiện các vấn đề mà nội bộ có thể bỏ sót.

Dịch vụ dữ liệu là thành phần trọng yếu trong hệ sinh thái số, đặc biệt trong mô hình chính phủ điện tử, đô thị thông minh và nền kinh tế dữ liệu, do đó việc kiểm tra an toàn của các dịch vụ này đòi hỏi quy trình khắt khe không kém gì đối với hạ tầng. Cần tiến hành đánh giá khả năng xác thực và phân quyền truy cập người dùng, kiểm soát luồng dữ liệu ra vào hệ thống, đặc biệt là các API – giao diện lập trình ứng dụng có thể bị khai thác nếu thiếu kiểm soát. Cần đánh giá khả năng lưu vết, ghi log và phân tích hành vi bất thường trên các lớp dịch vụ dữ liệu, đặc biệt khi các dịch vụ này được triển khai trên nền tảng điện toán đám mây hoặc kết nối với hệ sinh thái dữ liệu bên ngoài. Đối với các dịch vụ dữ liệu được phát triển nội bộ,

việc kiểm tra mã nguồn (code review) và thử nghiệm kiểm thử bảo mật (security testing) cần được thực hiện định kỳ và tích hợp trong quy trình DevSecOps nhằm phát hiện lỗi sớm ngay trong giai đoạn phát triển phần mềm.

Các nền tảng tích hợp – chia sẻ dữ liệu đóng vai trò then chốt trong việc kết nối và cộng tác giữa các cơ quan, tổ chức, do đó phải được giám sát và kiểm toán ở mức cao nhất về bảo mật, độ tin cậy và khả năng phục hồi. Việc kiểm tra cần tập trung vào các giao thức chia sẻ, cơ chế đồng bộ dữ liệu, khả năng phân định và kiểm soát quyền truy cập liên cơ quan, cũng như việc tuân thủ các quy định pháp luật hiện hành về bảo vệ dữ liệu cá nhân, an ninh mạng và bí mật nhà nước. Các nền tảng tích hợp – chia sẻ, nếu không được kiểm tra thường xuyên, rất dễ trở thành điểm yếu của hệ thống, là nơi bị tấn công để lấy cắp dữ liệu từ nhiều nguồn hoặc phá vỡ chuỗi kết nối dữ liệu phục vụ quản trị và ra quyết định. Trong bối cảnh đó, việc kiểm toán định kỳ có thể giúp phát hiện các nguy cơ sớm và đảm bảo rằng nền tảng luôn được vận hành trên các cấu hình an toàn nhất.

Ngoài kiểm tra kỹ thuật, cần đánh giá cả khía cạnh tuân thủ và quản trị rủi ro dữ liệu. Các cơ quan, tổ chức cần xây dựng bộ chỉ số an toàn thông tin và chỉ số rủi ro dữ liệu để làm căn cứ đánh giá định kỳ và xác định các điểm cần cải thiện. Công tác kiểm toán cần bao gồm việc rà soát các chính sách, quy trình, đào tạo nhân sự và nhận thức an toàn thông tin trong toàn tổ chức, vì con người luôn là mắt xích yếu nhất trong chuỗi an ninh mạng. Các lỗi do người dùng vô ý như lộ mật khẩu, chia sẻ file sai quy định, sử dụng thiết bị cá nhân không được kiểm soát kết nối vào mạng nội bộ là nguyên nhân phổ biến dẫn đến sự cố dữ liệu. Do đó, kiểm tra định kỳ cũng cần đánh giá mức độ tuân thủ các quy định nội bộ về sử dụng hệ thống, quản lý thiết bị và kiểm soát truy cập.

Việc thực hiện kiểm tra, đánh giá và kiểm toán định kỳ không chỉ dừng lại ở góc độ kỹ thuật, mà cần tích hợp vào chu trình quản trị chiến lược dữ liệu quốc gia và cơ quan. Kết quả của các đợt kiểm toán phải được báo cáo định kỳ lên cấp có thẩm quyền, đi kèm kế hoạch khắc phục, cải tiến, đồng thời làm căn cứ để xây dựng ngân sách đầu tư nâng cấp hệ thống và đào tạo nguồn nhân lực. Một hệ thống an toàn không thể chỉ dựa vào các công cụ kỹ thuật, mà cần gắn liền với cơ chế phản hồi chính sách, phân quyền kiểm soát và trách nhiệm giải trình rõ ràng từ người đứng đầu đến nhân viên vận hành hệ thống. Cần có hệ thống giám sát độc lập và đánh giá chéo giữa các cơ quan để đảm bảo không có khu vực "miễn kiểm tra" hoặc bị bỏ sót trong đánh giá định kỳ. Đây là yếu tố then chốt bảo đảm tính toàn vẹn và khả năng phục hồi trong vận hành hệ thống dữ liệu và nền tảng chia sẻ.

Trong điều kiện chuyển đổi số quốc gia đang diễn ra mạnh mẽ, hoạt động kiểm tra và kiểm toán an toàn thông tin cần được số hóa, tự động hóa và khai thác các công nghệ tiên tiến như học máy, AI để phát hiện các mẫu bất thường trong hệ thống dữ liệu lớn. Việc xây dựng hệ thống dashboard phân tích rủi ro thời gian thực, tích hợp các kết quả kiểm tra định kỳ với cảnh báo từ hệ thống giám sát an ninh mạng sẽ giúp đưa ra quyết định quản trị dữ liệu hiệu quả hơn. Các báo cáo đánh giá cần được số hóa và chuẩn hóa về định dạng, cấu trúc nhằm tạo điều kiện cho việc so sánh, tổng hợp, thống kê và lập kế hoạch cải thiện toàn diện ở cấp tổ chức và quốc gia. Tăng cường năng lực của các cơ quan chuyên trách kiểm toán CNTT – dữ liệu cả về nhân sự, công cụ kỹ thuật và cơ chế phối hợp liên ngành là nền tảng để đảm bảo tính hiệu quả và khả năng áp dụng thực tiễn của hoạt động kiểm tra định kỳ.

Trong bối cảnh dữ liệu trở thành nguồn lực chiến lược mới, nhiệm vụ kiểm tra, đánh giá, kiểm toán an toàn thông tin càng mang ý nghĩa sống còn đối với bảo vệ chủ quyền số và an ninh quốc gia. Lực lượng Công an nhân dân, với vai trò là lực

lượng nòng cốt trong bảo vệ an ninh trật tự, có trách nhiệm chủ động tham gia giám sát, thẩm định, hỗ trợ kỹ thuật và xử lý các sự cố liên quan đến an toàn dữ liệu, đặc biệt trong các hệ thống quan trọng như cơ sở dữ liệu quốc gia, hệ thống thông tin nghiệp vụ và nền tảng tích hợp – chia sẻ dữ liệu phục vụ quản lý nhà nước. Công an các đơn vị, địa phương cần phối hợp với các cơ quan chủ quản hệ thống để tổ chức kiểm tra an toàn thông tin định kỳ, phát hiện và xử lý sớm các điểm yếu, đồng thời tham mưu xây dựng các quy trình giám sát hiệu quả nhằm đảm bảo mọi hoạt động chia sẻ và sử dụng dữ liệu đều nằm trong tầm kiểm soát an ninh. Lực lượng Công an cũng cần đẩy mạnh công tác huấn luyện chuyên sâu về an toàn thông tin, an ninh mạng và kiểm toán hệ thống dữ liệu, sẵn sàng ứng phó với các tình huống tấn công mạng tinh vi trong thời đại chuyển đổi số. Đây chính là cơ sở để đảm bảo an toàn tuyệt đối cho các hệ thống dữ liệu quan trọng, bảo vệ vững chắc an ninh quốc gia trong môi trường số.

(5) Cập nhật liên tục chính sách bảo mật, quy trình xử lý dữ liệu và mô hình quản trị dữ liệu theo các xu hướng công nghệ mới như điện toán đám mây, dữ liệu lớn, trí tuệ nhân tạo và bảo mật không biên giới (Zero Trust)

Việc cập nhật liên tục chính sách bảo mật, quy trình xử lý dữ liệu và mô hình quản trị dữ liệu đóng vai trò then chốt trong việc bảo vệ thông tin trong bối cảnh công nghệ số phát triển nhanh chóng. Khi các xu hướng công nghệ mới như điện toán đám mây, dữ liệu lớn (Big Data), trí tuệ nhân tạo (AI) và mô hình bảo mật không biên giới (Zero Trust) ngày càng được ứng dụng sâu rộng, việc xây dựng và duy trì chính sách bảo mật không thể mang tính chất tĩnh hoặc rập khuôn theo các khuôn mẫu cũ. Cơ quan, tổ chức cần xác lập một cơ chế giám sát và điều chỉnh định kỳ đối với toàn bộ hệ thống chính sách, từ các văn bản nội bộ quy định về quyền truy cập, lưu trữ, truyền tải đến các giao thức xử lý, ứng cứu sự cố, đồng thời lồng ghép khả năng thích ứng với các thay đổi công nghệ. Mỗi thay đổi nhỏ trong cấu trúc công nghệ đều có thể dẫn đến thay đổi về

mức độ rủi ro, đòi hỏi các chính sách bảo mật phải có tính mềm dẻo và linh hoạt trong triển khai, nhưng vẫn phải đảm bảo tính toàn vẹn, bảo mật và khả năng kiểm soát.

Trong môi trường điện toán đám mây, nơi dữ liệu được lưu trữ và xử lý thông qua hệ thống máy chủ phân tán trên internet, các chính sách bảo mật cần được thiết kế theo hướng phi tập trung và tương thích với các tiêu chuẩn bảo mật của nhà cung cấp dịch vụ. Cần xác định rõ trách nhiệm giữa đơn vị lưu trữ, đơn vị cung cấp hạ tầng, và đơn vị khai thác dữ liệu. Việc này bao gồm cả việc quy định chính sách mã hóa dữ liệu tại chỗ (at-rest), khi truyền dẫn (in-transit) và trong quá trình xử lý (in-use), cũng như triển khai các công cụ giám sát, cảnh báo truy cập bất thường, tấn công từ bên trong và bên ngoài. Các quy trình xử lý dữ liệu cần có cơ chế phân tầng bảo vệ theo mức độ nhạy cảm và thiết lập quyền truy cập phù hợp theo vai trò người dùng. Ngoài ra, cần liên tục kiểm tra khả năng phục hồi dữ liệu sau sự cố, sao lưu định kỳ và đánh giá sự tuân thủ của các đối tác, nhà cung cấp thứ ba.

Đối với dữ liệu lớn, chính sách bảo mật không chỉ tập trung vào bảo vệ thông tin riêng lẻ mà còn phải xử lý được rủi ro tổng hợp từ việc phân tích khối lượng dữ liệu đồ sộ. Việc khai thác Big Data mang lại nhiều lợi ích trong dự báo, phát hiện gian lận, tối ưu vận hành nhưng cũng làm gia tăng nguy cơ rò rỉ dữ liệu diện rộng nếu không được bảo vệ đúng cách. Các quy trình bảo mật phải tích hợp sẵn khả năng gắn thẻ dữ liệu theo cấp độ bảo mật, định danh và ẩn danh hóa thông minh trước khi xử lý, cũng như kiểm soát chặt chẽ truy cập từ hệ thống phân tích hoặc người dùng có đặc quyền. Chính sách cần yêu cầu áp dụng các công cụ giám sát hành vi bất thường trong thời gian thực và phân tích lịch sử truy cập để phát hiện sớm nguy cơ nội gián hoặc tấn công có chủ đích (APT). Việc thiết kế kiến trúc dữ liệu phân lớp và tách biệt môi trường phân tích – môi trường thực thi cũng là bước quan trọng trong quy trình quản trị dữ liệu an toàn trong bối cảnh dữ liệu lớn.

Khi trí tuệ nhân tạo trở thành một phần trong hệ thống xử lý dữ liệu, chính sách bảo mật cần mở rộng sang cả khía cạnh đạo đức và kiểm soát thuật toán. AI có khả năng tự học và đưa ra quyết định từ tập dữ liệu huấn luyện, do đó cần quy định rõ các tiêu chuẩn bảo mật cho dữ liệu đào tạo, đánh giá định kỳ về độ thiên lệch và khả năng dẫn đến hành vi sai lệch trong hệ thống AI. Việc sử dụng AI để hỗ trợ trong bảo mật, như phát hiện xâm nhập, phân tích hành vi người dùng, cần đi kèm với quy trình xác minh, ghi nhận và phản ứng có kiểm soát nhằm hạn chế tác động của các quyết định sai hoặc kết quả phân tích bị tấn công. Ngoài ra, các tổ chức cần thường xuyên cập nhật khung pháp lý, chuẩn đạo đức và mô hình quản trị AI gắn với an toàn dữ liệu, đảm bảo rằng các hệ thống này không vô tình trở thành công cụ làm rò rỉ thông tin hoặc vi phạm quyền riêng tư người dùng.

Bảo mật không biên giới (Zero Trust) là xu thế tất yếu trong bối cảnh môi trường làm việc từ xa, thiết bị cá nhân tham gia vào hệ thống mạng doanh nghiệp ngày càng nhiều, ranh giới mạng truyền thống bị xóa nhòa. Chính sách bảo mật trong mô hình Zero Trust cần định nghĩa lại khái niệm "đáng tin cậy", không theo địa chỉ IP, mạng nội bộ hay vị trí địa lý, mà dựa vào phân tích hành vi, mức độ rủi ro và xác thực liên tục. Mỗi truy cập vào hệ thống, bất kể từ trong hay ngoài tổ chức, đều phải được kiểm tra, xác thực, phân quyền và giám sát liên tục. Quy trình xử lý dữ liệu phải đi kèm kiểm soát truy cập động (Dynamic Access Control), áp dụng xác thực đa yếu tố (MFA), kiểm tra thiết bị đầu cuối (Endpoint Security Posture) và mã hóa toàn diện. Cần thiết lập một cơ chế phản hồi nhanh đối với các vi phạm chính sách, có khả năng cô lập điểm truy cập nguy hiểm và khôi phục hệ thống trong thời gian ngắn. Việc xây dựng văn hóa Zero Trust cũng đòi hỏi đào tạo nhận thức bảo mật cho cán bộ, đồng thời tích hợp công nghệ AI để tự động hóa việc phát hiện và phản ứng với sự cố.

Tất cả các chính sách, quy trình và mô hình quản trị dữ liệu cần được rà soát, cập nhật định kỳ thông qua một cơ chế giám sát trung tâm. Cần có hệ thống đánh giá hiệu quả thực thi chính sách, bao gồm các chỉ số đo lường cụ thể như tỷ lệ vi phạm, thời gian phát hiện – xử lý sự cố, mức độ tuân thủ các tiêu chuẩn quốc tế như ISO/IEC 27001, GDPR hay NIST. Đồng thời, cần xây dựng quy trình tiếp nhận, phân tích và tích hợp các cảnh báo, báo cáo sự cố và xu hướng tấn công mới từ cộng đồng an ninh mạng toàn cầu để bổ sung, điều chỉnh kịp thời cho phù hợp. Việc hợp tác với các tổ chức nghiên cứu, nhà cung cấp công nghệ và các cơ quan chức năng là điều kiện cần thiết để bảo đảm hệ thống quản trị dữ liệu không bị lỗi thời hoặc tụt hậu trước các nguy cơ mới. Chính sách phải đảm bảo không chỉ hướng dẫn hành động cụ thể mà còn tạo nền tảng pháp lý, kỹ thuật và đạo đức cho toàn bộ hệ sinh thái dữ liệu hoạt động ổn định, hiệu quả và an toàn.

Bên cạnh cập nhật chính sách, việc thử nghiệm các mô hình giả lập tấn công (Red Team/Blue Team), tổ chức diễn tập an ninh mạng, kiểm tra xuyên suốt chuỗi cung ứng dữ liệu cũng cần được tích hợp thành một phần của quy trình bảo mật tổng thể. Những kết quả phân tích sau diễn tập hoặc tấn công thực tế sẽ là căn cứ để điều chỉnh chính sách phù hợp với môi trường vận hành thực tế, giảm thiểu độ trễ giữa lý thuyết và thực tiễn triển khai. Ngoài ra, chính sách cũng cần làm rõ cơ chế chia sẻ dữ liệu giữa các đơn vị, quy định chặt chẽ quyền sở hữu, quyền sử dụng, quyền chia sẻ và trách nhiệm xử lý khi xảy ra vi phạm hoặc tranh chấp về dữ liệu. Cần xây dựng một hệ thống nhật ký (log) đầy đủ và không thể chỉnh sửa nhằm đảm bảo truy vết, minh bạch trong điều tra, kiểm toán hoặc tranh tụng.

Trong bối cảnh đó, lực lượng Công an có vai trò đặc biệt quan trọng trong việc giám sát, định hướng và kiểm tra việc triển khai các chính sách bảo mật, xử lý dữ liệu và quản trị dữ liệu trong toàn xã hội. Trước hết, lực lượng Công an cần chủ động nghiên cứu, cập nhật thường xuyên các xu hướng công nghệ mới, làm chủ công nghệ trí tuệ nhân tạo, dữ liệu lớn và mô

hình Zero Trust để có thể đưa ra các khuyến nghị chính sách phù hợp, phát hiện kịp thời các nguy cơ an ninh mạng tiềm ẩn. Đồng thời, Công an nhân dân cần phát huy vai trò trong thanh tra, kiểm tra việc tuân thủ quy định của các tổ chức, doanh nghiệp về bảo mật dữ liệu, nhất là trong những lĩnh vực liên quan đến dữ liệu cá nhân, dữ liệu quốc gia trọng yếu và hoạt động xuyên biên giới. Việc phối hợp liên ngành giữa Công an và các cơ quan chuyên trách về công nghệ, truyền thông, an toàn thông tin sẽ giúp tạo dựng một hệ sinh thái an toàn số toàn diện, trong đó dữ liệu vừa là tài nguyên, vừa là đối tượng cần được bảo vệ nghiêm ngặt bằng cơ chế pháp lý, kỹ thuật và nghiệp vụ vững chắc. Lực lượng Công an cũng cần đảm nhận vai trò nòng cốt trong công tác tuyên truyền, nâng cao nhận thức của toàn dân về an ninh dữ liệu, từ đó góp phần giữ vững an ninh quốc gia và trật tự, an toàn xã hội trong kỷ nguyên số.

Giao dịch dữ liệu là một bước phát triển tất yếu trong nền kinh tế số, đòi hỏi khuôn khổ pháp lý bảo đảm tính minh bạch, an toàn và bảo vệ quyền lợi của các bên liên quan. Cần có quy định pháp luật về điều kiện cho phép giao dịch dữ liệu, thẩm quyền cấp phép, các loại dữ liệu được phép mua bán, định giá dữ liệu, cơ chế bảo vệ thông tin cá nhân trong quá trình giao dịch. Pháp luật cũng cần làm rõ trách nhiệm của sàn giao dịch dữ liệu, quyền và nghĩa vụ của bên cung cấp và bên sử dụng dữ liệu, cơ chế xử lý tranh chấp, vi phạm trong giao dịch. Giao dịch dữ liệu cũng cần tuân thủ các nguyên tắc về an ninh mạng, bảo vệ chủ quyền dữ liệu quốc gia và không làm ảnh hưởng đến lợi ích quốc gia, dân tộc.

2.1.2. Biện pháp giám sát hành vi có thể ảnh hưởng đến việc bảo vệ dữ liệu

(1) Thiết lập hệ thống giám sát an ninh mạng liên tục, sử dụng công nghệ AI và học máy để phát hiện bất thường, tấn công và hành vi rò rỉ dữ liệu kịp thời

Thiết lập hệ thống giám sát an ninh mạng liên tục là một trong những giải pháp cốt lõi nhằm bảo đảm an toàn dữ liệu và phòng ngừa các rủi ro an ninh mạng trong bối cảnh công nghệ số phát triển mạnh mẽ. Để triển khai hiệu quả giải pháp này, cần xây dựng một kiến trúc giám sát tổng thể, tích hợp từ hạ tầng mạng, máy chủ, thiết bị đầu cuối đến các dịch vụ đám mây và hệ thống lưu trữ, bảo đảm khả năng quan sát và ghi nhận toàn diện mọi hoạt động diễn ra trong không gian mạng của tổ chức. Việc triển khai cần bắt đầu từ việc thu thập và đồng bộ các nguồn dữ liệu log đa dạng, bao gồm log hệ điều hành, ứng dụng, firewall, IDS/IPS, thiết bị mạng và dữ liệu giao dịch, từ đó phục vụ cho việc phân tích và nhận diện các bất thường theo thời gian thực.

Tích hợp công nghệ trí tuệ nhân tạo (AI) và học máy (machine learning - ML) vào chu trình xử lý, phân tích dữ liệu. Ảnh minh họa. Nguồn từ Internet.

Trọng tâm của hệ thống giám sát hiện đại chính là tích hợp công nghệ trí tuệ nhân tạo (AI) và học máy (machine learning - ML) vào chu trình xử lý, phân tích dữ liệu nhằm phát hiện tự động các dấu hiệu bất thường, hành vi nguy hiểm hoặc tấn công mạng. Các mô hình AI có thể học từ hành vi bình thường của hệ thống và người dùng để phát hiện sự khác biệt, ví dụ như truy cập trái phép vào giờ bất thường, lưu lượng mạng tăng đột biến, hoặc các hành vi sao chép, tải xuống, truyền tải dữ liệu có dấu hiệu bất hợp lý. Hệ thống học máy không chỉ dựa trên quy tắc cố định như các giải pháp bảo mật truyền thống mà còn liên tục cải tiến dựa trên dữ liệu thực tế, giúp tăng khả năng ứng phó với các loại hình tấn công mới như tấn công zero-day, mã độc biến thể, hoặc các hành vi nội gián khó lường.

Bên cạnh AI và học máy, việc áp dụng công nghệ phân tích hành vi người dùng và thực thể (UEBA – User and Entity Behavior Analytics) đóng vai trò quan trọng trong hệ thống giám sát. UEBA cho phép xác định các hành vi sử dụng bất thường so với tiêu chuẩn hoạt động bình thường của từng cá nhân, phòng ban hoặc hệ thống. Sự khác biệt về mô hình truy cập, các thay đổi đột xuất trong quyền hạn, tần suất hoạt động hoặc địa điểm truy cập đều có thể được phát hiện và đưa vào danh sách cảnh báo. Điều này đặc biệt hữu ích trong việc phát hiện các cuộc tấn công nâng cao có chủ đích (APT), nơi mà kẻ tấn công đã chiếm quyền điều khiển tài khoản nội bộ và hoạt động như người dùng hợp pháp.

Hệ thống giám sát cần được thiết kế theo nguyên tắc phân lớp và đa tầng, trong đó mỗi tầng thực hiện một chức năng riêng biệt và tương tác với nhau để tạo nên một mạng lưới phòng thủ toàn diện. Tầng đầu tiên có thể là các cảm biến mạng (network sensors) dùng để thu thập và gửi dữ liệu lưu lượng về trung tâm giám sát. Tầng thứ hai là các hệ thống quản lý log tập trung (SIEM – Security Information and Event Management) thực hiện chức năng phân tích, tổng hợp và đưa ra cảnh báo.

Tầng thứ ba có thể là các nền tảng hỗ trợ ra quyết định tự động như SOAR (Security Orchestration, Automation and Response), giúp phối hợp phản ứng và xử lý sự cố nhanh chóng, giảm thiểu phụ thuộc vào can thiệp thủ công.

Để bảo đảm khả năng hoạt động 24/7, hệ thống giám sát cần được vận hành bởi một Trung tâm điều hành an ninh mạng (SOC – Security Operation Center) với đội ngũ chuyên gia an ninh được đào tạo bài bản. SOC có nhiệm vụ giám sát liên tục, phân tích cảnh báo, điều phối xử lý sự cố và liên kết với các bộ phận liên quan trong tổ chức để thực hiện các biện pháp khắc phục kịp thời. Việc thiết lập các ca trực luân phiên, quy trình kiểm tra chéo, đánh giá mức độ rủi ro và phân loại ưu tiên xử lý là điều cần thiết để bảo đảm tính liên tục và hiệu quả. SOC cũng cần xây dựng các kịch bản ứng phó với nhiều loại sự cố an ninh mạng khác nhau, từ tấn công từ chối dịch vụ (DDoS), tấn công leo thang đặc quyền, đến rò rỉ dữ liệu có chủ đích, nhằm bảo đảm sự sẵn sàng trước mọi tình huống.

Một nhiệm vụ trọng tâm khác là xây dựng kho dữ liệu huấn luyện phục vụ cho các mô hình AI/ML trong hệ thống giám sát. Các tập dữ liệu này cần được thu thập từ thực tế, có tính đại diện và được gắn nhãn rõ ràng để làm đầu vào cho thuật toán học sâu. Song song đó, cần triển khai các cơ chế giám sát liên tục hiệu suất của mô hình, đánh giá độ chính xác, tỷ lệ phát hiện dương tính giả hoặc âm tính giả, để điều chỉnh hoặc huấn luyện lại khi cần thiết. Việc thường xuyên cập nhật tập dữ liệu và cải tiến mô hình sẽ giúp hệ thống thích ứng tốt hơn với các mối đe dọa ngày càng tinh vi và có khả năng tự phục hồi khi bị tấn công.

Việc đảm bảo tích hợp giữa hệ thống giám sát an ninh mạng và các nền tảng CNTT hiện hữu là một yếu tố thiết yếu. Cần thiết lập khả năng tương thích, tích hợp hai chiều với các nền tảng ERP, CRM, hệ thống lưu trữ đám mây, nền tảng xử

lý dữ liệu lớn hoặc các hệ thống kiểm soát truy cập hiện có, nhằm bảo đảm không tạo ra các điểm mù trong giám sát. Ngoài ra, cần thiết kế các API bảo mật, chuẩn hóa giao thức giao tiếp và thiết lập các chính sách chia sẻ dữ liệu phù hợp để tạo điều kiện cho các thành phần khác nhau cùng tham gia vào quá trình phát hiện, cảnh báo và xử lý sự cố.

Việc đảm bảo khả năng mở rộng của hệ thống cũng cần được tính đến, đặc biệt là trong bối cảnh dữ liệu phát sinh ngày càng nhiều, thiết bị kết nối mạng tăng mạnh do sự phổ cập của IoT và công nghệ 5G. Do đó, hệ thống cần hỗ trợ hạ tầng đám mây lai (hybrid cloud), khả năng xử lý phân tán (distributed processing) và khai thác tính toán biên (edge computing) nhằm xử lý dữ liệu tại chỗ, giảm tải cho trung tâm và rút ngắn thời gian phản ứng. Ngoài ra, việc sử dụng kiến trúc microservices và container hóa (như Docker, Kubernetes) sẽ giúp hệ thống linh hoạt hơn, dễ nâng cấp và triển khai theo nhu cầu thực tế.

Song song với thiết lập kỹ thuật, cần phát triển chính sách và quy trình giám sát rõ ràng, bao gồm quyền truy cập, quy định về bảo mật, phân quyền trách nhiệm và các hình thức xử lý vi phạm. Quy trình này phải bảo đảm tuân thủ pháp luật, tôn trọng quyền riêng tư cá nhân nhưng vẫn đủ khả năng phát hiện và ngăn chặn hành vi gây hại cho tổ chức. Cần thiết lập các bảng phân tích rủi ro, ma trận quyền truy cập, định nghĩa các hành vi bất thường cụ thể và cơ chế phản ứng thích hợp cho từng mức độ đe dọa.

Một yêu cầu quan trọng là xây dựng cơ chế kiểm tra định kỳ, kiểm toán và đánh giá hiệu quả hoạt động của hệ thống giám sát. Việc thực hiện các bài kiểm tra thâm nhập (penetration testing), mô phỏng tấn công có kiểm soát (red team/blue team), đánh giá bảo mật định kỳ sẽ giúp phát hiện sớm các lỗ hổng, điểm yếu trong hệ thống và nâng cao tính sẵn sàng đối

phó với các cuộc tấn công thực tế. Các kết quả đánh giá cần được lưu trữ có hệ thống, phân tích xu hướng và dùng để cải tiến hoạt động giám sát theo thời gian.

Trong bối cảnh các mối đe dọa an ninh mạng không ngừng gia tăng cả về quy mô lẫn mức độ tinh vi, việc thiết lập hệ thống giám sát liên tục là yêu cầu bắt buộc trong mọi tổ chức hiện đại. Ngoài các yếu tố kỹ thuật, hệ thống giám sát cần gắn kết với chiến lược quản trị tổng thể của tổ chức, bảo đảm sự phối hợp giữa các bộ phận chức năng, từ công nghệ thông tin đến quản lý rủi ro và pháp chế, để tạo thành một hệ sinh thái phòng thủ chặt chẽ, chủ động và linh hoạt.

Đối với lực lượng Công an nhân dân, nhiệm vụ thiết lập hệ thống giám sát an ninh mạng có vai trò đặc biệt quan trọng trong công tác bảo vệ an ninh quốc gia, trật tự an toàn xã hội trong không gian mạng. Lực lượng Công an cần chủ động triển khai hệ thống giám sát tại các đơn vị chuyên trách về an ninh mạng, thu thập và phân tích thông tin từ nhiều nguồn, từ đó phát hiện và ngăn chặn kịp thời các hoạt động gián điệp mạng, phá hoại cơ sở hạ tầng trọng yếu, truyền bá thông tin xấu độc hoặc xâm phạm chủ quyền số quốc gia. Ngoài ra, lực lượng Công an cần tăng cường phối hợp với các cơ quan quản lý nhà nước, doanh nghiệp cung cấp dịch vụ số và cộng đồng nghiên cứu để hoàn thiện năng lực giám sát, đồng thời xây dựng các Trung tâm điều hành an ninh mạng cấp bộ, cấp tỉnh nhằm phát hiện sớm các mối nguy và tổ chức phản ứng nhanh, góp phần giữ vững ổn định chính trị, bảo vệ quyền và lợi ích chính đáng của người dân trong thời đại số.

(2) Thiết lập hệ thống cảnh báo sớm, trung tâm điều phối an ninh dữ liệu quốc gia để theo dõi, phát hiện và phản ứng kịp thời với các cuộc tấn công hoặc rủi ro bảo mật diện rộng

Việc thiết lập hệ thống cảnh báo sớm và trung tâm điều phối an ninh dữ liệu quốc gia là giải pháp chiến lược nhằm chủ động bảo vệ an toàn không gian mạng quốc gia trong bối cảnh tấn công mạng ngày càng tinh vi, có tính chất đa tầng và mang yếu tố xuyên quốc gia. Giải pháp này yêu cầu xây dựng một hệ thống kỹ thuật tích hợp các cảm biến an ninh mạng, công nghệ phân tích dữ liệu lớn (big data), trí tuệ nhân tạo (AI) và học máy (machine learning) để theo dõi liên tục các hành vi bất thường, phát hiện sớm các dấu hiệu tấn công mạng, rò rỉ dữ liệu, lỗ hổng bảo mật và những hoạt động đáng ngờ có khả năng gây ảnh hưởng diện rộng đến hệ thống thông tin quốc gia. Hệ thống cảnh báo sớm phải có khả năng thu thập dữ liệu từ nhiều nguồn phân tán trên toàn quốc, từ các tổ chức, cơ quan nhà nước, doanh nghiệp, hạ tầng số thiết yếu cho đến các điểm nút trong hệ thống hạ tầng mạng viễn thông và internet. Dữ liệu được thu thập phải đảm bảo tính toàn vẹn, liên tục và có độ tin cậy cao, đồng thời phải tuân thủ nghiêm ngặt các quy định pháp lý về bảo vệ dữ liệu cá nhân và an toàn thông tin.

Để hệ thống cảnh báo sớm hoạt động hiệu quả, cần xây dựng bộ tiêu chí phân loại các mức độ nguy cơ và rủi ro an ninh mạng, từ đó thiết lập ngưỡng kích hoạt cảnh báo tự động cho từng loại hình sự cố như tấn công từ chối dịch vụ phân tán (DDoS), tấn công bằng mã độc tống tiền (ransomware), tấn công chuỗi cung ứng phần mềm (supply chain attack), xâm nhập bất hợp pháp vào hệ thống điều hành trung tâm (APT), hoặc tấn công có chủ đích nhắm đến các hệ thống quan trọng như tài chính, năng lượng, giao thông, quốc phòng, y tế và dữ liệu dân cư. Cảnh báo khi được kích hoạt cần được định tuyến đến các đầu mối kỹ thuật chuyên trách tại từng bộ, ngành, địa phương và tổ chức có liên quan để phản ứng

kịp thời. Việc chuẩn hóa nội dung, định dạng, tốc độ truyền tải và cơ chế phân loại cảnh báo cũng là yêu cầu bắt buộc nhằm đảm bảo thông tin đến đúng người, đúng nơi, đúng thời điểm, tránh gây nhiễu loạn hệ thống hoặc làm quá tải năng lực xử lý sự cố.

Mô hình các yêu cầu về quản lý an toàn thông tin. Ảnh minh họa. Nguồn từ Internet.

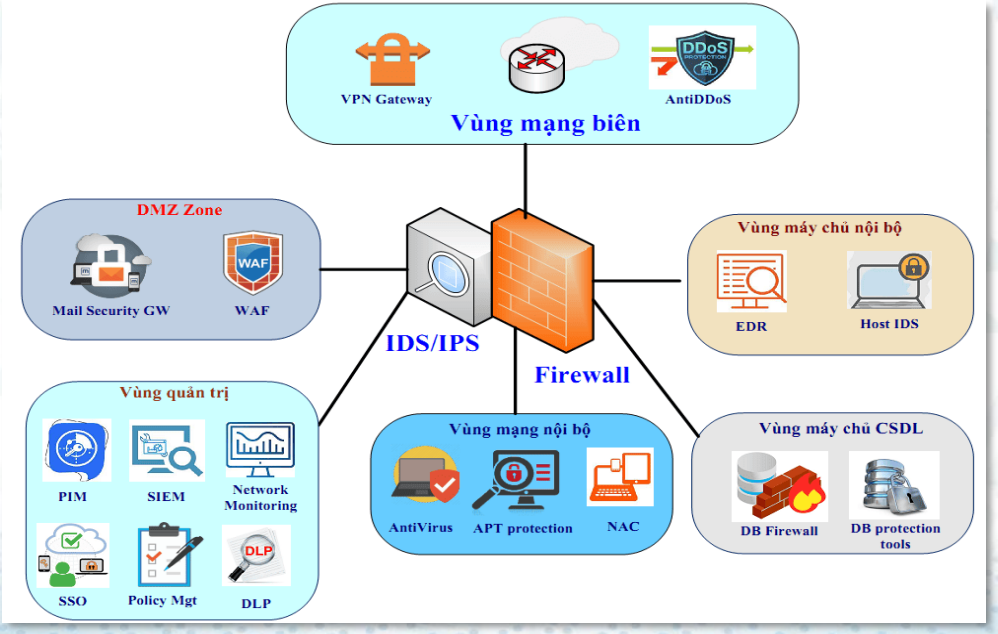
Trung tâm điều phối an ninh dữ liệu quốc gia đóng vai trò trung tâm chỉ huy tổng hợp, là đầu mối tiếp nhận, phân tích, đánh giá và chỉ đạo điều phối phản ứng liên ngành đối với các tình huống khẩn cấp về an ninh mạng và dữ liệu. Trung tâm này cần được thiết lập trực thuộc Chính phủ hoặc ủy quyền cho cơ quan chuyên trách về an ninh mạng quốc gia, được trang bị hạ tầng kỹ thuật tiên tiến, đội ngũ chuyên gia cao cấp và có quyền điều động, huy động các lực lượng ứng cứu sự cố cấp vùng và cấp địa phương. Trung tâm phải vận hành liên tục 24/7 với các quy trình chuẩn trong việc tiếp nhận tín hiệu cảnh

báo, đánh giá cấp độ rủi ro, lựa chọn phương án xử lý phù hợp, phối hợp liên ngành để dập tắt hoặc ngăn chặn sự cố lan rộng. Cần xây dựng hệ thống CSDL toàn diện về các loại mã độc, kịch bản tấn công, lỗ hổng phổ biến, tập hợp các tình huống mẫu và bài học kinh nghiệm trong nước và quốc tế để hỗ trợ ra quyết định trong thời gian thực.

Việc xây dựng trung tâm điều phối đòi hỏi phải ban hành đầy đủ khung pháp lý về mô hình tổ chức, chức năng, nhiệm vụ, quyền hạn, quan hệ phối hợp và trách nhiệm giữa các chủ thể tham gia. Trong đó, cần làm rõ mối liên hệ giữa trung tâm điều phối với các đơn vị bảo mật chuyên ngành của các bộ, ngành; xác định rõ đầu mối điều phối thông tin tại cấp bộ, ngành, địa phương và doanh nghiệp; thiết lập cơ chế phân quyền, chia sẻ dữ liệu, phối hợp xử lý sự cố có kiểm soát. Cơ chế vận hành trung tâm phải đặt yếu tố bảo mật lên hàng đầu, bảo đảm thông tin nhạy cảm, dữ liệu mật không bị rò rỉ trong quá trình xử lý. Việc ứng dụng công nghệ điện toán đám mây có thể giúp tăng tốc độ xử lý, nâng cao khả năng mở rộng và tích hợp, song cũng đặt ra yêu cầu nghiêm ngặt về bảo vệ dữ liệu tại các tầng hạ tầng ảo hóa.

Trung tâm điều phối cần tích hợp hệ thống hỗ trợ ra quyết định và mô hình mô phỏng các kịch bản tấn công để cung cấp cho lãnh đạo cấp cao các phương án xử lý khác nhau, ước lượng tác động và đánh giá hiệu quả của các giải pháp ứng phó trong thời gian thực. Cần xây dựng cơ chế báo cáo nhanh, phân loại các sự cố theo tiêu chí quốc gia, liên ngành, vùng và địa phương để phản ứng kịp thời theo thẩm quyền xử lý. Ngoài ra, trung tâm cần đảm bảo chức năng đào tạo, huấn luyện định kỳ cho đội ngũ nhân lực các cấp, tổ chức diễn tập thực chiến theo các tình huống tấn công mạng lớn nhằm rèn luyện năng lực ứng phó linh hoạt, phối hợp liên ngành hiệu quả. Việc kết nối với các trung tâm cảnh báo và điều phối quốc tế là cần thiết để nắm bắt sớm các mối đe dọa mới nổi, nhận diện hành vi tấn công có nguồn gốc nước ngoài, nâng cao năng lực phòng thủ chủ động cho hệ thống quốc gia.

Một phần quan trọng của hệ thống cảnh báo sớm và trung tâm điều phối là hạ tầng chia sẻ thông tin cảnh báo, phân tích mối đe dọa (Threat Intelligence Sharing Platform – TISP) cho phép các đơn vị gửi, nhận, phân tích và cập nhật các cảnh báo, chỉ báo tấn công (IoC), hành vi bất thường và mẫu mã độc theo thời gian thực. TISP cần được thiết kế mở, có khả năng tích hợp với các hệ thống SIEM (Security Information and Event Management) tại các tổ chức, cho phép tự động hóa phân tích và kích hoạt phản ứng, hạn chế sự can thiệp thủ công trong xử lý các tình huống thông thường. Hệ thống cần có cơ chế xác thực, phân quyền truy cập, ghi log đầy đủ, đảm bảo tính truy vết và minh bạch trong các hoạt động chia sẻ, phối hợp và phản hồi.



Mô hình tham chiếu về giải pháp và công nghệ. Ảnh minh họa. Nguồn từ Internet.

Để triển khai đồng bộ, cần tổ chức khảo sát, phân tích hiện trạng và nhu cầu thực tế tại các bộ, ngành, địa phương, doanh nghiệp trọng yếu để xác định các đầu mối tham gia mạng lưới cảnh báo sớm và điều phối. Từ đó, tiến hành chuẩn hóa hạ tầng kỹ thuật, xây dựng lộ trình kết nối hệ thống với trung tâm điều phối quốc gia theo từng giai đoạn, ưu tiên các lĩnh vực trọng yếu như y tế, ngân hàng, giao thông, năng lượng và hạ tầng số quốc gia. Việc lựa chọn công nghệ cần bảo đảm tính mở, khả năng mở rộng và tương thích lâu dài, tránh phụ thuộc vào nhà cung cấp hoặc công nghệ độc quyền từ nước ngoài, hạn chế rủi ro trong các kịch bản chiến lược hoặc khủng hoảng địa chính trị.

Song song với việc xây dựng hạ tầng, cần tổ chức tuyên truyền, nâng cao nhận thức cho đội ngũ cán bộ lãnh đạo, quản lý và kỹ thuật tại các tổ chức tham gia về ý nghĩa, mục tiêu, cơ chế vận hành và vai trò của hệ thống cảnh báo – điều phối quốc gia. Việc đào tạo không chỉ tập trung vào kỹ năng xử lý kỹ thuật mà còn chú trọng năng lực phân tích tình huống, đánh giá rủi ro và ra quyết định trong điều kiện khẩn cấp. Cần ban hành các quy định về trách nhiệm pháp lý, kỹ thuật, quy trình phối hợp, chế tài xử lý đối với các đơn vị không thực hiện đúng quy định cảnh báo, trì hoãn hoặc giấu giếm thông tin dẫn đến lan rộng thiệt hại.

Trong bối cảnh không gian mạng trở thành chiến trường phi truyền thống, việc thiết lập hệ thống cảnh báo sớm và trung tâm điều phối an ninh dữ liệu quốc gia là nhiệm vụ mang tính sống còn trong chiến lược bảo vệ chủ quyền số quốc gia. Lực lượng Công an nhân dân, với vai trò nòng cốt trong đảm bảo an ninh quốc gia và trật tự an toàn xã hội, cần chủ động tham mưu xây dựng khung pháp lý, phối hợp tổ chức vận hành trung tâm điều phối an ninh dữ liệu; tham gia trực tiếp vào mạng

lưới cảnh báo sớm, nắm chắc tình hình và phản ứng nhanh trước các mối đe dọa an ninh phi truyền thống. Đồng thời, lực lượng Công an cần phát triển năng lực kỹ thuật, bố trí nguồn lực con người chất lượng cao, chủ động thực hiện các chiến dịch điều tra, truy vết tấn công mạng, xử lý các đối tượng vi phạm pháp luật trong không gian mạng và tham gia các diễn đàn hợp tác quốc tế về an ninh dữ liệu nhằm nâng cao vị thế và năng lực bảo vệ Tổ quốc trong kỷ nguyên số.

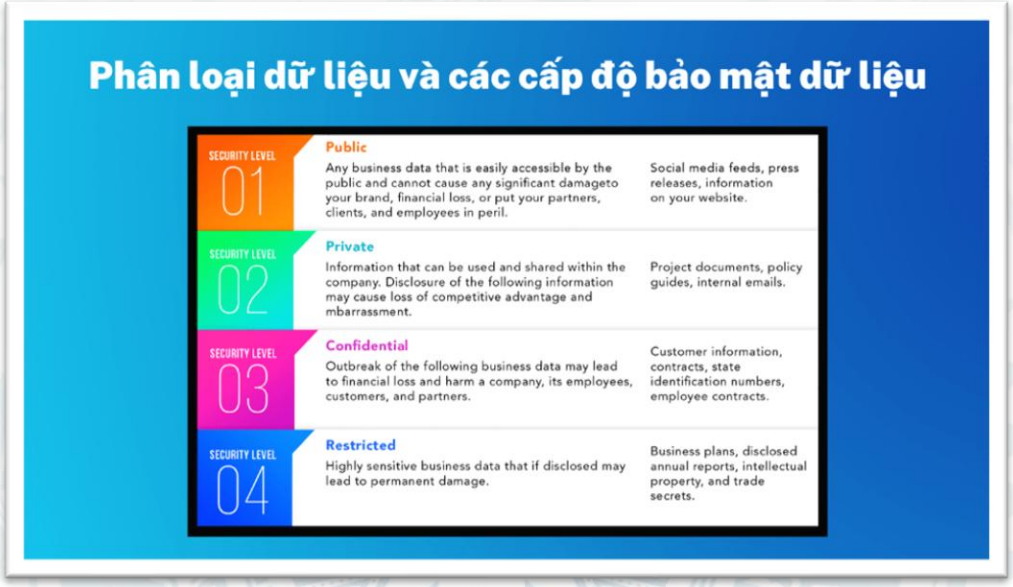
2.2. Nhóm 2: Nhóm các biện pháp phòng ngừa, ngăn chặn và xử lý rủi ro dữ liệu

2.2.1. Xây dựng và áp dụng hệ thống phân loại, phân tầng dữ liệu theo mức độ nhạy cảm, rủi ro và giá trị khai thác nhằm bảo đảm quản lý theo cấp độ an toàn thông tin tương ứng

Xây dựng và áp dụng hệ thống phân loại, phân tầng dữ liệu theo mức độ nhạy cảm, rủi ro và giá trị khai thác là một giải pháp quan trọng trong bối cảnh dữ liệu ngày càng trở thành nguồn lực thiết yếu cho phát triển kinh tế, xã hội và bảo đảm quốc phòng – an ninh quốc gia. Việc triển khai hệ thống này giúp định hướng rõ ràng cho các hoạt động thu thập, lưu trữ, khai thác và bảo vệ dữ liệu, đồng thời là cơ sở để thiết lập các biện pháp bảo mật phù hợp với từng cấp độ dữ liệu. Để thực hiện thành công nhiệm vụ này, trước hết cần xác lập một bộ tiêu chí khoa học, đồng bộ và linh hoạt nhằm định danh, đánh giá và phân loại dữ liệu theo các yếu tố cốt lõi như mức độ nhạy cảm *(tác động đến quyền riêng tư cá nhân, an ninh quốc gia, trật tự công cộng)*, mức độ rủi ro *(khả năng bị truy cập trái phép, tấn công, thất lạc hoặc bị khai thác sai mục đích)*, cũng như giá trị khai thác *(giá trị kinh tế, giá trị trong điều hành quản lý, giá trị xã hội)*. Các tiêu chí này cần được ban hành kèm theo hướng dẫn chi tiết áp dụng cho từng ngành, lĩnh vực, bảo đảm tính khả thi và phù hợp với thực tiễn triển khai ở các cơ quan, tổ chức.

Việc phân tầng dữ liệu cần dựa trên các cấp độ bảo mật, tối thiểu gồm bốn mức: dữ liệu công khai, dữ liệu hạn chế, dữ liệu mật và dữ liệu tuyệt mật. Mỗi cấp độ sẽ tương ứng với các quy định về quyền truy cập, quy trình xử lý, phương thức lưu trữ, các biện pháp bảo mật vật lý và kỹ thuật khác nhau. Đối với dữ liệu công khai, cần thiết lập cơ chế chuẩn hóa và số hóa để phục vụ mục tiêu chia sẻ và khai thác rộng rãi trong các hoạt động cung cấp dịch vụ công và phát triển kinh tế - xã hội. Với dữ liệu hạn chế, cần kiểm soát quyền truy cập theo nguyên tắc phân quyền, phân cấp chặt chẽ. Với dữ liệu mật và tuyệt mật, bắt buộc áp dụng các biện pháp bảo mật cao cấp như mã hóa, kiểm soát truy cập đa lớp, theo dõi nhật ký truy cập, giám sát an toàn mạng thời gian thực, lưu trữ trên hệ thống biệt lập có chứng nhận bảo mật cấp cao và có phương án khôi phục dữ liệu trong tình huống khẩn cấp. Quy trình phân tầng cần được thực hiện đồng bộ, xuyên suốt vòng đời dữ liệu, từ khi tạo lập đến khi lưu trữ, xử lý và tiêu hủy.

Để bảo đảm tính nhất quán, toàn diện và hiệu quả, cần xây dựng một hệ thống danh mục chuẩn hóa dữ liệu dùng chung ở cấp quốc gia, với khả năng phân loại và nhận diện dữ liệu theo từng chủng loại, lĩnh vực và đơn vị phát sinh. Danh mục này sẽ đóng vai trò là "từ điển dữ liệu quốc gia", giúp thống nhất định danh dữ liệu giữa các cơ quan, tổ chức và hệ thống thông tin, từ đó làm cơ sở để phân loại, phân tầng, chia sẻ và quản lý dữ liệu theo hướng minh bạch, hiệu quả, bảo đảm đúng mục đích và đối tượng sử dụng. Việc xây dựng danh mục cần kết hợp cả phương pháp thủ công và ứng dụng công nghệ trí tuệ nhân tạo (AI) để tự động phát hiện và gợi ý phân loại đối với các loại dữ liệu chưa được định danh. Ngoài ra, cần có cơ chế thường xuyên rà soát, cập nhật danh mục khi có phát sinh mới về chủng loại dữ liệu hoặc thay đổi trong giá trị, tính nhạy cảm và rủi ro đi kèm với dữ liệu.



Ảnh minh hoạ

Một nhiệm vụ trọng tâm là thiết kế và triển khai các công cụ kỹ thuật để hỗ trợ tự động hóa việc phân loại và phân tầng dữ liệu trong các hệ thống thông tin và cơ sở dữ liệu lớn. Các công cụ này cần tích hợp trực tiếp vào quy trình vận hành hệ thống, bảo đảm dữ liệu khi được tạo ra hoặc tiếp nhận đều được gắn nhãn và xác định mức độ nhạy cảm, rủi ro phù hợp. Việc tự động phân loại cũng cần đi kèm cơ chế xác thực, hiệu chỉnh thủ công do con người thực hiện trong các tình huống đặc biệt hoặc dữ liệu có độ phức tạp cao. Cần phát triển bộ phần mềm kiểm soát truy cập theo cấp độ dữ liệu, có khả năng liên thông

với hệ thống định danh điện tử quốc gia và các hệ thống xác thực đa yếu tố, nhằm bảo đảm chỉ người có thẩm quyền, đúng mục đích mới được truy cập dữ liệu ở cấp độ tương ứng. Ngoài ra, cần phát triển các thuật toán kiểm tra và phát hiện rò rỉ dữ liệu tự động, gắn với cảnh báo sớm về nguy cơ rủi ro thông tin.

Bên cạnh việc xây dựng hệ thống phân tầng, cần tổ chức đào tạo, tuyên truyền nâng cao nhận thức cho cán bộ, công chức, viên chức và người lao động trong hệ thống chính trị về vai trò, ý nghĩa và yêu cầu bảo vệ dữ liệu theo cấp độ. Các chương trình đào tạo cần gắn lý thuyết với thực hành, hướng tới việc sử dụng thành thạo các công cụ phân loại, kiểm soát truy cập và ứng phó sự cố dữ liệu. Cần thiết lập hệ thống kiểm tra, đánh giá định kỳ mức độ tuân thủ phân tầng dữ liệu của các đơn vị, đồng thời xác lập cơ chế giám sát liên ngành, bảo đảm minh bạch và chế tài xử lý đối với hành vi vi phạm phân tầng dữ liệu. Cũng cần xem xét đưa nội dung bảo vệ dữ liệu theo cấp độ vào tiêu chí đánh giá mức độ an toàn thông tin mạng, từ đó hình thành hệ thống đo lường hiệu quả quản lý dữ liệu của từng cơ quan, đơn vị.

Ảnh minh hoạ

Công tác pháp lý đóng vai trò cốt lõi trong việc thực thi giải pháp phân loại, phân tầng dữ liệu. Trước mắt, cần hoàn thiện hành lang pháp lý bao gồm quy định chi tiết về tiêu chí phân loại, trách nhiệm chủ quản dữ liệu, quyền và nghĩa vụ của người sử dụng, chế tài xử lý hành vi vi phạm, đặc biệt là các hành vi tiết lộ, chia sẻ hoặc chuyển giao dữ liệu sai quy định về cấp độ. Các quy định này cần được xây dựng phù hợp với Luật Dữ liệu, Luật An toàn thông tin mạng, Luật Bảo vệ bí mật Nhà nước, đồng thời đảm bảo hài hòa với các điều ước quốc tế mà Việt Nam là thành viên. Cần thiết lập cơ chế kiểm tra chéo giữa các cơ quan trong việc phân loại và bảo vệ dữ liệu, nhất là đối với dữ liệu chia sẻ giữa các ngành, các cấp hoặc chia sẻ

ra ngoài lãnh thổ. Việc phân loại dữ liệu xuyên biên giới cần được kiểm soát nghiêm ngặt, có đánh giá rủi ro toàn diện và yêu cầu minh bạch về mục đích, phương thức và đối tượng tiếp cận dữ liệu.

Đại tá Phạm Công Nguyên, Cục trưởng Cục Cảnh sát QLHC về TTXH phát biểu tại lễ công bố Ra mắt Trung tâm nghiên cứu, ứng dụng dữ liệu dân cư, căn cước công dân. Ảnh minh họa. Nguồn từ Internet.

Để tăng cường hiệu lực của hệ thống phân tầng dữ liệu, cần đầu tư xây dựng một nền tảng công nghệ quản trị dữ liệu tập trung ở cấp quốc gia, đóng vai trò điều phối hoạt động phân loại, phân tầng, kiểm soát truy cập và cảnh báo rủi ro. Nền

tảng này cần tích hợp các dịch vụ AI hỗ trợ nhận diện dữ liệu, blockchain để giám sát chuỗi hành trình dữ liệu, công nghệ mã hóa tiên tiến để bảo vệ nội dung nhạy cảm, cùng với các giao diện lập trình ứng dụng (API) bảo đảm liên thông với hệ thống thông tin của các bộ, ngành, địa phương. Việc xây dựng nền tảng cần theo hướng mở, linh hoạt, có khả năng mở rộng và nâng cấp trong tương lai, đồng thời bảo đảm tuân thủ đầy đủ các tiêu chuẩn kỹ thuật về an toàn thông tin và bảo vệ dữ liệu cá nhân. Chú trọng đến việc ứng dụng hệ thống phân tầng dữ liệu trong xây dựng Chính phủ số, đô thị thông minh, dịch vụ công trực tuyến và các hoạt động chuyển đổi số toàn diện. Việc tích hợp chức năng phân tầng dữ liệu ngay từ giai đoạn thiết kế kiến trúc hệ thống thông tin giúp bảo đảm dữ liệu được kiểm soát và bảo vệ ngay từ điểm khởi phát, hạn chế rủi ro từ lỗi hệ thống hoặc thao tác con người. Cần đẩy mạnh áp dụng các tiêu chuẩn quốc tế về quản trị dữ liệu như ISO/IEC 27001, ISO/IEC 27701 để bảo đảm tính tương thích và tin cậy trong chia sẻ, kết nối dữ liệu với các đối tác trong và ngoài nước, từ đó nâng cao năng lực cạnh tranh số của quốc gia.

Từ góc độ lực lượng Công an nhân dân, việc triển khai hệ thống phân loại, phân tầng dữ liệu có ý nghĩa chiến lược trong việc bảo vệ an ninh quốc gia, đấu tranh phòng chống tội phạm và bảo đảm trật tự an toàn xã hội. Công an các đơn vị, địa phương cần tổ chức rà soát toàn bộ hệ thống cơ sở dữ liệu hiện có, phân loại và gắn cấp độ bảo mật cho từng nhóm dữ liệu nghiệp vụ, dữ liệu cá nhân, dữ liệu điều tra, dữ liệu giám sát và dữ liệu chia sẻ liên ngành. Cần áp dụng công nghệ bảo mật chuyên sâu để bảo vệ dữ liệu thuộc danh mục bí mật Nhà nước và dữ liệu điều tra hình sự. Lực lượng Công an cần tham gia xây dựng và vận hành các nền tảng quản lý phân tầng dữ liệu quốc gia, chủ động phát hiện, ngăn chặn các hành vi truy cập trái phép, thu thập, tiết lộ hoặc buôn bán dữ liệu nhạy cảm. Ngoài ra, cần tăng cường công tác đào tạo cán bộ kỹ thuật dữ liệu chuyên trách, có khả năng ứng phó với các cuộc tấn công mạng có chủ đích, đồng thời phối hợp với các đơn vị chức năng

để bảo đảm dữ liệu phục vụ nghiệp vụ được kiểm soát chặt chẽ, an toàn tuyệt đối trong mọi tình huống. Việc thực hiện tốt nhiệm vụ này sẽ góp phần quan trọng vào việc xây dựng lực lượng Công an chính quy, tinh nhuệ, hiện đại, đủ sức bảo vệ an ninh, an toàn dữ liệu quốc gia trong kỷ nguyên số.

2.2.2. Tổ chức đào tạo chuyên sâu, huấn luyện định kỳ và nâng cao nhận thức toàn diện về an ninh dữ liệu cho cán bộ kỹ thuật, người dùng cuối và lãnh đạo tổ chức

Việc tổ chức đào tạo chuyên sâu, huấn luyện định kỳ và nâng cao nhận thức toàn diện về an ninh dữ liệu cho cán bộ kỹ thuật, người dùng cuối và lãnh đạo tổ chức là một giải pháp then chốt nhằm xây dựng năng lực nội tại và phát triển một hệ sinh thái an toàn thông tin bền vững. Trong bối cảnh số hóa diễn ra nhanh chóng và các cuộc tấn công mạng ngày càng tinh vi, việc chỉ dựa vào công nghệ là chưa đủ để bảo đảm an toàn dữ liệu. Nhân tố con người – với kiến thức, kỹ năng và ý thức bảo mật – mới thực sự là tuyến phòng thủ đầu tiên và quan trọng nhất. Đào tạo chuyên sâu không chỉ dừng ở việc truyền đạt kiến thức nền tảng mà cần tập trung vào việc nâng cao tư duy phân tích, khả năng đánh giá rủi ro, thực hành xử lý tình huống và ứng phó sự cố trong môi trường thực tế, phù hợp với từng nhóm đối tượng.

Ảnh minh họa. Nguồn từ Internet

Đối với đội ngũ cán bộ kỹ thuật, nội dung đào tạo cần bao phủ toàn diện các khía cạnh từ cấu hình hệ thống bảo mật, vận hành thiết bị an toàn mạng, triển khai các biện pháp mã hóa, xác thực, phân quyền truy cập đến việc giám sát, phân tích nhật ký hệ thống và điều tra kỹ thuật số. Họ cần được cập nhật liên tục các kỹ thuật tấn công mới, lỗ hổng bảo mật phổ biến và biện pháp khắc phục. Các chương trình đào tạo nên kết hợp lý thuyết với thực hành, mô phỏng tình huống tấn công giả định để tăng cường khả năng phản ứng nhanh và xử lý đúng quy trình. Đặc biệt, cần tổ chức các cuộc diễn tập an toàn thông tin định kỳ với nhiều cấp độ, giúp cán bộ kỹ thuật làm quen với môi trường có áp lực và nhiều biến động. Những cán bộ phụ

trách bảo mật cấp cao cần được huấn luyện nâng cao về chiến lược phòng thủ mạng, kiến trúc hệ thống an toàn, quy trình quản trị rủi ro và phối hợp ứng cứu khi xảy ra sự cố lớn.

Đối với người dùng cuối – thường là cán bộ hành chính, nhân viên văn phòng, giáo viên, bác sĩ, công nhân – cần tập trung đào tạo kỹ năng cơ bản về nhận diện các mối đe dọa mạng như email lừa đảo, đường dẫn độc hại, phần mềm gián điệp, cách sử dụng mật khẩu mạnh, tránh chia sẻ dữ liệu cá nhân, bảo vệ thiết bị di động, và cách phản hồi khi nghi ngờ bị xâm nhập. Việc đào tạo nên được tổ chức thường xuyên, kết hợp hình thức trực tiếp và trực tuyến, có nội dung đơn giản, dễ hiểu, tình huống thực tiễn, mang tính gợi mở và tương tác cao. Quan trọng hơn cả là phải xây dựng được văn hóa bảo mật trong cơ quan, tổ chức để người dùng cuối không xem đó là nghĩa vụ bị ép buộc mà là hành vi tự nhiên, có trách nhiệm với hệ thống chung. Các hình thức kiểm tra định kỳ, cấp chứng nhận sau đào tạo, đưa tiêu chí an toàn thông tin vào đánh giá thi đua sẽ là động lực thúc đẩy người dùng cuối chủ động học tập và tuân thủ quy định.

Với nhóm lãnh đạo tổ chức – những người giữ vai trò định hướng, quản lý và ra quyết định – cần được trang bị kiến thức về quản trị an toàn dữ liệu ở cấp độ chiến lược. Họ cần hiểu rõ tầm quan trọng của dữ liệu như một tài sản cốt lõi, các rủi ro về pháp lý, tài chính, uy tín do mất mát hay rò rỉ thông tin gây ra, cũng như nghĩa vụ phải tuân thủ các tiêu chuẩn, quy định về bảo mật. Việc đào tạo cho lãnh đạo nên tập trung vào kỹ năng ra quyết định trong bối cảnh khủng hoảng an ninh mạng, xây dựng và phê duyệt các chính sách bảo mật, phân bổ nguồn lực hợp lý cho công tác an toàn thông tin, và cách giám sát triển khai hiệu quả các kế hoạch ứng phó. Họ cũng cần được hướng dẫn về mô hình quản trị dữ liệu, vai trò của cán bộ phụ trách an toàn thông tin, cơ chế phối hợp với các cơ quan chức năng và đơn vị ứng cứu khẩn cấp. Chỉ khi lãnh đạo tổ chức có nhận thức và hành động đúng, các hoạt động bảo vệ dữ liệu mới được triển khai đồng bộ, lâu dài và hiệu quả.

Điểm cầu tỉnh Cà Mau tại hội nghị quán triệt triển khai Kế hoạch số 02-KH/BCĐTW ngày 19/6/2025 về việc thúc đẩy chuyển đổi số liên thông, đồng bộ, nhanh, hiệu quả đáp ứng yêu cầu sắp xếp tổ chức bộ máy của hệ thống chính trị

Chương trình đào tạo và huấn luyện về an ninh dữ liệu cần được thiết kế có hệ thống, bài bản, theo lộ trình từ cơ bản đến nâng cao, được cập nhật liên tục theo tình hình mới và yêu cầu phát triển công nghệ. Cơ sở xây dựng nội dung đào tạo cần dựa trên các tiêu chuẩn quốc tế như ISO/IEC 27001, NIST SP 800 series, cũng như quy định pháp luật Việt Nam về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng. Việc đánh giá nhu cầu đào tạo, khảo sát năng lực hiện tại và phân loại đối tượng

học viên là khâu quan trọng nhằm đảm bảo nội dung phù hợp, tránh dàn trải, kém hiệu quả. Các đơn vị có thể phối hợp với các trường đại học, viện nghiên cứu, tổ chức quốc tế, chuyên gia độc lập để xây dựng giáo trình chất lượng, cập nhật nhanh xu hướng và kinh nghiệm quốc tế.

