DỰ ÁN LUẬT AN NINH DỮ LIỆU

1. Sự cần thiết ban hành Luật An ninh dữ liệu

Trong kỷ nguyên chuyển đổi số, dữ liệu không còn đơn thuần là thông tin được lưu trữ, xử lý mà đã trở thành một loại tư liệu sản xuất đặc biệt, một tài sản chiến lược quyết định năng lực cạnh tranh, sự ổn định kinh tế và an ninh của mỗi quốc gia. Chủ quyền quốc gia trên không gian số, theo đó, không chỉ dừng lại ở việc bảo vệ hạ tầng mạng mà còn mở rộng sang quyền quản lý, kiểm soát và bảo vệ dữ liệu. Mỗi thao tác giao dịch, truy cập, chia sẻ thông tin diễn ra hằng ngày trên không gian mạng đều có thể trở thành mục tiêu bị đánh cắp, trục lợi hoặc bị lợi dụng để xâm phạm an ninh quốc gia nếu không được bảo vệ đúng cách.

- Về cơ sở chính trị:

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 xác định bảo đảm chủ quyền quốc gia trên không gian mạng và an ninh dữ liệu là điều kiện tiên quyết, không thể tách rời trong tiến trình chuyển đổi số. Đây là định hướng chính trị quan trọng hàng đầu, đặt ra yêu cầu phải sớm thể chế hóa thành luật chuyên ngành, toàn diện về an ninh dữ liệu, thay vì tiếp tục xử lý vấn đề này bằng các quy định tản mạn, nằm rải rác trong nhiều văn bản khác nhau.

- Về cơ sở thực tiễn:

Công tác bảo đảm an ninh mạng, an ninh dữ liệu tại Việt Nam thời gian qua cho thấy mức độ rủi ro ngày càng gia tăng cả về quy mô lẫn tính chất. Số vụ tấn công mạng có chủ đích, phần lớn nhằm thẳng vào dữ liệu, có xu hướng tăng nhanh qua từng năm; xuất hiện sự chuyển dịch rõ rệt từ các đợt tấn công dàn trải sang những chiến dịch tấn công có chủ đích, kéo dài, xâm nhập sâu và âm thầm thu thập dữ liệu trong thời gian dài trước khi bị phát hiện. Tình trạng dữ liệu cá nhân bị rao bán trái phép trên các diễn đàn ngầm diễn ra ở quy mô lớn; thiệt hại kinh tế do lừa đảo trực tuyến, mã độc tống tiền gây ra là rất đáng kể. Quy mô và tốc độ gia tăng của rủi ro an ninh dữ liệu đang vượt xa năng lực ứng phó hiện có; nếu không có một thể chế đủ mạnh để quản lý rủi ro ngay từ gốc, nguy cơ bị động, lúng túng trong ứng phó sự cố sẽ ngày càng lớn, gây thiệt hại cho cơ quan, tổ chức, cá nhân, thậm chí ảnh hưởng nghiêm trọng đến an ninh quốc gia.

- Về kinh nghiệm quốc tế:

Mỗi quốc gia, khu vực lựa chọn một cách tiếp cận khác nhau đối với quản trị dữ liệu, tùy theo điều kiện thể chế, trình độ phát triển công nghệ; điểm chung là hầu hết các nền kinh tế lớn đều đã hoặc đang xây dựng một khung pháp lý riêng, chuyên biệt để quản lý rủi ro an ninh đối với dữ liệu, tách bạch với khung pháp lý về an ninh mạng và về bảo vệ dữ liệu cá nhân. Đây là cơ sở thực tiễn

quốc tế quan trọng để khẳng định việc Việt Nam xây dựng Luật An ninh dữ liệu là bước đi phù hợp với xu thế chung.

- Về khoảng trống của pháp luật hiện hành:

Hệ thống pháp luật hiện hành của Việt Nam đã có Luật An ninh mạng, Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, Luật Trí tuệ nhân tạo, song mỗi luật chỉ điều chỉnh một khía cạnh riêng: Luật An ninh mạng tập trung bảo vệ an ninh mạng đối với hệ thống thông tin; Luật Bảo vệ dữ liệu cá nhân bảo vệ quyền, lợi ích hợp pháp của chủ thể dữ liệu cá nhân; Luật Dữ liệu điều chỉnh việc xây dựng, quản trị, khai thác, chia sẻ, phân loại dữ liệu theo tính chất quan trọng. Đến nay chưa có luật nào quy định toàn diện việc bảo vệ an ninh của chính dữ liệu, xuyên suốt từ khâu thu thập, tạo lập, lưu trữ, xử lý, truyền đưa, chia sẻ cho đến khi tiêu hủy. Khoảng trống này khiến nhiều hoạt động xử lý dữ liệu có nguy cơ cao - như xử lý dữ liệu quy mô lớn, huấn luyện trí tuệ nhân tạo bằng dữ liệu nhạy cảm, chuyển dữ liệu xuyên biên giới - chưa có cơ chế quản lý rủi ro tương xứng.

