

Số: 1841 /BC-BCA

Hà Nội, ngày 25 tháng 8 năm 2026

BÁO CÁO**Đánh giá thực trạng quan hệ xã hội
liên quan đến dự thảo Luật An ninh dữ liệu**

Kính gửi: Chính phủ

Thực hiện quy định của Luật Ban hành văn bản quy phạm pháp luật năm 2025, Bộ Công an báo cáo đánh giá thực trạng quan hệ xã hội liên quan đến dự thảo Luật An ninh dữ liệu, cụ thể như sau:

I. BỐI CẢNH THỰC HIỆN ĐÁNH GIÁ**1. Bối cảnh quốc tế**

Trong giai đoạn phát triển của cuộc Cách mạng công nghiệp lần thứ tư, thế giới đang ghi nhận sự chuyển dịch phương thức quản trị và gia tăng giá trị từ tài nguyên hữu hình sang tài nguyên số, trong đó dữ liệu là thành phần cốt lõi. Bối cảnh quốc tế hiện nay phản ánh sự cạnh tranh gay gắt về mặt công nghệ và chủ quyền không gian số giữa các quốc gia, trong đó công tác bảo đảm an ninh dữ liệu là yếu tố then chốt để bảo vệ chủ quyền quốc gia. Thực trạng các quan hệ xã hội trên phạm vi toàn cầu liên quan đến an ninh dữ liệu đang biến đổi phức tạp, đặt ra các yêu cầu mới đối với quy trình quản trị, biện pháp kỹ thuật và năng lực nguồn nhân lực của các quốc gia, bao gồm Việt Nam.

Thứ nhất, xu hướng gia tăng thẩm quyền tài phán dữ liệu (Data Nationalism): Các quốc gia không còn xem dữ liệu là tài nguyên lưu chuyển tự do mà xác định đây là tài sản chiến lược cần áp dụng cơ chế bảo vệ dài hạn. Các trung tâm công nghệ lớn như Mỹ, Trung Quốc và Liên minh Châu Âu (EU) đã ban hành các chuẩn mực pháp lý chặt chẽ để quản lý tài sản số. Điển hình, EU áp dụng Quy định chung về bảo vệ dữ liệu (GDPR) nhằm tối ưu hóa việc bảo vệ quyền riêng tư của chủ thể dữ liệu; trong khi đó, Trung Quốc thực thi Luật An ninh dữ liệu với trọng tâm kiểm soát nghiêm ngặt luồng dữ liệu xuyên biên giới nhằm bảo đảm an ninh quốc gia. Sự thay đổi quy định này tạo ra một thực trạng quan hệ xã hội mới: dòng lưu chuyển dữ liệu quốc tế bị kiểm soát bởi các hàng rào kỹ thuật số và quy định pháp lý hành chính. Thực trạng này hình thành các quan hệ pháp lý mới, bắt buộc các tổ chức, tập đoàn đa quốc gia phải tuân thủ quyền tài phán của nước sở tại. Việt Nam đang đứng trước yêu cầu phải chuẩn hóa, đồng bộ quy trình nội địa phù hợp với các tiêu chuẩn quốc tế nêu trên nhằm bảo vệ dữ liệu quốc gia, đồng thời duy trì khả năng hội nhập trong nền kinh tế số toàn cầu. Quan hệ giữa các quốc gia hiện nay đan xen giữa hợp tác thương mại và cạnh tranh quyền tài phán dữ liệu - trong đó chủ thể nắm giữ hạ tầng lưu trữ

và thuật toán xử lý dữ liệu sẽ nắm lợi thế quyết định đối với các hoạt động kinh tế liên quan.

Thứ hai, sự phát triển của trí tuệ nhân tạo (AI) và dữ liệu lớn (Big Data) đã thay đổi tính chất của các tương tác xã hội: Quan hệ giữa cá nhân và các tập đoàn công nghệ xuyên biên giới (Big Tech) đang có sự bất đối xứng lớn về khả năng kiểm soát thông tin. Các biện pháp kỹ thuật truyền thống như hệ thống tường lửa hoặc phần mềm phòng chống mã độc thông thường không còn bảo đảm hiệu quả trước các phương thức tấn công sử dụng AI để khai thác, chiếm đoạt và thao túng dữ liệu. Thực trạng này làm ảnh hưởng đến mức độ an toàn và độ tin cậy trong các giao dịch số trên quy mô toàn cầu. Khi dữ liệu cá nhân bị thu thập, rao bán công khai trên môi trường mạng hoặc bị lợi dụng để tạo ra các thông tin, dữ liệu giả mạo (Deepfake), quan hệ tương tác giữa công dân với công dân và giữa công dân với cơ quan Nhà nước gặp nhiều rủi ro bị sai lệch. Bối cảnh này đòi hỏi các biện pháp an ninh dữ liệu phải chuyển đổi từ phòng ngự thụ động sang quản trị chủ động, ứng dụng công nghệ trí tuệ nhân tạo để giám sát, bảo vệ dữ liệu theo thời gian thực, đồng thời thiết lập quy trình xác thực dữ liệu gốc nhằm duy trì trật tự xã hội trên môi trường số.

Thứ ba, yếu tố con người trong an ninh dữ liệu trở thành trọng tâm trong công tác phòng thủ không gian mạng: Toàn cầu đang đối mặt với sự thiếu hụt nghiêm trọng đội ngũ chuyên gia trình độ cao, am hiểu đồng thời về kỹ thuật công nghệ, quy định pháp luật và đạo đức dữ liệu. Quan hệ xã hội trong lĩnh vực lao động số đang có sự dịch chuyển: các quốc gia tập trung thu hút nhân lực an ninh mạng để bảo vệ các hệ thống hạ tầng thông tin trọng yếu như tài chính - ngân hàng, năng lượng và viễn thông. Thống kê thực tiễn chỉ ra rằng, hơn 80% các sự cố lộ lọt dữ liệu quy mô lớn trên thế giới có nguyên nhân xuất phát từ lỗi chủ quan của con người. Do đó, bối cảnh quốc tế hiện nay nhấn mạnh vào việc xây dựng nhận thức và thói quen an ninh dữ liệu cho toàn dân. Một quốc gia có năng lực an ninh dữ liệu mạnh không chỉ dựa vào số lượng hệ thống máy-tính cấu hình cao, mà phụ thuộc vào việc xây dựng đội ngũ nhân lực chuyên trách có năng lực và các công dân có kiến thức bảo mật hệ thống, đủ khả năng nhận diện, ngăn chặn các hành vi phá hoại kinh tế hoặc xâm phạm an ninh thông qua môi trường dữ liệu.