Ngoài ra, cần chú trọng áp dụng công nghệ vào hoạt động đào tạo như sử dụng các nền tảng e-learning, lớp học ảo, phần mềm mô phỏng, trò chơi hóa nội dung nhằm tăng sự hấp dẫn và tính linh hoạt. Một số công nghệ như trí tuệ nhân tạo (AI) có thể được tích hợp để cá nhân hóa chương trình đào tạo, tự động đánh giá tiến độ học tập và đưa ra gợi ý cải thiện. Các tổ chức nên duy trì cơ chế theo dõi, đánh giá hiệu quả sau đào tạo thông qua bài kiểm tra, khảo sát mức độ áp dụng vào công việc thực tế, cũng như thống kê số lượng sự cố an toàn thông tin được ngăn chặn nhờ nhận thức người dùng được nâng cao.

Việc xây dựng chính sách nội bộ bắt buộc tham gia đào tạo định kỳ về an toàn dữ liệu là cần thiết để đảm bảo tính tuân thủ và duy trì liên tục kiến thức. Cần có chế tài cụ thể đối với cá nhân không hoàn thành khóa học hoặc vi phạm quy định bảo mật sau đào tạo. Đồng thời, các tổ chức nên duy trì các chiến dịch truyền thông nội bộ thường xuyên như gửi bản tin an toàn thông tin, áp phích cảnh báo, tổ chức tuần lễ an ninh mạng, cuộc thi nhận diện lỗ hổng để tạo động lực học tập và duy trì sự chú ý đến vấn đề bảo mật. Văn hóa an ninh dữ liệu phải được xây dựng dựa trên sự tham gia của mọi thành viên, không chỉ giới hạn ở bộ phận kỹ thuật hay an toàn thông tin.

Việc tổ chức đào tạo và huấn luyện còn có ý nghĩa đặc biệt trong việc phòng ngừa các hành vi vô ý làm rò rỉ dữ liệu do thiếu hiểu biết hoặc chủ quan. Những sự cố phổ biến như gửi nhầm email, cài phần mềm không rõ nguồn gốc, chia sẻ mật khẩu nội bộ, truy cập Wi-Fi công cộng thiếu bảo mật… hoàn toàn có thể phòng tránh nếu người dùng được giáo dục đúng

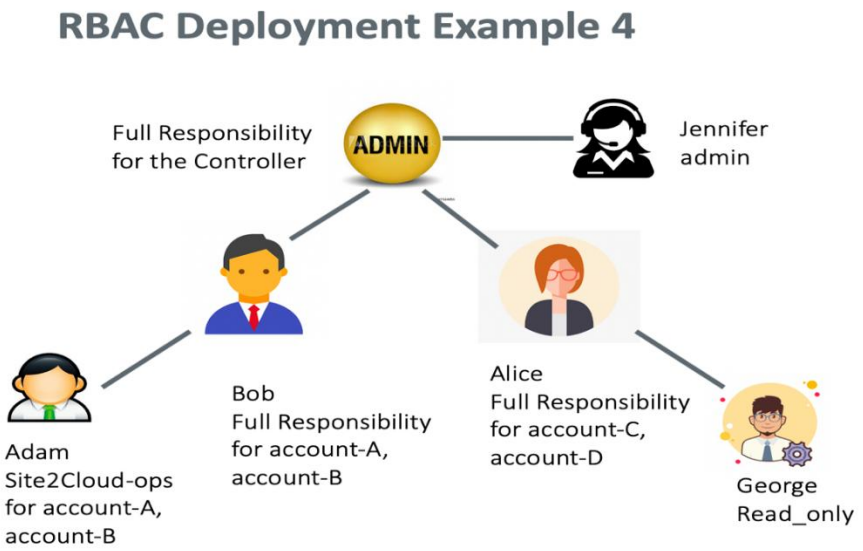
đắn. Đặc biệt trong các lĩnh vực nhạy cảm như y tế, tài chính, hành chính công, giáo dục, việc bảo vệ thông tin cá nhân và dữ liệu quan trọng càng cần có chuẩn mực cao, gắn với đạo đức nghề nghiệp và quy định pháp luật. Đây chính là nền tảng để xây dựng lòng tin với người dân và đối tác, cũng như tăng cường khả năng phục hồi của tổ chức khi xảy ra khủng hoảng.

Từ góc độ thực thi, việc tổ chức đào tạo về an ninh dữ liệu cần sự phối hợp chặt chẽ giữa các bộ phận trong tổ chức như nhân sự, kỹ thuật, pháp chế, truyền thông và lãnh đạo cấp cao. Cần phân công rõ ràng đơn vị đầu mối chịu trách nhiệm tổ chức đào tạo, lựa chọn đối tác uy tín, xây dựng kế hoạch chi tiết, xác định ngân sách phù hợp và kiểm tra giám sát định kỳ. Cần đảm bảo rằng chương trình đào tạo không chỉ diễn ra theo hình thức đối phó mà phải mang lại giá trị thực chất, góp phần nâng cao năng lực tổng thể của tổ chức trong bảo vệ tài sản số.

Đối với lực lượng Công an nhân dân, nhiệm vụ tổ chức đào tạo chuyên sâu và nâng cao nhận thức về an ninh dữ liệu mang ý nghĩa sống còn trong việc bảo vệ chủ quyền số quốc gia và an ninh trật tự trên không gian mạng. Trong bối cảnh các đối tượng phạm tội ngày càng triệt để lợi dụng công nghệ, lực lượng Công an không chỉ cần cán bộ kỹ thuật giỏi, mà còn cần sự vào cuộc của toàn thể cán bộ, chiến sĩ với nhận thức đúng đắn, kỹ năng chuẩn hóa và tinh thần trách nhiệm cao. Việc đào tạo chuyên sâu giúp lực lượng kỹ thuật xử lý hiệu quả các sự cố, truy vết tội phạm mạng và bảo vệ hệ thống dữ liệu trọng yếu. Việc huấn luyện định kỳ giúp lực lượng nắm bắt xu hướng tấn công mới, nâng cao khả năng ứng phó linh hoạt. Việc tuyên truyền, giáo dục nhận thức cho toàn lực lượng tạo thành lớp áo giáp kiên cố, ngăn chặn sự xâm nhập từ bên trong. Quan trọng hơn, thông qua đào tạo, lực lượng Công an sẽ đóng vai trò nòng cốt trong việc phổ biến kiến thức bảo mật đến toàn xã hội, định hướng cho các tổ chức, doanh nghiệp và người dân tự giác thực hiện trách nhiệm bảo vệ dữ liệu, góp phần xây dựng môi trường mạng an toàn, lành mạnh, chủ động ứng phó với mọi nguy cơ an ninh phi truyền thống.

2.2.3. Áp dụng cơ chế xác thực đa yếu tố (MFA) để tăng cường độ tin cậy và kiểm soát truy cập theo vai trò (RBAC) để ngăn chặn truy cập trái phép vào hệ thống dữ liệu nhạy cảm

Việc đảm bảo an toàn và bảo mật hệ thống dữ liệu ngày càng trở nên cấp thiết trong bối cảnh các cuộc tấn công mạng có xu hướng gia tăng cả về tần suất lẫn mức độ tinh vi. Một trong những giải pháp cốt lõi để giảm thiểu nguy cơ truy cập trái phép vào hệ thống dữ liệu nhạy cảm chính là áp dụng cơ chế xác thực đa yếu tố (MFA) kết hợp với kiểm soát truy cập theo vai trò (RBAC). Cơ chế xác thực đa yếu tố không đơn thuần dựa trên một yếu tố xác minh như mật khẩu, mà yêu cầu người dùng cung cấp thêm các yếu tố bổ sung như mã xác minh gửi qua thiết bị di động, sinh trắc học (vân tay, khuôn mặt), thẻ cứng mã hóa hoặc thiết bị xác thực phần cứng chuyên dụng. Việc này giúp tăng đáng kể độ tin cậy trong việc xác thực người dùng, từ đó hạn chế nguy cơ tấn công bằng hình thức đánh cắp danh tính hay sử dụng mật khẩu rò rỉ. Đồng thời, kiểm soát truy cập theo vai trò là cơ chế phân quyền rõ ràng dựa trên chức năng, nhiệm vụ và quyền hạn của người dùng trong hệ thống, giúp quản trị viên kiểm soát chính xác ai được phép truy cập vào loại dữ liệu nào, vào thời điểm nào, trong phạm vi nào và với mục đích gì.



Ảnh minh hoạ

Việc triển khai giải pháp này đòi hỏi xây dựng khung chính sách quản lý truy cập toàn diện, trong đó quy định cụ thể quy trình cấp quyền, giám sát, thu hồi quyền truy cập theo nguyên tắc "ít quyền nhất" (least privilege). Chính sách này cần được cụ thể hóa trong các quy chế nội bộ, đảm bảo mọi hành động truy cập vào dữ liệu đều được ghi nhận và kiểm tra định kỳ. Trong môi trường quản trị dữ liệu hiện đại, việc triển khai MFA cần được tích hợp trực tiếp vào hệ thống quản lý danh tính và truy cập (IAM), bảo đảm tính tương thích và khả năng mở rộng. Đặc biệt, MFA cần triển khai theo phương pháp

hướng tới trải nghiệm người dùng (user-centric), giảm thiểu tối đa phiền toái nhưng vẫn giữ được tính an toàn, ví dụ như sử dụng ứng dụng xác thực tự động, sinh trắc học tích hợp thiết bị cá nhân thay vì buộc người dùng nhập mã OTP bằng tay.

Công an tỉnh Cà Mau tuyên truyền, hướng dẫn người dân tích hợp và sử dụng sổ sức khoẻ điện tử trên ứng dụng VNeID. Ảnh Sưu tầm

Đối với kiểm soát truy cập theo vai trò, trước tiên cần thực hiện rà soát và phân tích chức năng, nhiệm vụ của từng nhóm người dùng trong hệ thống để xây dựng các "vai trò" phù hợp. Mỗi vai trò cần được mô tả đầy đủ quyền hạn truy cập

vào hệ thống, mức độ can thiệp vào dữ liệu (đọc, ghi, xóa, sửa) và các điều kiện hạn chế nếu có. Hệ thống thông tin phải được thiết kế theo nguyên tắc "phân tách quyền hạn" (segregation of duties), tránh để một người hoặc nhóm người có toàn quyền kiểm soát dữ liệu từ đầu đến cuối, hạn chế nguy cơ bị lạm dụng hoặc thao túng dữ liệu. Tất cả các thay đổi về quyền truy cập đều phải được ghi log đầy đủ và có cơ chế cảnh báo sớm khi phát hiện bất thường trong hành vi truy cập, ví dụ như một nhân viên thông thường truy cập dữ liệu quản trị cấp cao, hay có hoạt động truy cập vào thời điểm bất thường.

Phiên họp lần thứ nhất, Ban Chỉ đạo phát triển khoa học công nghệ, đổi mới sáng tạo, chuyển đổi số

tỉnh Cà Mau. Nguồn từ Internet.

Để nâng cao hiệu quả của việc áp dụng MFA và RBAC, cần kết hợp đồng bộ với các công cụ giám sát bảo mật tiên tiến như hệ thống quản lý sự kiện và thông tin bảo mật (SIEM), công cụ phân tích hành vi người dùng (UEBA), giải pháp phân tích nhật ký truy cập và cảnh báo theo thời gian thực. Những công cụ này cho phép theo dõi mọi hành vi truy cập vào hệ thống, phát hiện các dấu hiệu bất thường có thể là dấu hiệu của tấn công mạng hoặc hành vi nội gián. Việc cảnh báo sớm và can thiệp kịp thời sẽ giảm thiểu tối đa thiệt hại có thể xảy ra, đồng thời hỗ trợ hoạt động điều tra, truy vết trong trường hợp có sự cố an ninh dữ liệu.

Quá trình triển khai các cơ chế bảo mật này đòi hỏi nâng cao nhận thức và trách nhiệm của cán bộ, công chức, viên chức, người lao động trong các cơ quan, tổ chức về bảo mật dữ liệu. Cần xây dựng và tổ chức thường xuyên các chương trình đào tạo, tập huấn, mô phỏng tình huống tấn công mạng để nâng cao kỹ năng ứng phó và tuân thủ chính sách bảo mật. Người sử dụng hệ thống phải được huấn luyện kỹ càng về cách nhận biết hành vi đáng ngờ, cách bảo mật thiết bị đầu cuối cá nhân, cách quản lý mật khẩu an toàn và cách sử dụng các công cụ xác thực phụ trợ như token hoặc phần mềm OTP.

Cùng với đó, việc lựa chọn nền tảng công nghệ phù hợp cũng đóng vai trò quan trọng trong việc triển khai hiệu quả MFA và RBAC. Các nền tảng điện toán đám mây cần hỗ trợ tích hợp xác thực đa yếu tố theo chuẩn mở như OAuth2.0, SAML hay OpenID Connect, đồng thời có khả năng tùy biến cao để phù hợp với các mô hình RBAC phức tạp. Trong hạ tầng dữ liệu quốc gia hoặc các hệ thống quản trị công, việc triển khai nên được đồng bộ từ cấp trung ương tới địa phương, bảo đảm không

có lỗ hổng phân mảnh trong cấu trúc kiểm soát truy cập, đồng thời xây dựng các bộ chỉ số đánh giá an toàn truy cập nhằm theo dõi hiệu quả chính sách và nhanh chóng điều chỉnh khi cần thiết.

Ảnh minh hoạ về Oauth 2.0

Một yếu tố không thể bỏ qua là cơ chế đánh giá định kỳ và kiểm tra độc lập hiệu quả áp dụng MFA và RBAC. Các cơ quan, tổ chức nên chủ động thực hiện các bài kiểm tra thâm nhập (penetration testing), kiểm tra an ninh (security audit) và mô phỏng tấn công giả lập (red teaming) để đánh giá khả năng kháng cự của hệ thống. Các lỗ hổng phát hiện được cần nhanh

chóng được khắc phục, đồng thời cập nhật chính sách kiểm soát truy cập nhằm phản ánh đúng rủi ro thực tế. Hệ thống nên có cơ chế phục hồi nhanh sau sự cố để bảo đảm tính liên tục trong truy cập dữ liệu, giảm thiểu tác động tiêu cực đến hoạt động quản lý và cung cấp dịch vụ công.

Trong môi trường công nghệ số hiện đại, đặc biệt là trong bối cảnh triển khai Chính phủ điện tử, chuyển đổi số quốc gia và khai thác dữ liệu lớn, việc áp dụng MFA và RBAC không chỉ là yêu cầu về kỹ thuật mà còn là nội dung bắt buộc trong quản trị dữ liệu an toàn, minh bạch, tuân thủ pháp luật. Cần gắn kết các chính sách bảo mật truy cập với các văn bản pháp lý như Luật An toàn thông tin mạng, Luật Giao dịch điện tử, Luật Dữ liệu và các quy định chuyên ngành liên quan. Mọi hành vi vi phạm quy định truy cập cần được xử lý nghiêm minh để bảo đảm tính răn đe và nâng cao kỷ luật trong khai thác, xử lý thông tin số.

Ảnh minh hoạ

Việc áp dụng đồng thời MFA và RBAC cũng hỗ trợ rất lớn cho các cơ quan nhà nước trong việc kiểm soát chặt chẽ truy cập dữ liệu hành chính công, hạn chế tình trạng rò rỉ thông tin cá nhân, bảo vệ quyền riêng tư của công dân. Khi triển khai đúng đắn, hai cơ chế này còn giúp nâng cao niềm tin của người dân vào hệ thống số, tạo tiền đề cho các dịch vụ công trực tuyến phát triển, qua đó thúc đẩy hiệu quả cải cách hành chính, tiết kiệm chi phí xã hội và nâng cao năng lực cạnh tranh quốc gia trong kỷ nguyên số.

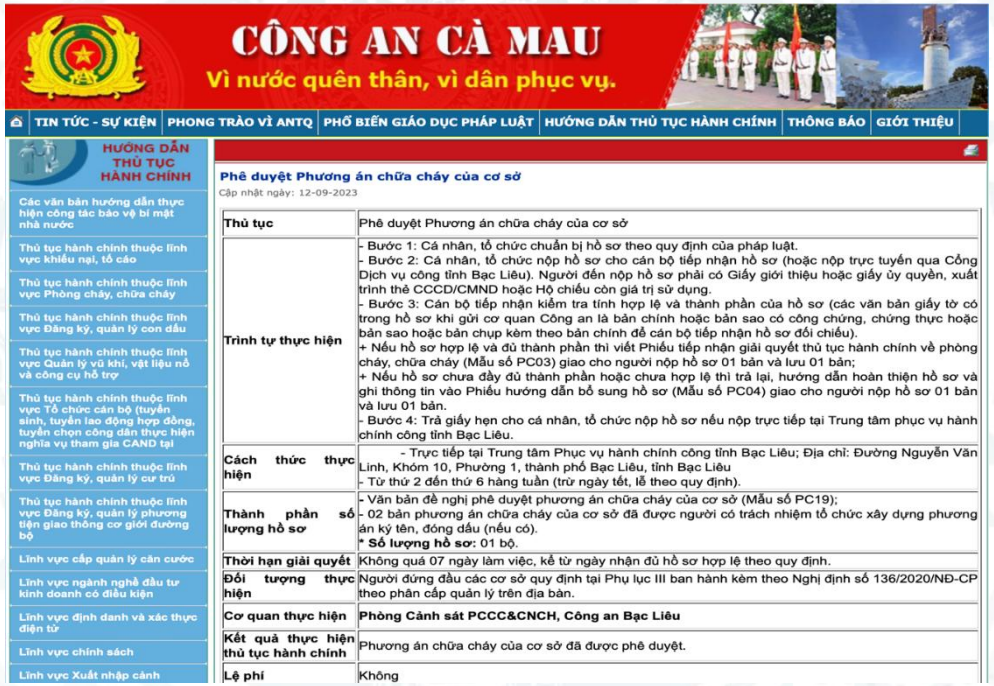
Đối với lực lượng Công an nhân dân, việc triển khai xác thực đa yếu tố và kiểm soát truy cập theo vai trò là yêu cầu mang tính chiến lược trong đảm bảo bí mật Nhà nước, bảo vệ dữ liệu nghiệp vụ và duy trì an ninh thông tin nội bộ. Hệ thống thông tin nghiệp vụ của lực lượng Công an chứa đựng dữ liệu đặc biệt quan trọng như hồ sơ đối tượng, thông tin trinh sát, dữ liệu điều tra… nên cần thiết lập các lớp xác thực bảo mật nhiều tầng nhằm ngăn chặn triệt để hành vi truy cập trái phép từ bên ngoài và bên trong. Đồng thời, việc kiểm soát truy cập dựa trên vai trò giúp phân quyền chặt chẽ theo chức năng tác chiến, điều tra, phân tích kỹ thuật hay hành chính, từ đó nâng cao tính kỷ luật, trách nhiệm cá nhân và hạn chế tối đa rủi ro nội gián hoặc lộ lọt thông tin mật. Đây là nền tảng bảo vệ vững chắc cho hoạt động nghiệp vụ, xây dựng niềm tin với nhân dân và đảm bảo tuyệt đối an toàn hệ thống thông tin quốc phòng - an ninh trong mọi tình huống.

Ảnh minh hoạ

2.2.4. Chuẩn hóa và áp dụng bắt buộc các tiêu chuẩn kỹ thuật quốc gia và quốc tế về bảo mật dữ liệu, an toàn thông tin trong toàn bộ vòng đời của sản phẩm, dịch vụ dữ liệu

Việc chuẩn hóa và áp dụng bắt buộc các tiêu chuẩn kỹ thuật quốc gia và quốc tế về bảo mật dữ liệu, an toàn thông tin là một yêu cầu cấp thiết trong bối cảnh dữ liệu đã và đang trở thành nguồn lực trọng yếu cho sự phát triển kinh tế - xã hội, quốc phòng – an ninh. Trong toàn bộ vòng đời của sản phẩm và dịch vụ dữ liệu, bao gồm từ khâu thu thập, lưu trữ, xử lý, chia sẻ đến khai thác và hủy dữ liệu, đều cần được đảm bảo bằng những tiêu chuẩn bảo mật nghiêm ngặt, nhất quán và có khả năng

thích ứng linh hoạt với sự phát triển nhanh chóng của công nghệ. Chuẩn hóa ở đây không chỉ dừng lại ở việc xây dựng các bộ tiêu chuẩn, mà còn là quá trình bắt buộc áp dụng đồng bộ, có sự kiểm tra, giám sát và đánh giá thường xuyên để đảm bảo rằng mọi tổ chức, cá nhân tham gia vào chuỗi giá trị dữ liệu đều tuân thủ tuyệt đối nguyên tắc bảo mật và an toàn thông tin.



Công bố thủ tục hành chính phê duyệt Phương án chữa cháy của cơ sở trên Trang Thông tin điện tử Công an tỉnh Cà Mau

Việc xây dựng hệ thống tiêu chuẩn kỹ thuật quốc gia cần được thực hiện dựa trên nguyên tắc hài hòa với các tiêu chuẩn quốc tế, đặc biệt là những bộ tiêu chuẩn do Tổ chức Tiêu chuẩn hóa quốc tế (ISO), Liên minh Viễn thông quốc tế (ITU),

Nhóm Công tác về Bảo mật Thông tin của Liên Hợp Quốc, hay các hiệp hội ngành như IEEE hay NIST ban hành. Những tiêu chuẩn này không chỉ giúp đảm bảo tính tương thích, khả năng liên thông và tích hợp trong môi trường số toàn cầu, mà còn là cơ sở để đánh giá mức độ an toàn, bảo mật, chất lượng của sản phẩm, dịch vụ dữ liệu trong nền kinh tế số. Trong quá trình chuẩn hóa, Việt Nam cần tổ chức rà soát, đánh giá các tiêu chuẩn hiện hành, đồng thời cập nhật, ban hành mới những tiêu chuẩn còn thiếu, ưu tiên các lĩnh vực trọng điểm như điện toán đám mây, trí tuệ nhân tạo, dữ liệu lớn, IoT, blockchain, dữ liệu mở và các nền tảng phân tích dữ liệu.

Để bảo đảm hiệu quả triển khai, cần xác lập cơ chế bắt buộc áp dụng đối với các tiêu chuẩn về bảo mật dữ liệu và an toàn thông tin trong toàn bộ vòng đời dữ liệu. Điều này không chỉ áp dụng đối với cơ quan nhà nước, mà cả doanh nghiệp cung cấp dịch vụ số, tổ chức trung gian dữ liệu, bên thứ ba, và người dùng cuối. Các tiêu chuẩn này phải được lồng ghép trong thiết kế hệ thống công nghệ thông tin, trong hợp đồng cung cấp dịch vụ, và trong quy trình vận hành hằng ngày. Việc áp dụng bắt buộc cần đi kèm với cơ chế thanh tra, kiểm tra định kỳ, đột xuất, xử lý vi phạm minh bạch, công khai. Đặc biệt, các sản phẩm, dịch vụ dữ liệu muốn được công nhận, đưa vào sử dụng trong hệ thống công hoặc cung cấp ra thị trường phải trải qua quá trình kiểm định chất lượng, đánh giá bảo mật dựa trên các tiêu chuẩn kỹ thuật hiện hành.

Bên cạnh đó, việc chuẩn hóa cần bảo đảm tính cập nhật liên tục theo sự thay đổi nhanh chóng của công nghệ và hành vi tấn công mạng. Cơ quan tiêu chuẩn quốc gia phải thiết lập mạng lưới theo dõi, đánh giá xu hướng tấn công mạng, các lỗ

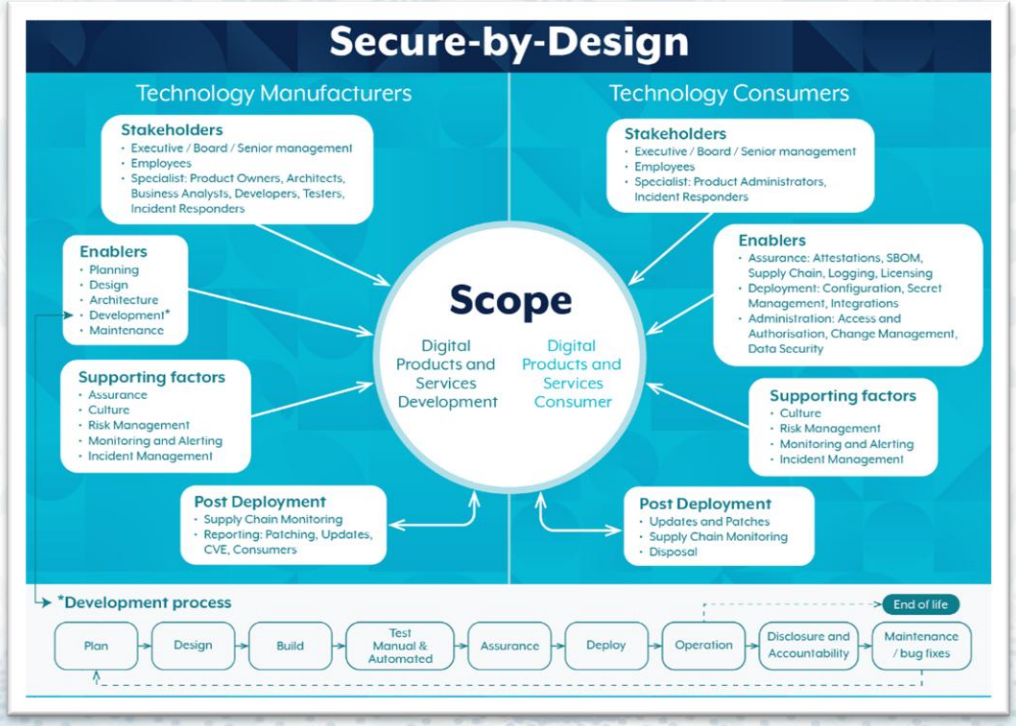
hổng bảo mật mới, từ đó điều chỉnh, cập nhật kịp thời các tiêu chuẩn, quy chuẩn kỹ thuật phù hợp. Việc xây dựng bộ tiêu chuẩn cũng cần lắng nghe phản hồi từ thực tiễn triển khai, tiếp nhận kinh nghiệm quốc tế, các điển hình tốt, và sự đóng góp từ cộng đồng chuyên gia an ninh mạng trong nước và quốc tế. Bên cạnh các tiêu chuẩn chung cho bảo mật dữ liệu, cần xây dựng các tiêu chuẩn riêng biệt cho từng loại hình dữ liệu đặc thù như dữ liệu cá nhân, dữ liệu tài chính, dữ liệu y tế, dữ liệu quốc phòng – an ninh, để có biện pháp bảo vệ phù hợp về kỹ thuật và tổ chức.

Công tác đào tạo, tuyên truyền và nâng cao nhận thức về các tiêu chuẩn bảo mật dữ liệu cũng cần được triển khai đồng bộ. Mọi tổ chức, cá nhân tham gia cung cấp, khai thác dữ liệu đều cần được bồi dưỡng kiến thức chuyên môn về chuẩn an toàn thông tin, cập nhật xu hướng và yêu cầu tuân thủ pháp luật. Các đơn vị đào tạo cần tích hợp nội dung về tiêu chuẩn kỹ thuật quốc gia và quốc tế vào giáo trình, tổ chức thi sát hạch chứng chỉ chuẩn bảo mật để nâng cao chất lượng nguồn nhân lực. Các chương trình truyền thông cần giúp người dân hiểu rõ vai trò của tiêu chuẩn trong bảo vệ quyền lợi, nâng cao niềm tin số và phòng ngừa rủi ro lộ lọt thông tin cá nhân. Song song đó, cần đẩy mạnh hợp tác quốc tế để chia sẻ kinh nghiệm xây dựng và triển khai các tiêu chuẩn bảo mật, mở rộng công nhận lẫn nhau về tiêu chuẩn giữa Việt Nam và các quốc gia, vùng lãnh thổ.

Các doanh nghiệp đồng hành, chung tay triển khai thực hiện Đề án 06. Nguồn từ Internet.

Trong lĩnh vực phát triển sản phẩm, dịch vụ số, việc áp dụng tiêu chuẩn bảo mật phải trở thành một tiêu chí bắt buộc trong quá trình nghiên cứu, thiết kế, thử nghiệm và đưa ra thị trường. Mỗi dòng mã lập trình, mỗi mô-đun hệ thống đều phải tuân thủ nguyên tắc bảo mật theo thiết kế (security by design), vận hành an toàn theo mặc định (secure by default), và được cập

nhật thường xuyên để phòng chống rủi ro. Các doanh nghiệp công nghệ cần thành lập bộ phận đảm bảo chất lượng và an toàn dữ liệu, kiểm tra tính tuân thủ chuẩn kỹ thuật trước khi sản phẩm được thương mại hóa hoặc triển khai trên diện rộng. Việc xây dựng và duy trì hệ thống kiểm thử bảo mật tự động, các công cụ đánh giá độ an toàn theo tiêu chuẩn quốc tế sẽ là yếu tố quyết định sự thành công, tính bền vững và khả năng cạnh tranh của sản phẩm dữ liệu Việt Nam trên thị trường toàn cầu.



Ảnh minh hoạ

Việc áp dụng bắt buộc tiêu chuẩn kỹ thuật cũng cần được tích hợp trong các văn bản pháp luật như Luật Dữ liệu, Luật An toàn thông tin mạng, Luật Giao dịch điện tử, cùng các nghị định, thông tư hướng dẫn thi hành. Các quy định này cần xác định rõ bộ tiêu chuẩn bắt buộc áp dụng, phạm vi áp dụng, chế tài xử phạt vi phạm và cơ chế khuyến khích đổi mới, nâng cao năng lực tuân thủ. Đồng thời, cần xây dựng hệ thống cấp chứng nhận tiêu chuẩn đối với sản phẩm, dịch vụ dữ liệu, tổ chức cung cấp dịch vụ trung gian dữ liệu, và cơ quan nhà nước trong cung cấp dịch vụ công số. Các chứng nhận này sẽ tạo điều kiện thúc đẩy niềm tin của công dân, doanh nghiệp đối với môi trường số an toàn, góp phần vào mục tiêu chuyển đổi số quốc gia bền vững, toàn diện.

Tăng cường ứng dụng công nghệ tự động hóa, trí tuệ nhân tạo và phân tích dữ liệu lớn vào công tác giám sát, phát hiện vi phạm tiêu chuẩn bảo mật cũng là một yêu cầu cấp bách. Cần triển khai các hệ thống giám sát an toàn dữ liệu thời gian thực, phân tích hành vi người dùng bất thường, xác định các rủi ro nội sinh và ngoại sinh đối với hệ thống dữ liệu quốc gia. Các cơ quan chức năng cần phối hợp chia sẻ dữ liệu cảnh báo sớm về tấn công mạng, vi phạm chuẩn bảo mật với các bên liên quan để kịp thời phòng chống. Việc ứng dụng công nghệ cũng cần tuân thủ chuẩn quốc tế như ISO/IEC 27001, ISO/IEC 27701, NIST Cybersecurity Framework, giúp bảo đảm tính minh bạch, đồng bộ và khả năng truy vết trong xử lý sự cố bảo mật.

Ảnh minh hoạ

Trong toàn bộ tiến trình chuẩn hóa và áp dụng bắt buộc tiêu chuẩn kỹ thuật, cần xác định rõ vai trò dẫn dắt, điều phối của cơ quan nhà nước trong thiết lập, ban hành, hướng dẫn và giám sát thực hiện. Cơ quan tiêu chuẩn quốc gia như Bộ Khoa học và Công nghệ, Bộ Thông tin và Truyền thông cần phối hợp chặt chẽ để thống nhất khung tiêu chuẩn quốc gia, đồng thời làm đầu mối phối hợp với các tổ chức quốc tế về tiêu chuẩn hóa. Chính phủ cũng cần ưu tiên bố trí ngân sách để hỗ trợ các cơ quan, tổ chức thực hiện chuyển đổi hạ tầng kỹ thuật, nâng cấp phần mềm, mua sắm công cụ kiểm định nhằm đáp ứng yêu cầu

tiêu chuẩn mới. Các chính sách ưu đãi về thuế, tín dụng, đấu thầu công nghệ có thể được thiết kế để khuyến khích doanh nghiệp đổi mới công nghệ, tuân thủ chuẩn bảo mật dữ liệu, nhất là các startup và doanh nghiệp nhỏ, vừa trong lĩnh vực dữ liệu.

Với lực lượng Công an nhân dân, việc chuẩn hóa và áp dụng bắt buộc các tiêu chuẩn bảo mật dữ liệu, an toàn thông tin trong toàn bộ vòng đời sản phẩm, dịch vụ dữ liệu có vai trò đặc biệt quan trọng trong bảo vệ an ninh quốc gia và trật tự an toàn xã hội. Các cơ sở dữ liệu chuyên ngành của ngành Công an như dữ liệu dân cư, dữ liệu tội phạm, dữ liệu nghiệp vụ kỹ thuật, thông tin điều tra hình sự… là tài sản có tính chiến lược, yêu cầu phải được bảo vệ tuyệt đối theo các tiêu chuẩn bảo mật cao nhất. Lực lượng Công an phải chủ động phối hợp với các cơ quan tiêu chuẩn để xây dựng các bộ tiêu chuẩn riêng phù hợp với tính đặc thù của hoạt động nghiệp vụ, đồng thời làm gương mẫu trong việc triển khai, áp dụng, kiểm định và giám sát chặt chẽ việc tuân thủ tiêu chuẩn. Ngoài ra, Công an nhân dân còn giữ vai trò nòng cốt trong thanh tra, điều tra các vi phạm về bảo mật dữ liệu, phòng chống tội phạm mạng, đặc biệt là những hành vi xâm phạm dữ liệu cá nhân, tấn công vào hệ thống thông tin trọng yếu quốc gia. Việc chuẩn hóa và áp dụng tiêu chuẩn bảo mật không chỉ là yêu cầu pháp lý mà còn là công cụ thiết yếu để lực lượng Công an bảo vệ chủ quyền số, bảo đảm an ninh dữ liệu trong mọi tình huống.

2.2.5. Triển khai chính sách sao lưu dữ liệu định kỳ, lưu trữ an toàn và xây dựng phương án phục hồi dữ liệu sau sự cố, bảo đảm tính sẵn sàng và khả năng phục hồi hoạt động

Triển khai chính sách sao lưu dữ liệu định kỳ là một bước thiết yếu nhằm bảo đảm tính liên tục trong hoạt động vận hành và duy trì độ tin cậy của hệ thống thông tin. Việc xác lập quy trình sao lưu cần được thực hiện trên cơ sở đánh giá rủi ro cụ thể đối với từng loại dữ liệu, qua đó phân loại các nhóm dữ liệu cần được sao lưu theo chu kỳ thời gian khác

nhau, từ hàng giờ, hàng ngày cho đến hàng tuần, phù hợp với mức độ nhạy cảm, giá trị và tần suất thay đổi của thông tin. Cơ quan, tổ chức cần lựa chọn mô hình sao lưu phù hợp như sao lưu toàn bộ, sao lưu gia tăng hoặc sao lưu vi sai, nhằm tối ưu hóa thời gian thực hiện và dung lượng lưu trữ sử dụng. Đồng thời, cần xây dựng một lịch trình sao lưu rõ ràng, có sự phân công cụ thể về trách nhiệm kiểm tra định kỳ tình trạng của bản sao lưu để bảo đảm tính toàn vẹn và khả năng phục hồi thực tế khi cần thiết.

Quá trình sao lưu không chỉ giới hạn ở máy chủ vật lý mà cần mở rộng đến toàn bộ hệ sinh thái thông tin bao gồm máy trạm, hệ thống lưu trữ đám mây, thiết bị đầu cuối, ứng dụng trực tuyến và dữ liệu luân chuyển trên môi trường mạng. Cần xác định rõ điểm lưu trữ bản sao là tại chỗ (on-premises), từ xa (off-site) hoặc trên nền tảng điện toán đám mây, đồng thời triển khai cơ chế mã hóa mạnh cho các bản sao lưu nhằm bảo đảm dữ liệu không bị truy cập trái phép trong quá trình lưu giữ hoặc truyền tải. Đối với các tổ chức có quy mô lớn và khối lượng dữ liệu khổng lồ, việc áp dụng các giải pháp sao lưu tự động, tích hợp trí tuệ nhân tạo để giám sát, cảnh báo các bất thường trong quá trình sao lưu cũng là một hướng đi hiệu quả để nâng cao tính chủ động trong quản lý dữ liệu.

Ảnh minh họa, nguồn từ Internet

Việc lưu trữ an toàn các bản sao lưu đòi hỏi cần phải có hạ tầng lưu trữ đáp ứng chuẩn an toàn vật lý và an toàn thông tin. Các bản sao nên được phân phối và lưu trữ tại nhiều vị trí địa lý khác nhau để giảm thiểu rủi ro mất mát do thiên tai, hỏa hoạn hoặc các cuộc tấn công mạng diện rộng. Cần đầu tư vào các trung tâm dữ liệu đạt chuẩn Tier III hoặc Tier IV, được trang bị hệ thống kiểm soát ra vào vật lý, giám sát 24/7, phòng chống cháy nổ và hỗ trợ nguồn điện dự phòng, điều hòa, chống rung động. Các hệ thống lưu trữ cần được phân vùng riêng biệt cho từng nhóm dữ liệu, có cơ chế kiểm soát truy cập chặt chẽ

dựa trên quyền hạn và vai trò của người dùng, kết hợp với hệ thống nhật ký truy cập để phục vụ công tác kiểm tra, truy vết khi có sự cố.

Song hành với chính sách sao lưu và lưu trữ, việc xây dựng phương án phục hồi dữ liệu sau sự cố giữ vai trò trung tâm trong chiến lược bảo đảm tính sẵn sàng và liên tục của hoạt động. Cần xác lập các tình huống sự cố tiêu biểu như mất điện đột ngột, hỏng hóc thiết bị, lỗi hệ điều hành, mã độc tống tiền, tấn công từ chối dịch vụ hoặc sự cố thiên tai để mô phỏng quy trình phục hồi tương ứng. Với mỗi tình huống, tổ chức cần thiết kế phương án phục hồi với các mốc thời gian cụ thể như RTO (Recovery Time Objective – thời gian cần để khôi phục hệ thống) và RPO (Recovery Point Objective – thời điểm gần nhất có thể phục hồi dữ liệu) để chủ động lên kế hoạch nguồn lực và phương tiện ứng cứu. Cần lập đội ngũ chuyên trách về phục hồi dữ liệu, tổ chức tập huấn định kỳ và diễn tập giả lập các tình huống mất mát dữ liệu để kiểm tra khả năng sẵn sàng ứng phó và rút kinh nghiệm thực tiễn.

Hệ thống phục hồi cần được tích hợp chặt chẽ với các giải pháp phát hiện sự cố như hệ thống giám sát an ninh mạng, hệ thống cảnh báo tấn công mạng, các công cụ quản lý rủi ro để bảo đảm việc phục hồi dữ liệu không chỉ là thao tác kỹ thuật mà còn là một thành phần trong chuỗi phản ứng nhanh khi có sự cố an toàn thông tin. Trong các tổ chức có dữ liệu trọng yếu, cần thiết lập các trung tâm dự phòng (Disaster Recovery Site) với năng lực xử lý tương đương hệ thống chính, bảo đảm việc chuyển đổi vận hành có thể diễn ra ngay lập tức mà không làm gián đoạn các dịch vụ cung cấp cho người dân, doanh nghiệp hoặc các hệ thống quản lý nhà nước. Phương án phục hồi cần bao gồm cả khía cạnh kỹ thuật, tổ chức nhân sự, thông tin liên lạc và tài chính để bảo đảm tính khả thi và hiệu quả trong thực tế.

Việc tổ chức kiểm thử định kỳ các bản sao lưu và phương án phục hồi là bước bắt buộc nhằm đánh giá mức độ tin cậy và kịp thời điều chỉnh nếu phát hiện điểm yếu. Cần xây dựng quy trình kiểm thử chuẩn hóa với các chỉ số đánh giá rõ ràng như tỷ lệ thành công của việc phục hồi, thời gian phục hồi, độ toàn vẹn của dữ liệu sau khi khôi phục. Các đợt kiểm thử cần được lập kế hoạch và giám sát bởi bộ phận độc lập để bảo đảm tính khách quan và toàn diện. Sau mỗi lần kiểm thử, cần lập báo cáo, phân tích nguyên nhân các điểm nghẽn, đề xuất cải tiến quy trình, cập nhật tài liệu vận hành và đào tạo lại đội ngũ nhân sự tham gia công tác khôi phục.

Về mặt chính sách, việc thể chế hóa nội dung về sao lưu, lưu trữ và phục hồi dữ liệu trong quy chế quản lý nội bộ của cơ quan, tổ chức là điều cần thiết để bảo đảm tính bắt buộc và kỷ luật triển khai. Các văn bản nội bộ cần quy định rõ trách nhiệm của từng bộ phận trong quá trình thực hiện, cơ chế báo cáo, giám sát, xử lý vi phạm khi không tuân thủ quy trình đã ban hành. Ngoài ra, cần có cơ chế cập nhật chính sách linh hoạt để thích ứng với sự thay đổi nhanh chóng của môi trường công nghệ, đặc biệt là trong bối cảnh các mô hình điện toán đám mây, dữ liệu lớn và trí tuệ nhân tạo ngày càng đóng vai trò trung tâm trong hoạt động số hóa của các cơ quan nhà nước và doanh nghiệp.

Trong mối liên hệ với nhiệm vụ của lực lượng Công an nhân dân, việc triển khai chính sách sao lưu, lưu trữ và phục hồi dữ liệu không chỉ bảo vệ hệ thống thông tin nghiệp vụ mà còn góp phần bảo đảm an ninh quốc gia trong không gian mạng. Lực lượng Công an cần chủ động phối hợp với các cơ quan, đơn vị liên quan để kiểm tra, giám sát việc thực thi các chính sách bảo mật dữ liệu, đồng thời triển khai các phương án dự phòng dữ liệu nghiệp vụ trọng yếu tại nhiều cấp độ để không bị động trước các cuộc tấn công mạng hoặc thiên tai, sự cố kỹ thuật. Trong công tác điều tra, truy vết tội phạm công nghệ cao, các bản sao lưu dữ liệu cũng là nguồn bằng chứng quan trọng phục vụ đấu tranh, truy nguyên nguồn gốc hành vi phạm tội. Do

đó, việc nâng cao năng lực bảo vệ và phục hồi dữ liệu của lực lượng Công an không chỉ mang ý nghĩa kỹ thuật mà còn là yếu tố then chốt trong xây dựng thế trận an ninh mạng toàn dân, phục vụ hiệu quả nhiệm vụ bảo vệ Tổ quốc trong tình hình mới.

2.2.6. Ứng dụng các nền tảng bảo vệ dữ liệu thế hệ mới (Next-Gen Data Protection) tích hợp các tính năng phòng chống mất mát dữ liệu (DLP), phát hiện mối đe dọa (Threat Detection), kiểm soát truy cập động (Dynamic Access Control)

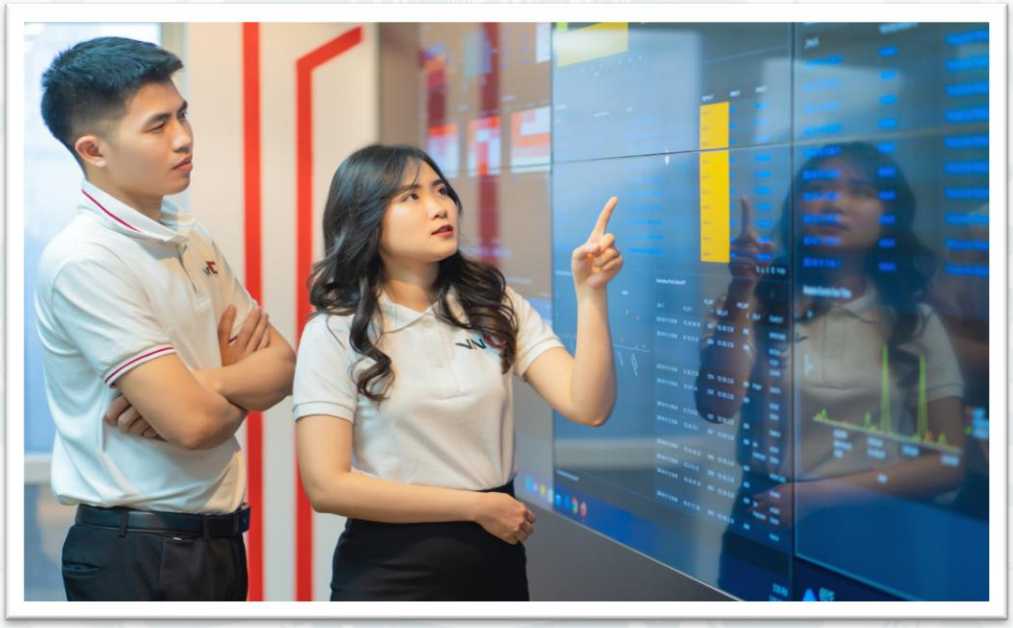
Việc ứng dụng các nền tảng bảo vệ dữ liệu thế hệ mới (Next-Gen Data Protection) là một bước tiến quan trọng nhằm tăng cường khả năng tự vệ của hệ thống thông tin trước các mối đe dọa ngày càng phức tạp. Trên nền tảng các công nghệ hiện đại như trí tuệ nhân tạo, học máy, phân tích hành vi và mã hóa thông minh, các giải pháp bảo vệ dữ liệu thế hệ mới không chỉ đơn thuần thực hiện chức năng giám sát, cảnh báo mà còn có khả năng phản ứng chủ động với sự cố an ninh, qua đó góp phần bảo đảm tính toàn vẹn, bí mật và khả dụng của dữ liệu trong toàn bộ vòng đời của nó. Nền tảng bảo vệ dữ liệu thế hệ mới là sự tích hợp đồng bộ giữa ba trụ cột công nghệ cốt lõi: phòng chống mất mát dữ liệu (Data Loss Prevention – DLP), phát hiện mối đe dọa (Threat Detection) và kiểm soát truy cập động (Dynamic Access Control), nhằm tạo nên một cơ chế bảo vệ dữ liệu theo thời gian thực, thích ứng với ngữ cảnh và mức độ rủi ro.

Triển khai các tính năng phòng chống mất mát dữ liệu (DLP) là nhiệm vụ ưu tiên hàng đầu trong ứng dụng nền tảng bảo vệ dữ liệu thế hệ mới. DLP giúp tổ chức giám sát, kiểm soát và ngăn chặn dữ liệu nhạy cảm bị rò rỉ, thất thoát hoặc truy cập trái phép thông qua nhiều hình thức như gửi email, chia sẻ qua đám mây, sao chép ra thiết bị lưu trữ di động, in ấn hoặc chụp màn hình. Để vận hành hiệu quả hệ thống DLP, cần xác định rõ các loại dữ liệu nhạy cảm và dữ liệu quan trọng chiến lược của tổ chức, sau đó phân loại, đánh dấu và gán nhãn bảo mật cho dữ liệu trên toàn bộ hệ thống CNTT. Công nghệ DLP

hiện đại có thể tự động phát hiện dữ liệu nhạy cảm thông qua nhận diện mẫu (pattern recognition), phân tích ngữ nghĩa (semantic analysis), từ khóa và thuật toán học máy, qua đó xác định những hành vi vi phạm chính sách bảo mật dữ liệu. Việc xây dựng các chính sách DLP phù hợp với đặc thù hoạt động và rủi ro của từng đơn vị, đảm bảo các chính sách đó có tính khả thi, có thể áp dụng linh hoạt theo vai trò người dùng, thời gian, thiết bị truy cập hoặc vị trí địa lý là điều kiện tiên quyết để hệ thống hoạt động hiệu quả. Bên cạnh đó, cần triển khai các biện pháp xử lý sự cố khi có vi phạm, như chặn hành vi, cảnh báo cho người dùng, gửi thông báo cho quản trị viên hoặc ghi lại log phục vụ điều tra truy vết. Để nâng cao năng lực của hệ thống DLP, cần tích hợp với các công cụ phân tích dữ liệu lớn và AI để tối ưu hóa phát hiện và giảm thiểu cảnh báo giả.

Tính năng phát hiện mối đe dọa (Threat Detection) trong các nền tảng bảo vệ dữ liệu thế hệ mới đóng vai trò then chốt trong việc phát hiện sớm và kịp thời các hành vi bất thường hoặc nguy cơ tấn công mạng. Các hệ thống này sử dụng kết hợp nhiều kỹ thuật tiên tiến như phân tích hành vi người dùng (User Behavior Analytics – UBA), phát hiện bất thường thống kê, phân tích log hệ thống và sử dụng trí tuệ nhân tạo để nhận diện các mô hình tấn công chưa từng biết trước đó. Khác với các phương pháp phát hiện dựa trên chữ ký truyền thống, giải pháp Threat Detection hiện đại có khả năng học hỏi và thích nghi, từ đó phát hiện các tấn công có chủ đích (APT), hành vi trích xuất dữ liệu lén lút, sử dụng tài khoản bị đánh cắp hoặc các hành vi nội gián gây nguy hiểm. Việc triển khai chức năng này đòi hỏi tổ chức phải thiết lập hệ thống thu thập và giám sát dữ liệu toàn diện từ nhiều nguồn như máy chủ, thiết bị đầu cuối, mạng lưới và các ứng dụng đám mây. Tổ chức cũng cần thiết kế các kịch bản cảnh báo phù hợp, phân loại mức độ ưu tiên và xây dựng quy trình phản ứng sự cố tự động hoặc bán tự động nhằm giảm thời gian phản hồi và tổn thất khi xảy ra vi phạm. Các mô hình Threat Intelligence – chia sẻ thông tin về mối đe dọa giữa các tổ chức – cũng cần được tích hợp vào hệ thống để tăng cường khả năng phát hiện các cuộc tấn công quy mô lớn

hoặc có dấu hiệu liên kết từ nhiều nguồn. Đào tạo cán bộ chuyên trách về kỹ năng nhận diện, phân tích và xử lý mối đe dọa là một phần quan trọng trong việc bảo đảm hiệu quả hoạt động của thành phần này.



Đào tạo cán bộ chuyên trách về kỹ năng nhận diện, phân tích và xử lý mối đe dọa khi xảy ra vi phạm.

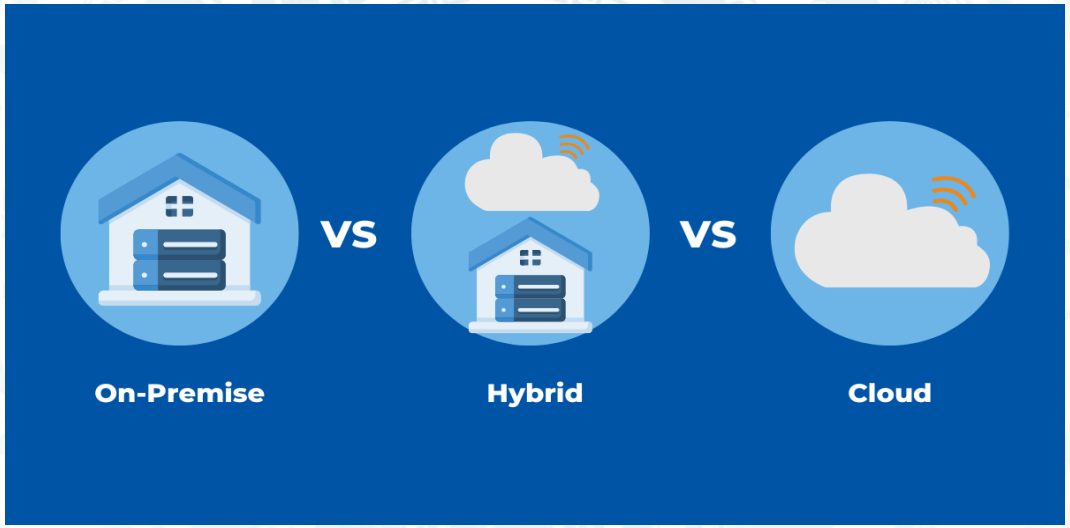
Ảnh minh họa. Nguồn từ Internet.

Kiểm soát truy cập động (Dynamic Access Control – DAC) là thành phần không thể thiếu trong nền tảng bảo vệ dữ liệu hiện đại, cho phép tổ chức áp dụng các chính sách truy cập dữ liệu theo thời gian thực, linh hoạt theo ngữ cảnh sử dụng.

Khác với các mô hình truy cập truyền thống dựa trên vai trò (RBAC), DAC cho phép xây dựng chính sách truy cập dựa trên các yếu tố như danh tính người dùng, loại thiết bị, vị trí địa lý, thời gian truy cập, mức độ nhạy cảm của dữ liệu hoặc hành vi gần đây của người dùng. Điều này giúp tăng cường mức độ chính xác và hiệu quả trong kiểm soát, giảm nguy cơ truy cập trái phép hoặc lạm quyền từ người dùng nội bộ. Để triển khai DAC hiệu quả, hệ thống cần có cơ sở hạ tầng xác thực hiện đại hỗ trợ xác thực đa yếu tố (MFA), công nghệ quản lý danh tính (IAM) và tích hợp đồng bộ với hệ thống phân loại dữ liệu, DLP và Threat Detection. Các chính sách DAC cần được thiết kế theo nguyên tắc "quyền truy cập tối thiểu" (least privilege) và "truy cập theo nhu cầu công việc" (need-to-know), đồng thời có khả năng điều chỉnh tự động khi phát hiện dấu hiệu bất thường. Việc kiểm toán các phiên truy cập, giám sát theo thời gian thực và ghi nhật ký đầy đủ cũng là yêu cầu bắt buộc để đảm bảo tính minh bạch và phục vụ công tác điều tra, xử lý vi phạm khi cần thiết. DAC không chỉ mang lại lợi ích trong môi trường doanh nghiệp truyền thống mà còn đặc biệt phù hợp với các mô hình làm việc từ xa, truy cập phân tán qua nền tảng đám mây, giúp bảo vệ dữ liệu trong khi vẫn duy trì tính linh hoạt và tiện ích cho người dùng.

Để tích hợp ba thành phần trên vào một nền tảng thống nhất, tổ chức cần xây dựng kiến trúc hệ thống bảo mật tổng thể, bảo đảm khả năng tương tác, chia sẻ dữ liệu và đồng bộ hóa chính sách giữa các mô-đun bảo vệ. Việc lựa chọn nền tảng bảo vệ dữ liệu thế hệ mới cần dựa trên các tiêu chí như khả năng tích hợp với hạ tầng công nghệ thông tin sẵn có, hỗ trợ đa nền tảng (on-premise, cloud, hybrid), khả năng mở rộng quy mô, hỗ trợ tuân thủ các quy định pháp lý và tiêu chuẩn kỹ thuật về bảo mật dữ liệu trong nước và quốc tế. Tổ chức cần đánh giá kỹ lưỡng các nhà cung cấp giải pháp, tiến hành thử nghiệm, triển khai thí điểm tại một số bộ phận trước khi nhân rộng toàn hệ thống. Đồng thời, cần xây dựng lộ trình triển khai theo từng giai

đoạn cụ thể, có quy định rõ ràng về trách nhiệm của các phòng ban chức năng và kế hoạch đầu tư hạ tầng, nhân lực, công cụ hỗ trợ. Hệ thống cần được vận hành bởi đội ngũ chuyên môn cao, thường xuyên được đào tạo và cập nhật kiến thức mới về an toàn dữ liệu. Ngoài ra, tổ chức cần xây dựng cơ chế giám sát, đánh giá định kỳ hiệu quả của các biện pháp bảo vệ dữ liệu, kịp thời điều chỉnh chính sách khi xuất hiện các công nghệ mới hoặc mối đe dọa mới.



Ảnh minh hoạ về hỗ trợ đa nền tảng (on-premise, cloud, hybrid)

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, các tổ chức ngày càng phụ thuộc nhiều vào dữ liệu, dẫn đến nguy cơ về mất mát, rò rỉ và bị khai thác trái phép gia tăng nhanh chóng. Việc đầu tư vào các nền tảng bảo vệ dữ liệu thế hệ mới không chỉ là nhu cầu nội tại mà còn là yêu cầu bắt buộc để đảm bảo sự phát triển bền vững, tuân thủ pháp luật và bảo vệ lợi ích của

tổ chức cũng như cá nhân có liên quan. Đồng thời, việc áp dụng các công nghệ này còn góp phần xây dựng niềm tin số, nâng cao uy tín của tổ chức trong môi trường số hóa toàn cầu. Để nền tảng phát huy hiệu quả tối đa, cần gắn kết với các hoạt động kiểm toán nội bộ, đánh giá rủi ro, và quản trị dữ liệu theo hướng tổng thể, lấy dữ liệu làm tài sản chiến lược và an toàn dữ liệu là nền tảng cho mọi hoạt động vận hành.

Với lực lượng Công an nhân dân, việc ứng dụng các nền tảng bảo vệ dữ liệu thế hệ mới có ý nghĩa đặc biệt quan trọng trong bảo đảm an ninh quốc gia và giữ gìn trật tự an toàn xã hội trong không gian mạng. Hệ thống DLP giúp phát hiện và ngăn chặn các hành vi đánh cắp hoặc rò rỉ thông tin mật, thông tin nghiệp vụ quan trọng; hệ thống Threat Detection hỗ trợ kịp thời phát hiện các hành vi tấn công có chủ đích nhằm vào cơ sở dữ liệu ngành Công an hoặc các hệ thống trọng yếu quốc gia; cơ chế kiểm soát truy cập động góp phần phòng ngừa nguy cơ xâm nhập từ bên trong hoặc lạm dụng quyền truy cập để thực hiện hành vi vi phạm. Việc chủ động triển khai các nền tảng bảo vệ dữ liệu thế hệ mới sẽ góp phần nâng cao năng lực đảm bảo an toàn thông tin, tạo nền tảng kỹ thuật vững chắc cho các hoạt động nghiệp vụ, đồng thời thể hiện vai trò tiên phong của lực lượng Công an trong kiến tạo môi trường số an toàn, tin cậy phục vụ sự nghiệp bảo vệ an ninh Tổ quốc trong thời đại mới.

2.2.7 Xây dựng chính sách chia sẻ và sử dụng dữ liệu một cách minh bạch, kiểm soát được quyền truy cập, mục đích sử dụng, đồng thời hạn chế chia sẻ dữ liệu xuyên biên giới nếu không có cơ chế bảo vệ rõ ràng

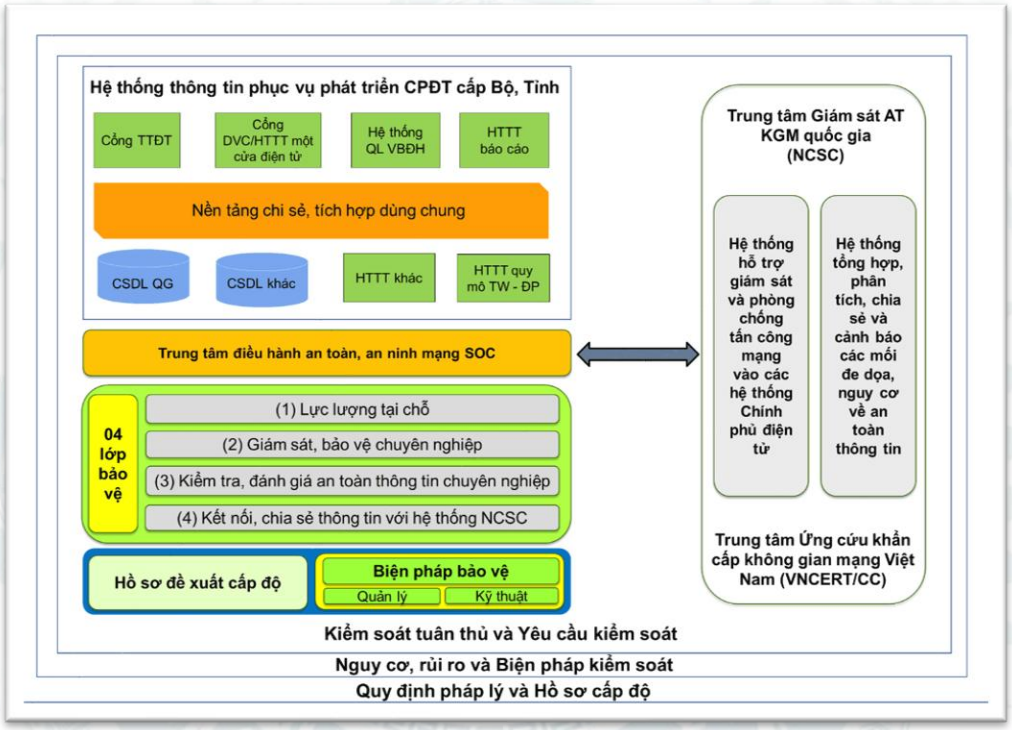
Việc xây dựng chính sách chia sẻ và sử dụng dữ liệu một cách minh bạch là yêu cầu cấp thiết trong bối cảnh chuyển đổi số ngày càng sâu rộng, dữ liệu trở thành tài sản chiến lược, ảnh hưởng trực tiếp đến an ninh quốc gia, quyền riêng tư cá nhân và năng lực quản trị của mỗi tổ chức. Để triển khai hiệu quả nội dung giải pháp này, trước hết cần xác lập rõ nguyên tắc chia sẻ và sử dụng dữ liệu, lấy minh bạch, kiểm soát và bảo vệ làm trọng tâm. Việc định nghĩa các khái niệm nền tảng như "chia sẻ dữ liệu", "sử dụng dữ liệu", "quyền truy cập", "mục đích sử dụng" phải được luật hóa hoặc cụ thể hóa thông qua các văn bản quy phạm pháp luật, bảo đảm không chồng chéo, mâu thuẫn với hệ thống pháp luật hiện hành về bảo vệ dữ liệu cá nhân, bí mật nhà nước và an ninh mạng.

Chính sách cần xây dựng cơ chế kiểm soát quyền truy cập dữ liệu dựa trên mô hình phân quyền chặt chẽ, áp dụng nguyên tắc "cần biết – cần dùng" và xác thực định danh số đối với mọi chủ thể truy cập dữ liệu. Mỗi hoạt động truy cập đều phải được ghi nhận bằng nhật ký hệ thống, bảo đảm khả năng truy vết, kiểm tra và xử lý trách nhiệm khi xảy ra sự cố lộ lọt dữ liệu. Mỗi cơ quan, tổ chức, doanh nghiệp có quyền quản lý tập dữ liệu thuộc phạm vi chức năng nhiệm vụ của mình cần thiết lập hệ thống quản trị truy cập, trong đó xác định rõ danh mục dữ liệu được chia sẻ, đối tượng được chia sẻ, thời điểm, hình thức và mục đích sử dụng. Việc phân tầng dữ liệu theo mức độ nhạy cảm, giá trị khai thác và rủi

ro bảo mật là bước tiền đề để thực hiện kiểm soát truy cập phù hợp, tránh tình trạng chia sẻ tràn lan hoặc thiếu kiểm soát dẫn đến mất an toàn dữ liệu.