2. Nội dung cơ bản và ý nghĩa của Luật An ninh dữ liệu

Dự thảo Luật An ninh dữ liệu được xây dựng với bố cục 06 chương, 29 điều.

a) Về ranh giới áp dụng pháp luật và xử lý chồng lấn thủ tục. Dự thảo Luật quy định rõ việc bảo đảm chủ quyền dữ liệu quốc gia không làm phát sinh quyền sở hữu của Nhà nước đối với dữ liệu không thuộc sở hữu nhà nước, không làm thay đổi quyền của chủ thể dữ liệu, qua đó phân định rạch ròi giữa thẩm quyền quản lý an ninh của Nhà nước với quyền sở hữu, khai thác hợp pháp của tổ chức, cá nhân, doanh nghiệp đối với dữ liệu của mình. Đối với vấn đề giao thoa với các luật hiện hành, Điều 3 dự thảo Luật quy định nguyên tắc phân định rõ ràng theo từng nội dung giao thoa cụ thể: nguyên tắc, điều kiện xử lý dữ liệu cá nhân, quyền của chủ thể dữ liệu cá nhân tiếp tục thực hiện theo pháp luật về bảo vệ dữ liệu cá nhân; việc bảo vệ an ninh mạng đối với hệ thống thông tin thực hiện theo pháp luật về an ninh mạng; hoạt động xây dựng, quản trị, khai thác, chia sẻ, phân loại dữ liệu theo tính chất quan trọng tiếp tục thực hiện theo pháp luật về dữ liệu; các nội dung về trí tuệ nhân tạo, công nghiệp công nghệ số, chuyển đổi số, giao dịch điện tử, lưu trữ thực hiện theo pháp luật chuyên ngành tương ứng; Luật An ninh dữ liệu chỉ bổ sung biện pháp bảo vệ an ninh dữ liệu phát sinh trong các hoạt động đó. Dự thảo Luật cũng đưa ra phương án xử lý chồng lấn ở cấp độ thủ tục hành chính: khi Luật này và luật khác cùng quy định thủ tục, đánh giá, thẩm định, kiểm tra hoặc chế độ báo cáo đối với cùng một đối tượng, cùng một nội dung thì tổ chức, cá nhân chỉ lập một bộ hồ sơ, thực hiện một thủ tục thông qua một đầu mối tiếp nhận; kết quả đánh giá, thẩm định, chứng nhận đã thực hiện hợp pháp theo luật khác và còn hiệu lực được công nhận, cơ quan nhà nước không yêu cầu thực hiện lại; báo cáo sự cố gửi qua hệ

thống điện tử.

b) Về cơ chế quản lý theo cấp độ rủi ro. Dự thảo Luật quy định 05 cấp độ rủi ro an ninh dữ liệu, từ Cấp độ 1 (thấp nhất) đến Cấp độ 5 (cao nhất), xác định dựa trên khả năng xảy ra sự cố và mức độ thiệt hại có thể gây ra. Toàn bộ nghĩa vụ cụ thể được phân bổ bám sát cấp độ này, áp dụng xuyên suốt từ hoạt động chuyển đổi số, hạ tầng số, xử lý dữ liệu quy mô lớn, công nghệ mới và trí tuệ nhân tạo cho đến hoạt động xuyên biên giới.

