FRASERS
LAW COMPANY
Established 1994

Dự thảo Luật An ninh Dữ liệu của Việt Nam

Cập Nhật Pháp Lý | Tháng 9 2026

Bộ Công an đã xây dựng dự thảo Luật An ninh dữ liệu (***Dự thảo Luật***), thiết lập một khuôn khổ mới về bảo vệ dữ liệu xuyên suốt vòng đời dữ liệu. Dự thảo Luật dự kiến được trình Quốc hội xem xét vào tháng 10 năm 2026 và có hiệu lực từ ngày 1 tháng 12 năm 2027. Dự thảo Luật vẫn có thể được sửa đổi trong quá trình xây dựng và trước khi được thông qua.

Việt Nam hiện đã có các quy định pháp luật điều chỉnh dữ liệu, bảo vệ dữ liệu cá nhân và an ninh mạng. Tuy nhiên, theo Bộ Công an, khuôn khổ pháp luật hiện hành chưa điều chỉnh một cách toàn diện việc bảo đảm an ninh đối với chính thực thể dữ liệu, từ khi dữ liệu được khởi tạo, lưu trữ đến khi được sử dụng, truyền đưa và tiêu hủy, dù dữ liệu đang nằm yên hay đang lưu chuyển. Dự thảo Luật nhằm khắc phục khoảng trống này thông qua việc thiết lập cơ chế quản lý dựa trên rủi ro, tập trung bảo đảm tính bảo mật, toàn vẹn, sẵn sàng, xác thực và khả năng chống chịu của dữ liệu.

Dự thảo Luật không chỉ điều chỉnh dữ liệu cá nhân mà còn áp dụng đối với dữ liệu nói chung, đồng thời đặt ra nhiều yêu cầu mới về tổ chức, kỹ thuật, báo cáo và chấp thuận. Dưới đây là một số nội dung có tác động đáng chú ý nhất đối với doanh nghiệp.

1. Phạm vi điều chỉnh dữ liệu

Dự thảo Luật áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài tại 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. Phạm vi này bao quát cả các chủ thể ở nước ngoài có tham gia hoặc liên quan đến hoạt động xử lý dữ liệu tại Việt Nam và do đó có thể bao gồm các nhà cung cấp dịch vụ điện toán đám mây, nhà cung cấp công nghệ và bên xử lý dữ liệu ở nước ngoài không có hiện diện tại Việt Nam.

Việc xử lý dữ liệu cá nhân tiếp tục được thực hiện theo pháp luật về bảo vệ dữ liệu cá nhân. Tuy nhiên, đối với các nội dung về an ninh, kỹ thuật và công nghệ đối với dữ liệu cá nhân chưa được quy định cụ thể tại pháp luật về bảo vệ dữ liệu cá nhân, Dự thảo Luật sẽ được áp dụng. Tương tự, việc bảo vệ an ninh không gian mạng tiếp tục được thực hiện theo pháp luật về an ninh mạng, trong khi Dự thảo Luật điều chỉnh chính thực thể dữ liệu xuyên suốt vòng đời dữ liệu. Do đó, doanh nghiệp có thể phải đồng thời tuân thủ Luật Dữ liệu số 60/2024/QH15 (***Luật Dữ liệu***), Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 (***Luật Bảo vệ dữ liệu cá nhân***), Luật An ninh mạng số 116/2025/QH15 (***Luật An ninh mạng***) và Dự thảo Luật.

Tuy nhiên, Dự thảo Luật cũng quy định các biện pháp bảo đảm an ninh dữ liệu phải bảo đảm tính tương xứng, phù hợp, không gây cản trở quá mức đối với hoạt động sản xuất, kinh doanh hợp pháp, đồng thời không được lợi dụng lý do an ninh để cản trở trái phép dòng chảy dữ liệu hợp pháp. Cách tiếp cận dự kiến là quản lý theo mức độ rủi ro thay vì áp dụng đồng loạt. Tuy nhiên, hiệu quả thực tế của các nguyên tắc này sẽ phụ thuộc vào các văn bản hướng dẫn quy định về phân loại dữ liệu, ngưỡng định lượng và các thủ tục chấp thuận.

