

Số: /BC-BCA

Hà Nội, ngày tháng năm 2026

BÁO CÁO**Đánh giá thực trạng quan hệ xã hội
liên quan đến chính sách của Luật An ninh dữ liệu**

Thực hiện quy định của Luật Ban hành văn bản quy phạm pháp luật năm 2025 và các văn bản quy phạm pháp luật quy định chi tiết, hướng dẫn thi hành có liên quan, Bộ Công an báo cáo đánh giá thực trạng quan hệ xã hội liên quan đến chính sách của Luật An ninh dữ liệu, cụ thể như sau:

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

Trong kỷ nguyên của cuộc Cách mạng công nghiệp lần thứ tư, thế giới đang chứng kiến một sự chuyển dịch quyền lực mang tính thời đại: từ quyền lực dựa trên tài nguyên hữu hình sang quyền lực dựa trên tài nguyên số, mà hạt nhân cốt lõi chính là dữ liệu. Bối cảnh quốc tế hiện nay không còn là một không gian phẳng về công nghệ mà đã trở thành một chiến trường địa chính trị gay gắt, nơi an ninh dữ liệu đóng vai trò là "lằn ranh đỏ" bảo vệ chủ quyền quốc gia. Thực trạng quan hệ xã hội toàn cầu liên quan đến an ninh dữ liệu đang biến đổi phức tạp, tạo ra những thách thức chưa từng có đối với các quy trình quản trị, biện pháp kỹ thuật và năng lực con người của mọi quốc gia, trong đó có Việt Nam.

Trước hết, bối cảnh thế giới đang chứng kiến sự trỗi dậy mạnh mẽ của "Chủ nghĩa dân tộc dữ liệu" (Data Nationalism). Các quốc gia không còn coi dữ liệu là tài nguyên tự do mà là tài sản chiến lược cần được bảo vệ vĩnh viễn. Các cường quốc như Mỹ, Trung Quốc và Liên minh Châu Âu (EU) đã xác lập những chuẩn mực pháp lý khắt khe để bảo vệ tài sản số của mình. Nếu như EU tiên phong với Quy định chung về bảo vệ dữ liệu (GDPR) nhằm đặt con người làm trung tâm của quyền riêng tư, thì Trung Quốc lại thực thi Luật An ninh dữ liệu với trọng tâm là kiểm soát luồng dữ liệu xuyên biên giới để bảo vệ an ninh quốc gia. Sự phân mảnh này tạo ra một thực trạng quan hệ xã hội mới: dữ liệu không còn được lưu chuyển tự do mà bị ngăn cách bởi các "hàng rào thuế quan số". Điều này hình thành nên các quan hệ pháp lý mới, yêu cầu các tập đoàn đa quốc gia phải tuân thủ quyền

tài phán địa phương. Việt Nam đang đứng trước yêu cầu phải đồng bộ hóa quy trình nội địa với các tiêu chuẩn quốc tế này để vừa bảo vệ dữ liệu quốc gia, vừa không bị cô lập trong nền kinh tế số toàn cầu. Quan hệ giữa các quốc gia hiện nay không chỉ là hợp tác thương mại mà còn là cuộc đấu tranh về quyền tài phán dữ liệu - nơi mà bên nào nắm giữ hạ tầng lưu trữ và thuật toán xử lý sẽ nắm giữ quyền quyết định vận mệnh kinh tế của bên đó.

Thứ hai, sự bùng nổ của Trí tuệ nhân tạo (AI) và dữ liệu lớn (Big Data) đã làm thay đổi hoàn toàn bản chất của các tương tác xã hội. Quan hệ giữa cá nhân và các tập đoàn công nghệ xuyên biên giới (Big Tech) đang trở nên bất đối xứng hơn bao giờ hết. Các biện pháp kỹ thuật truyền thống như tường lửa hay phần mềm diệt virus đơn thuần đã trở nên lạc hậu trước các cuộc tấn công sử dụng AI để đánh cắp và thao túng dữ liệu. Thực trạng này tạo ra một cuộc khủng hoảng niềm tin số trên quy mô toàn cầu. Khi dữ liệu cá nhân bị rao bán công khai trên các diễn đàn tin tặc hoặc bị lợi dụng để tạo ra các video giả mạo (Deepfake), quan hệ niềm tin giữa con người với con người và giữa công dân với Nhà nước bị rạn nứt nghiêm trọng. Bối cảnh này đòi hỏi các biện pháp an ninh dữ liệu phải chuyển từ phòng ngự thụ động sang quản trị chủ động, sử dụng chính AI để giám sát và bảo vệ dữ liệu theo thời gian thực, đồng thời phải có quy trình xác thực dữ liệu gốc để duy trì trật tự xã hội số.

Thứ ba, yếu tố con người trong an ninh dữ liệu đang trở thành trọng tâm của cuộc chạy đua vũ trang số toàn cầu. Thế giới đang thiếu hụt trầm trọng các "Vệ binh số" - những chuyên gia không chỉ giỏi kỹ thuật mà còn am hiểu về luật pháp và đạo đức dữ liệu. Quan hệ xã hội trong lĩnh vực lao động số đang dịch chuyển: các quốc gia ráo riết thu hút nhân tài an ninh mạng để bảo vệ các hạ tầng trọng yếu như ngân hàng, năng lượng và viễn thông. Thực trạng cho thấy, hơn 80% các vụ lộ lọt dữ liệu lớn trên thế giới vẫn xuất phát từ sai lầm của con người. Do đó, bối cảnh quốc tế hiện nay nhấn mạnh vào việc xây dựng "Văn hóa an ninh dữ liệu" cho toàn dân. Một quốc gia mạnh về an ninh dữ liệu không chỉ là quốc gia có nhiều siêu máy tính, mà là quốc gia có đội ngũ nhân lực chuyên trách tinh nhuệ và những công dân có "sức đề kháng số" cao, đủ khả năng nhận diện các âm mưu diễn biến hòa bình hay phá hoại kinh tế thông qua môi trường dữ liệu.

Thứ tư, sự cạnh tranh về hạ tầng số và chủ quyền lưu trữ đang tái cấu trúc các liên minh quốc tế. Việc lệ thuộc vào các nền tảng điện toán đám mây (Cloud) của nước ngoài đã bộc lộ những rủi ro địa chính trị cực lớn. Khi một quốc gia bị

cắt đứt quyền truy cập vào dữ liệu lưu trữ trên máy chủ nước ngoài, toàn bộ nền kinh tế có thể bị đình trệ. Điều này thúc đẩy xu hướng bảo vệ vĩnh viễn dữ liệu cốt lõi bằng cách lưu trữ tại các Trung tâm dữ liệu quốc gia (như mô hình DC1 của Việt Nam) và áp dụng mã hóa hậu lượng tử để chống lại sự can thiệp của các cường quốc công nghệ trong tương lai. Quan hệ xã hội giữa các quốc gia đang dần dịch chuyển sang việc hình thành các "vùng xanh dữ liệu" - những liên minh cam kết bảo vệ dữ liệu của nhau dựa trên các tiêu chuẩn an ninh đồng bộ và minh bạch.