c) Về trách nhiệm của Nhà nước, cơ quan, tổ chức, doanh nghiệp và cá nhân. Trên nền tảng cơ chế quản lý theo cấp độ rủi ro, dự thảo Luật phân định rõ trách nhiệm của từng chủ thể. Đối với Nhà nước, dự thảo xác định Chính phủ thống nhất quản lý nhà nước về an ninh dữ liệu. Đối với cơ quan, tổ chức, doanh nghiệp - với tư cách chủ quản dữ liệu - trách nhiệm trung tâm là tự xác định cấp độ rủi ro của dữ liệu mình quản lý và tự áp dụng biện pháp bảo vệ tương xứng, chịu trách nhiệm trước pháp luật về việc đó; Nhà nước thực hiện hậu kiểm là chủ yếu, chỉ tiền kiểm đối với dữ liệu, hệ thống có rủi ro cao. Mức độ trách nhiệm được phân hóa theo quy mô, cấp độ rủi ro: dữ liệu Cấp độ 1, Cấp độ 2 - chiếm phần lớn hoạt động xử lý dữ liệu thông thường - gần như không phát sinh thủ tục hành chính; hộ kinh doanh, doanh nghiệp nhỏ, siêu nhỏ, doanh nghiệp khởi nghiệp sáng tạo chỉ cần áp dụng biện pháp bảo vệ cơ bản theo hướng dẫn chung; chỉ từ Cấp độ 3 trở lên, chủ quản dữ liệu mới phải thực hiện đánh giá tác động, kiểm toán định kỳ, dữ liệu Cấp độ 4, Cấp độ 5 mới phải được thẩm định cùng với thẩm định an ninh mạng trước khi hệ thống được đưa vào vận hành chính thức. Đối với cá nhân, dự thảo Luật tiếp cận theo hai tư cách: với tư cách chủ thể dữ liệu, quyền và lợi ích hợp pháp tiếp tục được bảo vệ theo pháp luật về bảo vệ dữ liệu cá nhân, đồng thời được hưởng thêm lớp bảo vệ an ninh bổ sung theo cấp độ rủi ro khi dữ liệu được xử lý trong hệ thống có mức độ rủi ro cao; với tư cách nhân sự phụ trách an ninh dữ liệu hoặc chuyên gia hoạt động độc lập, dự thảo khuyến khích cá nhân chủ động phát hiện, kiểm thử, thông báo lỗ hổng an ninh dữ liệu với thiện chí, được bảo vệ danh tính, quyền, lợi ích hợp pháp và loại trừ trách nhiệm pháp lý tương ứng - cơ chế nhằm huy động nguồn lực xã hội thay vì chỉ trông chờ vào năng lực của bộ máy nhà nước.

d) Về hệ thống biện pháp bảo vệ an ninh dữ liệu. Để các trách nhiệm nêu trên đi vào thực chất, dự thảo Luật cụ thể hóa thành một hệ thống biện pháp bảo vệ bao quát toàn diện, tổ chức thành tám nhóm: biện pháp quản lý (xác định cấp độ rủi ro, đánh giá tác động, kiểm toán, thẩm định, thanh tra, kiểm tra); biện pháp kỹ thuật (mã hóa dữ liệu, quản lý truy cập, sao lưu, phục hồi, tiêu hủy dữ liệu an toàn); bảo vệ an ninh vật lý đối với thiết bị, hạ tầng lưu trữ; đánh giá sự phù hợp, chứng nhận theo tiêu chuẩn kỹ thuật; ứng phó, khắc phục sự cố; đào tạo, tuyên truyền; ngăn chặn, vô hiệu hóa dữ liệu độc hại; và xử lý vi phạm pháp luật. Các biện pháp này được áp dụng xuyên suốt vòng đời dữ liệu - từ thiết kế, thu thập, lưu trữ, xử lý, truyền đưa cho đến khi tiêu hủy - và khi cần thiết được

bổ sung bằng biện pháp kỹ thuật khẩn cấp đối với sự cố đặc biệt nghiêm trọng, đi kèm nguyên tắc áp dụng biện pháp ít hạn chế quyền nhất, có thời hạn rõ ràng và bảo đảm quyền khiếu nại, bồi thường của tổ chức, cá nhân bị áp dụng trái pháp luật.

