

Số: /TTr-BCA

Hà Nội, ngày tháng năm 2026

TỜ TRÌNH
Chính sách của dự án 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 kính trình Chính phủ Hồ sơ chính sách của dự án Luật An ninh dữ liệu như sau:

I. SỰ CẦN THIẾT XÂY DỰNG CHÍNH SÁCH

1. Cơ sở chính trị, pháp lý

Việc xây dựng Luật An ninh dữ liệu là bước cụ thể hóa các chủ trương lớn của Đảng về chuyển đổi số và bảo vệ Tổ quốc trên không gian mạng:

- Nghị quyết Đại hội đại biểu toàn quốc lần thứ XIV của Đảng nhấn mạnh mục tiêu xây dựng Đảng trong sạch, vững mạnh, phát triển kinh tế nhanh, bền vững dựa trên khoa học công nghệ, chuyển đổi số. Bảo vệ an ninh dữ liệu được xác định là một trong định hướng phát triển đất nước giai đoạn 2026-2030. Trong thời gian qua, Đảng và Nhà nước đã có nhiều chủ trương, giải pháp đẩy mạnh ứng dụng khoa học, công nghệ phục vụ công cuộc chuyển đổi số quốc gia, xây dựng Chính phủ điện tử, Chính phủ số, kinh tế số, xã hội số.

- 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 trong đó xác định dữ liệu là tài nguyên quan trọng và bảo đảm an ninh mạng là điều kiện tiên quyết.

- 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 xác định ưu tiên nguồn lực và có cơ chế, chính sách khuyến khích đủ mạnh để phát triển những lĩnh vực ưu tiên; trong đó có phát triển công nghệ số (ưu tiên phát triển trí tuệ nhân tạo, dữ liệu lớn, chuỗi khối, điện toán đám mây, Internet kết nối vạn vật, thiết bị điện tử - viễn thông, thiết kế và sản xuất chip bán dẫn).

- Nghị quyết số 44-NQ/TW ngày 24/11/2023 về Chiến lược bảo vệ Tổ quốc

trong tình hình mới khẳng định bảo vệ Tổ quốc không chỉ là bảo vệ lãnh thổ vật lý mà còn là bảo vệ “không gian mạng và lợi ích quốc gia trên không gian mạng”. Nghị quyết cũng nâng cao năng lực tự chủ quốc phòng, an ninh đặc biệt là các công nghệ lõi, công nghệ chiến lược. Với phương châm “bảo vệ Tổ quốc từ sớm, từ xa” Nghị quyết yêu cầu chủ động nhận diện, ngăn chặn các nguy cơ thách thức an ninh phi truyền thống ngay từ khi mới manh nha.

- Nghị quyết số 22-NQ/TW ngày 15/6/2023 của Bộ Chính trị về bảo vệ Tổ quốc trên không gian mạng khẳng định yêu cầu tự chủ về công nghệ, mật mã và hạ tầng dữ liệu để không bị lệ thuộc vào bên ngoài.

- 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 đã nhấn mạnh quan điểm *“bảo đảm chủ quyền quốc gia trên không gian mạng; bảo đảm an ninh mạng, an ninh dữ liệu, an toàn thông tin của tổ chức và cá nhân là yêu cầu xuyên suốt, không thể tách rời trong quá trình phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia”*.

- Nghị quyết số 59-NQ/TW ngày 24/1/2025 của Bộ Chính trị về Hội nhập quốc tế trong tình hình mới đã nhấn mạnh việc triển khai nhiệm vụ *“Nâng cao hiệu quả hội nhập kinh tế quốc tế phục vụ xây dựng nền kinh tế độc lập, tự chủ, tự lực, tự cường, đẩy mạnh cơ cấu lại nền kinh tế, đổi mới mô hình tăng trưởng và thúc đẩy chuyển đổi số”*.

- 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 đã xác định chính sách khoa học và công nghệ cho phát triển công nghiệp: *“Khuyến khích đầu tư, phát triển xây dựng các trung tâm dữ liệu lớn; đẩy mạnh phát triển khoa học phân tích, quản lý và xử lý dữ liệu lớn nhằm tạo ra các sản phẩm, tri thức mới”*.

- Nghị quyết số 66-NQ/TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới đã nhấn mạnh việc tập trung xây dựng pháp luật về khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số, tạo hành lang pháp lý cho những vấn đề mới, phi truyền thống (trí tuệ nhân tạo, chuyển đổi số, chuyển đổi xanh, khai thác nguồn lực dữ liệu, tài sản mã hóa...) để hình thành các động lực tăng trưởng mới, thúc đẩy phát triển lực lượng sản xuất mới, các ngành công nghiệp mới. Xây dựng cơ chế, chính sách đột phá, vượt trội, cạnh tranh cho trung tâm tài chính quốc tế,

khu thương mại tự do, khu kinh tế trọng điểm...

- Nghị quyết số 68-NQ/TW ngày 04/5/2025 của Bộ Chính trị về phát triển kinh tế tư nhân tiếp tục đề cập đến vấn đề hoàn thiện khung pháp lý cho các mô hình kinh tế mới, kinh doanh dựa trên công nghệ và nền tảng số, đặc biệt là công nghệ tài chính, trí tuệ nhân tạo, tài sản ảo, tiền ảo, tài sản mã hoá, tiền mã hoá, thương mại điện tử... Có cơ chế thử nghiệm đối với những ngành, lĩnh vực mới trên cơ sở hậu kiểm, phù hợp với thông lệ quốc tế. Hoàn thiện pháp luật, chính sách về dữ liệu, quản trị dữ liệu, tạo thuận lợi cho doanh nghiệp kết nối, chia sẻ, khai thác dữ liệu, bảo đảm an ninh, an toàn.

- Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ về phát triển Chính phủ số và bảo đảm an ninh mạng quốc gia đã yêu cầu các Bộ, ngành phải làm chủ công nghệ và bảo vệ dữ liệu dùng chung.

- Quyết định số 749/QĐ-TTg của Thủ tướng Chính phủ phê duyệt “Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030” xác định an ninh mạng là then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần không thể tách rời của chuyển đổi số.

- Chỉ thị số 57-CT/TW của Ban Bí thư ngày 31/12/2025 về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị xác định trước yêu cầu, nhiệm vụ đặt ra trong giai đoạn mới, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là yêu cầu cấp thiết nhằm kiến tạo một không gian mạng an toàn, tin cậy, thúc đẩy mạnh mẽ sự phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số quốc gia.

- Ban Chỉ đạo An ninh mạng quốc gia đã tổ chức Phiên họp lần thứ I năm 2026 đã xác định: “Trong năm 2025, công tác bảo đảm an ninh mạng quốc gia đã đạt được nhiều kết quả quan trọng, chuyển biến tích cực. Hệ thống thể chế, chính sách tiếp tục được hoàn thiện, nổi bật với việc tham mưu ban hành Luật An ninh mạng và Luật Bảo vệ dữ liệu cá nhân. Công tác kiểm tra, giám sát an ninh mạng được triển khai đồng bộ từ Trung ương đến địa phương; các cuộc diễn tập phòng, chống tấn công mạng được tổ chức định kỳ, góp phần nâng cao năng lực ứng cứu sự cố”.

- Điều 62 Hiến pháp năm 2013 cũng quy định: (1) Phát triển khoa học và công nghệ là quốc sách hàng đầu, giữ vai trò then chốt trong sự nghiệp phát triển kinh tế - xã hội của đất nước; (2) Nhà nước ưu tiên đầu tư và khuyến khích tổ chức, cá nhân đầu tư nghiên cứu, phát triển, chuyển giao, ứng dụng có hiệu quả

thành tựu khoa học và công nghệ; bảo đảm quyền nghiên cứu khoa học và công nghệ; bảo hộ quyền sở hữu trí tuệ; (3) Nhà nước tạo điều kiện để mọi người tham gia và được thụ hưởng lợi ích từ các hoạt động khoa học và công nghệ.

- 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 đã xác định “đưa Việt Nam trở thành một trong những trung tâm dữ liệu khu vực. Xây dựng các trung tâm dữ liệu gắn với các vùng động lực, cực tăng trưởng, hành lang kinh tế; phát triển các cụm trung tâm dữ liệu quốc gia tại khu vực phía Bắc và khu vực phía Nam.”

- 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 đã xác định xây dựng, phát triển hệ thống dữ liệu phục vụ triển khai Chính phủ điện tử hướng tới Chính phủ số tại Bộ, ngành, địa phương.

- 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 đã giao Bộ Công an thực hiện nhiệm vụ “Xây dựng, vận hành Trung tâm dữ liệu quốc gia. Nâng cao nhận thức của các tổ chức, doanh nghiệp và người dân về bảo vệ dữ liệu cá nhân, quản trị dữ liệu”.

Bên cạnh đó, Chính phủ cũng đã ban hành nhiều quyết định có tính định hướng quan trọng về phát triển dữ liệu, hoàn thiện cơ sở hạ tầng thông tin trong chuyển đổi số ở nước ta như: Chiến lược dữ liệu quốc gia quy định tại Quyết định số 142/QĐ-TTg ngày 02/02/2024 của Thủ tướng Chính phủ, Quy hoạch hạ tầng thông tin và truyền thông thời kỳ 2021 - 2030, tầm nhìn đến năm 2050 quy định tại Quyết định số 36/QĐ-TTg ngày 11/01/2024 của Thủ tướng Chính phủ.

Hệ thống các văn bản Nghị quyết, Chỉ thị, Quyết định của Đảng và Chính phủ đã xác lập một tư duy xuyên suốt: dữ liệu là tài nguyên, đảm bảo an ninh dữ liệu là vấn đề sống còn. *Do vậy, khi quy mô dữ liệu tăng lên, hệ thống dữ liệu càng lớn và mạnh thì việc bảo đảm an ninh dữ liệu không chỉ đơn thuần là cài phần mềm diệt virus hay bảo mật dữ liệu mà là đòi hỏi cấp bách và cần thiết về quy trình, công nghệ, nhân lực, biện pháp bảo đảm an ninh dữ liệu.* Hệ thống các chính sách của dự án Luật An ninh dữ liệu sẽ tạo ra 03 trụ cột chính: thống nhất quản lý nhà nước về an ninh dữ liệu như đối với hệ thống các tài nguyên, khoáng sản khác; phân loại dữ liệu để quản lý, bảo vệ chủ quyền số và áp dụng các chiến lược phát triển kinh tế số trên hệ thống cơ sở dữ liệu quốc gia; nâng cao năng lực

tự chủ tự cường đối với công nghiệp số: công nghệ lõi, công nghệ bảo mật dữ liệu. *Bảo đảm an ninh dữ liệu còn có một thiên chức vô cùng quan trọng, đó là “xây dựng và duy trì niềm tin số”* đây là một trong những yếu tố quyết định để chuyển đổi số quốc gia thành công, xây dựng kinh tế số, chính phủ số. Xây dựng Luật An ninh dữ liệu không chỉ là hoàn thiện hệ thống pháp luật mà còn là hành động cụ thể để bảo vệ nền tảng độc lập, tự chủ của quốc gia trong kỷ nguyên trí tuệ nhân tạo, đảm bảo Việt Nam không chỉ là quốc gia tiêu dùng công nghệ mà còn là quốc gia làm chủ an ninh số. Do vậy, việc hoàn thiện pháp luật, quy định những chính sách trong phát triển, ứng dụng dữ liệu, quản trị dữ liệu, bảo đảm an ninh dữ liệu vào công tác quản lý nhà nước và phát triển kinh tế - xã hội là yêu cầu rất cần thiết và cấp bách trong tình hình hiện nay.

2. Cơ sở thực tiễn

Thực tiễn Việt Nam cho thấy, công tác bảo đảm an ninh dữ liệu thời gian qua đang phải đối mặt với nhiều nguy cơ, thách thức mới, ngày càng đan xen, phức tạp, chi phối trực tiếp đến an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân, tác động tới chủ quyền quốc gia trên không gian mạng.

Thứ nhất, sự bùng nổ của tài nguyên dữ liệu và rủi ro an ninh phi truyền thống.