Bối cảnh thế giới liên quan đến an ninh dữ liệu hiện nay là một bức tranh đa sắc thái, nơi cơ hội phát triển kinh tế số đi đôi với rủi ro mất chủ quyền số. Thực trạng quan hệ xã hội cho thấy sự đan xen phức tạp giữa quy trình quản trị, biện pháp công nghệ và năng lực con người. Để không bị tụt hậu và bị tổn thương trong dòng chảy này, Việt Nam cần một chiến lược an ninh dữ liệu mang tính đồng bộ và toàn vẹn. Chúng ta phải xây dựng một hệ sinh thái mà ở đó, pháp luật đóng vai trò định hướng quy trình, công nghệ đóng vai trò lá chắn bảo vệ vĩnh viễn tài sản quốc gia, và con người là lực lượng nòng cốt vận hành và thực thi. Việc ban hành Luật An ninh dữ liệu lúc này chính là câu trả lời chiến lược, giúp Việt Nam khẳng định vị thế, bảo vệ tài nguyên số quý giá và kiến tạo một xã hội số an toàn, thịnh vượng trước những biến động không ngừng của tình hình quốc tế. Dữ liệu là máu thịt của quốc gia trong kỷ nguyên số, và bảo vệ an ninh dữ liệu chính là bảo vệ sự trường tồn của dân tộc trên không gian mạng vĩnh cửu.

2. Bối cảnh trong nước

Việt Nam đang bước vào giai đoạn bùng nổ của tiến trình chuyển đổi số quốc gia, nơi dữ liệu được xác định là nguồn tài nguyên chiến lược, là "mạch máu" nuôi dưỡng Chính phủ số, kinh tế số và xã hội số. Điểm sáng lớn nhất là sự hình thành và phát triển vượt bậc của hệ thống Trung tâm dữ liệu quốc gia (tiêu biểu là mô hình DC1), đóng vai trò là "pháo đài số" lưu trữ và kết nối các nguồn tài nguyên dữ liệu cốt lõi của quốc gia. Tuy nhiên, sự lớn mạnh về quy mô hạ tầng này lại chưa đi đôi với một chiến lược an ninh dữ liệu toàn diện. Thực tế cho thấy dữ liệu càng tập trung, giá trị càng cao thì mục tiêu tấn công của các thế lực thù địch và tội phạm mạng càng trở nên rõ rệt. Việc phát triển hạ tầng thần tốc nhưng thiếu một "luật khung" thống nhất về an ninh dữ liệu dẫn đến rủi ro mất an toàn hệ thống, đe dọa trực tiếp đến sự ổn định chính trị và trật tự xã hội. Phân tích bối cảnh Việt Nam hiện nay đòi hỏi một cái nhìn đa chiều, soi chiếu qua sự tương tác

giữa quy trình quản trị, biện pháp kỹ thuật và yếu tố con người trong một hệ sinh thái đang dần hình thành nhưng còn nhiều đứt gãy cần phải định hình, phát triển, để hướng tới nền an ninh dữ liệu bền vững.

Thứ nhất, sự chuyển dịch các quan hệ dân sự và cuộc khủng hoảng niềm tin số. Trong bối cảnh gần 80 triệu người dân Việt Nam hiện diện trên không gian mạng, các quan hệ xã hội truyền thống đã được số hóa toàn diện. Từ việc thanh toán không dùng tiền mặt, khám chữa bệnh từ xa đến thực hiện dịch vụ công trực tuyến, mọi hành vi của công dân đều để lại "dấu chân số". Thực trạng này đã nảy sinh một quan hệ xã hội mới: quan hệ giữa chủ thể dữ liệu (người dân) và bên kiểm soát dữ liệu (tổ chức, doanh nghiệp). Tuy nhiên, bối cảnh thực tế tại Việt Nam đang chứng kiến một cuộc khủng hoảng niềm tin trầm trọng do vấn nạn lộ lọt dữ liệu cá nhân. Các vụ rao bán hàng tỷ dòng dữ liệu trên các diễn đàn tin tặc không chỉ là sự cố kỹ thuật mà còn là sự đổ vỡ của các cam kết dân sự. Khi thông tin định danh, số điện thoại và tài khoản ngân hàng bị chiếm đoạt để phục vụ cho các chiến dịch lừa đảo công nghệ cao sử dụng AI (Deepfake), người dân rơi vào trạng thái "bất an số". Điều này phản ánh sự yếu kém trong quy trình bảo vệ và biện pháp kỹ thuật của nhiều đơn vị, khi họ thu thập dữ liệu thì tối đa nhưng bảo vệ thì tối thiểu.

Thứ hai, thực trạng quan hệ quản trị nhà nước và bài toán chủ quyền dữ liệu. Chính phủ Việt Nam đã có những bước đi đột phá với Đề án 06 và việc vận hành Cơ sở dữ liệu quốc gia về Dân cư. Đây là nền tảng cốt lõi để xác lập trật tự xã hội số. Tuy nhiên, mối quan hệ giữa các cơ quan nhà nước trong việc chia sẻ và kết nối dữ liệu đang gặp phải rào cản về tính đồng bộ. Quy trình liên thông dữ liệu qua trục NDXP đã hình thành nhưng các biện pháp kỹ thuật bảo vệ tại "điểm cuối" - đặc biệt là ở cấp địa phương - vẫn là mắt xích yếu nhất. Quan hệ quản trị còn đối mặt với thách thức về chủ quyền khi phần lớn dữ liệu quan trọng của các doanh nghiệp và tổ chức vẫn đang lưu trữ trên hạ tầng điện toán đám mây nước ngoài. Điều này đặt Việt Nam vào tình thế "lệ thuộc tài nguyên số", nơi quyền tài phán quốc gia bị hạn chế bởi các quy định của các tập đoàn Big Tech xuyên biên giới. Việc xác lập dữ liệu cốt lõi là tài sản quốc gia đặc biệt và áp dụng biện pháp bảo vệ vĩnh viễn chính là lời giải để khẳng định chủ quyền và quyền tự quyết của quốc gia trên không gian số.