Minh bạch hóa chính sách sử dụng dữ liệu đồng nghĩa với việc các tổ chức, cơ quan phải công khai các quy trình, tiêu chí và cơ chế xử lý liên quan đến việc khai thác dữ liệu. Cần quy định rõ các quyền và nghĩa vụ của bên cung cấp và bên tiếp nhận dữ liệu, đồng thời xác định rõ trách nhiệm pháp lý khi vi phạm các điều khoản sử dụng. Các chính sách này phải được cập nhật kịp thời, phù hợp với sự thay đổi của pháp luật, công nghệ và bối cảnh thực tiễn, đồng thời phải được truyền thông rộng rãi đến toàn bộ các đối tượng liên quan, từ cán bộ quản lý đến người dùng cuối. Việc tổ chức đào tạo, phổ biến kiến thức về chia sẻ và sử dụng dữ liệu một cách minh bạch sẽ góp phần hình thành văn hóa số lành mạnh, giảm thiểu rủi ro từ sự thiếu hiểu biết hoặc hành vi sử dụng dữ liệu sai mục đích.

Chính sách chia sẻ dữ liệu phải gắn liền với việc đánh giá, thẩm định và phân tích tác động dữ liệu trước khi ra quyết định chia sẻ, trong đó đặc biệt chú trọng đến các dữ liệu liên quan đến thông tin cá nhân, tài chính, y tế, hành vi tiêu dùng, di chuyển và các thông tin có khả năng gây tổn hại đến quyền riêng tư hoặc an ninh quốc gia. Việc sử dụng các công cụ đánh giá rủi ro như DPIA (Data Protection Impact Assessment) cần được bắt buộc triển khai đối với các cơ sở dữ liệu lớn, hệ thống thông tin trọng yếu hoặc các chương trình khai thác dữ liệu diện rộng. Đồng thời, cần có hội đồng tư vấn hoặc cơ quan chuyên trách độc lập đảm nhiệm việc đánh giá và giám sát liên tục quá trình chia sẻ và sử dụng dữ liệu tại các tổ chức, đặc biệt trong các hoạt động hợp tác công – tư, liên thông dữ liệu giữa các cơ quan nhà nước và doanh nghiệp.



Mô hình đảm bảo an toàn thông tin tổng thể cấp bộ, tỉnh. Ảnh minh họa. Nguồn từ Internet.

Vấn đề chia sẻ dữ liệu xuyên biên giới cần được đặt trong khuôn khổ pháp lý chặt chẽ, có sự điều tiết của Nhà nước, tránh tình trạng mất kiểm soát hoặc thất thoát dữ liệu nhạy cảm ra nước ngoài. Chính sách phải đưa ra yêu cầu rõ ràng về việc đánh giá mức độ an toàn pháp lý của quốc gia nhận dữ liệu, khả năng bảo vệ quyền riêng tư và cơ chế hợp tác quốc tế về an ninh mạng, bảo vệ dữ liệu. Cần áp dụng cơ chế "kiểm soát xuất khẩu dữ liệu" tương tự như kiểm soát hàng hóa chiến lược,

trong đó yêu cầu các tổ chức muốn chia sẻ dữ liệu ra nước ngoài phải đăng ký, thẩm định và được sự cho phép của cơ quan có thẩm quyền. Những dữ liệu có liên quan đến an ninh quốc gia, bí mật Nhà nước hoặc chưa có cơ chế bảo vệ rõ ràng thì tuyệt đối không được chia sẻ xuyên biên giới dưới bất kỳ hình thức nào.

Hệ thống chính sách chia sẻ và sử dụng dữ liệu minh bạch cũng cần tích hợp các công cụ công nghệ như blockchain để theo dõi chuỗi hành trình dữ liệu, các nền tảng quản trị dữ liệu tích hợp AI để tự động hóa quy trình phân tích rủi ro, cấp quyền truy cập, phát hiện sai phạm hoặc hành vi bất thường trong quá trình sử dụng dữ liệu. Các công cụ bảo vệ dữ liệu như tokenization, pseudonymization, differential privacy cần được triển khai để bảo đảm dữ liệu có thể được sử dụng vào mục đích phân tích, nghiên cứu, phát triển công nghệ mà không làm tổn hại đến thông tin cá nhân hay làm lộ lọt các đặc điểm nhận dạng cụ thể. Hệ sinh thái chia sẻ dữ liệu phải được phát triển dựa trên nguyên tắc đồng thuận, nghĩa là chỉ chia sẻ khi có sự cho phép rõ ràng, minh bạch từ chủ thể dữ liệu, đồng thời phải cung cấp cho họ khả năng kiểm tra, giám sát và thu hồi quyền chia sẻ nếu cần thiết.

Việc xây dựng chính sách chia sẻ dữ liệu hiệu quả đòi hỏi phải có khung thể chế đồng bộ, từ luật đến các văn bản hướng dẫn thi hành, đồng thời xây dựng một hệ thống chỉ số đánh giá định kỳ về mức độ tuân thủ, hiệu quả và tác động của chính sách đến các bên liên quan. Cơ chế phản hồi, khiếu nại, giải quyết tranh chấp về dữ liệu cần được xây dựng theo hướng nhanh chóng, minh bạch và công bằng. Các tổ chức độc lập, hiệp hội nghề nghiệp hoặc tổ chức xã hội dân sự có thể đóng vai trò giám sát, bảo vệ quyền lợi cho người dùng và góp phần nâng cao tính minh bạch của hệ thống chia sẻ dữ liệu.

Chính sách cần ưu tiên xây dựng các trung tâm dữ liệu quốc gia, nền tảng tích hợp dữ liệu dùng chung có kiểm soát, bảo đảm dữ liệu được lưu trữ, xử lý trong không gian mạng an toàn. Cơ chế kết nối, chia sẻ dữ liệu giữa các ngành, địa phương, cơ quan, doanh nghiệp phải đặt dưới sự điều phối tập trung, bảo đảm dữ liệu không bị trùng lặp, không bị thao túng, đồng thời giảm chi phí và tăng hiệu quả sử dụng. Trong quá trình chia sẻ dữ liệu, cần áp dụng các hợp đồng điện tử, điều khoản pháp lý minh bạch, có hiệu lực ràng buộc để tránh xảy ra tranh chấp, đồng thời xác định cơ chế xử lý vi phạm rõ ràng, có chế tài đủ mạnh, mang tính răn đe.

Đối với dữ liệu phục vụ nghiên cứu khoa học, phát triển công nghệ hoặc đổi mới sáng tạo, chính sách nên khuyến khích chia sẻ có kiểm soát thông qua các cơ chế như cấp phép truy cập, giới hạn mục đích và thời gian sử dụng, sử dụng dữ liệu đã được vô danh hóa. Tuy nhiên, ngay cả trong các trường hợp khuyến khích chia sẻ, vẫn cần tuân thủ nghiêm ngặt các quy định về bảo vệ dữ liệu cá nhân, quyền riêng tư, tránh việc sử dụng sai mục đích, làm tổn hại đến uy tín tổ chức, doanh nghiệp hoặc ảnh hưởng đến an ninh xã hội.

Việc liên hệ thực tiễn triển khai chính sách chia sẻ và sử dụng dữ liệu một cách minh bạch đối với lực lượng Công an nhân dân có ý nghĩa đặc biệt quan trọng, nhất là trong bối cảnh dữ liệu hình sự, dữ liệu dân cư, dữ liệu liên quan đến an ninh trật tự được coi là tài sản chiến lược, cốt lõi trong công tác nắm tình hình, phòng ngừa, đấu tranh và xử lý tội phạm. Lực lượng Công an cần chủ động phối hợp với các bộ, ngành xây dựng hệ thống chia sẻ dữ liệu liên ngành theo mô hình bảo mật ba lớp, áp dụng các công nghệ tiên tiến để bảo đảm chỉ cán bộ có thẩm quyền, có trách nhiệm và có định danh xác thực mới được truy cập. Đồng thời, phải kiểm soát chặt chẽ việc chia sẻ thông tin nghiệp vụ với các tổ chức, cá nhân ngoài ngành, nhất là trong các hợp tác quốc tế hoặc liên doanh công nghệ, bảo đảm không có hành vi lợi dụng, thu thập hoặc xuất khẩu trái phép

thông tin liên quan đến an ninh quốc gia. Công an nhân dân cũng phải là lực lượng nòng cốt trong giám sát thực thi chính sách chia sẻ dữ liệu tại các tổ chức, doanh nghiệp, đồng thời tổ chức thanh tra, kiểm tra chuyên đề và điều tra xử lý nghiêm các hành vi chia sẻ trái phép, sử dụng sai mục đích hoặc gây rò rỉ dữ liệu nghiêm trọng ảnh hưởng đến lợi ích quốc gia, quyền và lợi ích hợp pháp của tổ chức, công dân.

2.2.8. Tăng cường cơ chế phối hợp, chia sẻ thông tin và hỗ trợ kỹ thuật giữa các cơ quan quản lý nhà nước, doanh nghiệp, tổ chức trung gian và lực lượng chuyên trách về an ninh mạng, an ninh thông tin

Việc tăng cường cơ chế phối hợp, chia sẻ thông tin và hỗ trợ kỹ thuật giữa các cơ quan quản lý nhà nước, doanh nghiệp, tổ chức trung gian và lực lượng chuyên trách về an ninh mạng, an ninh thông tin là một giải pháp mang tính nền tảng và có ý nghĩa quyết định trong việc nâng cao năng lực phòng ngừa, ứng phó và khắc phục sự cố về dữ liệu và an toàn thông tin trong bối cảnh hiện nay. Trước tiên, cần xác định rõ trách nhiệm và quyền hạn của từng chủ thể tham gia vào hệ sinh thái an toàn thông tin, từ đó hình thành một cơ chế phối hợp liên ngành hiệu quả, chặt chẽ và liên tục. Trong đó, các bộ, ngành quản lý lĩnh vực dữ liệu và an ninh thông tin như Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng, Bộ Khoa học và Công nghệ… cần cùng nhau xây dựng khung pháp lý liên thông, đồng bộ, tạo điều kiện pháp lý thuận lợi cho quá trình chia sẻ thông tin và phối hợp hành động. Đây là bước khởi đầu để thiết lập một mạng lưới phòng thủ chủ động trên không gian mạng, trong đó mỗi cơ quan đều là một mắt xích đóng vai trò cảnh báo, ứng cứu, và điều phối nguồn lực trong trường hợp xảy ra sự cố.

Việc xây dựng cơ chế chia sẻ thông tin cần được đặt trên nền tảng tin cậy, bảo mật và bảo đảm các quy định pháp lý về bảo vệ dữ liệu cá nhân, bí mật doanh nghiệp, bí mật nhà nước. Do đó, cần thiết lập các giao thức chia sẻ thông tin thống nhất,

có sự chuẩn hóa theo mô hình quốc tế như STIX, TAXII… để các hệ thống kỹ thuật của các đơn vị khác nhau có thể tương tác và khai thác dữ liệu một cách mạch lạc, an toàn. Các trung tâm giám sát an toàn thông tin (SOC) quốc gia và địa phương đóng vai trò then chốt trong việc tiếp nhận, phân tích, đánh giá và lan truyền thông tin cảnh báo sự cố đến các đơn vị liên quan. Đồng thời, cũng cần quy định rõ về tần suất chia sẻ, loại thông tin cần chia sẻ, cấp độ cảnh báo, từ đó hình thành một "bản đồ" rủi ro an ninh mạng mang tính thời gian thực, giúp các cơ quan, doanh nghiệp chủ động hơn trong phòng ngừa và ứng phó.

Đối với doanh nghiệp, nhất là các doanh nghiệp công nghệ, viễn thông, ngân hàng, tài chính, bảo hiểm – những nơi sở hữu và xử lý khối lượng lớn dữ liệu nhạy cảm – cần được khuyến khích và tạo điều kiện để tham gia sâu vào quá trình chia sẻ thông tin và hỗ trợ kỹ thuật. Nhà nước cần có cơ chế bảo hộ và miễn trừ trách nhiệm phù hợp đối với doanh nghiệp khi cung cấp thông tin liên quan đến sự cố mạng, tránh tình trạng e ngại pháp lý hoặc tổn hại uy tín thương hiệu. Việc thiết lập các diễn đàn chuyên ngành, nhóm công tác công – tư (PPP) về an toàn thông tin, các chương trình đào tạo, hội nghị chia sẻ kinh nghiệm giữa doanh nghiệp và cơ quan quản lý là cách làm hiệu quả để xây dựng lòng tin, tăng cường gắn kết và nâng cao trình độ chuyên môn cho toàn hệ thống.

Tổ chức trung gian như các trung tâm hỗ trợ doanh nghiệp chuyển đổi số, viện nghiên cứu, trường đại học, các hiệp hội chuyên ngành cần đóng vai trò cầu nối kỹ thuật và tri thức giữa nhà nước và doanh nghiệp. Họ có thể cung cấp các nền tảng phân tích dữ liệu, công cụ mô phỏng rủi ro, đánh giá an ninh hệ thống hoặc hỗ trợ triển khai các công nghệ bảo mật tiên tiến như mã hóa dữ liệu, trí tuệ nhân tạo trong giám sát bất thường… Ngoài ra, cũng cần tăng cường hợp tác quốc tế với các tổ chức đa phương như ITU, ASEAN CERT, INTERPOL, FIRST... nhằm tiếp nhận kinh nghiệm, học hỏi mô hình quốc tế và

cập nhật liên tục các mối đe dọa mới trong không gian mạng. Các chương trình hỗ trợ kỹ thuật từ nước ngoài, viện trợ không hoàn lại về công nghệ bảo mật cũng cần được triển khai đúng đối tượng, đúng nhu cầu và giám sát chặt chẽ quá trình tiếp nhận, ứng dụng tại địa phương.

Một cơ chế phối hợp hiệu quả không thể thiếu sự phân tầng và phân cấp rõ ràng trong điều phối thông tin và hành động. Cần thiết lập hệ thống đầu mối liên lạc chuyên trách tại các cơ quan, doanh nghiệp, đơn vị sự nghiệp để đảm bảo mỗi đơn vị đều có ít nhất một cán bộ kỹ thuật, cán bộ pháp lý am hiểu về an ninh mạng và có quyền truy cập hệ thống chia sẻ cảnh báo. Ngoài ra, cần xây dựng bộ quy trình chuẩn khi xảy ra sự cố, trong đó mô tả cụ thể trình tự hành động, đối tượng chịu trách nhiệm, thời gian báo cáo, hình thức hỗ trợ kỹ thuật cần thiết… nhằm tránh tình trạng chồng chéo, đùn đẩy trách nhiệm hoặc phản ứng chậm trễ. Đặc biệt, việc xây dựng các bài tập mô phỏng, diễn tập an ninh mạng định kỳ là công cụ quan trọng để kiểm tra mức độ sẵn sàng phối hợp của các chủ thể, đồng thời củng cố khả năng điều hành thực tế khi khủng hoảng xảy ra.

Để tăng cường hiệu quả hỗ trợ kỹ thuật, cần đầu tư xây dựng hệ thống hỗ trợ từ xa có khả năng giám sát, khắc phục sự cố, cập nhật bản vá bảo mật và nâng cấp hệ thống theo yêu cầu. Các hình thức hỗ trợ có thể bao gồm đường dây nóng 24/7,

hệ thống cảnh báo sớm tự động, trung tâm tư vấn qua mạng, đội phản ứng nhanh (CSIRT) chuyên biệt theo lĩnh vực và khu vực địa lý. Việc chuẩn hóa quy trình hỗ trợ kỹ thuật và có cơ chế phân loại mức độ ưu tiên theo tính chất và quy mô sự cố sẽ giúp tối ưu nguồn lực kỹ thuật trong xử lý và phục hồi. Hơn nữa, các cơ quan quản lý nhà nước cần duy trì kho lưu trữ công cụ, phần mềm bảo mật bản quyền dùng chung cho các đơn vị khó khăn về tài chính hoặc hạ tầng, đặc biệt là các cơ quan cấp xã, huyện, trường học và bệnh viện.

Chính phủ cũng cần xem xét xây dựng quỹ hỗ trợ ứng cứu an ninh mạng tương tự như quỹ phòng chống thiên tai, trong đó có thể huy động nguồn lực xã hội hóa từ các doanh nghiệp, tổ chức quốc tế, viện trợ nước ngoài… để đảm bảo khả năng chi viện nhanh chóng khi cần thiết. Quỹ này cũng có thể tài trợ cho các sáng kiến nghiên cứu ứng dụng công nghệ bảo mật, phát triển phần mềm mã nguồn mở phục vụ công cộng hoặc tổ chức các chương trình đào tạo, sát hạch chuyên gia an ninh mạng trong nước. Việc đầu tư vào nguồn nhân lực chất lượng cao cũng cần được chú trọng thông qua học bổng ngành an toàn thông tin, chương trình hợp tác quốc tế trao đổi sinh viên – giảng viên, đào tạo giảng viên nòng cốt tại các trường kỹ thuật.

Trong bối cảnh nhiều vụ tấn công mạng xuất phát từ nước ngoài, liên kết xuyên quốc gia và có tổ chức tinh vi, vai trò của các hiệp định hợp tác song phương và đa phương trong lĩnh vực an ninh mạng cần được phát huy. Việt Nam cần chủ động đàm phán các hiệp định chia sẻ thông tin, tương trợ tư pháp và dẫn độ tội phạm công nghệ cao; đồng thời tham gia tích cực vào các tổ chức quốc tế để bảo vệ quyền lợi quốc gia, học hỏi kinh nghiệm, tranh thủ hỗ trợ và đóng góp tiếng nói của mình vào việc xây dựng luật chơi chung trên không gian mạng toàn cầu. Đây cũng là điều kiện để nâng cao vị thế của Việt Nam trên trường quốc tế trong lĩnh vực bảo đảm an ninh thông tin, an ninh dữ liệu và chủ quyền số.

Đối với lực lượng Công an nhân dân, việc tham gia vào cơ chế phối hợp, chia sẻ thông tin và hỗ trợ kỹ thuật là nhiệm vụ then chốt nhằm bảo đảm chủ quyền không gian mạng, giữ gìn an ninh chính trị, trật tự an toàn xã hội trong môi trường số. Lực lượng chuyên trách về an ninh mạng, an ninh thông tin trong Công an nhân dân cần phát huy vai trò nòng cốt trong tiếp nhận, xử lý, xác minh và cảnh báo sớm các mối đe dọa đối với hệ thống thông tin trọng yếu quốc gia, đặc biệt là các hệ thống liên quan đến quốc phòng, an ninh, tài chính – ngân hàng, giao thông, y tế, giáo dục… Đồng thời, lực lượng Công an cần phối hợp chặt chẽ với các cơ quan, doanh nghiệp để truy vết nguồn gốc tấn công, thu thập chứng cứ số, phục vụ điều tra và xử lý theo quy định pháp luật. Ngoài ra, cần thường xuyên tổ chức tập huấn, diễn tập phối hợp với các đơn vị ngoài ngành để nâng cao năng lực thực chiến, chủ động xây dựng kịch bản ứng phó với các tình huống tấn công mạng diện rộng, có yếu tố nước ngoài. Đây không chỉ là trách nhiệm nghiệp vụ mà còn là phương thức thể hiện vai trò tiên phong, là lá chắn vững chắc trên tuyến đầu bảo vệ an ninh không gian mạng quốc gia của lực lượng Công an nhân dân.

Tạm kết câu 7

Phần trả lời câu hỏi số 7 đã tập trung làm rõ các quy định liên quan đến sản phẩm, dịch vụ về dữ liệu trong bối cảnh chuyển đổi số, nhấn mạnh yêu cầu về tính pháp lý, minh bạch và tiêu chuẩn kỹ thuật đối với hoạt động cung cấp, khai thác dữ liệu. Đồng thời, nội dung cũng phân tích các giải pháp toàn diện nhằm bảo đảm an ninh, an toàn dữ liệu từ thể chế, công nghệ đến tổ chức thực thi, qua đó góp phần bảo vệ chủ quyền dữ liệu quốc gia, tăng cường niềm tin xã hội và tạo nền tảng phát triển kinh tế số, xã hội số an toàn, bền vững.

Tuổi trẻ Công an tỉnh Cà Mau tổ chức nhiều hoạt động hưởng ứng Ngày Chuyển đổi số (Ảnh Sưu tầm)

BÀI DỰ THI TÌM HIỂU

LUẬT DỮ LIỆU TRONG CÔNG AN NHÂN DÂN

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.

Tóm tắt: *Quản lý nhà nước về dữ liệu là quá trình tổ chức, điều hành các hoạt động liên quan đến dữ liệu nhằm bảo đảm thống nhất, hiệu quả trong xây dựng, quản lý, khai thác, chia sẻ, bảo vệ và phát triển dữ liệu phục vụ phát triển kinh tế – xã hội, quốc phòng – an ninh. Nội dung quản lý bao gồm xây dựng thể chế, kiến trúc dữ liệu, hạ tầng kỹ thuật, quy trình vận hành, tiêu chuẩn, định danh dữ liệu và bảo đảm an ninh, an toàn dữ liệu.*

Bộ Công an có vai trò nòng cốt trong quản lý nhà nước về dữ liệu liên quan đến an ninh quốc gia, trật tự, an toàn xã hội, trực tiếp xây dựng, vận hành Cơ sở dữ liệu quốc gia về dân cư, cấp số định danh cá nhân, bảo đảm an ninh hệ thống thông tin, an toàn dữ liệu; đồng thời phối hợp với các bộ, ngành khai thác, chia sẻ dữ liệu phục vụ cải cách hành chính, phát triển Chính phủ số. Công an các đơn vị, địa phương chịu trách nhiệm tổ chức thực hiện nhiệm vụ quản lý, bảo mật, khai thác, cập nhật dữ liệu đúng quy định pháp luật; chủ động tham mưu triển khai các giải pháp bảo vệ an ninh dữ liệu trên địa bàn.

Giai đoạn từ nay đến năm 2030, cần tập trung hoàn thiện thể chế quản lý dữ liệu, xây dựng đồng bộ hạ tầng kỹ thuật và kiến trúc dữ liệu quốc gia, nâng cao năng lực phân tích và khai thác dữ liệu lớn (big data), phát triển nguồn nhân lực chất lượng cao về dữ liệu, đẩy mạnh kết nối, chia sẻ, mở dữ liệu giữa các cơ quan nhà nước, bảo đảm dữ liệu an toàn, chính xác và phục vụ hiệu quả cho phát triển kinh tế – xã hội, bảo vệ an ninh quốc gia.

PHẦN I

NỘI DUNG QUẢN LÝ NHÀ NƯỚC VỀ DỮ LIỆU

I. NỘI DUNG QUẢN LÝ

1.1. 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.

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 là việc hoạch định tầm nhìn, 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 *(như Luật, Nghị định, Thông tư...)* 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 tạo dựng niềm tin để người dân sẵn sàng chia sẽ 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.

Xây dựng và hoàn thiện hệ thống văn bản quy phạm pháp luật về dữ liệu mang ý nghĩa cấp thiết nhằm tạo hành lang pháp lý đầy đủ, rõ ràng, minh bạch và có tính khả thi cao để điều chỉnh toàn diện các hoạt động phát sinh trong vòng đời dữ liệu. Pháp luật về dữ liệu cần bảo đảm điều chỉnh từ quá trình thu thập, lưu trữ, xử lý, khai thác, chia sẻ đến bảo vệ và thương mại hóa dữ liệu, đồng thời đáp ứng các yêu cầu về an toàn thông tin, quyền riêng tư và chủ quyền số quốc gia.

Ảnh minh họa. Nguồn từ Internet

Luật Dữ liệu là đạo luật nền tảng có vai trò thiết lập hệ thống nguyên tắc, định nghĩa, phạm vi điều chỉnh, quyền và nghĩa vụ của các chủ thể liên quan đến dữ liệu. Đây là bộ khung pháp lý cao nhất trong lĩnh vực dữ liệu, có chức năng làm rõ quan hệ giữa Nhà nước, doanh nghiệp, tổ chức và cá nhân trong quá trình tạo lập, kiểm soát và sử dụng dữ liệu. Luật Dữ liệu cần quy định rõ quyền sở hữu, quyền quản lý, quyền khai thác dữ liệu, phân loại dữ liệu theo các cấp độ công khai, hạn chế

truy cập hoặc mật theo tiêu chí an ninh quốc gia, bảo vệ quyền riêng tư và lợi ích hợp pháp của công dân. Trong Luật, cũng cần khẳng định nguyên tắc dữ liệu là tài sản đặc biệt có thể khai thác giá trị kinh tế nhưng không được vi phạm quyền lợi cá nhân và lợi ích cộng đồng.

Cùng với Luật Dữ liệu, hệ thống nghị định hướng dẫn thi hành đóng vai trò cụ thể hóa các quy định mang tính nguyên tắc thành các cơ chế, biện pháp tổ chức thực hiện. Các nghị định cần đề cập đến phương thức cấp phép hoặc cho phép sử dụng dữ liệu thuộc sở hữu nhà nước, cơ chế thu phí hoặc định giá dịch vụ dữ liệu, các mô hình hợp tác công – tư trong khai thác hạ tầng và dịch vụ dữ liệu. Nghị định cũng cần làm rõ các chế tài xử lý vi phạm đối với hành vi xâm phạm dữ liệu cá nhân, làm giả, làm sai lệch, đánh cắp hoặc chia sẻ dữ liệu trái phép, quy định về trách nhiệm của các cơ quan nhà nước, tổ chức, doanh nghiệp trong việc bảo đảm an toàn, bảo mật dữ liệu trong suốt vòng đời khai thác.

Hệ thống tiêu chuẩn và quy chuẩn kỹ thuật về dữ liệu có vai trò then chốt trong bảo đảm tính liên thông, khả năng tích hợp, tính tương thích và an toàn cho toàn bộ hệ sinh thái dữ liệu quốc gia. Việc xây dựng các bộ tiêu chuẩn phải bảo đảm đồng bộ giữa cấu trúc dữ liệu, mô hình siêu dữ liệu, ngôn ngữ đánh dấu, giao thức trao đổi, khung phân loại và các mã định danh dùng chung. Tiêu chuẩn hóa giúp giảm chi phí xử lý dữ liệu, tạo điều kiện thuận lợi cho chia sẻ, đồng bộ và khai thác dữ liệu xuyên ngành, liên thông các cấp chính quyền, giữa khu vực công và tư. Bên cạnh đó, quy chuẩn kỹ thuật về dữ liệu có chức năng điều chỉnh cụ thể đối với từng lĩnh vực, chẳng hạn như quy chuẩn dữ liệu về y tế, giáo dục, tài chính, môi trường, dân cư, an ninh trật tự… được ban hành bởi cơ quan quản lý chuyên ngành theo hướng dẫn chung của cơ quan quản lý về chuyển đổi số.

Định danh điện tử là nền tảng quan trọng để bảo đảm tính xác thực và an toàn trong các giao dịch số, là chìa khóa liên kết cá nhân, tổ chức với thế giới dữ liệu. Việc xây dựng hành lang pháp lý về định danh điện tử cần xác lập các nguyên tắc định danh duy nhất, không trùng lặp, khả năng kiểm chứng, cập nhật và sử dụng xuyên suốt trong các hoạt động điện tử của công dân và tổ chức. Pháp luật cần xác định rõ trách nhiệm của các cơ quan cung cấp định danh, phạm vi sử dụng, nguyên tắc bảo mật thông tin định danh và cơ chế xử lý khi có vi phạm hoặc sự cố phát sinh. Định danh điện tử cũng phải tương thích với hệ thống nhận diện công dân quốc gia và các nền tảng dữ liệu liên quan như cơ sở dữ liệu dân cư, căn cước công dân gắn chip, dữ liệu về giao dịch tài chính, thông tin y tế, giáo dục, an sinh xã hội.

Xác thực điện tử là quá trình kiểm tra và bảo đảm rằng chủ thể truy cập và sử dụng dữ liệu là người hoặc tổ chức đã được định danh hợp lệ. Quy định pháp luật về xác thực cần thiết lập các mức độ xác thực theo tính chất và độ nhạy cảm của dữ liệu, từ mức cơ bản đến mức nâng cao sử dụng công nghệ như OTP, sinh trắc học, chữ ký số hoặc chứng thực điện tử. Các hình thức xác thực cần được quy định rõ ràng, công khai, có cơ chế kiểm soát và lưu vết toàn bộ quá trình truy cập và giao dịch dữ liệu nhằm tăng cường tính minh bạch, hạn chế các hành vi giả mạo hoặc chiếm đoạt quyền truy cập.

Bảo mật dữ liệu là nội dung xuyên suốt trong mọi giai đoạn quản lý dữ liệu. Hành lang pháp lý cần đặt ra các yêu cầu tối thiểu về bảo mật trong thiết kế hệ thống dữ liệu, phân quyền truy cập, mã hóa, sao lưu, phục hồi, kiểm tra định kỳ và ứng phó với sự cố. Cần có quy định cụ thể về đánh giá rủi ro bảo mật dữ liệu theo từng lĩnh vực, xác định cấp độ an toàn thông tin tương ứng với từng loại dữ liệu. Cơ chế giám sát, thanh tra và xử lý vi phạm về bảo mật dữ liệu cũng cần được luật hóa với các quy định rõ ràng về trách nhiệm cá nhân, tổ chức, nhất là đối với cán bộ, công chức, viên chức được giao quản lý dữ liệu công vụ.

Chia sẻ dữ liệu là điều kiện tiên quyết để phát huy giá trị dữ liệu trong phục vụ người dân, doanh nghiệp và điều hành của Nhà nước. Cơ chế pháp lý cho hoạt động chia sẻ dữ liệu cần làm rõ nguyên tắc bắt buộc chia sẻ trong nội bộ hệ thống chính quyền, khuyến khích chia sẻ giữa khu vực công và tư, bảo đảm sự đồng thuận về quyền, trách nhiệm và lợi ích giữa các bên. Cần quy định rõ các hình thức chia sẻ như chia sẻ mở, chia sẻ có điều kiện, chia sẻ qua nền tảng trung gian hoặc thông qua các dịch vụ API. Luật hóa việc chia sẻ dữ liệu giúp tránh tình trạng cát cứ, độc quyền dữ liệu, thúc đẩy tính liên thông, giảm thiểu trùng lặp trong thu thập và lưu trữ dữ liệu.

Giao dịch dữ liệu là một bước phát triển tất yếu trong nền kinh tế số, đòi hỏi khuôn khổ pháp lý bảo đảm tính minh bạch, an toàn và bảo vệ quyền lợi của các bên liên quan. Cần có quy định pháp luật về điều kiện cho phép giao dịch dữ liệu, thẩm quyền cấp phép, các loại dữ liệu được phép mua bán, định giá dữ liệu, cơ chế bảo vệ thông tin cá nhân trong quá trình giao dịch. Pháp luật cũng cần làm rõ trách nhiệm của sàn giao dịch dữ liệu, quyền và nghĩa vụ của bên cung cấp và bên sử dụng dữ liệu, cơ chế xử lý tranh chấp, vi phạm trong giao dịch. Giao dịch dữ liệu cũng cần tuân thủ các nguyên tắc về an ninh mạng, bảo vệ chủ quyền dữ liệu quốc gia và không làm ảnh hưởng đến lợi ích quốc gia, dân tộc.

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.

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, đặc biệt là trong bộ máy hệ thống chính trị; 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 tiễn vi mô. Nhiều cơ quan, địa phương có thê còn lúng túng về mặt kỹ thuật, thiếu nhân lực và kinh nghiệm đề quản trị dữ liệu hiệu quả.

Sự hướng dẫn từ cơ quan quản lý nhà nước sẽ bảo đảm 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.

Tổ chức thực hiện các chính sách về phát triển hạ tầng dữ liệu, bao gồm việc xây dựng và vận hành Cơ sở dữ liệu quốc gia, các trung tâm dữ liệu, sàn dữ liệu, nền tảng chia sẻ dữ liệu và các hệ thống định danh số nhằm bảo đảm liên thông dữ liệu giữa các ngành, địa phương và doanh nghiệp

Quản lý nhà nước về dữ liệu là một lĩnh vực tổng hợp, phức tạp, đòi hỏi sự tham gia đồng bộ của nhiều cấp, nhiều ngành nhằm thiết lập một nền tảng dữ liệu vững chắc cho phát triển chính phủ số, kinh tế số và xã hội số. Trong đó, tổ chức thực hiện các chính sách phát triển hạ tầng dữ liệu là trụ cột quan trọng nhằm tạo ra hệ sinh thái dữ liệu thống nhất, liên thông, an toàn và hiệu quả. Nội dung này không chỉ bao gồm việc ban hành cơ chế, chính sách mà còn đòi hỏi tổ chức thực hiện đồng bộ từ trung ương đến địa phương, từ khu vực công đến khu vực tư nhân với sự đầu tư có trọng tâm, trọng điểm, đảm bảo hạ tầng dữ liệu trở thành nền móng kỹ thuật và thể chế cho toàn bộ quá trình quản trị dữ liệu quốc gia.

Xây dựng và vận hành Cơ sở dữ liệu quốc gia là nhiệm vụ trung tâm trong phát triển hạ tầng dữ liệu, có chức năng tích hợp, đồng bộ thông tin từ các cơ sở dữ liệu chuyên ngành, địa phương và doanh nghiệp, tạo nên một kho dữ liệu lớn có khả năng phục vụ đa mục đích. Cơ sở dữ liệu quốc gia cần được thiết kế theo hướng mở rộng, linh hoạt, có khả năng mở rộng quy

mô và tích hợp dữ liệu mới, bảo đảm tính toàn vẹn, nhất quán, chính xác và cập nhật liên tục. Quản lý nhà nước đối với cơ sở dữ liệu quốc gia đòi hỏi thiết lập các quy chế rõ ràng về quyền truy cập, phân quyền khai thác, cập nhật, sử dụng và giám sát chất lượng dữ liệu. Việc phân loại dữ liệu, định danh dữ liệu theo lĩnh vực, đối tượng và cấp độ bảo mật cần được quy định chặt chẽ để bảo đảm cơ sở dữ liệu vận hành an toàn, hiệu quả và không xâm phạm đến các quyền cá nhân, tổ chức.

Ảnh minh họa. Nguồn từ Internet

Phát triển các trung tâm dữ liệu là yêu cầu tất yếu trong quá trình số hóa, nhằm tạo lập các hạ tầng vật lý và logic phục vụ lưu trữ, xử lý, bảo mật và truyền tải dữ liệu số với khối lượng ngày càng lớn. Trung tâm dữ liệu cần được quy hoạch theo mô hình phân tán và tập trung, bảo đảm vừa có tính độc lập để giảm thiểu rủi ro cục bộ, vừa có khả năng liên kết để đồng bộ và chia sẻ dữ liệu. Các trung tâm dữ liệu của Nhà nước phải đạt các tiêu chuẩn kỹ thuật quốc tế về an toàn thông tin, tiết kiệm năng lượng, khả năng mở rộng và phục hồi sau sự cố. Việc đầu tư, vận hành và giám sát trung tâm dữ liệu cần được thực hiện bởi các cơ quan có năng lực, với sự phối hợp chặt chẽ giữa cơ quan chuyên môn, đơn vị quản lý vận hành và lực lượng an ninh mạng. Cần có quy định rõ về phân cấp quản lý, phân vùng dữ liệu theo mức độ quan trọng và cơ chế sao lưu để bảo đảm hoạt động thông suốt, ổn định trong mọi tình huống.

Sàn dữ liệu là mô hình mới trong hạ tầng dữ liệu quốc gia, đóng vai trò là trung gian kết nối giữa người sở hữu dữ liệu và người sử dụng dữ liệu. Quản lý nhà nước cần định hình khung pháp lý cho hoạt động của các sàn dữ liệu, bao gồm tiêu chí thành lập, điều kiện kỹ thuật, nghĩa vụ công bố thông tin, cơ chế định giá dữ liệu, bảo vệ quyền sở hữu và quyền riêng tư trong quá trình giao dịch. Sàn dữ liệu không chỉ là nơi giao dịch dữ liệu, mà còn là không gian thúc đẩy đổi mới sáng tạo, kết nối giữa các cơ quan nhà nước, doanh nghiệp và nhà nghiên cứu trong việc sử dụng dữ liệu cho các mục tiêu phát triển. Việc phát triển các sàn dữ liệu cần được gắn liền với chiến lược phát triển kinh tế số quốc gia, bảo đảm tính minh bạch, hiệu quả và kiểm soát được rủi ro liên quan đến dữ liệu cá nhân, dữ liệu nhạy cảm và dữ liệu thuộc phạm vi bí mật nhà nước.

Nền tảng chia sẻ dữ liệu là thành phần thiết yếu bảo đảm tính kết nối, liên thông và tái sử dụng dữ liệu giữa các hệ thống thông tin khác nhau, giữa các bộ, ngành, địa phương và khu vực tư nhân. Hạ tầng chia sẻ dữ liệu quốc gia cần được xây dựng trên nguyên tắc mở, bảo mật và tương thích, sử dụng các giao diện lập trình ứng dụng (API) tiêu chuẩn để tạo điều kiện cho việc tích hợp dữ liệu một cách linh hoạt, dễ dàng và có kiểm soát. Việc thiết lập nền tảng chia sẻ dữ liệu cần gắn liền với việc xây dựng kiến trúc tổng thể về dữ liệu quốc gia, bảo đảm mỗi loại dữ liệu chỉ được thu thập một lần, có thể sử dụng nhiều lần, được phân quyền theo mức độ và được giám sát bởi cơ quan có thẩm quyền. Cần có quy định rõ về quyền chia sẻ, nghĩa vụ bảo mật, quy trình kiểm duyệt và hậu kiểm việc chia sẻ để tránh lạm dụng, thất thoát hoặc sử dụng sai mục đích dữ liệu.

Hệ thống định danh số là nền móng để xác định chính xác các thực thể tham gia vào môi trường số, bảo đảm tính xác thực, minh bạch và an toàn trong truy cập, giao dịch và sử dụng dữ liệu. Xây dựng hệ thống định danh số quốc gia cần được đồng bộ với cơ sở dữ liệu dân cư, mã số định danh cá nhân, tổ chức và doanh nghiệp, đảm bảo mỗi đối tượng được gán một mã duy nhất, không thay đổi trong suốt vòng đời. Định danh số cần được mở rộng áp dụng trên toàn bộ hệ thống hành chính công, dịch vụ công, tài chính – ngân hàng, giáo dục, y tế và các lĩnh vực có yêu cầu bảo mật cao. Cần hoàn thiện quy định pháp lý về định danh số, trong đó xác định rõ cơ quan quản lý định danh, quy trình cấp, quản lý và hủy bỏ mã định danh, quyền và nghĩa vụ của người được định danh, cơ chế kiểm tra và xác minh định kỳ, xử lý sự cố và tranh chấp liên quan đến thông tin định danh.

Công an tỉnh Cà Mau hưởng ứng Ngày Chuyển đổi số quốc gia năm 2024 (ngày 10/10) với chủ đề "Phổ cập hạ tầng số và sáng tạo ứng dụng số để phát triển kinh tế số - Động lực mới cho tăng trưởng kinh tế và năng suất lao động".

Ảnh Báo Cà Mau

Việc bảo đảm liên thông dữ liệu giữa các ngành, địa phương và doanh nghiệp là mục tiêu trọng tâm trong phát triển hạ tầng dữ liệu quốc gia, nhằm xóa bỏ tình trạng phân mảnh, cát cứ dữ liệu và khai thác tối đa giá trị của dữ liệu cho phát triển bền vững. Quản lý nhà nước cần thiết lập cơ chế bắt buộc chia sẻ dữ liệu dùng chung giữa các cơ quan nhà nước, cơ chế

khuyến khích chia sẻ dữ liệu giữa khu vực công và khu vực tư nhân, có sự phân loại dữ liệu rõ ràng để xác định phạm vi chia sẻ, mức độ công khai và điều kiện tiếp cận. Việc thiết lập các nguyên tắc chia sẻ cần gắn liền với tiêu chuẩn kỹ thuật chung, sử dụng nền tảng tích hợp dữ liệu, bảo đảm mỗi đơn vị đều có quyền truy cập hợp pháp nhưng phải tuân thủ trách nhiệm về bảo mật, kiểm soát và giám sát việc sử dụng dữ liệu. Cần có hệ thống theo dõi việc chia sẻ, công cụ đánh giá hiệu quả và mức độ sử dụng dữ liệu để kịp thời phát hiện và xử lý vi phạm, đồng thời nâng cao chất lượng quản lý, điều hành và ra quyết định của các cơ quan nhà nước, doanh nghiệp.

Đối với lực lượng Công an nhân dân, việc tổ chức thực hiện các chính sách phát triển hạ tầng dữ liệu có ý nghĩa đặc biệt trong việc phục vụ bảo đảm an ninh quốc gia, trật tự an toàn xã hội và phòng, chống tội phạm trong môi trường số. Lực lượng Công an là đơn vị nắm giữ nhiều loại dữ liệu trọng yếu như dữ liệu dân cư, dữ liệu về tội phạm, an ninh, trật tự, giao thông, cư trú, xuất nhập cảnh và dữ liệu định danh công dân. Việc xây dựng và vận hành các trung tâm dữ liệu, hệ thống chia sẻ và nền tảng tích hợp dữ liệu liên thông giữa Bộ Công an với các bộ, ngành khác góp phần nâng cao hiệu quả điều tra, truy vết, phân tích tình hình, dự báo nguy cơ và điều hành tác chiến. Đồng thời, việc bảo vệ an toàn dữ liệu trong hạ tầng kỹ thuật số là nhiệm vụ sống còn, đòi hỏi lực lượng Công an triển khai các biện pháp giám sát, ứng phó và phản ứng nhanh với các hành vi tấn công mạng, xâm nhập dữ liệu, phá hoại cơ sở hạ tầng số. Bên cạnh đó, lực lượng Công an cần tham gia xây dựng tiêu chuẩn an ninh cho các trung tâm dữ liệu, hệ thống định danh và nền tảng chia sẻ dữ liệu, góp phần bảo vệ chủ quyền dữ liệu quốc gia, bảo đảm an ninh dữ liệu và bảo vệ người dân trong môi trường số hóa.

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 về kinh tế, xã hội và thậm chí là an ninh quốc gia, trật tự, an toàn xã hội.

Hoạt động quản lý và giám sát phải được thực hiện một cách chủ động, liên tục, thay vì chi phản ứng khi sự cố đã 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.

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 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 tính thượng tôn pháp luật và duy trì lợi thế cạnh tranh của quốc gia trong chuyển đổi số.

Bảo vệ quyền và lợi ích hợp pháp của chủ thể dữ liệu là một nội dung trung tâm trong quản lý nhà nước về dữ liệu, thể hiện rõ vai trò định hướng, kiểm soát và can thiệp của Nhà nước nhằm thiết lập môi trường dữ liệu số an toàn, công bằng, minh bạch. Trọng tâm là bảo vệ dữ liệu cá nhân và dữ liệu thuộc danh mục cốt lõi hoặc quan trọng, vừa để gìn giữ quyền riêng tư, vừa duy trì ổn định xã hội và đảm bảo an ninh quốc gia trong bối cảnh chuyển đổi số mạnh mẽ.

Dữ liệu cá nhân là một dạng tài sản phi vật chất, mang tính nhận diện cá thể, dễ bị tổn hại nếu bị thu thập, xử lý, chia sẻ hay sử dụng sai mục đích. Quản lý nhà nước về dữ liệu cần xây dựng các quy định pháp lý rõ ràng về phạm vi dữ liệu cá nhân, tiêu chí phân loại dữ liệu đặc biệt nhạy cảm, điều kiện xử lý dữ liệu và các chế tài nghiêm ngặt đối với hành vi vi phạm. Đối với dữ liệu cốt lõi hoặc quan trọng, bao gồm dữ liệu về quốc phòng, an ninh, sức khỏe cộng đồng, tài nguyên quốc gia hay thông tin tài chính – ngân hàng, cần có cơ chế quản lý riêng biệt, phân cấp tiếp cận rõ ràng và yêu cầu bảo mật nghiêm ngặt hơn so với dữ liệu thông thường.

Thiết lập cơ chế đồng ý là yêu cầu bắt buộc trong mọi quy trình xử lý dữ liệu. Cơ chế này đòi hỏi người dùng phải được thông báo đầy đủ, rõ ràng về mục đích, phạm vi, thời gian lưu trữ và bên thứ ba liên quan đến dữ liệu của họ. Việc thu thập dữ liệu không được diễn ra một cách mặc định hoặc đánh lừa, mà cần có sự chủ động và minh thị từ chủ thể dữ liệu, thể hiện qua các hành vi như đánh dấu vào ô đồng ý hoặc ký xác nhận điện tử. Ngoài ra, quyền được thu hồi sự đồng ý và phản đối xử lý dữ liệu phải được ghi nhận như một nguyên tắc cốt lõi nhằm trao lại quyền kiểm soát thông tin cho người dân. Nhà nước có trách nhiệm định nghĩa rõ điều kiện, thủ tục và hệ quả pháp lý của việc thu hồi đồng ý hay phản đối, đồng thời yêu cầu các tổ chức, doanh nghiệp xây dựng giao diện và quy trình kỹ thuật thân thiện, đơn giản để bảo đảm quyền này được thực thi thực tế.

Quá trình thu thập, lưu trữ, xử lý và sử dụng dữ liệu phải được thực hiện một cách minh bạch, có thể kiểm chứng, truy xuất nguồn gốc và giám sát chặt chẽ. Các đơn vị xử lý dữ liệu phải công bố chính sách quyền riêng tư, danh mục dữ liệu thu thập, mục đích sử dụng cụ thể và phương thức bảo vệ dữ liệu. Cơ quan nhà nước cần ban hành các quy chuẩn về công khai thông tin dữ liệu, giám sát định kỳ hoạt động dữ liệu và áp dụng các biện pháp công nghệ như mã hóa, nhật ký hoạt động (log), truy vết để phát hiện và xử lý vi phạm kịp thời. Cần thiết kế các cơ chế kiểm tra độc lập, có thể do cơ quan chuyên trách về bảo vệ dữ liệu cá nhân thực hiện, nhằm đánh giá định kỳ mức độ tuân thủ và yêu cầu điều chỉnh phù hợp. Đồng thời, việc minh bạch còn thể hiện ở trách nhiệm giải trình của tổ chức xử lý dữ liệu, đặc biệt khi có rò rỉ dữ liệu, sự cố an ninh mạng hoặc khi bị khiếu nại, tố cáo từ công dân.

Quản lý nhà nước cần xác lập cơ sở pháp lý về các quyền dữ liệu cơ bản của công dân như quyền được biết, quyền truy cập, quyền đính chính, quyền xóa dữ liệu và quyền chuyển dữ liệu. Những quyền này phải được thể chế hóa trong hệ thống pháp luật quốc gia, đặc biệt trong Luật Dữ liệu và các văn bản hướng dẫn thi hành. Việc thực hiện các quyền này không chỉ dựa trên quy định lý thuyết mà phải được thiết kế thành quy trình cụ thể trong hệ thống thông tin, đảm bảo người dân có thể thực hiện trực tuyến, thuận tiện và không bị gây cản trở. Đồng thời, các tổ chức xử lý dữ liệu cần có đội ngũ chịu trách nhiệm tiếp nhận và xử lý yêu cầu của chủ thể dữ liệu, bảo đảm phản hồi nhanh chóng, kịp thời và hiệu quả.

Việc bảo vệ dữ liệu cá nhân và dữ liệu quan trọng cũng yêu cầu đầu tư vào hạ tầng an ninh mạng, công nghệ bảo mật và đào tạo nguồn nhân lực chuyên sâu. Nhà nước cần có chiến lược tổng thể về an toàn thông tin, kết hợp cả giải pháp kỹ thuật và giải pháp thể chế. Trong đó, việc ứng dụng công nghệ mã hóa dữ liệu, định danh số an toàn, giám sát hành vi truy

cập bất thường và cảnh báo sớm nguy cơ tấn công mạng cần được ưu tiên hàng đầu. Cơ sở dữ liệu của các cơ quan nhà nước phải tuân thủ nghiêm ngặt tiêu chuẩn bảo mật quốc gia, được kiểm định định kỳ và đánh giá rủi ro thường xuyên.

Ảnh minh họa. Nguồn từ Internet.

Một nội dung quan trọng trong bảo vệ quyền dữ liệu là thiết lập cơ chế giải quyết tranh chấp giữa cá nhân với tổ chức xử lý dữ liệu. Cần hình thành các kênh tiếp nhận khiếu nại đơn giản, minh bạch và dễ truy cập, đồng thời có hệ thống trọng tài dữ liệu hoặc tòa án chuyên trách để xử lý vụ việc nhanh chóng, hiệu quả. Cơ quan quản lý nhà nước cần đóng vai trò trung gian giải thích, hướng dẫn, hòa giải và nếu cần thiết, xử phạt vi phạm hành chính hoặc khởi tố theo quy định pháp luật. Các

hành vi vi phạm quyền dữ liệu, đặc biệt là cố ý buôn bán dữ liệu cá nhân, xâm phạm thông tin sức khỏe, tài chính, đời sống riêng tư cần được xử lý nghiêm khắc để răn đe.

Nhà nước có trách nhiệm nâng cao nhận thức cộng đồng về quyền dữ liệu, xây dựng văn hóa tôn trọng quyền riêng tư và giáo dục công dân kỹ năng số cần thiết để tự bảo vệ thông tin của mình. Hệ thống giáo dục phổ thông, các chương trình truyền thông công cộng và các chiến dịch truyền thông xã hội cần tích cực lồng ghép nội dung về bảo vệ dữ liệu cá nhân, hướng dẫn cách thức kiểm soát quyền của mình trên môi trường số. Ngoài ra, cộng đồng doanh nghiệp cần được đào tạo và khuyến khích tuân thủ đạo đức dữ liệu, minh bạch với khách hàng, và xây dựng niềm tin kỹ thuật số trong quá trình cung cấp dịch vụ.

Trên bình diện quốc tế, cần thúc đẩy hợp tác xuyên biên giới về bảo vệ dữ liệu cá nhân, vì dòng chảy dữ liệu toàn cầu vượt qua lãnh thổ quốc gia. Việt Nam cần chủ động tham gia các công ước, tiêu chuẩn quốc tế về quyền dữ liệu như Quy định bảo vệ dữ liệu chung của EU (GDPR), từ đó nội luật hóa và điều chỉnh hệ thống pháp luật trong nước phù hợp. Việc công nhận lẫn nhau về cơ chế bảo vệ dữ liệu sẽ tạo điều kiện cho thương mại số, chuyển dữ liệu xuyên biên giới và bảo vệ tốt hơn quyền lợi của công dân trong môi trường quốc tế hóa.

Cần có sự phân định rõ ràng trách nhiệm giữa các cơ quan quản lý nhà nước, đặc biệt là vai trò của cơ quan chuyên trách về bảo vệ dữ liệu cá nhân, cơ quan an ninh mạng, thanh tra và kiểm tra dữ liệu. Cơ chế phối hợp liên ngành cần được thiết lập nhằm tránh chồng chéo chức năng, tăng hiệu quả giám sát và phản ứng nhanh với sự cố dữ liệu. Đồng thời, cần xây

dựng hệ thống báo cáo dữ liệu thống nhất, cho phép theo dõi toàn diện tình hình thực hiện các nghĩa vụ bảo vệ dữ liệu trong toàn quốc.

Lực lượng Công an nhân dân đóng vai trò nòng cốt trong việc bảo vệ dữ liệu cá nhân và dữ liệu quan trọng quốc gia, đặc biệt trong bối cảnh dữ liệu bị tội phạm mạng lợi dụng để thực hiện các hành vi lừa đảo, khủng bố, phá hoại và xuyên tạc. Công an các đơn vị, địa phương cần tăng cường năng lực giám sát an ninh mạng, điều tra các vụ việc liên quan đến vi phạm quyền dữ liệu, phối hợp chặt chẽ với các cơ quan chức năng khác và chủ thể dữ liệu để xử lý nhanh chóng, hiệu quả. Đồng thời, lực lượng Công an cần tham gia xây dựng, rà soát, hoàn thiện hệ thống pháp luật về bảo vệ dữ liệu phù hợp với thực tiễn an ninh, đảm bảo tính khả thi trong thực thi. Ngoài ra, cần chú trọng công tác tuyên truyền, phổ biến pháp luật cho người dân về các nguy cơ mất dữ liệu và phương thức tự bảo vệ, từ đó xây dựng thế trận an ninh dữ liệu toàn dân vững chắc.

1.4. 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

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 lý đưa ra quyết định dựa trên bằng chứng thay vì cảm tính. Việc thúc đẩy nghiên cứu, úng 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...

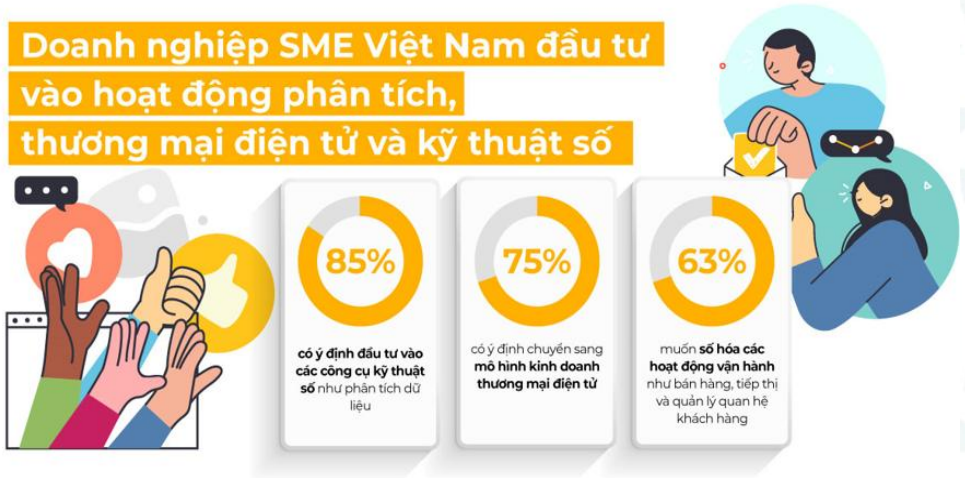
Quy định mang tính chiến lược của Luật Dữ liệu là định hướng phát triển thị trường dữ liệu. Điều này cho thấy sự chuyển dịch tư duy từ quản lý thuần túy sang kiến tạo phát triển. Một thị trường dữ liệu sôi động, nơi dữ liệu *(sau khi được*

ân danh và bảo đảm tuân thủ pháp luật) có the được chia sẻ, mua bán sê tạo ra một ngành côna nghiệp hoàn toàn mới, thúc đẩy đổi mới sáng tạo trong doanh nghiệp và tạo ra vô 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.

Quản lý nhà nước về dữ liệu trong bối cảnh hiện nay không còn đơn thuần là quản lý tài nguyên thông tin dưới dạng lưu trữ, mà đã trở thành một hoạt động kinh tế - kỹ thuật có tính chiến lược cao. Việc cấp phép và giám sát hoạt động kinh doanh sản phẩm, dịch vụ dữ liệu là một nội dung then chốt nhằm đảm bảo tính minh bạch, an toàn, hợp pháp và hiệu quả trong việc hình thành và phát triển thị trường dữ liệu quốc gia. Cơ chế cấp phép vừa là hàng rào kỹ thuật kiểm soát chất lượng và an toàn dữ liệu, vừa là công cụ thúc đẩy doanh nghiệp tham gia thị trường phải tuân thủ các chuẩn mực, tiêu chuẩn do Nhà nước quy định, đồng thời bảo vệ quyền và lợi ích hợp pháp của người tiêu dùng dữ liệu. Trong bối cảnh dữ liệu ngày càng trở thành tài sản số có giá trị cao, được khai thác và sử dụng cho nhiều mục đích kinh tế, xã hội, an ninh – quốc phòng, quản lý hiệu quả việc cấp phép và hoạt động thị trường dữ liệu góp phần tạo lập một môi trường cạnh tranh lành mạnh, thúc đẩy đổi mới sáng tạo, bảo vệ chủ quyền dữ liệu quốc gia.

Cấp phép kinh doanh sản phẩm, dịch vụ dữ liệu bao gồm việc xác định rõ danh mục hoạt động dữ liệu thuộc diện quản lý, phân loại theo nhóm hoạt động như cung cấp dữ liệu thô, dữ liệu đã xử lý, dữ liệu phân tích, dữ liệu đặc thù theo lĩnh vực; cấp quyền cho tổ chức, cá nhân triển khai các hoạt động có điều kiện như thu thập dữ liệu nhạy cảm, chia sẻ dữ liệu xuyên biên giới, khai thác dữ liệu trong không gian mạng. Việc thiết kế quy trình cấp phép cần dựa trên các tiêu chí định lượng, định tính nhằm đánh giá năng lực kỹ thuật, bảo mật, nguồn lực con người và tuân thủ pháp luật của các tổ chức tham gia. Quy trình cấp phép phải đảm bảo tính công khai, minh bạch, đồng thời tích hợp hệ thống kiểm tra định kỳ, tái cấp phép để giám sát liên

tục các hoạt động đã được cấp phép. Việc cấp phép còn phải gắn với việc công bố danh sách các tổ chức đủ điều kiện kinh doanh dữ liệu, tạo cơ sở để cộng đồng sử dụng dữ liệu lựa chọn nhà cung cấp tin cậy, đồng thời giúp Nhà nước dễ dàng thực hiện thanh tra, kiểm tra chuyên đề.



Ảnh minh hoạ

Cơ chế giám sát hoạt động kinh doanh dữ liệu được thiết lập trên nền tảng công nghệ và pháp lý nhằm đảm bảo các hoạt động dữ liệu diễn ra theo đúng quy định, không gây ảnh hưởng tiêu cực tới lợi ích quốc gia, trật tự xã hội và quyền riêng tư cá nhân. Giám sát bao gồm việc theo dõi việc sử dụng dữ liệu đã được cấp phép, xác minh tính trung thực của hoạt động thu thập – xử lý – phân phối dữ liệu, kiểm tra điều kiện an ninh mạng, bảo vệ dữ liệu cá nhân, an toàn hệ thống lưu trữ và truy cập dữ liệu. Cơ quan quản lý cần áp dụng các công cụ giám sát tự động thông qua nền tảng quản lý dữ liệu tập trung, tích hợp

trí tuệ nhân tạo để phát hiện bất thường, vi phạm. Các báo cáo định kỳ từ doanh nghiệp cung cấp dữ liệu sẽ được so sánh với hệ thống giám sát nhằm phát hiện các sai lệch, gian lận hoặc hành vi thao túng dữ liệu. Ngoài ra, giám sát còn được thực hiện thông qua cơ chế phản hồi từ người sử dụng, cho phép cộng đồng tham gia cảnh báo rủi ro và phản ánh hành vi vi phạm.

Ban Thanh niên Công an tỉnh Cà Mau tổ chức Cuộc vận động ứng xử văn minh trên không gian mạng giai đoạn 2024 - 2030. Ảnh Sưu tầm

Hoạt động chứng nhận đủ điều kiện tham gia thị trường dữ liệu là một phần không thể tách rời của hệ thống quản lý nhà nước, giúp xác lập chuẩn mực đầu vào cho các tổ chức tham gia chuỗi giá trị dữ liệu. Chứng nhận không chỉ bao gồm

xác thực tư cách pháp lý, mà còn đánh giá đầy đủ về hạ tầng công nghệ, năng lực kỹ thuật, khả năng bảo mật, quy trình xử lý và phân phối dữ liệu. Các tiêu chuẩn về chất lượng dịch vụ dữ liệu cần được xác lập cụ thể, ví dụ như thời gian cập nhật dữ liệu, độ chính xác thống kê, khả năng truy xuất nguồn gốc, bảo đảm quyền riêng tư. Để tạo thuận lợi cho doanh nghiệp và giảm chi phí hành chính, cơ chế chứng nhận nên tích hợp với các quy trình kiểm định, đánh giá định kỳ, đồng thời cho phép cấp lại nhanh khi có điều chỉnh hoặc mở rộng hoạt động. Cơ quan chứng nhận cần xây dựng kho dữ liệu quốc gia về các tổ chức đã được chứng nhận, tạo sự minh bạch và dễ tra cứu cho thị trường.

Trong hoạt động trung gian dữ liệu, quản lý nhà nước cần xác định rõ trách nhiệm của các tổ chức đóng vai trò kết nối giữa bên cung và bên sử dụng dữ liệu. Các đơn vị trung gian phải được chứng nhận về hệ thống bảo mật, khả năng lưu trữ và truyền tải dữ liệu an toàn, không can thiệp hoặc thay đổi nội dung dữ liệu gốc khi thực hiện hoạt động phân phối. Cơ quan quản lý cần có cơ chế giám sát hoạt động định giá, bảo đảm tính công bằng trong giao dịch, kiểm soát việc thu phí dịch vụ trung gian không vượt quá khung giá hợp lý. Ngoài ra, hoạt động trung gian còn phải thực hiện trách nhiệm lưu trữ nhật ký giao dịch, bảo đảm khả năng truy xuất trong trường hợp có tranh chấp pháp lý hoặc điều tra vi phạm.

Phân tích – tổng hợp dữ liệu là một lĩnh vực có hàm lượng công nghệ cao, đòi hỏi cơ quan quản lý phải ban hành các tiêu chuẩn kỹ thuật để đánh giá năng lực của các tổ chức cung cấp dịch vụ này. Các hoạt động phân tích dữ liệu lớn, dữ liệu hành vi người dùng, dữ liệu viễn thông, dữ liệu cảm biến phải được thực hiện theo nguyên tắc tôn trọng quyền riêng tư, không xâm phạm đời sống cá nhân và không sử dụng cho mục đích xấu. Các đơn vị tham gia phân tích – tổng hợp dữ liệu phải được thẩm định về quy trình xử lý, thuật toán sử dụng, khả năng kiểm soát sai lệch, độ chính xác của kết quả phân tích, khả năng tái sử dụng dữ liệu cho mục đích nghiên cứu hoặc phát triển chính sách công. Giám sát nhà nước trong lĩnh vực này cần bao

gồm cả khía cạnh đạo đức dữ liệu và tác động xã hội của các phân tích được công bố, đặc biệt là các dự báo chính sách hoặc mô hình dự đoán hành vi.

Dịch vụ cung cấp hạ tầng dữ liệu đóng vai trò nền tảng, đảm bảo khả năng kết nối và lưu trữ dữ liệu một cách an toàn, ổn định, có thể mở rộng. Nhà nước cần đặt ra yêu cầu cụ thể đối với các đơn vị cung cấp dịch vụ hạ tầng về bảo mật vật lý trung tâm dữ liệu, khả năng sao lưu – phục hồi, thời gian vận hành liên tục, mức độ dự phòng thảm họa, khả năng tương thích với kiến trúc dữ liệu quốc gia. Giám sát cần bao gồm cả khả năng cung ứng dịch vụ xuyên biên giới, đánh giá tác động đến chủ quyền dữ liệu và khả năng kiểm soát trong các tình huống khẩn cấp. Để đảm bảo hạ tầng dữ liệu phục vụ hiệu quả cho chính phủ số và nền kinh tế số, cần khuyến khích các mô hình hợp tác công – tư, thúc đẩy các doanh nghiệp trong nước đầu tư phát triển hạ tầng điện toán đám mây, trung tâm dữ liệu nội địa và nền tảng chia sẻ dữ liệu theo tiêu chuẩn mở.