2. Phân loại dữ liệu

Dự thảo Luật phân loại dữ liệu theo bốn cấp độ rủi ro, gồm Dữ liệu Thông thường (Cấp độ 1), Dữ liệu Nội bộ (Cấp độ 2), Dữ liệu Quan trọng (Cấp độ 3) và Dữ liệu Cốt lõi (Cấp độ 4). Dữ liệu Quan trọng và Dữ liệu Cốt lõi có tiêu chí tương thích với các khái niệm tương ứng tại Luật Dữ liệu, trong khi Dữ liệu Thông thường và Dữ liệu Nội bộ là hai nhóm phân loại bổ sung. Cụ thể:

(i) Dữ liệu Thông thường (Cấp độ 1) là dữ liệu mở hoặc dữ liệu hoạt động dân sự, thương mại thông thường; nếu bị xâm phạm chỉ gây rủi ro thấp đối với quyền và lợi ích hợp pháp của tổ chức, cá nhân.

(ii) Dữ liệu Nội bộ (Cấp độ 2) là dữ liệu phục vụ hoạt động quản lý, vận hành nội bộ của cơ quan, tổ chức, doanh nghiệp hoặc bí mật kinh doanh; nếu bị rò rỉ sẽ gây tổn thất cho hoạt động bình thường của tổ chức hoặc môi trường cạnh tranh.

(iii) Dữ liệu Quan trọng (Cấp độ 3) là dữ liệu có tiêu chí tương thích hoàn toàn với khái niệm "dữ liệu Quan trọng" tại Luật Dữ liệu, thuộc các ngành, lĩnh vực trọng điểm mà nếu bị rò rỉ, chiếm đoạt hoặc định hướng sai lệch sẽ gây nguy hại nghiêm trọng đến an ninh quốc gia, an ninh kinh tế vĩ mô hoặc lợi ích công cộng.

(iv) Dữ liệu Cốt lõi (Cấp độ 4) là dữ liệu có tiêu chí tương thích hoàn toàn với khái niệm "dữ liệu Cốt lõi" tại Luật Dữ liệu, liên quan trực tiếp đến quốc phòng, an ninh quốc gia, chủ quyền số và lợi ích chiến lược tối cao; nếu bị xâm phạm sẽ gây nguy hại đối với đất nước.

Việc phân loại dữ liệu theo cấp độ rủi ro không mang tính cố định. Dữ liệu ban đầu thuộc cấp độ thấp hơn có thể phải áp dụng cấp độ bảo vệ cao hơn nếu tích tụ đạt ngưỡng quy mô nhất định và làm thay đổi bản chất rủi ro tác động. Cơ quan, tổ chức vận hành hệ thống thông tin lưu trữ, xử lý dữ liệu phải thiết lập hệ thống công nghệ tự động để giám sát, phát hiện và cảnh báo khi tổng quy mô tích tụ dữ liệu đạt hoặc vượt ngưỡng quy định. Khi ngưỡng này bị vượt, chủ quản hệ thống thông tin phải nâng cấp ngay các biện pháp bảo vệ tương ứng và, đối với Dữ liệu Quan trọng và Dữ liệu Cốt lõi, khai báo biến động quy mô dữ liệu về hệ thống giám sát an ninh dữ liệu tập trung quốc gia thuộc Bộ Công an. Chính phủ sẽ quy định chi tiết các ngưỡng định lượng và thời gian khai báo.

Hệ thống phân loại này nhằm tập trung nguồn lực quản lý và kỹ thuật vào các dữ liệu có mức độ rủi ro cao hơn, thay vì áp dụng đồng loạt các yêu cầu đối với mọi loại dữ liệu theo cách có thể gây cản trở không cần thiết đối với các hoạt động kinh tế, xã hội thông thường. Do đó, việc xây dựng các ngưỡng định lượng rõ ràng sẽ có ý nghĩa quan trọng để doanh nghiệp có thể triển khai hiệu quả cơ chế phân loại và giám sát tự động theo Dự thảo Luật.