đ) Về ý nghĩa của việc ban hành Luật. Việc ban hành Luật An ninh dữ liệu mang nhiều tầng ý nghĩa gắn bó chặt chẽ với nhau. Trước hết là bảo vệ hạ tầng và bảo vệ dữ liệu; tiếp đến là tăng cường nhận thức xã hội về an ninh dữ liệu - việc luật hóa trách nhiệm đào tạo, tuyên truyền, cùng cơ chế khuyến khích cá nhân, chuyên gia, tổ chức xã hội - nghề nghiệp chủ động tham gia phát hiện, thông báo lỗ hổng, sẽ góp phần hình thành một nền văn hóa an ninh dữ liệu rộng khắp trong xã hội, thay vì chỉ dừng lại ở nhận thức của một nhóm chuyên gia kỹ thuật. Mặt khác, với nguyên tắc an ninh không được phép trở thành rào cản cho phát triển, Luật còn góp phần thúc đẩy kinh tế số và kiến tạo không gian phát triển cho ngành công nghiệp bảo vệ dữ liệu trong nước, thông qua các chính sách ưu đãi đầu tư, thuế đối với nghiên cứu, phát triển công nghệ bảo vệ an ninh dữ liệu, mật mã an ninh, mật mã kháng lượng tử, mật mã lượng tử; chính sách phát triển hệ sinh thái và công nghiệp an ninh dữ liệu tự chủ, tin cậy, ưu tiên hình thành năng lực nghiên cứu, phòng thử nghiệm, doanh nghiệp công nghệ nòng cốt và sản phẩm lưỡng dụng trong nước - mở ra dư địa để doanh nghiệp công nghệ Việt Nam tham gia nghiên cứu, sản xuất cả giải pháp phần cứng lẫn phần mềm bảo vệ an ninh dữ liệu, thay vì chỉ phụ thuộc hoàn toàn vào sản phẩm, công nghệ nước ngoài.

Từ những vấn đề trên, có thể khẳng định việc xây dựng, ban hành Luật An ninh dữ liệu không đơn thuần là hoàn thiện một mảnh ghép còn thiếu trong hệ thống pháp luật, mà là một bước đi tất yếu, có tính chiến lược, nhằm chuyển dịch mô hình quản trị quốc gia về dữ liệu từ trạng thái bị động, ứng phó sau sự cố sang chủ động phòng ngừa, kiểm soát rủi ro ngay từ đầu; bảo vệ vững chắc chủ quyền dữ liệu quốc gia trong tiến trình chuyển đổi số; đồng thời tạo nền tảng niềm tin và không gian phát triển để người dân, doanh nghiệp, ngành công nghiệp bảo vệ dữ liệu trong nước yên tâm tham gia, đóng góp vào nền kinh tế số của đất nước.

3. Những vấn đề cốt lõi của dự thảo Luật An ninh dữ liệu

Dự thảo Luật quy định toàn diện từ nguyên tắc chung đến các cơ chế bảo vệ cụ thể, nguồn lực bảo vệ và quản lý nhà nước. Trong số nhiều nội dung của dự thảo, có thể khái quát một số vấn đề mang tính cốt lõi, chi phối toàn bộ cách tiếp cận của đạo luật.

Về phương pháp luận, cách tiếp cận quản lý theo cấp độ rủi ro mà dự thảo Luật lựa chọn không phải là một mô hình biệt lập, mà phản ánh một xu thế lập pháp đã được nhiều quốc gia, tổ chức quốc tế vận dụng trong quản trị dữ liệu, an ninh mạng những năm gần đây: thay vì áp đặt một bộ quy tắc đồng nhất cho mọi

loại dữ liệu, pháp luật phân hóa nghĩa vụ tuân thủ theo đúng mức độ rủi ro thực tế mà việc xử lý dữ liệu đó có thể gây ra cho xã hội. Dưới góc độ lý luận pháp luật, đây là sự vận dụng nguyên tắc tương xứng (proportionality) - một nguyên tắc nền tảng của khoa học pháp lý hiện đại, theo đó mức độ can thiệp của công cụ quản lý nhà nước phải tương xứng với mức độ rủi ro cần kiểm soát. Việc lựa chọn nguyên tắc này giúp tránh hai thái cực đều không mong muốn: một mặt là buông lỏng quản lý trước rủi ro an ninh dữ liệu ngày càng tinh vi, mặt khác là áp đặt một cơ chế kiểm soát đồng loạt, gây lãng phí nguồn lực giám sát của Nhà nước và tạo gánh nặng tuân thủ không cần thiết cho những chủ thể chỉ xử lý dữ liệu có mức độ rủi ro thấp.

3.1. Về phạm vi điều chỉnh, nguyên tắc áp dụng pháp luật và ranh giới với các luật chuyên ngành có liên quan. Dự thảo phân định: nguyên tắc, điều kiện xử lý dữ liệu cá nhân, quyền của chủ thể dữ liệu cá nhân tiếp tục thực hiện theo pháp luật về bảo vệ dữ liệu cá nhân; hoạt động xây dựng, quản trị, khai thác, chia sẻ, phân loại dữ liệu theo tính chất quan trọng thực hiện theo pháp luật về dữ liệu; bảo vệ an ninh mạng đối với hệ thống thông tin thực hiện theo pháp luật về an ninh mạng, còn việc bảo vệ an ninh của chính dữ liệu, xuyên suốt vòng đời, thực hiện theo Luật An ninh dữ liệu. Cách phân định này giúp tránh tình trạng một tổ chức, doanh nghiệp phải thực hiện nhiều thủ tục trùng lặp cho cùng một nội dung quản lý; dự thảo còn quy định nguyên tắc một đối tượng, một nội dung rủi ro chỉ được đánh giá, thẩm định, kiểm tra một lần.

