QUỐC HỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Luật số: /QH16	*Hà Nội, ngày tháng năm 2026*

DỰ THẢO

LUẬT
AN NINH DỮ LIỆU

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam;
Quốc hội ban hành Luật An ninh dữ liệu.

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Luật này quy định về nguyên tắc, chính sách, biện pháp bảo đảm an ninh dữ liệu toàn diện và xuyên suốt vòng đời dữ liệu; thiết lập hệ thống bảo đảm an ninh dữ liệu quốc gia theo cấp độ rủi ro tác động; quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an ninh dữ liệu; quản lý chuyển giao dữ liệu xuyên biên giới; phát triển nguồn nhân lực, công nghệ và hợp tác quốc tế về an ninh dữ liệu.

2. Việc xử lý dữ liệu cá nhân thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân. Nội dung về an ninh, kỹ thuật, công nghệ đối với dữ liệu cá nhân chưa được quy định cụ thể tại pháp luật về bảo vệ dữ liệu cá nhân thì áp dụng theo quy định của Luật này.

3. Việc bảo vệ an ninh không gian mạng thực hiện theo quy định của pháp luật về an ninh mạng. Luật này điều chỉnh đối với thực thể dữ liệu xuyên suốt vòng đời dữ liệu, không phụ thuộc vào phương thức hoặc phương tiện lưu trữ vật lý, logic.

4. Trường hợp Điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên có quy định khác với quy định của Luật này thì áp dụng quy định của Điều ước quốc tế đó, trừ các nội dung liên quan trực tiếp đến quốc phòng, an ninh quốc gia và dữ liệu Cốt lõi.

Điều 2. Đối tượng áp dụng

Luật này 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.

Điều 3. Giải thích từ ngữ

Trong Luật này, các từ ngữ dưới đây được hiểu như sau:

1. An ninh dữ liệu là trạng thái bảo đảm tính bảo mật, tính nguyên vẹn, tính khả dụng của dữ liệu và khả năng chủ động phòng ngừa, phát hiện, ngăn chặn, ứng phó với các nguy cơ xâm phạm dữ liệu.

2. Bảo đảm an ninh dữ liệu là việc áp dụng tổng thể các biện pháp quản lý, kỹ thuật và pháp lý nhằm thiết lập, duy trì trạng thái an ninh dữ liệu; kiểm soát rủi ro và ngăn chặn hành vi xâm phạm an ninh dữ liệu.

3. Vòng đời dữ liệu là toàn bộ các giai đoạn tác động vật lý hoặc logic lên dữ liệu, bắt đầu từ khi thu thập, tạo lập, lưu trữ, sử dụng, chia sẻ, truyền đưa cho đến khi xóa bỏ, tiêu hủy vĩnh viễn.

4. Phân loại dữ liệu theo cấp độ rủi ro là việc căn cứ vào tính chất, quy mô tích tụ và mức độ tác động, hậu quả thực tế đối với quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội để phân định các cấp độ quản lý và áp dụng biện pháp bảo vệ tương ứng.

5. 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.

6. 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.

7. 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 số 60/2024/QH15, 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.

8. 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 số 60/2024/QH15, 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.

9. Chủ quyền dữ liệu quốc gia là quyền lực tối cao, độc lập và toàn vẹn của Nhà nước Việt Nam trong việc quản lý, kiểm soát, bảo vệ dữ liệu được phát sinh trên lãnh thổ Việt Nam hoặc liên quan đến lợi ích hợp pháp của quốc gia Việt Nam. (Việc Nhà nước thực hiện chủ quyền dữ liệu quốc gia theo khoản 9 Điều này không đồng nghĩa với việc Nhà nước sở hữu toàn bộ dữ liệu phát sinh trên lãnh thổ Việt Nam. Đối với dữ liệu do tổ chức, cá nhân hợp pháp tạo lập, thu thập bằng nguồn lực của mình phục vụ hoạt động sản xuất, kinh doanh, tiêu dùng, quyền sở hữu, quyền khai thác được Nhà nước công nhận, bảo hộ theo quy định của pháp luật về dân sự, sở hữu trí tuệ; Nhà nước chỉ thực hiện quyền quản lý, kiểm soát về an ninh đối với loại dữ liệu này trong phạm vi cần thiết để phòng ngừa, ngăn chặn hành vi vi phạm pháp luật hoặc ứng phó sự cố an ninh dữ liệu nghiêm trọng).