3. Nghĩa vụ quản trị dữ liệu

Chủ quản dữ liệu phải thực hiện kiểm kê dữ liệu thường xuyên, trong đó xác định, trong số các nội dung khác, loại dữ liệu, chủ sở hữu, vị trí lưu trữ, nơi xử lý và mức độ quan trọng của dữ liệu. Dữ liệu Quan trọng và Dữ liệu Cốt lõi còn phải được lập bản đồ dữ liệu, thể hiện vị trí và luồng dữ liệu, điểm truy cập, điểm kết nối, các hệ thống liên quan và sự phụ thuộc vào bên thứ ba.

Đánh giá tác động an ninh dữ liệu phải được thực hiện trước khi triển khai hệ thống dữ liệu mới, xử lý dữ liệu trọng yếu, thay đổi kiến trúc hệ thống, chuyển dữ liệu ra ngoài phạm vi quản lý hoặc sử dụng công nghệ mới có nguy cơ ảnh hưởng đến an ninh dữ liệu. Chủ quản hệ thống thông tin xử lý Dữ liệu Quan trọng hoặc Dữ liệu Cốt lõi còn phải tự tổ chức đánh giá rủi ro an ninh dữ liệu định kỳ hằng năm và báo cáo Bộ Công an.

Doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ và vừa không thuộc danh mục xử lý dữ liệu quy mô lớn hoặc không xử lý Dữ liệu Quan trọng, Dữ liệu Cốt lõi được miễn trừ các nghĩa vụ bảo vệ vòng đời dữ liệu. Tuy nhiên, quy định này không được thể hiện là miễn trừ chung đối với các nghĩa vụ khác theo Dự thảo Luật.

Doanh nghiệp cũng phải chịu trách nhiệm kiểm soát và bảo đảm an ninh dữ liệu trong suốt chuỗi cung ứng đối với các bên thứ ba, bao gồm nhà cung cấp dịch vụ điện toán đám mây, nhà cung cấp dịch vụ trí tuệ nhân tạo, đơn vị vận hành trung tâm dữ liệu, bên môi giới dữ liệu và bên nhận thuê ngoài xử lý dữ liệu. Trước khi thiết lập quan hệ hợp tác và định kỳ hằng năm trong quá trình vận hành, doanh nghiệp phải đánh giá năng lực kỹ thuật và biện pháp bảo vệ dữ liệu của bên thứ ba, các nguy cơ và lỗ hổng bảo mật có thể phát sinh, cũng như các biện pháp giảm thiểu rủi ro và phương án ứng phó sự cố an ninh dữ liệu. Việc chia sẻ, chuyển giao hoặc cho phép bên thứ ba tiếp cận dữ liệu chỉ được thực hiện sau khi các bên ký kết Hợp đồng an ninh dữ liệu hoặc có điều khoản thỏa thuận bảo mật dữ liệu bắt buộc trong hợp đồng dịch vụ chính thức. Hợp đồng phải quy định nghĩa vụ thông báo ngay lập

tức, trong thời hạn không quá 24 giờ, khi xảy ra hoặc có nguy cơ xảy ra sự cố rò rỉ dữ liệu. Doanh nghiệp đồng thời có quyền và nghĩa vụ thực hiện kiểm toán định kỳ hoặc đột xuất đối với hệ thống an ninh dữ liệu của bên thứ ba, hoặc yêu cầu bên thứ ba cung cấp báo cáo kiểm toán độc lập hợp pháp.