3.2. Về cơ chế quản lý theo cấp độ rủi ro. Dự thảo Luật quy định 05 cấp độ rủi ro an ninh dữ liệu, từ Cấp độ 1 (thấp nhất) đến Cấp độ 5 (cao nhất), xác định dựa trên khả năng xảy ra sự cố và mức độ thiệt hại có thể gây ra đối với quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội và quyền, lợi ích hợp pháp của tổ chức, cá nhân. Dữ liệu ở cấp độ càng cao, nghĩa vụ bảo vệ càng chặt chẽ: dữ liệu Cấp độ 1, Cấp độ 2 gần như không phát sinh thủ tục hành chính; từ Cấp độ 3 trở lên, chủ quản dữ liệu phải thực hiện đánh giá tác động, kiểm toán định kỳ; dữ liệu Cấp độ 4, Cấp độ 5 phải được thẩm định an ninh dữ liệu trước khi hệ thống được đưa vào vận hành chính thức. Việc phân cấp độ rủi ro, theo quy định của dự thảo, không thay thế việc phân loại dữ liệu theo pháp luật về dữ liệu và không làm thay đổi quyền sở hữu, quyền quản lý, khai thác, sử dụng dữ liệu của tổ chức, cá nhân, bảo đảm công cụ quản lý an ninh không ảnh hưởng đến quyền tài sản hợp pháp đối với dữ liệu.

3.3. Về bảo vệ an ninh dữ liệu theo vòng đời và chuyển dữ liệu xuyên biên giới. Dự thảo Luật xác lập định hướng bảo vệ an ninh dữ liệu xuyên suốt toàn bộ vòng đời - từ khâu thu thập, lưu trữ, xử lý, truyền đưa cho đến khi tiêu hủy - đồng thời kiểm soát chặt chẽ, có phân hóa theo cấp độ rủi ro đối với việc chuyển dữ liệu xuyên biên giới nhằm bảo vệ chủ quyền dữ liệu quốc gia. Theo định hướng chung, mức độ yêu cầu bảo vệ và kiểm soát tăng dần theo cấp độ rủi ro của dữ liệu; phần lớn dữ liệu có mức độ rủi ro thấp được tạo điều kiện lưu

thông thuận lợi, hạn chế tối đa phát sinh thủ tục hành chính, trong khi dữ liệu có mức độ rủi ro cao được quản lý chặt chẽ hơn tương xứng. Dự thảo cũng bổ sung cơ chế bảo vệ tổ chức, cá nhân trong nước trước yêu cầu cung cấp dữ liệu trực tiếp từ nước ngoài không thông qua kênh hợp pháp, phù hợp với nguyên tắc tôn trọng chủ quyền, an ninh quốc gia và thông lệ quốc tế về tương trợ tư pháp.

3.4. Về phòng ngừa, theo dõi và ứng phó sự cố an ninh dữ liệu. Dự thảo Luật xác lập định hướng chủ động phòng ngừa, theo dõi và ứng phó khi xảy ra sự cố an ninh dữ liệu, bảo đảm Nhà nước có công cụ phản ứng kịp thời đối với sự cố nghiêm trọng, đồng thời giới hạn chặt chẽ phạm vi, điều kiện áp dụng để không ảnh hưởng đến quyền, lợi ích hợp pháp của tổ chức, cá nhân. Theo định hướng chung, biện pháp mang tính hạn chế quyền chỉ được áp dụng khi có căn cứ rõ ràng, theo nguyên tắc ưu tiên biện pháp ít hạn chế nhất, có thời hạn áp dụng cụ thể, có cơ chế báo cáo, giám sát và bảo đảm quyền kiến nghị, khiếu nại, khởi kiện, được bồi thường của tổ chức, cá nhân trong trường hợp biện pháp được áp dụng trái pháp luật.