Hoạt động đấu giá dữ liệu là lĩnh vực mới, đòi hỏi Nhà nước xây dựng khuôn khổ pháp lý rõ ràng để đảm bảo tính minh bạch, công bằng và hiệu quả. Đấu giá dữ liệu bao gồm việc định giá tài sản dữ liệu công, xác định quyền sở hữu và quyền sử dụng dữ liệu, xây dựng sàn giao dịch dữ liệu quốc gia, tổ chức phiên đấu giá trực tuyến và quy định về xử lý kết quả đấu giá. Các bên tham gia đấu giá phải được chứng nhận đủ điều kiện về năng lực công nghệ, khả năng bảo vệ dữ liệu và tuân thủ các quy định về sử dụng dữ liệu sau khi trúng thầu. Việc quản lý nhà nước đối với hoạt động đấu giá cần đảm bảo cơ chế định giá không bị thao túng, cơ chế giám sát đấu giá công khai, lưu trữ lịch sử giao dịch và giải quyết tranh chấp một cách minh bạch.

Ảnh minh hoạ

Kiểm định chất lượng dữ liệu là khâu cuối cùng nhưng giữ vai trò then chốt trong việc đảm bảo dữ liệu lưu hành trên thị trường có độ tin cậy cao. Các tiêu chí kiểm định bao gồm độ đầy đủ, độ chính xác, tính kịp thời, tính nhất quán và khả năng truy xuất nguồn gốc. Nhà nước cần thiết lập hệ thống kiểm định độc lập, vận hành theo mô hình tổ chức được cấp quyền, có quy trình chứng nhận kết quả kiểm định và giám sát định kỳ. Cần quy định rõ trách nhiệm đối với các đơn vị cung cấp dữ liệu đã được kiểm định, đặc biệt trong trường hợp có khiếu nại về chất lượng dữ liệu gây thiệt hại cho người sử dụng. Kiểm định cũng cần được áp dụng trong việc đánh giá dữ liệu công trước khi chia sẻ công khai, đảm bảo dữ liệu phục vụ chính phủ số phải đạt chuẩn chất lượng trước khi khai thác đại trà.

Trong tổng thể các hoạt động cấp phép và giám sát thị trường dữ liệu, lực lượng Công an có vai trò đặc biệt quan trọng trong việc bảo vệ an ninh dữ liệu, phòng ngừa và xử lý các hành vi lợi dụng kinh doanh dữ liệu để thực hiện hành vi phạm tội như gian lận thương mại, lừa đảo công nghệ cao, xâm phạm đời tư, can thiệp vào hệ thống dữ liệu trọng yếu. Lực lượng Công an cần chủ động phối hợp với các bộ, ngành để kiểm tra, thanh tra các hoạt động dữ liệu có nguy cơ đe dọa đến an ninh quốc gia, đồng thời xây dựng cơ chế cảnh báo sớm, hệ thống phát hiện vi phạm tự động và kịp thời xử lý các hành vi vi phạm liên quan đến dữ liệu. Công an nhân dân còn có nhiệm vụ đảm bảo an ninh hệ thống hạ tầng dữ liệu quốc gia, bảo vệ hệ thống thông tin quan trọng, góp phần duy trì môi trường số an toàn, tin cậy cho phát triển kinh tế - xã hội và giữ vững chủ quyền không gian mạng.

1.5. Tổ chức thanh tra, kiểm tra, xử lý vi phạm, giải quyết khiếu nại, tố cáo trong lĩnh vực dữ liệu

Trong bối cảnh chuyển đổi số quốc gia đang được thúc đẩy mạnh mẽ, dữ liệu trở thành tài nguyên quan trọng bậc nhất, vừa là đầu vào cho quá trình hoạch định chính sách, vừa là tài sản chiến lược đối với phát triển kinh tế – xã hội, bảo đảm quốc phòng – an ninh. Do đó, việc tổ chức hệ thống thanh tra, kiểm tra, xử lý vi phạm và giải quyết các tranh chấp liên quan đến dữ liệu trở thành nhiệm vụ thiết yếu của quản lý nhà nước.

Thanh tra, kiểm tra trong lĩnh vực dữ liệu nhằm bảo đảm các tổ chức, cá nhân thực hiện đúng quy định pháp luật trong thu thập, lưu trữ, xử lý, chia sẻ và khai thác dữ liệu. Đây là công cụ phát hiện, phòng ngừa các hành vi vi phạm và sai sót trong hoạt động dữ liệu. Các nội dung trọng tâm cần thanh tra bao gồm việc tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật dữ liệu; việc bảo đảm an ninh mạng, an toàn thông tin cá nhân; các hành vi vi phạm liên quan đến thu thập, phân tích, chuyển giao và

thương mại hóa dữ liệu trái phép. Cơ quan nhà nước có thẩm quyền cần thiết lập quy trình kiểm tra chặt chẽ, định kỳ hoặc đột xuất, với phạm vi bao trùm các cơ sở dữ liệu quốc gia, trung tâm dữ liệu, sàn dữ liệu và các tổ chức, doanh nghiệp đang sở hữu hoặc khai thác lượng dữ liệu lớn.

Ảnh minh họa. Nguồn từ Internet

Công tác xử lý vi phạm trong lĩnh vực dữ liệu cần được thực hiện đồng bộ, nghiêm minh, đảm bảo tính răn đe và lập lại trật tự trong quản trị dữ liệu quốc gia. Vi phạm có thể xuất phát từ hành vi cố ý như tấn công mạng, rò rỉ dữ liệu, kinh

doanh dữ liệu trái phép, hoặc từ sự thiếu năng lực trong bảo vệ hệ thống. Các mức độ vi phạm cần được phân loại rõ ràng để áp dụng hình thức xử phạt phù hợp, từ xử phạt hành chính đến truy cứu trách nhiệm hình sự. Bên cạnh đó, các hành vi gian lận thông qua dữ liệu giả mạo, thao túng dữ liệu để trục lợi chính sách, lừa đảo người dùng, hoặc xuyên tạc thông tin cũng cần được xem là nguy cơ an ninh dữ liệu đặc biệt nghiêm trọng.

Giải quyết khiếu nại, tố cáo trong lĩnh vực dữ liệu đóng vai trò là cơ chế phản hồi và bảo vệ quyền lợi của các chủ thể dữ liệu. Trong môi trường dữ liệu mở, việc bị thu thập, phân tích, chia sẻ thông tin cá nhân trái ý muốn xảy ra thường xuyên. Người dân, doanh nghiệp cần có quyền được khiếu nại, yêu cầu xử lý những tổ chức vi phạm quyền riêng tư dữ liệu. Cơ quan nhà nước có trách nhiệm tiếp nhận, thẩm tra và giải quyết các khiếu nại theo đúng trình tự, thời hạn và công khai kết quả xử lý. Quy định pháp lý cần bảo đảm rằng mọi tổ chức, cá nhân bị xâm phạm dữ liệu đều có thể khởi kiện hoặc yêu cầu bồi thường thiệt hại thông qua cơ chế tố tụng rõ ràng, minh bạch.

Việc phối hợp với các lực lượng chuyên trách trong điều tra, xử lý hành vi xâm phạm an ninh dữ liệu là yêu cầu cấp thiết trong bối cảnh tội phạm công nghệ cao ngày càng tinh vi, có tính xuyên quốc gia và ẩn danh cao. Lực lượng Công an, an ninh mạng, tình báo công nghệ phải được huy động để phát hiện, truy vết, xử lý nghiêm các hành vi sử dụng dữ liệu cho mục đích khủng bố, gián điệp, gây rối trật tự công cộng hoặc phá hoại kinh tế. Những vụ việc rò rỉ dữ liệu quy mô lớn, các chiến dịch tấn công mạng có tổ chức cần sự tham gia phối hợp nhiều cấp, từ Trung ương đến địa phương, từ lực lượng kỹ thuật nghiệp vụ đến tư pháp. Việc hình thành các đơn vị chuyên trách về điều tra, xử lý tội phạm dữ liệu số là điều kiện tiên quyết để bảo vệ không gian dữ liệu quốc gia.

Buôn bán dữ liệu cá nhân, dữ liệu doanh nghiệp trên thị trường chợ đen đã trở thành ngành công nghiệp ngầm với lợi nhuận cao. Nhiều tổ chức khai thác dữ liệu khách hàng không có sự đồng ý của người dùng, sau đó mua bán, chia sẻ trái phép, vi phạm nghiêm trọng đến quyền riêng tư và tạo điều kiện cho các hoạt động lừa đảo, quảng cáo bất hợp pháp. Nhà nước cần tăng cường công cụ giám sát thị trường, phát hiện các sàn giao dịch dữ liệu trái phép, xử lý hình sự với hành vi kinh doanh dữ liệu không được cấp phép. Mô hình đánh dấu dữ liệu, truy vết nguồn gốc dữ liệu khi bị rò rỉ cần được áp dụng trong các hệ thống lớn để phục vụ quá trình điều tra.

Rò rỉ dữ liệu từ các hệ thống công hoặc tư xảy ra do cả yếu tố kỹ thuật lẫn con người. Cấu hình sai hệ thống bảo mật, thiếu mã hóa dữ liệu, sử dụng mật khẩu yếu, chia sẻ dữ liệu nội bộ không kiểm soát là những lỗ hổng phổ biến dẫn đến rò rỉ. Ngoài ra, hành vi cố ý của nhân viên nội bộ, bên thứ ba truy cập hệ thống trái phép cũng là nguyên nhân đáng lo ngại. Nhà nước cần thiết lập chế độ kiểm định, đánh giá mức độ an toàn thông tin của các hệ thống dữ liệu, đặc biệt là cơ sở dữ liệu quốc gia và nền tảng dữ liệu của các tổ chức tài chính, y tế, giáo dục. Mọi vi phạm làm rò rỉ dữ liệu cần được xác minh trách nhiệm cụ thể để xử lý theo quy định.

Giả mạo dữ liệu nhằm mục đích tạo thông tin sai lệch, gây hiểu lầm, thao túng dư luận hoặc gian lận tài chính là hình thức vi phạm nguy hiểm, có thể dẫn đến hậu quả nghiêm trọng về chính trị, kinh tế, xã hội. Việc giả mạo dữ liệu tài khoản ngân hàng, hồ sơ học thuật, giấy tờ hành chính đang ngày càng phổ biến trong không gian mạng. Hành vi này không chỉ ảnh hưởng đến quyền lợi cá nhân mà còn gây tổn hại đến uy tín và hiệu quả của hệ thống quản lý nhà nước. Biện pháp kỹ thuật như chữ ký số, công nghệ blockchain, hệ thống xác thực đa yếu tố cần được ứng dụng rộng rãi để chống lại việc tạo lập và sử dụng dữ liệu giả mạo.

Lợi dụng dữ liệu để thực hiện hành vi phạm pháp diễn ra trên nhiều phương diện, từ sử dụng thông tin cá nhân để chiếm đoạt tài sản, đến khai thác dữ liệu người dùng phục vụ cho hoạt động tuyên truyền sai lệch, xuyên tạc thông tin, kích động bạo lực hoặc chia rẽ cộng đồng. Mạng xã hội, nền tảng chia sẻ nội dung trở thành môi trường trung gian cho các hành vi này phát triển. Quản lý nhà nước cần ban hành hành lang pháp lý quy định trách nhiệm nền tảng trong phát hiện, ngăn chặn nội dung vi phạm; đồng thời có cơ chế xử lý nhanh, gọn đối với các hành vi lợi dụng dữ liệu xâm hại an ninh quốc gia, thuần phong mỹ tục, danh dự, nhân phẩm công dân.

Nâng cao năng lực thể chế, tăng cường hệ thống văn bản pháp luật và đội ngũ cán bộ chuyên trách là nền tảng để bảo đảm thực thi hiệu quả công tác thanh tra, kiểm tra, xử lý vi phạm trong lĩnh vực dữ liệu. Việc xây dựng hệ thống cảnh báo sớm, quy trình điều phối thông tin giữa các cơ quan chức năng, cơ chế báo cáo – phản hồi sự cố dữ liệu là giải pháp phòng ngừa rủi ro hiệu quả. Bên cạnh đó, tuyên truyền nâng cao nhận thức của người dân và tổ chức về bảo vệ dữ liệu, cách thức phản ánh vi phạm, tầm quan trọng của an toàn thông tin cần được đẩy mạnh trên mọi phương tiện truyền thông đại chúng và nền tảng kỹ thuật số.

Hoạt động này chính là "thanh gươm công lý" bảo đảm tính thực thi và sự nghiêm minh của pháp luật về dữ liệu. Mọi chiến lược, quy định pháp luật sẽ chỉ mang tính hình thức nếu không có một cơ chế, chế tài đủ mạnh để bảo đảm 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 nhiều chế tài xử lý của Nhà nước.

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 nhana phát hiện dữ liệu của mình bị lạm dụng, hoặc một công ty bị 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 các hành vi vi phạm sẽ củng cố lòng 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.

Công tác giải quyết khiếu nại, tố cáo của lực lượng Công an nhân dân góp phần đảm bảo an ninh, trật tự trong tình hình mới. Ảnh Sưu tầm

Lực lượng Công an giữ vai trò đặc biệt trong việc điều tra, xử lý các hành vi vi phạm pháp luật về dữ liệu, bảo vệ an ninh mạng và an ninh thông tin quốc gia. Nhiệm vụ của lực lượng Công an bao gồm thu thập chứng cứ, phân tích dấu vết điện tử, xác minh danh tính ảo, triệt phá các đường dây buôn bán dữ liệu và phối hợp với cơ quan tư pháp xử lý tội phạm dữ liệu xuyên biên giới. Ngoài ra, lực lượng Công an còn đóng vai trò giám sát, phát hiện sớm các nguy cơ xâm phạm từ không gian mạng, tham mưu xây dựng chính sách an ninh dữ liệu và hướng dẫn các cơ quan, tổ chức, doanh nghiệp triển khai biện pháp bảo vệ phù hợp.

Công an Thành phố Hồ Chí Minh tấn công quyết liệt tội phạm công nghệ cao.

Ảnh Sưu tầm

1.6. Đào tạo đào tạo, bồi dưỡng, phát triển nguồn nhân lực; thực hiện hợp tác quốc tế về 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 đâu tư cho tương lai bền vững, tạo ra năng lực cạnh tranh cốt lõi của quốc gia trong dài hạn.

Bộ Công an tổ chức Hội thảo "Xây dựng chính sách bảo vệ dữ liệu cá nhân" với sự phối hợp của Hiệp hội An ninh mạng quốc gia và Cục an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao. Ảnh Sưu tầm

Song hành với hoàn thiện hạ tầng kỹ thuật và pháp lý là phát triển nguồn nhân lực chất lượng cao, phục vụ vận hành, bảo trì và khai thác hiệu quả hạ tầng dữ liệu quốc gia. Cần xây dựng chiến lược đào tạo về khoa học dữ liệu, an toàn thông tin, điện toán đám mây, quản trị cơ sở dữ liệu ở tất cả các bậc học. Tổ chức các chương trình hợp tác quốc tế, trao đổi học thuật, nghiên cứu chuyên sâu về bảo mật, chuẩn hóa dữ liệu và kinh tế dữ liệu. Đồng thời, thúc đẩy cộng đồng công nghệ mở, khuyến khích doanh nghiệp đổi mới sáng tạo, tham gia vào quá trình cung ứng hạ tầng, dịch vụ dữ liệu theo hình thức đối tác công – tư. Cần phát triển hệ sinh thái khởi nghiệp xoay quanh dữ liệu, tạo môi trường thuận lợi cho các startup công nghệ tham gia vào chuỗi giá trị dữ liệu quốc gia.

Cuộc thi Dữ liệu với cuộc sống 2024 do Cục Cảnh sát quản lý hành chính về trật tự xã hội - Bộ Công an tổ chức với mục tiêu nhằm đẩy mạnh tiến trình Chuyển đổi số quốc gia. Ảnh Sưu tầm

Bên cạnh đó, hợp tác quốc tế trong lĩnh vực dữ liệu là xu thế tất yếu. Dữ liệu không có biên giới. 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 chuan mực chung của thế giới *(như Luật Quản trị Dữ - DGA, Quy định chung về bảo vệ dữ liệu - GDPR, Đạo luật Dữ liệu - DA của Liên minh Châu Âu, Luật Dữ liệu mở của Hàn Quốc...)*, 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.

Hợp tác quốc tế về dữ liệu là một nội dung cốt lõi trong quản lý nhà nước về dữ liệu trong bối cảnh chuyển đổi số và toàn cầu hóa. Khi dữ liệu trở thành tài nguyên chiến lược, việc xây dựng cơ chế hợp tác song phương và đa phương giữa các quốc gia, tổ chức quốc tế là yêu cầu khách quan nhằm bảo đảm tính kết nối, tương thích, an toàn và hiệu quả trong quản trị dữ liệu. Nhà nước cần chủ động xây dựng và thực hiện các chương trình hợp tác quốc tế về dữ liệu theo hướng toàn diện, cân bằng lợi ích quốc gia, tuân thủ luật pháp quốc tế và tôn trọng chủ quyền dữ liệu số.

Trao đổi thông tin dữ liệu giữa các quốc gia là cơ sở để xây dựng lòng tin số và phát triển hệ sinh thái dữ liệu mở toàn cầu. Cơ chế trao đổi cần được thiết kế minh bạch, có kiểm soát, bảo đảm mục tiêu chia sẻ đúng mục đích, đúng đối tượng, phòng ngừa nguy cơ lộ lọt dữ liệu, lợi dụng dữ liệu để xâm phạm an ninh quốc gia. Việt Nam cần ký kết các hiệp định hợp tác song phương với các nước có năng lực phát triển dữ liệu mạnh để xây dựng hệ thống cảnh báo sớm về rủi ro an ninh mạng, hỗ trợ truy vết tội phạm mạng xuyên biên giới, phối hợp bảo vệ chủ thể dữ liệu trong các vụ việc có yếu tố nước ngoài. Việc thiết lập kênh trao đổi dữ liệu phục vụ điều tra tội phạm, quản lý di cư, giám sát thương mại điện tử xuyên biên giới cần đặt trong khuôn khổ luật pháp quốc tế và luật quốc gia.

Lực lượng Công an triển khai tích cực công tác thu nhận hồ sơ cấp căn cước cho công dân. Ảnh Sưu tầm

Chia sẻ kinh nghiệm quản trị dữ liệu là một nội dung quan trọng của hợp tác quốc tế trong lĩnh vực này. Các nước phát triển đã ban hành luật dữ liệu, luật quyền riêng tư, hệ thống hóa quy trình phân loại, lưu trữ, phân tích và xử lý dữ liệu. Việt Nam có thể học hỏi cách thức các nước xây dựng mô hình trung tâm dữ liệu quốc gia, cơ chế chứng nhận dữ liệu, định danh số toàn dân, cơ chế kiểm toán dữ liệu, quy tắc chia sẻ dữ liệu giữa nhà nước và tư nhân. Việc mời chuyên gia quốc tế tư vấn xây dựng pháp luật, chính sách và mô hình vận hành hệ thống dữ liệu quốc gia có thể giúp nâng cao chất lượng quản trị, rút

ngắn thời gian xây dựng thể chế và bảo đảm tính tương thích quốc tế. Cần ưu tiên học tập mô hình quản trị dữ liệu của các nước ASEAN, EU, Nhật Bản, Hàn Quốc, Hoa Kỳ phù hợp với điều kiện chính trị, xã hội và pháp lý trong nước.

Tham gia các hiệp định đa phương về dữ liệu xuyên biên giới là bước đi chiến lược nhằm bảo đảm quyền truy cập dữ liệu hợp pháp trong không gian số toàn cầu. Khi hoạt động thương mại, tài chính, đầu tư và giáo dục ngày càng chuyển dịch sang nền tảng số, yêu cầu thiết lập hành lang pháp lý cho luồng dữ liệu xuyên biên giới trở thành nhu cầu thiết yếu. Việt Nam cần tích cực tham gia vào các diễn đàn như Hiệp định Đối tác kinh tế số (DEPA), Hiệp định khung ASEAN về thương mại điện tử, Diễn đàn hợp tác châu Á – Thái Bình Dương (APEC) về lưu chuyển dữ liệu, tiến tới đàm phán, ký kết các điều ước quốc tế về bảo vệ dữ liệu cá nhân, chuyển giao dữ liệu qua biên giới. Việc tham gia các hiệp định này giúp nâng cao vị thế Việt Nam trong chuỗi giá trị dữ liệu toàn cầu, đồng thời góp phần bảo vệ dữ liệu người Việt trong các hệ sinh thái số có yếu tố nước ngoài.

An ninh mạng là một cấu phần không thể tách rời trong hợp tác quốc tế về dữ liệu. Khi dữ liệu trở thành mục tiêu của tội phạm mạng, tin tặc và các nhóm lợi ích, quốc gia không thể đơn độc ứng phó mà cần tham gia vào mạng lưới cảnh báo, phản ứng và ứng cứu sự cố toàn cầu. Việt Nam cần đẩy mạnh hợp tác với INTERPOL, ASEANPOL, Cơ quan an ninh mạng của Liên minh châu Âu, Mạng lưới ứng cứu sự cố mạng toàn cầu (CSIRT) để nâng cao năng lực phát hiện, ngăn chặn và phục hồi dữ liệu sau tấn công. Việc chia sẻ dữ liệu kỹ thuật như địa chỉ IP, mã độc, hành vi tấn công, quy trình ứng phó cần được thực hiện có chọn lọc, phù hợp với cam kết quốc tế và quy định của pháp luật trong nước. Lực lượng kỹ thuật chuyên trách

về an ninh mạng cần được trang bị kỹ năng hợp tác quốc tế, sử dụng ngôn ngữ chuyên môn, nắm vững pháp lý để có thể đàm phán, tương tác và khai thác tối đa hiệu quả của hợp tác dữ liệu xuyên biên giới.

Phát triển công nghệ dữ liệu tiên tiến là nội dung đột phá trong hợp tác quốc tế. Công nghệ dữ liệu lớn (Big Data), trí tuệ nhân tạo (AI), học máy (Machine Learning), điện toán đám mây (Cloud Computing) đang làm thay đổi phương thức thu thập, xử lý và khai thác dữ liệu. Việt Nam cần chủ động tiếp cận các công nghệ mới thông qua các dự án hợp tác nghiên cứu, chuyển giao công nghệ, đào tạo chuyên gia, hình thành liên minh nghiên cứu với các viện, trường và doanh nghiệp công nghệ quốc tế. Việc tham gia mạng lưới dữ liệu y tế, giáo dục, giao thông, môi trường khu vực và toàn cầu sẽ tạo điều kiện để Việt Nam chuẩn hóa hệ thống, tăng năng lực phân tích dự báo, phục vụ hoạch định chính sách và cảnh báo sớm trong quản lý nhà nước. Các doanh nghiệp công nghệ trong nước cũng có cơ hội tiếp cận công nghệ lõi, cải thiện năng lực cạnh tranh và mở rộng thị trường khi tham gia vào chuỗi giá trị dữ liệu toàn cầu.

Hợp tác quốc tế về dữ liệu không chỉ giới hạn trong lĩnh vực kỹ thuật hay công nghệ mà còn liên quan mật thiết đến ngoại giao số và chủ quyền quốc gia. Việt Nam cần có chiến lược ngoại giao dữ liệu rõ ràng, xây dựng hình ảnh quốc gia có trách nhiệm, minh bạch, tôn trọng quyền riêng tư và cam kết bảo vệ dữ liệu cá nhân. Các hiệp định thương mại tự do mới thế hệ (như CPTPP, EVFTA) đều có nội dung về dòng dữ liệu xuyên biên giới, bảo vệ dữ liệu cá nhân và an ninh mạng, đòi hỏi Việt Nam phải nâng cao năng lực thể chế để đáp ứng cam kết. Đồng thời, việc thiết lập các khuôn khổ pháp lý riêng biệt về dữ liệu quốc phòng, dữ liệu chiến lược, dữ liệu bí mật nhà nước là cần thiết nhằm bảo đảm an ninh quốc gia trong bối cảnh mở rộng hợp tác dữ liệu quốc tế.

CPTPP gồm 11 quốc gia thành viên. Ảnh Sưu tầm

Để tổ chức thực hiện hiệu quả hợp tác quốc tế về dữ liệu, cần xác định rõ vai trò của các cơ quan nhà nước. Bộ Thông tin và Truyền thông giữ vai trò chủ trì về kỹ thuật, xây dựng các quy chuẩn, tiêu chuẩn bảo đảm tương thích với quốc tế, thực hiện thỏa thuận hợp tác trong lĩnh vực hạ tầng dữ liệu, an ninh mạng. Bộ Ngoại giao tham mưu xây dựng chiến lược ngoại giao số, chủ trì đàm phán các hiệp định quốc tế về dữ liệu, bảo vệ quyền lợi Việt Nam trong các tổ chức đa phương liên quan đến dữ liệu số. Bộ Công Thương phụ trách nội dung chuyển giao công nghệ, lưu chuyển dữ liệu trong thương mại điện tử, đảm bảo thực hiện các cam kết về dữ liệu trong hiệp định thương mại tự do. Bộ Công an đảm nhiệm chức năng bảo vệ an

ninh quốc gia trong hợp tác dữ liệu xuyên biên giới, giám sát hoạt động chia sẻ dữ liệu có yếu tố nước ngoài, chủ trì phối hợp xử lý tội phạm mạng xuyên quốc gia.

Lực lượng Công an nhân dân giữ vai trò nòng cốt trong bảo đảm an ninh dữ liệu trong quá trình hợp tác quốc tế. Cần xây dựng đội ngũ chuyên gia an ninh mạng có kiến thức pháp lý, trình độ ngoại ngữ và kỹ năng đàm phán quốc tế để chủ trì các cuộc đối thoại, trao đổi thông tin và phối hợp điều tra liên quốc gia. Đẩy mạnh chia sẻ thông tin về các tổ chức tội phạm công nghệ cao, hành vi xâm phạm dữ liệu công dân Việt Nam từ nước ngoài, yêu cầu cung cấp dữ liệu phục vụ điều tra và bảo vệ lợi ích quốc gia trong môi trường số. Phối hợp chặt chẽ với các lực lượng an ninh mạng quốc tế để theo dõi, xử lý và phòng ngừa các âm mưu tấn công vào hệ thống dữ liệu trọng yếu của Việt Nam. Đề xuất cơ chế kiểm soát dữ liệu ra nước ngoài, xây dựng danh mục dữ liệu cấm chia sẻ, tổ chức thẩm định các dự án có yếu tố nước ngoài liên quan đến khai thác dữ liệu. Chủ động phát hiện, xử lý và công khai các vụ việc vi phạm quyền dữ liệu của công dân Việt Nam trên nền tảng quốc tế nhằm răn đe, bảo đảm chủ quyền và an toàn dữ liệu quốc gia.

2. Chủ thể, đầu mối quản lý dữ liệu

Căn cứ khoản 2 Điều 8 Luật Dữ liệu 2024, chủ thể đầu mối quản lý về dữ liệu quy định như sau:

- Chính phủ thống nhất quản lý nhà nước về dữ liệu;

- Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về dữ liệu, trừ quy định tại điểm c khoản này;

- 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 quan lý nhà nước về dữ liệu cơ yếu thuộc phạm vi quản lý theo quy định của pháp luật về cơ yếu;

- 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;

- Uỷ ban nhân dân cấp tỉnh xây dựng, phát triển cơ sở dữ liệu; thực hiện quan lý nhà nước về dữ liệu tại địa phương.

Tổng Bí thư Tô Lâm và Thủ tướng Chính phủ Phạm Minh Chính chúc mừng Ban Thường vụ Hiệp hội Dữ liệu quốc gia nhiệm kỳ 2025-2030 - Ảnh: VGP/HM

Cụ thể hoá Luật Dữ liệu năm 2024, Nghị định 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành luật dữ liệu, quy định như sau:

Tại Điều 27, quy định về trách nhiệm của Bộ Quốc phòng trong quản lý nhà nước về dữ liệu như sau: (1) Chịu trách nhiệm trước Chính phủ trong thực hiện công tác quản lý nhà nước đối với các dữ liệu thuộc phạm vi quản lý; (2) Phối hợp với Bộ Công an, các cơ quan, tổ chức bố trí lực lượng, phương tiện thích hợp để phát hiện, ngăn chặn từ xa mọi hành vi xâm phạm Trung tâm dữ liệu quốc gia cả về địa lý và trên không gian mạng; (3) Chủ trì quản lý hoạt động lưu trữ, bảo vệ dữ liệu, bảo đảm an ninh dữ liệu; quản lý, theo dõi, giám sát, tổ chức thực hiện kết nối, chia sẻ, điều phối dữ liệu giữa hệ thống thông tin, cơ sở dữ liệu; ứng dụng khoa học trong xử lý, quản lý, khai thác, sử dụng dữ liệu; quản lý, cấp phép chuyển dữ liệu ra nước ngoài; sử dụng quỹ phát triển dữ liệu quốc gia đối với các dữ liệu thuộc phạm vi quản lý của Bộ Quốc phòng.

Tại Điều 28, quy định về trách nhiệm của Bộ Khoa học và Công nghệ trong quản lý nhà nước về dữ liệu như sau: (1) Hướng dẫn cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội phát triển, hoàn thiện hạ tầng kỹ thuật công nghệ thông tin và việc xây dựng tiêu chuẩn, quy chuẩn kỹ thuật về tổ chức, kết nối, chia sẻ, đồng bộ dữ liệu; thực hiện chuẩn hoá, kết nối, chia sẻ dữ liệu, tính toán tối ưu giữa việc đầu tư hạ tầng mới và sử dụng hạ tầng do Trung tâm dữ liệu quốc gia cung cấp; (2) Rà soát, đánh giá năng lực mạng truyền số liệu chuyên dùng của các cơ quan để xây dựng phương án nâng cấp, bảo đảm các đơn vị có thể truy cập, quản trị hệ thống đặt tại Trung tâm dữ liệu quốc gia thông qua mạng truyền số liệu chuyên dùng; (3) Phối hợp với Bộ Công an và cơ quan có liên quan trong nghiên cứu làm chủ và ứng dụng các công nghệ số, dữ liệu số hình thành các sản phẩm, dịch vụ phục vụ phát triển chính phủ số, chính quyền số và phát triển kinh tế - xã hội thông qua các Chương

trình khoa học và công nghệ trọng điểm cấp quốc gia; (4) Phối hợp với Bộ Công an trong việc xác 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.

Tại Điều 29, quy định về trách nhiệm của Văn phòng Chính phủ trong quản lý dữ liệu như sau: (1) Chủ trì xây dựng yêu cầu chức năng, nghiệp vụ, giao diện; hỗ trợ, hướng dẫn các bộ, ngành, địa phương xử lý các vấn đề về chức năng, quy trình nghiệp vụ, dữ liệu của Cổng Dịch vụ công quốc gia; phối hợp với Bộ Công an quản trị, vận hành Cổng Dịch vụ công quốc gia tại Trung tâm dữ liệu quốc gia; thực hiện các nhiệm vụ khác về phát triển Cổng Dịch vụ công quốc gia theo yêu cầu của Chính phủ, Thủ tướng Chính phủ; quản lý, vận hành Cơ sở dữ liệu quốc gia về thủ tục hành chính; (2) Phối hợp Bộ Công an và các đơn vị liên quan đánh giá nhu cầu, thực hiện chuyển dịch hạ tầng kỹ thuật công nghệ thông tin các hệ thống thông tin phục vụ chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ để đặt tại Trung tâm dữ liệu quốc gia.

Tại Điều 30, quy định về trách nhiệm của Ban Cơ yếu Chính phủ trong quản lý dữ liệu như sau: (1) Chủ trì phối hợp với các đơn vị có liên quan triển khai các sản phẩm mã hóa, giải mã dữ liệu; (2) Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện nhiệm vụ quản lý nhà nước đối với dữ liệu về cơ yếu; (3) Phối hợp với Bộ Công an triển khai các giải pháp bảo đảm an toàn, xác thực và bảo mật thông tin dùng mật mã; triển khai dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ cho các hệ thống thông tin và cơ sở dữ liệu của cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội.

Ảnh minh hoạ

Tại Điều 31, quy định về trách nhiệm của Bộ Tài chính trong quản lý dữ liệu như sau: (1) Phối hợp với Bộ Công an trong việc xác 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; (2) Ban hành Thông tư quy định thu phí khai thác và sử dụng thông tin trong cơ sở dữ liệu tổng hợp quốc gia, cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành trên cơ sở đề xuất của các bộ, cơ quan ngang bộ.

Ảnh minh hoạ

Tại Điều 32, quy định trách nhiệm của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương trong quản lý dữ liệu như sau: (1) Chủ trì, phối hợp với Bộ Công an, Bộ Quốc phòng và cơ quan có liên quan quản lý hoạt động thu thập, cập nhật, điều chỉnh, sao chép, chia sẻ, chuyển giao, xóa, hủy dữ liệu, lưu trữ, bảo vệ dữ liệu thuộc phạm vi quản lý; (2) Thực hiện đồng bộ dữ liệu thuộc phạm vi quản lý về Trung tâm dữ liệu quốc gia theo quy định của Nghị định này và phối hợp với Bộ Công an thực hiện giám sát và đối soát để bảo đảm tính chính xác của dữ liệu; (3) Các bộ, ngành, địa phương phối hợp Văn phòng Chính phủ, Bộ Công an và các đơn vị có liên quan thực hiện tái

cấu trúc quy trình, sửa đổi các văn bản pháp lý theo lộ trình thu thập, cập nhật, đồng bộ dữ liệu về Cơ sở dữ liệu tổng hợp quốc gia; (4) Thực hiện nâng cấp, bảo trì, sửa chữa hạ tầng, thiết bị của cơ quan khi sử dụng hạ tầng của Trung tâm dữ liệu quốc gia; (5) Kiến nghị Bộ Tài chính về mức thu, nộp, miễn, giảm, quản lý và sử dụng đối với phí khai thác và sử dụng thông tin trong cơ sở dữ liệu tổng hợp quốc gia, cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành thuộc ngành, lĩnh vực quản lý.

Sôi nổi hoạt động Ngày hội Chuyển đổi số tại Cà Mau. Ảnh Báo Cà Mau

II. 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

1. Vai trò, trách nhiệm của Bộ Công an trong công tác quản lý nhà nước về dữ liệu

Lễ ký kết bàn giao chức năng an toàn thông tin giữa Bộ Công an và Bộ Thông tin và Truyền thông. Ảnh Sưu tầm

Bộ Công an, với vai trò là cơ quan nòng cốt trong công tác đảm bảo an ninh quốc gia và trật tự an toàn xã hội, đồng thời cũng là lực lượng chủ lực trong chuyển đổi số quốc gia, được giao nhiệm vụ chủ trì tổ chức triển khai Nghị định số

165/2025/NĐ-CP của Chính phủ. Nghị định này là cơ sở pháp lý quan trọng trong việc điều chỉnh toàn diện các hoạt động quản lý, xây dựng, vận hành, kết nối và chia sẻ dữ liệu giữa các cơ quan, tổ chức, cá nhân trong hệ thống quản lý nhà nước và nền kinh tế số. Điều 26 của Nghị định đã quy định cụ thể, đầy đủ và chi tiết trách nhiệm của Bộ Công an trong quản lý nhà nước về dữ liệu, bao gồm từ công tác thể chế hóa chính sách, tổ chức triển khai, giám sát thực hiện, đến xây dựng hạ tầng kỹ thuật và vận hành các thiết chế dữ liệu trọng yếu của quốc gia.

Trước hết, Bộ Công an có trách nhiệm tổ chức triển khai, hướng dẫn và kiểm tra việc thực hiện Nghị định này trong toàn hệ thống chính trị. Với tư cách là cơ quan chủ trì, Bộ phối hợp với các bộ, ngành, địa phương và tổ chức có liên quan để đảm bảo các quy định về quản lý và sử dụng dữ liệu được thực thi một cách nghiêm túc, đồng bộ và hiệu quả. Quá trình triển khai không chỉ dừng lại ở việc ban hành văn bản hướng dẫn mà còn bao gồm cả việc đôn đốc, kiểm tra thường xuyên và xử lý nghiêm các hành vi vi phạm, đảm bảo tính thống nhất trong áp dụng pháp luật trên phạm vi cả nước.

Bộ Công an còn chịu trách nhiệm toàn diện trong việc quản lý các hoạt động liên quan đến dữ liệu, bao gồm xây dựng, phát triển, xử lý, bảo vệ và sử dụng dữ liệu. Bộ là đơn vị đầu mối điều phối và giám sát các quá trình vận hành dữ liệu trong hệ thống các cơ quan nhà nước cũng như giữa các bên liên quan. Một điểm đáng chú ý là Bộ không chỉ đảm nhận vai trò quản lý hành chính thuần túy mà còn chịu trách nhiệm bảo đảm an ninh dữ liệu – một khía cạnh mang tính sống còn trong kỷ nguyên số. Điều này bao gồm cả công tác đấu tranh phòng chống tội phạm sử dụng dữ liệu làm công cụ phạm tội, xử lý các hành vi thu thập, mua bán, chia sẻ dữ liệu trái phép và các hình thức xâm phạm dữ liệu cá nhân, dữ liệu nhà nước, bí mật doanh nghiệp. Ngoài ra, Bộ Công an còn thực hiện chức năng giám sát các hoạt động kinh doanh dữ liệu dưới dạng sản phẩm, dịch vụ – một lĩnh vực mới nổi nhưng mang lại nhiều nguy cơ nếu không được quản lý chặt chẽ.

Một trong những nhiệm vụ đặc biệt quan trọng là xây dựng và tổ chức vận hành Trung tâm dữ liệu quốc gia. Trung tâm này đóng vai trò như một "trái tim số" của toàn bộ hệ thống dữ liệu quốc gia, là nơi tích hợp, lưu trữ và điều phối dữ liệu từ các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội và cả các đơn vị cung cấp dịch vụ công. Bộ Công an có trách nhiệm đảm bảo Trung tâm dữ liệu quốc gia được thiết kế và vận hành theo đúng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, bảo mật, khả năng mở rộng, tính tương thích hệ thống và ổn định lâu dài. Việc vận hành thành công trung tâm này sẽ góp phần quan trọng vào việc nâng cao hiệu quả quản trị công, tăng cường khả năng dự báo, giám sát và đưa ra chính sách kịp thời dựa trên phân tích dữ liệu lớn (big data), đồng thời phục vụ kết nối liên thông, chia sẻ dữ liệu xuyên suốt trong toàn hệ thống hành chính nhà nước.

Bảo đảm Cơ sở dữ liệu quốc gia về cán bộ, công chức, viên chức được đầy đủ, cập nhật theo tiêu chí "đúng, đủ, sạch, sống" - Ảnh: VGP/Nhật Bắc

Về phương diện pháp lý, Bộ Công an có trách nhiệm xây dựng, ban hành hoặc trình cấp có thẩm quyền ban hành các văn bản quy phạm pháp luật liên quan đến lĩnh vực dữ liệu. Không chỉ dừng lại ở việc tạo lập hành lang pháp lý, Bộ còn hướng dẫn thi hành cụ thể các quy định này nhằm đảm bảo tính khả thi và hiệu quả trong thực tiễn. Đây là cơ sở quan trọng để xử lý các mối quan hệ phát sinh từ việc tạo lập, khai thác, lưu trữ và chia sẻ dữ liệu; đồng thời bảo vệ quyền và lợi ích hợp pháp của cá nhân, tổ chức trong môi trường số.

Trong quá trình triển khai các hoạt động xây dựng và vận hành Trung tâm dữ liệu quốc gia, Bộ Công an phối hợp chặt chẽ với Bộ Tư pháp, Văn phòng Chính phủ, Bộ Khoa học và Công nghệ cùng các bộ, ngành, địa phương tiến hành rà soát toàn bộ hệ thống văn bản pháp luật có liên quan. Từ đó, tổng hợp, đánh giá và đề xuất Chính phủ chỉ đạo sửa đổi, bổ sung hoặc xây dựng mới các văn bản quy phạm pháp luật nhằm hoàn thiện khung pháp lý, đảm bảo tính đồng bộ và thống nhất trong việc vận hành hệ thống dữ liệu quốc gia.

Một nhiệm vụ không thể thiếu của Bộ Công an là tổ chức điều phối, kết nối và chia sẻ dữ liệu giữa các hệ thống thông tin, cơ sở dữ liệu của các cơ quan, tổ chức, cá nhân với Cơ sở dữ liệu tổng hợp quốc gia. Việc này được thực hiện thông qua nền tảng kỹ thuật chia sẻ và điều phối dữ liệu đặt tại Trung tâm dữ liệu quốc gia. Bộ phải đảm bảo hoạt động này diễn ra một cách an toàn, liên thông, đồng bộ và hiệu quả, góp phần hình thành nền quản trị dữ liệu hiện đại, phục vụ tốt công tác chỉ đạo, điều hành, thống kê, kiểm tra và xây dựng chính sách.

Bộ Công an chịu trách nhiệm bảo đảm hạ tầng công nghệ thông tin cho các cơ quan Đảng, Nhà nước và tổ chức chính trị - xã hội trong việc vận hành, xử lý dữ liệu tại Trung tâm dữ liệu quốc gia. Nhiệm vụ này đòi hỏi Bộ không chỉ có năng lực

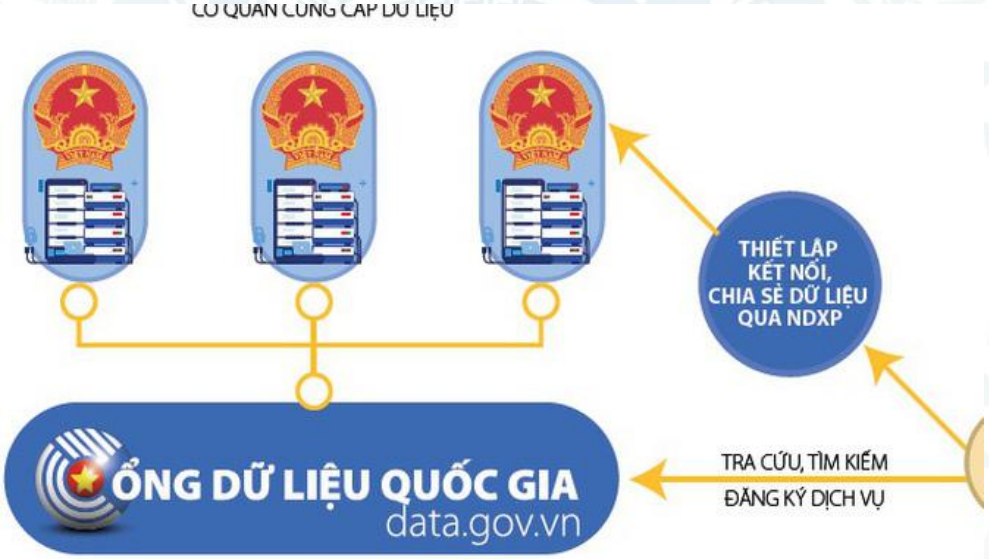
kỹ thuật mà còn phải chủ động trong việc phối hợp, đầu tư, ứng phó với các rủi ro công nghệ có thể xảy ra. Bảo đảm hạ tầng công nghệ thông tin vững chắc cũng là điều kiện tiên quyết để nâng cao hiệu suất xử lý dữ liệu, giảm thiểu gián đoạn và đảm bảo hoạt động ổn định cho toàn bộ hệ thống dữ liệu quốc gia.

Bộ Công an phối hợp với Bộ Khoa học và Công nghệ để tiến hành thẩm định, đánh giá và giám sát quá trình triển khai, vận hành các hệ thống thông tin, cơ sở dữ liệu thuộc Trung tâm dữ liệu quốc gia, trong đó bao gồm cả việc xử lý, ứng phó với các sự cố an toàn thông tin, tấn công mạng, mất dữ liệu và các rủi ro an ninh mạng khác. Đây là nhiệm vụ mang tính kỹ thuật cao và đòi hỏi sự phối hợp chặt chẽ giữa các đơn vị chuyên môn của các bộ, ngành, cũng như hệ thống cảnh báo sớm, phản ứng nhanh đối với mọi sự cố phát sinh.

Ngoài ra, Bộ Công an còn là cơ quan chủ trì trong việc xây dựng hệ thống tiêu chuẩn, quy chuẩn kỹ thuật về tổ chức, kết nối, chia sẻ và đồng bộ dữ liệu với Trung tâm dữ liệu quốc gia. Các tiêu chuẩn này vừa là công cụ kiểm soát kỹ thuật, vừa là nền tảng để đảm bảo hệ thống dữ liệu quốc gia vận hành theo đúng hướng dẫn, tuân thủ các yêu cầu về bảo mật, độ tin cậy và khả năng tích hợp hệ thống. Bộ cũng có trách nhiệm xây dựng kiến trúc hệ thống phần mềm dùng cho Trung tâm dữ liệu quốc gia, bảo đảm kiến trúc phần mềm có tính mở, dễ dàng mở rộng, bảo trì và tích hợp với các nền tảng số hiện có và tương lai.

Trên phạm vi cả nước, Bộ Công an hướng dẫn các cơ quan Đảng, Nhà nước và tổ chức chính trị - xã hội về cách thức phân loại dữ liệu theo mức độ quan trọng, nhạy cảm và bảo mật. Đồng thời, Bộ tổ chức các chương trình đào tạo, bồi dưỡng chuyên môn, nghiệp vụ cho đội ngũ cán bộ, công chức, viên chức trong lĩnh vực dữ liệu, nhằm nâng cao năng lực vận hành, xử lý và khai thác dữ liệu một cách hiệu quả, an toàn, đúng pháp luật.

Bộ Công an cũng là đơn vị được giao nhiệm vụ xây dựng, quản lý và vận hành Cổng dữ liệu quốc gia – nơi tập trung, cung cấp và cho phép truy cập dữ liệu theo các cấp độ được phân quyền. Cổng dữ liệu này phải đảm bảo tính minh bạch, thuận tiện, đồng thời đáp ứng các yêu cầu cao về an toàn thông tin, tạo điều kiện để dữ liệu được chia sẻ, sử dụng đúng mục đích và mang lại giá trị thiết thực trong hoạt động quản lý, nghiên cứu và kinh doanh.



Ảnh minh hoạ

Về mặt tài chính, Bộ trưởng Bộ Công an có quyền quyết định các mức chi hỗ trợ kinh phí cho hoạt động kết nối, chia sẻ dữ liệu, hỗ trợ các chi phí liên quan đến việc thu thập, tạo lập dữ liệu, duy trì hoạt động vận hành hệ thống. Việc này được

thực hiện trên cơ sở thống nhất với Bộ trưởng Bộ Tài chính và Bộ trưởng Bộ Khoa học và Công nghệ nhằm bảo đảm tính hợp lý, minh bạch và hiệu quả trong sử dụng ngân sách nhà nước phục vụ cho phát triển dữ liệu quốc gia.

Như vậy, toàn bộ hệ thống nhiệm vụ được giao cho Bộ Công an tại Điều 26 Nghị định 165/2025/NĐ-CP không chỉ thể hiện rõ vai trò trung tâm của Bộ trong bảo đảm an ninh dữ liệu mà còn đặt ra yêu cầu rất cao về năng lực kỹ thuật, tổ chức phối hợp liên ngành và định hướng phát triển dài hạn. Đây là tiền đề quan trọng để hình thành một hệ sinh thái dữ liệu quốc gia an toàn, hiệu quả, đáp ứng yêu cầu của tiến trình chuyển đổi số, bảo vệ chủ quyền số và phục vụ người dân, doanh nghiệp một cách thiết thực, hiệu quả nhất.

2. Vai trò, trách nhiệm của Trung tâm dữ liệu quốc gia

Trung tâm Dữ liệu quốc gia có vai trò trọng yếu trong kiến tạo và vận hành hạ tầng dữ liệu quốc gia, với nhiều trách nhiệm cụ thể được quy định tại **Điều 31 Luật Dữ liệu năm 2024**. Trước hết, Trung tâm có trách nhiệm tích hợp, đồng bộ, lưu trữ, phân tích và khai thác dữ liệu từ các cơ quan nhà nước theo quy định pháp luật, nhằm tạo lập và quản trị Cơ sở dữ liệu tổng hợp quốc gia – nền tảng trung tâm trong hệ sinh thái dữ liệu số quốc gia. Đồng thời, Trung tâm trực tiếp quản trị, vận hành hạ tầng kỹ thuật, hạ tầng công nghệ thông tin và sàn dữ liệu; chủ động cung cấp hạ tầng công nghệ cho các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị – xã hội có nhu cầu. Một trong những chức năng cốt lõi của Trung tâm là tổ chức vận hành, điều phối, lưu trữ, khai thác và quản lý Cơ sở dữ liệu tổng hợp quốc gia, bảo

đảm phục vụ đúng chức năng, nhiệm vụ của các cơ quan nhà nước cũng như đáp ứng yêu cầu từ các chủ sở hữu dữ liệu, chủ thể dữ liệu theo đúng quy định pháp luật.

Trung tâm Dữ liệu quốc gia có trách nhiệm giám sát chất lượng dữ liệu và hiệu quả của các hoạt động điều phối dữ liệu, thông qua việc xây dựng các chỉ số đo lường và hệ thống đánh giá hiệu suất quản trị dữ liệu một cách bài bản và khách quan. Trung tâm cũng được giao nhiệm vụ thực hiện các biện pháp bảo vệ dữ liệu nhằm bảo đảm an toàn, an ninh và tính toàn vẹn của thông tin. Trong lĩnh vực đổi mới sáng tạo và phát triển công nghệ, Trung tâm đóng vai trò đầu tàu trong nghiên cứu khoa học về dữ liệu, ứng dụng công nghệ hiện đại vào xử lý dữ liệu, cung cấp các sản phẩm – dịch vụ dữ liệu; đồng thời hỗ trợ tổ chức, cá nhân trong khai thác dữ liệu, xây dựng trung tâm đổi mới sáng tạo về khoa học dữ liệu, thúc đẩy hệ sinh thái khởi nghiệp trên nền tảng dữ liệu quốc gia. Song song với đó, Trung tâm cũng tổ chức triển khai các hoạt động hợp tác quốc tế trong lĩnh vực dữ liệu nhằm học hỏi, trao đổi công nghệ, thể chế và kinh nghiệm quản trị. Chi tiết về tổ chức, vận hành và cơ chế thực hiện các trách nhiệm nêu trên sẽ do Chính phủ quy định cụ thể.

Trung tâm dữ liệu quốc gia được kỳ vọng trở thành công cụ giải quyết, tháo gỡ các điểm nghẽn, tạo đột phá trong phát triển cơ sở dữ liệu quốc gia. Ảnh Sưu tầm

**** Trách nhiệm của Trung tâm dữ liệu quốc gia:***

Điều 21 Nghị định số 165/2025/NĐ-CP quy định cụ thể về Trách nhiệm của Trung tâm dữ liệu quốc gia gồm những nội dung sau:

(1) Hướng dẫn cơ quan, tổ chức, cá nhân trong việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu thuộc phạm vi đồng bộ về Trung tâm dữ liệu quốc gia

Một trong những trách nhiệm thiết yếu của Trung tâm Dữ liệu quốc gia trong tiến trình kiến tạo hệ sinh thái dữ liệu quốc gia chính là việc hướng dẫn các cơ quan, tổ chức, cá nhân áp dụng thống nhất các tiêu chuẩn và quy chuẩn kỹ thuật về dữ liệu trong phạm vi cần đồng bộ với Trung tâm. Đây không chỉ là công tác kỹ thuật thuần túy mà còn là một nhiệm vụ quản trị chiến lược, có tác động trực tiếp đến hiệu quả vận hành của Cơ sở dữ liệu tổng hợp quốc gia và toàn bộ nền tảng dữ liệu của quốc gia.

Trong thực tế, sự khác biệt về tiêu chuẩn kỹ thuật, định dạng dữ liệu, phương thức kết nối hoặc mức độ sẵn sàng về hạ tầng giữa các bộ, ngành, địa phương thường gây ra tình trạng phân mảnh thông tin, thiếu đồng bộ, dẫn đến việc không thể liên thông, tích hợp hoặc khai thác dữ liệu hiệu quả. Việc Trung tâm Dữ liệu quốc gia thực hiện hướng dẫn áp dụng các tiêu chuẩn và quy chuẩn kỹ thuật sẽ giúp khắc phục tình trạng trên bằng cách xây dựng khung tham chiếu thống nhất, định hình các yêu cầu kỹ thuật cụ thể mà hệ thống dữ liệu của các chủ thể (cơ quan nhà nước, tổ chức, thậm chí cả doanh nghiệp tư nhân khi tham gia vào hệ thống dữ liệu quốc gia) phải tuân thủ.

Tăng cường hợp tác quốc tế trong ngăn chặn và xử lý tin giả trên không gian mạng. Ảnh minh họa. Nguồn từ Internet.

Cụ thể, Trung tâm cần tổ chức ban hành hoặc tham mưu ban hành bộ tiêu chuẩn kỹ thuật chung cho các loại dữ liệu đầu vào – đầu ra; xây dựng tài liệu hướng dẫn chi tiết về định dạng dữ liệu, cấu trúc dữ liệu, giao thức truyền tải, phương thức mã hóa và bảo mật thông tin; đồng thời quy định rõ các mức độ ưu tiên về dữ liệu cần tích hợp. Trách nhiệm triển khai thực hiện các quy chuẩn kỹ thuật này sẽ thuộc về các đơn vị chủ quản hệ thống cơ sở dữ liệu tại các bộ, ngành, địa phương và các tổ chức được giao nhiệm vụ xây dựng hoặc quản lý dữ liệu trong lĩnh vực chuyên ngành. Trung tâm sẽ đóng vai trò kiểm tra,

rà soát, hỗ trợ kỹ thuật và đánh giá sự tuân thủ định kỳ, đồng thời thiết lập cơ chế phản hồi, điều chỉnh nếu có sai lệch hoặc sự cố phát sinh trong quá trình tích hợp dữ liệu.

Về phương thức thực hiện, Trung tâm có thể phối hợp với Bộ Thông tin và Truyền thông, các đơn vị chuyên trách công nghệ thông tin tại các bộ, ngành, tỉnh/thành phố để tổ chức các lớp tập huấn chuyên môn, hội thảo kỹ thuật, diễn đàn chia sẻ kinh nghiệm, từ đó nâng cao năng lực cho cán bộ dữ liệu ở cơ sở. Việc này cũng cần được gắn liền với các quy định pháp lý và chế tài cụ thể. Trong trường hợp các cơ quan, tổ chức, cá nhân không tuân thủ các tiêu chuẩn kỹ thuật đã hướng dẫn, Trung tâm có thể kiến nghị cơ quan có thẩm quyền tạm dừng tích hợp dữ liệu, đánh giá lại chất lượng hệ thống dữ liệu nguồn, hoặc báo cáo Chính phủ để xem xét xử lý theo quy định.

Nếu không thực hiện nghiêm túc trách nhiệm này, hệ quả sẽ là tình trạng dữ liệu rời rạc, khó liên thông, chi phí xử lý tăng cao, đồng thời ảnh hưởng đến khả năng ra quyết định của Chính phủ dựa trên dữ liệu, làm chậm tiến trình chuyển đổi số quốc gia. Ngược lại, khi thực hiện đầy đủ và hiệu quả, việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật thống nhất sẽ tạo ra một môi trường dữ liệu minh bạch, an toàn, dễ tích hợp và phân tích; tạo tiền đề cho việc triển khai các công nghệ hiện đại như trí tuệ nhân tạo, phân tích dữ liệu lớn, từ đó phục vụ hiệu quả các mục tiêu quản lý, điều hành và phát triển kinh tế – xã hội bền vững.

(2) Thực hiện các biện pháp giám sát, đánh giá chất lượng dữ liệu được chia sẻ, đồng bộ về Trung tâm dữ liệu quốc gia

Trong hệ sinh thái dữ liệu số quốc gia, nơi dữ liệu trở thành tài nguyên chiến lược phục vụ trực tiếp cho quá trình ra quyết định, điều hành và phát triển kinh tế – xã hội, việc chia sẻ và đồng bộ dữ liệu giữa các bộ, ngành, địa phương với Trung tâm Dữ liệu Quốc gia không thể chỉ dừng lại ở mức độ đảm bảo kết nối kỹ thuật hay tương thích hệ thống. Trái lại, bài toán lớn hơn và có tính quyết định là làm thế nào để dữ liệu được chia sẻ và tích hợp vào hệ thống trung tâm đạt chất lượng cao về mọi mặt: chính xác, đầy đủ, cập nhật kịp thời, nhất quán và có giá trị sử dụng thực tế. Trong bối cảnh đó, một trong những trách nhiệm cốt lõi và thường xuyên của Trung tâm Dữ liệu Quốc gia là thực hiện các biện pháp giám sát và đánh giá chất lượng của toàn bộ dữ liệu được chia sẻ, đồng bộ và tích hợp vào hệ thống. Đây là chức năng không thể thay thế nếu muốn xây dựng một nền tảng dữ liệu trung tâm đáng tin cậy, hiệu quả và đủ năng lực phục vụ các mục tiêu lớn của quốc gia trong kỷ nguyên số.

Tổng Bí thư Tô Lâm thăm, kiểm tra hoạt động của Trung tâm Phục vụ hành chính công xã Nghĩa Trụ, tỉnh Hưng Yên, ngày 14-7-2024_Ảnh: TTXVN

Việc giám sát và đánh giá chất lượng dữ liệu cần được tiến hành một cách bài bản, có hệ thống và liên tục, từ khâu thiết kế kiến trúc dữ liệu đến giai đoạn tích hợp và khai thác sử dụng. Trước tiên, Trung tâm Dữ liệu Quốc gia cần thiết lập một bộ chỉ số đánh giá chất lượng dữ liệu thống nhất trên toàn quốc, đóng vai trò như bộ khung tham chiếu bắt buộc để các bộ, ngành,

địa phương và đơn vị chuyên ngành áp dụng trong quá trình xây dựng và chia sẻ dữ liệu. Bộ chỉ số này phải bao gồm các tiêu chí cơ bản như: độ chính xác (tỷ lệ dữ liệu phản ánh đúng thực trạng), độ đầy đủ (mức độ hoàn chỉnh của dữ liệu so với yêu cầu nghiệp vụ), mức độ cập nhật *(tính kịp thời theo thời gian thực hoặc theo chu kỳ)*, tính nhất quán *(không mâu thuẫn giữa các trường, bảng, hệ thống khác nhau)*, và khả năng tương thích *(khả năng tích hợp với kiến trúc kỹ thuật và mô hình dữ liệu trung tâm)*. Ngoài ra, một số chỉ tiêu mở rộng có thể được bổ sung tùy theo loại hình dữ liệu như khả năng tái sử dụng, truy xuất nguồn gốc, mức độ phản ánh dữ liệu thực tiễn hoặc mức độ an toàn, bảo mật.

Trên nền tảng các tiêu chí này, Trung tâm Dữ liệu Quốc gia cần thiết lập một hệ thống giám sát dữ liệu tự động hoạt động theo thời gian thực. Hệ thống này sẽ được tích hợp với các công cụ kiểm định logic dữ liệu, công nghệ học máy và phân tích dữ liệu lớn *(big data analytics)* nhằm sàng lọc, phát hiện sớm các lỗi thường gặp như: trùng lặp bản ghi, sai định dạng, thiếu trường thông tin bắt buộc, không khớp mã định danh, sai sót về mặt nội dung hoặc không cập nhật theo yêu cầu. Những cảnh báo bất thường từ hệ thống giám sát sẽ được gửi đến đơn vị sở hữu dữ liệu để phối hợp xử lý, đồng thời ghi nhận trong hệ thống nhật ký để phục vụ kiểm toán và đánh giá sau này. Đây chính là bước đầu tiên để thiết lập một cơ chế kiểm soát dữ liệu mang tính phòng ngừa, thay vì chỉ khắc phục hậu quả sau khi dữ liệu lỗi đã được khai thác và sử dụng.

Hoạt động giám sát chất lượng dữ liệu cần được tổ chức như một chuỗi quy trình kiểm định toàn diện, gồm giám sát liên tục, kiểm tra định kỳ và đánh giá chuyên đề. Trung tâm cần xây dựng cơ chế đánh giá định kỳ theo chu kỳ quý, bán niên hoặc hàng năm, trong đó kiểm tra không chỉ tính hợp lệ của dữ liệu mà còn năng lực quản lý, vận hành và bảo trì hệ thống dữ liệu tại các đơn vị cung cấp. Bên cạnh đó, các cuộc kiểm tra chuyên đề theo chiều sâu nên được triển khai tại những đơn vị giữ vai trò quan trọng như các bộ, ngành trọng điểm *(Tài chính, Công an, Y tế, Giáo dục, Giao thông…)*, địa phương trung

tâm hoặc những nơi đang xây dựng hệ thống cơ sở dữ liệu ngành quy mô lớn. Thông qua các hoạt động kiểm tra này, Trung tâm có thể phát hiện những điểm nghẽn trong công tác chuẩn hóa dữ liệu, xác định lỗ hổng trong năng lực con người và công nghệ, từ đó có cơ sở đưa ra các khuyến nghị hoặc điều chỉnh về chính sách, tiêu chuẩn kỹ thuật phù hợp hơn với thực tiễn triển khai.

Một điểm đặc biệt quan trọng trong cơ chế giám sát là việc sử dụng các báo cáo đánh giá chất lượng dữ liệu như một công cụ để xếp hạng, phân loại và khuyến khích hoặc xử lý các đơn vị cung cấp dữ liệu. Trung tâm có thể công khai hóa các chỉ số đánh giá theo từng bộ, ngành, địa phương – tạo động lực cạnh tranh lành mạnh và minh bạch trong hệ thống hành chính. Đồng thời, các kết quả đánh giá này cũng là căn cứ quan trọng để Chính phủ và các cơ quan cấp trên xây dựng chính sách ưu tiên đầu tư, hỗ trợ kỹ thuật, đào tạo năng lực hoặc xử lý trách nhiệm hành chính với các đơn vị chưa đáp ứng được yêu cầu. Cách tiếp cận này biến hoạt động giám sát chất lượng dữ liệu từ một khâu kỹ thuật sang một đòn bẩy quản lý công cụ chính sách, gắn kết trực tiếp với hiệu quả vận hành hệ thống hành chính công hiện đại.