Thứ tư, sự cạnh tranh về hạ tầng số và chủ quyền lưu trữ dữ liệu đang làm thay đổi cấu trúc hợp tác quốc tế: Việc phụ thuộc hoàn toàn vào các nền tảng điện toán đám mây (Cloud) do nước ngoài quản lý đã bộc lộ các rủi ro pháp lý và kỹ thuật lớn. Khi một quốc gia bị hạn chế hoặc ngắt quyền truy cập vào nguồn dữ liệu lưu trữ trên máy chủ đặt tại nước ngoài, toàn bộ hoạt động vận hành kinh tế có nguy cơ bị đình trệ. Yếu tố này thúc đẩy xu hướng bảo vệ dài hạn dữ liệu cốt lõi bằng giải pháp lưu trữ tập trung tại các Trung tâm dữ liệu quốc gia và nghiên cứu áp dụng công nghệ mã hóa hậu lượng tử nhằm ngăn chặn sự can thiệp kỹ thuật từ các tổ chức công nghệ nước ngoài trong tương lai. Quan hệ xã hội giữa các quốc gia đang dần dịch chuyển sang việc hình thành

các liên kết, hợp tác bảo vệ dữ liệu dựa trên việc áp dụng các tiêu chuẩn an ninh đồng bộ, công khai và minh bạch.

Bối cảnh thế giới liên quan đến an ninh dữ liệu hiện nay phản ánh thực trạng đan xen giữa cơ hội phát triển kinh tế số và rủi ro mất chủ quyền kiểm soát tài nguyên số. Thực trạng quan hệ xã hội cho thấy sự gắn kết chặt chẽ giữa quy trình quản trị, biện pháp công nghệ và năng lực con người. Để bảo đảm tiến độ phát triển và hạn chế các tổn thương trong quá trình hội nhập, Việt Nam cần một chiến lược an ninh dữ liệu mang tính đồng bộ và toàn vẹn. Hệ thống quy định pháp luật cần đóng vai trò định hướng quy trình quy chuẩn, công nghệ đóng vai trò bảo vệ tài sản số quốc gia và con người là lực lượng nòng cốt vận hành. Việc ban hành Luật An ninh dữ liệu trong giai đoạn hiện nay là giải pháp chiến lược nhằm xác lập vị thế pháp lý, bảo vệ tài nguyên số và xây dựng môi trường xã hội số an toàn, ổn định trước các biến động công nghệ quốc tế. Dữ liệu cấu thành tài sản chiến lược của quốc gia trong giai đoạn chuyển đổi số, và bảo đảm an ninh dữ liệu là yêu cầu bắt buộc để duy trì chủ quyền quốc gia trên không gian mạng.

2. Bối cảnh trong nước

Việt Nam đang đẩy mạnh tiến trình chuyển đổi số quốc gia, trong đó dữ liệu được xác định là nguồn tài nguyên chiến lược, phục vụ công tác xây dựng Chính phủ số, phát triển kinh tế số và xã hội số. Kết quả nổi bật là sự hình thành và đưa vào vận hành hệ thống Trung tâm dữ liệu quốc gia (điển hình là mô hình DC1), đóng vai trò lưu trữ, kết nối các nguồn tài nguyên dữ liệu cốt lõi của cơ quan Nhà nước. Tuy nhiên, sự phát triển về quy mô hạ tầng kỹ thuật chưa đồng bộ với việc triển khai một chiến lược an ninh dữ liệu toàn diện. Thực tế cho thấy khi dữ liệu được lưu trữ tập trung với khối lượng và giá trị cao, hệ thống trở thành mục tiêu của các phương thức tấn công mạng từ các tổ chức tội phạm xuyên quốc gia. Việc phát triển hạ tầng kỹ thuật tốc độ cao nhưng thiếu một văn bản luật khung thống nhất về an ninh dữ liệu dẫn đến các rủi ro về an toàn hệ thống, ảnh hưởng đến an ninh chính trị và trật tự an toàn xã hội. Việc phân tích bối cảnh Việt Nam hiện nay cần đánh giá đa chiều thông qua mối tương tác giữa quy trình quản trị, biện pháp kỹ thuật và yếu tố con người trong một hệ sinh thái dữ liệu đang trong giai đoạn hoàn thiện, hướng tới mục tiêu bảo đảm an ninh dữ liệu bền vững.

Thứ nhất, sự chuyển dịch các quan hệ dân sự và thực trạng lộ lọt dữ liệu: Với quy mô gần 80 triệu người dân tham gia hoạt động trên không gian mạng, các quan hệ xã hội truyền thống đã được chuyển đổi sang hình thức số hóa. Các hoạt động như thanh toán không dùng tiền mặt, khám chữa bệnh từ xa, thực hiện thủ tục hành chính qua dịch vụ công trực tuyến đã hình thành nên các tập dữ liệu cá nhân lớn. Thực trạng này làm phát sinh quan hệ xã hội mới: quan hệ giữa chủ thể dữ liệu (công dân) và bên kiểm soát, xử lý dữ liệu (tổ chức, doanh nghiệp). Tuy nhiên, bối cảnh thực tế tại Việt Nam đang ghi nhận tình trạng lộ lọt dữ liệu cá nhân diễn biến phức tạp. Các vụ việc rao bán khối lượng lớn dữ liệu trên các diễn đàn trực tuyến phản ánh sự thiếu sót trong quy trình quản lý hành chính và giải pháp kỹ thuật của các đơn vị chủ quản. Khi thông tin định danh cá nhân, số

điện thoại, tài khoản ngân hàng bị các đối tượng xấu chiếm đoạt để thực hiện các hành vi lừa đảo chiếm đoạt tài sản bằng công nghệ cao sử dụng AI (Deepfake), gây ảnh hưởng đến tâm lý an toàn của người dân. Thực trạng này phản ánh việc nhiều đơn vị tập trung thu thập dữ liệu phục vụ mục đích kinh doanh nhưng chưa đầu tư tương xứng cho các biện pháp kỹ thuật bảo vệ an toàn thông tin.

Thứ hai, thực trạng quan hệ quản trị nhà nước và chủ quyền dữ liệu: Chính phủ Việt Nam đã triển khai các bước đi mang tính đột phá thông qua Đề án 06 và việc vận hành Cơ sở dữ liệu quốc gia về Dân cư, tạo nền tảng xác lập trật tự quản lý xã hội trên môi trường số. Tuy nhiên, mối quan hệ phối hợp giữa các cơ quan Nhà nước trong việc chia sẻ, kết nối dữ liệu đang gặp rào cản về tính đồng bộ kỹ thuật. Quy trình liên thông dữ liệu qua Trục liên thông văn bản quốc gia (NDXP) đã hình thành nhưng các biện pháp kỹ thuật bảo vệ tại các điểm cuối - đặc biệt là ở cấp hệ thống thông tin của địa phương - vẫn là mắt xích tồn tại nhiều lỗ hổng bảo mật. Quan hệ quản trị còn đối mặt với thách thức về chủ quyền số khi phần lớn dữ liệu vận hành kinh doanh của các doanh nghiệp, tổ chức trong nước vẫn đang được lưu trữ trên hạ tầng điện toán đám mây do các tập đoàn công nghệ nước ngoài quản lý. Thực trạng này dẫn đến việc quyền tài sản quốc gia đối với dữ liệu bị hạn chế bởi các quy định nội bộ của các tập đoàn công nghệ xuyên biên giới. Việc xác lập danh mục dữ liệu cốt lõi là tài sản quốc gia và áp dụng quy trình bảo vệ nghiêm ngặt là giải pháp cần thiết để khẳng định chủ quyền và quyền tự quyết trên không gian mạng.