Sự phát triển mạnh mẽ của các công nghệ mới như trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data), điện toán đám mây (Cloud Computing) làm gia tăng khối lượng, tốc độ và phạm vi lưu chuyển dữ liệu. Thực tiễn quá trình chuyển đổi số ở Việt Nam cho thấy dữ liệu đã trở thành “dầu mỏ” của nền kinh tế song cũng là mục tiêu tấn công hàng đầu. Với gần 80 triệu người dùng Internet, khối lượng dữ liệu cá nhân và dữ liệu chuyên ngành phát sinh hàng ngày là cực lớn. Tuy nhiên, việc quản lý hiện nay còn phân tán, thiếu các tiêu chuẩn bảo vệ thống nhất. Tội phạm mạng và Ransomware: năm 2025 ghi nhận sự gia tăng đột biến các chiến dịch tấn công mã hóa dữ liệu nhắm vào các tập đoàn tài chính, năng lượng và hệ thống quản lý nhà nước. Theo IDC (trung tâm dữ liệu), lượng dữ liệu toàn cầu năm 2025 đạt mốc 175 Zettabytes, năm 2025, các hệ thống thông tin dữ liệu của Việt Nam đối mặt với khoảng 552.000 cuộc tấn công mạng; 5230 cơ quan, doanh nghiệp từng ghi nhận chịu sự tổn hại do tấn công mạng trong năm, 34.13% người dùng từng gặp sự cố mã độc, với 62.952 loại mã độc mới trên điện thoại di động; 47.72% cơ quan doanh nghiệp thiếu hụt nhân sự an ninh mạng, 9.38% cơ quan doanh nghiệp cho biết không có biện pháp kiểm soát truy cập Internet như tường lửa tại cửa ngõ hệ thống, 931 phần mềm giả mạo được phát hiện bởi Hệ thống

phòng chống lừa đảo nTrust của NCA¹ Thực tế cho thấy nhiều đơn vị lúng túng trong việc ứng phó do thiếu quy trình cưỡng chế kỹ thuật và giải mã dữ liệu kịp thời. Hoạt động tấn công mạng, gián điệp mạng và lộ, mất bí mật nhà nước tại Việt Nam diễn ra ngày càng phức tạp, ảnh hưởng nghiêm trọng đến an ninh quốc gia. Tin tặc sử dụng nhiều thủ đoạn tinh vi, không ngừng nâng cấp, cải tiến các dòng mã độc để tiến hành các chiến dịch tấn công mạng nhằm vào các cơ quan, tổ chức, doanh nghiệp của Việt Nam. Mục tiêu chủ yếu nhằm vào hệ thống mạng thông tin của các cơ quan Trung ương và các tập đoàn, doanh nghiệp quan trọng. Mục tiêu tấn công không chỉ nhằm thu thập thông tin tình báo, bí mật nhà nước, đặc biệt là các chủ trương, chính sách đối ngoại, an ninh, quốc phòng của Việt Nam mà còn chuẩn bị sẵn để tiến hành các hành động tình báo, phát động các cuộc tấn công phá hoại khi cần thiết. Trung bình mỗi năm, Bộ Công an phát hiện trên 2.600 trang/cổng thông tin điện tử của Việt Nam (có tên miền “.vn”) bị tin tặc tấn công, thay đổi giao diện hoặc chèn tập tin; hàng chục vụ lộ tài liệu bí mật nhà nước với hàng trăm đầu tài liệu; hàng trăm TB dữ liệu của các bộ, ban, ngành, địa phương bị tin tặc chiếm đoạt, trong đó có nhiều tài liệu bí mật nhà nước. Một số cơ quan, đơn vị mặc dù đã được kiểm tra, cảnh báo về các nguy cơ gây mất an ninh mạng, lộ mất bí mật nhà nước, nhưng vẫn để xảy ra tình trạng tiếp diễn. Các vụ việc mất an toàn dữ liệu không chỉ gây thiệt hại kinh tế mà còn ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự an toàn xã hội và quyền, lợi ích hợp pháp của tổ chức, cá nhân. Hoạt động mua bán thông tin, dữ liệu cá nhân diễn ra phức tạp trên các diễn đàn, hội nhóm, phát hiện 300 vụ rao bán với tổng số hơn 1,7 triệu bản ghi dữ liệu trên các lĩnh vực, như: y tế, giáo dục, dịch vụ công, ngân hàng, điện lực, bảo hiểm, chứng khoán, căn cước công dân, vận chuyển, viễn thông... Đáng chú ý, Bộ Công an đã phát hiện tin tặc chiếm đoạt, rao bán hơn 160 triệu bản thông tin khách hàng của Trung tâm Thông tin ứng dụng quốc gia thuộc Ngân hàng Nhà nước Việt Nam². Triển khai Đề án 06 của Chính phủ, lực lượng chức năng tiến hành kiểm tra, đánh giá an ninh mạng hệ thống tin tại 07 Bộ, ngành, địa phương kết nối Cơ sở dữ liệu quốc gia về dân cư và hệ thống định danh xác thực điện tử VneID, phát hiện 1.315 lỗ hổng bảo mật mức độ nghiêm trọng, 4.095 lỗ hổng bảo mật mức độ cao tại các máy chủ hệ thống. Một trong những nguyên nhân chính dẫn đến thực trạng trên là do sự bất cập, thiếu đồng bộ trong hệ thống chính sách, pháp luật về lĩnh vực an ninh dữ liệu.

¹ Báo cáo nghiên cứu, khảo sát an ninh mạng năm 2025 của NCA

² Báo cáo tổng kết công tác năm 2025

Thứ hai, nguy cơ lệ thuộc vào công nghệ mật mã và hạ tầng nước ngoài.

Hiện nay, phần lớn các hệ thống lưu trữ dữ liệu tại Việt Nam (kể cả một số hạ tầng quan trọng) vẫn đang sử dụng các tiêu chuẩn mật mã quốc tế mà Việt Nam chưa hoàn toàn làm chủ. Điều này tạo ra rủi ro về “cửa sau” (Backdoor) và khả năng bị giải mã từ xa bởi các thế lực nước ngoài. Vấn đề chảy máu dữ liệu xuyên biên giới khi một lượng lớn dữ liệu định danh, thói quen tiêu dùng và dữ liệu nhạy cảm của công dân Việt Nam đang được lưu trữ tại các trung tâm dữ liệu ngoài lãnh thổ. Việc thiếu cơ chế “lưu trữ nội địa” và “chủ quyền khóa mật mã” khiến công tác điều tra, truy xuất dữ liệu của cơ quan chức năng gặp nhiều khó khăn, kéo dài. Đặc biệt, hiện nay chiến lược “*lấy dữ liệu trước, mở khóa sau*” (Harvest Now, Decrypt Later) vô cùng nguy hiểm với sự phát triển và ra đời của máy tính lượng tử, máy tính lượng tử không còn ở phạm vi lý thuyết mà đã dần hình thành trong thực tế. Điều này đặc biệt quan trọng và nguy hiểm đối với các dữ liệu là “*di sản dữ liệu quốc gia*” có giá trị vĩnh cửu nếu lọt vào tay tội phạm dữ liệu và các thế lực thù địch, điều này có thể đe dọa nghiêm trọng đến an ninh chính trị, sự tồn vong của đất nước Việt Nam.

Thứ ba, thách thức từ trí tuệ nhân tạo (AI) và “Hộp đen” thuật toán và máy tính lượng tử.

Vấn đề thao túng thông tin và sự thiếu minh bạch của các thuật toán, sự xuất hiện của các mô hình ngôn ngữ lớn và AI tạo hình (Deepfake) đang được sử dụng để xuyên tạc thông tin, lừa đảo tài chính và tác động đến tư tưởng xã hội. Các tập đoàn công nghệ xuyên biên giới vận hành các thuật toán điều phối thông tin theo cơ chế “hộp đen”, gây khó khăn cho công tác thanh tra, kiểm soát của Nhà nước đối với các nội dung gây phương hại đến an ninh quốc gia. Thách thức từ máy tính lượng tử đối với an ninh dữ liệu không còn là lý thuyết viễn tưởng mà đã trở thành một “án treo” thực tế đối với các hệ thống mật mã hiện đại. Hầu hết các hệ thống bảo mật hiện nay (như RSA, ECC) dựa trên việc máy tính truyền thống rất khó giải các bài toán toán học phức tạp. Máy tính lượng tử với thuật toán Shor có thể “bẻ gãy” các lớp khóa này một cách dễ dàng, đòi hỏi các giải pháp bảo mật mới.

Thứ tư, những hạn chế của hệ thống pháp luật hiện hành.

Thực tiễn pháp luật hiện hành còn phân tán, chưa đồng bộ, các quy định về dữ liệu và an ninh dữ liệu đang nằm rải rác trong nhiều văn bản như Luật Dữ liệu, Luật An ninh mạng, Luật Bảo vệ dữ liệu cá nhân, Luật Giao dịch điện tử, Luật Tiếp cận thông tin... Sự chồng chéo và khoảng trống giữa các văn bản quy

phạm pháp luật là một trong những điểm hạn chế lớn nhất hiện nay, Luật An ninh mạng tập trung vào hệ thống và hành vi vi phạm an ninh mạng song chưa có văn bản nào tập trung chuyên sâu vào bảo vệ “vật thể dữ liệu” xuyên suốt chu trình sống (từ khởi tạo đến tiêu hủy), chưa có cơ chế kiểm soát hiệu quả đối với hoạt động xử lý, lưu trữ, chia sẻ và chuyển dữ liệu xuyên biên giới, thiếu quy định về vấn đề sử dụng khai thác hiệu quả dữ liệu công, thiếu các quy định về bảo đảm an ninh đối với hoạt động xây dựng cơ sở dữ liệu, phát triển dữ liệu, sử dụng dữ liệu, kinh doanh các sản phẩm, dịch vụ về dữ liệu, phát triển thị trường dữ liệu, bảo đảm an ninh đối với các sàn giao dịch dữ liệu trong tương lai. Bên cạnh đó, thực tiễn thực thi pháp luật cho thấy thiếu chế tài đủ mạnh và cơ chế thực thi đồng bộ. Các chế tài xử phạt hiện nay chủ yếu là mức phạt tiền cố định, không đủ sức răn đe đối với các tập đoàn đa quốc gia có doanh thu khổng lồ. Việc áp dụng các tiêu chuẩn của quốc tế chưa rõ ràng dẫn đến việc lúng túng giữa việc tạo điều kiện cho doanh nghiệp và thắt chặt quản lý an ninh.

Mặt khác, xuất phát từ thực tế mối quan hệ giữa bảo đảm an ninh mạng và an ninh dữ liệu trong tình hình hiện nay. Luật An ninh mạng 2025 được ban hành và có hiệu lực thi hành từ tháng 07/2026. Thực tế những quy định của Luật An ninh mạng tập trung vào việc bảo vệ hạ tầng, đường truyền, thiết bị đầu cuối và ngăn chặn các hành vi xâm nhập trái phép từ bên ngoài, đóng vai trò là "lớp vỏ" bảo vệ. Tuy nhiên những quy định về bảo vệ chính thực thể dữ liệu (tính nguyên vẹn, tính bảo mật và tính khả dụng) xuyên suốt chu trình sống của nó, dù dữ liệu đó đang nằm yên (data at rest) hay đang lưu chuyển (data in motion) với vai trò là "nhân" bên trong thì chưa có nội luật nào quy định cụ thể và hiệu quả. Mối quan hệ giữa an ninh dữ liệu và an ninh mạng không phải là hai thực thể tách rời mà là mối quan hệ hữu cơ, biện chứng theo mô hình "vật thể và không gian". Trong kỷ nguyên số, dữ liệu là "trái tim", còn mạng lưới là "mạch máu". Nếu mạng không an toàn, dữ liệu sẽ bị đánh cắp; nếu dữ liệu không được bảo vệ, mọi nỗ lực bảo mật mạng đều vô nghĩa. Vì vậy, an ninh mạng tạo ra "không gian an toàn", còn an ninh dữ liệu bảo đảm "giá trị cốt lõi" bên trong không gian đó. Hai yếu tố này tạo thành cặp bài trùng không thể tách rời trong bất kỳ chiến lược an ninh quốc gia nào. Vì vậy, việc ban hành **Luật An ninh dữ liệu** không chỉ là một bước hoàn thiện hệ thống pháp luật, mà còn là hành động mang tính chiến lược nhằm giải quyết các "khoảng tối" (dark spots) và "khoảng trống" (legislative gaps) mà các đạo luật hiện hành chưa bao quát hết.

Thứ năm, xuất phát từ kinh nghiệm quốc tế và yêu cầu thực tiễn từ công tác quản lý nhà nước và phát triển kinh tế - xã hội ở Việt Nam hiện nay.

Trên thế giới, nhiều quốc gia như Trung Quốc, Singapore, Anh, các nước EU đã ban hành luật riêng về an ninh dữ liệu. Nghiên cứu các đạo luật này đều có xu hướng: phân loại dữ liệu theo cấp độ, kiểm soát chặt chẽ dữ liệu quan trọng, cốt lõi xuyên biên giới, tăng cường trách nhiệm của tổ chức, cá nhân trong bảo vệ dữ liệu. Việc thiếu hệ thống quy định về bảo đảm an ninh dữ liệu đang gây ra các vấn đề khó khăn trong công tác phân công, phân cấp dữ liệu, cơ chế phối hợp giữa các cơ quan trong bảo vệ dữ liệu, mặt khác còn làm giảm niềm tin của người dân và doanh nghiệp khi tham gia môi trường số. Cần thiết phải có các chính sách để giải quyết triệt để vấn đề này, tạo hành lang pháp lý xây dựng xã hội số, kinh tế số, bảo vệ chủ quyền số quốc gia.