3.5. Về bảo vệ an ninh dữ liệu đối với công nghệ mới và trí tuệ nhân tạo. Dự thảo Luật xác lập định hướng bảo vệ an ninh dữ liệu đối với công nghệ mới và trí tuệ nhân tạo, gắn với xu thế phát triển công nghệ hiện nay. Tổ chức, cá nhân nghiên cứu, phát triển, triển khai công nghệ mới, hệ thống trí tuệ nhân tạo xử lý dữ liệu có mức độ rủi ro cao có trách nhiệm tích hợp biện pháp bảo vệ an ninh ngay từ khâu thiết kế, bảo đảm nguồn gốc hợp pháp và tính nguyên vẹn của dữ liệu được sử dụng. Đồng thời, dự thảo quy định rõ định hướng không chồng chéo thủ tục: việc đánh giá an ninh dữ liệu đối với hệ thống trí tuệ nhân tạo được tích hợp trong quy trình đánh giá rủi ro theo pháp luật về trí tuệ nhân tạo, không lập hồ sơ riêng, không tổ chức thẩm định riêng; cơ quan có thẩm quyền không được yêu cầu bàn giao mã nguồn, trọng số mô hình, trừ trường hợp phục vụ điều tra vụ án hình sự - qua đó vừa quản lý được rủi ro, vừa bảo vệ bí mật kinh doanh, bí mật công nghệ của doanh nghiệp.

3.6. Về trách nhiệm kiểm soát an ninh dữ liệu trong chuỗi cung ứng. Dự thảo Luật xác lập định hướng trách nhiệm kiểm soát an ninh dữ liệu trong toàn bộ chuỗi cung ứng sản phẩm, dịch vụ dữ liệu, không chỉ dừng lại trong phạm vi nội bộ một tổ chức. Chủ quản dữ liệu có trách nhiệm đánh giá rủi ro, giới hạn phạm vi tiếp cận dữ liệu đối với bên cung cấp sản phẩm, dịch vụ trước khi kết nối; quy định rõ nghĩa vụ bảo mật, chế tài xử lý khi để rò rỉ dữ liệu ngay trong hợp đồng; chủ động giám sát và thu hồi quyền tiếp cận khi phát hiện nguy cơ, sự cố. Đối với hệ thống xử lý dữ liệu có mức độ rủi ro cao, định hướng chung là kiểm soát chặt chẽ hơn việc tiếp cận từ xa của bên cung cấp. Đây là định hướng đặt trách nhiệm quản lý rủi ro xuyên suốt cả các khâu trung gian, bên thứ ba tham gia xử lý dữ liệu, vốn là một trong những điểm yếu phổ biến hiện nay trong thực tiễn bảo đảm an ninh dữ liệu.

3.7. Về chính sách phát triển hạ tầng, công nghệ và nguồn nhân lực. Dự thảo Luật quy định chính sách của Nhà nước nhằm thúc đẩy phát triển hạ tầng, công nghệ và nguồn nhân lực về an ninh dữ liệu, gắn kết chặt chẽ với mục tiêu an ninh. Nhà nước có chính sách ưu tiên phát triển điện toán đám mây chủ quyền, hạ tầng dữ liệu, trung tâm dữ liệu an toàn, xanh, có khả năng chống chịu, phục hồi; áp dụng chính sách ưu đãi về đầu tư, thuế đối với hoạt động nghiên cứu, phát triển công nghệ bảo vệ an ninh dữ liệu, mật mã an ninh, mật mã kháng lượng tử; hỗ trợ doanh nghiệp nhỏ và vừa, doanh nghiệp khởi nghiệp sáng tạo nâng cao năng lực bảo vệ an ninh dữ liệu bằng công cụ tự đánh giá, hướng dẫn, đào tạo và dịch vụ dùng chung. Đồng thời, dự thảo quy định nguyên tắc không được áp dụng biện pháp tạo vị trí độc quyền cho một sản phẩm, một nhà cung cấp cụ thể, bảo đảm môi trường cạnh tranh bình đẳng trong quá trình hình thành hệ sinh thái công nghiệp an ninh dữ liệu trong nước.

Những nội dung cốt lõi nêu trên cho thấy dự thảo Luật An ninh dữ liệu được thiết kế theo hướng vừa bảo đảm chặt chẽ về an ninh, chủ quyền dữ liệu quốc gia, vừa hạn chế tối đa tác động đến hoạt động sản xuất, kinh doanh hợp pháp của tổ chức, cá nhân, doanh nghiệp, tạo nền tảng pháp lý để phát triển kinh tế dữ liệu, kinh tế số trong giai đoạn tới.