4. Yêu cầu tăng cường đối với Dữ liệu Quan trọng và Dữ liệu Cốt lõi

Dự thảo Luật áp dụng các yêu cầu ngày càng nghiêm ngặt tương ứng với cấp độ dữ liệu. Đối với Dữ liệu Quan trọng:

(i) Dữ liệu Quan trọng phải được lưu trữ, xử lý trong các hệ thống thông tin đáp ứng tiêu chuẩn tối thiểu từ cấp độ 3 trở lên;

(ii) cơ quan, tổ chức xử lý Dữ liệu Quan trọng hoặc dữ liệu ở cấp độ cao hơn phải thiết lập hệ thống quản trị rủi ro, chỉ định nhân sự phụ trách an ninh dữ liệu và bố trí bộ phận chuyên trách bảo vệ an ninh dữ liệu;

(iii) chủ quản Dữ liệu Quan trọng phải lưu vết và bảo vệ an toàn nhật ký hệ thống trong thời gian tối thiểu sáu tháng; và

(iv) hệ thống thông tin chứa Dữ liệu Quan trọng phải áp dụng xác thực đa yếu tố, cơ chế phân quyền truy cập tối thiểu và mã hóa dữ liệu trong cả trạng thái lưu trữ và truyền dẫn.

Bộ Công an có thể thực hiện giám sát từ xa và yêu cầu tạm dừng hoạt động xử lý dữ liệu để khắc phục sự cố khi phát hiện nguy cơ rò rỉ hoặc mất an ninh dữ liệu nghiêm trọng.

Đối với Dữ liệu Cốt lõi, dữ liệu về nguyên tắc phải được lưu trữ, xử lý trong hệ thống thông tin cấp độ 4 hoặc cấp độ 5. Dữ liệu Cốt lõi liên quan đến an ninh, quốc phòng hoặc hạ tầng trọng yếu phải áp dụng các biện pháp cách ly vật lý hoặc phân vùng an ninh đặc biệt với mạng Internet công cộng và không được chuyển ra nước ngoài, trừ trường hợp đặc biệt phục vụ lợi ích tối cao của quốc gia do Thủ tướng Chính phủ quyết định bằng văn bản.

Hệ thống thông tin dự kiến lưu trữ, xử lý Dữ liệu Quan trọng hoặc Dữ liệu Cốt lõi, cũng như các dự án đầu tư và chuyển giao công nghệ có cấu phần xử lý các loại dữ liệu này, phải được Bộ Công an thẩm định về điều kiện bảo đảm an ninh dữ liệu trước khi đưa vào vận hành hoặc phê duyệt. Văn bản thẩm định là căn cứ bắt buộc trong hồ sơ quyết định đầu tư hoặc chuyển giao công nghệ liên quan.

Cơ quan, tổ chức sử dụng chuyên gia, đối tác nước ngoài tham gia các dự án dữ liệu Cấp độ 3 hoặc Cấp độ 4 còn phải thực hiện thẩm tra an ninh nhân sự, ký thỏa thuận bảo mật và áp dụng giải pháp kỹ thuật cách ly độc lập khi các chuyên gia hoặc đối tác này truy cập hệ thống. Tổ chức, cá nhân nước ngoài vi phạm pháp luật về an ninh dữ liệu của Việt Nam có thể bị tước quyền truy cập hệ thống hoặc trục xuất khỏi lãnh thổ Việt Nam. Đây là một yêu cầu mới có ý nghĩa thực tiễn đối với các tập đoàn đa quốc gia phụ thuộc vào nhân sự kỹ thuật ở nước ngoài hoặc nhân sự di chuyển nội bộ.

Đối với hệ thống thông tin đồng thời thuộc đối tượng phải thẩm định, phê duyệt cấp độ an ninh hệ thống thông tin theo pháp luật về an ninh mạng, việc thẩm định an ninh dữ liệu được thực hiện đồng thời và tích hợp trong cùng một hồ sơ, một quy trình thẩm định do Bộ Công an chủ trì, để ban hành một văn bản chấp thuận duy nhất.