II. MỤC ĐÍCH, QUAN ĐIỂM XÂY DỰNG CHÍNH SÁCH

1. Mục đích

Một là, xác lập chủ quyền số quốc gia: khẳng định quyền tối cao, bất khả xâm phạm của Nhà nước đối với tài nguyên dữ liệu quốc gia, thiết lập “Biên giới số” và hệ thống mật mã tiên tiến, độc lập để bảo vệ lợi ích dân tộc trong kỷ nguyên số, kỷ nguyên trí tuệ nhân tạo.

Hai là, hoàn thiện hành lang pháp lý an ninh phi truyền thống, lấp đầy các khoảng trống pháp lý về quản trị thuật toán, AI và lưu thông dữ liệu xuyên biên giới, thiết lập các tiêu chuẩn và quy định bảo đảm an ninh trong các khâu xây dựng, phát triển, sử dụng, lưu trữ dữ liệu, trong quá trình chuyển đổi số mà các luật hiện hành chưa điều chỉnh chuyên sâu.

Ba là, bảo vệ quyền và các lợi ích hợp pháp của tổ chức, cá nhân; tạo ra môi trường số tin cậy, bảo vệ dữ liệu cá nhân của công dân và bí mật kinh doanh của doanh nghiệp trước các nguy cơ tấn công mạng, tống tiền và lộ lọt thông tin.

Bốn là, thúc đẩy kinh tế số tự chủ chiến lược, tự cường công nghệ, chuyển từ tư duy quản lý hành chính sang quản trị kỹ thuật số tạo điều kiện cho dòng chảy dữ liệu an toàn, thúc đẩy Việt Nam trở thành trung tâm dữ liệu của khu vực.

2. Quan điểm xây dựng chính sách

Một là, kiên định mục tiêu an ninh quốc gia là trọng yếu, thường xuyên, đặt lợi ích quốc gia dân tộc lên trên hết. Dữ liệu Cốt lõi, Quan trọng phải được lưu trữ nội địa và bảo vệ bằng mật mã quốc gia. Không đánh đổi an ninh dữ liệu lấy lợi ích kinh tế thuần túy.

Hai là, lấy doanh nghiệp và người dân làm trung tâm. Chính sách phải minh bạch, khả thi, hạn chế mức thấp nhất tạo thêm thủ tục hành chính, tạo cơ chế thông thoáng tạo điều kiện cho người dân và doanh nghiệp phát triển kinh tế số trên nền tảng quy định cần thiết và hiệu quả của an ninh dữ liệu.

Ba là, chính sách phải đảm bảo tính thống nhất, đồng bộ, tuân thủ Hiến pháp, phù hợp với Luật An ninh mạng và các luật chuyên ngành khác. Tránh chồng chéo về thẩm quyền giữa các cơ quan quản lý nhà nước.

Bốn là, tiếp cận dựa trên rủi ro, không cào bằng việc áp dụng biện pháp quản lý. Dữ liệu càng quan trọng cấp độ bảo vệ càng cao. Dữ liệu thương mại thông thường được khuyến khích lưu chuyển tự do để tối ưu hóa giá trị và phát triển.

Năm là, tham khảo có chọn lọc pháp luật về an ninh dữ liệu của một số nước, phù hợp với điều kiện thực tiễn Việt Nam. Chủ động hội nhập và tương thích quốc tế, nội luật hóa các tiêu chuẩn quốc tế phù hợp về an ninh dữ liệu.

III. PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG CỦA CHÍNH SÁCH

1. Phạm vi điều chỉnh

- Quy định về hoạt động xử lý, phân loại dữ liệu theo cấp độ, bảo đảm an ninh dữ liệu toàn diện; quyền và nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân; hành lang pháp lý cho chuyển đổi số, phát triển nguồn nhân lực và hợp tác quốc tế nhằm bảo vệ chủ quyền dữ liệu và an ninh, trật tự đất nước.

- Bảo vệ dữ liệu cá nhân là một nội dung quan trọng thuộc bảo đảm an ninh dữ liệu. Các quy định về bảo vệ dữ liệu cá nhân không được điều chỉnh bởi các chính sách của dự án Luật An ninh dữ liệu sẽ thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

2. Đối tượng áp dụng

- Cơ quan, tổ chức, cá nhân Việt Nam.
- Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động xử lý dữ liệu tại Việt Nam hoặc dữ liệu của công dân Việt Nam.
- Cơ quan, tổ chức, cá nhân có liên quan đến các hoạt động về dữ liệu tại Việt Nam.

IV. QUÁ TRÌNH XÂY DỰNG CHÍNH SÁCH

Ngày / /2026, Ủy ban Thường vụ Quốc hội ban hành Nghị quyết số ... /2026/UBTVQH16 điều chỉnh Chương trình xây dựng luật, pháp lệnh năm 2026, trong đó giao Chính phủ trình Quốc hội cho ý kiến về dự án Luật An ninh dữ liệu

tại kỳ họp thứ 1 (tháng 4/2026) và thông qua tại kỳ họp thứ 1 (tháng 4/2026). Trên cơ sở đó, Chính phủ đã chỉ đạo Bộ Công an thực hiện trình tự, thủ tục xây dựng dự án Luật An ninh dữ liệu theo đúng quy định của Luật Ban hành văn bản quy phạm pháp luật, cụ thể như sau:

1. Thành lập Tổ soạn thảo xây dựng dự án Luật.
2. Ban hành Kế hoạch xây dựng dự án Luật.
3. Xây dựng Hồ sơ chính sách dự án Luật.
4. Lấy ý kiến nội bộ Ngành Công an, Công an các đơn vị, địa phương trong toàn quốc về Hồ sơ chính sách dự án Luật.
5. Lấy ý kiến các Bộ, ngành và đơn vị, địa phương trong toàn quốc.
6. Tổ chức hội nghị tham vấn chính sách dự án Luật An ninh dữ liệu.
7. Tiếp thu, giải trình các ý kiến tham gia, chỉnh lý, hoàn thiện Hồ sơ chính sách dự án Luật gửi Bộ Tư pháp thẩm định.
8. Tiếp thu ý kiến thẩm định của Bộ Tư pháp để chỉnh lý, hoàn thiện hồ sơ chính sách dự án Luật.
9. Trình Chính phủ Hồ sơ chính sách dự án Luật An ninh dữ liệu.

V. MỤC TIÊU, NỘI DUNG CỦA CHÍNH SÁCH

1. Chính sách 1. Xác lập và bảo vệ chủ quyền dữ liệu quốc gia. Bảo đảm an ninh dữ liệu hướng tới sự an toàn, bền vững nhằm kiến tạo hệ sinh thái an ninh dữ liệu quốc gia. Thống nhất quản lý nhà nước trong điều tiết nguồn tài nguyên dữ liệu và bảo đảm an ninh dữ liệu toàn diện; xây dựng danh mục, phân loại dữ liệu để áp dụng cơ chế quản lý, bảo vệ phù hợp. Tạo lập hành lang pháp lý an toàn nhằm hài hòa giữa khai thác giá trị tài nguyên số phát triển kinh tế - xã hội với nhiệm vụ bảo vệ an ninh quốc gia, trật tự, an toàn xã hội.

1.1. Mục tiêu của chính sách

- Về chính trị: xác lập và bảo vệ chủ quyền dữ liệu quốc gia, khẳng định vai trò của Nhà nước trong việc quản lý, bảo vệ dữ liệu và bảo đảm thực thi pháp luật Việt Nam đối với các hoạt động xử lý dữ liệu có tác động đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cụ thể hóa chủ trương bảo vệ Tổ quốc trên không gian mạng.

- Về quản lý: bảo đảm an ninh dữ liệu toàn diện tới sự an toàn, bền vững nhằm kiến tạo hệ sinh thái an ninh dữ liệu quốc gia, phân bổ nguồn lực quốc gia một cách khoa học, tập trung bảo vệ tuyệt đối nhóm dữ liệu trọng yếu nhưng không làm nghẽn dòng chảy kinh tế.

- Về kinh tế: tạo lập niềm tin số cho doanh nghiệp và người dân, thúc đẩy khai thác, chia sẻ và lưu chuyển dữ liệu an toàn, hợp pháp, qua đó phát huy giá trị của dữ liệu như một nguồn lực cho tăng trưởng và đổi mới sáng tạo.

1.2. Nội dung của chính sách

- Xác định khẳng định chủ quyền số quốc gia. Dữ liệu là tài sản quốc gia, là bộ phận không thể tách rời của chủ quyền không gian mạng. Nhà nước Việt Nam thực hiện quyền tài phán tuyệt đối đối với dữ liệu phát sinh trên lãnh thổ, dữ liệu của công dân và tổ chức Việt Nam. Xóa bỏ tình trạng “vô chủ” hoặc lệ thuộc pháp lý vào các nền tảng nước ngoài. Việc xác lập chủ quyền tạo cơ sở pháp lý để yêu cầu các tập đoàn đa quốc gia phải tuân thủ pháp luật Việt Nam khi xử lý dữ liệu của người Việt, đảm bảo quyền tự quyết về thông tin của dân tộc.

- Bảo đảm an ninh dữ liệu toàn diện đối với tất cả các loại dữ liệu, trong tất cả các khâu liên quan đến dữ liệu và trong suốt vòng đời của dữ liệu; xây dựng danh mục, phân loại dữ liệu để áp dụng cơ chế quản lý, bảo vệ phù hợp. Ưu tiên nguồn lực, giải pháp để bảo vệ dữ liệu Cốt lõi, dữ liệu Quan trọng, bảo vệ trường tồn di sản dữ liệu quốc gia. Dữ liệu Cốt lõi bao gồm dữ liệu quốc phòng, an ninh, cơ yếu, lãnh đạo cấp cao. Mục tiêu là thiết lập cơ chế bảo vệ đặc biệt, sử dụng mật mã quốc gia và lưu trữ tại hệ thống cô lập để đảm bảo tuyệt đối không bị xâm nhập. Đối với dữ liệu Quan trọng bao gồm dữ liệu về hạ tầng trọng yếu (điện, nước, tài chính) dữ liệu dân cư quy mô lớn, hạ tầng số...mục tiêu là duy trì tính sẵn sàng và toàn vẹn, đảm bảo quốc gia không bị tê liệt trước các cuộc tấn công Ransomware hoặc chiến tranh thông tin. Việc ưu tiên nguồn lực bảo vệ sẽ giúp tối ưu hóa ngân sách nhà nước và nguồn lực của lực lượng chuyên trách tập trung vào những khu vực có nguy cơ sụp đổ hệ thống.

- Thúc đẩy dòng chảy dữ liệu phục vụ kinh tế - xã hội gắn liền với bảo đảm an ninh dữ liệu.

An ninh không phải là rào cản mà là “đại an toàn” cho dòng chảy dữ liệu. Dữ liệu có lưu thông mới tạo ra giá trị kinh tế nhưng dòng chảy đó phải nằm trong hành lang an toàn để không bị “xâm phạm” hoặc “chảy máu” tài nguyên số ra nước ngoài. Về cơ chế vận hành: khuyến khích lưu chuyển tự do đối với dữ liệu thương mại, tiêu dùng để thúc đẩy AI, thương mại điện tử và đổi mới sáng tạo. Nhà nước chỉ can thiệp bằng các biện pháp cưỡng chế kỹ thuật khi dòng chảy có nguy cơ bị xâm phạm đến an ninh quốc gia như lộ lọt bí mật nhà nước hoặc thao túng thị trường. Điều này nhằm tạo ra một thị trường dữ liệu minh bạch an toàn

giúp doanh nghiệp yên tâm đầu tư và người dân tin tưởng khi tham gia các hoạt động trên không gian số.

Nội dung chính sách này cũng là sự cụ thể hóa tinh thần Nghị quyết số 44-NQ/TW chuyển trạng thái từ phòng ngự thụ động sang chủ động kiểm soát tài nguyên số để bảo vệ Tổ quốc từ sớm, từ xa.

1.3. Các giải pháp thực hiện chính sách

Giải pháp 1: Thực hiện quản trị tập trung và khép kín

- Nội dung: yêu cầu tất cả dữ liệu phát sinh tại Việt Nam phải lưu trữ nội địa; mọi dòng chảy ra nước ngoài đều phải được cơ quan chuyên trách phê duyệt kiểm tra, đánh giá cho phép về an ninh.

- Ưu điểm: nội dung này bảo đảm an ninh tối đa, ngăn chặn triệt để vấn đề chảy máu dữ liệu.

- Nhược điểm: việc thiết lập quy trình an ninh nghiêm ngặt, nhiều bước có thể vô hình gây tắc nghẽn kinh tế số, làm tăng chi phí tuân thủ cho doanh nghiệp, vi phạm các cam kết FTA quốc tế.