Thứ ba, sự xung đột lợi ích kinh tế số và an ninh thuật toán: Dữ liệu đã trở thành tư liệu sản xuất quan trọng, đóng góp tỷ trọng lớn vào giá trị thặng dư của nền kinh tế Việt Nam. Tuy nhiên, quan hệ giữa các doanh nghiệp cung cấp dịch vụ công nghệ và người sử dụng dịch vụ đang phát sinh các mặt trái liên quan đến tình trạng độc quyền dữ liệu và khai thác, sử dụng trái phép thông tin để trục lợi. Thực trạng cho thấy, phần lớn doanh nghiệp nhỏ và vừa (SMEs) tại Việt Nam chưa đáp ứng các chuẩn mực về an ninh dữ liệu do hạn chế về chi phí đầu tư hạ tầng. Các biện pháp kỹ thuật như mã hóa dữ liệu hoặc xây dựng hệ thống sao lưu dự phòng (Backup) thường bị cắt giảm để tối ưu hóa lợi nhuận kinh doanh. Khi các sự cố tấn công mã hóa dữ liệu tống tiền (Ransomware) nhắm vào các doanh nghiệp quy mô lớn (như sự cố tại VNDIRECT hoặc PVOIL) xảy ra, hậu quả không chỉ dừng lại ở thiệt hại tài chính cục bộ mà còn gây gián đoạn các chuỗi cung ứng kinh tế, ảnh hưởng đến tâm lý các nhà đầu tư. Thực trạng này đặt ra yêu cầu cấp thiết về việc ban hành quy trình kiểm soát an ninh dữ liệu bắt buộc và cơ chế bảo hiểm rủi ro công nghệ để bảo vệ các quan hệ kinh tế số.

Thứ tư, yếu tố con người và sự thiếu hụt năng lực chuyên trách: Trong hệ sinh thái an ninh dữ liệu của Việt Nam, nhân sự vận hành đóng vai trò quyết định nhưng cũng là thành phần dễ phát sinh rủi ro bảo mật. Các phương thức tấn công mạng có tổ chức nhắm vào nguồn dữ liệu cốt lõi (thuộc lĩnh vực tài chính, năng lượng, quốc phòng) đòi hỏi đội ngũ chuyên gia chuyên trách của Việt Nam phải

có năng lực chuyên môn cao. Thực trạng hiện nay phản ánh sự thiếu hụt nguồn nhân lực chuyên sâu có khả năng quản trị dữ liệu ở tầm chiến lược. Mặc dù lực lượng chuyên trách thuộc Bộ Công an và Bộ Quốc phòng đã được kiện toàn và nâng cao năng lực, lực lượng chuyên trách tại các Bộ, ngành và địa phương khác chủ yếu hoạt động theo hình thức kiêm nhiệm, thiếu hụt công cụ giám sát và kỹ năng xử lý sự cố thực tế. Quan hệ xã hội trong lĩnh vực nhân sự số ghi nhận xu hướng dịch chuyển nguồn nhân lực chất lượng cao từ khối cơ quan Nhà nước sang khu vực tư nhân, làm ảnh hưởng đến năng lực thực thi công vụ bảo đảm an ninh dữ liệu của các cơ quan quản lý. Ngoài ra, nhận thức về an ninh dữ liệu của đại bộ phận người dân còn hạn chế, thói quen chia sẻ thông tin cá nhân trên mạng xã hội tạo điều kiện cho các loại tội phạm mạng khai thác thông tin.

Thực trạng bối cảnh Việt Nam hiện nay đan xen giữa yêu cầu đẩy mạnh chuyển đổi số và các nguy cơ mất an toàn thông tin do hệ thống quản trị chưa đồng bộ. Thực trạng các quan hệ xã hội liên quan đến an ninh dữ liệu đòi hỏi phải có sự hoàn thiện về mặt thể chế pháp lý. Việc ban hành Luật An ninh dữ liệu không chỉ thiết lập các thủ tục hành chính, mà nhằm kiến tạo một hệ sinh thái quản lý đồng bộ: trong đó quy trình bảo vệ vòng đời dữ liệu được chuẩn hóa, các biện pháp kỹ thuật tự chủ được triển khai đồng bộ, và yếu tố con người được đào tạo chuyên sâu. Khi tài sản dữ liệu cốt lõi được bảo vệ và các quan hệ xã hội số được vận hành trên nền tảng an toàn, Việt Nam mới bảo đảm khả năng tự chủ trong quá trình chuyển đổi số. Dữ liệu cấu thành tài nguyên, nhưng bảo đảm an ninh dữ liệu là yếu tố quyết định đến sự ổn định và phát triển của quốc gia.

3. Chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an ninh dữ liệu

Các chủ trương, đường lối của Đảng đóng vai trò định hướng chiến lược đối với việc điều chỉnh và phát triển các quan hệ xã hội trong quá trình chuyển đổi số. Trước thực trạng các quan hệ xã hội về an ninh dữ liệu diễn biến phức tạp, Đảng đã ban hành nhiều Nghị quyết, Chỉ thị nhằm xác lập mục tiêu bảo vệ chủ quyền quốc gia trên không gian mạng và xác định dữ liệu là tài nguyên chiến lược.

Tính đến thời điểm hiện tại, hệ thống văn bản quy phạm pháp luật quy định về vấn đề phát triển, đẩy mạnh ứng dụng dữ liệu, công tác lưu trữ dữ liệu và bảo đảm an ninh dữ liệu đã được ban hành, bao gồm các văn bản cơ bản sau: Luật Dữ liệu số 60/2024/QH15 được Quốc hội khóa XV ban hành ngày 30/11/2024 và có hiệu lực thi hành ngày 01/7/2025, quy định về công tác xây dựng, phát triển, xử lý, quản trị dữ liệu; Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 được Quốc hội khóa XV ban hành ngày 26/6/2025 và có hiệu lực thi hành ngày 01/01/2026, quy định về quyền, nghĩa vụ bảo vệ dữ liệu cá nhân, thiết lập khung pháp lý trong việc thu thập, xử lý và bảo vệ quyền riêng tư của công dân trên môi trường số; Luật An ninh mạng số 116/2025/QH15 được Quốc hội khóa XV ban hành ngày 10/12/2025 và có hiệu lực thi hành ngày 01/7/2026,

thực hiện luật hóa khái niệm an ninh dữ liệu và xác định bảo đảm an ninh dữ liệu là thành phần cốt lõi của công tác bảo vệ an ninh mạng quốc gia (đây là luật được xây dựng trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015, có hiệu lực thi hành từ ngày 01/7/2026).

Hệ thống văn bản pháp luật quy định về dữ liệu, phát triển dữ liệu và hoàn thiện hạ tầng thông tin phục vụ chuyển đổi số tại Việt Nam đã được ban hành kịp thời nhằm điều chỉnh các quan hệ mới phát sinh, phù hợp với tiến trình ứng dụng khoa học công nghệ trong xử lý dữ liệu. Tuy nhiên, bên cạnh những kết quả tích cực, thực tiễn thi hành cũng cho thấy một số quy định pháp luật liên quan đến dữ liệu, đặc biệt là nội dung bảo đảm an ninh dữ liệu xét trên các khía cạnh quy trình, công nghệ và con người còn hạn chế. Thực trạng này dẫn đến việc tổ chức thực hiện chức năng quản lý, bảo đảm an ninh dữ liệu tại nhiều bộ, ngành, địa phương thiếu tính thống nhất, hiệu quả chưa cao, chưa thu hút được nguồn nhân lực công nghệ cao và còn tiềm ẩn nhiều rủi ro đối với hệ thống dữ liệu quốc gia, ảnh hưởng trực tiếp đến quá trình xây dựng, phát triển Chính phủ số, xã hội số và kinh tế số.