Thứ ba, sự xung đột lợi ích trong quan hệ kinh tế số và an ninh thuật toán. Dữ liệu đã trở thành tư liệu sản xuất chính, tạo ra giá trị thặng dư khổng lồ cho

nền kinh tế Việt Nam. Tuy nhiên, quan hệ giữa các doanh nghiệp công nghệ và người dùng đang nảy sinh những mặt trái về "độc quyền dữ liệu" và khai thác trái phép thông tin để trục lợi. Thực trạng cho thấy, nhiều doanh nghiệp nhỏ và vừa (SMEs) tại Việt Nam vẫn đứng ngoài lề của các tiêu chuẩn an ninh dữ liệu do chi phí đầu tư lớn. Các biện pháp kỹ thuật như mã hóa hay sao lưu dự phòng (Backup) thường bị bỏ qua để ưu tiên lợi nhuận. Khi các cuộc tấn công mã hóa dữ liệu (Ransomware) nhắm vào các tập đoàn lớn như VNDIRECT hay PVOIL xảy ra, nó không chỉ gây thiệt hại kinh tế cục bộ mà còn làm gián đoạn dòng chảy kinh tế quốc gia, gây hoang mang cho các nhà đầu tư. Điều này đặt ra yêu cầu cấp thiết về việc phải có một quy trình kiểm soát an ninh dữ liệu bắt buộc và cơ chế bảo hiểm rủi ro số để bảo vệ các quan hệ kinh tế số bền vững.

Thứ tư, yếu tố con người và khoảng cách về năng lực chuyên trách. Trong hệ sinh thái an ninh dữ liệu của Việt Nam, con người vừa là lực lượng bảo vệ, vừa là điểm yếu chí mạng. Các chiến dịch tấn công mạng có bảo trợ của quốc gia nhắm vào Dữ liệu cốt lõi (tài chính, năng lượng, quốc phòng) đòi hỏi đội ngũ chuyên gia nòng cốt của Việt Nam phải có năng lực đối kháng tầm quốc tế. Thực trạng hiện nay cho thấy sự thiếu hụt trầm trọng đội ngũ chuyên gia nòng cốt có khả năng quản trị dữ liệu ở tầm chiến lược. Trong khi lực lượng chuyên trách của Bộ Công an và Bộ Quốc phòng đã có những bước tiến về tinh nhuệ, thì lực lượng chuyên trách tại các Bộ, ngành và địa phương lại thường xuyên ở trạng thái "kiêm nhiệm", thiếu hụt công cụ và kỹ năng xử lý sự cố thực tế. Quan hệ xã hội trong lĩnh vực nhân sự số cũng bộc lộ sự dịch chuyển "chảy máu chất xám" từ khu vực công sang khu vực tư, làm suy yếu năng lực thực thi pháp luật an ninh dữ liệu của các cơ quan nhà nước. Hơn nữa, văn hóa an ninh dữ liệu của đại bộ phận công dân vẫn còn sơ khai, thói quen chia sẻ thông tin nhạy cảm trên mạng xã hội vô hình trung đã "tiếp tay" cho tội phạm mạng.

Có thể nói, bối cảnh Việt Nam hiện nay là một bức tranh đan xen giữa khát vọng chuyển đổi số mạnh mẽ và những nguy cơ an ninh hiện hữu do sự thiếu đồng bộ trong quản trị. Thực trạng các quan hệ xã hội liên quan đến an ninh dữ liệu đang đòi hỏi một cuộc cách mạng về thể chế. Việc ban hành Luật An ninh dữ liệu không chỉ là để tạo ra những rào cản hành chính, mà là để kiến tạo một hệ sinh thái đồng bộ: nơi Quy trình bảo vệ vòng đời dữ liệu được chuẩn hóa, các Biện pháp kỹ thuật tự chủ "Make in Vietnam" trở thành lá chắn vững chắc, và yếu tố Con người được đặt ở vị trí trung tâm của mọi nỗ lực bảo vệ. Chỉ khi tài sản dữ

liệu cốt lõi được bảo vệ vĩnh viễn và các quan hệ xã hội số được vận hành trên nền tảng niềm tin và sự an toàn, Việt Nam mới thực sự làm chủ được vận mệnh của mình trong kỷ nguyên số hóa toàn cầu. Dữ liệu là tài nguyên, nhưng an ninh dữ liệu là sự sống còn của quốc gia.

3. Các chủ trương đường lối của Đảng, chính sách pháp luật của Nhà nước về an ninh dữ liệu

Các chủ trương, đường lối của Đảng đóng vai trò là "kim chỉ nam" chiến lược, quyết định tính chất và định hướng phát triển của các quan hệ xã hội trong kỷ nguyên số. Trước thực trạng các quan hệ xã hội về an ninh dữ liệu đang diễn biến phức tạp, Đảng ta đã ban hành nhiều Nghị quyết, Chỉ thị mang tính đột phá, thể hiện tầm nhìn xa về việc bảo vệ chủ quyền quốc gia trên không gian mạng và coi dữ liệu là tài nguyên chiến lược đặc biệt.

Thời điểm hiện tại, nhiều văn bản quy phạm pháp luật quy định về vấn đề phát triển, đẩy mạnh dữ liệu và công tác lưu trữ dữ liệu, bảo đảm an ninh dữ liệu đã được ban hành, có thể kể đến một số văn bản như sau:

Luật An toàn thông tin mạng số 86/2015/QH13 được Quốc hội khóa XII thông qua vào ngày 19/11/2015 và có hiệu lực thi hành từ ngày 01/7/2016 quy định các nguyên tắc, biện pháp bảo đảm an toàn thông tin.

Luật An ninh mạng số 24/2018/QH14 được Quốc hội khóa XIV thông qua ngày 12/6/2018 và có hiệu lực thi hành từ ngày 01/01/2019 có quy định yêu cầu các doanh nghiệp cung cấp dịch vụ mạng (trong và ngoài nước) phải lưu trữ dữ liệu cá nhân người dùng tại Việt Nam.

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 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 và nghĩa vụ bảo vệ dữ liệu cá nhân, thiết lập khung pháp lý chặt chẽ trong thu thập, xử lý và bảo vệ quyền riêng tư của người 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 1/7/2026 quy định về, lần đầu tiên Luật hóa khái niệm an ninh dữ liệu và xác định bảo đảm an ninh dữ liệu là một

phần cốt lõi của bảo vệ an ninh mạng quốc gia (là luật hợp nhất Luật an ninh mạng 2018 và Luật An toàn thông tin 2015, có hiệu lực thi hành từ ngày 01/7/2026).