Tuy nhiên, nếu trách nhiệm giám sát và đánh giá chất lượng dữ liệu không được thực hiện nghiêm túc và bài bản, Trung tâm Dữ liệu Quốc gia có nguy cơ trở thành một "kho lưu trữ dữ liệu rác" – nơi tích hợp thông tin thiếu độ tin cậy, không đồng nhất hoặc lỗi thời. Khi đó, các hệ thống phân tích, dự báo sẽ tạo ra kết quả sai lệch, ảnh hưởng trực tiếp đến các quyết định điều hành kinh tế – xã hội của Chính phủ. Nghiêm trọng hơn, nếu dữ liệu kém chất lượng trở thành cơ sở cho các thuật toán AI hay hệ thống ra quyết định tự động, hậu quả sẽ lan rộng, khó kiểm soát và gây tổn thất về cả chi phí lẫn uy tín của hệ thống dữ liệu quốc gia. Ngoài ra, tình trạng lặp đi lặp lại lỗi kỹ thuật trong tích hợp dữ liệu cũng sẽ làm gia tăng sự thiếu tin tưởng của người dân, doanh nghiệp và tổ chức đối với hiệu quả thực chất của chuyển đổi số trong khu vực công.

Ngược lại, khi Trung tâm Dữ liệu Quốc gia thực hiện hiệu quả vai trò giám sát chất lượng dữ liệu, giá trị mà dữ liệu mang lại sẽ được nhân lên theo cấp số nhân. Dữ liệu tốt là nền tảng cho các hệ thống hỗ trợ ra quyết định thông minh, cho phép Chính phủ ứng dụng hiệu quả trí tuệ nhân tạo, học máy, mô hình dự báo kinh tế – xã hội và các dịch vụ hành chính số được cá nhân hóa, tối ưu hóa. Chất lượng dữ liệu đồng thời còn là yếu tố tạo dựng niềm tin xã hội đối với Chính phủ số, tạo điều kiện để thúc đẩy các mô hình hợp tác công – tư trong chia sẻ, khai thác dữ liệu và mở rộng hệ sinh thái dịch vụ số trên phạm vi toàn quốc.

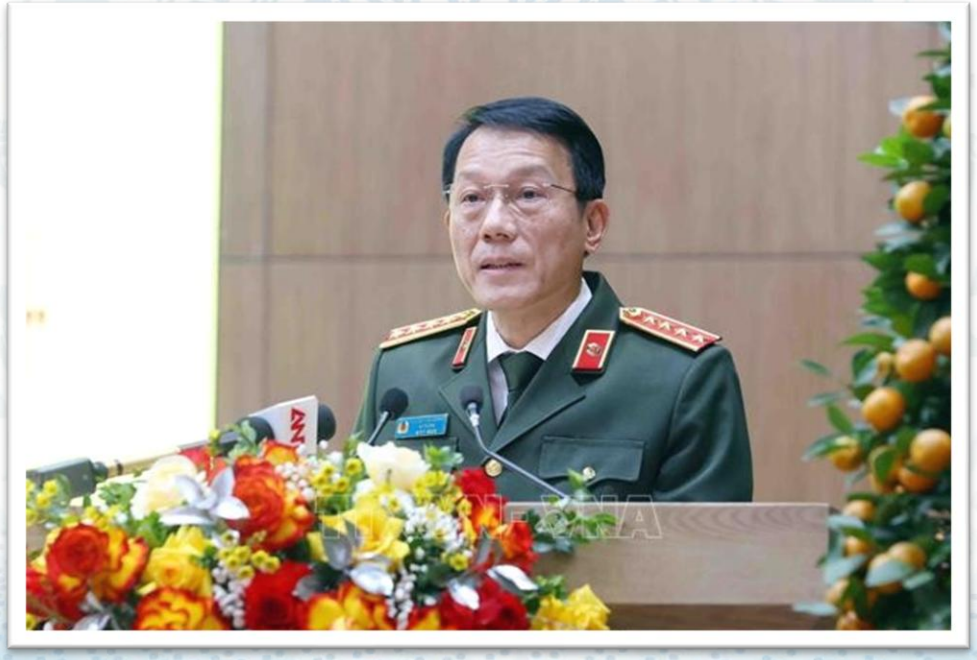
Từ những phân tích trên có thể thấy, giám sát và đánh giá chất lượng dữ liệu không đơn thuần là một mắt xích kỹ thuật phụ trợ, mà là một trụ cột chiến lược trong hệ thống vận hành dữ liệu quốc gia. Nó đòi hỏi sự đầu tư nghiêm túc về nguồn lực con người có chuyên môn cao, hạ tầng công nghệ tiên tiến và một hệ thống thể chế vận hành rõ ràng, minh bạch, có chế tài đủ mạnh. Trong trung và dài hạn, việc phát triển một cơ chế giám sát dữ liệu tự chủ, minh bạch và đạt chuẩn quốc tế sẽ là chìa khóa để bảo đảm sự ổn định, bền vững và giá trị khai thác thực tiễn của toàn bộ hạ tầng dữ liệu số Việt Nam, hướng tới mục tiêu xây dựng một Chính phủ số thông minh, phục vụ người dân, thúc đẩy tăng trưởng kinh tế dựa trên tri thức và dữ liệu thực chứng.

Ảnh minh hoạ

(3) Điều phối dữ liệu của Cơ sở dữ liệu tổng hợp quốc gia

Trong hệ sinh thái dữ liệu số quốc gia, trách nhiệm điều phối dữ liệu của Trung tâm Dữ liệu quốc gia không chỉ là một nhiệm vụ kỹ thuật đơn thuần, mà còn là biểu hiện rõ nét vai trò "bộ não trung tâm" trong việc bảo đảm sự vận hành trơn tru, thông suốt và hiệu quả của toàn bộ hệ thống dữ liệu quốc gia. Điều phối dữ liệu không chỉ dừng lại ở việc thu thập, lưu trữ dữ liệu từ các bộ, ngành, địa phương và tổ chức liên quan, mà còn bao hàm một loạt các hoạt động chuyên sâu, đòi hỏi tầm nhìn chiến lược và khả năng điều hành linh hoạt, khoa học. Đây là nhiệm vụ vừa mang tính tổ chức, kỹ thuật, vừa có tính pháp lý và điều hành vĩ mô.

Cụ thể, Trung tâm Dữ liệu quốc gia cần đảm nhiệm vai trò điều phối toàn diện Cơ sở dữ liệu tổng hợp quốc gia – nơi quy tụ các nguồn dữ liệu chuyên ngành, dữ liệu cấp địa phương, dữ liệu hành chính công và dữ liệu từ các hệ thống thông tin hiện hành. Trung tâm cần chủ động xây dựng một kiến trúc dữ liệu tổng thể, thống nhất, có khả năng kết nối liên ngành, liên vùng và liên lĩnh vực. Kiến trúc này phải xác định rõ các tầng lớp dữ liệu, vai trò và quyền hạn của từng chủ thể tham gia vào quá trình cung – cầu dữ liệu, cũng như cơ chế trao đổi, xử lý và chia sẻ dữ liệu theo thời gian thực. Đây là nền tảng để bảo đảm dữ liệu được điều phối không trùng lặp, không mâu thuẫn, không bị phân mảnh và có thể tái sử dụng hiệu quả.



Bộ trưởng Bộ Công an Lương Tam Quang tại lễ ra mắt Trung tâm dữ liệu quốc gia. Ảnh: TTXVN

Trong vai trò "trục trung tâm kết nối", Trung tâm phải duy trì kết nối thường xuyên với các bộ, ngành, địa phương, đồng thời thiết lập cơ chế điều phối linh hoạt thông qua các giao thức kỹ thuật và thể chế pháp lý phù hợp. Điều này đòi hỏi phải có các quy định cụ thể về quyền truy cập dữ liệu, phân định rõ trách nhiệm trong việc cung cấp, cập nhật và sử dụng dữ liệu, đồng thời kiểm soát được tần suất, thời điểm và chất lượng dữ liệu luân chuyển. Một quy trình điều phối hiệu quả cũng cần có sự giám sát chặt chẽ để xử lý các bất đồng về tiêu chuẩn dữ liệu, xác thực nguồn gốc dữ liệu, loại trừ dữ liệu lỗi hoặc dữ liệu gây nhiễu – từ đó tạo ra một không gian dữ liệu nhất quán, đáng tin cậy và có khả năng phân tích chuyên sâu.

Ngoài ra, điều phối dữ liệu không chỉ là quá trình mang tính hành chính – kỹ thuật thuần túy, mà còn phải được triển khai theo định hướng nhu cầu thực tiễn. Dữ liệu cần được điều phối linh hoạt để đáp ứng yêu cầu phân tích, dự báo và hỗ trợ ra quyết định trong các tình huống đặc biệt như ứng phó thiên tai, kiểm soát dịch bệnh, phòng chống tội phạm mạng, hoặc hỗ trợ phát triển chiến lược kinh tế – xã hội dài hạn. Trong những tình huống này, Trung tâm không chỉ là nơi tập hợp dữ liệu, mà còn phải là "tổng đài điều phối" các luồng dữ liệu từ nhiều nguồn khác nhau, tích hợp theo thời gian thực để phục vụ điều hành nhanh chóng, chính xác và hiệu quả.

Nếu vai trò điều phối dữ liệu không được thực hiện hiệu quả, toàn bộ hệ thống dữ liệu quốc gia sẽ trở nên cồng kềnh, rời rạc và thiếu đồng bộ. Điều này sẽ kéo theo những hệ lụy nghiêm trọng như: các cơ quan nhà nước ra quyết định dựa trên dữ liệu thiếu chính xác hoặc mâu thuẫn; người dân và doanh nghiệp gặp khó khăn trong tiếp cận dịch vụ công do thông tin phân tán; chi phí vận hành hệ thống tăng cao do dữ liệu bị trùng lặp, không thể tái sử dụng; và nguy cơ thất thoát, rò rỉ dữ liệu ngày càng lớn. Đáng lo ngại hơn, sự thiếu hiệu quả trong điều phối dữ liệu có thể làm giảm sút niềm tin của xã hội vào tiến trình chuyển đổi số và năng lực điều hành của Nhà nước.

Ngược lại, nếu công tác điều phối dữ liệu được tổ chức một cách bài bản, có cơ chế phối hợp liên thông – liên ngành, có sự hỗ trợ mạnh mẽ từ nền tảng công nghệ số và hành lang pháp lý chặt chẽ, thì dữ liệu sẽ trở thành một "tài nguyên chiến lược" thực sự. Nó có thể phục vụ đồng thời cho nhiều mục tiêu: từ hoạch định chính sách vĩ mô, nâng cao hiệu quả quản trị công, đến phát triển dịch vụ công chất lượng cao, hỗ trợ cải cách hành chính, và mở ra không gian đổi mới sáng tạo cho doanh nghiệp và xã hội.

Do đó, trách nhiệm điều phối dữ liệu đặt ra yêu cầu rất cao đối với Trung tâm Dữ liệu quốc gia về năng lực tổ chức, năng lực công nghệ, và năng lực thể chế. Trung tâm cần thường xuyên cập nhật công nghệ điều phối dữ liệu tiên tiến *(như hệ thống quản lý luồng dữ liệu tự động, phân tích dữ liệu lớn theo thời gian thực, học máy trong xác minh và phân loại dữ liệu…)*, hoàn thiện khung pháp lý cho các hoạt động điều phối, đồng thời đầu tư bài bản vào đào tạo, phát triển đội ngũ nhân lực có chuyên môn sâu và tư duy chiến lược về dữ liệu. Bên cạnh đó, cần khơi dậy và duy trì niềm tin, cam kết phối hợp từ các bộ, ngành, địa phương và khu vực tư nhân – để hình thành một cơ chế điều phối dữ liệu dựa trên sự tin cậy, hợp tác và cùng phát triển.

(4) Thực hiện các biện pháp bảo vệ dữ liệu được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu theo quy định tại khoản 6 Điều 16 Nghị định 165/2025/NĐ-CP

Đây phải là một trụ cột trong quản trị dữ liệu số quốc gia – được triển khai một cách chủ động, toàn diện, nhất quán và liên tục. Khoản 6 Điều 16 của Nghị định 165/2025/NĐ-CP đã xác lập nguyên tắc pháp lý cốt lõi: các biện pháp bảo vệ dữ liệu

phải được thiết kế và áp dụng ngay từ đầu, tức là được tích hợp xuyên suốt trong toàn bộ quy trình xử lý dữ liệu – từ thu thập, truyền tải, lưu trữ, phân tích đến chia sẻ và khai thác.

Trách nhiệm này đặt lên vai Trung tâm Dữ liệu quốc gia với yêu cầu không chỉ tuân thủ quy định, mà còn phải trở thành một chủ thể tiên phong trong triển khai nguyên lý "privacy by design" (quyền riêng tư ngay từ khâu thiết kế) và "security by default" (bảo mật mặc định). Điều đó có nghĩa là hệ thống bảo vệ dữ liệu không thể chỉ được thêm vào sau cùng, mà phải được lồng ghép ngay trong kiến trúc công nghệ, quy trình vận hành và các chính sách quản trị dữ liệu. Trung tâm, với vai trò trung tâm tích hợp và điều phối dữ liệu cấp quốc gia, cần thể hiện năng lực chủ động trong việc thiết kế, phát triển và duy trì hệ thống dữ liệu có khả năng chống chịu cao trước các nguy cơ tấn công mạng, rò rỉ thông tin và các hành vi khai thác dữ liệu trái phép.

Trên phương diện kỹ thuật, Trung tâm cần triển khai đồng bộ một hệ sinh thái các công cụ và lớp bảo vệ dữ liệu tiên tiến. Cụ thể bao gồm: mã hóa dữ liệu đầu vào – đầu ra theo chuẩn quốc tế; xác thực đa tầng kết hợp với quản lý truy cập chi tiết theo vai trò và cấp độ người dùng; ghi nhật ký đầy đủ các hoạt động xử lý nhằm phục vụ truy vết khi cần thiết; tích hợp hệ thống giám sát và phát hiện bất thường theo thời gian thực; áp dụng các giải pháp bảo mật chủ động như tường lửa đa lớp, hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), công nghệ chống giả mạo, giải pháp ngăn ngừa thất thoát dữ liệu (DLP); cũng như tạo dựng môi trường xử lý tách biệt – đặc biệt là giữa môi trường phát triển, thử nghiệm và vận hành chính thức. Việc kiểm soát chặt chẽ luồng dữ liệu giữa các môi trường là một biện pháp phòng ngừa quan trọng trước các nguy cơ lạm dụng lỗ hổng trong quá trình thử nghiệm để đánh cắp hoặc phá hoại dữ liệu thật.

Trên phương diện tổ chức, Trung tâm cần ban hành và thực hiện đầy đủ quy trình vận hành chuẩn (SOP) về bảo vệ dữ liệu, với các nội dung cụ thể như quy trình kiểm tra an ninh định kỳ, kịch bản ứng phó khi xảy ra sự cố bảo mật, phân công rõ trách nhiệm giữa các bộ phận kỹ thuật, giám sát và quản lý. Đặc biệt, cần coi trọng đào tạo và nâng cao nhận thức cho toàn bộ đội ngũ cán bộ, từ kỹ sư công nghệ đến nhân viên vận hành hệ thống và người sử dụng cuối – bởi lẽ yếu tố con người vẫn luôn là mắt xích dễ bị tổn thương nhất trong chuỗi an toàn dữ liệu. Những sai sót nhỏ trong thao tác, sự thiếu hiểu biết về các rủi ro hoặc sự chủ quan trong xử lý thông tin đều có thể dẫn đến hậu quả nghiêm trọng và không thể khắc phục.

Ảnh minh hoạ

Trong bối cảnh các mối đe dọa mạng ngày càng tinh vi và mang tính xuyên biên giới, việc Trung tâm Dữ liệu quốc gia không thực hiện nghiêm túc và đầy đủ các biện pháp bảo vệ dữ liệu ngay từ đầu sẽ tiềm ẩn những hậu quả khôn lường. Đó có thể là việc bị tấn công mã hóa tống tiền (ransomware) làm tê liệt hệ thống điều hành quốc gia, bị đánh cắp dữ liệu cá nhân

diện rộng gây mất lòng tin của người dân, hay bị thao túng dữ liệu điều hành khiến các quyết sách trở nên sai lệch. Nghiêm trọng hơn, một vụ rò rỉ dữ liệu ở cấp độ quốc gia có thể trở thành mối đe dọa đối với an ninh quốc gia và chủ quyền số, kéo theo hệ lụy cả về chính trị, kinh tế và xã hội.

Ảnh minh hoạ

Ngược lại, khi các biện pháp bảo vệ được áp dụng đầy đủ ngay từ giai đoạn thiết kế, và được duy trì nghiêm ngặt trong toàn bộ vòng đời dữ liệu, Trung tâm sẽ thực sự trở thành một "pháo đài số" – nơi hội tụ niềm tin của hệ thống chính trị, các bộ ngành, địa phương và người dân. Khi đó, dữ liệu không chỉ là nguyên liệu cho ra quyết định, mà còn là nguồn lực chiến

lược để vận hành chính quyền số, thúc đẩy đổi mới sáng tạo, cung cấp dịch vụ công chất lượng cao, và làm nền móng cho phát triển bền vững.

Từ góc độ tổng thể, có thể khẳng định rằng: trách nhiệm bảo vệ dữ liệu không thể bị xem nhẹ, bị trì hoãn hay bị phân tán. Đó là nhiệm vụ trung tâm, cần được đặt ngang hàng với các nhiệm vụ thu thập, xử lý và khai thác dữ liệu. Việc bảo vệ phải bắt đầu từ thiết kế hệ thống, lan tỏa đến toàn bộ chuỗi xử lý, gắn chặt với công nghệ hiện đại, khung pháp lý vững chắc và con người được đào tạo bài bản, có trách nhiệm. Đây chính là nền tảng vững chắc để Trung tâm Dữ liệu quốc gia phát huy vai trò đầu tàu trong bảo vệ tài nguyên dữ liệu, đảm bảo an toàn – an ninh thông tin, và góp phần xây dựng một quốc gia số thịnh vượng, tự chủ và bền vững trong thế kỷ XXI.

(5) 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

Trong bối cảnh toàn cầu đang bước vào thời kỳ của nền kinh tế dữ liệu, khi dữ liệu không chỉ là nguồn tài nguyên chiến lược mà còn là động lực cốt lõi thúc đẩy đổi mới sáng tạo, phát triển khoa học – công nghệ và năng lực quản trị quốc gia, việc mở rộng hợp tác quốc tế trong lĩnh vực dữ liệu trở thành yêu cầu tất yếu. Trước yêu cầu này, Trung tâm Dữ liệu quốc gia được giao trọng trách đặc biệt quan trọng: kết nối Việt Nam với hệ sinh thái dữ liệu toàn cầu thông qua việc chủ động ký kết các thỏa thuận hợp tác, biên bản ghi nhớ (MoU) với các tổ chức, cơ quan, mạng lưới dữ liệu quốc tế. Trách nhiệm này không

chỉ mang tính ngoại giao chuyên ngành mà còn là một phần của chiến lược bảo vệ chủ quyền số, định vị vị thế quốc gia trên bản đồ công nghệ dữ liệu thế giới.

Trước hết, Trung tâm Dữ liệu quốc gia cần xây dựng kế hoạch hợp tác quốc tế một cách bài bản, có trọng tâm, trọng điểm, lựa chọn đúng đối tác chiến lược theo từng nhóm lĩnh vực ưu tiên. Với các tổ chức như Liên Hợp Quốc (UNDP, ITU), OECD, ASEAN, APEC, WEF, Ngân hàng Thế giới, các cơ quan liên chính phủ hoặc trung tâm dữ liệu hàng đầu thế giới (như Gaia-X của EU, GovTech Singapore, Bộ Nội vụ Hàn Quốc, Cơ quan Dữ liệu Nhật Bản…), Trung tâm có thể chủ động đề xuất hợp tác về các nội dung như: chuẩn hóa kỹ thuật dữ liệu, chia sẻ kinh nghiệm quản trị dữ liệu công, an toàn thông tin mạng, bảo vệ quyền riêng tư, phát triển dữ liệu mở, kiểm soát luồng dữ liệu xuyên biên giới, hoặc đồng tổ chức các diễn đàn, hội nghị quốc tế về dữ liệu.

Một nội dung mang tính kỹ thuật – pháp lý phức tạp và nhạy cảm là chuyển giao dữ liệu xuyên biên giới (cross-border data transfer). Trong bối cảnh dữ liệu ngày càng trở thành tài sản xuyên lãnh thổ, việc đảm bảo dòng chảy dữ liệu an toàn, hợp pháp giữa Việt Nam và các quốc gia khác đòi hỏi phải có khuôn khổ hợp tác song phương và đa phương chặt chẽ. Trung tâm Dữ liệu quốc gia có trách nhiệm thiết lập các thoả thuận bảo mật dữ liệu (Data Protection Agreements), các nguyên tắc xử lý dữ liệu chung (Joint Data Processing Guidelines) với đối tác quốc tế, trong đó làm rõ quy định về chủ quyền dữ liệu, giới hạn truy cập, điều kiện chia sẻ và cơ chế giám sát, nhằm tránh tình trạng dữ liệu công dân Việt Nam bị sử dụng sai mục đích, hoặc thất thoát ra nước ngoài ngoài tầm kiểm soát.

Song song với đó, đào tạo và nâng cao năng lực chuyên môn là một nội dung đặc biệt cần nhấn mạnh trong các chương trình hợp tác. Trung tâm cần tổ chức hoặc tham gia các chương trình học bổng, thực tập sinh, khóa đào tạo chuyên sâu, trao đổi cán bộ kỹ thuật, các dự án nghiên cứu chung với tổ chức quốc tế về khoa học dữ liệu, điện toán đám mây, trí tuệ nhân tạo, phân tích dữ liệu lớn (big data analytics), quản trị dữ liệu theo mô hình quốc tế. Có thể triển khai hình thức "đồng đào tạo" (co-training) với các viện công nghệ của Hàn Quốc, Nhật Bản, Singapore, EU, thiết lập các trung tâm R&D liên quốc gia trong lĩnh vực dữ liệu để Việt Nam tiếp thu tri thức công nghệ đỉnh cao và giảm sự phụ thuộc vào công nghệ nước ngoài theo hướng bị động.

Trung tâm Dữ liệu quốc gia cũng có thể phát triển các liên minh đổi mới sáng tạo khu vực, khuyến khích việc xây dựng và thử nghiệm các sản phẩm số dùng chung, các giao thức quản trị dữ liệu minh bạch và tiên tiến, từ đó hỗ trợ cộng đồng doanh nghiệp khởi nghiệp sáng tạo trong nước vươn ra toàn cầu. Đặc biệt, cần ưu tiên thúc đẩy trao đổi chuyên gia dữ liệu cấp cao, mời gọi chuyên gia quốc tế đến Việt Nam làm việc ngắn hạn hoặc dài hạn, đồng thời cử chuyên gia Việt Nam ra nước ngoài tu nghiệp, nhằm tạo ra nguồn nhân lực hạt nhân chất lượng cao, đủ sức vận hành hệ thống dữ liệu quy mô quốc gia và khu vực.

Thủ tướng và các đại biểu tham dự phiên họp. Ảnh minh họa. Nguồn từ Internet.

Nếu Trung tâm Dữ liệu quốc gia thực hiện hiệu quả nhiệm vụ hợp tác quốc tế, Việt Nam sẽ không chỉ tận dụng được nguồn lực bên ngoài về tài chính, công nghệ, kinh nghiệm quản trị, mà còn nâng cao vị thế trong mạng lưới dữ liệu toàn cầu, thúc đẩy công cuộc chuyển đổi số quốc gia đi vào chiều sâu và thực chất. Ngược lại, nếu buông lỏng nhiệm vụ này, Việt Nam sẽ bị lệ thuộc vào công nghệ nước ngoài, khó kiểm soát dòng chảy dữ liệu xuyên biên giới, và mất cơ hội tiếp cận những tri thức công nghệ tiên tiến đang biến đổi từng ngày.

Như vậy, trách nhiệm thực hiện hợp tác quốc tế của Trung tâm Dữ liệu quốc gia không chỉ đơn thuần là ký kết biên bản ghi nhớ mang tính nghi lễ, mà là một nhiệm vụ chiến lược, dài hạn, liên ngành, đòi hỏi tầm nhìn toàn cầu, sự phối hợp chặt chẽ với các bộ, ngành và sự chủ động cao trong vận hành. Thành công trong hợp tác quốc tế về dữ liệu chính là chìa khóa để Việt Nam giữ vững chủ quyền số, đẩy mạnh phát triển khoa học công nghệ, và hội nhập sâu rộng trong kỷ nguyên số toàn cầu.

(6) Giúp Bộ Công an thực hiện quản lý nhà nước về dữ liệu

Trung tâm dữ liệu quốc gia là một trong những trụ cột quan trọng của hạ tầng số quốc gia, giữ vai trò trung tâm trong việc lưu trữ, quản lý, chia sẻ và khai thác dữ liệu một cách thống nhất, hiệu quả và bảo mật. Đối với Bộ Công an, cơ quan được giao nhiệm vụ quản lý nhà nước về an ninh quốc gia, trật tự an toàn xã hội, phòng chống tội phạm và bảo vệ quyền, lợi ích hợp pháp của công dân, sự ra đời và vận hành của Trung tâm dữ liệu quốc gia mang ý nghĩa chiến lược trong việc nâng cao năng lực quản lý dữ liệu, tạo lập nền tảng dữ liệu tin cậy để hỗ trợ công tác nghiệp vụ, hành chính và dự báo chiến lược. Với hệ thống lưu trữ và xử lý dữ liệu tập trung, đồng bộ, có khả năng tích hợp dữ liệu từ các bộ, ngành, địa phương, các cơ sở dữ liệu chuyên ngành, Trung tâm này cung cấp cho Bộ Công an nguồn dữ liệu đầy đủ, chính xác, được cập nhật theo thời gian thực, giúp giảm thiểu thời gian xử lý thông tin, tăng cường hiệu quả quản lý nhà nước và điều hành lực lượng.

Chiều ngày 4/7/2025, tại Hà Nội, Trung tâm Dữ liệu quốc gia - Bộ Công an tổ chức Lễ ra mắt Trung tâm Sáng tạo, khai thác dữ liệu và Phòng An ninh, an toàn hệ thống. Ảnh sưu tầm

Trung tâm dữ liệu quốc gia giúp Bộ Công an thực hiện hiệu quả công tác thu thập, xác minh, đối chiếu và phân tích dữ liệu từ nhiều nguồn khác nhau. Trong bối cảnh dữ liệu ngày càng phong phú, phân tán và có tính biến động cao, việc sở hữu một cơ sở dữ liệu tổng hợp tập trung là điều kiện tiên quyết để bảo đảm tính liên thông và toàn vẹn của dữ liệu, giúp lực lượng Công an tránh được tình trạng phân mảnh thông tin, lệ thuộc vào nguồn dữ liệu riêng lẻ từ các đơn vị. Việc đồng bộ hóa dữ

liệu dân cư, dữ liệu di biến động, dữ liệu doanh nghiệp, tài chính, đất đai, giao thông, viễn thông, y tế, giáo dục và các cơ sở dữ liệu khác tại Trung tâm dữ liệu quốc gia cho phép Bộ Công an truy cập nhanh chóng và có độ chính xác cao, từ đó phục vụ hiệu quả cho các hoạt động nghiệp vụ như điều tra, truy xét, phòng chống tội phạm công nghệ cao, giám sát an ninh trật tự, quản lý cư trú, xuất nhập cảnh, cấp phát giấy tờ và xử lý vi phạm hành chính.

Với khả năng kết nối, phân tích và xử lý dữ liệu lớn (Big Data), Trung tâm dữ liệu quốc gia tạo điều kiện để Bộ Công an ứng dụng các công nghệ mới như trí tuệ nhân tạo (AI), học máy (Machine Learning), xử lý ngôn ngữ tự nhiên (NLP) và phân tích dự báo trong các hoạt động nghiệp vụ. Các hệ thống phân tích dựa trên dữ liệu lớn giúp Bộ Công an phát hiện sớm các nguy cơ tiềm ẩn về an ninh quốc gia, tội phạm có tổ chức, tội phạm xuyên quốc gia, các hành vi vi phạm pháp luật diễn biến phức tạp trên không gian mạng. Khi có thể tích hợp dữ liệu từ nhiều nguồn, các mô hình phân tích dự đoán tội phạm hay nhận diện hành vi bất thường sẽ trở nên hiệu quả và chính xác hơn. Nhờ đó, Bộ Công an có thể chủ động triển khai các biện pháp phòng ngừa, ngăn chặn từ sớm, từ xa, thay vì chỉ phản ứng sau khi sự việc đã xảy ra, giảm thiểu tổn thất cho người dân và Nhà nước.

Công an xã Vĩnh Lợi, tỉnh Cà Mau thu thập dữ liệu, cấp đổi thẻ đảng viên

Trung tâm dữ liệu quốc gia đóng vai trò quan trọng trong việc thiết lập cơ chế chia sẻ, phân quyền và giám sát việc sử dụng dữ liệu, từ đó giúp Bộ Công an tăng cường năng lực quản lý nhà nước về dữ liệu trên phạm vi toàn quốc. Thông qua việc xác lập các quy định thống nhất về chuẩn hóa dữ liệu, phân loại dữ liệu, cấp quyền truy cập và sử dụng, kiểm tra và đánh giá hiệu suất khai thác dữ liệu tại các cơ quan, đơn vị, Trung tâm sẽ hỗ trợ Bộ Công an trong vai trò xây dựng chính sách, ban hành hướng dẫn, kiểm tra giám sát việc thực thi pháp luật về dữ liệu. Đồng thời, cơ chế này cũng bảo đảm quyền tiếp cận dữ liệu một cách minh bạch, có kiểm soát, không để xảy ra tình trạng lạm dụng, sai mục đích, rò rỉ hoặc sử dụng dữ liệu vì mục

đích cá nhân hay lợi ích nhóm. Đây là tiền đề để Bộ Công an bảo vệ quyền riêng tư cá nhân, an toàn thông tin và chủ quyền dữ liệu quốc gia.

Việc tích hợp hệ thống dữ liệu chuyên ngành trong lực lượng Công an vào Trung tâm dữ liệu quốc gia sẽ làm tăng mức độ phối hợp liên ngành trong phòng chống tội phạm và đảm bảo an ninh trật tự. Dữ liệu do lực lượng Công an tạo lập và thu thập sẽ không còn đơn độc mà sẽ trở thành một phần trong hệ thống dữ liệu quốc gia, có thể được kết nối với dữ liệu y tế để quản lý người nghiện ma túy, dữ liệu giáo dục để kiểm soát tội phạm học đường, dữ liệu tài chính để theo dõi rửa tiền, dữ liệu môi trường để giám sát các hành vi vi phạm pháp luật về tài nguyên. Nhờ việc chia sẻ dữ liệu hai chiều này, Bộ Công an có thể nắm bắt đầy đủ hơn về đối tượng, bối cảnh và quy luật hoạt động của các loại tội phạm, từ đó nâng cao hiệu quả công tác điều tra, truy tố, xét xử và thi hành án.

Trung tâm dữ liệu quốc gia cũng hỗ trợ Bộ Công an trong việc triển khai dịch vụ công trực tuyến và cải cách thủ tục hành chính trên môi trường số. Với hệ thống cơ sở dữ liệu tập trung, các thủ tục như cấp căn cước công dân, đăng ký cư trú, đăng ký phương tiện, khai báo tạm vắng, khai sinh, khai tử… sẽ được xử lý nhanh chóng, liên thông và hạn chế tối đa tiếp xúc trực tiếp, giảm gánh nặng cho cán bộ chiến sĩ, đồng thời tạo thuận lợi cho người dân và doanh nghiệp. Các thông tin cần thiết sẽ được tự động lấy từ kho dữ liệu quốc gia, thay vì yêu cầu người dân nộp lại nhiều lần, từ đó giảm chi phí xã hội, nâng cao chỉ số hài lòng của người dân đối với dịch vụ công ngành công an. Việc số hóa thủ tục hành chính còn giúp tăng tính minh bạch, chống tiêu cực, tham nhũng, sai lệch trong quá trình xử lý hồ sơ.

Trong lĩnh vực quản lý cư trú và kiểm soát di biến động dân cư, Trung tâm dữ liệu quốc gia có vai trò như một bản đồ số dân cư sống động, cập nhật liên tục, giúp Bộ Công an theo dõi chặt chẽ tình hình cư trú, quản lý người nước ngoài, phát hiện các trường hợp cư trú bất hợp pháp, ngăn ngừa tội phạm lợi dụng kẽ hở trong quản lý nhân khẩu để hoạt động trái phép. Khi được tích hợp với dữ liệu xuất nhập cảnh, dữ liệu giáo dục, y tế, tài chính và viễn thông, việc nhận diện các đối tượng nghi vấn sẽ trở nên nhanh chóng và hiệu quả hơn, hỗ trợ lực lượng chức năng đưa ra các biện pháp nghiệp vụ phù hợp.

Trong lĩnh vực an ninh mạng, Trung tâm dữ liệu quốc gia hỗ trợ Bộ Công an tăng cường khả năng giám sát không gian mạng, phát hiện sớm các chiến dịch tấn công mạng, lan truyền thông tin xấu độc, hoạt động gián điệp mạng, tội phạm sử dụng công nghệ cao. Dữ liệu mạng xã hội, dữ liệu hành vi số, dữ liệu kết nối mạng viễn thông nếu được xử lý và phân tích tại Trung tâm với sự phối hợp của các hệ thống bảo mật tiên tiến sẽ cho phép Bộ Công an chủ động hơn trong việc bảo vệ an ninh quốc gia trên không gian số. Ngoài ra, Trung tâm còn đóng vai trò là nơi kiểm thử và đánh giá các giải pháp an ninh mạng quốc gia, góp phần xây dựng các kịch bản ứng phó sự cố, đảm bảo khả năng phục hồi hệ thống trong tình huống khẩn cấp.

Việc phát triển nguồn nhân lực số trong ngành Công an cũng được thúc đẩy mạnh mẽ thông qua hợp tác giữa Bộ Công an và Trung tâm dữ liệu quốc gia. Việc tham gia khai thác, phân tích, bảo mật và vận hành dữ liệu đòi hỏi đội ngũ cán bộ có trình độ chuyên môn cao về công nghệ thông tin, khoa học dữ liệu, an ninh mạng và quản trị dữ liệu. Trung tâm sẽ là nơi tổ chức đào tạo, bồi dưỡng, chuyển giao công nghệ, thực hành thực tế cho lực lượng công an kỹ thuật và nghiệp vụ, từ đó nâng cao chất lượng nhân lực, tạo ra thế hệ cán bộ chiến sĩ có khả năng làm chủ công nghệ và thích ứng nhanh với bối cảnh mới.

Trung tướng Nguyễn Minh Chính nhấn mạnh vai trò của bảo vệ an toàn không gian mạng tại Việt Nam trong bối cảnh hiện nay

Trong việc thực hiện chức năng xây dựng và hoàn thiện hệ thống pháp luật về dữ liệu, Trung tâm dữ liệu quốc gia là nguồn cung cấp thực tiễn phong phú, làm cơ sở để Bộ Công an nghiên cứu, đề xuất chính sách phù hợp, sát thực tế và có tính khả thi cao. Những bài học từ việc chia sẻ, khai thác, bảo mật và xử lý dữ liệu trong thực tiễn sẽ được tổng hợp, đánh giá, từ

đó giúp Bộ Công an hoàn thiện pháp luật liên quan đến an ninh dữ liệu, bảo vệ thông tin cá nhân, trách nhiệm pháp lý về dữ liệu, xử lý vi phạm hành chính và hình sự liên quan đến dữ liệu số. Đồng thời, Trung tâm còn có vai trò phối hợp tổ chức giám sát, đánh giá tác động của các quy định pháp luật liên quan đến dữ liệu trong quá trình thực thi, từ đó kiến nghị điều chỉnh cho phù hợp với sự phát triển nhanh chóng của công nghệ và xu thế hội nhập quốc tế.

Vai trò của Trung tâm dữ liệu quốc gia trong hỗ trợ Bộ Công an thực hiện quản lý nhà nước về dữ liệu không chỉ thể hiện ở chiều rộng *(tích hợp, chia sẻ, đồng bộ)* mà còn ở chiều sâu *(phân tích, dự báo, quản lý rủi ro)*. Đây chính là một công cụ chiến lược để lực lượng Công an chuyển mình từ mô hình vận hành truyền thống sang mô hình điều hành dựa trên dữ liệu, hướng tới hình thành lực lượng Công an thông minh, phản ứng nhanh, chính xác và chủ động trong mọi tình huống. Đó cũng là bước đi cụ thể để thực hiện thắng lợi các mục tiêu của Đề án 06, Chiến lược phát triển Chính phủ số và đảm bảo vững chắc an ninh quốc gia trong thời đại dữ liệu.

3. Vai trò, trách nhiệm của Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu

Trong kỷ nguyên chuyển đổi số và phát triển kinh tế số, dữ liệu đang dần trở thành tài nguyên chiến lược, có giá trị không kém gì tài nguyên truyền thống như đất đai, khoáng sản hay nguồn nhân lực. Dữ liệu không chỉ là "nhiên liệu" để vận hành các hệ thống số, trí tuệ nhân tạo và dịch vụ thông minh, mà còn là yếu tố sống còn để nâng cao hiệu lực, hiệu quả quản lý nhà nước, phục vụ người dân và phát triển kinh tế - xã hội. Tuy nhiên, song song với cơ hội là những thách thức nghiêm trọng về an ninh, an toàn dữ liệu và nguy cơ gia tăng tội phạm mạng, lạm dụng dữ liệu cá nhân, tấn công hạ tầng số quốc gia.

Trong bối cảnh đó, lực lượng Công an nhân dân – đặc biệt là Công an các đơn vị, địa phương – có vai trò, trách nhiệm hết sức quan trọng trong công tác quản lý nhà nước về dữ liệu. Đây không chỉ là một yêu cầu nghiệp vụ thông thường mà là nhiệm vụ chiến lược có tính lâu dài, xuyên suốt và mang ý nghĩa quyết định đối với việc bảo vệ chủ quyền số, quyền riêng tư và sự ổn định của hệ thống dữ liệu quốc gia.

Trước hết, Công an các đơn vị, địa phương đóng vai trò nòng cốt trong việc triển khai thực hiện các chủ trương, chính sách và quy định pháp luật của Nhà nước về quản lý dữ liệu. Dưới sự chỉ đạo trực tiếp của Bộ Công an và chính quyền địa phương, lực lượng công an cơ sở là cầu nối giữa cấp trung ương với cơ sở, tổ chức thực hiện các nội dung quản lý dữ liệu gắn liền với thực tiễn địa bàn. Công tác này bao gồm việc nắm chắc tình hình thu thập, lưu trữ, xử lý và chia sẻ dữ liệu trên địa bàn; tham gia rà soát, đánh giá mức độ rủi ro và phân loại các hệ thống dữ liệu trọng yếu cần bảo vệ đặc biệt; phối hợp với các ngành chức năng kiểm tra, giám sát việc chấp hành quy định pháp luật về bảo vệ dữ liệu cá nhân, dữ liệu nhạy cảm, dữ liệu định danh... Trong nhiều trường hợp, chính Công an cấp huyện, cấp xã là đơn vị đầu tiên phát hiện ra dấu hiệu bất thường về lưu chuyển dữ liệu, hoạt động khai thác dữ liệu trái phép, hay hành vi giả mạo, can thiệp vào hệ thống dữ liệu công vụ – từ đó kịp thời báo cáo, tham mưu, xử lý nhằm ngăn chặn nguy cơ phát sinh các sự cố nghiêm trọng.

Công nghệ hiện đại giúp tiết kiệm thời gian cho người dân. Ảnh minh họa. Nguồn từ Internet.

Một trong những nhiệm vụ nổi bật của Công an các đơn vị, địa phương trong quản lý nhà nước về dữ liệu là đảm bảo an ninh dữ liệu, an toàn hệ thống thông tin phục vụ công tác bảo vệ an ninh quốc gia, trật tự an toàn xã hội. Dữ liệu, nhất là dữ liệu định danh công dân, dữ liệu sinh trắc học, dữ liệu giao dịch tài chính, hồ sơ sức khỏe, học tập hay thông tin hành chính công – đều là mục tiêu hấp dẫn đối với tội phạm mạng. Các thế lực thù địch, tổ chức phản động, nhóm tin tặc trong và ngoài nước luôn tìm cách khai thác các lỗ hổng trong quản trị dữ liệu để phá hoại uy tín hệ thống chính quyền, gây mất ổn định xã

hội hoặc trục lợi tài chính. Trước tình hình đó, Công an địa phương giữ vai trò chủ công trong việc phát hiện, phòng ngừa, đấu tranh và xử lý các hành vi vi phạm pháp luật liên quan đến dữ liệu như xâm nhập trái phép vào hệ thống mạng, phát tán mã độc, đánh cắp thông tin, buôn bán dữ liệu cá nhân, làm giả hồ sơ dữ liệu điện tử, hay lợi dụng dữ liệu để thực hiện hành vi lừa đảo, chiếm đoạt tài sản.

Thiếu tướng Trần Nguyên Quân - Phó Cục trưởng V03 - Bộ Công an khẳng định, việc hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân là yêu cầu cấp bách nhằm xây dựng Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam trong giai đoạn mới

tại hội thảo "Tăng cường hoàn thiện pháp luật bảo vệ dữ liệu cá nhân trong kỷ nguyên số" do V03 - Bộ Công an phối hợp với Công an tỉnh Thanh Hoá tổ chức ngày 01/8/2025. Ảnh Sưu tầm

Công tác nắm tình hình, thu thập và xử lý thông tin nghiệp vụ liên quan đến dữ liệu là một phần không thể tách rời trong hoạt động thường xuyên của Công an các cấp. Trong đó, việc quản lý chặt chẽ các hệ thống thu thập dữ liệu có liên quan đến quốc phòng, an ninh, dữ liệu trọng yếu quốc gia tại địa phương như cơ sở dữ liệu dân cư, dữ liệu đăng ký cư trú, dữ liệu giám sát an ninh trật tự qua camera, dữ liệu y tế công cộng, dữ liệu giáo dục – đào tạo, dữ liệu về tài nguyên – môi trường... là nhiệm vụ ưu tiên. Lực lượng Công an cần phối hợp với các sở, ban, ngành và doanh nghiệp công nghệ triển khai các biện pháp kiểm tra, đánh giá độ an toàn, kiểm thử bảo mật định kỳ, từ đó kịp thời phát hiện lỗ hổng, kiến nghị biện pháp vá lỗi hoặc khắc phục sự cố kỹ thuật. Ngoài ra, Công an địa phương cũng phải trực tiếp tham gia xây dựng, vận hành và giám sát các hệ thống ứng dụng dữ liệu phục vụ quản lý nhà nước trên địa bàn, như hệ thống quản lý di biến động dân cư, quản lý người nước ngoài, hệ thống định danh điện tử, hay ứng dụng quản lý thông tin an ninh – trật tự.

Trong vai trò là lực lượng giữ gìn trật tự, an toàn xã hội tại cơ sở, Công an các đơn vị, địa phương cũng đóng vai trò quan trọng trong công tác tuyên truyền, phổ biến pháp luật và nâng cao nhận thức cộng đồng về bảo vệ dữ liệu. Việc tuyên truyền cần được tổ chức thường xuyên, linh hoạt, phù hợp với từng nhóm đối tượng như học sinh – sinh viên, người lao động phổ thông, người cao tuổi, doanh nghiệp nhỏ và vừa... để mọi người đều nhận thức được quyền, trách nhiệm và cách thức tự bảo vệ dữ liệu cá nhân. Những nội dung cơ bản như: không chia sẻ thông tin định danh, mã OTP, tài khoản ngân hàng trên mạng; không truy cập liên kết lạ; không cài đặt phần mềm không rõ nguồn gốc; phải sử dụng mật khẩu mạnh và xác thực hai lớp... cần được truyền đạt bằng hình thức dễ hiểu, sinh động, có tình huống minh họa cụ thể. Công an cấp xã, công an phường

– những đơn vị gần dân, sát dân nhất – có thể lồng ghép nội dung tuyên truyền về bảo vệ dữ liệu vào các buổi họp tổ dân phố, hội nghị khu dân cư, sinh hoạt đoàn thể để lan tỏa ý thức dữ liệu đến từng hộ dân, từng người dân.

Công an các đơn vị, địa phương xử lý sự cố, điều tra và hỗ trợ pháp lý khi xảy ra vi phạm pháp luật liên quan đến dữ liệu. Khi có sự cố rò rỉ thông tin, tấn công mạng hoặc hành vi gian lận liên quan đến dữ liệu xảy ra trên địa bàn, lực lượng Công an địa phương cần nhanh chóng kích hoạt quy trình tiếp nhận, xác minh, phối hợp điều tra và truy vết thủ phạm. Trong nhiều trường hợp, sự phối hợp hiệu quả giữa Công an cấp huyện với các cơ quan kỹ thuật trung ương như Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Cục Kỹ thuật nghiệp vụ hoặc đơn vị chuyên trách của Bộ Thông tin và Truyền thông có thể giúp sớm bóc gỡ các đường dây lừa đảo, mạng botnet hoặc tổ chức phát tán mã độc tinh vi. Ngoài ra, lực lượng Công an còn hỗ trợ doanh nghiệp, người dân lập biên bản sự việc, thu thập chứng cứ điện tử, xử lý yêu cầu kỹ thuật và thực hiện các biện pháp pháp lý theo quy định hiện hành.

Trong hoạt động quản lý dữ liệu, Công an các đơn vị, địa phương còn có nhiệm vụ tổ chức đào tạo, bồi dưỡng nâng cao năng lực cho đội ngũ cán bộ, chiến sĩ về kiến thức, kỹ năng bảo vệ dữ liệu, an ninh mạng, phân tích mã độc, điều tra số và pháp luật liên quan. Bên cạnh đó, cần chủ động cập nhật tình hình tội phạm công nghệ cao, xu hướng tấn công mới, kỹ thuật tàng hình, mã hóa dữ liệu và ứng dụng trí tuệ nhân tạo vào các hành vi vi phạm để nâng cao khả năng phản ứng, xử lý các tình huống phức tạp. Việc xây dựng đội ngũ cán bộ chuyên sâu về dữ liệu tại Công an tỉnh, thành phố và lực lượng nòng cốt tại Công an cấp huyện là yêu cầu cấp thiết để đáp ứng yêu cầu bảo vệ dữ liệu trong điều kiện thực tiễn ngày càng khó lường.

Cán bộ Công an xã Cái Đôi Vàm, tỉnh Cà Mau tuyên truyền về bảo vệ dữ liệu cá nhân cho các cơ sở kinh doanh về điện thoại trên địa bàn. Ảnh Sưu tầm

Công an các đơn vị, địa phương cũng phải thực hiện trách nhiệm báo cáo, thống kê, phân tích và đề xuất các giải pháp quản lý dữ liệu trên địa bàn. Các báo cáo định kỳ hoặc đột xuất về tình hình an ninh dữ liệu, vi phạm pháp luật, các sự cố điển hình cần được gửi về Bộ Công an và chính quyền các cấp để phục vụ công tác tổng hợp, điều chỉnh chính sách, xây dựng văn bản quy phạm pháp luật và hoàn thiện các cơ chế phối hợp liên ngành. Đồng thời, thông qua các báo cáo, lực lượng Công an

có thể kiến nghị các mô hình ứng dụng dữ liệu hiệu quả, các biện pháp phòng ngừa chủ động, đề xuất đầu tư nâng cấp hạ tầng bảo mật tại địa phương hoặc đưa vào danh sách giám sát đặc biệt các lĩnh vực dữ liệu có nguy cơ cao.

Từ tất cả những phân tích trên, có thể khẳng định rằng, vai trò và trách nhiệm của Công an các đơn vị, địa phương trong công tác quản lý nhà nước về dữ liệu là toàn diện, xuyên suốt và gắn chặt với cả khía cạnh quản lý hành chính lẫn bảo vệ an ninh quốc gia. Lực lượng Công an không chỉ là người "gác cửa" cho hệ thống dữ liệu, mà còn là người "dẫn đường" trong việc tuyên truyền, giáo dục, hỗ trợ người dân và doanh nghiệp nâng cao năng lực bảo vệ thông tin cá nhân. Sự chủ động, trách nhiệm, chuyên nghiệp và kịp thời của Công an các cấp chính là một trong những yếu tố quyết định thành công của công cuộc xây dựng chính phủ số, xã hội số và kinh tế số tại Việt Nam trong những năm tới. Trong bối cảnh công nghệ biến đổi không ngừng, dữ liệu ngày càng gắn bó sâu rộng với đời sống con người, thì việc nâng cao vai trò của Công an trong quản lý và bảo vệ dữ liệu không chỉ là nhiệm vụ ngành, mà là yêu cầu tất yếu của phát triển bền vững quốc gia.

III. NHIỆM VỤ TRỌNG TÂM CẦN TẬP TRUNG TRONG GIAI ĐOẠN TỪ NAY ĐẾN NĂM 2030

1. Về dữ liệu

- Hoàn thành xây dựng và đưa vào khai thác kho dữ liệu tổng hợp, triển khai ngay việc tổng hợp dữ liệu liên quan đến cộng dân Việt Nam và người nước ngoài sinh sống, có hoạt động tại nước ta làm tiền đề phát triển các cơ sở dữ liệu quốc gia phục vụ bảo đảm an ninh quốc gia, phát triển kinh tế - xã hội *(hoàn thành cơ bản năm 2025)*; bảo đảm dữ liệu đúng, đủ, sạch, sống cho các cơ sở dữ liệu quốc gia cũng như cơ sở dữ liệu của các cơ quan, tô chức do dữ liệu được tổng hợp, đôi sánh từ

nhiêu nguôn; giảm thiêu các bước trung gian trong quá trình kết nồi, chia sẻ. Kho dữ liệu về con người bao gồm dữ liệu thuộc các lĩnh vực.

- Đến hết năm 2025, hoàn thành cơ bản xây dựng và đưa vào khai thác kho dữ liệu tổng hợp được đồng bộ từ các cơ sở dữ liệu quốc gia và phối hợp khai thác với kho dữ liệu về con người; từ năm 2026, triển khai thực hiện việc phân tích dữ liệu chuyên sâu hỗ trợ công tác xây dựng cơ chế chính sách, quy hoạch chiến lược phát triển quốc gia, góp phần thúc đẩy phát triển kinh tế - xã hội.

- Từ năm 2025, đưa Trung tâm dữ liệu quốc gia đóng vai trò là nơi để trao đổi, kết nối quốc tế nhằm chia sẽ thông tin, nghiên cứu phát triển các chiến lược phát triển và đặt nền tảng nghiên cứu, hỗ trợ khai thác, phát triển nền tảng khoa học công nghệ đất nước.

- Đên 2030, hoàn thành việc triên khai Trung tâm dữ liệu quốc gia là nơi lưu trữ dữ liệu, hệ thông thông tin của các cơ sở dữ liệu quôc gia, kêt nồi liên thông dữ liệu với các cơ sở dữ liệu chuyên ngành, các hệ thống thông tin trong nước và tổ chức Chính phủ các nước để phục vụ các hoạt động trên môi trường số bảo đảm lợi ích hợp pháp của nước ta.

2. Về quy hoạch kiến trúc dữ liệu của Trung tâm dữ liệu quốc gia

- Đến năm 2025, hoàn thành xây dựng và triển khai Bộ tiêu chuẩn áp dụng cho công tác quy hoạch kiến trúc các cơ sở dữ liệu quốc gia tại Trung tâm dữ liệu quốc gia về việc phân cấp, phân loại dữ liệu theo các độ mở, cấp độ mật, tối mật, tuyệt mật và mức độ ảnh hưởng đến quốc gia, người dân và doanh nghiệp; hoàn thành quy hoạch cụ thể phân kho lưu trữ và thiết

lập các chính sách an ninh an toàn thông tin phù hợp với đối tượng, phương thức truy cập, quyền khai thác đối với từng loại dữ liệu.

- Đến năm 2030, hoàn thành việc triển khai các quy hoạch, tiêu chuẩn, kiến trúc dữ liệu tại Trung tâm dữ liệu quốc gia cũng như cơ sở dữ liệu của bộ, ngành, địa phương

3. Về phân tích và khai thác dữ liệu

- Đến hết năm 2025, triển khai thành công các công nghệ, giải pháp hiện đại và đào tạo được chuyên gia khoa học dữ liệu, đặc biệt là chuyên gia phân tích dữ liệu có trình độ cao để thực hiện công tác phát triển, tổng hợp và khai thác, phân tích dữ liệu tổng thể, đa chiều, khách quan,...

- Từ năm 2026, triển khai công tác lập các báo cáo dự báo tham mưu cho Chính phủ và các bộ, ngành, địa phương phục vụ công tác quản lý, điều hành thông qua dữ liệu. Thực hiện cung cấp một số dữ liệu dùng chung, dữ liệu mở quan trọng đáp ứng nhu cầu sử dụng cho người dân, doanh nghiệp và đối tác nước ngoài khai thác phục vụ phát triên kinh tế - xã hội.

- Đến năm 2030, trên 90% các 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 từ các kho dữ liệu tổng hợp trong Trung tâm dữ liệu quốc gia.

4. Về hạ tầng, thiết bị công nghệ thông tin

- Đến hết 2025, hoàn thành cơ bản việc xây dựng hạ tâng nhà trạm của Trung tâm dữ liệu quốc gia tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật của quốc tè về trung tâm dữ liệu, về an toàn thông tin, bảo đảm độ sẵn sàng của hệ thông, 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 mục tiêu của cuộc cách mạng 4.0.

- Từ năm 2026, thực hiện cung cấp hạ tầng nhà trạm 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 các bộ, ngành và địa phương (có nhu câu) nhằm bảo đảm 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 cả trong và xung quanh khu vực Trung tâm dữ liệu quốc gia; bảo đảm cung cấp hạ tầng công nghệ thông tin cho các cơ sở dữ liệu quốc gia; các bộ, ngành, địa phương (có nhu cầu) và 100% các tổ chức chính trị - xã hội sử dụng; tích hợp với ha tầng công nghệ thông tin có sẵn của các đơn vị để thống nhất, đồng bộ trong công tác vận hành, quản trị và bảo đảm an ninh, an toàn, tiết kiệm, hiệu quả.

- Đến năm 2030, cơ bản các hệ thống thông tin của bộ, ngành, địa phương được quản lý, lưu trữ ở Trung tâm dữ liệu quốc gia.

5. 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 phú số. Đến năm 2025, tối thiểu 80% hồ sơ thủ tục hành chính được xử lý hoàn toàn trực tuyến, người dân, tổ chức và đơn vị phải nhập dữ liệu một lần. Cắt giảm tối thiểu 20% thành phần hồ sơ thủ tục hành chính của các cơ quan nhà nước so với hiện nay. Mức độ hải 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 thực 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%.

6. Về phát triển Chính phủ điện tử

Đến năm 2025, Việt Nam thuộc nhóm: 70 nước dẫn đầu về Chính phủ điện tử (EGDI); 50 nước dẫn đầu về công nghệ thông tin (IDI); 40 nước dẫn đầu về an toàn, an ninh mạng (GCl).

Đến năm 2030, Việt Nam thuộc nhóm: 50 nước dẫn đầu về Chính phủ điện tử (EGDI); 30 nước dẫn dầu về công nghệ thông tin (IDI); 30 nước dẫn đầu về an toàn, an ninh mạng (GCI).

7. Về phát triển kinh tế - xã hội

Phát triển thêm các lĩnh vực, ngành nghề kinh tế mới dựa trên dữ liệu và đóng góp vào tăng trưởng tỷ trọng kinh tế số trong Tổng sản phẩm trong nước (GDP) theo mục tiêu quốc gia *"Đến năm 2025, kinh tế số Việt Nam đạt khoảng 20% GDP, đưa Việt Nam vươn lên đứng thứ hai về kinh tế số ở Đông Nam Á. Đến năm 2030, kinh tế số chiếm 30% GDP"*. Tham gia quan trọng vào phát triển nền kinh tế dữ liệu, bảo đảm mục tiêu kinh tế dữ liệu đóng góp vào GDP đất nước.

IV. ĐỀ XUẤT 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

1. Hoàn thiện thể chế, xây dựng chiến lược, cơ sở pháp lý về dữ liệu phục vụ an ninh quốc gia

Nhiệm vụ này không chỉ là phát triển kinh tế, mà là thiết lập một hệ thống văn bản quy phạm pháp luật để bảo vệ chủ quyền số, ngăn chặn các hoạt động lợi dụng không gian mạng để xâm phạm an ninh quốc gia; theo đó, giải pháp để thực hiện nhiệm vụ này cần:

1.1. Hoàn thiện thể chế, chủ động tháo gỡ các rào cản pháp lý, hành chính, tạo lập môi trường thuận lợi cho sáng tạo, nghiên cứu và ứng dụng khoa học công nghệ, biến thể chế thành lợi thế cạnh tranh quốc gia

Việc hoàn thiện thể chế nhằm tháo gỡ các rào cản pháp lý và hành chính để tạo lập môi trường thuận lợi cho sáng tạo, nghiên cứu và ứng dụng khoa học công nghệ là một nhiệm vụ cấp thiết trong bối cảnh toàn cầu đang chuyển dịch mạnh mẽ sang nền kinh tế tri thức. Trong hệ sinh thái đổi mới sáng tạo, thể chế đóng vai trò như một "bệ đỡ" pháp lý đảm bảo cho các hoạt động nghiên cứu, phát triển và ứng dụng công nghệ được vận hành thông suốt, hiệu quả, bền vững. Khi thể chế chưa theo kịp tốc độ phát triển của khoa học công nghệ, sẽ xuất hiện khoảng trống chính sách, làm chậm nhịp độ chuyển đổi số, hạn chế khả năng thương mại hóa kết quả nghiên cứu, đồng thời tạo ra tâm lý e ngại trong việc đầu tư cho sáng tạo. Do đó, việc rà soát, sửa đổi và xây dựng mới các văn bản quy phạm pháp luật liên quan đến khoa học công nghệ phải được đặt lên hàng đầu, vừa đảm bảo tính đồng bộ hệ thống, vừa linh hoạt, mở đường cho thử nghiệm chính sách (sandbox), từ đó hình thành khuôn khổ pháp lý ổn định và tiên tiến, có tính dự báo, dẫn dắt thị trường đổi mới sáng tạo.

Môi trường pháp lý thuận lợi cần được thiết kế theo hướng khuyến khích mạo hiểm, thúc đẩy sáng tạo, thay vì nặng về kiểm soát hành chính. Các rào cản thủ tục như quy định cấp phép, thẩm định, kiểm định công nghệ mới phải được rút gọn, tinh giản hoặc chuyển đổi theo mô hình quản lý rủi ro dựa trên dữ liệu thay vì dựa trên thủ tục hành chính cứng nhắc. Đặc biệt trong lĩnh vực công nghệ số, trí tuệ nhân tạo, dữ liệu lớn, các quy định pháp luật cần "đi trước một bước", chấp nhận độ trễ trong đánh giá để không kìm hãm các ý tưởng đột phá. Việc áp dụng cơ chế "chấp thuận có điều kiện", "thử nghiệm có kiểm soát" là công cụ thể chế hóa hiệu quả tinh thần linh hoạt, thúc đẩy đổi mới. Bên cạnh đó, cần mạnh dạn cắt bỏ các quy định không còn phù hợp, không tạo ra giá trị cho xã hội, hoặc gây cản trở cho doanh nghiệp khởi nghiệp sáng tạo và các tổ chức nghiên cứu công lập, tư nhân. Cải cách thể chế không chỉ gắn với cải thiện môi trường đầu tư kinh doanh nói chung, mà phải đặc biệt hướng đến thúc đẩy sự phát triển của hệ sinh thái đổi mới sáng tạo quốc gia, từ chính sách thuế ưu đãi cho nghiên cứu phát triển, bảo hộ quyền sở hữu trí tuệ, đến quy trình thương mại hóa sản phẩm khoa học công nghệ.

Song song với việc hoàn thiện pháp luật chuyên ngành, cần cải cách mạnh mẽ bộ máy tổ chức quản lý nhà nước về khoa học công nghệ, đảm bảo tính nhất quán, hiệu lực, hiệu quả trong chỉ đạo, điều hành. Việc chồng chéo về chức năng giữa các cơ quan, sự phân tán trong ban hành chính sách, thiếu cơ chế phối hợp liên ngành đã và đang là rào cản lớn trong việc tạo lập môi trường thể chế thuận lợi. Cần tái cấu trúc cơ quan chủ trì quản lý khoa học công nghệ theo hướng chuyên nghiệp, đủ năng lực nắm bắt xu thế công nghệ mới, am hiểu thị trường và có khả năng kết nối các nguồn lực. Đồng thời, các bộ, ngành, địa phương phải được phân cấp mạnh mẽ, chủ động trong việc xây dựng chính sách hỗ trợ nghiên cứu, đổi mới sáng tạo, trên cơ sở phù hợp định hướng chung của quốc gia. Cơ chế điều phối vùng, liên kết giữa trung ương và địa phương cũng phải

được hoàn thiện để bảo đảm sự lan tỏa của thể chế đổi mới, không để một số trung tâm đô thị trở thành "ốc đảo" sáng tạo trong khi các địa phương khác bị bỏ lại phía sau.

Một phần không thể thiếu trong việc hoàn thiện thể chế là tăng cường tính minh bạch, trách nhiệm giải trình, đảm bảo quyền tiếp cận và phản hồi chính sách của cộng đồng khoa học, doanh nghiệp và người dân. Các cơ chế tham vấn chính sách cần được thiết kế mở, lấy ý kiến rộng rãi và thực chất, đặc biệt từ các nhóm khởi nghiệp, nhà đầu tư công nghệ, viện trường và chuyên gia độc lập. Hệ thống thông tin pháp luật, cổng dữ liệu mở và các công cụ chính phủ số cần được tích hợp nhằm tạo điều kiện thuận lợi cho tra cứu, sử dụng và giám sát chính sách công liên quan đến khoa học công nghệ. Minh bạch thể chế chính là nền tảng để nâng cao niềm tin và khuyến khích các chủ thể đầu tư dài hạn cho nghiên cứu, sáng tạo.

Cùng với quá trình hoàn thiện thể chế, cần triển khai quyết liệt các giải pháp tháo gỡ rào cản hành chính đang tồn tại trong quản lý hoạt động khoa học công nghệ, từ cấp kinh phí nghiên cứu, xét duyệt đề tài, thanh quyết toán cho đến đánh giá nghiệm thu sản phẩm. Nhiều quy trình hiện nay vẫn áp dụng tư duy "xin – cho", phụ thuộc vào thẩm quyền cá nhân, dẫn đến tình trạng kéo dài thời gian, làm mất động lực nghiên cứu hoặc bóp méo mục tiêu học thuật. Việc chuyển từ quản lý đầu vào sang quản lý theo kết quả đầu ra, tăng cường cơ chế đặt hàng nhiệm vụ nghiên cứu từ nhu cầu thực tiễn của doanh nghiệp, địa phương, xã hội sẽ góp phần nâng cao hiệu quả sử dụng ngân sách khoa học công nghệ. Hơn nữa, cần phát triển hệ thống định giá sản phẩm khoa học công nghệ, tạo hành lang pháp lý cho hoạt động đấu giá tài sản trí tuệ, chuyển giao công nghệ, đảm bảo tính thị trường và công bằng trong phân phối kết quả nghiên cứu.