10. Dữ liệu, chủ quản dữ liệu, bên kiểm soát dữ liệu, bên xử lý dữ liệu, chủ thể dữ liệu được hiểu theo quy định của pháp luật về bảo vệ dữ liệu cá nhân và pháp luật về dữ liệu.

11. Hợp tác quốc tế về an ninh dữ liệu là các hoạt động đối ngoại, ký kết và thực thi điều ước quốc tế, thỏa thuận quốc tế nhằm tương thích tiêu chuẩn kỹ thuật, phối hợp điều tra tội phạm mạng và ứng cứu sự cố dữ liệu xuyên biên giới.

12. Sự cố an ninh dữ liệu là tình trạng tính bảo mật, tính nguyên vẹn hoặc tính khả dụng của dữ liệu bị xâm phạm, gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội hoặc quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

13. Hạ tầng dữ liệu quốc gia trọng yếu là hệ thống thông tin, trung tâm dữ liệu hoặc cơ sở lưu trữ dữ liệu có ý nghĩa chiến lược phục vụ vận hành Chính phủ số, kinh tế số, xã hội số, quốc phòng, an ninh quốc gia, tài chính, tiền tệ, giao thông vận tải quốc gia mà sự cố đối với hạ tầng này sẽ làm tê liệt hoạt động của một hoặc nhiều lĩnh vực thiết yếu của đời sống xã hội.

14. Tập dữ liệu đào tạo cho hệ thống trí tuệ nhân tạo là tập hợp thông tin, dữ liệu được cấu trúc hóa dùng để nạp vào mô hình trí tuệ nhân tạo và hệ thống thuật toán tự động nhằm tối ưu hóa, định hình tư duy logic và khả năng nhận thức của hệ thống.

15. Danh mục dữ liệu quốc gia bao gồm dữ liệu của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội và dữ liệu của tổ chức, cá nhân khác có ý nghĩa chiến lược phục vụ phát triển kinh tế - xã hội, quản lý nhà nước và bảo đảm quốc phòng, an ninh. Danh mục dữ liệu quốc gia là căn cứ pháp lý thống nhất để đối chiếu, đồng nhất, bổ sung và làm rõ các tiêu chí xác định danh mục Dữ liệu Quan trọng (Cấp độ 3) và Dữ liệu Cốt lõi (Cấp độ 4) quy định tại Điều 6 Luật này.

16. Trung tâm Quản trị an ninh dữ liệu quốc gia là hạ tầng chỉ huy, giám sát tối cao trực thuộc Bộ Công an để bảo vệ các hạ tầng dữ liệu trọng yếu của quốc gia, thực hiện chức năng giám sát theo thời gian thực, điều phối quốc gia về ứng cứu sự cố và quản trị rủi ro dữ liệu.

Điều 4. Nguyên tắc bảo đảm an ninh dữ liệu

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm sự quản lý thống nhất của Nhà nước; bảo vệ chủ quyền số và lợi ích quốc gia.

2. Bảo đảm an ninh dữ liệu theo phân loại cấp độ rủi ro tác động; cấp độ rủi ro càng cao thì yêu cầu quản lý và kỹ thuật càng nghiêm ngặt.

3. Gắn kết chặt chẽ giữa bảo đảm an ninh dữ liệu với phát triển kinh tế số, xã hội số; không lợi dụng lý do an ninh để cản trở trái phép dòng chảy dữ liệu hợp pháp và các cam kết quốc tế về thương mại số mà Việt Nam là thành viên.

4. Bảo đảm trách nhiệm giải trình của chủ thể xử lý dữ liệu; tôn trọng quyền con người, quyền công dân và quyền riêng tư theo Hiến pháp.

5. Kết hợp phát huy nội lực với tăng cường hợp tác quốc tế; tham chiếu, áp dụng có chọn lọc các tiêu chuẩn, thông lệ quốc tế tiên tiến.

6. Áp dụng các giải pháp an ninh dữ liệu ngay từ giai đoạn thiết kế và theo mặc định hệ thống xuyên suốt vòng đời dữ liệu.

7. Bảo đảm tính tương thích, hài hòa với các điều ước quốc tế có liên quan mà Việt Nam là thành viên trên nguyên tắc bảo vệ tối đa lợi ích quốc gia, dân tộc.

Điều 5. Chính sách của Nhà nước về an ninh dữ liệu

1. Hoàn thiện thể chế quản lý tài nguyên dữ liệu và xác lập chủ quyền dữ liệu quốc gia. Chính phủ cụ thể hóa chính sách của Nhà nước về an ninh dữ liệu trong từng thời kỳ.