Có thể thấy, hệ thống các văn bản pháp luật quy định về dữ liệu, quy định về vấn đề phát triển dữ liệu, hoàn thiện cơ sở hạ tầng thông tin trong chuyển đổi số ở Việt Nam đã được ban hành kịp thời điều chỉnh, phù hợp với sự phát triển của dữ liệu, ứng dụng khoa học công nghệ trong xử lý dữ liệu. Tuy nhiên, đến nay bên cạnh những kết quả tích cực đạt được, thực tiễn cũng cho thấy một số quy định của pháp luật liên quan đến dữ liệu, đặc biệt là vấn đề bảo đảm an ninh dữ liệu: quy trình, công nghệ, con người vẫn còn rất hạn chế dẫn đến trong thực tiễn việc tổ chức thực hiện chức năng quản lý, bảo đảm an ninh dữ liệu tại nhiều bộ, ngành, địa phương thiếu thống nhất, hiệu quả đạt được còn hạn chế, chưa thu hút nhân lực công nghệ cao và còn tiềm ẩn rất nhiều rủi ro đối với hệ thống dữ liệu quốc gia, điều này ảnh hưởng trực tiếp đến quá trình xây dựng, phát triển Chính phủ số, xã hội số và kinh tế số.

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

1.1. 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 đang đứng trước ngưỡng cửa của kỷ nguyên số với tốc độ tăng trưởng kinh tế số thuộc hàng cao nhất khu vực ASEAN. Dữ liệu không còn là một khái niệm kỹ thuật thuần túy mà đã trở thành "huyết mạch" duy trì sự vận hành của toàn bộ hệ thống chính trị, kinh tế và xã hội. Trong bối cảnh đó, các quan hệ xã hội truyền thống đang dịch chuyển mạnh mẽ sang môi trường không gian mạng, hình thành nên các mối liên kết mới giữa Nhà nước - Doanh nghiệp - Công dân dựa trên nền tảng trao đổi và khai thác dữ liệu.

Tuy nhiên, thực trạng hiện nay cho thấy sự phát triển của các quan hệ xã hội này đang chạy nhanh hơn năng lực quản trị an ninh. Khi dữ liệu trở thành tài sản, nó đồng thời trở thành mục tiêu tấn công hàng đầu của các loại tội phạm công nghệ cao và các thế lực thù địch. Thực trạng an ninh dữ liệu tại Việt Nam đang bộc lộ những lỗ hổng mang tính hệ thống, đe dọa trực tiếp đến an ninh quốc gia, trật tự an toàn xã hội và quyền lợi hợp pháp của mọi thành viên trong cộng đồng.

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

Thể chế và quy trình đóng vai trò là "bộ não" điều hành các quan hệ xã hội. Tuy nhiên, thực trạng tại Việt Nam đang đối mặt với sự đứt gãy trong 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. Quy trình bảo mật tại các khâu nhạy cảm như chia sẻ, Phân tích và đặc biệt là tiêu hủy vĩnh viễn hầu như đang bị bỏ ngỏ. Nhiều tổ chức thu thập dữ liệu người dùng một cách ồ ạt nhưng lại thiếu quy trình kiểm soát khi dữ liệu này được chuyển giao cho bên thứ ba hoặc khi dữ liệu đã hết giá trị sử dụng. Việc thiếu một quy trình tiêu hủy chuẩn hóa dẫn đến tình trạng "rác dữ liệu" tồn tại trên các máy chủ cũ, trở thành "mỏ vàng" cho tin tặc 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 an ninh dữ liệu vẫn nằm tản mát, thiếu tính hệ thống. Quan hệ giữa các cơ quan quản lý nhà nước đôi khi còn chồng chéo về chức năng hoặc đùn đẩy trách nhiệm khi xảy ra sự cố lộ lọt dữ liệu. Đặc biệt, chúng ta chưa có quy trình pháp lý cụ thể để xác lập và bảo vệ Dữ liệu cốt lõi quốc gia như một loại tài sản công đặc biệt. Điều này dẫn đến thực trạng các túi dữ liệu chiến lược bị bảo vệ dàn trải, không có sự ưu tiên nguồn lực tương xứng với tầm quan trọng của chúng.

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

Công nghệ là "lá chắn" thực thi các quan hệ an ninh, nhưng tại Việt Nam, lá chắn này vẫn còn nhiều điểm yếu chí mạng.

- Sự lệ thuộc vào hạ tầng quốc tế và nguy cơ mất chủ quyền số. Một thực trạng đáng báo động trong quan hệ kinh tế số hiện nay là sự lệ thuộc quá lớn vào hạ tầng lưu trữ xuyên biên giới. Ước tính khoảng 80% dữ liệu điện toán đám mây của doanh nghiệp Việt Nam đang đặt tại các máy chủ của nước ngoài. Quan hệ xã hội về dữ liệu vì thế bị chi phối bởi quyền tài phán của các quốc gia khác. Các biện pháp kỹ thuật hiện nay chưa đủ mạnh để thiết lập một "hàng rào kỹ thuật" tự động nhằm kiểm soát luồng dữ liệu quan trọng chảy ra khỏi biên giới quốc gia, tiềm ẩn nguy cơ "chảy máu tài nguyên số" vĩnh viễn.

- Biện pháp kỹ thuật chưa tương xứng với sự phát triển của AI Tội phạm mạng đang sử dụng Trí tuệ nhân tạo (AI) để thực hiện các cuộc tấn công mã hóa dữ liệu (Ransomware) và tạo ra thông tin giả mạo (Deepfake). Trong khi đó, biện pháp bảo vệ tại phần lớn các đơn vị tại Việt Nam vẫn chỉ dừng lại ở các bức tường lửa (Firewall) truyền thống và phần mềm diệt virus cơ bản. Việc ứng dụng mã hóa hậu lượng tử (Post-Quantum Cryptography) để bảo vệ vĩnh viễn dữ liệu cốt lõi vẫn còn là khái niệm mới mẻ. Sự bất đối xứng về công nghệ giữa bên tấn công và bên phòng thủ đang đẩy các quan hệ xã hội về niềm tin số vào thế bấp bênh.

d) Khía cạnh con người và lực lượng: mất xích yếu nhất và tài sản quý giá nhất

Trong mọi quan hệ xã hội, con người luôn là trung tâm. 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.