Thể chế thuận lợi cho đổi mới sáng tạo không thể thiếu một hệ thống tiêu chuẩn – quy chuẩn kỹ thuật tiên tiến, cập nhật với thông lệ quốc tế. Việc xây dựng, sửa đổi, ban hành và áp dụng tiêu chuẩn phải dựa trên sự tham gia của cộng đồng

khoa học, viện nghiên cứu, hiệp hội doanh nghiệp, và đặc biệt là cộng đồng công nghệ. Không thể có đổi mới sáng tạo hiệu quả nếu các sản phẩm mới không được chứng nhận hoặc bị "mắc kẹt" do thiếu tiêu chuẩn phù hợp. Do đó, thể chế về tiêu chuẩn hóa phải đi kèm với các chương trình hỗ trợ doanh nghiệp thử nghiệm, đánh giá, chuyển đổi tiêu chuẩn theo mô hình mở, chấp nhận rủi ro ở mức hợp lý và thúc đẩy quá trình thương mại hóa sáng chế.

Hội nghị trao đổi, tháo gỡ các "điểm nghẽn" trong quá trình triển khai Đề án Trung tâm Dữ liệu quốc gia. Nguồn từ Internet.

Chuyển đổi số trong xây dựng và vận hành thể chế là một yêu cầu cấp thiết, góp phần nâng cao tính linh hoạt, khả năng đáp ứng nhanh và hiệu quả thực thi chính sách về khoa học công nghệ. Việc số hóa quy trình xây dựng, rà soát, cập nhật văn bản quy phạm pháp luật sẽ cho phép phát hiện kịp thời các xung đột, chồng chéo và lạc hậu của các văn bản hiện hành, đồng thời tăng cường năng lực hoạch định chính sách dựa trên dữ liệu lớn. Hệ thống trí tuệ nhân tạo có thể được tích hợp để hỗ trợ cơ quan nhà nước trong phân tích tác động chính sách, mô phỏng các kịch bản điều chỉnh pháp lý, từ đó đưa ra lựa chọn tối ưu. Việc số hóa cũng giúp rút ngắn thời gian xây dựng chính sách, tăng cường tương tác với cộng đồng, nâng cao hiệu quả thực thi và giám sát chính sách.

Quá trình hoàn thiện thể chế phải đồng thời hướng đến mục tiêu xây dựng lợi thế cạnh tranh quốc gia dựa trên nền tảng khoa học công nghệ và đổi mới sáng tạo. Trong kỷ nguyên số, thể chế không chỉ là khung pháp lý nội địa, mà còn là công cụ cạnh tranh trong hội nhập quốc tế. Một thể chế năng động, thông minh, có khả năng điều chỉnh linh hoạt theo thị trường sẽ tạo niềm tin cho các nhà đầu tư, thu hút chất xám toàn cầu, định vị Việt Nam như một trung tâm đổi mới sáng tạo trong khu vực. Lợi thế cạnh tranh không còn nằm ở tài nguyên hay nhân công giá rẻ, mà phụ thuộc vào khả năng sáng tạo, năng suất đổi mới, tốc độ thương mại hóa công nghệ và năng lực thích ứng chính sách. Do đó, xây dựng một thể chế đổi mới sáng tạo vượt trội chính là điều kiện tiên quyết để Việt Nam vươn lên thành quốc gia phát triển nhanh, bền vững.

Dưới góc độ lực lượng Công an nhân dân, hoàn thiện thể chế trong lĩnh vực khoa học công nghệ còn mang ý nghĩa chiến lược trong việc nâng cao năng lực phòng ngừa, phát hiện, điều tra và xử lý tội phạm sử dụng công nghệ cao, tội phạm mạng, gián điệp mạng và các hành vi xâm phạm an ninh quốc gia trong không gian số. Việc xây dựng hành lang pháp lý phù hợp cho phép lực lượng Công an tiếp cận, ứng dụng và làm chủ các thành tựu khoa học công nghệ tiên tiến như trí tuệ nhân

tạo, phân tích dữ liệu lớn, mã hóa và bảo mật thông tin, nhận dạng sinh trắc học, công nghệ giám sát thông minh, từ đó củng cố năng lực nghiệp vụ hiện đại, giảm thiểu sự phụ thuộc vào công nghệ ngoại nhập. Đồng thời, thể chế thuận lợi cũng tạo điều kiện cho việc hợp tác nghiên cứu giữa lực lượng Công an với các viện nghiên cứu, trường đại học, doanh nghiệp công nghệ trong và ngoài nước, nhằm nâng cao năng lực nội sinh, phát triển các sản phẩm công nghệ đặc thù phục vụ yêu cầu bảo vệ an ninh quốc gia, trật tự an toàn xã hội trong tình hình mới. Thể chế tiên tiến cũng giúp Công an các đơn vị, địa phương triển khai hiệu quả các đề án chuyển đổi số trong lĩnh vực an ninh, xây dựng trung tâm dữ liệu an ninh, hệ thống cảnh báo sớm, giám sát hành vi tội phạm trên không gian mạng, góp phần bảo vệ lợi ích quốc gia – dân tộc và quyền riêng tư chính đáng của người dân trong kỷ nguyên số hóa.

1.2. Xây dựng và hoàn thiện hệ thống pháp luật về dữ liệu gồm Luật Dữ liệu, các nghị định, thông tư hướng dẫn, tiêu chuẩn – quy chuẩn kỹ thuật về định danh, xác thực, chia sẻ, bảo mật và giao dịch dữ liệu.

Việc xây dựng và hoàn thiện hệ thống pháp luật về dữ liệu là một trong những trụ cột nền tảng nhằm đảm bảo sự phát triển lành mạnh, bền vững và hiệu quả của nền kinh tế số, xã hội số và chính phủ số. Trong bối cảnh dữ liệu trở thành tài nguyên cốt lõi, việc thiếu hành lang pháp lý rõ ràng, đồng bộ và thực thi hiệu quả sẽ tạo ra khoảng trống nghiêm trọng, gây khó khăn cho công tác quản lý, điều hành và phát triển các mô hình ứng dụng dữ liệu vào mọi lĩnh vực đời sống. Vì vậy, một trong những nhiệm vụ cấp thiết hiện nay là xây dựng Luật Dữ liệu với tính bao quát, đồng bộ, minh bạch và có khả năng điều chỉnh các quan hệ xã hội mới phát sinh trong môi trường số. Luật Dữ liệu phải đặt nền móng cho hệ thống pháp luật chuyên sâu về dữ liệu, trong đó xác lập rõ các khái niệm pháp lý nền tảng như dữ liệu cá nhân, dữ liệu nhạy cảm, dữ liệu mở, dữ liệu

công, dữ liệu thương mại; làm rõ quyền và nghĩa vụ của các chủ thể trong hoạt động tạo lập, thu thập, xử lý, phân tích, chia sẻ, lưu trữ và sử dụng dữ liệu.

Cùng với việc xây dựng Luật Dữ liệu, cần thiết ban hành các nghị định hướng dẫn thi hành, cụ thể hóa các điều khoản mang tính nguyên tắc của luật thành các quy định chi tiết, khả thi trong thực tiễn. Các nghị định này cần quy định rõ quy trình, thủ tục, điều kiện cấp phép, giám sát, xử lý vi phạm, quyền và trách nhiệm của các tổ chức, cá nhân tham gia vào hoạt động dữ liệu. Đặc biệt, cần đảm bảo sự phân định rạch ròi giữa dữ liệu công và dữ liệu tư nhân, giữa quyền sở hữu, quyền sử dụng và quyền định đoạt dữ liệu để tránh chồng chéo, xung đột và làm phát sinh rủi ro pháp lý cho các chủ thể liên quan. Đồng thời, các nghị định cần làm rõ các cơ chế bảo vệ dữ liệu cá nhân, bảo đảm an ninh, an toàn thông tin, và phòng ngừa các hành vi xâm phạm, mua bán, khai thác trái phép dữ liệu.

Việc ban hành hệ thống thông tư hướng dẫn là bước quan trọng nhằm cụ thể hóa và thống nhất cách hiểu, cách áp dụng luật và nghị định tại các cơ quan, tổ chức, doanh nghiệp, địa phương. Các thông tư cần có sự tham gia soạn thảo của các cơ quan chuyên môn kỹ thuật, cơ quan quản lý ngành, các chuyên gia pháp lý, nhằm bảo đảm tính đồng bộ và phù hợp với thực tiễn triển khai ở từng lĩnh vực. Nội dung các thông tư phải định hướng rõ ràng về quy trình xử lý dữ liệu trong từng khâu, từ định danh số, xác thực danh tính, đến lưu trữ, chia sẻ và giao dịch dữ liệu. Mỗi quy định kỹ thuật trong thông tư cần được minh chứng bằng mô hình vận hành mẫu, bài học thực tiễn hoặc quy chuẩn quốc tế để đảm bảo tính khả thi và khả năng hội nhập.

Việc xây dựng và ban hành hệ thống tiêu chuẩn – quy chuẩn kỹ thuật về dữ liệu là nhiệm vụ không thể thiếu trong việc hình thành nền tảng hạ tầng dữ liệu quốc gia. Tiêu chuẩn kỹ thuật phải đặt ra yêu cầu đồng bộ về định danh điện tử, mã hóa dữ liệu, xác thực người dùng, chia sẻ dữ liệu xuyên biên giới, bảo mật trong lưu trữ – xử lý – phân tích dữ liệu, và an toàn trong giao dịch dữ liệu. Việc áp dụng các tiêu chuẩn cần thống nhất với hệ sinh thái số quốc gia, đồng thời có khả năng liên kết với các nền tảng khu vực và quốc tế. Các tiêu chuẩn kỹ thuật phải thường xuyên cập nhật để thích ứng với tiến bộ công nghệ, các hình thức tấn công mới, cũng như yêu cầu ngày càng cao về bảo vệ quyền riêng tư và chủ quyền số.

Hệ thống quy chuẩn kỹ thuật về dữ liệu phải được thiết kế với tính ràng buộc bắt buộc đối với các cơ quan nhà nước và khuyến khích áp dụng trong khu vực tư nhân. Cần có cơ chế đánh giá, kiểm định, chứng nhận khả năng tuân thủ quy chuẩn, làm cơ sở cho việc xếp hạng, chấm điểm chuyển đổi số và năng lực quản trị dữ liệu của các tổ chức. Ngoài ra, quy chuẩn phải được nội luật hóa bằng các công cụ pháp lý đủ mạnh để xử phạt các hành vi không tuân thủ, đồng thời khuyến khích sự tham gia của cộng đồng doanh nghiệp, tổ chức tiêu chuẩn quốc tế và các hiệp hội ngành nghề trong quá trình xây dựng và rà soát định kỳ hệ thống này.

Phó Chủ tịch Quốc hội Nguyễn Khắc Định chủ trì phiên họp về nội dung xem xét, quyết định điều chỉnh Chương trình lập pháp năm 2025. Nguồn từ Internet.

Cần phát triển hệ thống quy định về định danh điện tử nhằm bảo đảm mỗi cá nhân, tổ chức, thiết bị được nhận diện duy nhất, đầy đủ và có thể xác thực qua không gian mạng. Việc định danh phải bảo đảm tính bảo mật, độ tin cậy và khả năng tích hợp với các hệ thống dữ liệu khác nhau như dữ liệu dân cư, dữ liệu y tế, dữ liệu học tập, dữ liệu tài chính. Định danh điện tử

cũng là cơ sở quan trọng để triển khai các dịch vụ công trực tuyến, các hoạt động thanh toán số và giao dịch thương mại điện tử, giúp tiết kiệm chi phí xã hội và gia tăng hiệu quả quản lý của nhà nước.

Cần xây dựng hệ thống quy định pháp luật về xác thực dữ liệu và xác thực danh tính để kiểm tra độ tin cậy của dữ liệu, đảm bảo dữ liệu không bị giả mạo, không bị can thiệp trái phép. Cơ chế xác thực cần được phân cấp theo mức độ rủi ro, từ mức xác thực cơ bản đến xác thực nâng cao, có thể ứng dụng công nghệ sinh trắc học, mã hóa hai lớp, chữ ký số, xác thực bằng trí tuệ nhân tạo. Việc thiết lập các quy định này cần được tích hợp vào hệ thống văn bản pháp luật hiện hành về an ninh mạng, bảo mật thông tin, và được triển khai đồng bộ trong các cơ quan hành chính, tổ chức tài chính – ngân hàng, y tế và giáo dục.

Việc chia sẻ dữ liệu giữa các cơ quan, tổ chức, doanh nghiệp cần được điều chỉnh bởi một hành lang pháp lý rõ ràng, quy định rõ điều kiện, phương thức, đối tượng, giới hạn và trách nhiệm trong việc chia sẻ. Cần ưu tiên xây dựng cơ chế chia sẻ dữ liệu theo mô hình "dữ liệu mở có kiểm soát", trong đó bảo đảm quyền tiếp cận dữ liệu công cho người dân và doanh nghiệp, đồng thời giữ vững an toàn, an ninh quốc gia. Cơ chế này cần được triển khai theo nguyên tắc dữ liệu chia sẻ theo yêu cầu chính đáng, có mục đích cụ thể, có sự đồng ý hoặc ủy quyền rõ ràng của chủ thể dữ liệu, và có công cụ giám sát việc sử dụng dữ liệu sau chia sẻ.

Việc bảo mật dữ liệu phải được nâng tầm thành nghĩa vụ pháp lý bắt buộc đối với mọi tổ chức và cá nhân tham gia hệ sinh thái dữ liệu. Cần ban hành các quy định cụ thể về mức độ bảo mật đối với từng loại dữ liệu, từ dữ liệu nhạy cảm, dữ liệu cá nhân, đến dữ liệu chiến lược quốc gia. Các tổ chức phải có nghĩa vụ triển khai hệ thống bảo mật đa lớp, tiến hành kiểm thử

lỗ hổng bảo mật định kỳ, xây dựng kế hoạch phòng ngừa, ứng phó sự cố dữ liệu và chịu trách nhiệm pháp lý trong trường hợp để xảy ra vi phạm. Hệ thống pháp luật cần đi kèm chế tài đủ mạnh để ngăn ngừa hành vi xâm phạm dữ liệu, đồng thời bảo đảm quyền khởi kiện, yêu cầu bồi thường của người bị thiệt hại do mất dữ liệu hoặc lộ lọt thông tin.

Cần thiết lập cơ chế pháp lý cho giao dịch dữ liệu, xác lập địa vị pháp lý của dữ liệu như một loại tài sản đặc biệt, có thể được định giá, chuyển nhượng, cấp phép, mua bán hoặc dùng làm tài sản thế chấp. Pháp luật cần quy định về điều kiện hợp đồng giao dịch dữ liệu, xác lập giá trị pháp lý của chữ ký điện tử, quyền sở hữu trí tuệ đối với dữ liệu phát sinh, trách nhiệm các bên trong giao dịch và cơ chế giải quyết tranh chấp. Pháp luật về giao dịch dữ liệu cũng cần điều chỉnh các nền tảng trung gian dữ liệu, như sàn dữ liệu, trung tâm môi giới dữ liệu, trong đó bảo đảm tính minh bạch, công bằng và quyền lợi của các bên liên quan, đặc biệt là người tiêu dùng và doanh nghiệp nhỏ.

Cần đẩy mạnh công tác phổ biến pháp luật về dữ liệu tới các cấp chính quyền, tổ chức, doanh nghiệp và người dân nhằm tạo sự đồng thuận xã hội, nâng cao ý thức tuân thủ và khuyến khích sáng tạo trong khai thác dữ liệu. Việc tuyên truyền cần sử dụng đa dạng phương thức, từ đào tạo chuyên sâu, hội thảo, diễn đàn, đến truyền thông số, các tài liệu phổ thông bằng hình ảnh, infographic dễ hiểu. Song song đó, cần thiết lập cơ chế phản biện xã hội, lấy ý kiến cộng đồng, chuyên gia, doanh nghiệp trong quá trình xây dựng và sửa đổi các văn bản pháp luật về dữ liệu, nhằm bảo đảm tính dân chủ, thực tiễn và bám sát nhu cầu thị trường.

Lực lượng Công an nhân dân có vai trò nòng cốt trong việc bảo vệ an ninh dữ liệu, điều tra, xử lý các hành vi vi phạm pháp luật về dữ liệu, đồng thời phối hợp xây dựng hệ thống pháp luật có khả năng phòng ngừa, răn đe và bảo vệ quyền lợi

của tổ chức, cá nhân. Nhiệm vụ của lực lượng Công an không chỉ dừng lại ở khâu giám sát, phát hiện, xử lý vi phạm mà còn phải tham gia trực tiếp vào quá trình xây dựng chính sách, hoàn thiện luật pháp liên quan đến định danh số, xác thực điện tử, an toàn thông tin, tội phạm mạng và giao dịch dữ liệu. Bên cạnh đó, Công an các đơn vị, địa phương cần đẩy mạnh công tác tuyên truyền, giáo dục pháp luật về dữ liệu cho người dân, doanh nghiệp, đặc biệt tại các khu vực trọng điểm kinh tế, vùng biên giới và địa bàn phức tạp về an ninh mạng. Việc phát hiện, điều tra, xử lý các vụ việc buôn bán, giả mạo, xâm phạm dữ liệu cần được tiến hành nghiêm minh, công khai, có tính răn đe và tạo niềm tin cho xã hội. Lực lượng Công an cũng cần làm chủ các công cụ kỹ thuật, công nghệ phục vụ công tác xác thực, bảo mật, phân tích dữ liệu, từng bước khẳng định vai trò trung tâm trong bảo vệ chủ quyền số quốc gia và an ninh dữ liệu quốc gia trong thời đại mới.

2. Tuyên truyền, phổ biến nhằm xây dựng thế trận An ninh Nhân dân trong công tác xây dựng, quản trị, quản lý, xử lý, bảo vệ dữ liệu

Đây là nhiệm vụ chuyển 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:

2.1. Nâng cao nhận thức toàn xã hội, đặc biệt là cộng đồng doanh nghiệp và các cơ quan hoạch định, thực thi chính sách về vai trò đặc biệt quan trọng của khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số đối với sự nghiệp phát triển đất nước

Nâng cao nhận thức toàn xã hội, đặc biệt là cộng đồng doanh nghiệp và các cơ quan hoạch định, thực thi chính sách về vai trò đặc biệt quan trọng của khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số là giải pháp mang tính nền tảng, xuyên suốt và có ý nghĩa quyết định đến thành công của tiến trình phát triển quốc gia. Trong bối cảnh toàn cầu đang bước vào cuộc cách mạng công nghiệp lần thứ tư, tri thức, công nghệ và dữ liệu đã trở thành những nguồn lực cốt lõi, thay thế cho các yếu tố truyền thống như lao động phổ thông hay tài nguyên thiên nhiên. Chính vì vậy, việc định hình lại tư duy phát triển, thúc đẩy nhận thức sâu sắc về khoa học – công nghệ không chỉ là một yêu cầu khách quan mà còn là một bước đi chiến lược nhằm mở rộng dư địa phát triển mới, gia tăng nội lực của nền kinh tế và bảo đảm vị thế quốc gia trên trường quốc tế.

Trung tâm dữ liệu quốc gia về dân cư. Ảnh: Sưu tầm

Để thực hiện mục tiêu trên, cần triển khai một loạt các hoạt động nhằm khơi dậy và bồi dưỡng tư duy tiếp cận khoa học – công nghệ cho mọi tầng lớp trong xã hội, đặc biệt là đội ngũ cán bộ lãnh đạo, quản lý trong các cơ quan hoạch định chính sách. Việc tăng cường tuyên truyền, giáo dục chính trị – tư tưởng về vai trò của đổi mới sáng tạo và chuyển đổi số phải được tích hợp vào các chương trình đào tạo, bồi dưỡng cán bộ công chức viên chức, đồng thời gắn liền với yêu cầu thực tiễn trong

quá trình hoạch định và tổ chức thực thi chính sách phát triển ngành, lĩnh vực và địa phương. Nhận thức của đội ngũ này có ý nghĩa then chốt bởi họ là lực lượng nắm giữ quyền lực thể chế, có khả năng tạo ra hoặc xóa bỏ những "nút thắt" trong quá trình cải cách và sáng tạo. Khi nhận thức thay đổi đúng hướng, họ sẽ đóng vai trò là những "kiến trúc sư thể chế", kiến tạo môi trường thuận lợi cho đổi mới sáng tạo nảy mầm và lan tỏa.

Cộng đồng doanh nghiệp cần được coi là trung tâm trong nỗ lực nâng cao nhận thức về vai trò của khoa học – công nghệ và chuyển đổi số. Đây là lực lượng trực tiếp quyết định mức độ đổi mới trong sản xuất – kinh doanh, cũng như khả năng hấp thụ, làm chủ công nghệ và ứng dụng dữ liệu lớn. Nhà nước cần thúc đẩy các cơ chế hỗ trợ doanh nghiệp tiếp cận thông tin, tri thức khoa học – công nghệ một cách nhanh chóng, minh bạch và hiệu quả. Đồng thời, phải thiết lập các hình thức liên kết bền vững giữa doanh nghiệp với các viện nghiên cứu, trường đại học, trung tâm đổi mới sáng tạo để lan tỏa tư duy công nghệ, kích thích tinh thần khởi nghiệp sáng tạo và nâng cao năng lực cạnh tranh. Một mặt, phải khuyến khích doanh nghiệp tự thân đầu tư nghiên cứu – phát triển (R&D), mặt khác, cần có các chính sách ưu đãi, hỗ trợ tài chính, thuế khóa cho các hoạt động đổi mới sáng tạo mang tính chất dẫn dắt thị trường. Việc tổ chức các chương trình truyền thông đại chúng, diễn đàn công nghệ, hội thảo chuyên đề cũng đóng vai trò quan trọng trong việc truyền tải thông điệp và kiến tạo không gian chia sẻ kinh nghiệm giữa các doanh nghiệp tiên phong và cộng đồng.

Trong lĩnh vực giáo dục và đào tạo, việc nâng cao nhận thức về vai trò của khoa học – công nghệ và chuyển đổi số cần được lồng ghép vào các chương trình giảng dạy chính quy ở mọi cấp học. Hệ thống giáo dục phải chuyển hướng từ truyền thụ kiến thức sang phát triển năng lực tư duy sáng tạo, khả năng giải quyết vấn đề, khai thác dữ liệu và ứng dụng công nghệ. Trường học không chỉ là nơi tiếp nhận kiến thức mà còn phải trở thành "vườn ươm" cho các ý tưởng sáng tạo và tư duy khoa

học. Cần đặc biệt quan tâm đến việc bồi dưỡng năng lực số cho học sinh – sinh viên, xây dựng kỹ năng học tập suốt đời và tiếp cận công nghệ một cách an toàn, nhân văn. Ngoài ra, giáo dục cộng đồng và truyền thông đại chúng về chuyển đổi số cũng cần được thúc đẩy mạnh mẽ. Truyền thông số, mạng xã hội, các nền tảng trực tuyến cần được sử dụng như công cụ lan tỏa nhận thức, phổ biến kiến thức và thúc đẩy sự tham gia tích cực của người dân vào quá trình chuyển đổi số quốc gia.

Đối với các cơ quan quản lý nhà nước, cần xác lập cơ chế trách nhiệm rõ ràng trong việc chủ động nâng cao trình độ khoa học – công nghệ, cập nhật xu hướng chuyển đổi số và ứng dụng dữ liệu lớn vào công tác quản lý, điều hành. Từng bộ, ngành, địa phương phải xác định rõ lộ trình chuyển đổi số nội bộ, coi dữ liệu và công nghệ là "tài sản chiến lược" trong xây dựng thể chế và phục vụ người dân, doanh nghiệp. Các sáng kiến chuyển đổi số cần được thiết kế theo hướng lấy người dân và doanh nghiệp làm trung tâm, lấy hiệu quả công khai, minh bạch làm thước đo. Đồng thời, phải phát huy vai trò của đội ngũ trí thức, chuyên gia, nhà khoa học trong việc tư vấn chính sách, phản biện và truyền cảm hứng cho quá trình đổi mới. Việc thiết lập các cơ chế khuyến khích, ghi nhận và tôn vinh đóng góp của lực lượng này sẽ góp phần xây dựng hệ sinh thái sáng tạo bền vững, lấy tri thức làm nền tảng cho phát triển.

Hệ thống chính trị và các tổ chức chính trị – xã hội cũng cần đồng hành tích cực trong việc nâng cao nhận thức toàn dân về vai trò của khoa học – công nghệ và chuyển đổi số. Đảng, Nhà nước và Mặt trận Tổ quốc Việt Nam cần phát huy vai trò định hướng dư luận xã hội, tổ chức các phong trào thi đua yêu nước gắn với sáng tạo và ứng dụng khoa học – công nghệ trong đời sống. Các tổ chức đoàn thể như Đoàn Thanh niên, Hội Phụ nữ, Hội Nông dân… cần chủ động triển khai các chương trình giáo dục, hướng dẫn cộng đồng, đặc biệt là ở vùng sâu vùng xa, vùng đồng bào dân tộc thiểu số tiếp cận công nghệ số,

khai thác dữ liệu, phát triển kinh tế số và nâng cao đời sống tinh thần. Việc kết hợp giữa truyền thống và hiện đại, giữa văn hóa dân tộc và tinh thần đổi mới sẽ tạo nên sức mạnh nội sinh giúp đất nước phát triển hài hòa, bền vững và tự cường.

Cùng với đó, việc xây dựng một hệ sinh thái truyền thông có trách nhiệm là rất cần thiết nhằm góp phần hình thành tư duy khoa học trong xã hội. Các cơ quan báo chí, truyền thông cần nâng cao năng lực chuyên môn, đổi mới cách thức truyền tải thông tin khoa học – công nghệ một cách sinh động, dễ hiểu, dễ tiếp cận. Cần khuyến khích sản xuất các chương trình truyền hình, podcast, video, infographic và bài viết chuyên sâu để lan tỏa tinh thần đổi mới sáng tạo trong xã hội, đồng thời phản bác kịp thời các luận điệu xuyên tạc, tiêu cực cản trở quá trình phát triển khoa học – công nghệ và chuyển đổi số. Vai trò của các nhà báo, KOLs, các nhà sáng tạo nội dung trên nền tảng số cần được phát huy như những "đại sứ tri thức" đưa thông điệp đổi mới đến gần hơn với công chúng, đặc biệt là thế hệ trẻ.

Nâng cao nhận thức về chuyển đổi số còn gắn liền với việc bảo đảm an toàn thông tin và xây dựng niềm tin số trong xã hội. Người dân, doanh nghiệp và các cơ quan nhà nước chỉ có thể chủ động tham gia vào quá trình chuyển đổi khi cảm thấy an tâm về tính bảo mật, minh bạch và công bằng trong môi trường số. Do đó, cần thúc đẩy các chiến dịch giáo dục kỹ năng số an toàn, tăng cường hiểu biết về quyền riêng tư dữ liệu, bảo vệ dữ liệu cá nhân và các hình thức phòng chống tội phạm mạng. Các cơ chế bảo vệ người dùng trên không gian số cần được phổ biến một cách rộng rãi, dễ hiểu, giúp nâng cao năng lực tự bảo vệ của người dân và doanh nghiệp, từ đó tạo nên niềm tin xã hội bền vững cho sự phát triển của nền kinh tế số.

Cuối cùng, trong bối cảnh tội phạm sử dụng công nghệ cao ngày càng tinh vi, phức tạp, nhiệm vụ nâng cao nhận thức về khoa học – công nghệ và chuyển đổi số đặt ra yêu cầu cấp thiết đối với lực lượng Công an nhân dân. Công an các đơn vị,

địa phương phải chủ động cập nhật xu hướng phát triển khoa học – công nghệ, đặc biệt là các công nghệ liên quan đến dữ liệu lớn, trí tuệ nhân tạo, blockchain, nhận dạng sinh trắc học, giám sát không gian mạng để nâng cao hiệu quả đấu tranh phòng, chống tội phạm và bảo vệ an ninh quốc gia trong môi trường số. Đồng thời, lực lượng Công an cần tích cực tuyên truyền, phổ biến kỹ năng số an toàn, giáo dục ý thức pháp luật số trong cộng đồng, nhất là học sinh, sinh viên, thanh niên, nhằm góp phần hình thành một xã hội số văn minh, an toàn và kỷ cương. Đây không chỉ là yêu cầu nghiệp vụ mà còn là trách nhiệm chính trị – xã hội của lực lượng Công an trong tiến trình hiện đại hóa đất nước dưới ánh sáng của khoa học, đổi mới và chuyển đổi số toàn diện.

Lực lượng Công an các cấp tiên phong đi đầu trong số hóa dữ liệu, hỗ trợ các bộ, ngành, địa phương xây dựng dữ liệu quốc gia, dữ liệu chuyên ngành

2.2. Củng cố quyết tâm chính trị, tạo sự thống nhất cao trong toàn hệ thống về chủ trương lấy khoa học - công nghệ và đổi mới sáng tạo làm động lực chủ yếu của phát triển

Củng cố quyết tâm chính trị và tạo sự thống nhất cao trong toàn hệ thống về chủ trương lấy khoa học, công nghệ và đổi mới sáng tạo làm động lực chủ yếu của phát triển là một định hướng mang tính nền tảng, định hình chiều sâu và tính bền vững

của quá trình hiện đại hóa đất nước. Điều này đòi hỏi sự thống nhất từ nhận thức đến hành động trong toàn bộ hệ thống chính trị, từ Trung ương đến địa phương, từ các cơ quan Đảng, chính quyền đến các tổ chức chính trị – xã hội, nhằm khẳng định vai trò trung tâm, then chốt của khoa học – công nghệ trong bối cảnh phát triển kinh tế số, xã hội số và chính phủ số. Việc củng cố quyết tâm chính trị không chỉ dừng lại ở tuyên truyền, mà phải được thể hiện bằng hành động cụ thể, bằng sự chỉ đạo quyết liệt, dứt khoát, tránh hình thức, chiếu lệ. Đặc biệt, người đứng đầu cấp ủy, chính quyền các cấp phải gương mẫu đi đầu, trực tiếp chỉ đạo, theo dõi và chịu trách nhiệm về kết quả thực hiện các nhiệm vụ liên quan đến khoa học – công nghệ và đổi mới sáng tạo tại cơ quan, đơn vị mình phụ trách.

Cần đổi mới toàn diện phương thức chỉ đạo, điều hành công cuộc phát triển khoa học – công nghệ, trong đó trọng tâm là xây dựng các chiến lược phát triển tầm quốc gia, gắn với tầm nhìn dài hạn và định hướng đến từng lĩnh vực cụ thể. Việc lồng ghép các mục tiêu đổi mới sáng tạo vào kế hoạch phát triển kinh tế – xã hội hàng năm, 5 năm, các chương trình mục tiêu quốc gia, các chiến lược ngành, vùng và địa phương sẽ giúp gia tăng hiệu quả triển khai thực tiễn. Hệ thống cơ chế chính sách cũng cần đồng bộ, thông suốt, giảm tối đa các rào cản thể chế, hành chính cản trở đổi mới sáng tạo. Việc ban hành các nghị quyết, chỉ thị, quyết định mang tính đột phá của Trung ương về thúc đẩy khoa học – công nghệ, xây dựng nền kinh tế tri thức cần được triển khai đi đôi với công tác giám sát, kiểm tra, sơ kết, tổng kết để kịp thời điều chỉnh, bổ sung, hoàn thiện.

Phải làm cho toàn thể cán bộ, đảng viên, công chức, viên chức và người dân nhận thức rõ ràng rằng khoa học – công nghệ không phải là lĩnh vực hàn lâm, xa rời thực tiễn mà là công cụ mạnh mẽ để giải quyết các bài toán của cuộc sống, nâng

cao chất lượng điều hành, tối ưu hóa nguồn lực, tăng năng suất lao động, tạo ra giá trị gia tăng và năng lực cạnh tranh quốc gia. Từ nhận thức đó, cần tạo ra phong trào thi đua nghiên cứu, sáng tạo, ứng dụng khoa học – công nghệ trong mọi lĩnh vực, khơi dậy tinh thần đổi mới từ trong từng cơ quan, tổ chức, doanh nghiệp đến cộng đồng. Mỗi cán bộ, đảng viên phải là hạt nhân lan tỏa tư duy khoa học, tinh thần đổi mới, sẵn sàng học hỏi, tiếp cận cái mới, chấp nhận cái khác biệt, hướng tới cái hiệu quả và bền vững. Cần xây dựng văn hóa đổi mới sáng tạo, đề cao vai trò cá nhân dám nghĩ, dám làm, dám chịu trách nhiệm, trong khi thiết lập hệ thống đánh giá, khen thưởng minh bạch, công bằng để thúc đẩy động lực nội tại.

Bên cạnh quyết tâm chính trị, cần thiết lập các cơ chế phối hợp liên ngành, liên cấp và liên vùng trong việc triển khai các chương trình đổi mới sáng tạo trọng điểm. Việc hình thành các trung tâm điều phối chiến lược đổi mới sáng tạo cấp quốc gia có vai trò kết nối các chủ thể nhà nước – doanh nghiệp – viện nghiên cứu – trường đại học sẽ tạo thành hệ sinh thái tri thức gắn kết chặt chẽ, từ đó rút ngắn chu trình nghiên cứu – thử nghiệm – thương mại hóa – mở rộng quy mô. Các cơ chế hợp tác công – tư trong lĩnh vực khoa học – công nghệ cần được xây dựng theo hướng rõ ràng, bình đẳng, minh bạch, đảm bảo hài hòa lợi ích nhà nước và lợi ích của doanh nghiệp, nhà đầu tư. Việc trao quyền nhiều hơn cho các tổ chức khoa học công lập, đồng thời thúc đẩy sự tham gia của khu vực tư nhân vào nghiên cứu ứng dụng và đổi mới sáng tạo là yêu cầu tất yếu.

Cần huy động và phân bổ nguồn lực một cách hợp lý, hiệu quả để hiện thực hóa chủ trương phát triển khoa học – công nghệ và đổi mới sáng tạo. Ngân sách nhà nước cần đóng vai trò "vốn mồi" để kích hoạt các dòng vốn xã hội đầu tư vào lĩnh vực này, đặc biệt là thông qua các quỹ phát triển khoa học – công nghệ ở các cấp, các chương trình quốc gia về đổi mới công nghệ, phát triển sản phẩm quốc gia, vườn ươm sáng tạo, hỗ trợ khởi nghiệp sáng tạo. Hệ thống tài chính –

tín dụng cần được cải cách để phục vụ đặc thù đầu tư dài hạn, rủi ro cao của khoa học – công nghệ. Các chính sách thuế, ưu đãi đất đai, hạ tầng, cơ chế chia sẻ lợi ích cần được hoàn thiện theo hướng tạo môi trường thuận lợi nhất để doanh nghiệp và tổ chức khoa học đầu tư mạnh vào R&D, chuyển giao công nghệ, nâng cấp dây chuyền sản xuất, phát triển sản phẩm mới, công nghệ lõi.

Nguồn nhân lực là yếu tố quyết định thành công của mọi chiến lược phát triển khoa học – công nghệ. Cần có chính sách thu hút, đãi ngộ, tôn vinh nhân tài, đặc biệt là các chuyên gia giỏi trong và ngoài nước, nhà khoa học trẻ, doanh nhân công nghệ, kỹ sư đổi mới sáng tạo. Hệ thống giáo dục đại học và dạy nghề phải được cải tổ mạnh mẽ theo hướng gắn đào tạo với thực tiễn sản xuất, nghiên cứu và ứng dụng, khuyến khích đào tạo đa ngành, liên ngành, song hành cùng kỹ năng số và tư duy sáng tạo. Các cơ chế học tập suốt đời, học tập mở, đào tạo lại và nâng cao kỹ năng cũng cần được chú trọng để đảm bảo người lao động không bị tụt hậu trong kỷ nguyên công nghệ thay đổi nhanh chóng. Việc phát triển đội ngũ trí thức gắn liền với môi trường học thuật dân chủ, sáng tạo, không bị ràng buộc bởi hành chính hóa, đồng thời có đủ điều kiện vật chất và tài chính để tập trung nghiên cứu chuyên sâu, dài hạn.

Việc truyền thông, giáo dục và nâng cao nhận thức cộng đồng về tầm quan trọng của khoa học – công nghệ và đổi mới sáng tạo là nhiệm vụ xuyên suốt, cần được tổ chức thành các chiến dịch thường kỳ và chuyên đề, lồng ghép trong hệ thống giáo dục phổ thông và đại học, đồng thời được phát huy qua các phương tiện truyền thông đại chúng, mạng xã hội, nền tảng số. Phải làm cho đổi mới sáng tạo trở thành một giá trị xã hội, một tiêu chuẩn đánh giá năng lực tổ chức và cá nhân, một biểu tượng của sự phát triển tiến bộ, bền vững. Hình ảnh quốc gia khởi nghiệp, quốc gia đổi mới sáng tạo, quốc gia công nghệ cần

được định hình rõ trong tư duy công chúng, truyền cảm hứng cho thế hệ trẻ và định hướng sự tham gia tích cực của người dân vào các tiến trình phát triển khoa học – công nghệ.

Cần thiết lập hệ thống chỉ số đánh giá mức độ đổi mới sáng tạo và hiệu quả ứng dụng khoa học – công nghệ ở từng bộ, ngành, địa phương, đơn vị. Việc đưa các chỉ số này vào đánh giá kết quả thực hiện nhiệm vụ của người đứng đầu, vào tiêu chí xếp hạng cơ quan hành chính, đánh giá chất lượng phát triển doanh nghiệp công nghệ sẽ tạo áp lực tích cực thúc đẩy hành động cụ thể. Các chỉ số cần đo lường cả đầu vào (nguồn lực), quá trình (cơ chế, tổ chức) và đầu ra (sản phẩm, tác động thực tế), đặc biệt chú trọng yếu tố chuyển đổi công nghệ và năng lực hấp thụ công nghệ mới. Hệ thống đánh giá phải được công bố định kỳ, công khai, minh bạch, có thể so sánh và liên thông với các chỉ số quốc tế để đảm bảo sự tiến bộ thực chất, không hình thức.

Thiếu tướng Nguyễn Ngọc Cương trình bày báo cáo về các "điểm nghẽn" trong quá trình triển khai Trung tâm Dữ liệu quốc gia. Ảnh minh họa. Nguồn từ Internet.

Từ góc độ lực lượng Công an nhân dân, việc củng cố quyết tâm chính trị, tạo sự thống nhất trong chủ trương phát triển khoa học – công nghệ và đổi mới sáng tạo có ý nghĩa đặc biệt quan trọng nhằm nâng cao năng lực bảo đảm an ninh, trật tự trong bối cảnh mới. Công an các đơn vị, địa phương cần tiên phong trong ứng dụng các thành tựu công nghệ hiện đại vào

công tác nghiệp vụ như phân tích dữ liệu lớn, trí tuệ nhân tạo trong điều tra tội phạm, sử dụng camera thông minh và hệ thống giám sát đô thị, triển khai mô hình cảnh sát số, bản đồ số tội phạm, điều tra số, nhận dạng khuôn mặt, phân tích giọng nói, điều hành an ninh trên nền tảng điện toán đám mây. Đồng thời cần chủ động nghiên cứu, chế tạo và làm chủ các công cụ, thiết bị kỹ thuật chuyên dụng phục vụ đấu tranh phòng, chống tội phạm công nghệ cao, bảo vệ dữ liệu quốc gia, an ninh mạng, an toàn thông tin. Mỗi cán bộ chiến sĩ phải xác lập tinh thần đổi mới, học tập suốt đời, nắm bắt và làm chủ công nghệ để góp phần xây dựng lực lượng Công an hiện đại, chính quy, tinh nhuệ, từng bước đáp ứng yêu cầu bảo vệ an ninh quốc gia, giữ gìn trật tự an toàn xã hội trong thời đại số.

2.3. Thúc đẩy chia sẻ, mở dữ liệu giữa các cơ quan nhà nước, đặc biệt là dữ liệu hành chính công, nhằm phục vụ công dân, doanh nghiệp, nâng cao tính minh bạch và hiệu quả điều hành

Thúc đẩy chia sẻ và mở dữ liệu giữa các cơ quan nhà nước là một yêu cầu tất yếu trong tiến trình chuyển đổi số quốc gia, nhằm tạo lập một hệ sinh thái dữ liệu minh bạch, hiệu quả và lấy người dân, doanh nghiệp làm trung tâm phục vụ. Để triển khai giải pháp này, trước hết cần hoàn thiện khuôn khổ pháp lý, cơ chế, chính sách về chia sẻ và mở dữ liệu giữa các cơ quan nhà nước theo hướng thống nhất, đồng bộ, rõ ràng về trách nhiệm, quyền hạn, tiêu chuẩn kỹ thuật, bảo mật và kiểm soát truy cập. Việc sửa đổi, bổ sung các văn bản quy phạm pháp luật cần bảo đảm quy định cụ thể về việc mở dữ liệu công, đặc biệt là dữ liệu hành chính công, bao gồm thông tin về đất đai, xây dựng, đăng ký doanh nghiệp, đầu tư, giáo dục, y tế, bảo hiểm xã hội, thuế và hải quan, từ đó tạo nền tảng pháp lý vững chắc để các cơ quan nhà nước thực hiện đầy đủ nghĩa vụ chia sẻ dữ liệu theo lộ trình rõ ràng và minh bạch.

Cùng với đó, cần xây dựng hệ thống tiêu chuẩn quốc gia, quy chuẩn kỹ thuật và mô hình dữ liệu thống nhất phục vụ kết nối, chia sẻ và mở dữ liệu, giúp dữ liệu được liên thông, sử dụng được trên nhiều nền tảng và dễ dàng tích hợp vào các dịch vụ số cung cấp cho người dân, doanh nghiệp. Công tác chuẩn hóa dữ liệu không chỉ giới hạn ở mặt kỹ thuật như định dạng, cấu trúc, mà còn bao gồm cả việc phân loại, gắn nhãn dữ liệu, xác định mức độ mở, tần suất cập nhật và đơn vị chịu trách nhiệm duy trì dữ liệu. Đồng thời, các cơ quan cần xác định rõ danh mục dữ liệu bắt buộc phải chia sẻ, bắt buộc phải mở và dữ liệu được phép chia sẻ có điều kiện, làm căn cứ cho việc tổ chức triển khai và kiểm soát hoạt động chia sẻ, mở dữ liệu một cách hợp pháp, đúng mục tiêu, không gây lãng phí hoặc phát sinh rủi ro mất an toàn.

Việc xây dựng và vận hành hiệu quả các nền tảng tích hợp, chia sẻ dữ liệu quốc gia, nền tảng chia sẻ dữ liệu vùng, ngành và địa phương có vai trò trung tâm trong việc hiện thực hóa mục tiêu chia sẻ và mở dữ liệu. Các nền tảng này cần được đầu tư đồng bộ, hiện đại, bảo đảm khả năng xử lý dữ liệu lớn, tính tương thích cao và tích hợp được với các hệ thống thông tin của các bộ, ngành, địa phương, cơ quan chuyên môn, từ đó thiết lập mạng lưới dữ liệu liên thông, mở rộng khả năng phân tích, hỗ trợ ra quyết định chính sách dựa trên dữ liệu. Cần đặc biệt chú trọng xây dựng hạ tầng kỹ thuật hỗ trợ chia sẻ dữ liệu thời gian thực, bảo đảm khả năng tương tác linh hoạt và giảm độ trễ trong truyền tải thông tin giữa các cơ quan quản lý.

Nhiệm vụ cốt lõi là tổ chức lại toàn bộ quy trình thu thập, quản lý, xử lý và chia sẻ dữ liệu trong nội bộ từng cơ quan nhà nước theo hướng dữ liệu hóa, số hóa, tự động hóa và đặt mục tiêu phục vụ người dân, doanh nghiệp lên hàng đầu. Điều này đòi hỏi phải có sự thay đổi cả về tư duy quản lý lẫn mô hình tổ chức dữ liệu, hướng đến nguyên tắc "thu thập một lần – dùng nhiều lần", tránh tình trạng thu thập trùng lặp, lãng phí và gia tăng gánh nặng thủ tục cho người dân. Các cơ quan cần xây dựng các kho dữ liệu dùng chung, hệ thống cơ sở dữ liệu nội bộ liên thông theo quy chuẩn thống nhất và đảm bảo cập

nhật thường xuyên, chính xác, từ đó hình thành các "trung tâm tri thức" dữ liệu có thể dễ dàng chia sẻ, tái sử dụng cho các mục tiêu công vụ và phát triển kinh tế - xã hội.

Ảnh minh họa. Nguồn từ Internet

Việc phân cấp, phân quyền trong chia sẻ dữ liệu cần rõ ràng, gắn liền với trách nhiệm cụ thể của từng đơn vị trong việc cung cấp, cập nhật, bảo mật và kiểm soát dữ liệu. Cơ chế giám sát, kiểm tra, đánh giá việc chia sẻ và mở dữ liệu phải được thiết lập minh bạch, có chế tài xử lý nghiêm đối với các hành vi từ chối chia sẻ, gây khó khăn trong tiếp cận hoặc làm sai lệch

dữ liệu. Cần phát triển hệ thống báo cáo, thống kê dữ liệu chia sẻ và mở dữ liệu giữa các cơ quan nhằm thúc đẩy tính minh bạch, công khai và nâng cao trách nhiệm giải trình trong quản lý công. Ngoài ra, các cơ quan nhà nước cần chủ động rà soát lại hiện trạng dữ liệu đang quản lý, phân loại, làm sạch, chuẩn hóa, đối chiếu với các tiêu chuẩn mở quốc tế và công bố lộ trình mở dữ liệu từng bước cho người dân và cộng đồng doanh nghiệp tiếp cận, khai thác và phát triển các sản phẩm dịch vụ trên nền dữ liệu công.

Nguồn lực triển khai chia sẻ và mở dữ liệu phải được ưu tiên phân bổ trong kế hoạch tài chính – ngân sách nhà nước, nhất là cho các nhiệm vụ hạ tầng kỹ thuật, nhân lực và bảo mật. Cần thiết lập cơ chế tài chính phù hợp để khuyến khích các bộ, ngành, địa phương chủ động mở dữ liệu theo lộ trình định sẵn, đồng thời cho phép khai thác dữ liệu công một cách hợp pháp, hợp lý, có thu phí đối với các hình thức tái sử dụng dữ liệu phục vụ mục đích thương mại nhưng vẫn bảo đảm quyền tiếp cận dữ liệu cơ bản cho người dân. Hợp tác công tư trong việc xây dựng nền tảng công nghệ mở, lưu trữ dữ liệu và vận hành hệ sinh thái số cũng cần được thúc đẩy để huy động các nguồn lực xã hội cùng tham gia phát triển dữ liệu công, tránh phụ thuộc vào một số nhà cung cấp công nghệ độc quyền, từ đó giảm chi phí vận hành và tăng tính bền vững của hệ thống dữ liệu mở.

Nâng cao năng lực cán bộ, công chức trong việc thu thập, chuẩn hóa, phân tích và chia sẻ dữ liệu là yếu tố then chốt để triển khai hiệu quả giải pháp chia sẻ và mở dữ liệu. Cần tổ chức đào tạo bài bản về kỹ năng quản trị dữ liệu, phân tích dữ liệu, đảm bảo an toàn thông tin, xây dựng API chia sẻ dữ liệu và ứng dụng các công nghệ mới như trí tuệ nhân tạo, học máy, blockchain trong quản lý và khai thác dữ liệu. Đồng thời, cần nâng cao nhận thức và trách nhiệm của người đứng đầu các cơ quan nhà nước về vai trò của dữ liệu trong chỉ đạo, điều hành, minh bạch hóa hoạt động quản lý và cải thiện chất lượng dịch

vụ công. Cần phát động các phong trào thi đua, sáng kiến chia sẻ dữ liệu điển hình, lấy đó làm tiêu chí đánh giá mức độ chuyển đổi số trong các cơ quan hành chính nhà nước.

Việc đảm bảo an toàn, bảo mật và quyền riêng tư dữ liệu trong quá trình chia sẻ và mở dữ liệu là điều kiện bắt buộc. Cần xây dựng hệ thống công nghệ và quy trình kỹ thuật kiểm soát quyền truy cập, mã hóa, xác thực, giám sát dữ liệu theo thời gian thực và phát hiện sớm các hành vi xâm nhập, rò rỉ, đánh cắp dữ liệu. Việc mở dữ liệu hành chính công phải được thực hiện theo nguyên tắc "mở có kiểm soát", đảm bảo không làm lộ lọt các thông tin cá nhân, bí mật nhà nước hoặc dữ liệu thuộc phạm vi bảo vệ đặc biệt. Ngoài ra, cần thiết lập cơ chế phản hồi và xử lý kiến nghị của người dân, doanh nghiệp liên quan đến sai sót hoặc sử dụng sai mục đích dữ liệu, qua đó nâng cao niềm tin vào hệ thống dữ liệu công.

Cần khuyến khích các sáng kiến xã hội, các mô hình cộng đồng khai thác và phát triển ứng dụng trên nền dữ liệu mở, như xây dựng bản đồ tương tác, cổng dịch vụ công mở, hệ thống phản ánh hiện trường, đánh giá dịch vụ hành chính công, nhằm lan tỏa văn hóa sử dụng dữ liệu, thúc đẩy đổi mới sáng tạo, cải thiện chất lượng chính sách, quản lý đô thị, y tế, giáo dục và các dịch vụ khác phục vụ đời sống người dân. Hệ sinh thái dữ liệu mở sẽ tạo điều kiện cho các doanh nghiệp khởi nghiệp, doanh nghiệp nhỏ và vừa tiếp cận nguồn tài nguyên số quý giá để xây dựng sản phẩm, dịch vụ mới, giảm chi phí nghiên cứu thị trường, rút ngắn thời gian triển khai, tăng năng lực cạnh tranh và thúc đẩy phát triển kinh tế số quốc gia.

Để thúc đẩy chia sẻ, mở dữ liệu hành chính công một cách hiệu quả và đồng bộ, cần xây dựng hệ thống đánh giá, xếp hạng mức độ chia sẻ và mở dữ liệu của các cơ quan nhà nước, lấy đó làm tiêu chí trong chấm điểm chuyển đổi số, đánh giá thi đua, khen thưởng và quy hoạch, bổ nhiệm cán bộ quản lý. Các chỉ số đánh giá cần bao gồm tỷ lệ dữ liệu được mở công

khai, tần suất cập nhật, mức độ tương tác với người dùng, tính đầy đủ, chính xác và khả năng tái sử dụng dữ liệu. Ngoài ra, có thể thiết lập các cổng dữ liệu mở quốc gia với công cụ phân tích, truy vấn nâng cao, bản đồ dữ liệu và giao diện thân thiện với người dùng, tạo điều kiện thuận lợi nhất cho việc khai thác dữ liệu từ mọi đối tượng xã hội.

Trong phạm vi chức năng, nhiệm vụ của lực lượng Công an nhân dân, việc thúc đẩy chia sẻ, mở dữ liệu giữa các cơ quan nhà nước có ý nghĩa quan trọng nhằm phục vụ công tác bảo vệ an ninh quốc gia, giữ gìn trật tự, an toàn xã hội và phòng chống tội phạm. Thông qua kết nối, chia sẻ dữ liệu hành chính công, đặc biệt là dữ liệu về căn cước công dân, đăng ký cư trú, phương tiện, doanh nghiệp, y tế, giáo dục, xuất nhập cảnh và giao dịch tài chính, lực lượng Công an có thể nâng cao khả năng phân tích, giám sát, phát hiện sớm các nguy cơ vi phạm pháp luật, truy vết tội phạm, đồng thời rút ngắn thời gian xử lý hồ sơ hành chính cho người dân và doanh nghiệp. Việc ứng dụng dữ liệu mở trong xây dựng bản đồ an ninh, dự báo điểm nóng tội phạm, phân tích hành vi trên không gian mạng, điều tra các vụ án kinh tế – công nghệ cao cũng tạo ra lợi thế vượt trội trong triển khai nhiệm vụ bảo đảm an ninh dữ liệu quốc gia và giữ gìn trật tự xã hội trong kỷ nguyên số.

2.4. Bảo vệ quyền và lợi ích hợp pháp của chủ thể dữ liệu, nhất là dữ liệu cá nhân, thông qua việc thiết lập cơ chế thu hồi, phản đối, đồng ý sử dụng dữ liệu rõ ràng, minh bạch.

Việc bảo vệ quyền và lợi ích hợp pháp của chủ thể dữ liệu trong bối cảnh chuyển đổi số và phát triển kinh tế số không chỉ là một yêu cầu cấp thiết mang tính pháp lý mà còn là điều kiện tiên quyết nhằm xây dựng niềm tin xã hội, đảm bảo công bằng, minh bạch và phát triển bền vững. Để hiện thực hóa mục tiêu này, cần xây dựng khuôn khổ pháp lý đầy đủ, đồng bộ và có tính thực thi cao về bảo vệ dữ liệu cá nhân, làm cơ sở cho việc định danh quyền, nghĩa vụ và trách nhiệm của các chủ thể

liên quan. Các quy định này phải quy định rõ ràng về khái niệm dữ liệu cá nhân, phân loại dữ liệu theo mức độ nhạy cảm, từ đó thiết lập các mức độ bảo vệ khác nhau tương ứng với mức độ rủi ro của việc xử lý dữ liệu đó, đồng thời xác lập quyền cho người dân được kiểm soát, truy cập, chỉnh sửa, phản đối hoặc yêu cầu xóa dữ liệu liên quan đến bản thân mình.

Cơ chế thu thập dữ liệu phải đảm bảo tính tự nguyện, có sự đồng thuận rõ ràng và được thông tin đầy đủ từ phía chủ thể dữ liệu. Trong mọi hoạt động thu thập, sử dụng, chia sẻ dữ liệu cá nhân, bắt buộc phải công khai mục đích, phạm vi, thời hạn, phương thức sử dụng và các bên liên quan được phép truy cập hoặc nhận dữ liệu, nhằm đảm bảo tính minh bạch và tránh lạm dụng. Các mẫu biểu xin ý kiến đồng thuận cần được thiết kế thân thiện, dễ hiểu, không sử dụng thuật ngữ pháp lý phức tạp hay gây hiểu lầm, đồng thời phải có tính khả dụng trên các nền tảng số đa dạng, từ web đến ứng dụng di động. Trong trường hợp dữ liệu được chia sẻ cho bên thứ ba, chủ thể dữ liệu phải có quyền phản đối nếu cảm thấy không an toàn hoặc vượt quá phạm vi đã cho phép ban đầu. Mỗi người dân cần được trao quyền quyết định đối với dữ liệu của chính mình và điều này phải được pháp luật bảo vệ bằng những chế tài rõ ràng, cụ thể.

Việc thiết lập cơ chế đồng ý sử dụng dữ liệu cá nhân phải tuân thủ nguyên tắc rõ ràng, cụ thể và có thể thu hồi bất kỳ lúc nào. Cơ chế này cần được thiết kế theo mô hình "opt-in" – tức là chỉ được phép xử lý dữ liệu khi người dùng chủ động đồng ý sau khi đã nhận đủ thông tin cần thiết. Bên cạnh đó, cần xây dựng hệ thống quản lý đồng ý tập trung, nơi người dân có thể theo dõi, cập nhật, sửa đổi hoặc thu hồi các quyết định trước đây liên quan đến việc chia sẻ dữ liệu. Những thay đổi về quyết định sử dụng dữ liệu cần được thực hiện tức thời và phải có thông báo xác nhận rõ ràng gửi đến người dùng để đảm bảo quyền kiểm soát dữ liệu một cách hiệu quả. Đồng thời, các hệ thống này phải có tính tương thích cao với nhiều nền tảng công nghệ khác nhau, đảm bảo khả năng liên thông và chia sẻ dữ liệu nhưng vẫn giữ được quyền kiểm soát của cá nhân.

Đại tá TS Vũ Văn Tấn, Phó Cục trưởng Cục Cảnh sát Quản lý hành chính về trật tự xã hội phát biểu khai mạc hội thảo "Huy động nguồn lực nhân dân đồng hành xây dựng chiến lược Dữ liệu quốc gia, Dự thảo Luật dữ liệu

Hệ thống pháp luật cần thiết lập các cơ chế phản đối sử dụng dữ liệu trong những trường hợp cụ thể như dữ liệu bị sử dụng sai mục đích, vượt quá phạm vi cho phép, hoặc có dấu hiệu bị chia sẻ trái phép. Khi chủ thể dữ liệu gửi yêu cầu phản đối, hệ thống xử lý phải được thiết kế để tiếp nhận và phản hồi nhanh chóng, có quy trình xử lý minh bạch và có thể truy vết

từng bước để đảm bảo tính trách nhiệm. Đồng thời, các tổ chức, doanh nghiệp và cơ quan nhà nước phải có nghĩa vụ tiếp nhận, giải quyết và lưu trữ hồ sơ liên quan đến phản đối sử dụng dữ liệu, phục vụ công tác thanh tra, kiểm tra và giải trình khi có tranh chấp. Việc phản đối không được xem là yếu tố gây bất lợi hay ảnh hưởng tiêu cực đến quyền lợi hợp pháp của công dân trong việc tiếp cận các dịch vụ số, mà phải được tôn trọng và bảo vệ như một phần của quyền nhân thân.

Một nhiệm vụ quan trọng khác là xây dựng cơ chế thu hồi quyền sử dụng dữ liệu đã cho phép trước đó một cách đơn giản, thuận tiện và hiệu quả. Việc thu hồi phải được thực hiện ngay lập tức sau khi chủ thể dữ liệu đưa ra yêu cầu, đồng thời tổ chức xử lý dữ liệu có nghĩa vụ xóa toàn bộ thông tin liên quan khỏi hệ thống lưu trữ, trừ những trường hợp pháp luật cho phép lưu trữ để phục vụ mục đích an ninh quốc gia hoặc điều tra tội phạm. Cơ chế thu hồi phải được thiết kế dựa trên công nghệ hiện đại, đảm bảo tự động hóa và khả năng xác thực chủ thể yêu cầu, tránh trường hợp bị mạo danh hoặc xâm nhập trái phép. Các đơn vị cung cấp dịch vụ dữ liệu phải xây dựng quy trình nội bộ và hệ thống giám sát việc xử lý yêu cầu thu hồi, nhằm đảm bảo tính tuân thủ và tăng cường trách nhiệm giải trình.

Cần xây dựng và triển khai hệ thống giám sát, đánh giá và kiểm định định kỳ việc tuân thủ các quy định về bảo vệ dữ liệu cá nhân của các tổ chức, doanh nghiệp và cơ quan nhà nước. Các cơ quan có thẩm quyền cần thiết lập hệ thống thanh tra chuyên ngành về dữ liệu, có quyền yêu cầu cung cấp thông tin, kiểm tra quy trình xử lý dữ liệu, phát hiện hành vi vi phạm và xử lý nghiêm minh theo pháp luật. Các doanh nghiệp phải có trách nhiệm báo cáo định kỳ về việc xử lý dữ liệu cá nhân, đồng thời công bố chính sách bảo vệ dữ liệu công khai trên nền tảng dịch vụ số của mình. Những hành vi thu thập, lưu trữ, xử lý hoặc chia sẻ dữ liệu cá nhân mà không có sự đồng ý hoặc vi phạm quyền của chủ thể dữ liệu cần bị xử phạt nghiêm khắc, bao gồm cả trách nhiệm dân sự, hành chính và hình sự, tùy theo mức độ vi phạm.

Xây dựng năng lực cho đội ngũ cán bộ, công chức, viên chức và nhân sự trong doanh nghiệp liên quan đến việc xử lý dữ liệu cá nhân là một yêu cầu trọng yếu. Cần tổ chức đào tạo, tập huấn thường xuyên để nâng cao nhận thức pháp lý, kỹ năng kỹ thuật, phương pháp quản trị rủi ro và đạo đức nghề nghiệp trong việc xử lý dữ liệu. Các đơn vị cung cấp dịch vụ số, đặc biệt là các nền tảng công nghệ, phải có bộ phận chuyên trách về bảo vệ dữ liệu cá nhân, với đầy đủ công cụ hỗ trợ kỹ thuật như mã hóa, ẩn danh hóa, phát hiện xâm nhập, giám sát hoạt động xử lý và đánh giá lỗ hổng bảo mật. Đồng thời, cần khuyến khích sự tham gia của các tổ chức xã hội, cơ quan báo chí và người dân trong việc phát hiện, phản ánh các vi phạm về bảo vệ dữ liệu, nhằm hình thành hệ sinh thái quản trị dữ liệu toàn diện, minh bạch và hiệu quả.

Bên cạnh khung pháp lý, cần thúc đẩy phát triển các công cụ công nghệ số để hỗ trợ việc bảo vệ dữ liệu cá nhân. Việc ứng dụng trí tuệ nhân tạo, học máy và phân tích dữ liệu lớn cần được đặt trong giới hạn kiểm soát rõ ràng nhằm ngăn ngừa việc sử dụng dữ liệu vượt quá mục đích ban đầu. Các hệ thống xử lý dữ liệu cá nhân phải tích hợp sẵn các giải pháp bảo mật, kiểm soát truy cập, mã hóa đầu cuối, phân quyền người dùng và cảnh báo sớm khi có rủi ro rò rỉ. Ngoài ra, cần khuyến khích việc phát triển các giải pháp mã nguồn mở, cho phép cơ quan quản lý và cộng đồng đánh giá độ an toàn, minh bạch và khả năng tương thích với các tiêu chuẩn quốc tế.

Cần thúc đẩy truyền thông, nâng cao nhận thức của người dân về quyền được bảo vệ dữ liệu cá nhân, thông qua các chương trình giáo dục, truyền hình, ứng dụng tương tác, hội thảo và mạng xã hội. Mỗi công dân cần được trang bị kiến thức cơ bản về quyền dữ liệu cá nhân, cách kiểm soát quyền riêng tư trên các nền tảng số, nhận biết dấu hiệu bị xâm phạm dữ liệu và cách thức phản hồi, khiếu nại. Việc xây dựng "văn hóa dữ liệu" trong cộng đồng là yếu tố nền tảng để chủ thể dữ liệu thực

sự trở thành trung tâm của quá trình phát triển số, đồng thời tạo nên rào chắn xã hội tự nhiên trước các hành vi xâm phạm quyền riêng tư.

Việc hoàn thiện thể chế và xây dựng hệ sinh thái bảo vệ dữ liệu cá nhân cần gắn kết với chiến lược chuyển đổi số quốc gia, đảm bảo vừa phát triển công nghệ vừa tôn trọng và bảo vệ quyền công dân. Nhà nước cần đóng vai trò chủ đạo trong định hướng, điều phối và giám sát quá trình này, đồng thời tạo điều kiện cho sự tham gia của các chủ thể xã hội một cách hài hòa, bình đẳng. Bảo vệ dữ liệu cá nhân không phải là rào cản mà chính là động lực để thúc đẩy niềm tin số, từ đó thúc đẩy đổi mới sáng tạo, đầu tư và phát triển bền vững trong nền kinh tế số và xã hội số.