5. Quản trị thuật toán và hệ thống trí tuệ nhân tạo

Dự thảo Luật đặt ra các nghĩa vụ cụ thể đối với tổ chức, doanh nghiệp nghiên cứu, phát triển, vận hành và cung cấp dịch vụ trí tuệ nhân tạo tại Việt Nam, đặc biệt là hệ thống trí tuệ nhân tạo tạo sinh. Các tổ chức, doanh nghiệp này phải thiết lập quy trình kiểm chứng và làm sạch dữ liệu đào tạo, bảo đảm nguồn gốc dữ liệu hợp pháp và không vi phạm quyền sở hữu trí tuệ; tích hợp giải pháp gắn nhãn kỹ thuật số đối

với nội dung do trí tuệ nhân tạo tạo ra; và xây dựng bộ lọc kỹ thuật chủ động ngăn chặn nội dung thông tin sai lệch, gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

Bộ Công an có thẩm quyền yêu cầu tổ chức, doanh nghiệp cung cấp dịch vụ trí tuệ nhân tạo giải trình về tính minh bạch của thuật toán và nguồn dữ liệu đào tạo khi phát hiện hệ thống đưa ra thông tin sai lệch về chủ quyền, lịch sử, biên giới, văn hóa hoặc chính trị của Việt Nam. Doanh nghiệp vận hành nền tảng trí tuệ nhân tạo phải thiết lập kênh tiếp nhận báo cáo vi phạm hoạt động liên tục và thực hiện ngăn chặn thông tin sai lệch xâm phạm trực diện an ninh quốc gia ngay khi có yêu cầu khẩn cấp của Bộ Công an. Trường hợp hệ thống trí tuệ nhân tạo vi phạm nghiêm trọng quy định pháp luật gây hậu quả đặc biệt lớn, Bộ Công an có thể quyết định tạm ngừng cung cấp dịch vụ hoặc áp dụng các biện pháp ngăn chặn kỹ thuật đối với hệ thống đó.

Các quy định này đặt ra một tầng nghĩa vụ tuân thủ mới và đáng kể đối với doanh nghiệp công nghệ và trí tuệ nhân tạo hoạt động tại Việt Nam, mở rộng từ các nghĩa vụ thuần túy về dữ liệu sang tính minh bạch của thuật toán và quản trị nội dung.

6. Chuyển dữ liệu xuyên biên giới

Việc chuyển Dữ liệu Quan trọng và Dữ liệu Cốt lõi xuyên biên giới hiện đã được điều chỉnh theo Luật Dữ liệu và các văn bản hướng dẫn thi hành, bao gồm yêu cầu thực hiện đánh giá tác động đối với việc chuyển, xử lý dữ liệu xuyên biên giới. Dự thảo Luật bổ sung các biện pháp kiểm soát về an ninh dữ liệu đối với một số trường hợp chuyển dữ liệu ra nước ngoài.

Theo Dự thảo Luật, việc chuyển Dữ liệu Quan trọng hoặc Dữ liệu Cốt lõi ra nước ngoài phải được Bộ Công an thẩm định và cấp văn bản chấp thuận về an ninh trước khi thực hiện. Việc chuyển dữ liệu nhìn chung bị nghiêm cấm nếu dữ liệu có tác động trực tiếp, tức thời đến quốc phòng, an ninh, an toàn xã hội, tài chính - ngân hàng, năng lượng, viễn thông hoặc điều hành khẩn cấp, trừ những trường hợp đặc biệt phục vụ lợi ích tối cao của quốc gia được Chính phủ cho phép.

Đối với dữ liệu là bí mật kinh doanh của doanh nghiệp, việc chuyển ra nước ngoài không phải thẩm định trước nếu đáp ứng một trong các điều kiện sau:

(i) quốc gia, vùng lãnh thổ tiếp nhận được Bộ Công an công nhận có hệ thống pháp luật bảo vệ dữ liệu ở mức độ tương đương;

(ii) các bên ký kết Hợp đồng tiêu chuẩn về bảo vệ dữ liệu theo mẫu do Bộ Công an ban hành; hoặc

(iii) chủ thể chuyển giao đã được cấp Chứng nhận hợp quy về an ninh dữ liệu xuyên biên giới.