- Khủng hoảng nhân lực quản trị dữ liệu chuyên sâu: Việt Nam đang thiếu trầm trọng đội ngũ chuyên gia về Quản trị dữ liệu (Data Governance). Lực lượng chuyên trách tại các Bộ, ngành và địa phương hiện nay chủ yếu làm nhiệm vụ kiêm nhiệm, thiên về xử lý hạ tầng hơn là quản trị an ninh nội dung dữ liệu. Sự dịch chuyển nhân tài từ khu vực công sang khu vực tư vì lý do thu nhập đang làm suy yếu năng lực thực thi của lực lượng "vệ binh số" nòng cốt.

- Ý thức bảo mật và văn hóa dữ liệu của cộng đồng: Thực trạng đau lòng nhất là phần lớn các vụ lộ lọt dữ liệu quy mô lớn tại Việt Nam thời gian qua đều có nguyên nhân từ sai sót của con người. Quan hệ xã hội trên không gian mạng hiện nay đang bị chi phối bởi tâm lý "hòn nhiên số" - người dân sẵn sàng đánh đổi dữ liệu cá nhân nhạy cảm để lấy những tiện ích nhỏ hoặc tham gia vào các trào lưu mạng xã hội thiếu an toàn. Việc thiếu một nền tảng giáo dục về an ninh dữ liệu toàn dân khiến xã hội trở nên dễ bị tổn thương trước các chiến dịch tấn công tâm lý và lừa đảo dựa trên dữ liệu.

e) Quan hệ quốc tế hiện nay: xung đột về quyền tài phán và hợp tác xuyên biên giới

Dữ liệu không có biên giới, do đó quan hệ xã hội về an ninh dữ liệu tại Việt Nam chịu tác động sâu sắc từ bối cảnh quốc tế.

- Thách thức từ các nền tảng xuyên biên giới Quan hệ giữa Nhà nước Việt Nam và các tập đoàn công nghệ đa quốc gia (Facebook, Google, TikTok...) là một

bài toán phức tạp. Thực trạng cho thấy các tập đoàn này thu thập một lượng khổng lồ dữ liệu của công dân Việt Nam nhưng việc thực thi các yêu cầu về an ninh, lưu trữ dữ liệu tại Việt Nam vẫn gặp nhiều rào cản từ các thỏa thuận quốc tế và quy định nội bộ của họ.

- Yêu cầu về đồng bộ quy trình quốc tế Để tham gia vào các hiệp định thương mại tự do thế hệ mới, Việt Nam buộc phải chuẩn hóa quy trình bảo vệ dữ liệu tương đương với các chuẩn mực như GDPR của Châu Âu. Tuy nhiên, việc đồng bộ này đang gặp khó khăn do khoảng cách về trình độ công nghệ và sự khác biệt trong tư duy quản lý.

1.2. Kết quả triển khai thực hiện các văn bản quy phạm pháp luật khác có liên quan đến an ninh dữ liệu

Trong lộ trình xây dựng và 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 có ý nghĩa vô cùng quan trọng. Nhìn lại hành trình này, từ năm 2015 chúng ta thấy rõ một sự chuyển dịch tư duy mang tính bước ngoặt, từ việc chỉ chú trọng bảo vệ hạ tầng vật lý sang việc quản trị nội dung và giá trị cốt lõi của dữ liệu. Việc triển khai Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 đã tạo ra "lá chắn" pháp lý đầu tiên, xác lập trách nhiệm của các cơ quan chuyên trách và hình thành quy trình phân loại hệ thống thông tin theo năm cấp độ bảo mật. Đến hết năm 2025, hệ thống văn bản quy phạm pháp luật hoàn thiện hơn, với sự ra đời của Luật An ninh mạng 2025, Luật Dữ liệu 2024, Luật Bảo vệ dữ liệu cá nhân 2025 đã dần tạo ra những mảnh ghép hoàn chỉnh vào hệ thống pháp luật bảo vệ dữ liệu. Điển hình việc gần 80 % hệ thống thông tin của các cơ quan nhà nước được phê duyệt hồ sơ cấp độ là một minh chứng cho sự nỗ lực chuẩn hóa quy trình vận hành. Tuy nhiên, khi đi sâu vào thực tiễn, chúng ta nhận thấy các quy định này chủ yếu mới dừng lại ở việc bảo vệ "vỏ" hệ thống, trong khi "lõi" dữ liệu bên trong vẫn chưa được bảo vệ xuyên suốt vòng đời. Minh chứng điển hình nhất là vụ rao bán 30 triệu hồ sơ giáo dục năm 2022 và các đợt rò rỉ dữ liệu y tế năm 2024, cho thấy dù hệ thống hạ tầng đạt chuẩn cấp độ nhưng quy trình kiểm soát nội dung tại các đơn vị địa phương vẫn còn rất lỏng lẻo.

Thực trạng này trở nên rõ rệt hơn khi soi chiếu qua 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, nhưng khả năng tự chủ về công nghệ lõi vẫn là một điểm nghẽn 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 một hệ lụy trực tiếp về quyền tài phán: khi dữ liệu của công dân Việt Nam nằm trên máy chủ nước ngoài, việc thực thi các quy trình kiểm soát luồng dữ liệu xuyên biên giới gặp rất nhiều trở ngại. Sự gia tăng đột biến 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, đã phơi bày một thực tế nghiệt ngã rằng chỉ có khoảng 25% tổ chức có quy trình sao lưu và phục hồi dữ liệu đáp ứng tiêu chuẩn hồi phục dưới 24 giờ. Các cuộc tấn công này không chỉ gây đình trệ giao dịch hàng nghìn tỷ đồng mỗi ngày mà còn chứng minh rằng các biện pháp kỹ thuật hiện tại thiếu tính dự phòng chiến lược và chưa đủ sức đối phó với sự tinh vi của tội phạm mạng sử dụng trí tuệ nhân tạo để dò quét lỗ hổng.