Giải pháp 2: Quản trị dựa trên rủi ro và phân lớp bảo vệ hướng đến xây dựng một “hệ sinh thái tự chủ, tự cường”.

- Nội dung: đối với nhóm dữ liệu Cốt lõi, áp dụng cơ chế bảo vệ đặc biệt, sử dụng mật mã nội địa và hạ tầng dùng riêng (Air - gapped), đối với nhóm dữ liệu Quan trọng, lưu trữ dữ liệu gốc tại Việt Nam, giám sát bằng hệ thống cảnh báo sớm (trừ những trường hợp đặc biệt được quy định bởi Chính phủ). Đối với nhóm dữ liệu còn lại, lưu thông linh hoạt, có thể sử dụng cơ chế quản lý bằng “hậu kiểm” và tuân theo tiêu chuẩn an toàn thông lệ quốc tế.

- Ưu điểm: cân bằng giữa an ninh và phát triển, phù hợp với các hiệp định thương mại thế hệ mới.

- Nhược điểm: đòi hỏi năng lực giám sát kỹ thuật của cơ quan chuyên trách phải rất cao.

1.4. Giải pháp tối ưu được lựa chọn và lý do lựa chọn

- Lựa chọn giải pháp 2, quản trị dựa trên rủi ro và phân lớp bảo vệ hướng đến xây dựng một “hệ sinh thái tự chủ, tự cường”.

Các bước thực thi của giải pháp tối ưu:

- + Xây dựng danh mục dữ liệu quốc gia, phân loại rõ ràng các nhóm dữ liệu để áp dụng cấp độ bảo vệ tương ứng, tránh đánh đồng dữ liệu kinh doanh với dữ liệu an ninh.

+ Thiết lập “biên giới số” thông minh: vận hành đơn vị quản trị an ninh dữ liệu quốc gia để theo dõi dòng chảy dữ liệu tự động 24/7, phát hiện bất thường và không cần đọc nội dung dữ liệu của doanh nghiệp.

+ Làm chủ hạ tầng lưu trữ: ban hành các quy chuẩn kỹ thuật bắt buộc để các nhà cung cấp dịch vụ hạ tầng trong nước đạt tiêu chuẩn bảo vệ dữ liệu.

+ Có thể nghiên cứu cơ chế “hậu kiểm kỹ thuật số”, thay thế giấy phép bằng việc giám sát trực tuyến và thanh tra dựa trên dấu hiệu vi phạm.

Việc lựa chọn giải pháp này dựa trên 03 lý do mang tính chiến lược như sau:

+ Tính khả thi và hiện đại: đây là xu hướng chung của các quốc gia tiên tiến như EU với GDPR hay Trung Quốc với Luật An ninh dữ liệu 2021. Điều này cho thấy Việt Nam không đóng cửa dữ liệu mà đang xây dựng một “luật chơi” công bằng, an toàn.

+ Tối ưu hóa nguồn lực quốc gia: Nhà nước không đủ nguồn lực để bảo vệ tất cả dữ liệu như nhau. Việc tập trung đảm bảo an ninh đối với “dữ liệu Cốt lõi”, “dữ liệu Quan trọng” giúp lực lượng chuyên trách phát huy tối đa nguồn lực vào các điểm yếu chiến lược.

+ Trấn an cộng đồng doanh nghiệp và nhà đầu tư: giải pháp này khẳng định Nhà nước chỉ can thiệp khi có nguy cơ an ninh quốc gia. Việc cho phép dữ liệu kinh tế lưu thông linh hoạt giúp giữ chân các tập đoàn đa quốc gia tiếp tục đầu tư tại Việt Nam đồng thời thúc đẩy các Start up số phát triển nhanh chóng.

Việc lựa chọn giải pháp này sẽ mang lại hiệu quả cao nhất vừa đảm bảo Việt nam giữ vững được độc lập tự chủ trên không gian mạng, giữ vững được chủ quyền số song không bị tụt hậu trong cuộc đua kinh tế toàn cầu.

2. Chính sách 2. Bảo đảm an ninh dữ liệu dựa trên cơ chế phân loại 04 cấp độ rủi ro, làm căn cứ xác định biện pháp quản lý, phân bổ nguồn lực và trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan, xác lập các tiêu chuẩn mật mã tiên tiến và biện pháp bảo vệ xuyên suốt vòng đời dữ liệu; kiểm soát rủi ro, ứng phó sự cố và phục hồi dữ liệu. Tập trung các biện pháp bảo vệ nghiêm ngặt hơn đối với các hệ thống dữ liệu tác động trực tiếp đến quốc phòng, an ninh và ổn định chính trị, hoạt động thiết yếu của cơ quan, tổ chức, quyền và lợi ích hợp pháp của tổ chức, cá nhân. Tối ưu hóa bảo đảm an ninh dữ liệu thông qua vai trò điều phối tập trung của đơn vị chuyên trách quản trị an ninh dữ liệu quốc gia.

2.1. Mục tiêu của chính sách

- Tối ưu hóa nguồn lực quốc gia, chấm dứt tình trạng đầu tư dàn trải, kém hiệu

quả. Tập trung ưu tiên bảo vệ đối với các nhóm dữ liệu có mức độ rủi ro cao.

- Nâng cao năng lực phòng ngừa, phát hiện và ứng phó sự cố dữ liệu: hình thành cơ chế bảo vệ phân tầng theo cấp độ rủi ro, qua đó tăng cường khả năng bảo vệ các dữ liệu có ảnh hưởng lớn đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, hoạt động thiết yếu và quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- Xác định các biện pháp bảo đảm an ninh xuyên suốt vòng đời dữ liệu. Các biện pháp và quy định bảo đảm an ninh dữ liệu được áp dụng toàn diện từ các khâu xây dựng, tạo lập dữ liệu, lưu chuyển dữ liệu, phát triển dữ liệu, quy định an ninh đối với các sản phẩm dữ liệu, sử dụng dữ liệu, sử dụng các sản phẩm, dịch vụ về dữ liệu, tiêu hủy dữ liệu.

- Bảo đảm tính minh bạch, thống nhất và khả thi trong tổ chức thực hiện: xây dựng hệ thống phân loại dữ liệu rõ ràng, có tiêu chí cơ bản để các cơ quan, tổ chức, doanh nghiệp áp dụng thống nhất; tạo thuận lợi cho hoạt động giám sát, thanh tra, kiểm tra và tổ chức thực hiện pháp luật.

2.2. Nội dung của chính sách

- Thiết lập khung phân loại dựa trên mức độ thiệt hại đối với lợi ích quốc gia và quyền lợi công dân nếu dữ liệu bị xâm phạm.

- + Cấp độ 1: tác động trực tiếp đến độc lập, chủ quyền, quốc phòng, an ninh và sự ổn định của chế độ.

- + Cấp độ 2: tác động trực tiếp đến sự vận hành của hạ tầng thông tin quốc gia, trật tự an toàn xã hội và nền kinh tế vĩ mô.

- + Cấp độ 3: tác động đến quyền riêng tư, danh dự của công dân và lợi ích hợp pháp của tổ chức trên quy mô lớn.

- + Cấp độ 4: Các loại dữ liệu công khai, thương mại có mức độ ảnh hưởng thấp nhưng vẫn phải được quản lý, bảo vệ theo quy định của pháp luật.

- Cơ chế phòng thủ cho hệ thống trọng điểm.

- + Biện pháp kỹ thuật đặc biệt: đối với cấp độ 1 và 2 bắt buộc áp dụng công nghệ “lá chắn dữ liệu”, cô lập vật lý đối với dữ liệu tuyệt mật và kiểm soát quyền truy cập dựa trên định danh sinh trắc học quốc gia.

- + Làm chủ công nghệ lõi: ưu tiên sử dụng các giải pháp phần cứng, phần mềm và mật mã nội địa để loại bỏ nguy cơ “cửa sau” từ các nhà cung cấp nước ngoài.

- Tối ưu hóa nguồn lực thông qua Đơn vị quản trị an ninh dữ liệu quốc gia

- + Điều phối tập trung: dữ liệu từ tất cả các Bộ, ngành, địa phương được đầu

nổi đồng bộ về một đầu mối giám sát an ninh duy nhất.

+ Phân tích rủi ro bằng AI: sử dụng trí tuệ nhân tạo để tự động phát hiện các hành vi truy cập bất thường hoặc các dấu hiệu tấn công mạng theo thời gian thực đối với dữ liệu mức độ cao.

+ Chia sẻ chi phí: thay vì mỗi đơn vị tự xây dựng hệ thống phòng thủ riêng lẻ, nhà nước đầu tư mạnh cho đơn vị quản trị an ninh dữ liệu quốc gia để cung cấp dịch vụ bảo mật dữ liệu dùng chung cho các cơ quan nhà nước, giúp tiết kiệm ngân sách đáng kể.

- Quy định bảo đảm an ninh dữ liệu xuyên suốt vòng đời của dữ liệu. Các biện pháp và quy định bảo đảm an ninh dữ liệu được áp dụng toàn diện từ các khâu xây dựng, tạo lập dữ liệu, vận đề lưu chuyển dữ liệu, phát triển dữ liệu, sử dụng dữ liệu, sử dụng các sản phẩm, dịch vụ về dữ liệu, quy định an ninh đối với các sản phẩm dữ liệu, tiêu hủy dữ liệu.

- Cơ chế trách nhiệm dựa trên cấp độ.

+ Quy định rõ trách nhiệm người đứng đầu cơ quan, tổ chức tương ứng với cấp độ dữ liệu đang quản lý. Dữ liệu cấp độ càng cao, trách nhiệm pháp lý và yêu cầu về năng lực chuyên môn của đội ngũ vận hành càng khắt khe.

2.3. Các giải pháp thực hiện chính sách

Giải pháp 1: Mô hình quản trị đồng nhất (không phân cấp)

- Nội dung: áp dụng một tiêu chuẩn bảo vệ chung cho toàn bộ dữ liệu khi đưa về Trung tâm dữ liệu quốc gia. Dữ liệu được bảo vệ bởi cùng một hệ thống tường lửa và quy trình an ninh.

- Ưu điểm: thiết kế hệ thống đơn giản, dễ vận hành ở giai đoạn đầu, quy trình quản lý hành chính đồng nhất.

- Nhược điểm: gây lãng phí cực lớn nguồn lực khi phải bảo vệ dữ liệu công cộng bằng công nghệ của dữ liệu tuyệt mật; tạo ra rào cản quá mức cho các dòng chảy dữ liệu kinh tế (cấp độ 4); dễ gây “ngheh cở chai” hệ thống.

Giải pháp 2: Mô hình quản trị theo 4 cấp độ rủi ro và quản trị an ninh xuyên suốt vòng đời của dữ liệu

- Nội dung: thiết lập 4 phân vùng an ninh logic tại đơn vị quản trị dữ liệu an ninh dữ liệu quốc gia tương ứng với 4 cấp độ rủi ro và quản trị an ninh xuyên suốt vòng đời của dữ liệu: xây dựng, tạo lập dữ liệu, lưu chuyển dữ liệu, sử dụng dữ liệu, phát triển dữ liệu, quy định an ninh đối với các sản phẩm dữ liệu, sử dụng các sản phẩm, dịch vụ về dữ liệu, tiêu hủy dữ liệu.

+ Cấp độ 1 và 2: sử dụng hạ tầng dùng riêng, mật mã nội địa, kiểm soát truy cập đa nhân tố đặc biệt.

+ Cấp độ 3 và 4: sử dụng hạ tầng dùng chung có tính linh hoạt cao, ưu tiên tốc độ kết nối và chia sẻ

+ Thiết lập quy định an ninh xuyên suốt vòng đời của dữ liệu: xây dựng, tạo lập dữ liệu, lưu chuyển dữ liệu, sử dụng dữ liệu, phát triển dữ liệu, quy định an ninh đối với các sản phẩm dữ liệu, sử dụng các sản phẩm, dịch vụ về dữ liệu, tiêu hủy dữ liệu.

- Ưu điểm: tối ưu hóa chi phí đầu tư, bảo vệ đúng trọng tâm dữ liệu trọng yếu quốc gia quốc gia, tạo luồng xanh cho phát triển kinh tế số và tạo lập hành lang pháp lý an toàn, môi trường an ninh, an toàn cho kinh tế dữ liệu phát triển.

- Nhược điểm: Đòi hỏi quy trình phải gắn nhãn dữ liệu đầu vào cực kỳ nghiêm ngặt và đội ngũ chuyên sâu, tinh nhuệ để quản lý các phân vùng khác nhau và giám sát an ninh các hoạt động xuyên suốt vòng đời của dữ liệu.

2.4. Giải pháp tối ưu được lựa chọn và lý do lựa chọn

Lựa chọn giải pháp 2, mô hình quản trị theo 4 cấp độ rủi ro, quản trị an ninh xuyên suốt vòng đời của dữ liệu.