Bên cạnh 03 văn bản nền tảng nêu trên, thực trạng quan hệ xã hội liên quan đến an ninh dữ liệu còn chịu sự điều chỉnh giao thoa của Luật Cơ yếu, Luật Giao dịch điện tử, Luật Chuyển đổi số và Luật Trí tuệ nhân tạo. Kết quả rà soát nội dung giao thoa với 06 luật nêu trên đã được thể hiện cụ thể tại Điều 24 dự thảo Luật (khoản 1: nguyên tắc áp dụng; khoản 2: sửa đổi, bổ sung, bãi bỏ một số điều, khoản của các luật có liên quan; khoản 3: dẫn chiếu, sử dụng chung kết quả, không quy định lại), theo nguyên tắc Luật An ninh dữ liệu chỉ bổ sung yêu cầu, biện pháp bảo đảm an ninh, không quy định lại đối tượng, phạm vi, quyền, nghĩa vụ đã được luật chuyên ngành xác lập.

II. THỰC TRẠNG QUAN HỆ XÃ HỘI VÀ KẾT QUẢ THI HÀNH CÁC VĂN BẢN QUY PHẠM PHÁP LUẬT KHÁC CÓ LIÊN QUAN ĐẾN CHÍNH SÁCH CỦA LUẬT AN NINH DỮ LIỆU

1. Thực trạng quan hệ xã hội

a) Khái quát chung về bối cảnh chuyển đổi số và sự hình thành các quan hệ xã hội mới

Việt Nam ghi nhận tốc độ tăng trưởng kinh tế số thuộc nhóm cao trong khu vực ASEAN. Dữ liệu hiện đóng vai trò là yếu tố kỹ thuật và kinh tế duy trì hoạt động vận hành của hệ thống chính trị, kinh tế và xã hội. Trong bối cảnh đó, các quan hệ xã hội truyền thống đang chuyển dịch sang môi trường không gian mạng, hình thành mối liên kết mới giữa Nhà nước - Doanh nghiệp - Công dân dựa trên hoạt động trao đổi, khai thác và xử lý dữ liệu. Tuy nhiên, thực trạng hiện nay cho thấy tốc độ phát triển của các quan hệ xã hội này nhanh hơn năng lực quản trị an ninh hệ thống. Khi dữ liệu có giá trị tài sản, thành phần này trở thành mục tiêu tấn công của các loại tội phạm công nghệ cao và các tổ chức mạng có mục đích xấu. Thực trạng an ninh dữ liệu tại Việt Nam đang bộc lộ các

hạn chế mang tính hệ thống, ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự an toàn xã hội và quyền lợi hợp pháp của các chủ thể tham gia.

b) Khía cạnh thể chế và quy trình: thực trạng phân mảnh và thiếu đồng bộ

Thể chế và quy trình quy chuẩn cấu thành nền tảng điều hành các quan hệ xã hội. Tuy nhiên, thực trạng tại Việt Nam đang đối mặt với sự thiếu đồng bộ trong việc quản trị vòng đời dữ liệu:

Quy trình quản trị vòng đời dữ liệu chưa khép kín: Hiện nay, các quan hệ xã hội về dữ liệu mới chỉ tập trung vào khâu thu thập và lưu trữ đầu vào. Quy trình bảo mật tại các khâu có tính rủi ro cao như chia sẻ, phân tích nội bộ và tiêu hủy dữ liệu chưa được quy định chi tiết. Nhiều tổ chức thực hiện thu thập dữ liệu người dùng với khối lượng lớn nhưng thiếu quy trình kiểm soát khi chuyển giao dữ liệu cho bên thứ ba hoặc khi dữ liệu đã hết thời hạn sử dụng. Việc thiếu quy trình tiêu hủy chuẩn hóa dẫn đến tình trạng lưu trữ dữ liệu dư thừa trên các hệ thống máy chủ cũ, tạo điều kiện cho các đối tượng mạng khai thác và tái dựng thông tin cá nhân.

Sự chồng chéo và khoảng trống pháp lý hiện tại: Mặc dù đã có Luật An ninh mạng, Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu nhưng các quy định về bảo đảm an ninh dữ liệu vẫn phân tán tại nhiều văn bản, chưa bảo đảm tính hệ thống. Quan hệ phối hợp giữa các cơ quan quản lý Nhà nước có thời điểm còn chồng chéo về chức năng hoặc chưa xác định rõ trách nhiệm khi xảy ra sự cố lộ lọt dữ liệu. Đặc biệt, hiện chưa có quy trình pháp lý cụ thể để xác lập và áp dụng cơ chế bảo vệ đặc biệt đối với Danh mục dữ liệu cốt lõi quốc gia theo tính chất tài sản công. Điều này dẫn đến thực trạng các nguồn dữ liệu chiến lược bị áp dụng biện pháp bảo vệ dàn trải, chưa tập trung nguồn lực tương xứng với tầm quan trọng.

c) Khía cạnh công nghệ và biện pháp: thách thức về tính tự chủ và bảo mật dài hạn

Công nghệ là công cụ thực thi các yêu cầu an ninh, nhưng tại Việt Nam, khía cạnh này vẫn tồn tại một số điểm yếu kỹ thuật:

Sự phụ thuộc vào hạ tầng quốc tế và chủ quyền dữ liệu: Một thực trạng đáng lưu ý trong quan hệ kinh tế số hiện nay là mức độ phụ thuộc lớn vào hạ tầng lưu trữ xuyên biên giới. Theo thống kê, khoảng 80% dữ liệu điện toán đám mây của các doanh nghiệp Việt Nam đang đặt tại các hệ thống máy chủ đặt ngoài lãnh thổ Việt Nam. Quan hệ xã hội về dữ liệu do đó bị chi phối bởi quyền tài phán của các quốc gia quản lý hạ tầng. Các biện pháp kỹ thuật nội địa chưa đủ khả năng thiết lập hàng rào kỹ thuật tự động nhằm kiểm soát, ngăn chặn luồng dữ liệu quan trọng chuyển dịch ra khỏi biên giới quốc gia, tiềm ẩn nguy cơ thất thoát tài nguyên số.

Biện pháp kỹ thuật chưa tương thích với sự phát triển của công nghệ mới: Tội phạm mạng đang tăng cường sử dụng trí tuệ nhân tạo (AI) để thực hiện các cuộc tấn công mã hóa dữ liệu (Ransomware) và tạo thông tin giả mạo (Deepfake).