Đáng lo ngại nhất trong đánh giá thực thi pháp luật chính là yếu tố con người - mắt xích yếu nhất nhưng lại quyết định sự thành bại của mọi quy trình. Tổng kết các vụ án về dữ liệu trong hai năm qua cho thấy một con số đáng báo động khi có tới 60% đến 70% vụ lộ lọt dữ liệu bắt nguồn từ chính các sai phạm nội bộ hoặc sự thiếu trách nhiệm của cán bộ quản trị. Việc Bộ Công an triệt phá các đường dây mua bán dữ liệu cá nhân quy mô lên tới 1.300 tỷ chi tiết thông tin vào năm 2023 là minh chứng đanh thép nhất. Các đối tượng đã khai thác quyền truy cập từ nhân viên nội bộ của các ngân hàng và công ty bảo hiểm để trích xuất dữ liệu thô. Điều này chứng minh rằng các quy định hiện hành quá chú trọng vào việc chống tấn công từ bên ngoài mà bỏ quên việc kiểm soát đặc quyền truy cập bên trong. Chế tài xử phạt hành chính hiện nay, dù đã được cập nhật, vẫn bị coi là quá thấp so với lợi nhuận khổng lồ từ việc buôn bán tài nguyên số trái phép. Khi một bộ dữ liệu nhạy cảm có giá hàng trăm triệu đồng nhưng mức phạt chỉ dừng lại ở ngưỡng vài chục triệu, nhiều doanh nghiệp sẵn sàng chấp nhận nộp phạt như một chi phí vận hành thay vì đầu tư nghiêm túc vào hệ thống bảo mật chuyên sâu. Đồng thời, sự thiếu hụt khoảng 150.000 đến 200.000 chuyên gia trình độ cao về an ninh dữ liệu dự kiến vào năm 2026 đã khiến cho việc thực thi pháp luật ở cấp cơ sở thường xuyên rơi vào tình trạng hình thức và thiếu tính giám sát.

Tuy nhiên, không thể phủ nhận những thành tựu mang tính đột phá từ việc thực hiện Đề án 06 về phát triển ứng dụng dữ liệu dân cư. Việc Cơ sở dữ liệu quốc gia về Dân cư thực hiện xác thực hơn 1,2 tỷ lượt yêu cầu mỗi năm và chuẩn hóa hơn 125 triệu thuê bao viễn thông đã tạo ra một môi trường dữ liệu "đúng, đủ, sạch, sống". Chiến dịch làm sạch dữ liệu này đã giúp khóa hơn 20 triệu sim rác,

trực tiếp chặt đứt công cụ gây án của tội phạm lừa đảo công nghệ cao. Đây là ví dụ điển hình cho việc dùng biện pháp kết nối tập trung để giải quyết các thực trạng xã hội nhức nhối. Tuy nhiên, kết quả này cũng chỉ ra một điểm nghẽn mới: do thiếu một đạo luật thống nhất, việc chia sẻ thông tin giữa các bộ, ngành vẫn gặp rào cản về tâm lý sợ mất an toàn. Nhiều đơn vị vẫn giữ tư duy "cát cứ dữ liệu", gây lãng phí nguồn lực và kìm hãm sự phát triển của kinh tế số trong khi thiệt hại từ lừa đảo trực tuyến tại Việt Nam vẫn duy trì ở mức cao, ước tính từ 15 đến 20 tỷ USD mỗi năm, chiếm gần 4% GDP quốc gia.

Từ những đánh giá thực thi nêu trên, yêu cầu đặt ra cho giai đoạn tới là phải chuyển dịch sang một hệ sinh thái an ninh dữ liệu mang tính vĩnh cửu và toàn vẹn. Luật An ninh dữ liệu cần phải xác lập được danh mục dữ liệu cốt lõi quốc gia - những tài sản vĩnh cửu cần được bảo vệ bằng các biện pháp đặc biệt như mã hóa hậu lượng tử và lưu trữ biệt lập hoàn toàn (Air-gapped) như cách chúng ta đang thực hiện với dữ liệu Kỳ thi Tốt nghiệp THPT quốc gia. Quy trình quản trị không được phép đứt gãy ở bất kỳ khâu nào, từ việc gắn nhãn bảo mật tự động bằng trí tuệ nhân tạo đến việc quy định trách nhiệm hình sự rõ ràng đối với chức danh cán bộ quản trị dữ liệu. Chế tài xử phạt cần phải được nâng cấp mạnh mẽ, áp dụng cơ chế xử phạt theo tỷ lệ phần trăm doanh thu của tổ chức vi phạm để đảm bảo tính răn đe tuyệt đối.

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

Công tác bảo đảm an ninh, an toàn hệ thống thông tin và Cơ sở dữ liệu (CSDL) quốc gia trong giai đoạn 2021 - 2025 đã có những bước chuyển mình mạnh mẽ, từ nhận thức đến hành động thực tiễn. Việt Nam đã hình thành một mạng lưới đơn vị chuyên trách và chuyên gia an ninh mạng quy mô lớn với sự tham gia của hơn 200 cơ quan, tổ chức. Mạng lưới này tạo thành một hệ sinh thái 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; 17 Tập đoàn, Tổng công ty Nhà nước; 45 Ngân hàng và tổ chức tài chính; cùng 30 doanh nghiệp ISP và nhiều tổ chức xã hội khác.

Đặc biệt, sự vận hành của Liên minh xử lý mã độc và phòng, chống tấn công mạng đã thiết lập cơ chế phản ứng nhanh hiệu quả. Hệ thống kỹ thuật bảo đảm an ninh mạng quy mô quốc gia đã được nâng cấp toàn diện, tiêu biểu là các hệ thống: theo dõi xu hướng không gian mạng; điều phối xử lý phát tán thông tin vi phạm; và đặc biệt là 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) của ITU đã có sự thăng tiến vượt bậc, vươn lên nhóm các quốc gia dẫn đầu (Top 25-30 thế giới vào năm 2025). Theo báo cáo của Kaspersky và các tổ chức quốc tế, Việt Nam duy trì vị thế là quốc gia có tỷ lệ lây nhiễm mã độc di động thấp thuộc nhóm dẫn đầu Đông Nam Á, chỉ xếp sau Singapore.

Sự lớn mạnh về quy mô hạ tầng Trung tâm dữ liệu quốc gia lại đang đối mặt với một thực tế đầy thách thức: quy mô càng lớn, tính tập trung càng cao thì áp lực bảo vệ càng nặng nề. Hiện nay, chiến lược an ninh dữ liệu quốc gia vẫn chưa thực sự đảm bảo tính đồng bộ xuyên suốt toàn bộ vòng đời của dữ liệu. Chúng ta đang chứng kiến một nghịch lý “vỏ cứng - nhân mềm”, khi các lớp hạ tầng bên ngoài được trang bị tường lửa và thiết bị hiện đại, nhưng quy trình quản trị nội bộ và bảo mật nội dung bên trong vẫn còn nhiều sơ hở.