Các bước thực thi của giải pháp tối ưu:

- Về hạ tầng: nâng cấp trung tâm dữ liệu quốc gia thành mô hình “đa phân vùng an ninh”. Trong đó, xây dựng “phân vùng đặc biệt” cô lập hoàn toàn cho dữ liệu cấp độ 1 (dữ liệu Cốt lõi). Đơn vị quản trị an ninh dữ liệu quốc gia là đơn vị độc lập về nghiệp vụ, giữ vai trò là “tổng tư lệnh” về an ninh. Đơn vị này trực tiếp đưa ra các tiêu chuẩn, quy trình, giải pháp, kiểm soát an ninh và có quyền can thiệp, ngắt kết nối logic khi phát hiện rủi ro trên hạ tầng Trung tâm dữ liệu quốc gia. Việc phân định như vậy thể hiện chuyên môn hóa cao, *tách bạch giữa “vận hành hạ tầng” và “giám sát an ninh”* đẩy nhanh tốc độ đấu nối dữ liệu nhưng vẫn đảm bảo an toàn tuyệt đối qua 4 cấp độ rủi ro. Điều này đòi hỏi mối quan hệ phối hợp cực kỳ chặt chẽ giữa đơn vị quản lý hạ tầng và đơn vị quản trị về an ninh.

- Về công nghệ: triển khai hệ thống gắn nhãn dữ liệu tự động dựa trên thuật toán nhận diện từ khóa và tính chất dữ liệu để phân loại vào 4 cấp độ ngay khi dữ liệu được đẩy về đơn vị quản trị dữ liệu quốc gia.

- Về quản lý: thành lập Hội đồng thẩm định cấp độ dữ liệu để rà soát danh mục dữ liệu của các Bộ, ngành trước khi tích hợp vào Trung tâm dữ liệu quốc gia. Thiết lập các quy định bảo đảm an ninh và thực hiện quản trị an ninh xuyên suốt

vòng đời của dữ liệu: xây dựng, tạo lập dữ liệu, lưu chuyển dữ liệu, sử dụng dữ liệu, phát triển dữ liệu, quy định an ninh đối với các sản phẩm dữ liệu, sử dụng các sản phẩm, dịch vụ về dữ liệu, tiêu hủy dữ liệu.

Lý do lựa chọn giải pháp này bởi vì:

- Tính kế thừa chiến lược: Hiện tại Việt Nam đã có Trung tâm dữ liệu quốc gia, việc phân thành 4 cấp độ là bổ sung phần mềm quản trị và tư duy điều hành, điều này giúp tiết kiệm thời gian và ngân sách so với việc xây mới các trung tâm chuyên biệt.

- Giải quyết bài toán “thắt nút cổ chai”: thực tế triển khai cho thấy, nếu áp dụng tiêu chuẩn an ninh quá cao cho tất cả dữ liệu, các dịch vụ công trực tuyến sẽ bị chậm, doanh nghiệp khó tiếp cận dữ liệu. Phân thành 4 cấp độ giúp dữ liệu cấp độ 3, 4 được lưu thông cực nhanh, thúc đẩy xã hội số, kinh tế số.

- Bảo đảm an ninh toàn diện tạo hệ sinh thái an ninh dữ liệu an toàn và bền vững dựa trên quản trị an ninh xuyên suốt vòng đời của dữ liệu: xây dựng, tạo lập dữ liệu, lưu chuyển dữ liệu, sử dụng dữ liệu, phát triển dữ liệu, quy định an ninh đối với các sản phẩm dữ liệu, sử dụng các sản phẩm, dịch vụ về dữ liệu, tiêu hủy dữ liệu.

- Tập trung sức mạnh phòng thủ: trong bối cảnh tấn công mạng ngày càng tinh vi, việc “dàn hàng ngang” bảo vệ là bất khả thi. Lựa chọn này cho phép lực lượng chuyên trách dồn toàn bộ tinh hoa công nghệ và mật mã để canh giữ dữ liệu cấp độ 1 để đảm bảo quốc gia luôn ở thế chủ động và bất khả xâm phạm.

Chính sách 3. Bảo đảm an ninh trong chuyển giao dữ liệu xuyên biên giới và lưu trữ dữ liệu tại Việt Nam. Nhà nước thực hiện điều phối việc chuyển giao dữ liệu ra nước ngoài theo hướng mở có kiểm soát, dựa trên phân loại rủi ro và mục đích xử lý dữ liệu; quy định về việc lưu trữ dữ liệu tại Việt Nam và áp dụng điều kiện bảo mật phù hợp đối với từng loại dữ liệu nhằm bảo đảm an ninh dữ liệu, bảo vệ lợi ích quốc gia, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân đồng thời giảm thiểu rào cản hành chính, chi phí tuân thủ và bảo đảm tính tương thích với thông lệ, cam kết quốc tế.

3.1. Mục tiêu của chính sách

- Thực thi chủ quyền số và bảo đảm an ninh quốc gia: Khẳng định quyền tài phán tối cao của Nhà nước đối với dữ liệu phát sinh trên lãnh thổ Việt Nam. Việc yêu cầu lưu trữ dữ liệu tại Việt Nam đối với các loại dữ liệu nhạy cảm đảm bảo rằng cơ quan quản lý luôn có khả năng tiếp cận, kiểm soát và bảo vệ tài nguyên

này trước các nguy cơ can thiệp hoặc cấm vận từ bên ngoài. Điều này nhằm duy trì sự ổn định của hệ thống chính trị và an ninh quốc phòng trong mọi tình huống.

- Thiết lập cơ chế quản trị dòng chảy dữ liệu "mở có kiểm soát": Chuyển đổi từ tư duy "cấm đoán" sang "điều phối dựa trên rủi ro". Bằng cách phân loại rủi ro và mục đích xử lý, Nhà nước tạo ra các "luồng xanh" cho dữ liệu thông thường để phát triển kinh tế, đồng thời thiết lập các "luồng đỏ" kiểm soát chặt chẽ dữ liệu cốt lõi và quan trọng. Điều này sẽ tạo sự linh hoạt cho nền kinh tế dữ liệu nhưng không đánh đổi an ninh quốc gia.

- Tối ưu hóa môi trường kinh doanh và giảm thiểu chi phí tuân thủ: Cải cách thủ tục hành chính trong việc chuyển giao dữ liệu. Thay vì các quy trình xét duyệt rườm rà, chính sách hướng tới việc áp dụng các quy chuẩn bảo mật phù hợp, cho phép doanh nghiệp tự tuân thủ và tự chứng nhận dưới sự giám sát của cơ quan chức năng, từ đó giảm gánh nặng tài chính cho tổ chức, cá nhân, thúc đẩy doanh nghiệp Việt Nam tham gia sâu vào chuỗi cung ứng số toàn cầu.

- Bảo vệ quyền và lợi ích hợp pháp của các chủ thể dữ liệu: Thiết lập các tiêu chuẩn bảo mật bắt buộc khi dữ liệu rời khỏi biên giới. Đảm bảo rằng quyền lợi của cơ quan, tổ chức và cá nhân Việt Nam không bị xâm phạm khi dữ liệu được xử lý tại các quốc gia có tiêu chuẩn bảo vệ thấp hơn, góp phần xây dựng niềm tin số cho người dân và doanh nghiệp trong các hoạt động giao thương quốc tế.

- Thúc đẩy hội nhập và tương thích quốc tế: Nội hóa các cam kết quốc tế về dòng chảy dữ liệu tự do có tin cậy (DFFT) và các hiệp định thương mại tự do thế hệ mới (CPTPP, EVFTA). Việc thiết lập các quy định phù hợp với thông lệ quốc tế giúp Việt Nam tránh được các xung đột pháp lý và rào cản thương mại kỹ thuật. Điều này khẳng định vị thế và trách nhiệm của Việt Nam trong hệ sinh thái dữ liệu toàn cầu.

3.2. Nội dung của chính sách

- Thực thi chủ quyền số và bảo đảm an ninh quốc gia: Khẳng định quyền tài phán tối cao của Nhà nước đối với dữ liệu phát sinh trên lãnh thổ Việt Nam. Việc yêu cầu lưu trữ dữ liệu tại Việt Nam đối với các loại dữ liệu nhạy cảm đảm bảo rằng cơ quan quản lý luôn có khả năng tiếp cận, kiểm soát và bảo vệ tài nguyên này trước các nguy cơ can thiệp hoặc cấm vận từ bên ngoài. Điều này nhằm duy trì sự ổn định của hệ thống chính trị và an ninh quốc phòng trong mọi tình huống.

- Thiết lập cơ chế quản trị dòng chảy dữ liệu "mở có kiểm soát": Chuyển đổi từ tư duy "cấm đoán" sang "điều phối dựa trên rủi ro". Bằng cách phân loại rủi ro

và mục đích xử lý, Nhà nước tạo ra các "luồng xanh" cho dữ liệu thông thường để phát triển kinh tế, đồng thời thiết lập các "luồng đỏ" kiểm soát chặt chẽ dữ liệu cốt lõi và quan trọng. Điều này sẽ tạo sự linh hoạt cho nền kinh tế dữ liệu nhưng không đánh đổi an ninh quốc gia.

- Tối ưu hóa môi trường kinh doanh và giảm thiểu chi phí tuân thủ: Cải cách thủ tục hành chính trong việc chuyển giao dữ liệu. Thay vì các quy trình xét duyệt rườm rà, chính sách hướng tới việc áp dụng các quy chuẩn bảo mật phù hợp, cho phép doanh nghiệp tự tuân thủ và tự chứng nhận dưới sự giám sát của cơ quan chức năng, từ đó giảm gánh nặng tài chính cho tổ chức, cá nhân, thúc đẩy doanh nghiệp Việt Nam tham gia sâu vào chuỗi cung ứng số toàn cầu.

- Bảo vệ quyền và lợi ích hợp pháp của các chủ thể dữ liệu: Thiết lập các tiêu chuẩn bảo mật bắt buộc khi dữ liệu rời khỏi biên giới. Đảm bảo rằng quyền lợi của cơ quan, tổ chức và cá nhân Việt Nam không bị xâm phạm khi dữ liệu được xử lý tại các quốc gia có tiêu chuẩn bảo vệ thấp hơn, góp phần xây dựng niềm tin số cho người dân và doanh nghiệp trong các hoạt động giao thương quốc tế.

- Thúc đẩy hội nhập và tương thích quốc tế: Nội hóa các cam kết quốc tế về dòng chảy dữ liệu tự do có tin cậy (DFFT) và các hiệp định thương mại tự do thế hệ mới (CPTPP, EVFTA). Việc thiết lập các quy định phù hợp với thông lệ quốc tế giúp Việt Nam tránh được các xung đột pháp lý và rào cản thương mại kỹ thuật. Điều này khẳng định vị thế và trách nhiệm của Việt Nam trong hệ sinh thái dữ liệu toàn cầu.

3.3. Các giải pháp thực hiện chính sách

Giải pháp 1: Quản trị tập trung và kiểm soát chặt chẽ (Centric & Strict Control)

- Lưu trữ bắt buộc: Yêu cầu tất cả các loại dữ liệu từ mức "Quan trọng" trở lên và dữ liệu cá nhân của người dùng Việt Nam quy mô lớn phải lưu trữ bản sao gốc tại Việt Nam.

- Tiền kiểm chuyển giao: Thiết lập cơ chế cấp phép theo từng vụ việc (Case-by-case) đối với mọi hoạt động chuyển dữ liệu ra nước ngoài. Cơ quan chuyên trách sẽ thẩm định chi tiết phương án bảo mật của đối tác tiếp nhận.

- Cổng kiểm soát an ninh: Bắt buộc luồng dữ liệu xuyên biên giới phải đi qua hệ thống giám sát an ninh dữ liệu tập trung để kiểm tra nội dung và ngăn chặn mã độc.

Ưu điểm: Bảo đảm cao nhất quyền tài phán quốc gia; ngăn chặn tức thời

việc chảy máu dữ liệu nhạy cảm.

Hạn chế: Tăng chi phí tuân thủ cho doanh nghiệp; có thể tạo ra rào cản kỹ thuật làm chậm tốc độ hội nhập kinh tế số và phát triển kinh tế số.

Giải pháp 2: Quản trị dựa trên rủi ro và hậu kiểm dựa trên tự chứng nhận (Risk-based & Self-regulation)

- Lưu trữ theo phân loại: Chỉ bắt buộc lưu trữ tại Việt Nam đối với dữ liệu "Cốt lõi" và dữ liệu liên quan đến an ninh quốc gia. Dữ liệu "Phổ thông" được lưu trữ linh hoạt theo nhu cầu kinh doanh.

- Cơ chế "Danh sách trắng" (Whitelisting): Nhà nước công bố danh sách các quốc gia/tổ chức có hệ thống pháp luật bảo vệ dữ liệu tương đương Việt Nam. Doanh nghiệp chuyển dữ liệu sang các đối tượng này chỉ cần thông báo, không cần xin phép.