Trong khi đó, biện pháp bảo vệ tại phần lớn các cơ quan, đơn vị tại Việt Nam vẫn chỉ dừng lại ở việc áp dụng các hệ thống tường lửa (Firewall) truyền thống và phần mềm kháng mã độc cơ bản. Việc ứng dụng công nghệ mã hóa hậu lượng tử (Post-Quantum Cryptography) để bảo vệ dài hạn dữ liệu cốt lõi chưa được triển khai rộng rãi. Sự chênh lệch về công nghệ giữa phương thức tấn công và năng lực phòng thủ gây rủi ro cho mức độ an toàn của các quan hệ giao dịch số.

d) Khía cạnh con người và lực lượng: thực trạng năng lực và nhận thức xã hội

Trong cấu trúc các quan hệ xã hội, yếu tố con người đóng vai trò quyết định. Thực trạng an ninh dữ liệu tại Việt Nam phản ánh rõ nét sự thiếu hụt về năng lực chuyên môn và nhận thức xã hội:

Thiếu hụt nguồn nhân lực quản trị dữ liệu chuyên sâu: Việt Nam đang đối mặt với tình trạng thiếu chuyên gia có trình độ về Quản trị dữ liệu (Data Governance). Lực lượng chuyên trách tại các Bộ, ngành và địa phương hiện nay đa số thực hiện nhiệm vụ theo chế độ kiêm nhiệm, tập trung xử lý hạ tầng kỹ thuật vật lý hơn là quản trị an ninh nội dung dữ liệu. Sự dịch chuyển nhân lực trình độ cao từ khu vực công sang khu vực tư nhân do cơ chế đãi ngộ làm suy giảm năng lực thực thi của lực lượng chuyên trách tại các cơ quan Nhà nước.

Ý thức bảo mật và nhận thức của cộng đồng: Thực tế chứng minh phần lớn các sự cố lộ lọt dữ liệu quy mô lớn tại Việt Nam thời gian qua có nguyên nhân từ sai sót chủ quan hoặc sự thiếu cảnh giác của con người trong quá trình vận hành hệ thống. Quan hệ xã hội trên không gian mạng hiện nay chịu ảnh hưởng bởi nhận thức chưa đầy đủ về an ninh thông tin của người dân; nhiều cá nhân sẵn sàng cung cấp dữ liệu cá nhân để sử dụng các tiện ích công nghệ hoặc tham gia các hoạt động trên mạng xã hội không bảo đảm an toàn. Việc thiếu chương trình giáo dục phổ cập về an ninh dữ liệu toàn dân khiến xã hội dễ bị tác động bởi các phương thức tấn công tâm lý và lừa đảo trực tuyến dựa trên dữ liệu.

e) Quan hệ quốc tế hiện nay: thực trạng quyền tài phán và hợp tác xuyên biên giới

Do đặc tính lưu chuyển không giới hạn địa lý của dữ liệu, quan hệ xã hội về an ninh dữ liệu tại Việt Nam chịu tác động từ bối cảnh quốc tế:

Thách thức từ hoạt động của các nền tảng xuyên biên giới: Quan hệ giữa Nhà nước Việt Nam và các tập đoàn công nghệ đa quốc gia cung cấp dịch vụ xuyên biên giới gặp nhiều vướng mắc pháp lý. Các tập đoàn này thu thập và xử lý khối lượng lớn dữ liệu của công dân Việt Nam nhưng việc thực thi các yêu cầu về bảo đảm an ninh, lưu trữ dữ liệu tại Việt Nam theo quy định pháp lý nội địa vẫn gặp rào cản từ các thỏa thuận quốc tế và quy định nội bộ của doanh nghiệp nước ngoài.

Yêu cầu về chuẩn hóa quy trình theo tiêu chuẩn quốc tế: Để thực hiện các cam kết trong các hiệp định thương mại tự do thế hệ mới, Việt Nam có nghĩa vụ

chuẩn hóa quy trình bảo vệ dữ liệu tương đương với các chuẩn mực quốc tế như GDPR của Châu Âu. Tuy nhiên, việc đồng bộ này đang gặp khó khăn do khoảng cách về trình độ công nghệ hạ tầng và sự khác biệt trong phương thức quản lý hành chính.

2. Kết quả triển khai các văn bản quy phạm pháp luật có liên quan

Trong lộ trình hoàn thiện hệ thống pháp luật số, việc tổng kết thực thi các văn bản quy phạm pháp luật liên quan đến an ninh dữ liệu là cơ sở quan trọng để đánh giá chính sách. Giai đoạn từ năm 2015 đến nay ghi nhận sự chuyển dịch từ duy quản lý, từ việc tập trung bảo vệ hạ tầng vật lý sang quản trị nội dung và giá trị của dữ liệu. Việc triển khai Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 đã xác lập trách nhiệm của các cơ quan chuyên trách và hình thành quy trình phân loại hệ thống thông tin theo 5 cấp độ bảo mật. Đến hết năm 2025, hệ thống văn bản quy phạm pháp luật được bổ sung với sự ra đời của Luật An ninh mạng năm 2025, Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân năm 2025, từng bước hoàn thiện khung pháp lý bảo vệ dữ liệu. Việc gần 80% hệ thống thông tin của các cơ quan Nhà nước được phê duyệt hồ sơ đề xuất cấp độ là kết quả của công tác chuẩn hóa quy trình vận hành.

Tuy nhiên, thực tiễn thi hành cho thấy các quy định này chủ yếu mới dừng lại ở việc bảo vệ hạ tầng kỹ thuật (vỏ hệ thống), trong khi nội dung dữ liệu bên trong (lõi dữ liệu) chưa được bảo vệ xuyên suốt vòng đời. Minh chứng cụ thể là vụ việc rò rỉ 30 triệu hồ sơ ngành giáo dục năm 2022 và các đợt lộ lọt dữ liệu ngành y tế năm 2024, phản ánh thực trạng mặc dù hệ thống hạ tầng đạt chuẩn cấp độ bảo mật nhưng quy trình kiểm soát nội dung tại các đơn vị thực thi ở địa phương chưa bảo đảm quy chuẩn.

Thực trạng này rõ rệt hơn khi đánh giá các biện pháp kỹ thuật và tính tự chủ công nghệ. Mặc dù mô hình bảo vệ 4 lớp đã được triển khai rộng rãi, khả năng tự chủ về công nghệ lõi vẫn là hạn chế lớn. Hiện nay, khoảng 80% dữ liệu điện toán đám mây của các doanh nghiệp nội địa vẫn đang được lưu trữ trên các nền tảng xuyên biên giới của các tập đoàn đa quốc gia như AWS, Google Cloud hay Azure. Điều này dẫn đến hệ lụy trực tiếp về quyền tài phán: khi dữ liệu của công dân Việt Nam đặt trên máy chủ nước ngoài, việc thực thi các quy trình kiểm soát luồng dữ liệu xuyên biên giới gặp nhiều trở ngại pháp lý. Sự gia tăng của các cuộc tấn công mã hóa dữ liệu tống tiền (Ransomware) vào đầu năm 2024, tiêu biểu là sự cố tại tập đoàn tài chính VNDIRECT và tập đoàn năng lượng PVOIL, chứng minh thực tế là chỉ có khoảng 25% tổ chức có quy trình sao lưu và phục hồi dữ liệu đáp ứng tiêu chuẩn khôi phục hoạt động dưới 24 giờ. Các cuộc tấn công này gây gián đoạn các giao dịch kinh tế quy mô lớn và cho thấy các biện pháp kỹ thuật hiện tại thiếu tính dự phòng chiến lược, chưa đủ năng lực đối phó với sự tinh vi của tội phạm mạng sử dụng trí tuệ nhân tạo để dò quét lỗ hổng hệ thống.