Đối với lực lượng Công an nhân dân, việc bảo vệ dữ liệu cá nhân gắn chặt với nhiệm vụ bảo đảm an ninh con người và an ninh mạng trong thời đại số. Công an là lực lượng nòng cốt trong phát hiện, điều tra và xử lý các hành vi xâm phạm dữ liệu cá nhân, tấn công mạng, đánh cắp thông tin nhạy cảm, giả mạo danh tính và sử dụng dữ liệu cá nhân vào mục đích phạm tội. Công an các đơn vị, địa phương cần đẩy mạnh triển khai các biện pháp nghiệp vụ, công nghệ và hợp tác quốc tế để phát hiện sớm các mối đe dọa, đồng thời tích cực tham gia xây dựng thể chế, hướng dẫn thực thi và tuyên truyền nâng cao ý thức người dân về bảo vệ dữ liệu. Công an nhân dân cũng phải là lực lượng tiên phong trong xây dựng hệ thống dữ liệu quốc gia an toàn, bảo mật, phục vụ công tác quản lý nhà nước, đảm bảo trật tự an toàn xã hội và đáp ứng yêu cầu của Chính phủ điện tử, Chính phủ số.

3. Quản lý, giám sát chủ động nhằm phòng ngừa, ngăn chặn các mối đe doạ an ninh dữ liệu

Đây là công tác nghiệp vụ cốt lõi, chuyển từ 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:

3.1. Phát triển hạ tầng dữ liệu quốc gia hiện đại, bảo mật cao, bao gồm trung tâm dữ liệu, nền tảng tích hợp – chia sẻ, sàn giao dịch dữ liệu, các hệ thống định danh số phục vụ kết nối liên thông.

Phát triển hạ tầng dữ liệu quốc gia hiện đại, bảo mật cao là nhiệm vụ trọng tâm trong quá trình xây dựng nền kinh tế số, xã hội số tại Việt Nam. Việc hình thành một hệ sinh thái dữ liệu bền vững không thể tách rời với việc đầu tư đồng bộ, bài bản vào các cấu phần hạ tầng kỹ thuật, bảo đảm tính kết nối liên thông, khả năng mở rộng và an toàn thông tin ở mức cao nhất. Trước hết, cần tiến hành xây dựng các trung tâm dữ liệu quốc gia đạt chuẩn quốc tế về khả năng lưu trữ, xử lý dữ liệu lớn, với các cụm máy chủ đặt tại nhiều địa điểm chiến lược trên lãnh thổ, bảo đảm tính sẵn sàng, độ dự phòng cao và khả năng phục hồi sau thảm họa. Trung tâm dữ liệu quốc gia không chỉ lưu trữ dữ liệu hành chính công mà còn cần được thiết kế linh hoạt để tiếp nhận, xử lý dữ liệu từ các lĩnh vực thiết yếu như y tế, giáo dục, giao thông, tài chính, an ninh quốc phòng.

Việc xây dựng các trung tâm dữ liệu cần đi đôi với triển khai hạ tầng kết nối tốc độ cao, bao gồm cả mạng truyền dẫn vật lý và hạ tầng điện toán đám mây. Cần ban hành tiêu chuẩn kỹ thuật về trung tâm dữ liệu, từ yêu cầu về cơ sở vật lý, kiểm soát nhiệt độ, độ ẩm, nguồn điện, hệ thống phòng cháy chữa cháy đến các tiêu chuẩn về phần mềm điều hành, tự động hóa và

bảo mật nội dung. Các tiêu chuẩn này cần phù hợp với thông lệ quốc tế để thúc đẩy việc công nhận, chia sẻ và hợp tác quốc tế trong lĩnh vực dữ liệu.

Song song với đó là nhiệm vụ xây dựng và vận hành hiệu quả các nền tảng tích hợp, chia sẻ dữ liệu giữa các bộ, ngành, địa phương. Hạ tầng tích hợp – chia sẻ cần được xem như xương sống kỹ thuật của toàn bộ nền hành chính số, giúp loại bỏ tình trạng cát cứ dữ liệu, tạo điều kiện cho việc đồng bộ hóa thông tin, tiết giảm chi phí hành chính và nâng cao năng suất lao động. Các nền tảng này cần áp dụng mô hình kiến trúc mở, cho phép mở rộng kết nối với các hệ thống quản lý ngành dọc cũng như kết nối với các hệ sinh thái dữ liệu từ khu vực tư nhân. Quá trình xây dựng nền tảng chia sẻ dữ liệu cần đi kèm cơ chế quản trị dữ liệu rõ ràng, phân quyền, kiểm soát truy cập chặt chẽ và theo dõi lịch sử truy cập nhằm phòng ngừa rò rỉ hoặc sử dụng sai mục đích.

Phát triển sàn giao dịch dữ liệu là bước đi chiến lược để thúc đẩy thị trường dữ liệu, biến dữ liệu thành tài sản số có giá trị kinh tế. Sàn giao dịch dữ liệu cần được tổ chức như một hạ tầng số trung lập, do Nhà nước bảo trợ, bảo đảm an toàn và tin cậy cho các hoạt động chào bán, đấu giá, mua bán, cấp phép sử dụng dữ liệu giữa các bên tham gia. Cần xây dựng cơ chế pháp lý chặt chẽ về quyền sở hữu dữ liệu, định giá dữ liệu, trách nhiệm trong bảo mật và sử dụng lại dữ liệu; đồng thời phát triển hệ thống định danh người dùng, đơn vị, tổ chức tham gia sàn giao dịch để bảo đảm truy vết, giải trình khi cần thiết. Các sàn dữ liệu không chỉ là nơi giao dịch mà còn cần có cơ chế kiểm định chất lượng, phân loại, chứng nhận nguồn gốc và hỗ trợ các công cụ phân tích dữ liệu.

Ảnh minh họa. Nguồn từ Internet

Hệ thống định danh số là yếu tố then chốt để bảo đảm liên thông dữ liệu và thực hiện các dịch vụ công trực tuyến, thương mại điện tử, thanh toán số một cách an toàn và thuận tiện. Hệ thống định danh điện tử cần được tích hợp vào mọi ứng dụng, dịch vụ số, đảm bảo mỗi cá nhân, tổ chức, thiết bị đều có mã định danh duy nhất, gắn với dữ liệu nhân thân và quyền hạn sử dụng dịch vụ. Việc triển khai định danh số cần đồng bộ với cơ sở dữ liệu dân cư, doanh nghiệp, phương tiện, tài sản,

bảo hiểm xã hội và y tế, tạo nền tảng pháp lý và kỹ thuật vững chắc để quản lý thông minh, phản ứng nhanh với các tình huống khẩn cấp. Cần đầu tư cho hệ thống xác thực mạnh, như xác thực hai yếu tố, sinh trắc học, chữ ký số, nhằm bảo đảm an toàn giao dịch và quyền riêng tư của người dùng.

Để đảm bảo tính bảo mật cao trong toàn bộ hạ tầng dữ liệu quốc gia, cần xây dựng chiến lược an toàn thông tin ở cấp độ quốc gia, trong đó có hệ thống cảnh báo sớm, giám sát an ninh mạng 24/7, phát hiện và phản ứng kịp thời với các nguy cơ tấn công mạng. Mỗi cấu phần của hạ tầng – từ trung tâm dữ liệu, nền tảng tích hợp, đến các sàn giao dịch và hệ thống định danh – đều phải được thiết kế theo nguyên tắc "an toàn theo thiết kế", có lớp bảo mật đa tầng, cập nhật định kỳ, kiểm thử thường xuyên. Cần thiết lập trung tâm điều hành an ninh mạng quốc gia với chức năng giám sát tập trung, thu thập và phân tích log hệ thống từ các đơn vị đầu mối, cảnh báo sớm, điều phối phản ứng trên toàn quốc. Đồng thời, phát triển lực lượng chuyên trách về an toàn dữ liệu, đào tạo chuyên sâu, tổ chức diễn tập định kỳ để nâng cao khả năng phòng thủ trước các hình thức tấn công mạng ngày càng tinh vi.

Bên cạnh hạ tầng kỹ thuật, cần hoàn thiện khung pháp lý điều chỉnh toàn bộ hoạt động trong hệ sinh thái dữ liệu, bảo đảm rõ ràng về quyền và nghĩa vụ của các bên, từ cơ quan nhà nước, doanh nghiệp, tổ chức đến công dân. Cần luật hóa các yêu cầu về tiêu chuẩn kỹ thuật, tiêu chuẩn bảo mật, thời gian lưu trữ, phân loại dữ liệu, trách nhiệm báo cáo và kiểm tra định kỳ. Các nghị định, thông tư hướng dẫn phải cụ thể hóa quy trình xử lý dữ liệu, cơ chế chia sẻ và mức độ truy cập giữa các hệ thống. Phải có quy định ràng buộc về việc đánh giá tác động của dữ liệu, giám sát an ninh mạng khi triển khai các hệ thống công nghệ thông tin mới trong bộ máy hành chính. Cơ quan quản lý dữ liệu nhà nước cần có quyền thanh tra, xử phạt và đình chỉ hoạt động của những đơn vị vi phạm quy định về vận hành và khai thác hạ tầng dữ liệu.

Song hành với hoàn thiện hạ tầng kỹ thuật và pháp lý là phát triển nguồn nhân lực chất lượng cao, phục vụ vận hành, bảo trì và khai thác hiệu quả hạ tầng dữ liệu quốc gia. Cần xây dựng chiến lược đào tạo về khoa học dữ liệu, an toàn thông tin, điện toán đám mây, quản trị cơ sở dữ liệu ở tất cả các bậc học. Tổ chức các chương trình hợp tác quốc tế, trao đổi học thuật, nghiên cứu chuyên sâu về bảo mật, chuẩn hóa dữ liệu và kinh tế dữ liệu. Đồng thời, thúc đẩy cộng đồng công nghệ mở, khuyến khích doanh nghiệp đổi mới sáng tạo, tham gia vào quá trình cung ứng hạ tầng, dịch vụ dữ liệu theo hình thức đối tác công – tư. Cần phát triển hệ sinh thái khởi nghiệp xoay quanh dữ liệu, tạo môi trường thuận lợi cho các startup công nghệ tham gia vào chuỗi giá trị dữ liệu quốc gia.

Để bảo đảm tính thống nhất trong triển khai, cần thiết lập cơ quan điều phối hạ tầng dữ liệu quốc gia trực thuộc Chính phủ hoặc Thủ tướng, có quyền điều hành xuyên suốt, phối hợp giữa các bộ, ngành, địa phương, tổ chức tư nhân và quốc tế. Cơ quan này cần ban hành kế hoạch đầu tư công trung hạn về dữ liệu, phân bổ ngân sách hiệu quả, theo dõi tiến độ xây dựng, giám sát chất lượng công trình và năng lực khai thác. Đồng thời, cần xây dựng chỉ số đánh giá hiệu quả sử dụng hạ tầng dữ liệu ở cấp bộ, ngành, địa phương, doanh nghiệp để làm cơ sở cho việc phân loại, xếp hạng, khen thưởng hoặc xử lý vi phạm. Cơ chế giám sát cộng đồng cũng cần được phát huy, thông qua báo chí, mạng xã hội, các tổ chức xã hội dân sự để bảo đảm tính minh bạch, hiệu quả và dân chủ hóa trong quản trị hạ tầng dữ liệu.

Ảnh minh hoạ

Với đặc thù là lực lượng nòng cốt bảo vệ an ninh quốc gia, lực lượng Công an nhân dân có trách nhiệm đặc biệt trong việc tham gia xây dựng và khai thác hạ tầng dữ liệu quốc gia hiện đại, bảo mật cao. Trước hết, cần chủ động tham mưu trong quá trình xây dựng tiêu chuẩn, quy chuẩn về an ninh dữ liệu, tích hợp an toàn mạng vào các cấu phần hạ tầng ngay từ giai đoạn thiết kế. Lực lượng Công an cần triển khai các hệ thống giám sát, phát hiện sớm hành vi xâm nhập trái phép, tấn công mạng nhằm vào hạ tầng dữ liệu trọng yếu, đồng thời phối hợp với các cơ quan chuyên môn trong xử lý sự cố, điều tra tội phạm công nghệ cao. Cần đào tạo đội ngũ chuyên gia an ninh mạng có trình độ cao, thường xuyên cập nhật công nghệ mới, diễn tập ứng

phó tình huống phức tạp, đồng thời xây dựng hệ thống dữ liệu chuyên ngành Công an tích hợp liên thông với các nền tảng quốc gia, phục vụ hiệu quả cho công tác phòng ngừa, đấu tranh tội phạm, quản lý xã hội và bảo vệ chủ quyền số quốc gia.

3.2. Tổ chức cấp phép, kiểm định chất lượng và giám sát hoạt động cung cấp dịch vụ dữ liệu, đặc biệt là các tổ chức trung gian dữ liệu, dịch vụ phân tích, lưu trữ, đấu giá, thương mại hóa dữ liệu.

Việc tổ chức cấp phép, kiểm định chất lượng và giám sát hoạt động cung cấp dịch vụ dữ liệu là nhiệm vụ quan trọng, góp phần xây dựng một hệ sinh thái dữ liệu minh bạch, tin cậy và an toàn, làm nền tảng thúc đẩy phát triển kinh tế số, xã hội số và chính phủ số. Để thực hiện hiệu quả nhiệm vụ này, cần thiết lập khuôn khổ pháp lý cụ thể, rõ ràng và có tính khả thi cao cho các hoạt động cấp phép, trong đó xác định rõ điều kiện, tiêu chuẩn, quy trình thẩm định và phê duyệt các tổ chức, doanh nghiệp tham gia cung cấp dịch vụ dữ liệu. Các điều kiện cấp phép cần bảo đảm yêu cầu về năng lực hạ tầng kỹ thuật, nhân sự chuyên môn, khả năng bảo mật và an toàn thông tin dữ liệu, cũng như nghĩa vụ cam kết thực hiện đúng các chuẩn mực về quản lý, xử lý và bảo vệ dữ liệu. Bên cạnh đó, phải phân loại rõ các loại hình dịch vụ dữ liệu như dịch vụ trung gian dữ liệu, dịch vụ phân tích dữ liệu, dịch vụ lưu trữ dữ liệu, dịch vụ đấu giá và thương mại hóa dữ liệu, để từ đó quy định các điều kiện cấp phép và nghĩa vụ giám sát phù hợp với từng loại hình.

Cần xây dựng hệ thống kiểm định chất lượng dịch vụ dữ liệu theo hướng khoa học, khách quan, độc lập, lấy tiêu chuẩn quốc gia và quốc tế làm căn cứ đánh giá, đồng thời tăng cường ứng dụng công nghệ hiện đại vào quy trình kiểm định nhằm bảo đảm hiệu lực, hiệu quả và tiết kiệm nguồn lực. Công tác kiểm định phải được tiến hành định kỳ và đột xuất, gắn liền với trách nhiệm giải trình của đơn vị cung cấp dịch vụ và nghĩa vụ công khai kết quả kiểm định để người sử dụng có thông tin

lựa chọn, đồng thời tạo động lực để các đơn vị nâng cao chất lượng dịch vụ. Ngoài ra, cần thiết lập cơ chế phản hồi và tiếp nhận khiếu nại của người sử dụng dịch vụ dữ liệu để làm cơ sở cải tiến hoạt động kiểm định, đồng thời xử lý kịp thời các sai phạm. Tăng cường đào tạo, bồi dưỡng đội ngũ cán bộ làm công tác kiểm định về nghiệp vụ, đạo đức nghề nghiệp và khả năng tiếp cận công nghệ, đảm bảo tính chuyên nghiệp, minh bạch và tránh xung đột lợi ích trong quá trình thực hiện nhiệm vụ.

Hội thảo lấy ý kiến đối với các văn bản quy phạm pháp luật quy định chi tiết, hướng dẫn thi hành Luật Dữ liệu đã đạt mục

tiêu, yêu cầu đã đề ra. Ảnh minh họa. Nguồn từ Internet.

Triển khai hoạt động giám sát thường xuyên đối với các tổ chức cung cấp dịch vụ dữ liệu, đặc biệt là tổ chức trung gian dữ liệu – nơi giữ vai trò kết nối giữa các chủ thể dữ liệu và bên sử dụng dữ liệu, có khả năng tác động đến quyền riêng tư và lợi ích hợp pháp của người dân, doanh nghiệp. Hệ thống giám sát cần có tính liên tục, tự động và tích hợp cơ chế cảnh báo sớm các hành vi vi phạm như thu thập dữ liệu trái phép, chuyển nhượng dữ liệu không có sự đồng ý của chủ thể, sử dụng dữ liệu để thao túng thị trường hoặc phục vụ mục đích phi pháp. Cần thiết lập hệ thống báo cáo điện tử để các đơn vị cung cấp dịch vụ dữ liệu định kỳ báo cáo các chỉ số hoạt động và việc tuân thủ quy định pháp luật, từ đó cơ quan quản lý có cơ sở phân tích, đối chiếu, phát hiện dấu hiệu bất thường để kịp thời can thiệp. Đồng thời, cần hoàn thiện hệ thống quy chuẩn kỹ thuật, tiêu chuẩn dữ liệu và khung đạo đức nghề nghiệp trong lĩnh vực dữ liệu nhằm nâng cao năng lực giám sát, khắc phục tình trạng hoạt động "xám" của các đơn vị chưa được cấp phép hoặc lợi dụng kẽ hở pháp luật để trục lợi từ dữ liệu.

Tăng cường hợp tác giữa các cơ quan nhà nước, tổ chức nghề nghiệp, hiệp hội ngành nghề và khu vực tư nhân trong công tác kiểm tra, giám sát, đặc biệt với các dịch vụ dữ liệu xuyên biên giới, nhằm đối phó với các hành vi chuyển dữ liệu ra nước ngoài không kiểm soát, trốn tránh nghĩa vụ thuế, hoặc vi phạm chủ quyền số quốc gia. Cần ký kết các thỏa thuận hợp tác, chia sẻ thông tin về hoạt động cung cấp dịch vụ dữ liệu, thiết lập cơ chế phối hợp kiểm tra liên ngành, thanh tra chuyên đề để nâng cao hiệu quả quản lý nhà nước. Ngoài ra, nên khuyến khích các doanh nghiệp, tổ chức tự nguyện tham gia hệ thống chứng nhận tuân thủ các tiêu chuẩn đạo đức và bảo mật dữ liệu, làm cơ sở để cơ quan quản lý đánh giá mức độ tín nhiệm và áp dụng chính sách ưu đãi, hỗ trợ phát triển phù hợp.

Phát triển các công cụ và nền tảng số phục vụ công tác cấp phép, kiểm định và giám sát một cách thông minh, kết nối dữ liệu từ nhiều nguồn khác nhau nhằm phát hiện hành vi gian lận, vi phạm hoặc lỗ hổng trong hệ thống. Ứng dụng trí tuệ nhân tạo và công nghệ học máy để phân tích hành vi người dùng và hoạt động của đơn vị cung cấp dịch vụ, từ đó đưa ra cảnh báo rủi ro và đề xuất giải pháp điều chỉnh chính sách linh hoạt, phù hợp thực tiễn. Việc số hóa toàn bộ quy trình cấp phép và kiểm định còn giúp nâng cao tính minh bạch, giảm thủ tục hành chính, tạo điều kiện thuận lợi cho doanh nghiệp nhưng vẫn giữ vững nguyên tắc bảo vệ dữ liệu. Cần đặc biệt lưu ý bảo mật các hệ thống quản lý giấy phép và cơ sở dữ liệu liên quan đến hoạt động giám sát để tránh nguy cơ bị tấn công mạng hoặc thao túng thông tin phục vụ mục đích xấu.

Nâng cao nhận thức xã hội về vai trò của dịch vụ dữ liệu và trách nhiệm của các bên liên quan trong hệ sinh thái dữ liệu quốc gia. Tổ chức truyền thông, tập huấn và phổ biến kiến thức pháp luật về dữ liệu đến các tổ chức cung cấp dịch vụ, người sử dụng và cộng đồng nói chung, nhấn mạnh quyền và nghĩa vụ pháp lý khi tham gia vào hoạt động cung cấp hoặc khai thác dữ liệu. Cần lồng ghép nội dung quản trị dữ liệu, bảo vệ thông tin cá nhân và đạo đức số vào chương trình đào tạo của các trường đại học, viện nghiên cứu để hình thành nguồn nhân lực chất lượng cao, có ý thức tuân thủ pháp luật và sẵn sàng tham gia quản lý dịch vụ dữ liệu theo hướng chuyên nghiệp, hiệu quả.

Đối với các tổ chức cung cấp dịch vụ phân tích dữ liệu, phải yêu cầu có phương án quản lý vòng đời dữ liệu rõ ràng, bảo đảm không lưu trữ, xử lý dữ liệu quá thời hạn quy định, tránh tình trạng lạm dụng dữ liệu cho các mục đích ngoài phạm vi cho phép. Việc phân tích dữ liệu, đặc biệt là dữ liệu lớn và dữ liệu hành vi người dùng, cần có cơ chế thẩm định mục đích sử dụng, đánh giá tác động và rủi ro đạo đức, nhất là khi áp dụng các thuật toán tự động hóa có khả năng tạo ra định kiến hoặc sai lệch trong kết quả phân tích. Do đó, cơ quan quản lý nhà nước cần thiết lập hội đồng thẩm định chuyên môn, phối hợp

cùng các viện nghiên cứu độc lập để đánh giá, giám sát các dịch vụ phân tích dữ liệu mang tính ảnh hưởng lớn, có nguy cơ gây tổn hại cho cộng đồng hoặc thao túng hành vi người tiêu dùng.

Đối với dịch vụ lưu trữ dữ liệu, cần phân hạng rõ ràng các cấp độ bảo mật, quy định yêu cầu tối thiểu đối với từng mức độ lưu trữ, nhất là dữ liệu nhạy cảm, dữ liệu cá nhân, dữ liệu trọng yếu của nhà nước. Việc cấp phép cho các đơn vị lưu trữ phải đi kèm kiểm tra thực địa, đánh giá năng lực vận hành trung tâm dữ liệu, các biện pháp phòng cháy chữa cháy, an ninh vật lý và an toàn thông tin. Bên cạnh đó, phải quy định rõ trách nhiệm lưu trữ dự phòng, phục hồi dữ liệu khi có sự cố và nghĩa vụ báo cáo kịp thời các rủi ro mất an toàn dữ liệu cho cơ quan chức năng. Cần quy định cơ chế xử phạt nghiêm khắc đối với hành vi lưu trữ dữ liệu không được phép, cố tình giấu giếm vi phạm hoặc hợp tác với bên thứ ba không rõ ràng trong hoạt động lưu trữ.

Hoạt động đấu giá và thương mại hóa dữ liệu phải được kiểm soát chặt chẽ, tránh để hình thành thị trường dữ liệu phi chính thức, tạo ra bất bình đẳng tiếp cận thông tin hoặc lạm dụng dữ liệu để chi phối thị trường. Việc tổ chức đấu giá dữ liệu cần minh bạch, có cơ sở pháp lý vững chắc và đảm bảo quyền lợi của chủ thể dữ liệu. Cần yêu cầu các đơn vị tham gia đấu giá phải được cấp phép và có phương án sử dụng dữ liệu sau đấu giá, được thẩm định và công khai. Tăng cường vai trò của cơ quan quản lý trong giám sát các giao dịch thương mại hóa dữ liệu, yêu cầu báo cáo định kỳ doanh thu, đối tác và sản phẩm dữ liệu cung cấp, từ đó phát hiện và ngăn chặn kịp thời các hành vi vi phạm như rửa tiền qua giao dịch dữ liệu, mua bán dữ liệu cá nhân trái phép hoặc tiết lộ dữ liệu bí mật nhà nước.

Lực lượng Công an nhân dân có vai trò then chốt trong việc bảo đảm an ninh dữ liệu và giám sát chặt chẽ các hoạt động cung cấp dịch vụ dữ liệu. Trên cơ sở chức năng được giao, lực lượng Công an cần chủ động phối hợp với các cơ quan chuyên môn kiểm tra định kỳ, đột xuất các đơn vị cung cấp dịch vụ dữ liệu để phát hiện, xử lý các hành vi xâm phạm an ninh quốc gia qua không gian mạng, buôn bán dữ liệu cá nhân, làm giả giấy phép hoạt động dữ liệu hoặc cố tình cung cấp sai lệch kết quả phân tích nhằm phục vụ mục đích xấu. Bên cạnh đó, cần xây dựng đội ngũ cán bộ kỹ thuật chuyên sâu về an ninh mạng và dữ liệu, có khả năng xử lý các tình huống phức tạp, đồng thời nâng cao năng lực dự báo, phát hiện sớm các nguy cơ từ hoạt động trung gian dữ liệu xuyên biên giới. Lực lượng Công an cũng cần tham mưu hoàn thiện khung pháp lý liên quan đến kiểm tra, xử lý vi phạm trong lĩnh vực dữ liệu, phối hợp chặt chẽ với các bộ, ngành, địa phương và quốc tế nhằm giữ vững chủ quyền dữ liệu quốc gia trong bối cảnh phát triển nhanh chóng của kinh tế số.

4. Quản lý phát triển thị trường dữ liệu

Dữ liệu với vai trò là tài nguyên quan trọng trong chuyển đổi số, là động lực phát triên các hoạt động khoa học, công nghệ và đổi mới sáng tạo, cần đẩy mạnh việc khai thác, sử dụng, phát huy giá trị kinh tế của dữ liệu. Do vậy, việc quản lý, phát triên thị trường dữ liệu là rất quan trọng; cần phải thiết lập cơ chế quản lý chặt chẽ, không đề 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:

4.1. Xây dựng kho dữ liệu tổng hợp quốc gia và kết nối với cơ sở dữ liệu chuyên ngành, bảo đảm chuẩn hóa, liên thông, phục vụ phân tích dữ liệu lớn và ra quyết định quản lý

Xây dựng kho dữ liệu tổng hợp quốc gia là một bước đi chiến lược nhằm hiện thực hóa tầm nhìn chuyển đổi số toàn diện trong quản lý nhà nước, phát triển kinh tế - xã hội và bảo đảm quốc phòng, an ninh. Trước tiên, cần rà soát toàn bộ các nguồn dữ liệu hiện có trong các cơ quan nhà nước ở trung ương và địa phương, phân loại rõ dữ liệu thuộc nhóm dữ liệu cơ bản, dữ liệu chuyên ngành, dữ liệu mở và dữ liệu dùng chung. Việc phân loại phải dựa trên giá trị sử dụng, tần suất cập nhật, mức độ nhạy cảm và vai trò trong hoạt động quản lý. Trên cơ sở đó, xây dựng kiến trúc tổng thể của kho dữ liệu tổng hợp quốc gia, bảo đảm khả năng tích hợp từ nhiều nguồn khác nhau, sử dụng các công nghệ mã nguồn mở, dữ liệu lớn (big data), điện toán đám mây và blockchain để tăng khả năng mở rộng và tính minh bạch.

Tiếp theo, cần thiết lập cơ chế khai thác dữ liệu thống nhất giữa các cơ quan nhà nước, bảo đảm quyền truy cập dữ liệu theo phân cấp, phân quyền, đúng mục đích, tránh lạm dụng hoặc xung đột lợi ích. Kho dữ liệu tổng hợp quốc gia phải đóng vai trò như một "trạm trung chuyển" dữ liệu, nơi dữ liệu được chuẩn hóa, xử lý, gắn định danh và đồng bộ theo các tiêu chuẩn kỹ thuật quốc gia. Việc kết nối với các cơ sở dữ liệu chuyên ngành như dân cư, đất đai, y tế, giáo dục, giao thông, tài chính – ngân hàng... phải được tiến hành đồng bộ thông qua hạ tầng tích hợp dữ liệu cấp quốc gia, bảo đảm độ chính xác, tính thời gian thực và khả năng phân tích chuyên sâu.

Một nhiệm vụ cấp bách khác là xây dựng bộ tiêu chuẩn kỹ thuật và quy chuẩn dữ liệu dùng chung cho toàn quốc, làm nền tảng cho việc liên thông, chia sẻ dữ liệu giữa các hệ thống khác nhau. Việc ban hành các tiêu chuẩn này cần được đặt dưới sự điều phối của một cơ quan trung tâm có năng lực kỹ thuật và quyền lực điều phối mạnh mẽ, có thể là Bộ Thông tin và Truyền thông hoặc Ủy ban Quốc gia về chuyển đổi số. Các tiêu chuẩn phải bao gồm cả định dạng dữ liệu, phương thức mã hóa, giao thức trao đổi, chính sách bảo mật và mô hình siêu dữ liệu. Cùng với đó là hệ thống hóa các danh mục dữ liệu

quốc gia, danh mục ngành nghề, danh mục địa bàn, danh mục tổ chức, mã số định danh để bảo đảm tính đồng bộ khi tích hợp dữ liệu từ nhiều nguồn.

Lực lượng Công an cơ sở hướng dẫn người dân khai thác dữ liệu đất đai để thực hiện thủ tục hành chính trong lĩnh vực cư trú.

Quá trình xây dựng kho dữ liệu tổng hợp quốc gia phải đi đôi với việc hiện đại hóa hạ tầng kỹ thuật, đặc biệt là các trung tâm dữ liệu quốc gia. Các trung tâm này phải đáp ứng các yêu cầu về bảo mật cấp cao, khả năng lưu trữ và xử lý dữ liệu lớn, khả năng phục hồi sau thảm họa và tính sẵn sàng cao. Đầu tư vào trung tâm dữ liệu không chỉ là đầu tư hạ tầng mà còn là đầu tư chiến lược về an ninh dữ liệu quốc gia, cần được lồng ghép trong các kế hoạch trung và dài hạn về phát triển công nghệ số. Ngoài ra, việc phát triển các nền tảng điện toán biên, điện toán đám mây phân tán, AI và học máy cần được tích hợp vào hệ sinh thái dữ liệu để tận dụng tối đa giá trị dữ liệu trong ra quyết định điều hành.

Để kho dữ liệu tổng hợp quốc gia thực sự phát huy hiệu quả, cần phát triển hệ sinh thái các dịch vụ dữ liệu, trong đó các cơ quan nhà nước đóng vai trò là nhà cung cấp – sử dụng dữ liệu đồng thời, các doanh nghiệp công nghệ số tham gia với tư cách là đơn vị trung gian phân tích, khai thác, cung cấp các công cụ hỗ trợ ra quyết định. Chính phủ cần tạo cơ chế khuyến khích khu vực tư nhân tham gia vào việc phân tích, xử lý dữ liệu trong khuôn khổ pháp luật cho phép, bảo đảm an toàn, bảo mật và không xâm phạm đến dữ liệu cá nhân, dữ liệu nhạy cảm của Nhà nước. Các công cụ phân tích dữ liệu lớn cần được tích hợp trực tiếp vào hệ thống chỉ đạo điều hành, giúp người đứng đầu các bộ, ngành, địa phương có thể nắm bắt nhanh xu hướng, phát hiện sớm nguy cơ, đưa ra quyết định kịp thời và hiệu quả.

Một trong những vấn đề quan trọng trong quá trình này là xây dựng cơ chế chia sẻ, kết nối dữ liệu một cách bền vững, lâu dài. Điều này đòi hỏi phải hoàn thiện hành lang pháp lý về quyền truy cập dữ liệu, xác lập nghĩa vụ cập nhật và chia sẻ dữ liệu định kỳ giữa các cơ quan, thiết lập cơ chế giám sát việc chia sẻ dữ liệu. Cần phát triển các mô hình quản trị dữ liệu thông minh, trong đó có sự phối hợp liên ngành, liên cấp, liên vùng, xây dựng các chỉ số đo lường hiệu quả chia sẻ dữ liệu và đánh giá tác động đến hoạt động quản lý. Cùng với đó, cần triển khai các khóa đào tạo, bồi dưỡng chuyên sâu cho cán bộ kỹ thuật,

chuyên gia dữ liệu và cán bộ quản lý trong các cơ quan nhà nước để nâng cao năng lực tiếp cận và ứng dụng dữ liệu lớn trong thực tiễn.

Ngoài ra, phải tổ chức triển khai các chiến dịch thu thập, làm sạch, chuẩn hóa và đồng bộ hóa dữ liệu quy mô lớn, đặc biệt là các loại dữ liệu cơ bản phục vụ công tác dân cư, hành chính công, phát triển đô thị, y tế, giáo dục, an sinh xã hội. Việc xử lý dữ liệu không chính xác, dữ liệu trùng lặp, thiếu đồng bộ hiện nay là một trong những thách thức lớn cản trở việc hình thành kho dữ liệu tổng hợp quốc gia. Do đó, cần có sự vào cuộc quyết liệt của các bộ, ngành, địa phương để rà soát, cập nhật dữ liệu, bảo đảm chất lượng và độ tin cậy.

Hoàn thiện quy trình thu thập, xử lý, lưu trữ và khai thác dữ liệu theo nguyên tắc bảo vệ quyền riêng tư và lợi ích chính đáng của cá nhân, tổ chức. Phải có cơ chế xin phép – đồng ý minh bạch đối với dữ liệu cá nhân, bảo đảm việc khai thác chỉ được thực hiện khi có căn cứ pháp lý rõ ràng. Các dữ liệu có yếu tố nhạy cảm như y tế, tài chính, định vị, lịch sử tương tác phải được mã hóa, ẩn danh và phân quyền truy cập phù hợp với từng cấp độ người dùng.

Cần triển khai các công cụ giám sát, cảnh báo sớm nguy cơ rò rỉ dữ liệu, tấn công mạng, phá hoại hệ thống dữ liệu quốc gia. Các giải pháp an ninh mạng, mã hóa dữ liệu, kiểm soát truy cập đa tầng, công nghệ nhận diện hành vi bất thường cần được tích hợp đồng bộ trong hạ tầng dữ liệu quốc gia, có khả năng thích ứng và phục hồi nhanh trước các kịch bản tấn công phức tạp. Bộ máy quản lý dữ liệu cần được thiết lập theo mô hình hiện đại, chuyên nghiệp, có sự tham gia của các trung tâm an toàn dữ liệu, các tổ chức độc lập giám sát và phản biện xã hội.

Việc phát triển kho dữ liệu tổng hợp quốc gia không thể tách rời khỏi tiến trình xây dựng chính phủ số và đô thị thông

minh. Dữ liệu là nguồn lực chiến lược, là cơ sở để vận hành các hệ thống giám sát điều hành thông minh, dự báo chính sách, cung cấp dịch vụ công trực tuyến cấp độ cao. Do đó, mọi hoạt động thu thập, lưu trữ, xử lý và chia sẻ dữ liệu cần được đặt trong tầm nhìn chiến lược dài hạn về phát triển quốc gia số, gắn kết chặt chẽ giữa trung ương và địa phương, giữa nhà nước và doanh nghiệp, giữa quản lý và sáng tạo.

Trong bối cảnh đó, lực lượng Công an nhân dân đóng vai trò then chốt trong việc bảo vệ kho dữ liệu tổng hợp quốc gia, phòng chống các hành vi tấn công mạng, rò rỉ dữ liệu, xâm phạm quyền riêng tư và phá hoại hạ tầng thông tin quốc gia. Công an các đơn vị, địa phương cần phối hợp chặt chẽ với các cơ quan chức năng triển khai các biện pháp nghiệp vụ nhằm bảo vệ an toàn dữ liệu chuyên ngành, đặc biệt là dữ liệu liên quan đến an ninh quốc gia, dữ liệu dân cư, dữ liệu tài chính – ngân hàng, dữ liệu điều hành quản lý nhà nước. Bên cạnh đó, lực lượng Công an cũng cần nâng cao năng lực phân tích, khai thác dữ liệu lớn phục vụ công tác điều tra, phòng chống tội phạm, đảm bảo trật tự an toàn xã hội trong không gian mạng, đồng thời tham gia góp ý, xây dựng thể chế pháp luật về bảo vệ dữ liệu và an ninh mạng trong tiến trình xây dựng kho dữ liệu tổng hợp quốc gia.

4.2. Xây dựng bộ chỉ số đánh giá hiệu quả khai thác, sử dụng dữ liệu, đo lường tác động của dữ liệu đến phát triển kinh tế – xã hội, cải cách hành chính và nâng cao năng lực cạnh tranh quốc gia.

Việc xây dựng bộ chỉ số đánh giá hiệu quả khai thác, sử dụng dữ liệu là một trong những giải pháp then chốt nhằm hiện thực hóa mục tiêu phát triển quốc gia dựa trên dữ liệu. Trước hết, cần tiến hành rà soát, tổng hợp thực trạng khai thác và sử dụng dữ liệu tại các bộ, ngành, địa phương, doanh nghiệp và tổ chức xã hội. Việc đánh giá hiện trạng phải bảo đảm phản ánh trung thực mức độ khai thác dữ liệu trong các hoạt động quản lý, điều hành, cung cấp dịch vụ công, sản xuất kinh doanh và đời sống xã hội. Trên cơ sở đó, xác định các khoảng trống thông tin, điểm nghẽn về thể chế, công nghệ, nhân lực và nguồn

lực tài chính đang cản trở hiệu quả sử dụng dữ liệu, từ đó làm cơ sở xây dựng các chỉ số đánh giá phù hợp với bối cảnh quốc gia và định hướng phát triển bền vững.

Cần tổ chức nghiên cứu, tham khảo kinh nghiệm quốc tế về xây dựng hệ thống chỉ số đánh giá dữ liệu quốc gia, nhất là từ các nước có trình độ phát triển cao về kinh tế số và chính phủ số. Việc học hỏi các bộ chỉ số như OECD OURData Index, Digital Economy and Society Index (DESI) của Liên minh Châu Âu hay các bộ chỉ số đo lường năng lực dữ liệu của Singapore, Estonia sẽ là nguồn tham khảo quan trọng. Tuy nhiên, không rập khuôn máy móc mà cần phân tích chọn lọc, điều chỉnh để phù hợp với điều kiện chính trị, kinh tế, văn hóa và đặc điểm hạ tầng dữ liệu tại Việt Nam. Huy động các nhà khoa học, chuyên gia dữ liệu, các cơ quan hoạch định chính sách và cộng đồng doanh nghiệp tham gia đóng góp xây dựng bộ chỉ số, bảo đảm tính toàn diện và khả thi trong thực tiễn triển khai. Các chỉ số cần bao quát được các khía cạnh cơ bản như mức độ sẵn sàng và kết nối dữ liệu; hiệu quả khai thác dữ liệu trong hoạch định chính sách công, điều hành chính quyền; giá trị dữ liệu trong đổi mới sáng tạo, phát triển dịch vụ số và sản xuất kinh doanh; mức độ bảo đảm quyền riêng tư dữ liệu cá nhân và an toàn dữ liệu; năng lực quản trị dữ liệu của các cơ quan nhà nước và tổ chức xã hội.

Việc thiết kế bộ chỉ số cần được thực hiện theo hướng có thể lượng hóa, dễ thu thập, có khả năng so sánh theo thời gian và giữa các đơn vị hành chính hoặc lĩnh vực kinh tế – xã hội khác nhau. Các chỉ số cần phân tầng theo cấp độ quốc gia, ngành, địa phương, tổ chức để phục vụ cho cả việc đánh giá tổng thể lẫn phân tích chuyên sâu. Đối với mỗi chỉ số, cần xác định rõ phương pháp đo lường, nguồn dữ liệu, đơn vị chịu trách nhiệm thu thập và tần suất cập nhật. Ngoài ra, cần thiết lập các mức chuẩn hoặc ngưỡng đánh giá để phân loại mức độ hiệu quả, từ đó giúp đưa ra các cảnh báo sớm, đề xuất giải pháp cải thiện.

Một nhiệm vụ quan trọng là xây dựng hạ tầng kỹ thuật phục vụ thu thập, xử lý và phân tích dữ liệu cho hệ thống chỉ

số. Hệ thống này cần có khả năng tích hợp với các nền tảng dữ liệu quốc gia và dữ liệu chuyên ngành, bảo đảm kết nối liên thông, đồng bộ và cập nhật theo thời gian thực hoặc gần thực. Đồng thời, cần ứng dụng trí tuệ nhân tạo và phân tích dữ liệu lớn để phát hiện xu hướng, mối liên hệ ẩn, quy luật vận động từ dữ liệu, qua đó nâng cao giá trị sử dụng của bộ chỉ số trong thực tiễn điều hành và hoạch định chính sách.

Cần có cơ chế bảo đảm tính khách quan, độc lập trong đánh giá chỉ số, tránh tình trạng hình thức, chạy theo thành tích hoặc can thiệp số liệu. Vì vậy, nên thiết lập một cơ quan đầu mối có năng lực và thẩm quyền để quản lý vận hành hệ thống chỉ số quốc gia về dữ liệu, đồng thời trao quyền giám sát cho các tổ chức nghiên cứu độc lập, cộng đồng chuyên gia và cơ quan báo chí. Cũng cần có quy định rõ về trách nhiệm giải trình của các bộ, ngành, địa phương khi kết quả chỉ số thấp, nhằm tạo động lực thay đổi thực chất.

Việc định kỳ công bố kết quả đánh giá chỉ số sẽ góp phần tạo áp lực cải cách, thúc đẩy cạnh tranh lành mạnh giữa các địa phương và đơn vị, đồng thời nâng cao nhận thức xã hội về vai trò của dữ liệu trong phát triển kinh tế – xã hội và cải cách hành chính. Bên cạnh đó, các kết quả đánh giá cũng cần được tích hợp vào các báo cáo chiến lược, quy hoạch, kế hoạch phát triển quốc gia, ngành và địa phương để bảo đảm dữ liệu thực sự trở thành yếu tố nền tảng cho hoạch định chính sách và quản trị quốc gia hiện đại.

Việc xây dựng bộ chỉ số cũng cần tính đến khả năng mở rộng, điều chỉnh linh hoạt theo thời gian, nhằm thích ứng với sự phát triển nhanh chóng của công nghệ và những thay đổi trong thực tiễn. Các chỉ số cần được rà soát, cập nhật định kỳ, bổ sung các nội dung mới về bảo vệ dữ liệu cá nhân, dữ liệu phi cấu trúc, dữ liệu do người dân và doanh nghiệp tạo ra trên không gian mạng, nhằm bảo đảm tính toàn diện và cập nhật của hệ thống đo lường.

Trong quá trình triển khai, cần đặc biệt chú trọng đào tạo và nâng cao năng lực cho đội ngũ cán bộ quản lý, thống kê và công nghệ thông tin tại các bộ, ngành, địa phương để đảm nhiệm tốt việc thu thập, phân tích và sử dụng kết quả bộ chỉ số. Các chương trình đào tạo phải hướng tới xây dựng tư duy dữ liệu, kỹ năng xử lý, trực quan hóa và truyền thông dữ liệu, góp phần hình thành văn hóa sử dụng dữ liệu trong toàn hệ thống chính trị và bộ máy hành chính.

Giám sát, phản ứng sự cố an toàn thông tin 24/7 của Viettel Security.

Ảnh minh họa. Nguồn từ Internet.

Bên cạnh đó, cần hoàn thiện thể chế, quy định pháp lý liên quan đến việc sử dụng bộ chỉ số, bao gồm cơ chế phối hợp liên ngành, chia sẻ dữ liệu giữa các cơ quan, chế tài xử lý khi có sai lệch, gian lận trong cung cấp thông tin đánh giá. Cũng cần có các chính sách khuyến khích sự tham gia của khu vực tư nhân, viện nghiên cứu, tổ chức quốc tế trong quá trình triển khai và vận hành hệ thống chỉ số.

Một nội dung không thể thiếu là đẩy mạnh truyền thông về bộ chỉ số đến toàn xã hội, nhất là đối với cộng đồng doanh nghiệp, người dân, các cơ sở đào tạo và nghiên cứu, nhằm lan tỏa nhận thức đúng đắn và sự ủng hộ rộng rãi đối với chủ trương này. Các hình thức truyền thông cần đa dạng, phù hợp với từng nhóm đối tượng, nhấn mạnh vai trò của dữ liệu như một nguồn lực chiến lược tương đương với đất đai, vốn, tài nguyên hay lao động trong nền kinh tế hiện đại.

Liên quan đến lực lượng Công an nhân dân, việc xây dựng và vận hành bộ chỉ số đánh giá hiệu quả sử dụng dữ liệu cũng có ý nghĩa đặc biệt quan trọng trong công tác bảo đảm an ninh trật tự, phòng chống tội phạm và xây dựng Chính phủ số trong ngành Công an. Việc định lượng hiệu quả khai thác dữ liệu sẽ giúp lực lượng Công an đánh giá chính xác mức độ phát huy giá trị của các cơ sở dữ liệu chuyên ngành như dân cư, căn cước, xuất nhập cảnh, hình sự, ma túy, an ninh mạng... Từ đó có căn cứ để điều chỉnh chiến lược khai thác, phát hiện các điểm nghẽn về hạ tầng, nhân lực hoặc phối hợp liên thông giữa các đơn vị. Đồng thời, các chỉ số còn giúp đo lường tác động của dữ liệu đến hiệu quả xử lý hồ sơ hành chính công trong Công an, mức độ hài lòng của người dân và doanh nghiệp, góp phần cải cách thủ tục hành chính, nâng cao năng lực cạnh tranh quốc gia theo hướng bảo đảm an ninh, an toàn, chính xác và thuận tiện nhất. Đây cũng là cơ sở để ngành Công an tiếp tục hoàn thiện hệ sinh thái dữ liệu an ninh quốc gia, nâng cao năng lực phân tích, cảnh báo, dự báo các nguy cơ, đe dọa từ sớm, từ xa, bảo vệ vững chắc an ninh quốc gia trong bối cảnh chuyển đổi số.

5. Thanh tra, kiểm tra, xử lý vi phạm pháp luật về dữ liệu, phối hợp chặt chẽ với các cơ quan chuyên trách trong phòng chống buôn bán, đánh cắp, rò rỉ và xâm phạm dữ liệu

Thanh tra, kiểm tra và xử lý vi phạm pháp luật về dữ liệu là một trong những nhiệm vụ trọng yếu trong quản lý nhà nước về dữ liệu, có ý nghĩa sống còn đối với sự phát triển an toàn, bền vững của hệ sinh thái dữ liệu quốc gia. Trước bối cảnh dữ liệu ngày càng trở thành nguồn tài nguyên quan trọng, việc bảo đảm tính minh bạch, liêm chính và hiệu quả trong thu thập, lưu trữ, xử lý và sử dụng dữ liệu là điều kiện tiên quyết để xây dựng niềm tin xã hội, bảo vệ quyền và lợi ích của công dân, tổ chức, đồng thời duy trì kỷ cương, pháp luật trong không gian số. Cơ chế thanh tra, kiểm tra cần được tổ chức đồng bộ từ trung ương đến địa phương, với sự phối hợp giữa các cơ quan chuyên môn về dữ liệu, thanh tra nhà nước và các đơn vị chuyên trách về an ninh mạng, công nghệ thông tin. Các cơ quan quản lý cần xác lập quy trình thanh tra, kiểm tra rõ ràng, cụ thể, theo hướng công khai, minh bạch, có trọng tâm, trọng điểm, ưu tiên vào các lĩnh vực nhạy cảm, các hệ thống cơ sở dữ liệu lớn, các nền tảng kỹ thuật số có mức độ thu thập và xử lý dữ liệu quy mô lớn, các tổ chức có dấu hiệu vi phạm quyền riêng tư của người dùng, thao túng thông tin hoặc buôn bán dữ liệu bất hợp pháp.

Việc xây dựng hệ thống tiêu chuẩn, chỉ số, công cụ đánh giá và đo lường việc tuân thủ pháp luật về dữ liệu là nền tảng để các hoạt động thanh tra, kiểm tra diễn ra có hiệu lực, hiệu quả. Các tiêu chuẩn cần được hoàn thiện theo hướng đồng bộ với thông lệ quốc tế, bảo đảm tính tương thích với các cam kết về bảo vệ dữ liệu trong các hiệp định thương mại tự do thế hệ mới mà Việt Nam là thành viên. Hệ thống giám sát cần ứng dụng công nghệ hiện đại như trí tuệ nhân tạo, phân tích dữ liệu lớn để phát hiện kịp thời các bất thường, cảnh báo sớm rủi ro vi phạm, tạo tiền đề cho hoạt động kiểm

tra đột xuất hoặc định kỳ. Đồng thời, cần đẩy mạnh đào tạo, nâng cao năng lực cho đội ngũ cán bộ thanh tra, kiểm tra trong lĩnh vực dữ liệu, bảo đảm hiểu biết chuyên sâu cả về pháp luật, công nghệ lẫn kỹ năng phân tích, xử lý tình huống phức tạp trong thực tế.

Công tác xử lý vi phạm pháp luật về dữ liệu phải được thực hiện nghiêm minh, đúng quy định, đủ sức răn đe, nhưng đồng thời cũng phải bảo đảm tính nhân văn, linh hoạt, tránh gây thiệt hại không đáng có cho sự phát triển của các tổ chức, doanh nghiệp. Việc xác định mức độ vi phạm, hình thức xử phạt cần căn cứ vào bản chất hành vi, hậu quả thực tế và mức độ hợp tác của tổ chức, cá nhân liên quan. Trong một số trường hợp, có thể áp dụng cơ chế xử lý mềm dẻo như nhắc nhở, cảnh báo, hỗ trợ khắc phục sai phạm, đặc biệt đối với các đơn vị lần đầu vi phạm hoặc vô ý mắc lỗi do thiếu hiểu biết. Tuy nhiên, đối với những hành vi có tính chất nghiêm trọng như buôn bán trái phép dữ liệu cá nhân, đánh cắp hoặc làm rò rỉ dữ liệu quy mô lớn, xâm phạm hệ thống dữ liệu quan trọng của quốc gia thì cần áp dụng các biện pháp mạnh như xử phạt hành chính ở mức cao nhất, truy cứu trách nhiệm hình sự, đình chỉ hoạt động hoặc thu hồi giấy phép để bảo đảm tính nghiêm minh của pháp luật và an toàn cho toàn bộ không gian dữ liệu quốc gia.

Các đại biểu tham dự Lễ khai trương hệ thống cơ sở dữ liệu quốc gia về dân cư và hệ thống sản xuất, cấp và quản lý căn cước công dân. Ảnh: Nguyễn Hiếu

Phối hợp giữa các cơ quan chức năng là yếu tố then chốt trong thanh tra, kiểm tra và xử lý vi phạm pháp luật về dữ liệu. Cần hình thành cơ chế điều phối liên ngành rõ ràng giữa các cơ quan nhà nước quản lý dữ liệu, cơ quan thanh tra chuyên ngành, cơ quan an ninh mạng, lực lượng công an, kiểm sát, tòa án và các tổ chức độc lập về bảo vệ dữ liệu. Mỗi cơ quan cần xác định rõ vai trò, trách nhiệm, quyền hạn của mình trong chuỗi xử lý vi phạm, tránh chồng chéo, đùn đẩy hoặc bỏ sót trách

nhiệm. Cần thiết lập cơ chế chia sẻ thông tin về các vụ việc, các dấu hiệu vi phạm, kết quả thanh tra để tạo thành một hệ sinh thái đồng bộ trong quản lý và bảo vệ dữ liệu. Cần phát huy vai trò của hệ thống tiếp nhận phản ánh, kiến nghị của người dân, tổ chức trong phát hiện vi phạm, đặc biệt thông qua nền tảng số và cơ chế bảo vệ người tố giác vi phạm pháp luật về dữ liệu. Đồng thời, hợp tác quốc tế trong xử lý vi phạm xuyên biên giới, truy vết các hành vi phạm tội công nghệ cao liên quan đến dữ liệu cũng cần được ưu tiên đẩy mạnh nhằm nâng cao hiệu quả phòng ngừa và răn đe trong môi trường số toàn cầu.

Việc ngăn chặn và xử lý hành vi buôn bán, đánh cắp, rò rỉ và xâm phạm dữ liệu đòi hỏi các cơ quan chức năng, đặc biệt là lực lượng chuyên trách về an ninh mạng và dữ liệu, phải có khả năng chủ động giám sát không gian mạng, phân tích, truy vết và bóc gỡ các đường dây tội phạm sử dụng kỹ thuật cao để tiếp cận và khai thác dữ liệu trái phép. Cần thiết lập hệ thống cảnh báo sớm các hành vi bất thường như việc khai thác dữ liệu vượt mức cho phép, truyền dữ liệu ra nước ngoài không có kiểm soát, hành vi thu thập thông tin từ thiết bị đầu cuối mà không được sự đồng ý của người dùng. Những công cụ như hệ thống chặn lọc, các thiết bị an ninh mạng tích hợp trí tuệ nhân tạo, blockchain và mã hóa dữ liệu cần được ưu tiên đầu tư nhằm tăng cường khả năng phòng ngừa và ngăn chặn từ xa. Các đơn vị chức năng cần lập kế hoạch kiểm tra đột xuất đối với các tổ chức trung gian dữ liệu, doanh nghiệp công nghệ lớn, nền tảng mạng xã hội nước ngoài hoạt động tại Việt Nam, đồng thời nâng cao vai trò kiểm tra đối với khối cơ quan nhà nước trong tuân thủ quy định bảo mật và khai thác dữ liệu công.

Song hành với hoạt động thanh tra, kiểm tra, cần tăng cường công tác truyền thông, phổ biến pháp luật và nâng cao nhận thức cộng đồng về quyền và nghĩa vụ liên quan đến dữ liệu. Việc cung cấp thông tin minh bạch, dễ hiểu về các quy định pháp luật, chế tài xử lý vi phạm, cách thức khiếu nại hoặc phản ánh hành vi xâm phạm dữ liệu cần được triển khai thường xuyên trên các phương tiện truyền thông đại chúng và các nền tảng số. Cộng đồng người dùng, doanh nghiệp và cơ quan nhà

nước đều cần được trang bị kiến thức và kỹ năng để chủ động bảo vệ dữ liệu cá nhân, nhận diện rủi ro và phản ứng kịp thời với các hành vi vi phạm. Việc xây dựng văn hóa tuân thủ pháp luật về dữ liệu cần bắt đầu từ hệ thống giáo dục và đào tạo, tích hợp nội dung pháp luật về dữ liệu vào chương trình học ở các cấp, đặc biệt trong các ngành công nghệ thông tin, luật, an ninh mạng và quản lý nhà nước.

Trong xu thế phát triển mạnh mẽ của chuyển đổi số, các hành vi vi phạm pháp luật về dữ liệu ngày càng tinh vi, có tính xuyên quốc gia và gắn liền với các hoạt động tội phạm công nghệ cao, khủng bố mạng, gián điệp mạng, gây ảnh hưởng nghiêm trọng đến an ninh quốc gia, trật tự an toàn xã hội và quyền con người. Do vậy, việc nâng cao năng lực điều tra, truy tố, xét xử các hành vi vi phạm pháp luật về dữ liệu là đòi hỏi cấp thiết. Cần có các đơn vị chuyên trách đủ năng lực về kỹ thuật, pháp luật, ngoại ngữ và hợp tác quốc tế để xử lý các vụ việc phức tạp, có yếu tố nước ngoài hoặc diễn ra trên các nền tảng công nghệ mới. Việc hình thành hệ thống cơ sở dữ liệu phục vụ điều tra, xác minh và truy vết tội phạm dữ liệu cũng cần được đầu tư đồng bộ, tạo điều kiện cho các cơ quan chức năng dễ dàng chia sẻ thông tin, kết nối dữ liệu phục vụ hoạt động tố tụng.

Lực lượng Công an nhân dân, với vai trò nòng cốt trong bảo vệ an ninh quốc gia và giữ gìn trật tự, an toàn xã hội, cần phát huy vai trò xung kích trong hoạt động thanh tra, kiểm tra và xử lý vi phạm pháp luật về dữ liệu. Lực lượng này cần chủ động xây dựng và vận hành hệ thống giám sát dữ liệu phục vụ an ninh mạng quốc gia, triển khai các biện pháp nghiệp vụ nhằm phát hiện, điều tra, truy bắt và xử lý các đối tượng buôn bán, đánh cắp hoặc xâm phạm dữ liệu, đặc biệt là dữ liệu cá nhân, dữ liệu nhạy cảm, dữ liệu quan trọng liên quan đến bí mật Nhà nước. Bên cạnh đó, cần đẩy mạnh tuyên truyền, hướng dẫn người dân và doanh nghiệp nâng cao ý thức cảnh giác, phối hợp chặt chẽ với các cơ quan quản lý nhà nước, các tổ chức quốc tế trong việc chia sẻ thông tin và truy vết các hành vi phạm tội dữ liệu xuyên biên giới.

6. Xây dựng nguồn nhân lực chất lượng cao về an ninh dữ liệu và đẩy mạnh hợp tác quốc tế có chọn lọc

Trong chuyển đổi số, yếu tố con người sẽ đóng vai trò quyết định thành công; do vậy, cần xây dựng một 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:

6.1. Hiện đại hóa các cơ sở đào tạo trong Công an nhân dân; trong đó, đầu tư trọng diêm, nâng cấp các học viện, nhà trường Công an nhân dân thành các trung tâm đào tạo và nghiên cứu hàng đầu về khoa học dữ liệu, chuyển đổi số

Trong công tác đào tạo, bồi dưỡng thường xuyên, Bộ Công an đã từng bước thực hiện hiệu quả một số chủ trương quan trọng nhằm nâng cao chất lượng công tác đào tạo, bồi dưỡng, như: tăng cường chỉ tiêu đào tạo tập trung tại trường; đào tạo vì yêu cầu công việc, không vì thực hiện chính sách cán bộ; tập trung đào tạo các ngành, chuyên ngành đang thiếu hụt về nhân lực; kết hợp giữa đào tạo, bồi dưỡng với cơ cấu lại đội ngũ cán bộ ở các cấp Công an. Công tác thi, kiểm tra, đánh giá và bảo đảm chất lượng đào tạo được quan tâm, chú trọng đổi mới cả về hình thức và nội dung. Việc xây dựng và tổ chức đào tạo theo chuẩn đầu ra trong các trường Công an nhân dân được điều chỉnh và thực hiện theo đúng quy định, hướng dẫn của Nhà nước và Bộ Công an.

Bộ Công an tăng cường công tác hợp tác đào tạo với các ngành và hợp tác với các đối tác quốc tế nhằm đáp ứng yêu cầu nâng cao chất lượng nguồn nhân lực của lực lượng Công an nhân dân, nhất là hợp tác đào tạo những lĩnh vực mà các

trường Công an nhân dân không đào tạo; quan tâm đầu tư cơ sở hạ tầng, cơ sở vật chất, điều kiện đảm bảo về hậu cần, kỹ thuật, tài chính nhằm phục vụ yêu cầu nhiệm vụ giáo dục và đào tạo của lực lượng Công an nhân dân.

Bộ Công an Việt Nam thúc đẩy hợp tác đào tạo và an ninh với các đối tác Ấn Độ. Trong khuôn khổ triển khai kế hoạch đối ngoại và hợp tác quốc tế năm 2024, đoàn đại biểu cấp cao Bộ Công an Việt Nam do Thượng tướng Trần Quốc Tỏ, Ủy viên Trung ương Đảng, Thứ trưởng làm Trưởng đoàn đã có chuyến thăm, làm việc tại Ấn Độ từ ngày 14-19/12/2024. Ảnh Sưu tầm

Một số trường Công an nhân dân đã chủ động xây dựng dự án, phối hợp các đơn vị nghiệp vụ thuộc Bộ đề xuất trang cấp thiết bị thực hành phục vụ công tác dạy học; chủ động nghiên cứu, đẩy mạnh ứng dụng công nghệ thông tin, chuyển đổi số trong các khâu, quy trình công tác. Công an một số địa phương tranh thủ và sử dụng có hiệu quả nguồn kinh phí và trang thiết bị do cấp ủy, chính quyền địa phương hỗ trợ phục vụ nhiệm vụ đào tạo, bồi dưỡng cán bộ Công an nhân dân …

Thời gian tới, Bộ Công an cần tiếp tục gương mẫu, đi đầu thực hiện chỉ đạo của đồng chí Tổng Bí thư Tô Lâm về *"Hoàn thành sự nghiệp đổi mới giáo dục đào tạo, hoàn thành mục tiêu tạo nguồn nhân lực cho xây dựng và bảo vệ Tổ quốc trong kỷ nguyên vươn mình của dân tộc trong nhiệm kỳ Đại hội XIV của Đảng"* với các nhiệm vụ cụ thể như:

(1) Cụ thể hóa, triển khai có hiệu quả Kết luận số 91 của Bộ Chính trị khóa XIII về tiếp tục thực hiện Nghị quyết số 29 ngày 4/11/2013 của Ban Chấp hành Trung ương Đảng khóa XI "Về đổi mới căn bản, toàn diện giáo dục và đào tạo, đáp ứng yêu cầu công nghiệp hóa, hiện đại hóa trong điều kiện kinh tế thị trường định hướng xã hội chủ nghĩa và hội nhập quốc tế" gắn với Đề án về "Nâng cao chất lượng giáo dục, đào tạo trong Công an nhân dân đến năm 2030 đáp ứng mục tiêu xây dựng lực lượng Công an nhân dân thật sự trong sạch, vững mạnh, chính quy, tinh nhuệ, hiện đại"; rà soát, tiếp thu, hoàn chỉnh dự thảo các văn bản về triển khai Kết luận 91 của Bộ Chính trị; tiếp tục thực hiện Nghị quyết số 17 của Đảng ủy Công an Trung ương và Chỉ thị của Bộ Công an về tiếp tục đổi mới căn bản toàn diện giáo dục đào tạo trong Công an nhân dân để sớm ban hành, thống nhất thực hiện.

(2) Tiếp tục đổi mới mạnh mẽ mục tiêu, chương trình, nội dung, phương pháp đào tạo, quản trị nhà trường theo hướng khoa học, hiện đại, đồng bộ, liên thông, phù hợp với tiến trình hội nhập quốc tế về an ninh, trật tự, gắn chặt với thực tiễn công tác bảo vệ an ninh, trật tự, xây dựng lực lượng Công an nhân dân; có giải pháp hữu hiệu khắc phục triệt để tình trạng xa rời

giữa giảng dạy với thực tiễn hiện nay, trong đó nhu cầu, nội dung đào tạo phải trên cơ sở mục tiêu, nhiệm vụ bảo vệ an ninh Quốc gia trong kỷ nguyên mới.