- Tự đánh giá tác động (DPIA): Doanh nghiệp tự thực hiện đánh giá rủi ro và ký kết các điều khoản bảo mật chuẩn (Standard Contractual Clauses - SCC) với đối tác ngoại. Nhà nước không can thiệp vào từng hồ sơ mà thực hiện giám sát thông minh qua hệ thống quản trị tập trung. Cơ quan chuyên trách thực hiện hậu kiểm xác suất hoặc hậu kiểm dựa trên dấu hiệu rủi ro. Nếu hậu kiểm phát hiện việc "tự chứng nhận" sai sự thật hoặc vi phạm cam kết bảo mật, Nhà nước áp dụng các biện pháp cưỡng chế kỹ thuật và chế tài tài chính.

Ưu điểm: Giảm tối đa chi phí hành chính; thúc đẩy dòng chảy dữ liệu tự do có tin cậy, thu hút đầu tư công nghệ cao.

Hạn chế: Đòi hỏi năng lực giám sát công nghệ của cơ quan chuyên trách phải cực kỳ hiện đại để phát hiện vi phạm sau khi dữ liệu đã chuyển đi.

3.4. Giải pháp tối ưu được lựa chọn và lý do lựa chọn

Lựa chọn giải pháp 2: Quản trị dựa trên rủi ro và hậu kiểm dựa trên cơ chế tự chứng nhận (Risk-based & Self-regulation), có sự điều chỉnh linh hoạt cho các đối tượng đặc thù.

Giải pháp này không quản lý theo kiểu "cào bằng" mà thực hiện phân hóa đối tượng để tối ưu hóa nguồn lực quản lý:

- Phân luồng dữ liệu: Thiết lập các "hàng rào kỹ thuật" khác nhau. Dữ liệu Cốt lõi được bảo vệ bằng cơ chế nghiêm ngặt nhất (lưu trữ nội địa hoàn toàn, chuyển giao phải có phê duyệt cấp Chính phủ). Dữ liệu Phổ thông được vận hành theo cơ chế thị trường và các tiêu chuẩn tự chứng nhận.

- Chuyển đổi từ "tiền kiểm" sang "hậu kiểm số": Thay vì bắt doanh nghiệp chờ đợi phê duyệt hành chính (vốn dễ gây ách tắc), Nhà nước ban hành bộ tiêu chuẩn kỹ thuật và các "điều khoản mẫu". Doanh nghiệp tự cam kết tuân thủ và Nhà nước thực hiện giám sát thông qua dữ liệu (Data-driven oversight).

Cơ chế liên thông quốc tế: Áp dụng các chứng nhận an toàn dữ liệu xuyên biên giới (như CBPRs) để dữ liệu Việt Nam có thể lưu chuyển trong các khối liên minh kinh tế mà không cần đàm phán lại từ đầu.

Lý do lựa chọn giải pháp này

- Tính tương thích với các cam kết quốc tế (CPTPP, EVFTA)

Việt Nam đã ký kết các hiệp định thương mại tự do thế hệ mới, trong đó cam kết "không ngăn cản việc chuyển giao thông tin bằng phương tiện điện tử". Giải pháp 2 giúp Việt Nam tuân thủ cam kết quốc tế, tránh các tranh chấp thương mại, đồng thời vẫn giữ được quyền kiểm soát thông qua các ngoại lệ về an ninh quốc gia (nhóm dữ liệu Cốt lõi).

- Giảm tối đa chi phí tuân thủ và rào cản hành chính

Nếu chọn giải pháp tập trung (Giải pháp 1), gánh nặng thủ tục sẽ làm nản lòng các nhà đầu tư công nghệ. Giải pháp 2 giúp doanh nghiệp tiết kiệm thời gian và chi phí, tạo điều kiện cho các doanh nghiệp khởi nghiệp (Startup) và doanh nghiệp nhỏ tiếp cận thị trường toàn cầu một cách bình đẳng.

- Phù hợp với thực tiễn công nghệ và xu hướng quản trị số

Trong kỷ nguyên dữ liệu lớn (Big Data), việc duyệt từng hồ sơ chuyển giao dữ liệu bằng con người là bất khả thi. Giải pháp này cho phép ứng dụng AI và các hệ thống giám sát tự động để kiểm soát dòng chảy dữ liệu (học tập mô hình của Chính phủ Anh).

- Thiết lập "Hệ sinh thái tin cậy" bền vững

Giải pháp này thúc đẩy các doanh nghiệp tự nâng cao năng lực bảo mật để đạt được các "Danh sách trắng". Thay vì bị ép buộc, doanh nghiệp chủ động xây dựng hệ thống an toàn để được hưởng lợi từ cơ chế chuyển giao mở. Điều này tạo ra một hệ sinh thái ổn định, nơi an ninh dữ liệu là trách nhiệm chung của cả Nhà nước và doanh nghiệp.

Chính sách 4. Bảo đảm an ninh trong hoạt động trí tuệ nhân tạo và ứng dụng công nghệ mới. Nhà nước thống nhất quản lý và bảo đảm an ninh trong hoạt động trí tuệ nhân tạo (AI), công nghệ mới thông qua việc kiểm soát nguồn dữ liệu huấn luyện, thẩm định tính minh bạch của thuật toán và xác lập khung trách nhiệm

pháp lý đối với các chủ thể phát triển công nghệ. Quy định cơ chế giám sát, kiểm định định kỳ để chủ động phòng ngừa, ngăn chặn việc lạm dụng AI, công nghệ mới phát tán thông tin giả mạo, thao túng dư luận hoặc xâm phạm chủ quyền số; đồng thời áp dụng các tiêu chuẩn đạo đức số nhằm bảo đảm công nghệ vận hành an toàn, tin cậy và phục vụ lợi ích quốc gia.

4.1. Mục tiêu của chính sách

- Thúc đẩy ứng dụng AI và công nghệ mới phát triển: Khuyến khích phát triển các mô hình ngôn ngữ lớn và hệ thống AI thuần Việt, giảm sự lệ thuộc vào các thuật toán nước ngoài.

- Thiết lập cơ chế kiểm soát “Hộp đen thuật toán”: đảm bảo các hệ thống AI hoặc các công nghệ mới vận hành minh bạch, không bị cài cắm các thuật toán điều phối thông tin sai lệch, tạo dựng tin giả (Deepfake) hoặc thao túng dư luận gây bất ổn chính trị.

- Xác lập trách nhiệm pháp lý rõ ràng: định danh rõ trách nhiệm của thực thể phát triển và vận hành AI đối với các hệ quả do thuật toán gây ra, bảo vệ nền tảng tư tưởng và an ninh xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

4.2. Nội dung của chính sách:

- Quy định về phân loại và quản lý hệ thống AI theo mức độ rủi ro
- + Xác lập 04 cấp độ rủi ro của AI: rủi ro không thể chấp nhận, rủi ro cao, rủi ro trung bình, rủi ro thấp.

- + Cơ chế quản lý tương ứng: nghiêm cấm các hệ thống AI thuộc nhóm “rủi ro không thể chấp nhận. Các hệ thống rủi ro cao phải tuân thủ các điều kiện nhất định về minh bạch và giám sát.

- Quy định về tính minh bạch và trung lập của thuật toán.

- + Công bố tiêu chuẩn thuật toán: quy định các tổ chức phát triển AI phải công bố nguyên tắc vận hành cốt lõi của thuật toán, bảo đảm không cài đặt các “thiên kiến độc hại”, xuyên tạc lịch sử, bôi nhọ lãnh đạo hoặc gây chia rẽ khối đại đoàn kết dân tộc.

- + Quyền tiếp cận mã nguồn: trong các trường hợp đặc biệt liên quan đến an ninh quốc gia, cơ quan nhà nước chuyên trách có quyền yêu cầu giải trình và kiểm tra logic vận hành của thuật toán để ngăn chặn việc điều phối thông tin sai lệch.

- Quy định về nhận diện nội dung do AI tạo ra.

- + Dán nhãn bắt buộc: mọi sản phẩm nội dung số (văn bản, hình ảnh, âm

thanh, video) được tạo ra hoặc chỉnh sửa đáng kể bởi AI (như deepfake) phải được gắn dấu hiệu nhận biết kỹ thuật (dẫn nhãn số) để người dùng phân biệt được đâu là nội dung thực, đâu là sản phẩm của máy tính.

+ Trách nhiệm lưu vết: các nền tảng cung cấp công cụ AI phải lưu trữ nhật ký (Log) quá trình tạo ra nội dung để phục vụ công tác truy vết khi có hành vi vi phạm pháp luật.

- Quy định về trách nhiệm pháp lý và đạo đức AI .

+ Định danh chủ thể chịu trách nhiệm: xác lập trách nhiệm pháp lý của đơn vị sở hữu thuật toán đối với các sai phạm do AI gây ra.

+ Tuân thủ quy tắc đạo đức AI quốc gia: thiết lập các nguyên tắc về sự công bằng, bảo mật dữ liệu huấn luyện và tính nhân văn trong việc phát triển AI tại Việt Nam.

- Cơ chế hậu kiểm và xử lý thuật toán điều phối thông tin.

+ Giám sát đầu ra: quy định quyền năng của Nhà nước trong việc hậu kiểm các kết quả mà AI trả về trên các nền tảng mạng xã hội, công cụ tìm kiếm.

+ Biện pháp can thiệp: nếu thuật toán bị lợi dụng để đẩy “trend” tin giả hoặc thao túng dư luận theo hướng tiêu cực, cơ quan quản lý có quyền yêu cầu doanh nghiệp điều chỉnh trọng số thuật toán hoặc tạm dừng cung cấp dịch vụ.

4.3. Các giải pháp thực hiện chính sách

Giải pháp 1: Quản trị theo mô hình “tiền kiểm và cấp phép thuật toán”

- Nội dung: yêu cầu mọi hệ thống AI và thuật toán điều phối thông tin phải được cơ quan chức năng kiểm tra mã nguồn, phê duyệt dữ liệu huấn luyện và cấp phép trước khi vận hành.

- Ưu điểm: Ngăn chặn rủi ro ngay từ gốc, đảm bảo tính định hướng chính trị tuyệt đối của thuật toán.

- Nhược điểm: thiếu khả năng về kỹ thuật do AI tự học và thay đổi liên tục, triệt tiêu động lực đổi mới sáng tạo, gây rào cản hành chính rất lớn cho doanh nghiệp công nghệ.

Giải pháp 2: quản trị dựa trên rủi ro và giải pháp hậu kiểm

- Nội dung: Phân loại AI theo mức độ tác động xã hội. Thiết lập các “vành đai an toàn” và cơ chế kiểm soát kỹ thuật số:

+ Nhóm rủi ro cao: bắt buộc đầu nối cổng giám sát, lưu trữ nhật ký thuật toán và chịu sự đánh giá định kỳ.

+ Nhóm rủi ro thấp: tự công bố hợp chuẩn và chịu sự thanh tra xác xuất

- Ưu điểm: cân bằng giữa thúc đẩy ứng dụng và kiểm soát an ninh, phù hợp với tốc độ phát triển của công nghệ, linh hoạt ứng phó với các kịch bản thao túng thông tin mới.

- Nhược điểm: đòi hỏi năng lực giám sát kỹ thuật chuyên sâu và bộ tiêu chí đánh giá thuật toán cực kỳ khoa học.

4.4. Giải pháp tối ưu được lựa chọn và lý do lựa chọn

Lựa chọn giải pháp 2, quản trị dựa trên rủi ro và giải pháp hậu kiểm. Các bước thực thi của giải pháp:

- Giải pháp hạ tầng - AI giám sát AI: xây dựng hệ thống kiểm soát độc lập để chạy thử nghiệm và đối soát các thuật toán AI nhạy cảm. Sử dụng các công cụ AI chuyên dụng để quyết và phát hiện các xu hướng điều phối thông tin sai lệch trên không gian mạng theo thời gian thực.

- Giải pháp kỹ thuật: triển khai tiêu chuẩn kỹ thuật bắt buộc về việc gắn nhãn số cho sản phẩm AI. Phát triển các công cụ miễn phí cho người dân để nhận diện video/hình ảnh deepfake, giúp cộng đồng tự sàng lọc thông tin.

- Giải pháp quản lý, hậu kiểm rủi ro: định kỳ thực hiện “thử nghiệm xâm nhập” đối với các hệ thống AI lớn để kiểm tra xem thuật toán có bị lợi dụng để tuyên truyền thông tin độc hại, xuyên tạc lịch sử hoặc thao túng tâm lý người dùng hay không.

Lý do lựa chọn giải pháp này bởi vì:

- Ngăn chặn chiều quả “chiến tranh thông tin”: Trong bối cảnh các thế lực thù địch sử dụng AI để tạo tin giả quy mô lớn, việc giám sát hậu kiểm là cách tiếp cận “phòng thủ chủ động” hiệu quả nhất, giúp nhận diện chiến dịch thao túng ngay khi chúng vừa bắt đầu.