Hạn chế lớn nhất trong công tác thực thi pháp luật nằm ở yếu tố con người. Tổng kết các vụ án xâm phạm an ninh dữ liệu trong hai năm qua cho thấy có tới

60% đến 70% vụ lộ lọt dữ liệu bắt nguồn từ sai phạm nội bộ hoặc sự thiếu trách nhiệm của cán bộ quản trị hệ thống. Việc Bộ Công an đấu tranh, triệt phá các đường dây mua bán dữ liệu cá nhân quy mô lớn với khối lượng thông tin đáng kể vào năm 2023 là minh chứng cụ thể. Các đối tượng đã lợi dụng quyền truy cập của nhân viên nội bộ thuộc các ngân hàng và công ty bảo hiểm để trích xuất dữ liệu thô. Thực trạng này chứng minh các quy định hiện hành tập trung nhiều vào việc phòng chống tấn công từ bên ngoài, chưa có cơ chế kiểm soát chặt chẽ đặc quyền truy cập nội bộ. Chế tài xử phạt hành chính hiện nay chưa đủ tính răn đe so với lợi nhuận thu được từ việc buôn bán dữ liệu trái phép. Khi một bộ dữ liệu có giá trị cao trên thị trường nhưng mức phạt tiền tối đa chỉ dừng lại ở ngưỡng vài chục triệu đồng, nhiều doanh nghiệp có xu hướng chấp nhận nộp phạt thay vì đầu tư kinh phí xây dựng hệ thống bảo mật chuyên sâu. Đồng thời, việc dự kiến thiếu hụt khoảng 150.000 đến 200.000 chuyên gia trình độ cao về an ninh dữ liệu vào năm 2026 khiến công tác thực thi pháp luật ở cấp cơ sở gặp khó khăn về năng lực giám sát.

Mặc dù vậy, công tác thực hiện Đề án 06 về phát triển ứng dụng dữ liệu dân cư đã đạt được các kết quả quan trọng. Việc Cơ sở dữ liệu quốc gia về Dân cư thực hiện xác thực hơn 1,2 tỷ lượt yêu cầu mỗi năm và phối hợp chuẩn hóa hơn 125 triệu thuê bao viễn thông đã nâng cao chất lượng dữ liệu bảo đảm nguyên tắc "đúng, đủ, sạch, sống". Hoạt động làm sạch dữ liệu này đã hỗ trợ xử lý và khóa hơn 20 triệu SIM không chính chủ, hạn chế công cụ hoạt động của tội phạm lừa đảo công nghệ cao. Đây là ví dụ về việc áp dụng biện pháp kết nối dữ liệu tập trung để giải quyết các vấn đề xã hội phức tạp. Tuy nhiên, kết quả này cũng chỉ ra hạn chế mới: do thiếu một đạo luật thống nhất quy định chung, việc chia sẻ thông tin giữa các bộ, ngành vẫn gặp rào cản về tâm lý e ngại mất an toàn hệ thống. Nhiều đơn vị duy trì phương thức quản lý khép kín đối với nguồn dữ liệu do mình quản lý, gây lãng phí nguồn lực và hạn chế khả năng phát triển của kinh tế số, trong khi thiệt hại từ hoạt động lừa đảo trực tuyến tại Việt Nam vẫn ở mức cao, ước tính từ 15 đến 20 tỷ USD mỗi năm, chiếm gần 4% GDP quốc gia.

Từ thực trạng đánh giá nêu trên, yêu cầu đặt ra cho giai đoạn tới là phải chuyển dịch sang hệ thống bảo đảm an ninh dữ liệu mang tính ổn định và toàn vẹn. Luật An ninh dữ liệu cần xác lập danh mục dữ liệu cốt lõi quốc gia — những tài sản cần bảo vệ bằng các biện pháp kỹ thuật đặc biệt như mã hóa hậu lượng tử và áp dụng giải pháp lưu trữ biệt lập hoàn toàn (Air-gapped) tương tự phương thức áp dụng với dữ liệu Kỳ thi Tốt nghiệp THPT quốc gia. Quy trình quản trị cần bảo đảm tính liên tục ở mọi khâu, từ việc gắn nhãn bảo mật tự động bằng ứng dụng trí tuệ nhân tạo đến quy định rõ ràng trách nhiệm pháp lý đối với chức danh cán bộ quản trị dữ liệu. Chế tài xử phạt cần được nghiên cứu sửa đổi theo hướng tăng nặng, áp dụng cơ chế xử phạt theo tỷ lệ phần trăm doanh thu của tổ chức vi phạm nhằm bảo đảm tính răn đe.

3. Kết quả công tác bảo đảm an ninh dữ liệu

Công tác bảo đảm an ninh hệ thống thông tin và Cơ sở dữ liệu (CSDL) quốc gia trong giai đoạn 2021 - 2025 đã đạt được các chuyển biến về nhận thức

và tổ chức thực hiện. Việt Nam đã hình thành mạng lưới đơn vị chuyên trách và chuyên gia an ninh mạng với sự tham gia của hơn 200 cơ quan, tổ chức. Mạng lưới này tạo thành hệ thống phòng thủ đa tầng, bao gồm: 17 Bộ và cơ quan ngang Bộ; 05 cơ quan thuộc Chính phủ; 34 Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc trung ương; 17 Tập đoàn, Tổng công ty Nhà nước; 45 Ngân hàng và tổ chức tài chính; cùng 30 doanh nghiệp cung cấp dịch vụ Internet (ISP) và các tổ chức liên quan khác.

Đặc biệt, sự vận hành Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia đã xây dựng được cơ chế phản ứng nhanh đối với các sự cố. Hệ thống kỹ thuật bảo đảm an ninh mạng quy mô quốc gia đã được đầu tư nâng cấp, bao gồm các hệ thống: theo dõi xu hướng không gian mạng; điều phối xử lý phát tán thông tin vi phạm; và hệ thống chia sẻ, giám sát thông tin phục vụ Chính phủ điện tử/Chính phủ số. Nhờ đó, thứ hạng của Việt Nam trong bảng xếp hạng Chỉ số An toàn thông tin mạng toàn cầu (GCI) do Liên minh Viễn thông Quốc tế (ITU) công bố đã có sự tăng tiến, thuộc nhóm các quốc gia dẫn đầu (vị trí Top 25-30 thế giới vào năm 2025). Theo báo cáo đánh giá của các tổ chức quốc tế như Kaspersky, Việt Nam duy trì tỷ lệ lây nhiễm mã độc trên thiết bị di động ở mức thấp trong khu vực Đông Nam Á, đứng sau Singapore.

Tuy nhiên, sự gia tăng về quy mô hạ tầng Trung tâm dữ liệu quốc gia đang đặt ra các thách thức lớn về công tác quản lý: quy mô dữ liệu càng lớn và tính tập trung càng cao thì yêu cầu bảo đảm an ninh càng lớn. Hiện nay, chiến lược an ninh dữ liệu quốc gia chưa bảo đảm tính đồng bộ xuyên suốt toàn bộ vòng đời của dữ liệu. Thực trạng cho thấy có hiện tượng tập trung đầu tư cho lớp hạ tầng kỹ thuật bên ngoài bằng hệ thống tường lửa và thiết bị hiện đại, nhưng quy trình quản trị nội bộ và bảo mật nội dung dữ liệu bên trong chưa được hoàn thiện.