(3) Kết hợp chặt chẽ giữa giảng dạy và nghiên cứu khoa học; giữa nhà trường và các đơn vị thực tiễn; đổi mới mạnh mẽ nội dung giáo dục, phương pháp giáo dục theo hướng thiết thực, tăng kỹ năng của người học, tăng thực hành, vận dụng kiến thức vào thực tiễn; nhạy bén, chủ động tham gia tích cực các chương trình phát triển nguồn nhân lực của đất nước…

Các học viện, trường Công an nhân dân cần lan tỏa cách làm để gia tăng đóng góp của giáo dục, đào tạo Công an nhân dân trong phát triển nguồn nhân lực của đất nước, nhất là đối với nhân lực chất lượng cao, nhân lực các ngành về bảo đảm an ninh, an toàn quá trình đột phá phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia. Bám sát và triển khai có hiệu quả các chủ trương của Đảng về học tập suốt đời, về học tập số, về đào tạo ngoại ngữ. Đầu tư xây dựng, hoàn thiện cơ sở vật chất giáo dục, đào tạo có trọng tâm, trọng điểm, tập trung một số ngành, nghề, lĩnh vực đào tạo nhân lực trình độ cao gắn với nghiên cứu, phát triển khoa học, công nghệ và đổi mới sáng tạo.

(4) Phấn đấu tăng hạng giáo dục Công an nhân dân trong hệ thống giáo dục Việt Nam, khu vực và quốc tế. Đến năm 2030, giáo dục Công an nhân dân ít nhất có 2 trường đạt chuẩn quốc gia; Học viện An ninh nhân dân và Học viện Cảnh sát nhân dân trở thành các trung tâm nghiên cứu khoa học, công nghệ, đào tạo chuyên gia về an ninh mạng, phòng, chống tội phạm sử dụng công nghệ cao được xếp hạng trong khu vực. Tập trung xây dựng đội ngũ nhà giáo, cán bộ quản lý giáo dục trong Công an nhân dân có đức, có tài, đam mê, nhiệt huyết, có kỹ năng, kiến thức, năng lực truyền thụ, ham học hỏi, đổi mới sáng tạo, thật sự là những tấm gương để học viên học tập, noi theo; phấn đấu các nhà giáo đồng thời là những chuyên gia, nhà khoa học của chuyên ngành mình giảng dạy; có cơ chế để nhà giáo có thể tham gia tích cực, hiệu quả giải quyết các vấn đề phức tạp nổi lên về an ninh, trật tự có liên quan…

(5) Cục Đào tạo - Bộ Công an và các đơn vị chức năng cần khẩn trương có kế hoạch cụ thể; phát huy cao độ vai trò tham mưu nòng cốt; huy động sự vào cuộc tích cực của các nhà trường, Công an các đơn vị, địa phương, tháo gỡ triệt để các điểm nghẽn của giáo dục, đào tạo trong Công an nhân dân; xác định chính xác nhu cầu đào tạo cụ thể trên cơ sở thực tiễn yêu cầu công tác bảo đảm an ninh, của Công an các đơn vị, địa phương; bảo đảm thực hiện tốt các nhiệm vụ theo chương trình, kế hoạch đào tạo, bồi dưỡng mà Đảng ủy Công an Trung ương, lãnh đạo Bộ Công an đã đề ra..

Học viện Cảnh sát nhân dân ứng dụng công nghệ trong tổ chức Hội thi Olympic Luật Hiến pháp và Olympic Luật Hình sự theo hình thức trắc nghiệm trên hệ thống mạng nội bộ. Ảnh Sưu tầm

6.2. Đột phá tư duy phát triển, xóa bỏ mọi rào cản nhận thức lạc hậu, khơi dậy tinh thần dám nghĩ, dám làm, dám đổi mới, dám chịu trách nhiệm.

Đột phá tư duy phát triển là một yêu cầu tất yếu trong bối cảnh đất nước đang chuyển mình mạnh mẽ dưới tác động của cách mạng công nghiệp lần thứ tư và tiến trình chuyển đổi số quốc gia. Tư duy phát triển không còn là sự lặp lại của những mô hình cũ kỹ, mà là sự vận dụng linh hoạt, sáng tạo và phù hợp với thực tiễn của từng lĩnh vực, từng địa phương. Để thúc đẩy tiến trình phát triển, cần phải thực sự xóa bỏ các rào cản nhận thức lạc hậu vốn đã tồn tại dai dẳng trong bộ máy hành chính và trong tâm lý xã hội, bao gồm tâm lý ỷ lại vào cấp trên, sợ sai, sợ trách nhiệm, ngại va chạm, ngại thay đổi. Những biểu hiện như trì trệ trong cải cách thủ tục hành chính, chậm trễ trong ứng dụng công nghệ mới, bảo thủ trong điều hành, thiên về hình thức hơn nội dung đều là sản phẩm của một tư duy cũ kỹ, không còn phù hợp với yêu cầu phát triển hiện nay.

Tinh thần dám nghĩ, dám làm, dám đổi mới và dám chịu trách nhiệm cần được khơi dậy và nuôi dưỡng như một phẩm chất cốt lõi trong đội ngũ cán bộ, công chức, viên chức các cấp. Mỗi cán bộ không chỉ là người thực hiện chính sách, mà còn phải là chủ thể kiến tạo chính sách, dám đề xuất cái mới, dám chịu trách nhiệm về quyết định của mình trong khuôn khổ pháp luật và vì lợi ích chung. Điều này đòi hỏi phải xây dựng một cơ chế chính sách phù hợp để bảo vệ những người đổi mới sáng tạo, khuyến khích sự dấn thân vào việc cải cách, cải tiến, đề xuất các phương án mới, kể cả khi các phương án đó chưa từng có tiền lệ. Bên cạnh đó, cần tăng cường công tác giáo dục chính trị tư tưởng, đạo đức công vụ, gắn với bồi dưỡng năng lực chuyên môn, để người cán bộ có thể tự tin thực hiện nhiệm vụ trong môi trường biến động nhanh và có nhiều thách thức.

Một trong những yếu tố quyết định đến việc thúc đẩy tư duy phát triển là thiết lập được môi trường làm việc minh bạch, khuyến khích sự phản biện và đối thoại, chấp nhận rủi ro có kiểm soát và đánh giá hiệu quả bằng kết quả thực chất. Cần loại bỏ tâm lý sợ bị quy trách nhiệm khi thất bại trong đổi mới, nếu việc đổi mới đó dựa trên tinh thần cầu thị, có căn cứ khoa học, có quá trình thẩm định rõ ràng. Việc xây dựng hệ thống đánh giá cán bộ phải đặt trọng tâm vào sản phẩm cụ thể, kết quả thực tế chứ không đơn thuần chỉ dựa vào quy trình hay hình thức báo cáo. Đồng thời, các cơ quan kiểm tra, giám sát phải hoạt động công tâm, khách quan, không vì sợ trách nhiệm mà bóp nghẹt sự sáng tạo chính đáng.

Để xóa bỏ rào cản tư duy, công tác tổ chức cán bộ cũng cần cải tiến theo hướng linh hoạt, mở rộng không gian để phát hiện và trọng dụng nhân tài. Nhiều cán bộ trẻ có năng lực, có khát vọng cống hiến cần được trao cơ hội thể hiện và thăng tiến thông qua các tiêu chí minh bạch, công bằng và dựa vào hiệu quả công việc. Cần tạo ra các cơ chế luân chuyển, đào tạo, đánh giá và sàng lọc cán bộ một cách khoa học, công tâm nhằm làm mới tư duy trong hệ thống và giảm thiểu tình trạng cục bộ, bảo thủ, trì trệ. Tổ chức bộ máy hành chính cũng cần tinh gọn, hiệu lực, hiệu quả và thích ứng linh hoạt với yêu cầu mới, trong đó nhấn mạnh vai trò lãnh đạo của người đứng đầu trong việc truyền cảm hứng, khuyến khích đổi mới và dẫn dắt tổ chức vượt qua giới hạn cũ.

Tư duy phát triển không chỉ bó hẹp trong khuôn khổ hành chính nhà nước mà còn phải lan tỏa mạnh mẽ trong toàn xã hội. Cộng đồng doanh nghiệp, nhất là các doanh nghiệp nhỏ và vừa, cần được tiếp cận các chính sách hỗ trợ đổi mới sáng tạo, thúc đẩy nghiên cứu – phát triển, ứng dụng công nghệ số và mô hình kinh doanh mới. Nhà nước cần đóng vai trò định hướng và dẫn dắt, đồng thời gỡ bỏ các rào cản thể chế, tạo điều kiện cho doanh nghiệp tự do sáng tạo trong khuôn khổ pháp luật. Hệ sinh thái khởi nghiệp sáng tạo phải thực sự được nuôi dưỡng bằng nguồn vốn, tri thức, hạ tầng công nghệ và môi trường pháp

lý thuận lợi. Vai trò của các tổ chức xã hội, các viện nghiên cứu, trường đại học, các trung tâm đổi mới sáng tạo cũng cần được phát huy nhằm thúc đẩy chuyển giao tri thức, tăng cường hợp tác công – tư, tạo ra giá trị gia tăng cho nền kinh tế.

Giáo dục – đào tạo là lĩnh vực trọng yếu để tạo nền tảng tư duy mới cho cả thế hệ tương lai. Cần đổi mới toàn diện phương pháp giảng dạy, chuyển từ dạy chữ sang dạy làm người, dạy cách tư duy phản biện, sáng tạo và giải quyết vấn đề. Chương trình giáo dục cần khuyến khích học sinh, sinh viên tự học, tự nghiên cứu, dám đặt câu hỏi và phản biện có cơ sở. Các mô hình giáo dục khai phóng, STEM, giáo dục số cần được mở rộng và phát triển sâu rộng trong toàn hệ thống. Giáo viên cần được đào tạo lại để thích nghi với yêu cầu mới, trở thành người hướng dẫn, đồng hành và khơi dậy tiềm năng sáng tạo của học trò, thay vì chỉ truyền thụ kiến thức một chiều như trước đây.

Truyền thông đóng vai trò quan trọng trong việc hình thành và thúc đẩy tư duy phát triển. Các cơ quan báo chí, truyền thông phải làm tốt vai trò định hướng dư luận, phản ánh trung thực thực tiễn, tôn vinh những tấm gương đổi mới sáng tạo, đồng thời phê phán những biểu hiện trì trệ, bảo thủ, né tránh trách nhiệm. Cần phát huy vai trò của mạng xã hội như một kênh lắng nghe phản biện xã hội, khuyến khích thảo luận công khai, minh bạch các chính sách phát triển. Truyền thông hiện đại không chỉ dừng lại ở việc cung cấp thông tin, mà còn là công cụ để kích thích sự thay đổi trong tư duy cộng đồng, thúc đẩy nhận thức tích cực, truyền cảm hứng hành động và lan tỏa khát vọng phát triển.

Việc khơi dậy tinh thần đổi mới sáng tạo và dám chịu trách nhiệm cần được thể chế hóa bằng các quy định pháp luật cụ thể, rõ ràng về trách nhiệm và quyền hạn của từng vị trí công tác. Không thể yêu cầu cán bộ dám chịu trách nhiệm khi cơ chế lại không bảo vệ được những người dám làm, dám đổi mới. Vì vậy, cần khẩn trương rà soát, sửa đổi, bổ sung các văn bản

pháp luật có liên quan, bảo đảm tính minh bạch, nhất quán trong thực thi, để cán bộ không phải "liệu cơm gắp mắm" hay rơi vào tình trạng "dám làm nhưng không dám chịu trách nhiệm". Hệ thống pháp luật phải trở thành bệ đỡ cho sự đổi mới chứ không phải là rào cản trói buộc tư duy sáng tạo.

Cần thiết lập một nền văn hóa đổi mới sáng tạo trong toàn xã hội. Văn hóa này cần được định hình từ trong tổ chức Đảng, cơ quan nhà nước đến từng hộ gia đình, từng lớp học. Trong đó, mỗi người dân là một mắt xích sáng tạo, mỗi tổ chức là một tế bào đổi mới, mỗi địa phương là một trung tâm thực hành tư duy phát triển. Văn hóa đổi mới không chấp nhận sự thỏa hiệp với trì trệ, bảo thủ, mà cổ vũ cho khát vọng vươn lên, sẵn sàng thay đổi và tự làm mới chính mình. Việc tôn vinh và lan tỏa các điển hình tiên tiến, người tốt – việc tốt, sáng kiến hiệu quả cần được thực hiện thường xuyên, liên tục, như một cơ chế khen thưởng tinh thần đổi mới và dám chịu trách nhiệm.

Với lực lượng Công an nhân dân, đột phá tư duy phát triển và khơi dậy tinh thần dám nghĩ, dám làm, dám đổi mới, dám chịu trách nhiệm là yêu cầu cấp thiết trong tình hình mới, đặc biệt khi chuyển đổi số và an ninh phi truyền thống đang đặt ra những thách thức ngày càng lớn. Cán bộ, chiến sĩ Công an không chỉ thực hiện nhiệm vụ bảo vệ an ninh trật tự theo phương thức truyền thống, mà còn phải chủ động nắm bắt, ứng dụng công nghệ số, phân tích dữ liệu lớn, trí tuệ nhân tạo để đấu tranh phòng, chống tội phạm một cách hiệu quả. Tư duy bảo vệ an ninh phải chuyển từ bị động sang chủ động, từ cá thể hóa sang tổng thể hóa, từ địa phương hóa sang tích hợp dữ liệu toàn ngành. Mỗi đơn vị Công an cần phát huy vai trò hạt nhân đổi mới trong nội bộ, dám thí điểm các mô hình quản lý, xử lý nghiệp vụ mới, dám đề xuất giải pháp phi truyền thống trong điều kiện pháp luật cho phép, gắn với trách nhiệm cụ thể. Việc nâng cao nhận thức, cải cách hành chính, hiện đại hóa lực lượng, bồi dưỡng cán bộ có tư duy số, đổi mới phương thức tuyên truyền, vận động quần chúng đều là những biểu hiện cụ thể

của tư duy phát triển trong ngành Công an. Chính sự đổi mới tư duy và quyết liệt hành động của lực lượng Công an sẽ góp phần giữ vững an ninh chính trị, trật tự an toàn xã hội, đồng thời dẫn dắt công cuộc chuyển đổi số quốc gia đi vào thực chất và hiệu quả.

Thứ trưởng Nguyễn Văn Long yêu cầu hoàn thiện công tác chuẩn bị, đưa Trung tâm Dữ liệu quốc gia và Cổng Dịch vụ công quốc gia vào vận hành thử trong tháng 5/2025. Ảnh minh họa. Nguồn từ Internet.

6.2. Phát triển đội ngũ cán bộ quản lý và chuyên gia dữ liệu chất lượng cao, thông qua các chương trình đào tạo, bồi dưỡng, chuẩn hóa kỹ năng về phân tích, an ninh mạng và quản trị dữ liệu.

Phát triển đội ngũ cán bộ quản lý và chuyên gia dữ liệu chất lượng cao là giải pháp trọng tâm nhằm đáp ứng yêu cầu chuyển đổi số quốc gia, xây dựng nền kinh tế số, xã hội số và chính phủ số hiện đại. Việc xây dựng một lực lượng nhân lực có trình độ chuyên môn sâu, tư duy chiến lược và đạo đức nghề nghiệp vững vàng đòi hỏi một chiến lược bài bản, nhất quán và liên tục. Trước hết, cần thiết lập khung năng lực chuẩn quốc gia đối với cán bộ dữ liệu, chuyên gia phân tích dữ liệu, chuyên gia an toàn thông tin và cán bộ quản lý dữ liệu cấp trung ương, địa phương. Khung năng lực này phải dựa trên tiêu chuẩn quốc tế, được điều chỉnh phù hợp với thực tiễn Việt Nam, phản ánh đầy đủ các yêu cầu về trình độ học vấn, kỹ năng chuyên môn, kỹ năng mềm, đạo đức nghề nghiệp và khả năng thích ứng công nghệ. Đây là cơ sở để xây dựng chương trình đào tạo thống nhất và chuẩn hóa chất lượng đầu ra.

Tiếp theo, cần phát triển hệ thống đào tạo, bồi dưỡng chuyên sâu về phân tích dữ liệu, quản trị dữ liệu và an ninh mạng tại các cơ sở giáo dục đại học, viện nghiên cứu và học viện chuyên ngành. Các chương trình này phải được thiết kế theo hướng thực hành, cập nhật thường xuyên các tiến bộ khoa học – công nghệ, đồng thời gắn kết chặt chẽ với nhu cầu thực tiễn của cơ quan nhà nước, doanh nghiệp và tổ chức trung gian dữ liệu. Đặc biệt, phải ưu tiên xây dựng chương trình đào tạo liên ngành giữa công nghệ thông tin, phân tích dữ liệu, luật pháp, đạo đức số và kỹ năng lãnh đạo. Việc tổ chức đào tạo cần được triển khai theo nhiều hình thức: chính quy dài hạn, ngắn hạn chuyên sâu, đào tạo tại chỗ, đào tạo trực tuyến và chương trình trao đổi quốc tế. Đào tạo phải lấy người học làm trung tâm, khuyến khích tư duy phản biện, sáng tạo và làm chủ công nghệ thay vì học thuộc, máy móc.

Xây dựng mạng lưới chuyên gia dữ liệu quốc gia là yêu cầu cấp thiết nhằm phát huy sức mạnh tổng hợp, kết nối cộng đồng tri thức và đẩy nhanh ứng dụng dữ liệu trong mọi lĩnh vực. Cần hình thành các hội đồng chuyên gia dữ liệu ở cấp trung ương và địa phương để tham mưu chính sách, tư vấn kỹ thuật, phản biện chiến lược phát triển dữ liệu. Mạng lưới này phải bao gồm các nhà khoa học, chuyên gia công nghệ, nhà quản lý và đại diện doanh nghiệp có kinh nghiệm thực tiễn, được tổ chức linh hoạt theo ngành, lĩnh vực, khu vực địa lý. Các cơ chế khuyến khích chuyên gia trong và ngoài nước tham gia tư vấn, đào tạo và phát triển nhân lực dữ liệu cần được luật hóa, nhất là cơ chế đặt hàng, chuyển giao công nghệ, tài trợ nghiên cứu và công nhận trình độ theo năng lực thực tế thay vì bằng cấp hình thức.

Thực hiện kiểm kê, đánh giá và phân loại nguồn nhân lực dữ liệu hiện có trong hệ thống cơ quan nhà nước là nhiệm vụ quan trọng để xác định nhu cầu đào tạo, bổ sung và luân chuyển cán bộ hợp lý. Cần xây dựng hệ thống cơ sở dữ liệu nhân sự ngành dữ liệu quốc gia, tích hợp với hệ thống dữ liệu cán bộ, công chức, viên chức hiện hành để quản lý tập trung, thống nhất và hỗ trợ ra quyết định điều phối nhân lực phù hợp với yêu cầu nhiệm vụ của từng bộ, ngành, địa phương. Việc đánh giá cán bộ dữ liệu cần căn cứ trên hiệu suất công việc, khả năng đổi mới, mức độ hiểu biết công nghệ, năng lực tư duy hệ thống và đạo đức nghề nghiệp. Cần có chính sách khen thưởng, đãi ngộ đặc thù để thu hút, giữ chân và phát triển nguồn nhân lực chất lượng cao.

Khuyến khích hình thành các trung tâm nghiên cứu, đào tạo và chuyển giao công nghệ về dữ liệu tại các trường đại học, viện nghiên cứu và doanh nghiệp lớn, tạo môi trường học thuật – thực tiễn liên thông để phát triển chuyên gia. Những trung tâm này cần đóng vai trò là hạt nhân sáng tạo, nơi phát triển các thuật toán mới, mô hình phân tích tiên tiến và giải pháp bảo mật dữ liệu thông minh, đồng thời cung cấp dịch vụ đào tạo và tư vấn cho khu vực công – tư. Nhà nước cần có chính sách

hỗ trợ khởi nghiệp sáng tạo trong lĩnh vực phân tích và quản trị dữ liệu, tạo điều kiện để chuyên gia trẻ thể hiện năng lực và cống hiến. Việc thúc đẩy hợp tác quốc tế giữa các trung tâm dữ liệu trong nước với tổ chức nghiên cứu toàn cầu sẽ tạo điều kiện thuận lợi để tiếp cận công nghệ mới, phương pháp đào tạo hiện đại và chuẩn mực quốc tế về quản trị dữ liệu.

Xây dựng chương trình liên thông đào tạo giữa các cấp học, ngành học để hình thành đội ngũ chuyên gia dữ liệu trong tương lai là nhiệm vụ chiến lược. Cần đưa các kiến thức cơ bản về dữ liệu và tư duy số vào chương trình giáo dục phổ thông, khơi dậy niềm yêu thích và định hướng nghề nghiệp sớm cho học sinh. Ở bậc đại học, các ngành công nghệ thông tin, toán ứng dụng, thống kê, kinh tế, luật và an ninh mạng cần được tích hợp đào tạo kiến thức liên ngành về dữ liệu, với định hướng hình thành các chuyên ngành mới như khoa học dữ liệu, kỹ thuật dữ liệu, luật dữ liệu và đạo đức số. Chính phủ cần khuyến khích các trường đại học xây dựng chương trình đào tạo đạt chuẩn quốc tế, cấp bằng song ngành và hợp tác với doanh nghiệp để đào tạo theo nhu cầu thực tiễn.

Xây dựng hệ sinh thái học tập suốt đời cho cán bộ dữ liệu là điều kiện tiên quyết để bảo đảm năng lực cập nhật, thích ứng và đổi mới sáng tạo liên tục. Cần phát triển các nền tảng học tập trực tuyến mở (MOOC) quốc gia về dữ liệu, kết nối với các thư viện điện tử, tài nguyên học liệu số và mạng lưới cố vấn chuyên gia để hỗ trợ người học mọi lúc, mọi nơi. Cơ chế công nhận tín chỉ học tập trực tuyến, cấp chứng chỉ kỹ năng nghề nghiệp, học qua trải nghiệm thực tế và chứng nhận năng lực dựa trên sản phẩm/dự án thay vì bằng cấp truyền thống cần được thể chế hóa, tạo điều kiện cho mọi người, đặc biệt là cán bộ đang công tác, được học tập linh hoạt và hiệu quả. Việc kết hợp giữa học tập chính quy và phi chính quy sẽ giúp xây dựng đội ngũ cán bộ dữ liệu có khả năng hội nhập, phản ứng linh hoạt với thay đổi công nghệ và bối cảnh toàn cầu.

Nghị quyết 57: Hệ sinh thái dữ liệu - nền tảng chủ quyền số quốc gia.

Triển khai cơ chế tuyển dụng, bổ nhiệm và sử dụng cán bộ quản lý dữ liệu theo hướng cạnh tranh, minh bạch, dựa trên năng lực thực tiễn và thành tích đổi mới sáng tạo. Các vị trí chủ chốt trong hệ thống quản lý dữ liệu quốc gia, bao gồm giám đốc dữ liệu (Chief Data Officer), chuyên gia an toàn thông tin, cán bộ phân tích dữ liệu cấp chiến lược cần được xác lập tiêu chuẩn cụ thể, gắn với trách nhiệm pháp lý và quyền hạn tương xứng. Cần tách bạch giữa chức năng kỹ thuật, hành chính và quản lý để chuyên môn hóa đội ngũ và nâng cao hiệu quả điều hành. Những cán bộ có trình độ cao, được đào tạo chuyên sâu

và có kinh nghiệm quốc tế cần được bố trí vào các vị trí trung tâm để lan tỏa tri thức, dẫn dắt đổi mới và xây dựng văn hóa dữ liệu trong toàn hệ thống.

Tăng cường giám sát, đánh giá và kiểm định chất lượng đào tạo nhân lực dữ liệu là điều kiện để bảo đảm hiệu quả đầu tư công và nâng cao chất lượng đầu ra. Cần thiết lập bộ chỉ số đánh giá năng lực cán bộ dữ liệu quốc gia, bao gồm năng lực công nghệ, tư duy hệ thống, kỹ năng phân tích và đạo đức nghề nghiệp. Việc kiểm định chương trình đào tạo, cơ sở đào tạo và giảng viên phải được thực hiện độc lập, công khai và định kỳ, kết hợp giữa đánh giá nội bộ, đánh giá ngoài và phản hồi của người học/doanh nghiệp sử dụng lao động. Các cơ quan nhà nước cần đóng vai trò trung tâm trong việc bảo đảm chất lượng đầu ra thông qua việc đặt hàng đào tạo, xác lập chuẩn đầu vào, kiểm tra đầu ra và gắn kết nhu cầu nhân lực với chiến lược phát triển ngành, địa phương.

Liên hệ với nhiệm vụ của lực lượng Công an, việc phát triển đội ngũ cán bộ dữ liệu chất lượng cao đóng vai trò then chốt trong việc bảo đảm an ninh quốc gia, an ninh mạng và phòng chống tội phạm công nghệ cao. Trong bối cảnh tội phạm mạng ngày càng tinh vi, có yếu tố nước ngoài và tận dụng tối đa khoảng trống dữ liệu để hoạt động, lực lượng Công an cần chủ động đào tạo chuyên sâu các chuyên gia phân tích dữ liệu tội phạm, chuyên viên bảo mật hệ thống, cán bộ điều tra số và cán bộ quản lý dữ liệu nghiệp vụ. Việc xây dựng lực lượng này không chỉ phục vụ đấu tranh phòng chống tội phạm mà còn góp phần hoạch định chính sách, dự báo nguy cơ, phát hiện sớm hành vi bất thường và bảo vệ quyền dữ liệu của công dân. Các học viện, trường Công an nhân dân cần trở thành trung tâm đào tạo mũi nhọn về dữ liệu trong ngành nội chính, kết hợp đào tạo chuyên sâu với rèn luyện bản lĩnh chính trị, kỹ năng tác chiến trong môi trường số, góp phần xây dựng lực lượng Công an nhân dân cách mạng, chính quy, tinh nhuệ, hiện đại.

6.3. Đẩy mạnh hợp tác quốc tế về dữ liệu thông qua việc ký kết, tham gia các điều ước, hiệp định song phương, đa phương về dữ liệu xuyên biên giới, bảo mật và chia sẻ dữ liệu công – tư

Đẩy mạnh hợp tác quốc tế về dữ liệu là một yêu cầu tất yếu trong bối cảnh toàn cầu hóa thông tin và chuyển đổi số đang diễn ra mạnh mẽ trên phạm vi toàn thế giới. Khi dữ liệu đã trở thành một loại tài nguyên chiến lược, có tác động sâu sắc đến mọi mặt của đời sống xã hội và an ninh quốc gia, việc thúc đẩy hợp tác quốc tế nhằm tạo hành lang pháp lý, kỹ thuật và thể chế cho việc chia sẻ, bảo vệ và khai thác dữ liệu là vô cùng cần thiết. Việt Nam cần chủ động, tích cực tham gia xây dựng và ký kết các điều ước quốc tế, hiệp định song phương, đa phương có liên quan đến dữ liệu xuyên biên giới, vừa bảo đảm chủ quyền dữ liệu quốc gia, vừa mở rộng khả năng tiếp cận và trao đổi dữ liệu phục vụ phát triển kinh tế – xã hội, quốc phòng – an ninh, và hội nhập quốc tế sâu rộng.

Cần tổ chức rà soát và đánh giá hệ thống các hiệp định, cam kết quốc tế đã ký kết hoặc đang tham gia, đặc biệt là các cam kết liên quan đến Tổ chức Thương mại Thế giới (WTO), Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP), Hiệp định Đối tác Kinh tế Toàn diện Khu vực (RCEP), Hiệp định Thương mại tự do Việt Nam – EU (EVFTA), và các hiệp định thương mại song phương có điều khoản liên quan đến dữ liệu và thương mại số. Trên cơ sở đánh giá, cần xác định các điểm tương đồng, khác biệt, các khoảng trống pháp lý để điều chỉnh phù hợp với xu thế toàn cầu hóa dữ liệu, đặc biệt trong các vấn đề bảo mật, quyền riêng tư, tiêu chuẩn kỹ thuật và mô hình chia sẻ dữ liệu công – tư.

Thúc đẩy quá trình nghiên cứu và đàm phán các hiệp định mới phù hợp với nhu cầu, lợi ích và năng lực quốc gia. Trong các cuộc đàm phán hợp tác, Việt Nam cần đưa ra các đề xuất cụ thể nhằm bảo vệ quyền lợi của người dân và doanh nghiệp,

không chấp nhận các điều khoản ép buộc, gây bất lợi cho an ninh dữ liệu quốc gia. Các thỏa thuận cần hướng đến xây dựng các nguyên tắc chung về quyền sở hữu dữ liệu, phạm vi và điều kiện chia sẻ dữ liệu, trách nhiệm của các bên khi xảy ra rò rỉ dữ liệu, xâm phạm quyền riêng tư hoặc tấn công mạng, cũng như quy định về kiểm soát luồng dữ liệu ra vào lãnh thổ quốc gia một cách minh bạch, công bằng và có kiểm soát.

Xây dựng cơ chế phối hợp liên ngành chặt chẽ trong quá trình đàm phán, ký kết và thực thi các cam kết quốc tế về dữ liệu. Bộ Ngoại giao, Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng, Bộ Tư pháp, Bộ Công thương và các cơ quan liên quan cần được phân công rõ ràng vai trò, trách nhiệm để đảm bảo tiếng nói thống nhất trong các diễn đàn quốc tế. Mỗi cơ quan không chỉ chịu trách nhiệm về lĩnh vực chuyên môn mà còn phải phối hợp để nhận diện nguy cơ, thách thức và cơ hội từ các dòng dữ liệu xuyên biên giới đối với chủ quyền, quyền riêng tư cá nhân, và năng lực cạnh tranh của doanh nghiệp Việt Nam.

Phát triển năng lực pháp lý và kỹ thuật để đáp ứng các yêu cầu mới trong quá trình hội nhập. Việt Nam cần khẩn trương nghiên cứu, hoàn thiện hệ thống pháp luật trong nước phù hợp với các cam kết quốc tế về dữ liệu, bao gồm Luật Dữ liệu quốc gia, Luật Bảo vệ dữ liệu cá nhân, và các văn bản dưới luật liên quan. Các quy định pháp luật này phải đảm bảo nguyên tắc chủ quyền dữ liệu, quyền kiểm soát của công dân đối với thông tin cá nhân, đồng thời tạo điều kiện thuận lợi cho việc chia sẻ dữ liệu giữa các cơ quan, tổ chức, cá nhân trong và ngoài nước, trên cơ sở hài hòa lợi ích giữa Nhà nước, doanh nghiệp và người dân.

Đẩy mạnh tham gia các diễn đàn, sáng kiến quốc tế về quản trị dữ liệu, bao gồm Diễn đàn Kinh tế Thế giới (WEF), Nhóm G20, ASEAN Digital Ministers' Meeting (ADGMIN), Diễn đàn Hợp tác Kinh tế châu Á – Thái Bình Dương (APEC), Diễn đàn Quản trị Internet (IGF), và các tổ chức thiết lập tiêu chuẩn dữ liệu toàn cầu như ISO, ITU. Qua đó, Việt Nam có thể tiếp cận và đóng góp vào việc xây dựng các quy tắc ứng xử, bộ tiêu chuẩn chung về bảo mật, chia sẻ dữ liệu và chống phân mảnh không gian số, từ đó nâng cao vị thế quốc gia trong chuỗi giá trị dữ liệu toàn cầu.

Tăng cường hợp tác song phương với các quốc gia có nền công nghệ phát triển như Hoa Kỳ, Nhật Bản, Hàn Quốc, Đức, Úc, Singapore để trao đổi kinh nghiệm, hỗ trợ kỹ thuật, chuyển giao công nghệ và nâng cao năng lực quản lý dữ liệu. Việc ký kết các bản ghi nhớ, thỏa thuận hợp tác về dữ liệu công – tư, an ninh mạng, bảo mật thông tin cá nhân không chỉ giúp Việt Nam học hỏi cách xây dựng thể chế dữ liệu hiệu quả mà còn góp phần thúc đẩy thương mại điện tử, đầu tư công nghệ và tăng tính minh bạch trong quản trị nhà nước.

Phát triển hạ tầng kỹ thuật, đặc biệt là hệ thống định danh điện tử quốc gia, các nền tảng tích hợp dữ liệu, trung tâm dữ liệu quốc gia, hệ thống bảo mật đạt chuẩn quốc tế để đảm bảo khả năng tiếp nhận và chia sẻ dữ liệu xuyên biên giới. Đây là điều kiện tiên quyết để đáp ứng các yêu cầu về kết nối, tin cậy và an toàn trong các hiệp định quốc tế. Cần xây dựng cơ chế giám sát kỹ thuật đối với việc truy cập, truyền dẫn dữ liệu ra nước ngoài để kiểm soát nguy cơ rò rỉ, thất thoát dữ liệu trọng yếu liên quan đến an ninh quốc gia và quyền lợi công dân.

Thúc đẩy các mô hình chia sẻ dữ liệu công – tư giữa các cơ quan nhà nước và doanh nghiệp thông qua cơ chế hợp tác rõ ràng về quyền sử dụng, quyền sở hữu dữ liệu, phân chia lợi ích và trách nhiệm pháp lý. Cần học hỏi các mô hình thành

công như Data Trust, Data Cooperative tại châu Âu, Bắc Mỹ để xây dựng khung hợp tác dữ liệu minh bạch, hiệu quả, vừa khuyến khích đổi mới sáng tạo, vừa bảo đảm an toàn thông tin. Việc thiết lập các trung tâm trung gian dữ liệu (data intermediary) có sự tham gia giám sát của cả khu vực công và tư nhân cũng là một hướng đi quan trọng để điều phối luồng dữ liệu giữa các bên liên quan trong và ngoài nước.

Tăng cường đào tạo nguồn nhân lực chất lượng cao, có hiểu biết sâu sắc về pháp luật quốc tế, công nghệ dữ liệu, đạo đức dữ liệu và an ninh mạng để phục vụ cho các hoạt động hợp tác quốc tế về dữ liệu. Việc xây dựng đội ngũ chuyên gia về pháp lý dữ liệu, kỹ sư dữ liệu xuyên biên giới, và cán bộ ngoại giao số là nhiệm vụ cấp thiết nhằm đảm bảo chủ động trong các cuộc đàm phán và thực thi các hiệp định quốc tế, tránh lệ thuộc vào chuyên gia nước ngoài hoặc bên thứ ba trong xử lý tranh chấp.

Thiết lập cơ chế đánh giá định kỳ về tác động của các hiệp định dữ liệu xuyên biên giới đối với kinh tế – xã hội, an ninh – quốc phòng và quyền riêng tư công dân. Trên cơ sở đó, cần có các điều chỉnh kịp thời về thể chế, kỹ thuật, mô hình hợp tác để bảo đảm lợi ích quốc gia trong bối cảnh dữ liệu đang trở thành một lĩnh vực cạnh tranh chiến lược giữa các quốc gia. Việc xây dựng các công cụ giám sát và cảnh báo sớm về rủi ro an ninh dữ liệu quốc tế cũng cần được tích hợp vào các kế hoạch hợp tác quốc tế về dữ liệu.

Ứng dụng NDA Key được coi là "lá chắn số" trên không gian mạng. (Nguồn: NDA)

Trong quá trình đẩy mạnh hợp tác quốc tế về dữ liệu, lực lượng Công an nhân dân có vai trò đặc biệt trong việc bảo vệ an ninh dữ liệu quốc gia, phòng chống các hành vi gián điệp mạng, tội phạm công nghệ cao và xâm phạm quyền riêng tư công dân. Công an các cấp cần chủ động tham mưu, phối hợp với các cơ quan chức năng trong việc thẩm định, đánh giá rủi ro an ninh mạng trong các hiệp định dữ liệu xuyên biên giới, từ đó có các phương án kiểm soát chặt chẽ luồng dữ liệu

ra nước ngoài, không để xảy ra sơ hở trong việc chia sẻ dữ liệu công – tư. Đồng thời, cần nâng cao năng lực điều tra, phát hiện và xử lý các hành vi vi phạm pháp luật về an ninh dữ liệu, xây dựng mạng lưới hợp tác quốc tế giữa lực lượng công an Việt Nam với các tổ chức thực thi pháp luật nước ngoài trong trao đổi thông tin, truy vết và ngăn chặn tội phạm sử dụng dữ liệu để thực hiện hành vi khủng bố, xuyên tạc, phá hoại. Lực lượng Công an phải là trụ cột trong việc gìn giữ chủ quyền không gian mạng và đảm bảo rằng quá trình hợp tác quốc tế về dữ liệu luôn đặt lợi ích và an ninh quốc gia lên hàng đầu.

7. Triển khai các mô hình thí điểm ứng dụng dữ liệu trong quản trị công và dịch vụ công, làm cơ sở nhân rộng các mô hình hiệu quả trong các lĩnh vực như y tế, giáo dục, giao thông, tài chính.

Việc triển khai các mô hình thí điểm ứng dụng dữ liệu trong quản trị công và dịch vụ công là một bước đi chiến lược, góp phần chuyển đổi phương thức điều hành, cung ứng dịch vụ của bộ máy nhà nước theo hướng minh bạch, linh hoạt và lấy người dân, doanh nghiệp làm trung tâm. Trước hết, cần xác lập cơ chế lựa chọn lĩnh vực ưu tiên để triển khai mô hình thí điểm dựa trên mức độ sẵn sàng dữ liệu, tính chất cấp thiết của dịch vụ và tiềm năng tác động xã hội. Các lĩnh vực như y tế, giáo dục, giao thông và tài chính là những khu vực thiết yếu, có mật độ tương tác lớn giữa chính quyền với người dân, thường xuyên phát sinh các nhu cầu dịch vụ công, đồng thời cũng là nơi tạo ra lượng dữ liệu lớn và có giá trị phục vụ điều hành.

Để triển khai thí điểm hiệu quả, cần thành lập tổ công tác liên ngành bao gồm các chuyên gia về dữ liệu, công nghệ thông tin, quản trị công và đại diện các bộ, ngành liên quan nhằm đảm bảo sự phối hợp đồng bộ từ khâu thiết kế, thử nghiệm đến đánh giá hiệu quả mô hình. Tổ công tác này có nhiệm vụ xây dựng tiêu chí lựa chọn địa phương, đơn vị tham gia thí điểm; xác định hạ tầng kỹ thuật cần thiết; lựa chọn nền tảng công nghệ mở, an toàn và tương thích với hệ sinh thái dữ liệu quốc gia. Các địa phương hoặc bộ, ngành được lựa chọn triển khai thí điểm cần cam kết mạnh mẽ về chính trị, tổ chức và nhân lực, tạo lập nhóm triển khai chuyên trách có khả năng vận hành, điều chỉnh kịp thời các mô hình trong thực tiễn.

Trong lĩnh vực y tế, mô hình thí điểm có thể tập trung vào việc xây dựng hệ thống hồ sơ sức khỏe điện tử liên thông giữa các cơ sở y tế, giúp nâng cao hiệu quả khám chữa bệnh, giảm chi phí chẩn đoán trùng lặp và hỗ trợ công tác phòng, chống dịch bệnh. Dữ liệu thu thập từ các trạm y tế xã, bệnh viện tuyến huyện và tỉnh sẽ được số hóa, lưu trữ trên nền tảng bảo mật cao, từ đó phục vụ phân tích xu hướng bệnh tật, dự báo nhu cầu thuốc men, hỗ trợ ra quyết định cho cơ quan quản lý nhà nước. Thí điểm có thể mở rộng sang việc ứng dụng trí tuệ nhân tạo trong đọc kết quả cận lâm sàng, phân tích hình ảnh y khoa nhằm hỗ trợ bác sĩ trong chẩn đoán và điều trị.

Công an tỉnh Cà Mau tổ chức thu nhận mẫu ADN thân nhân liệt sĩ chưa xác định danh tính. Ảnh Sưu tầm

Trong lĩnh vực giáo dục, mô hình thí điểm có thể tập trung vào xây dựng hệ thống học bạ điện tử, quản lý hồ sơ học sinh – sinh viên, quá trình học tập, điểm số, kết quả thi và hành vi học tập từ mầm non đến đại học. Việc tích hợp và phân tích dữ liệu này sẽ giúp nhà trường có phương án giảng dạy phù hợp với từng cá nhân, hỗ trợ phát hiện học sinh có nguy cơ bỏ học sớm hoặc cần hỗ trợ đặc biệt. Đồng thời, dữ liệu giáo dục sẽ là cơ sở để cơ quan quản lý nhà nước điều chỉnh chính sách

giáo dục, phân bổ ngân sách, đầu tư hạ tầng một cách hiệu quả hơn. Mô hình này cũng giúp phụ huynh dễ dàng theo dõi tiến trình học tập của con em thông qua ứng dụng trên điện thoại thông minh, tăng cường sự kết nối giữa nhà trường và gia đình.

Trong lĩnh vực giao thông, mô hình thí điểm có thể triển khai ở các đô thị lớn với hệ thống cảm biến, camera, bản đồ số để thu thập dữ liệu thời gian thực về lưu lượng phương tiện, mức độ ùn tắc, tình trạng tai nạn. Trên cơ sở đó, cơ quan quản lý giao thông có thể tự động điều phối đèn tín hiệu, hướng dẫn dòng xe, cảnh báo khu vực có sự cố, từ đó nâng cao hiệu quả điều hành và giảm thiểu tai nạn. Bên cạnh đó, dữ liệu về hành vi lái xe, mức độ tuân thủ luật giao thông có thể được phân tích để xây dựng hệ thống điểm tín nhiệm giao thông, làm cơ sở cho việc đánh giá và cấp lại giấy phép lái xe. Việc thí điểm cũng có thể mở rộng ra các mô hình vận tải công cộng thông minh, tích hợp dữ liệu từ các tuyến xe buýt, tàu điện, phương tiện chia sẻ để tối ưu hóa tuyến đường và giờ hoạt động.

Trong lĩnh vực tài chính công, mô hình thí điểm ứng dụng dữ liệu tập trung vào việc xây dựng hệ thống quản lý ngân sách điện tử, theo dõi thu – chi ngân sách theo thời gian thực, phân tích hiệu quả chi tiêu công và phát hiện các dấu hiệu rủi ro tham nhũng. Thông qua việc thu thập và phân tích dữ liệu từ các cơ quan thuế, kho bạc, hải quan, có thể thiết lập hệ thống cảnh báo sớm các hành vi gian lận tài chính, đồng thời tăng cường tính minh bạch trong quá trình phân bổ và sử dụng ngân sách nhà nước. Việc kết nối dữ liệu giữa các cơ quan quản lý tài chính và đơn vị cung ứng dịch vụ công cũng tạo điều kiện cho việc thanh toán điện tử, giảm thiểu tiền mặt và gia tăng khả năng kiểm soát dòng tiền công.

Việc triển khai các mô hình thí điểm cần được gắn liền với cơ chế đánh giá toàn diện về hiệu quả, tác động, tính mở rộng và sự hài lòng của người dân. Các bộ chỉ số đánh giá cần bao gồm cả khía cạnh kỹ thuật (mức độ hoàn thiện hệ thống,

an ninh mạng, tốc độ xử lý dữ liệu), khía cạnh quản trị (tính minh bạch, hiệu quả vận hành, năng lực cán bộ) và khía cạnh xã hội (mức độ tiếp cận, tiện ích đối với người dân). Kết quả của mô hình thí điểm phải được báo cáo định kỳ lên các cấp có thẩm quyền, công bố rộng rãi để khuyến khích phản hồi từ xã hội và điều chỉnh mô hình kịp thời trước khi triển khai nhân rộng. Đồng thời, cần xây dựng cơ chế hỗ trợ tài chính, kỹ thuật cho các địa phương, đơn vị có kết quả thí điểm tốt nhằm khuyến khích đổi mới sáng tạo trong khu vực công.

Trung tâm Sáng tạo, khai thác dữ liệu thuộc Trung tâm Dữ liệu quốc gia và Hiệp hội Dữ liệu quốc gia đã chính thức giới thiệu 6 sản phẩm dữ liệu lõi tiên phong, do chính người Việt nghiên cứu, phát triển và làm chủ toàn diện. Nguồn từ Internet.

Để thúc đẩy nhân rộng mô hình hiệu quả sau thí điểm, cần có chính sách chuẩn hóa quy trình triển khai, xây dựng bộ khung kỹ thuật, quy định bảo mật dữ liệu, tiêu chuẩn kết nối và liên thông giữa các hệ thống. Việc hình thành các nền tảng chia sẻ dữ liệu dùng chung là yêu cầu thiết yếu nhằm tránh tình trạng phân mảnh, trùng lặp và lãng phí nguồn lực. Ngoài ra, cần nâng cao năng lực cho đội ngũ cán bộ công chức về quản trị dữ liệu, phân tích dữ liệu và sử dụng hệ thống kỹ thuật số trong điều hành, thông qua các chương trình đào tạo chuyên sâu, cấp chứng chỉ và hỗ trợ kỹ thuật thường xuyên. Việc thiết lập mạng lưới chuyên gia, trung tâm hỗ trợ triển khai mô hình tại các bộ, ngành và địa phương cũng là yếu tố then chốt để duy trì và mở rộng quy mô các ứng dụng dữ liệu.

Một yếu tố quan trọng bảo đảm sự thành công của các mô hình thí điểm là khuyến khích sự tham gia của khu vực tư nhân và cộng đồng trong quá trình thiết kế, vận hành và đánh giá mô hình. Các doanh nghiệp công nghệ có thể đóng vai trò cung cấp giải pháp kỹ thuật, chia sẻ kinh nghiệm triển khai, đồng đầu tư hoặc cung cấp hạ tầng theo mô hình đối tác công – tư (PPP). Người dân có thể tham gia đóng góp dữ liệu, phản ánh chất lượng dịch vụ công, từ đó góp phần hoàn thiện mô hình. Cơ chế chính sách cần bảo đảm quyền lợi, bảo vệ dữ liệu cá nhân và tạo môi trường khuyến khích sáng tạo, kết nối hệ sinh thái đổi mới sáng tạo quốc gia với quá trình cải cách hành chính và chuyển đổi số trong khu vực công.

Việc triển khai mô hình thí điểm ứng dụng dữ liệu trong quản trị công và dịch vụ công là tiền đề để lực lượng Công an nhân dân nghiên cứu, phát triển các mô hình tương tự phục vụ công tác đảm bảo an ninh trật tự, phòng ngừa tội phạm và nâng cao hiệu quả quản lý nhà nước về an ninh. Dữ liệu từ các lĩnh vực y tế, giáo dục, giao thông hay tài chính có thể được tích hợp, phân tích để nhận diện các nguy cơ an ninh phi truyền thống, hỗ trợ điều tra, truy vết đối tượng phạm tội, phát hiện hành vi lừa đảo, chiếm đoạt tài sản qua mạng, hay quản lý cư trú và di biến động dân cư. Bên cạnh đó, lực lượng Công an cũng có

thể chủ động triển khai thí điểm các nền tảng dữ liệu lớn trong lĩnh vực quản lý cư trú, căn cước công dân, an ninh mạng và trật tự đô thị, góp phần hình thành Chính phủ số an toàn, hiệu quả và vì nhân dân phục vụ.

***

Tạm kết câu 8

Phần trả lời câu hỏi số 8 đã làm rõ các nội dung cốt lõi trong quản lý nhà nước về dữ liệu, bao gồm: xây dựng và hoàn thiện thể chế pháp luật; tổ chức thu thập, xử lý, khai thác, chia sẻ, bảo vệ và lưu trữ dữ liệu; bảo đảm an ninh, an toàn dữ liệu; kiểm tra, thanh tra, xử lý vi phạm và hợp tác quốc tế. Bộ Công an giữ vai trò nòng cốt trong bảo đảm an ninh dữ liệu quốc gia, tổ chức thực hiện các chính sách, giải pháp bảo vệ hệ thống dữ liệu trọng yếu, đồng thời hướng dẫn, kiểm tra, đôn đốc công an các đơn vị, địa phương thực hiện nhiệm vụ được giao. Từ nay đến năm 2030, nhiệm vụ trọng tâm là hoàn thiện hành lang pháp lý, hiện đại hóa hạ tầng dữ liệu, phát triển nhân lực chất lượng cao, nâng cao năng lực giám sát – ứng phó sự cố và đẩy mạnh hợp tác công – tư trong quản lý dữ liệu phục vụ phát triển bền vững.

Lời kết

Cuộc thi tìm hiểu Luật Dữ liệu trong Công an nhân dân không chỉ là một hoạt động chuyên môn thuần túy, mà còn là đợt sinh hoạt chính trị sâu rộng, thiết thực và giàu ý nghĩa. Qua hành trình nghiên cứu, suy ngẫm và lan tỏa, mỗi cán bộ, chiến sĩ có cơ hội được tiếp cận, hiểu đúng, hiểu sâu và nâng cao ý thức trách nhiệm đối với nhiệm vụ bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội trong kỷ nguyên số. Có thể nói, Luật Dữ liệu không chỉ là một công cụ pháp lý, mà còn là biểu hiện của tầm nhìn chiến lược, khẳng định vị thế quốc gia và sứ mệnh của lực lượng Công an nhân dân trong việc giữ vững chủ quyền dữ liệu, bảo vệ an ninh mạng, an toàn thông tin, vì lợi ích của Tổ quốc và Nhân dân.

Bài dự thi của Nhóm chúng tôi đã tập trung làm rõ tám nội dung cốt lõi, thể hiện đầy đủ tinh thần nghiên cứu, trách nhiệm và tâm huyết của một chiến sĩ công an nhân dân trước yêu cầu cấp thiết của thực tiễn. Từ việc tìm hiểu chính sách pháp luật về dữ liệu của các nước trên thế giới đến sự cần thiết xây dựng khung pháp lý dữ liệu tại Việt Nam, nhóm tác giả nhận thức sâu sắc rằng bảo vệ dữ liệu không chỉ là bảo vệ thông tin, mà còn là bảo vệ niềm tin, giá trị cốt lõi của quốc gia trong kỷ nguyên số. Việc phân tích quyền, nghĩa vụ và cơ chế bảo đảm thực thi các quyền dữ liệu cho thấy rõ nét hướng tiếp cận quyền con người trong chính sách pháp luật hiện đại của Việt Nam – lấy con người làm trung tâm, dữ liệu phục vụ con người và do con người làm chủ. Bên cạnh đó, các nội dung về hành vi bị nghiêm cấm, hoạt động đổi mới sáng tạo trong lĩnh vực dữ liệu, quy định về khai thác, chia sẻ dữ liệu trong cơ sở dữ liệu tổng hợp quốc gia hay trách nhiệm của Trung tâm dữ liệu quốc gia đã được luận giải một cách thấu đáo, vừa thể hiện chiều sâu lý luận, vừa bám sát thực tiễn phát triển của hạ tầng số quốc gia.

Từ đó, khẳng định rằng nếu không có một chiến lược dữ liệu thống nhất, minh bạch và an toàn, Việt Nam sẽ khó có thể chuyển mình mạnh mẽ trong cuộc đua toàn cầu về kinh tế số và quản trị thông minh.

Đặc biệt, với lực lượng Công an nhân dân – cơ quan chủ trì, tiên phong trong quản lý nhà nước về dữ liệu, bài dự thi đã nêu bật được vai trò then chốt của Bộ Công an và Công an các đơn vị, địa phương trong thực hiện nhiệm vụ: từ xây dựng Trung tâm dữ liệu quốc gia, triển khai các sản phẩm dữ liệu bảo mật, cho đến tham gia các hiệp định quốc tế về chia sẻ dữ liệu, trao đổi cảnh báo sớm và phối hợp xử lý sự cố xuyên biên giới. Những nhiệm vụ trọng tâm đặt ra từ nay đến năm 2030 chính là kim chỉ nam để lực lượng Công an không ngừng đổi mới, nâng cao năng lực công nghệ, chủ động ứng phó với thách thức an ninh phi truyền thống, đặc biệt là tội phạm mạng, tội phạm sử dụng công nghệ cao.

Cuộc thi ***"Tìm hiểu Luật Dữ liệu trong Công an nhân dân"*** vì thế không đơn thuần là một đợt sinh hoạt chính trị sâu rộng, mà là nơi hội tụ trí tuệ, trách nhiệm và khát vọng đổi mới của những người lính thời đại số. Với chúng tôi – những chiến sĩ Công an tỉnh Cà Mau, nơi tận cùng đất nước nhưng luôn trọn vẹn ý chí và lòng trung thành – Cuộc thi này là cơ hội quý báu để hun đúc tinh thần học tập, rèn luyện bản lĩnh chính trị, nhận diện rõ ràng hơn vai trò của mình trong công cuộc chuyển đổi số toàn diện của lực lượng. Mỗi dòng chữ viết ra không chỉ phản ánh nhận thức cá nhân, mà còn là lời hứa, là cam kết về sự tận tụy phụng sự, sẵn sàng góp phần vào sự nghiệp xây dựng *"nền dữ liệu Việt Nam thống nhất, đồng bộ, an toàn, hiện đại và giàu bản sắc dân tộc"* như Tổng Bí thư Tô Lâm đã định hướng.

Cuộc thi rồi sẽ khép lại, nhưng những giá trị, nhận thức và động lực từ đó sẽ còn lan tỏa, sẽ tiếp tục tiếp sức cho hành trình xây dựng lực lượng Công an nhân dân cách mạng, chính quy, tinh nhuệ, hiện đại, đủ năng lực làm chủ không gian số, đủ bản lĩnh gìn giữ sự thật, bảo vệ Đảng, Nhà nước và Nhân dân trong thời đại dữ liệu. Đó là vinh dự, là trách nhiệm, là mệnh lệnh từ trái tim người chiến sĩ Công an giữa thời đại mới.

Xin chân thành cám ơn và Lễ phép kính chào.

DANH MỤC TÀI LIỆU THAM KHẢO

1. Ban Chấp hành Trung ương (2018), Nghị quyết số 23-NQ/TW ngày 22/3/2018 của Bộ Chính trị về định hướng xây dựng chính sách phát triển công nghiệp quốc gia đến năm 2030, tầm nhìn đến năm 2045.
2. Ban Chấp hành Trung ương (2019), Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư.
3. Ban Chấp hành Trung ương (2024), Kết luận số 69-KL/TW ngày 11/01/2024 của Bộ Chính trị tiếp tục thực hiện Nghị quyết số 20-NQ/TW, ngày 01/11/2012 của Ban Chấp hành Trung ương Đảng khóa XI về phát triển khoa học và công nghệ phục vụ sự nghiệp công nghiệp hóa, hiện đại hóa trong điều kiện kinh tế thị trường định hướng xã hội chủ nghĩa và hội nhập quốc tế.
4. Ban Chấp hành Trung ương (2022), Nghị quyết số 29-NQ/TW ngày 17/11/2022 Hội nghị lần thứ sáu Ban Chấp hành Trung ương Đảng khóa XIII về tiếp tục đẩy mạnh công nghiệp hóa, hiện đại hóa đất nước đến năm 2030, tầm nhìn đến năm 2045.
5. Ban Chấp hành Trung ương (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.

6. Ban Chấp hành Trung ương (2024), Kết luận số 69-KL/TW ngày 11/01/2024 của Bộ Chính trị tiếp tục thực hiện Nghị quyết số 20-NQ/TW, ngày 01/11/2012 của Ban Chấp hành Trung ương Đảng khóa XI về phát triển khoa học và công nghệ phục vụ sự nghiệp công nghiệp hóa, hiện đại hóa trong điều kiện kinh tế thị trường định hướng xã hội chủ nghĩa và hội nhập quốc tế.
7. Báo Công an nhân dân (2024), Xây dựng cơ sở dữ liệu số thúc đẩy quá trình phát triển, truy cập ngày 05/8/2025, từ: https://cand.com.vn/Hoat-dong-LL-CAND/xay-dung-co-so-du-lieu-so-thuc-day-qua-trinh-phat-trien-i748152/.
8. Báo Công an nhân dân (2025), Chuyển đổi số hiệu quả để đáp ứng nhiệm vụ đảm bảo an ninh trật tự địa phương, truy cập ngày 10/8/2025, từ: https://cand.com.vn/Hoat-dong-LL-CAND/chuyen-doi-so-hieu-qua-de-dap-ung-nhiem-vu-dam-bao-an-ninh-trat-tu-dia-phuong-i777352/.
9. Báo Công an nhân dân (2025), Đẩy nhanh tiến độ xây dựng các Cơ sở dữ liệu quốc gia, chuyên ngành, truy cập ngày 10/8/2025, từ: https://cand.com.vn/lanh-dao-bo-cong-an/day-nhanh-tien-do-xay-dung-cac-co-so-du-lieu-quoc-gia-chuyen-nganh-i774886/
10. Báo Công an nhân dân (2025), Đề xuất cơ chế phát hiện sớm rủi ro và truy xuất trách nhiệm đối với từng sản phẩm lưu hành trực tuyến, truy cập 18/7/2025, từ: https://cand.com.vn/su-kien-binh-luan-thoi-su/de-xuat-co-che-phat-hien-som-rui-ro-va-truy-xuat-trach-nhiem-doi-voi-tung-san-pham-luu-hanh-truc-tuyen-i768660/

11. Báo điện tử Chính phủ (2023), Đã đối soát xong 33,5 triệu giấy phép lái xe với cơ sở dữ liệu dân cư, truy cập 11/7/2025, từ https://baochinhphu.vn/da-doi-soat-xong-335-trieu-giay-phep-lai-xe-voi-co-so-du-lieu-dan-cu-102231204110728559.htm.
12. Báo điện tử Chính phủ (2024), Thứ trưởng Nguyễn Khánh Ngọc: Xây dựng Cơ sở dữ liệu LLTP 'đúng, đủ, sạch, sống', truy cập 03/8/2025, từ: https://baochinhphu.vn/thu-truong-nguyen-khanh-ngoc-xay-dung-co-so-du-lieu-lltp-dung-du-sach-song-102240927152705193.htm
13. Báo điện tử Chính phủ (2024), Cấp phiếu Lý lịch tư pháp: Nhiều kết quả sau 01 năm thực hiện Chỉ thị của Thủ tướng Chính phủ, truy cập ngày 30/7/2025, từ https://baochinhphu.vn/cap-phieu-ly-lich-tu-phap-nhieu-ket-qua-sau-01-nam-thuc-hien-chi-thi-cua-thu-tuong-chinh-phu-102240926183252465.htm.
14. Bộ Công an (2024), Thông tư số 14/2024/TT-BCA ngày 28/5/2024 quy định về quản lý, vận hành, khai thác Cơ sở dữ liệu quốc gia về dân cư.
15. Bộ Công an (2025), Báo cáo tổng kết công tác bảo vệ dữ liệu cá nhân và an ninh mạng năm 2024.
16. Bộ Khoa học và Công nghệ (2024), Báo cáo khoa học, công nghệ và đổi mới sáng tạo Việt Nam
17. Bộ Thông tin và Truyền thông (2023), Sách trắng về công nghệ thông tin và truyền thông Việt Nam.
18. Chính phủ (2021), Nghị quyết số 76/NQ-CP ngày 15/7/2021 của Chính phủ ban hành Chương trình tổng thể cải cách hành chính nhà nước giai đoạn 2021-2030.

19. Chính phủ (2023), Nghị quyết số 175/NQ-CP ngày 31/10/2023 của Chính phủ Phê duyệt Đề án Trung tâm dữ liệu quốc gia.
20. Chính phủ (2024), Nghị định số 13/2024/NĐ-CP ngày 17/4/2024 về bảo vệ dữ liệu cá nhân.
21. Chính phủ (2025), Nghị định số 102/2025/NĐ-CP ngày 13/5/2025 của Chính phủ quy định về quy định quản lý dữ liệu y tế.
22. Chính phủ (2025), Nghị định số 160/2025/NĐ-CP ngày 29/6/2025 của Chính phủ quy định về quỹ phát triển dữ liệu quốc gia.
23. Chính phủ (2025), Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu
24. Chính phủ (2025), 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.
25. Chính phủ (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.
26. ISO (2022), Tiêu chuẩn ISO/IEC 27701 về quản lý thông tin cá nhân (PIMS)
27. Liên Hiệp Quốc (2021), Báo cáo chuyển đổi số toàn cầu
28. Liên minh Châu Âu (2016), *Quy định chung về bảo vệ dữ liệu – GDPR*

29. Harvard Business Review (2021), The Age of Data and Digital Trust

30. McKinsey & Company (2022), *Unlocking Value in Data: Global Trends*.

31. Ngân hàng Nhà nước Việt Nam (2024), Quy chế bảo vệ dữ liệu trong lĩnh vực ngân hàng

32. Thủ tướng Chính phủ (2020), Quyết định số 2289/QĐ-TTg ngày 31/12/2020 của Thủ tướng Chính phủ về ban hành Chiến lược quốc gia về Cách mạng công nghiệp lần thứ tư đến năm 2030

33. Thủ tướng Chính phủ (2022), *Quyết định số 964/QĐ-TTg* ngày 10/8/2022 phê duyệt Chiến lược An toàn, An ninh mạng quốc gia đến năm 2025, tầm nhìn 2030

34. Thủ tướng Chính phủ (2024), Quyết định số 36/QĐ-TTg ngày 11/01/2024 của Thủ tướng Chính phủ Phê duyệt Quy hoạch hạ tầng thông tin và truyền thông thời kỳ 2021 - 2030, tầm nhìn đến năm 2050

35. Thủ tướng Chính phủ (2024), Quyết định số 142/QĐ-TTg ngày 02/02/2024 của Thủ tướng Chính phủ Phê duyệt Chiến lược dữ liệu quốc gia đến năm 2030

36. Thủ tướng Chính phủ (2025), Quyết định số 75/QĐ-TTg ngày 11/01/2025 của Thủ tướng Chính phủ Ban hành kế hoạch triển khai thi hành Luật Dữ liệu

37. Thủ tướng Chính phủ (2025), Quyết định số 20/2025/QĐ-TTg ngày 01/7/2025 của Thủ tướng Chính phủ Ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi.

38. Thủ tướng Chính phủ (2025), Quyết định số 25/2025/QĐ-TTg ngày 22/7/2025 của Thủ tướng Chính phủ Quy định về xây dựng cơ sở dữ liệu và chế độ báo cáo trực tuyến trên Hệ thống trong giám sát, đánh giá các chương trình mục tiêu quốc gia.
39. Tổ chức Hợp tác và Phát triển Kinh tế – OECD (2022), *OECD Privacy Guidelines*
40. Văn phòng Trung ương Đảng (2023), Công văn số 7455-CV/VPTW ngày 31/7/2023 của Văn phòng Trung ương Đảng thông báo kết luận của Bộ Chính trị về Đề án Trung tâm dữ liệu quốc gia.
41. Viện Chiến lược Thông tin và Truyền thông (2024), Tài liệu nghiên cứu về dữ liệu mở và chia sẻ dữ liệu
42. Quốc hội (2013), Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam năm 2013
43. Quốc hội (2016), Luật Tiếp cận thông tin
44. Quốc hội (2023), Nghị quyết số 81/2023/QH15 ngày 09/01/2023 của Quốc hội về Quy hoạch tổng thể quốc gia thời kỳ 2021 - 2030, tầm nhìn đến năm 2050
45. Quốc hội (2024), Luật Dữ liệu.
46. Quốc hội (2024), Luật Lưu trữ
47. Ủy ban Quốc gia về Chuyển đổi số (2024), Báo cáo thường niên chuyển đổi số Việt Nam
48. World Bank (2023), Data Governance in the Digital Economy