Tuy nhiên, tổ chức chuyển dữ liệu ra nước ngoài vẫn phải tự lập hồ sơ đánh giá tác động an ninh dữ liệu, báo cáo định kỳ hằng năm về Bộ Công an và chịu sự hậu kiểm. Bộ Công an có quyền đình chỉ luồng truyền dữ liệu ra nước ngoài nếu phát hiện vi phạm cam kết bảo mật.

7. Lưu trữ dữ liệu tại Việt Nam

Pháp luật về an ninh mạng hiện đã có yêu cầu lưu trữ dữ liệu tại Việt Nam đối với một số doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet hoặc dịch vụ gia tăng trên không gian mạng có hoạt động thu thập, khai thác, phân tích hoặc xử lý một số loại dữ liệu của người sử dụng tại Việt Nam. Dự thảo Luật thiết lập một cơ chế lưu trữ dữ liệu riêng, dựa trên cấp độ phân loại và ý nghĩa chiến lược của dữ liệu.

Cụ thể, Dữ liệu Cốt lõi và Dữ liệu Quan trọng có ý nghĩa chiến lược quốc gia, tác động trực tiếp, tức thời đến quốc phòng, an ninh, an toàn xã hội, tài chính - ngân hàng, năng lượng, viễn thông hoặc điều hành khẩn cấp bắt buộc phải được lưu trữ tại

trung tâm dữ liệu đặt trên lãnh thổ Việt Nam. Trường hợp lưu trữ trên hệ thống điện toán đám mây quốc tế, chủ quản dữ liệu phải duy trì liên tục bản sao lưu cập nhật theo thời gian thực tại Việt Nam và bảo đảm quyền kiểm soát tối cao thuộc về cơ quan nhà nước có thẩm quyền của Việt Nam. Đối với nhóm Dữ liệu Quan trọng khác, áp dụng cơ chế sao lưu đồng bộ theo chu kỳ, sao lưu định kỳ hoặc cơ chế khôi phục phù hợp với mức độ rủi ro.

Việc một lượng đáng kể dữ liệu của Việt Nam được lưu trữ tại các trung tâm dữ liệu ngoài lãnh thổ, cùng với sự phụ thuộc vào các tiêu chuẩn mật mã nước ngoài, được cho là gây khó khăn cho cơ quan có thẩm quyền của Việt Nam trong việc điều tra và truy xuất dữ liệu. Yêu cầu lưu trữ dữ liệu trong nước nhằm tránh việc Việt Nam mất khả năng tiếp cận các dữ liệu có ý nghĩa chiến lược trong trường hợp các dữ liệu này phụ thuộc hoàn toàn vào hạ tầng nước ngoài, kể cả khi xảy ra gián đoạn do yếu tố địa chính trị.

Hệ thống giám sát tập trung được đề cập xuyên suốt Dự thảo Luật là Hệ thống giám sát an ninh dữ liệu tập trung quốc gia, đặt tại Trung tâm Quản trị an ninh dữ liệu quốc gia thuộc Bộ Công an. Trung tâm này được xác định là hạ tầng chỉ huy, giám sát tối cao để bảo vệ các hạ tầng dữ liệu trọng yếu của quốc gia. Chủ quản hệ thống thông tin xử lý Dữ liệu Cốt lõi phải truyền nhật ký an ninh qua thiết bị một chiều, trong khi chủ quản Dữ liệu Quan trọng phải kết nối kỹ thuật và chia sẻ thông tin cảnh báo an ninh theo quy chuẩn kỹ thuật. Hoạt động giám sát phải bảo đảm bí mật nghiệp vụ; việc can thiệp hoặc trích xuất nội dung dữ liệu cụ thể chỉ được thực hiện trong trường hợp khẩn cấp về an ninh quốc gia hoặc phục vụ điều tra hình sự theo quy định của pháp luật.