Đánh giá thực tiễn triển khai tại các bộ, ngành và địa phương cho thấy vẫn tồn tại các rủi ro hệ thống về an ninh dữ liệu. Một số đơn vị chủ chốt tiềm ẩn nguy cơ mất an toàn do việc thực hiện thuê dịch vụ hạ tầng công nghệ thông tin thiếu cơ chế kiểm soát chặt chẽ hoặc chưa hoàn thiện hệ thống bảo vệ đồng bộ. Tại nhiều bộ, ngành, việc thiếu hụt các tiêu chuẩn bảo mật nghiêm ngặt và sự dàn trải trong phân bổ nguồn lực đầu tư đã dẫn đến các lỗ hổng bảo mật tích tụ qua nhiều năm. Thực trạng này tạo điều kiện cho các chiến dịch tấn công mã hóa dữ liệu (Ransomware) nhắm trực tiếp vào các hệ thống quản lý chuyên ngành của Nhà nước. Minh chứng là các sự cố tấn công vào các tập đoàn tài chính và năng lượng lớn đầu năm 2024, gây ngưng trệ hoạt động vận hành trong nhiều ngày và bộc lộ hạn chế về năng lực ứng phó tại chỗ của đội ngũ kỹ thuật. Thống kê chỉ có khoảng 25% tổ chức tại Việt Nam áp dụng quy trình sao lưu và phục hồi dữ liệu đáp ứng tiêu chuẩn khôi phục hoạt động dưới 24 giờ sau khi xảy ra sự cố, phản ánh sự thiếu chủ động trong việc chuẩn bị các phương án xử lý tình huống khẩn cấp.

Hậu quả của các hạn chế kỹ thuật này không chỉ dừng lại ở nguy cơ thất thoát dữ liệu mà còn gây gián đoạn quá trình liên thông dữ liệu quốc gia. Nhiều hệ thống thông tin của các Bộ, ngành chưa bảo đảm đầy đủ các điều kiện an ninh mạng để kết nối, khai thác dữ liệu từ Cơ sở dữ liệu quốc gia về dân cư, làm ảnh hưởng đến tiến độ cải cách thủ tục hành chính và gây lãng phí nguồn lực. Sự thiếu đồng bộ về thông tin giữa các cơ quan chủ quản tác động đến công tác điều hành của Chính phủ, khiến việc chuyển đổi từ hồ sơ giấy sang dữ liệu số tại một số lĩnh vực bị chậm tiến độ, gây khó khăn cho người dân và doanh nghiệp trong việc tiếp cận dịch vụ công trực tuyến.

Phân tích nguyên nhân của các tồn tại nêu trên chỉ ra rằng yếu tố con người và quy trình quản lý nội bộ là nguyên nhân gốc rễ. Khoảng 60% đến 70% số vụ lộ lọt dữ liệu ghi nhận có nguyên nhân từ sai phạm nội bộ hoặc do sự thiếu trách nhiệm, thiếu kiến thức chuyên môn của cán bộ quản trị hệ thống. Việt Nam đang thiếu hụt nguồn nhân lực chất lượng cao về Quản trị dữ liệu (Data Governance); lực lượng chuyên trách tại nhiều địa phương chủ yếu thực hiện nhiệm vụ theo chế độ kiêm nhiệm, thiếu công cụ phân tích kỹ thuật và kỹ năng xử lý sự cố thực tế. Ngoài ra, các đơn vị chưa chủ động phối hợp với các cơ quan chuyên trách thuộc Bộ Công an, Bộ Thông tin và Truyền thông để thực hiện đánh giá lại an ninh hệ thống mỗi khi thay đổi cấu trúc kỹ thuật hoặc cập nhật tính năng phần mềm mới. Chế tài xử phạt hành chính hiện hành ở mức thấp, chưa đủ sức răn đe so với lợi nhuận từ các hoạt động mua bán dữ liệu trái phép trên thị trường tự do, dẫn đến việc doanh nghiệp chưa đầu tư đúng mức cho hệ thống bảo mật chuyên sâu.

Trong thời gian tới, tình hình an ninh dữ liệu dự báo diễn biến phức tạp hơn dưới tác động của công nghệ trí tuệ nhân tạo (AI). Tội phạm mạng tăng cường sử dụng AI để tự động hóa các phương thức tấn công, tạo ra các biến thể mã độc liên tục và thực hiện các hành vi lừa đảo bằng công nghệ Deepfake với trình độ tinh vi cao. Thực trạng này tạo ra sự chênh lệch về năng lực công nghệ khi phương thức tấn công được cập nhật liên tục, trong khi công tác phòng thủ của các cơ quan, tổ chức còn chịu ràng buộc bởi các quy trình hành chính và công cụ bảo mật truyền thống. Sự hình thành của công nghệ máy tính lượng tử cũng đặt ra các thách thức đối với các thuật toán mã hóa hiện tại, đòi hỏi phải khẩn trương nghiên cứu và triển khai các giải pháp mã hóa hậu lượng tử để bảo vệ nguồn dữ liệu nhạy cảm của quốc gia.

4. Nguyên nhân của những tồn tại, hạn chế

Qua công tác thanh tra, kiểm tra đến năm 2025, ba nguyên nhân chính được xác định là:

- Thiếu cơ chế bắt buộc đánh giá lại an ninh hệ thống khi có thay đổi về cấu trúc kỹ thuật hoặc tính năng, dẫn đến phát sinh điểm yếu bảo mật mới không được phát hiện kịp thời.

- Nhiều đơn vị tập trung bảo vệ hệ thống dịch vụ công trực tiếp với người dùng, chưa bảo vệ tương xứng hệ thống lõi và các điểm kết nối trung gian, nơi lưu trữ, xử lý phần lớn dữ liệu quan trọng.

- Chưa ban hành đầy đủ quy chế, quy trình vận hành và bảo đảm an toàn theo tiêu chuẩn kỹ thuật (như ISO/IEC 27001 hoặc tương đương), là một nguyên nhân trực tiếp dẫn đến các vụ việc mất dữ liệu, lộ lọt thông tin cá nhân quy mô lớn.

III. ĐỀ XUẤT, KIẾN NGHỊ

Từ thực trạng phân tán trong quản lý, hạn chế về biện pháp kỹ thuật tại một số bộ, ngành và thiếu cơ chế phối hợp đánh giá an ninh dữ liệu định kỳ, việc xây dựng hệ thống giải pháp đồng bộ theo ba nhóm: hoàn thiện thể chế, quy trình; nâng cao năng lực công nghệ; phát triển nguồn nhân lực là cần thiết.