Đi sâu vào thực tiễn triển khai tại các bộ, ngành và địa phương, mặc dù đã có những thành tựu chung, nhưng vẫn tồn tại những “khoảng tối” đáng lo ngại về an ninh dữ liệu. Hiện nay, một nhóm các đơn vị chủ chốt vẫn tiềm ẩn nhiều rủi ro hệ thống do việc thuê dịch vụ hạ tầng công nghệ thông tin thiếu kiểm soát hoặc chưa hoàn thiện hệ thống bảo vệ đồng bộ. Tại nhiều đơn vị bộ, ngành việc thiếu hụt các tiêu chuẩn bảo mật nghiêm ngặt và sự dàn trải trong đầu tư đã dẫn đến những lỗ hổng bảo mật tích tụ qua nhiều năm. Điều này tạo điều kiện thuận lợi cho các chiến dịch tấn công mã hóa dữ liệu (Ransomware) nhắm trực tiếp vào các hệ thống quản lý nhà nước cốt yếu. Minh chứng rõ nét nhất là các vụ tấn công vào các tập đoàn tài chính và năng lượng lớn đầu năm 2024, gây ngưng trệ hoạt động trong nhiều ngày và bộc lộ năng lực ứng phó còn hạn chế của đội ngũ kỹ thuật tại chỗ. Chỉ có khoảng 25% tổ chức tại Việt Nam có quy trình sao lưu và phục hồi dữ liệu đáp ứng tiêu chuẩn phục hồi dưới 24 giờ sau khi bị tấn công, một con số cho thấy sự thiếu chuẩn bị chiến lược cho các tình huống khẩn cấp.

Hệ lụy của những lỗ hổng này không chỉ dừng lại ở nguy cơ mất dữ liệu mà còn gây ra sự đứt gãy trong liên thông dữ liệu quốc gia. Nhiều hệ thống của các Bộ, ngành không đủ điều kiện an ninh để kết nối, khai thác dữ liệu từ Cơ sở dữ liệu quốc gia về dân cư, làm chậm tiến trình cắt giảm thủ tục hành chính và gây lãng phí nguồn lực xã hội vô cùng lớn. Sự thiếu đồng bộ về thông tin giữa các Bộ chủ quản làm ảnh hưởng trực tiếp đến công tác điều hành chung của Chính phủ, khiến việc chuyển đổi từ hồ sơ giấy sang dữ liệu số bị đình trệ, gây khó khăn cho người dân và doanh nghiệp trong việc tiếp cận dịch vụ công trực tuyến.

Phân tích sâu về nguyên nhân của những tồn tại này, có thể thấy yếu tố con người và quy trình nội bộ chính là gốc rễ của vấn đề. Có tới 60% đến 70% vụ lộ lọt dữ liệu bắt nguồn từ chính sai phạm nội bộ hoặc sự thiếu trách nhiệm, thiếu hiểu biết của cán bộ quản trị. Việt Nam đang đối mặt với sự khủng hoảng nhân lực chất lượng cao về Quản trị dữ liệu (Data Governance), khi lực lượng chuyên trách tại nhiều địa phương chủ yếu vẫn là kiêm nhiệm, thiếu hụt các công cụ phân tích hiện đại và kỹ năng xử lý sự cố thực tế. Bên cạnh đó, các đơn vị chưa chủ động phối hợp với cơ quan chuyên trách (như Bộ Công an, Bộ Thông tin và Truyền thông) để đánh giá lại an ninh hệ thống mỗi khi thay đổi cấu trúc kỹ thuật hoặc cập nhật tính năng mới. Chế tài xử phạt hành chính hiện nay cũng bị coi là quá thấp, chưa đủ sức răn đe so với lợi nhuận khổng lồ từ việc buôn bán tài nguyên số trái phép trên thị trường đen, khiến nhiều doanh nghiệp thà chấp nhận nộp phạt còn hơn là đầu tư bài bản cho bảo mật chuyên sâu.

Trong tương lai gần, tình hình an ninh dữ liệu sẽ còn diễn biến phức tạp hơn nữa dưới sự hỗ trợ của trí tuệ nhân tạo (AI). Tội phạm mạng đã bắt đầu sử dụng AI để tự động hóa các cuộc tấn công, tạo ra các mã độc biến thể liên tục và thực hiện các chiến dịch lừa đảo bằng công nghệ Deepfake với độ tinh vi cực cao. Điều này tạo ra một sự bất đối xứng công nghệ nghiêm trọng khi bên tấn công luôn đi trước một bước với những công cụ tối tân, trong khi bên phòng thủ vẫn loay hoay với các quy trình hành chính rườm rà và các công cụ bảo mật truyền thống. Sự xuất hiện của máy tính lượng tử cũng đang đe dọa trực tiếp đến các thuật toán mã hóa hiện tại, đặt ra yêu cầu cấp bách về việc nghiên cứu và triển khai các giải pháp mã hóa hậu lượng tử để bảo vệ dữ liệu nhạy cảm của quốc gia.

1.4. Những nguyên nhân cốt lõi của sự mất an toàn dữ liệu

Qua công tác thanh tra và giám sát vận hành tính đến năm 2025, ba vấn đề tồn tại lớn nhất được xác định là:

- Thiếu phối hợp trong thẩm định thay đổi: Các đơn vị chưa chủ động phối hợp với Bộ Công an và cơ quan chuyên trách để đánh giá lại an ninh hệ thống mỗi khi thay đổi cấu trúc kỹ thuật hoặc cập nhật tính năng, dẫn đến các điểm yếu bảo mật mới phát sinh.

- Tư duy bảo vệ phiến diện: Nhiều đơn vị mới chỉ tập trung bảo vệ hệ thống Dịch vụ công (phần nổi) mà "bỏ quên" các hệ thống lõi và các cổng kết nối trung gian - vốn là nơi chứa đựng các tài sản dữ liệu quan trọng nhất.

- Hồng quy trình nội bộ: Chưa thực hiện đầy đủ việc ban hành quy chế, quy trình vận hành và bảo đảm an toàn theo tiêu chuẩn (ISO/IEC 27001 hoặc tương đương). Đây chính là nguyên nhân trực tiếp dẫn đến nhiều vụ việc mất dữ liệu và lộ lọt thông tin cá nhân quy mô lớn trong thời gian qua.

III. ĐỀ XUẤT, KIẾN NGHỊ

Trong bối cảnh kỷ nguyên số đang tái định nghĩa các khái niệm về chủ quyền và tài sản quốc gia, dữ liệu không còn chỉ là những dòng mã nhị phân lưu trữ trên máy chủ, mà đã trở thành "huyết mạch" của nền kinh tế, "tư liệu sản xuất" của doanh nghiệp và là "tài sản công đặc biệt" thuộc chủ quyền quốc gia. Từ thực trạng phân mảnh trong quản trị, những lỗ hổng chí mạng tại một số bộ ngành và sự đứt gãy trong quy trình phối hợp kiểm tra, đánh giá an ninh thời gian qua, việc kiến nghị một hệ thống giải pháp mang tính chiến lược và đồng bộ là yêu cầu cấp thiết. Hệ sinh thái này phải được xây dựng vững chắc dựa trên "kiềng ba chân": Thể chế quy trình chặt chẽ, Biện pháp công nghệ tiên phong và Lực lượng con người tinh nhuệ.