8. Báo cáo sự cố và chế tài

Dự thảo Luật đặt ra các thời hạn báo cáo sự cố an ninh dữ liệu nghiêm ngặt. Đối với Dữ liệu Cốt lõi, sự cố phải được đánh giá và báo cáo trong vòng 02 giờ kể từ khi phát hiện. Đối với các dữ liệu khác, phải thông báo ban đầu trong thời hạn 24 giờ kể từ khi phát hiện sự cố. Báo cáo đầy đủ về phạm vi, nguyên nhân và biện pháp khắc phục phải được thực hiện trong thời hạn 72 giờ kể từ khi phát hiện sự cố, sau đó là báo cáo tổng kết, đánh giá sau xử lý trong thời hạn 30 ngày kể từ khi sự cố được khắc phục. Chủ thể dữ liệu bị ảnh hưởng cũng phải được thông báo khi sự cố xâm phạm đến quyền, lợi ích hợp pháp của họ. Tuy nhiên, trên thực tế, thời hạn báo cáo 02 giờ có thể là một yêu cầu khó đáp ứng.

Các hành vi vi phạm đặc biệt nghiêm trọng liên quan đến Dữ liệu Quan trọng hoặc Dữ liệu Cốt lõi có thể bị phạt tiền tối đa không quá 5% tổng doanh thu của tổ chức vi phạm tại Việt Nam trong năm tài chính liền kề trước đó. Đối với tổ chức là thành viên của tập đoàn đa quốc gia mà doanh thu tại Việt Nam không tương xứng với quy mô, mức độ nghiêm trọng của hành vi vi phạm, mức phạt có thể được xem xét tính trên cơ sở doanh thu toàn cầu của tập đoàn trong năm tài chính liền kề trước đó nhưng không vượt quá 5% doanh thu toàn cầu đó. Tổ chức, cá nhân vi phạm còn có thể bị truy cứu trách nhiệm hình sự tùy theo tính chất, mức độ vi phạm; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

Dự thảo Luật cũng hướng tới việc bảo đảm an ninh dữ liệu trong dài hạn trước sự phát triển của công nghệ mật mã. Dữ liệu Cốt lõi, Dữ liệu Quan trọng có ý nghĩa chiến lược quốc gia và dữ liệu chứa bí mật nhà nước phải được áp dụng các biện pháp bảo mật dài hạn, có khả năng phòng vệ trước sự phát triển của điện toán lượng tử và các công nghệ mới. Chủ quản hệ thống thông tin liên quan phải đánh giá định kỳ độ sẵn sàng kháng công nghệ và thực hiện lộ trình chuyển đổi sang mật mã kháng lượng tử theo hướng dẫn của cơ quan nhà nước có thẩm quyền. Theo quy định chuyển tiếp, kể từ ngày 1 tháng 1 năm 2035, toàn bộ hệ thống thông tin lưu trữ, xử lý Dữ liệu Cốt lõi và Dữ liệu Quan trọng thuộc hệ thống cơ quan Đảng, Nhà nước, lực lượng vũ trang và các lĩnh vực tài chính - ngân hàng, năng lượng, viễn thông và giáo dục phải hoàn thành lộ trình kiểm đếm, di cư dữ liệu và dịch chuyển

hoàn toàn sang sử dụng giải pháp mật mã kháng lượng tử đã được cấp chứng nhận hợp quy. Điều này đặt ra một mốc chuyển đổi công nghệ dài hạn cụ thể mà các doanh nghiệp có liên quan, đặc biệt trong các lĩnh vực được điều chỉnh, cần tính đến trong kế hoạch của mình.