- Tối ưu hóa nguồn lực quốc gia. Nhà nước không can thiệp vào các ứng dụng AI dân sự (y tế, giáo dục, nông nghiệp) mà tập trung toàn bộ tinh hoa kỹ thuật để kiểm soát các hệ thống AI có khả năng tác động mạnh đến nhận thức xã hội và an ninh quốc gia.

- Phù hợp xu thế quản trị hiện đại. Giải pháp này tương đồng với Đạo luật AI của EU (AI Act) và các tiêu chuẩn an toàn AI của các cường quốc số, giúp Việt Nam khẳng định vị thế quản trị công nghệ chuyên nghiệp, trách nhiệm trên trường quốc tế.

Chính sách 5. Thúc đẩy chuyển đổi số, phát triển kinh tế dữ liệu và tự chủ công nghệ có kiểm soát. Khuyến khích các hoạt động khai thác, sử dụng, chia sẻ

dữ liệu nhằm tạo giá trị kinh tế đi đôi với việc thiết lập hành lang thử nghiệm các công nghệ mới và bảo đảm quyền, lợi ích hợp pháp của tổ chức, cá nhân. Trong đó, ưu tiên đầu tư, phát triển hạ tầng số và các giải pháp bảo mật “Make in Việt Nam” nhằm làm chủ các thuật toán mật mã, công nghệ lưu trữ và xử lý dữ liệu quốc gia phục vụ bảo vệ dữ liệu, nhất là trong khu vực công và đối với hệ thống thông tin quan trọng; xác lập cơ chế hỗ trợ doanh nghiệp công nghệ trong nước tối ưu hóa năng lực tự chủ, thực hiện lộ trình nội địa hóa hạ tầng dữ liệu trọng yếu nhằm giảm thiểu sự lệ thuộc vào công nghệ nước ngoài và bảo đảm an ninh quốc gia bền vững.

5.1. Mục tiêu của chính sách

- Khơi thông nguồn lực dữ liệu. Chuyển đổi dữ liệu từ trạng thái “lưu trữ” sang trạng thái “tạo giá trị”, hình thành thị trường dữ liệu minh bạch, an toàn.
- Xây dựng hệ sinh thái “Make in Việt Nam”. Ưu tiên phát triển và sử dụng các sản phẩm, giải pháp bảo mật nội địa. Hỗ trợ doanh nghiệp trong nước làm chủ các công nghệ lõi về thuật toán, mã hóa và an ninh thông tin.
- Đổi mới sáng tạo có kiểm soát: thiết lập cơ chế thử nghiệm (Sandbox) để các công nghệ dữ liệu mới được vận hành an toàn trước khi triển khai rộng rãi.

5.2. Nội dung của chính sách

- Phát triển thị trường và dịch vụ dữ liệu
- + Quy định điều kiện hình thành và vận hành, tiêu chuẩn đảm bảo an ninh các sản phẩm dịch vụ dữ liệu, các tổ chức trung gian dữ liệu để kết nối bên cung và bên cầu một cách hợp pháp.
- + Xác lập quyền sở hữu, khai thác và quyền hưởng lợi từ dữ liệu của các tổ chức, cá nhân, tạo cơ sở pháp lý để định giá và giao dịch dữ liệu như một loại hàng hóa đặc biệt.
- Ưu tiên phát triển giải pháp bảo mật nội địa
- + Thiết lập danh mục các sản phẩm, giải pháp an ninh dữ liệu trọng yếu ưu tiên sử dụng hàng Việt Nam trong các cơ quan Nhà nước và hệ thống thông tin quan trọng quốc gia.
- + Cơ chế hỗ trợ doanh nghiệp công nghệ trong nước nghiên cứu, phát triển các chuẩn mã hóa dân sự và mật mã quốc gia, đảm bảo tính tự cường trong việc bảo vệ dữ liệu Cốt lõi và Quan trọng.
- + Cơ chế thử nghiệm đổi mới sáng tạo: quy định phạm vi, không gian, thời gian thử nghiệm đối với công nghệ dữ liệu mới (AI, Blockchain, tính toán bảo

mật đa bên).

+ Cơ chế miễn trừ trách nhiệm dân sự có thời hạn đối với các sai sót kỹ thuật trong quá trình thử nghiệm nếu đơn vị vận hành tuân thủ đúng quy trình kiểm soát rủi ro đã được phê duyệt.

- Hỗ trợ làm chủ thuật toán và mã hóa

+ Chính sách ưu đãi thuế, tín dụng và đầu tư cho các dự án nghiên cứu làm chủ thuật toán lõi, giải mã dữ liệu và an ninh thông tin

+ Xây dựng các tiêu chuẩn kỹ thuật nội địa về an ninh dữ liệu để làm rào cản kỹ thuật hợp pháp, bảo vệ thị trường nội địa và các doanh nghiệp công nghệ trong nước.

5.3. Các giải pháp thực hiện chính sách

Giải pháp 1: Thúc đẩy kinh tế dữ liệu tự do

- Nội dung: đề thị trường tự điều tiết, khuyến khích sử dụng công nghệ phổ biến toàn cầu (kể cả ngoại nhập) để tối ưu chi phí và tốc độ chuyển đổi số.

- Ưu điểm: Tốc độ tăng trưởng kinh tế số nhanh; doanh nghiệp dễ dàng tiếp cận công nghệ rẻ và sẵn có.

- Nhược điểm: nguy cơ mất an ninh từ lõi. Quốc gia bị phụ thuộc vào các “chìa khóa” mã hóa của nước ngoài, doanh nghiệp nội địa khó cạnh tranh và bị triệt tiêu năng lực sáng tạo tự chủ.

Giải pháp 2: Thúc đẩy kinh tế dữ liệu tự cường

- Nội dung: Kết hợp giữa mở cửa thị trường và bảo hộ công nghệ lõi. Nhà nước dẫn dắt bằng đầu tư công cho các sản phẩm bảo mật nội địa và hỗ trợ doanh nghiệp làm chủ thuật toán mã hóa thông qua các đặc khu thử nghiệm.

- Ưu điểm: Hình thành hệ sinh thái an ninh dữ liệu bền vững, đảm bảo bí mật quốc gia được bảo vệ bằng nội lực, tạo ra các doanh nghiệp công nghệ đủ mạnh để cạnh tranh quốc tế.

- Nhược điểm: Đòi hỏi nguồn lực tài chính lớn và quy trình thẩm định kỹ thuật nghiêm ngặt ngay từ đầu.

5.4. Giải pháp tối ưu được lựa chọn và lý do lựa chọn

Lựa chọn giải pháp 2, Thúc đẩy kinh tế dữ liệu tự cường. Các bước thực thi của giải pháp:

- Tính độc lập chiến lược, trong lĩnh vực an ninh dữ liệu, việc dùng “ổ khóa” của đối tác nước ngoài để bảo vệ “kho báu” của Việt Nam là rủi ro tiềm ẩn. Làm chủ thuật toán và mã hóa là “lá chắn” cuối cùng bảo vệ chủ quyền số.

- Kích hoạt động lực tăng trưởng mới, dữ liệu chỉ tạo ra tiền khi được chia sẻ và sử dụng. Chính sách thử nghiệm có kiểm soát và thị trường dữ liệu giúp giải phóng hàng tỷ GB dữ liệu đang bị đóng băng tại các Bộ, ngành, biến chúng thành tài nguyên cho doanh nghiệp sáng tạo.

- Phù hợp với tinh thần tự chủ, tự cường, giải pháp này cụ thể hóa tinh thần đưa Việt Nam trở thành quốc gia mạnh về số, nơi an ninh dữ liệu không phải “phanh hãm” mà là “bệ phóng” giúp kinh tế số phát triển một cách bền vững.

Lý do lựa chọn giải pháp này bởi vì:

- Bảo đảm chủ quyền và tính tự chủ chiến lược.
- Tạo thị trường “môi” để hình thành các tập đoàn công nghệ độc lập.
- Hóa giải mâu thuẫn giữa “kiểm soát” và “sáng tạo”.
- Tối ưu hóa lợi ích kinh tế và giảm chi phí xã hội dài hạn.

Việc lựa chọn giải pháp là sự khẳng định “lấy an ninh làm nền tảng, lấy kinh tế làm động lực”. Đây là con đường duy nhất để Việt Nam không chỉ dừng lại ở việc bảo vệ dữ liệu mà còn biến dữ liệu thành năng lực cạnh tranh quốc gia, đưa đất nước thoát khỏi sự lệ thuộc vào công nghệ ngoại và trở thành một thực thể số tự chủ trên bản đồ thế giới.

Chính sách 6. Phát triển nguồn nhân lực tinh nhuệ, bảo đảm nguồn lực tài chính thực thi và đẩy mạnh hợp tác quốc tế về an ninh dữ liệu và chủ quyền số. Nhà nước ưu tiên bố trí ngân sách, thiết lập cơ chế tài chính đặc thù, xã hội hóa nguồn lực tài chính để đào tạo, thu hút, đãi ngộ đội ngũ chuyên gia, lực lượng chuyên trách an ninh dữ liệu trình độ cao và bảo đảm an ninh dữ liệu. Chủ động mở rộng hợp tác quốc tế trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi và phù hợp với pháp luật Việt Nam, điều ước quốc tế mà Việt Nam là thành viên, bảo đảm an ninh dữ liệu, chủ quyền và lợi ích quốc gia trên không gian mạng.

6.1. Mục tiêu của chính sách

- Xây dựng lực lượng nòng cốt: hình thành đội ngũ chuyên gia an ninh dữ liệu trình độ cao, đủ năng lực làm chủ công nghệ hiện đại, vận hành các đơn vị về an ninh dữ liệu và bảo vệ chủ quyền số.

- Tạo đột phá trong thu hút nhân tài: thiết lập các cơ chế đãi ngộ đặc thù, vượt trội để thu hút các chuyên gia giỏi trong và ngoài nước tham gia vào công tác an ninh dữ liệu quốc gia.

- Bảo đảm nguồn lực tài chính thực thi và xã hội hóa nguồn lực tài chính để

đào tạo, thu hút, đãi ngộ đội ngũ chuyên gia, lực lượng chuyên trách an ninh dữ liệu trình độ cao và bảo đảm an ninh dữ liệu.

- Khẳng định vị thế quốc tế: tích cực hội nhập, hợp tác quốc tế trong phòng chống tội phạm dữ liệu xuyên biên giới dựa trên nguyên tắc tôn trọng độc lập, chủ quyền và bình đẳng, bảo vệ lợi ích quốc gia từ sớm, từ xa.

6.2. Nội dung của chính sách:

- Đào tạo và phát triển nguồn nhân lực chất lượng cao về an ninh dữ liệu.
+ Quy định chương trình đào tạo chuyên sâu về an ninh dữ liệu, mật mã và thuật toán tại các cơ sở giáo dục đại học trọng điểm quốc gia.

+ Thiết lập hệ thống chứng chỉ hành nghề an ninh dữ liệu tiêu chuẩn quốc tế nhưng có sự công nhận tương đương tại Việt Nam để chuẩn hóa đội ngũ chuyên gia.

- Chính sách đặc thù thu hút và đãi ngộ nhân tài.

+ Xác lập cơ chế tiền lương, thưởng và các điều kiện làm việc đặc biệt đối với vị trí “Chuyên gia an ninh dữ liệu chiến lược” trong các cơ quan nhà nước.

+ Cho phép áp dụng các hình thức khoán việc, thuê chuyên gia tư vấn cao cấp (trong và ngoài nước) theo đơn đặt hàng kỹ thuật cụ thể mà không bị gò bó bởi các thang bảng lương hành chính thông thường.

- Bảo đảm nguồn lực tài chính thực thi và thực hiện xã hội hóa nguồn lực tài chính để đào tạo, thu hút, đãi ngộ đội ngũ chuyên gia, lực lượng chuyên trách an ninh dữ liệu trình độ cao và triển khai bảo đảm an ninh dữ liệu.

- Hợp tác quốc tế và phòng chống tội phạm dữ liệu xuyên biên giới

+ Quy định cơ chế phối hợp chia sẻ thông tin về nguy cơ an ninh dữ liệu với các tổ chức quốc tế và cơ quan thực thi pháp luật nước ngoài.

+ Thiết lập các hiệp định tương trợ tư pháp về dữ liệu, tập trung vào việc dẫn độ tội phạm dữ liệu và thu hồi tài sản dữ liệu bị chiếm đoạt trái phép ra nước ngoài.

6.3. Các giải pháp thực hiện chính sách

Giải pháp 1: Phát triển nguồn nhân lực, bảo đảm nguồn lực tài chính thực thi, hợp tác quốc tế theo mô hình truyền thống

- Nội dung: đào tạo nhân lực dựa trên hệ thống đại học hiện có, tuyển dụng và đãi ngộ chuyên gia theo quy định chung của công chức, viên chức hiện hành, triển khai hợp tác quốc tế theo quy định hiện hành, bảo đảm nguồn lực tài chính thực thi bằng ngân sách nhà nước.