1. Về thể chế, quy trình: hoàn thiện khung pháp luật thống nhất bảo đảm an ninh xuyên suốt vòng đời dữ liệu

Kiến nghị ban hành Luật An ninh dữ liệu làm cơ sở áp dụng thống nhất với Luật An ninh mạng, Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, khắc phục tình trạng quy định phân tán hiện nay. Nội dung này được thể chế hóa tại Điều 1 dự thảo Luật, xác lập nguyên tắc: nội dung an ninh của bản thân dữ liệu xuyên suốt vòng đời áp dụng theo Luật này; nội dung an toàn hệ thống thông tin áp dụng theo pháp luật về an ninh mạng; quyền của chủ thể dữ liệu cá nhân áp dụng theo pháp luật về bảo vệ dữ liệu cá nhân.

Kiến nghị thiết lập cơ chế đánh giá, phân cấp rủi ro an ninh dữ liệu áp dụng thống nhất, làm căn cứ xác định biện pháp bảo vệ tương xứng, đồng thời kế thừa Danh mục dữ liệu quan trọng, dữ liệu cốt lõi đã có theo Luật Dữ liệu, không xây dựng danh mục trùng lặp. Nội dung này được thể chế hóa tại Điều 8 dự thảo Luật (04 cấp độ rủi ro an ninh dữ liệu) và Điều 10 dự thảo Luật (nghĩa vụ đánh giá tác động khi triển khai hệ thống mới hoặc thay đổi công nghệ).

2. Về công nghệ, biện pháp kỹ thuật: bảo vệ dữ liệu xuyên suốt vòng đời, tăng cường tự chủ hạ tầng

Kiến nghị quy định nghĩa vụ lưu trữ trong nước đối với dữ liệu có mức độ rủi ro cao thuộc lĩnh vực có tác động trực tiếp đến quốc phòng, an ninh, tài chính - ngân hàng, năng lượng, viễn thông, hạn chế phụ thuộc vào hạ tầng lưu trữ nước ngoài. Nội dung này được thể chế hóa tại Điều 17 dự thảo Luật.

Kiến nghị quy định lộ trình bắt buộc chuyển đổi sang mật mã kháng lượng tử theo mức độ ưu tiên, kèm cơ chế rà soát định kỳ về mức độ sẵn sàng công nghệ. Nội dung này được thể chế hóa tại Điều 15 dự thảo Luật.

Kiến nghị quy định cơ chế giám sát an ninh dữ liệu tập trung, kết nối với mạng lưới cơ quan, tổ chức chuyên trách đã hình thành, giới hạn thẩm quyền tiếp nhận, phân tích ở lớp siêu dữ liệu, không can thiệp nội dung dữ liệu thô trừ trường hợp khẩn cấp về an ninh quốc gia hoặc phục vụ điều tra theo trình tự tố tụng. Nội dung này được thể chế hóa tại Điều 18 dự thảo Luật.

3. Về con người, lực lượng: phát triển nguồn nhân lực chuyên trách an ninh dữ liệu

Kiến nghị quy định yêu cầu về chứng nhận chuyên môn an ninh dữ liệu đối với nhân sự vận hành trực tiếp hệ thống xử lý dữ liệu Cấp độ 3, Cấp độ 4; việc chuẩn hóa chức danh cụ thể trong bộ máy tổ chức của từng cơ quan, doanh nghiệp thuộc phạm vi văn bản hướng dẫn thi hành và pháp luật về tổ chức bộ máy. Nội dung này được thể chế hóa tại Điều 21 dự thảo Luật.

Kiến nghị xác lập lực lượng bảo vệ an ninh dữ liệu quốc gia trong lực lượng chuyên trách bảo vệ an ninh mạng đã có theo pháp luật về an ninh mạng, không hình thành lực lượng chuyên trách mới, với Bộ Công an chủ trì, điều phối tổng thể, Bộ Quốc phòng chủ trì đối với dữ liệu quân sự, quốc phòng. Nội dung này được thể chế hóa tại Điều 21 dự thảo Luật.

Kiến nghị quy định trách nhiệm tuyên truyền, phổ biến pháp luật về an ninh dữ liệu cho cơ quan, tổ chức, cá nhân, góp phần nâng cao nhận thức, hạn chế rủi ro từ yếu tố con người. Nội dung này được thể chế hóa tại Điều 23 dự thảo Luật.

Kiến nghị quy định mức phạt tiền theo tỷ lệ doanh thu đối với hành vi vi phạm đặc biệt nghiêm trọng gây rò rỉ, chiếm đoạt, phá hoại dữ liệu Cấp độ 3, Cấp độ 4, bảo đảm tính răn đe tương xứng với lợi ích thu được từ hành vi vi phạm. Nội dung này được thể chế hóa tại Điều 23 dự thảo Luật.

Việc thực hiện đồng bộ ba nhóm giải pháp về thể chế, công nghệ và nguồn nhân lực nêu trên là cơ sở để khắc phục những hạn chế đã nêu tại Mục II Báo cáo này, đáp ứng yêu cầu quản lý nhà nước về an ninh dữ liệu và phát triển kinh tế số, Chính phủ số, xã hội số.

Lực lượng này sẽ đóng vai trò nòng cốt để khắc phục các tồn tại về việc thiếu quy trình, quy chế vận hành nội bộ hoặc thiếu phối hợp kiểm tra an ninh hệ thống như thực trạng đã nêu. Đồng thời, cần triển khai chiến lược phổ cập nhận thức và thói quen an ninh dữ liệu cho toàn dân thông qua ứng dụng VNeID. Khi mỗi công dân và cán bộ vận hành đều có ý thức bảo mật, khả năng phòng thủ của toàn xã hội sẽ được nâng cao. Cần nâng tầm sự phối hợp giữa hơn 200 đơn vị chuyên trách và các tập đoàn công nghệ lớn (như Viettel, VNPT, FPT...) thành cơ chế phối hợp bảo vệ chủ quyền dữ liệu quốc gia, thực hiện chia sẻ thông tin sự cố theo thời gian thực để chủ động ứng phó với các cuộc tấn công mạng quy mô lớn.

Công tác bảo đảm an ninh dữ liệu đòi hỏi quy trình quản trị và cập nhật liên tục. Các kết quả về thăng tiến thứ hạng quốc tế theo đánh giá của ITU hoặc sự suy giảm tỷ lệ lây nhiễm mã độc là những chỉ số tích cực, nhưng các lỗ hổng bảo mật tại một số bộ, ngành và các sự cố mất dữ liệu thời gian qua đòi hỏi phải có giải pháp khắc phục triệt để. Việc thực hiện đồng bộ ba nhóm giải pháp: Thống nhất thể chế pháp lý - Tự chủ công nghệ hạ tầng - Chuyên nghiệp hóa

nguồn nhân lực là giải pháp để Việt Nam bảo vệ tài nguyên số quốc gia, bảo đảm niềm tin của người dân và thúc đẩy sự phát triển bền vững trong quá trình chuyển đổi số.

Trên đây là Báo cáo đánh giá thực trạng quan hệ xã hội liên quan đến dự thảo Luật An ninh dữ liệu, Bộ Công an kính trình Chính phủ. / *lg*

Nơi nhận:

- Như trên;
- Thủ tướng, các Phó Thủ tướng (để báo cáo);
- Bộ trưởng Bộ Công an (để báo cáo);
- Văn phòng Chính phủ (để phối hợp);
- Bộ Tư pháp;
- Lưu: VT, A05. NTXT.

**KT. BỘ TRƯỞNG
THỦ TRƯỞNG**



Thượng tướng Phạm Thế Tùng