9. Kinh doanh, giao dịch dữ liệu, bảo hiểm và các biện pháp khẩn cấp

Dự thảo Luật xác định hoạt động kinh doanh dịch vụ xử lý, phân tích, môi giới, lưu trữ và tiêu hủy dữ liệu là ngành, nghề đầu tư kinh doanh có điều kiện về an ninh, trật tự và yêu cầu doanh nghiệp hoạt động trong lĩnh vực này đáp ứng các tiêu chuẩn an ninh theo quy định. Việc mua bán Dữ liệu Cốt lõi hoặc Dữ liệu Quan trọng có tác động trực tiếp, tức thời đến quốc phòng, an ninh, an toàn xã hội, tài chính - ngân hàng, năng lượng, viễn thông hoặc điều hành khẩn cấp bị nghiêm cấm, trừ những trường hợp đặc biệt được Chính phủ cho phép. Tổ chức, cá nhân hoạt động môi giới hoặc cung cấp sàn dữ liệu phải đăng ký hoạt động, xác minh nguồn gốc hợp pháp của dữ liệu và lưu trữ đầy đủ lịch sử giao dịch để phục vụ thanh tra, kiểm tra. Nhà nước công nhận, bảo hộ quyền sở hữu, khai thác tài sản dữ liệu hợp pháp của cơ quan, tổ chức, cá nhân và nghiêm cấm các hành vi chiếm đoạt dữ liệu, bí mật thương mại hoặc tấn công phá hoại hạ tầng dữ liệu của doanh nghiệp.

Doanh nghiệp là chủ quản dữ liệu được khuyến khích, nhưng không bắt buộc, mua bảo hiểm rủi ro an ninh dữ liệu tùy theo cấp độ dữ liệu đang lưu trữ, xử lý để chủ động giảm thiểu tổn thất tài chính khi xảy ra sự cố. Chính phủ sẽ quy định chi tiết hạn mức, điều kiện, loại hình bảo hiểm và chính sách ưu đãi thuế có liên quan.

Trong tình huống khẩn cấp đe dọa trực tiếp chủ quyền dữ liệu hoặc an ninh quốc gia, Bộ Công an hoặc Bộ Quốc phòng, trong phạm vi thẩm quyền, có quyền ban hành lệnh điều phối đặc biệt và áp dụng biện pháp kỹ thuật khẩn cấp đối với doanh nghiệp cung cấp hạ tầng, dịch vụ mạng có liên quan, bao gồm việc trưng dụng hạ tầng, tài sản và nhân lực theo quy định của pháp luật về trưng mua, trưng dụng tài sản. Đây là những quyền can thiệp đáng kể của Nhà nước mà các doanh nghiệp cung cấp hạ tầng số trọng yếu cần tính đến trong quá trình đánh giá rủi ro.

Dự thảo Luật nhằm khắc phục các khoảng trống trong khuôn khổ pháp luật hiện hành về dữ liệu tại Việt Nam, bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân và hình thành môi trường số an toàn, tin cậy hơn. Cơ chế được thiết kế theo hướng quản lý dựa trên rủi ro, lấy người dân và doanh nghiệp làm trung tâm và hạn chế tối đa việc phát sinh thêm thủ tục hành chính. Tuy nhiên, việc các mục tiêu này có đạt được trên thực tế hay không sẽ phụ thuộc đáng kể vào các văn bản quy định chi tiết và hướng dẫn thi hành. Do đó, việc xây dựng một cơ chế thực thi đồng bộ, phối hợp và tương xứng sẽ có ý nghĩa quan trọng để Dự thảo Luật có thể củng cố niềm tin đối với nền kinh tế số của Việt Nam mà không tạo ra gánh nặng không cần thiết đối với các hoạt động kinh doanh hợp pháp.

FRASERS
LAW COMPANY
Established 1994

Tác giả

Dương Thị Mai Hương
Luật Sư Thành Viên
huong.duong@frasersvn.com

Bùi Thọ Kiên
Luật Sư
kien.bui@frasersvn.com

Văn phòng TP. Hồ Chí Minh

Số 19.01, tầng 19, Tòa nhà Đức
33 Lê Duẩn, Phường Sài Gòn
Thành phố Hồ Chí Minh
Điện thoại: +84 28 3824 2733

Văn phòng Hà Nội

Số 1503, tầng 15, Tòa nhà Pacific Place
83B Lý Thường Kiệt, Phường Cửa Nam
Hà Nội, Việt Nam
Điện thoại: +84 24 3946 1203

Website www.frasersvn.com
Email legalenquiries@frasersvn.com