1. Về quy trình và thể chế: thiết lập "Luật khung" thống nhất vòng đời dữ liệu

Kiến nghị đầu tiên và mang tính nền tảng nhất là việc đẩy nhanh tiến độ ban hành và thực thi Luật An ninh dữ liệu để làm "bệ đỡ" cho toàn bộ hệ thống pháp luật liên quan như Luật An ninh mạng, Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân. Thể chế phải đi trước một bước để xóa bỏ tình trạng "mạnh ai nấy làm" hoặc thuê dịch vụ hạ tầng tiềm ẩn rủi ro như tại một số bộ, ngành như hiện nay.

Luật mới cần thiết lập một quy trình quản trị vòng đời dữ liệu khép kín, bắt buộc các đơn vị phải phối hợp chặt chẽ với Bộ Công an và các đơn vị liên quan để kiểm tra, đánh giá lại hệ thống mỗi khi có sự thay đổi về cấu trúc hoặc tính năng. Đặc biệt, Nhà nước cần xác lập và luật hóa Danh mục dữ liệu cốt lõi quốc gia. Đây là những "túi dữ liệu" nhạy cảm về địa chính trị, tài chính vĩ mô và định danh công dân cần được áp dụng chế độ bảo vệ vĩnh viễn, không thể xâm phạm. Việc chuẩn hóa quy trình không chỉ bảo vệ hệ thống dịch vụ công mà phải bắt buộc đánh giá định kỳ các hệ thống lõi và các hệ thống kết nối trung gian, nhằm triệt tiêu nguy cơ "hệ quả dây chuyền" làm ảnh hưởng đến hiệu quả quản lý nhà nước khi một mắt xích bị tổn thương.

2. Về biện pháp và công nghệ: từ bảo vệ "vỏ" sang bảo mật "lõi" vĩnh cửu

Nếu Thẻ chế là bộ khung thì Công nghệ chính là lớp giáp bảo vệ. Từ thực tế nhiều đơn vị chưa hoàn thiện hệ thống hoặc còn tồn tại lỗ hổng bảo mật, kiến nghị chiến lược là việc kiên quyết Tụt chủ hạ tầng số quốc gia thông qua các Trung tâm dữ liệu quốc gia (DC1). Chúng ta cần giảm thiểu việc thuê dịch vụ hạ tầng rời rạc, thiếu kiểm soát, thay vào đó là tập trung dữ liệu về các "pháo đài số" được đầu tư bài bản.

Để bảo đảm an ninh vĩnh cửu, cần thay đổi tư duy bảo mật: chuyển từ việc chỉ bảo vệ "vỏ" hệ thống (như tường lửa, phần mềm diệt virus) sang việc bảo vệ "lõi" dữ liệu. Các giải pháp mã hóa hậu lượng tử (Post-Quantum Cryptography) và công nghệ Blockchain trong lưu vết truy cập cần được triển khai để đảm bảo dữ liệu không bị thay đổi hoặc giải mã trái phép trong tương lai. Bên cạnh đó, việc ứng dụng AI trong giám sát an ninh mạng sẽ giúp các hệ thống quốc gia tự động nhận diện các xu hướng tấn công mới, phát hiện sớm các lỗ hổng điểm yếu trước khi chúng bị khai thác. Các hệ thống này phải được kết nối liên thông với mạng lưới chuyên trách gồm 200 cơ quan, tổ chức đã hình thành, tạo thành một hệ thống phòng thủ đa tầng, xuyên suốt từ Trung ương đến địa phương.

3. Về Con người và lực lượng: Hình thành chức danh cán bộ quản trị dữ liệu chuyên trách

Mọi quy trình chặt chẽ và công nghệ tiên tiến sẽ trở nên vô nghĩa nếu mất xích con người bị phá vỡ hoặc thiếu chuyên môn. Kiến nghị trọng tâm là việc chính thức hình thành và chuẩn hóa chức danh Cán bộ quản trị dữ liệu (Data Officer) chuyên trách tại các cơ quan nhà nước và doanh nghiệp trọng yếu. Đây không phải là vị trí kiêm nhiệm kỹ thuật thông thường mà là chức danh nghiệp vụ cao cấp, có chứng chỉ hành nghề và chịu trách nhiệm pháp lý cao nhất về tính an toàn của dữ liệu tại đơn vị.

Lực lượng này sẽ là nòng cốt để khắc phục tình trạng "quên" ban hành quy trình, quy chế hoặc "ngại" phối hợp kiểm tra an ninh như thực trạng đã nêu. Đồng thời, cần đẩy mạnh chiến lược phổ cập văn hóa an ninh dữ liệu cho toàn dân thông qua ứng dụng VNeID. Khi mỗi công dân, mỗi cán bộ đều có ý thức bảo mật và biết cách nhận diện các nguy cơ, chúng ta sẽ có hàng triệu "lá chắn số" sống động. Sự tham gia của gần 200 đơn vị chuyên trách và các tập đoàn công nghệ lớn như Viettel, VNPT, FPT cần được nâng tầm thành một "Liên minh bảo vệ chủ quyền số", nơi tri thức và kinh nghiệm được chia sẻ thời gian thực để ứng phó với mọi cuộc tấn công quy mô quốc gia.

An ninh dữ liệu không phải là một đích đến kỹ thuật đơn thuần, mà là một hành trình quản trị liên tục. Những thành tựu về thứ hạng quốc tế (thứ 50 toàn cầu theo ITU) hay sự sụt giảm lây nhiễm mã độc là những tín hiệu tích cực, nhưng những lỗ hổng tại các bộ ngành chủ chốt và các vụ mất dữ liệu thời gian qua là lời cảnh báo đanh thép. Việc thực hiện đồng bộ ba nhóm giải pháp: Thống nhất thể chế - Tự chủ công nghệ - Chuyên nghiệp hóa con người chính là lời giải duy nhất để Việt Nam bảo vệ vĩnh cửu tài nguyên số quốc gia, kiến tạo niềm tin cho người dân và thúc đẩy sự phát triển bền vững trong kỷ nguyên trí tuệ nhân tạo.

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

Nơi nhận:

- Như trên;
- Văn phòng Chính phủ;
- Lưu: VT, BCA(A05).

BỘ TRƯỞNG

Đại tướng Lương Tam Quang