- Ưu điểm: đảm bảo tính thống nhất của hệ thống quản lý nhà nước; chi phí

ngân sách ổn định, dễ dự toán.

- Nhược điểm: nguy cơ chảy máu chất xám. Không đủ sức cạnh tranh với khu vực tư nhân và các tập đoàn đa quốc gia, nhân sự nhà nước sẽ lạc hậu so với tốc độ phát triển của tội phạm công nghệ cao, không nâng cao được hiệu quả hợp tác quốc tế trong bối cảnh rủi ro, vi phạm pháp luật về dữ liệu ngày càng phức tạp, khó lường.

Giải pháp 2: phát triển theo mô hình đặc thù và hội nhập chủ động, bảo đảm nguồn lực tài chính thực thi bằng sự kết hợp giữa Ngân sách nhà nước và xã hội hóa nguồn lực tài chính.

- Nội dung: xây dựng các biệt đội an ninh dữ liệu với cơ chế tuyển dụng, đãi ngộ như một ngành nghề đặc biệt (tương đương với các ngạch quân sự, mật mã cao cấp). Kết hợp đào tạo trong nước với việc gửi nhân sự tinh nhuệ tu nghiệp tại các cường quốc số; tăng cường hợp tác quốc tế trong đào tạo nhân lực, chuyển giao công nghệ, xây dựng quy định, tiêu chuẩn, quy trình bảo đảm an ninh luồng chảy dữ liệu xuyên biên giới, phối hợp biện pháp nghiệp vụ để phòng ngừa, ngăn chặn tội phạm và vi phạm pháp luật về dữ liệu xuyên biên giới; tối ưu hóa nguồn lực tài chính bằng phương thức xã hội hóa, đảm bảo hiệu quả và quy định của pháp luật.

- Ưu điểm: thu hút được những trí tuệ hàng đầu, xây dựng được lực lượng phản ứng nhanh có khả năng đối trọng với tội phạm quốc tế, nâng cao hiệu quả hợp tác quốc tế, tạo vị thế bình đẳng cho Việt Nam trong các diễn đàn an ninh mạng toàn cầu.

- Nhược điểm: hiệu quả triển khai phụ thuộc nhiều vào việc cụ thể hóa bằng văn bản dưới luật, chính sách nhân lực và cơ chế phối hợp thực thi của các cơ quan có liên quan.

6.4. Giải pháp tối ưu được lựa chọn và lý do lựa chọn

Lựa chọn giải pháp 2, phát triển theo mô hình đặc thù và hội nhập chủ động, bảo đảm nguồn lực tài chính thực thi bằng sự kết hợp giữa Ngân sách nhà nước và xã hội hóa nguồn lực tài chính. Các bước thực thi của giải pháp:

- Quy định các nguyên tắc, định hướng lớn về phát triển nguồn nhân lực chất lượng cao trong lĩnh vực dữ liệu và an ninh dữ liệu;

- Xác lập cơ sở chính sách cho việc thu hút, trọng dụng, sử dụng chuyên gia và nhân lực trình độ cao trong các hoạt động xây dựng, tổ chức thực hiện pháp luật, tư vấn, đào tạo, hỗ trợ kỹ thuật và xử lý các vấn đề chuyên sâu;

- Quy định nguyên tắc hợp tác quốc tế trong trao đổi thông tin, chia sẻ kinh nghiệm, hỗ trợ nâng cao năng lực và phối hợp phòng, chống vi phạm pháp luật về dữ liệu trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng và phù hợp với pháp luật Việt Nam, điều ước quốc tế mà Việt Nam là thành viên;

- Giao Chính phủ và các Bộ, ngành liên quan quy định chi tiết, hướng dẫn và tổ chức thực hiện các nội dung cụ thể về đào tạo, bồi dưỡng, thu hút nhân lực, hợp tác quốc tế và cơ chế phối hợp.

Lí do lựa chọn giải pháp này bởi vì:

- Con người là nhân tố quyết định. Trong cuộc chiến an ninh dữ liệu, công nghệ chỉ là công cụ, con người mới là thực thể vận hành. Một chuyên gia giỏi có thể ngăn chặn những thiệt hại hàng nghìn tỷ đồng; do đó, đầu tư vào nhân tài là khoản đầu tư có lợi nhuận cao nhất cho an ninh quốc gia.

- Xử lý tận gốc bài toán “chảy máu chất xám”. Nếu không có chính sách đãi ngộ đột phá, các chuyên gia an ninh dữ liệu giỏi nhất của Việt Nam sẽ làm việc cho các tập đoàn nước ngoài, vô tình tạo ra sự chênh lệch về năng lực phòng thủ giữa Nhà nước và các thực thể khác.

- Nguồn lực tài chính mạnh sẽ tạo ra hàng rào bảo vệ chủ động và hiệu quả trong thực thi nhiệm vụ bảo đảm an ninh dữ liệu.

- Phù hợp với tinh thần tự chủ, tự cường, giải pháp này cụ thể hóa tinh thần đưa Việt Nam trở thành quốc gia mạnh về số, nơi an ninh dữ liệu không phải “phanh hãm” mà là “bệ phóng” giúp kinh tế số phát triển một cách bền vững.

- Bảo vệ chủ quyền số từ xa: tội phạm dữ liệu thường có tính chất xuyên biên giới. Việc hội nhập quốc tế dựa trên nguyên tắc bình đẳng giúp Việt Nam xây dựng được “mạng lưới đồng minh số” cho phép chúng ta ngăn chặn các cuộc tấn công dữ liệu ngay khi chúng còn nằm ngoài lãnh thổ.

- Việc xây dựng đội ngũ chuyên gia tinh tuệ với chế độ đãi ngộ xứng tầm và vị thế quốc tế chủ động là sự chuẩn bị tốt nhất để Việt Nam bảo vệ vững chắc chủ quyền số và tham gia có trách nhiệm vào trật tự an ninh dữ liệu toàn cầu.

VI. NHỮNG NỘI DUNG BỔ SUNG MỚI SO VỚI HỒ SƠ CHÍNH SÁCH GỬI THẨM ĐỊNH (NẾU CÓ)

VI. DỰ KIẾN NGUỒN LỰC, ĐIỀU KIỆN BẢO ĐẢM CHO VIỆC THỰC HIỆN CHÍNH SÁCH

1. Về bảo đảm nguồn nhân lực

- Kien toàn bộ máy quản lý nhà nước về an ninh dữ liệu từ Trung ương đến

địa phương. Trọng tâm là hình thành đội ngũ lãnh đạo chỉ huy, quản lý và đội ngũ chuyên gia tinh nhuệ vận hành các đơn vị bảo đảm an ninh dữ liệu.

- Cơ chế đặc thù: xây dựng và áp dụng bảng lương chuyên gia và chế độ phụ cấp độc hại, nguy hiểm đặc thù cho lực lượng làm công tác liên quan đến an ninh dữ liệu, mật mã, tác chiến trên không gian mạng.

- Đào tạo: dự kiến hằng năm đào tạo và cấp chứng chỉ an ninh dữ liệu chuyên sâu cho khoảng 1000 cán bộ nòng cốt thuộc các Bộ, ngành và địa phương.

2. Về điều kiện hạ tầng và công nghệ

- Ưu tiên hạ tầng dùng chung, tận dụng tối đa hạ tầng sẵn có của các đơn vị quản lý vận hành về dữ liệu và bảo đảm an ninh dữ liệu để thực hiện lưu trữ tập trung, tránh đầu tư dàn trải, lãng phí tại các Bộ, ngành lẻ tẻ kém ngân sách.

- Đầu tư và triển khai hệ thống tường lửa quốc gia, “cổng an ninh dữ liệu”, ngân sách nhà nước ưu tiên đầu tư cho hệ thống giám sát luồng chảy dữ liệu xuyên biên giới và các nền tảng “AI giám sát AI” để thực hiện hậu kiểm thuật toán.

- Làm chủ công nghệ nội địa: dành một phần kinh phí từ chương trình Chuyển đổi số quốc gia để hỗ trợ các doanh nghiệp nội địa nghiên cứu, sản xuất các sản phẩm mã hóa và bảo mật “Make in Việt Nam”.

3. Về bảo đảm nguồn tài chính

- Ngân sách nhà nước: chi thường xuyên và chi đầu tư theo quy định của Luật Ngân sách nhà nước.

- Nguồn thu từ dịch vụ dữ liệu: trích một phần từ việc cung cấp các dịch vụ dữ liệu có thu phí để tái đầu tư cho công tác bảo đảm an ninh dữ liệu, bảo mật.

- Xã hội hóa: khuyến khích các tập đoàn, doanh nghiệp đầu tư nghiên cứu giải pháp an ninh dữ liệu thông qua các chính sách miễn giảm thuế.

Việc sử dụng kinh phí phải đúng mục đích, nội dung, chế độ, định mức chi theo quy định của pháp luật về quản lý, sử dụng ngân sách nhà nước đối với hoạt động thuộc lĩnh vực quốc phòng, an ninh.

4. Đánh giá tác động thủ tục hành chính

- Cắt giảm “giấy phép con”, việc chuyển dịch từ cơ chế “tiền kiểm” sang “hậu kiểm số” giúp giảm khoảng 40% thủ tục hành chính cho doanh nghiệp hoạt động trong lĩnh vực kinh tế số.

- Hỗ trợ doanh nghiệp: cơ chế Sandbox và danh mục quốc gia an toàn về dữ liệu sẽ giúp doanh nghiệp rút ngắn thời gian tiếp cận thị trường quốc tế, giảm chi phí tư vấn pháp lý và kỹ thuật.

- Các chính sách có phát sinh thủ tục hành chính song mục tiêu là thiết lập hệ sinh thái an ninh dữ liệu hoàn chỉnh, bền vững để Nhà nước nhận diện và bảo vệ tài nguyên số, là sự chuyển dịch từ kiểm soát sang quản trị, thay vì để dữ liệu trôi nổi tự do dẫn đến nguy cơ thất thoát có thể gây thiệt hại hàng nghìn tỉ đô thì việc quản lý thông qua thủ tục hành chính đề cử giúp định danh và bảo vệ di sản dữ liệu quốc gia, tạo nền móng vững chắc cho chủ quyền số, xã hội số và kinh tế số.

- Đề tối ưu hóa và giảm gánh nặng cho thủ tục hành chính từ các chính sách, các giải pháp được lựa chọn áp dụng triển khai:

+ Sử dụng dịch vụ công trực tuyến: dự kiến toàn bộ thủ tục về an ninh dữ liệu được thực hiện trên môi trường số, kết nối liên thông giữa đơn vị chuyên trách bảo đảm an ninh dữ liệu với các Bộ, ngành.

+ Thực hiện cơ chế hậu kiểm thay vì tiền kiểm: đối với các nhóm dữ liệu cấp độ 3 và 4, nghiên cứu áp dụng cơ chế tự công bố tiêu chuẩn và Nhà nước chỉ thực hiện thanh tra, kiểm tra dựa trên xác suất hoặc khi có dấu hiệu vi phạm.

+ Tiêu chuẩn quốc tế hóa: áp dụng các tiêu chuẩn mật mã và dữ liệu tương đồng với thế giới để doanh nghiệp không phải làm lại thủ tục khi hội nhập

Mặc dù việc thiết lập hệ sinh thái an ninh dữ liệu có phát sinh một số thủ tục hành chính mới nhưng đây là “chi phí an ninh thiết yếu” để ngăn ngừa các rủi ro, thảm họa có thể gây thiệt hại không thể đảo ngược cho nền kinh tế và chủ quyền quốc gia. Về lâu dài, các thủ tục hành chính này chính là bộ lọc giúp loại bỏ các yếu tố độc hại, tạo ra một không gian số minh bạch, an toàn, từ đó thúc đẩy dòng chảy dữ liệu tạo ra giá trị kinh tế bền vững theo tinh thần của Hiến pháp và chiến lược chuyển đổi số quốc gia.

Trên đây là Tờ trình hồ sơ chính sách dự án Luật An ninh dữ liệu, Bộ Công an kính trình Chính phủ xem xét, quyết định.

(Xin gửi kèm theo: (1) Báo cáo đánh giá tác động của chính sách; (2) Báo cáo rà soát các chủ trương, đường lối của Đảng, văn bản quy phạm pháp luật, điều ước quốc tế có liên quan đến chính sách; (3) Báo cáo thực trạng quan hệ xã hội liên quan đến an ninh dữ liệu; (4) Bản thuyết minh quy phạm hóa chính sách)./.

Nơi nhận:

- Như trên;
- Văn phòng Chính phủ
- Thủ tướng, các Phó Thủ tướng (để báo cáo);
- Lưu: VT, BCA(A05).

BỘ TRƯỞNG

Đại tướng Lương Tam Quang