2. Bảo đảm an ninh dữ liệu theo cấp độ rủi ro và xuyên suốt vòng đời dữ liệu. Xây dựng và phát triển hệ sinh thái dữ liệu an toàn, tin cậy, có khả năng chống chịu cao.

3. Bảo đảm an ninh trong lưu trữ và chuyển giao dữ liệu xuyên biên giới.

4. Bảo đảm an ninh dữ liệu trong nghiên cứu, phát triển, ứng dụng trí tuệ nhân tạo và công nghệ mới.

5. Bảo đảm an ninh dữ liệu trong phát triển kinh tế dữ liệu, đổi mới sáng tạo và tự chủ công nghệ.

6. Đa dạng hóa các nguồn lực tài chính, thực hiện xã hội hóa, thu hút dòng vốn đầu tư trong và ngoài nước phục vụ phát triển hạ tầng công nghệ, nghiên cứu mật mã thế hệ mới; ưu tiên phát triển nguồn nhân lực chất lượng cao và thúc đẩy hợp tác quốc tế sâu rộng về an ninh dữ liệu.

Điều 6. Phân loại dữ liệu theo cấp độ rủi ro an ninh

1. Dữ liệu được phân loại theo 04 cấp độ rủi ro từ thấp đến cao căn cứ vào tính chất, quy mô tích tụ và mức độ tác động 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, bao gồm:

a) Dữ liệu Thông thường (Cấp độ 1);

b) Dữ liệu Nội bộ (Cấp độ 2);

c) Dữ liệu Quan trọng (Cấp độ 3);

d) Dữ liệu Cốt lõi (Cấp độ 4).

2. Dữ liệu thuộc cấp độ thấp hơn khi tích tụ đạt ngưỡng quy mô lớn, làm thay đổi bản chất rủi ro tác động thì được áp dụng cấp độ bảo vệ cao hơn tương ứng.

3. 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 giám sát, phát hiện và cảnh báo khi tổng quy mô tích tụ dữ liệu đạt hoặc vượt ngưỡng quy định tại Khoản 2 Điều này. Ngay khi hệ thống tự động phát ra cảnh báo ngưỡng tích tụ dữ liệu dịch chuyển sang cấp độ rủi ro cao hơn, chủ quản hệ thống thông tin có trách nhiệm:

a) Thực hiện nâng cấp tức thời các biện pháp bảo vệ kỹ thuật và quản lý tương ứng với cấp độ dữ liệu mới;

b) 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 sau khi hệ thống ghi nhận tín hiệu cảnh báo, đối với dữ liệu ở cấp độ Quan trọng và Cốt lõi.

4. Nghiêm cấm chuyển dữ liệu Cốt lõi hoặc 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, điều

hành khẩn cấp ra nước ngoài, trừ những trường hợp đặc biệt phục vụ lợi ích tối cao của quốc gia được Chính phủ cho phép.

5. Chính phủ quy định chi tiết tiêu chí, ngưỡng định lượng quy mô tích tụ dữ liệu, thời gian khai báo biến động quy mô dữ liệu và trình tự, thủ tục ban hành danh mục dữ liệu thuộc Cấp độ 3 và Cấp độ 4.

Điều 7. Các hành vi bị nghiêm cấm

1. Chiếm đoạt, phá hoại, mua bán, làm tiết lộ, rò rỉ, mất mát dữ liệu Cốt lõi, dữ liệu Quan trọng; lưu trữ, xử lý dữ liệu nhằm chống phá Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, xâm phạm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội.

2. Thực hiện gián điệp dữ liệu; cài đặt mã độc, phần mềm gián điệp nhằm thu thập dữ liệu trái phép; phá mã dữ liệu của cơ quan, tổ chức, cá nhân khi không được phép.

3. Chuyển giao, mua bán, lưu trữ, xử lý trái phép dữ liệu của tổ chức, công dân Việt Nam cho tổ chức, cá nhân nước ngoài; lợi dụng biện pháp an ninh dữ liệu để hạn chế cạnh tranh lành mạnh hoặc vi phạm các cam kết quốc tế về thương mại.

4. Che giấu, không thông báo hoặc báo cáo sai sự thật về sự cố an ninh dữ liệu; cản trở hoạt động thanh tra, kiểm tra, điều tra của cơ quan nhà nước có thẩm quyền.

Điều 8. Các biện pháp bảo đảm an ninh dữ liệu

1. Các biện pháp bảo đảm an ninh dữ liệu bao gồm:

a) Biện pháp quản lý và kỹ thuật theo cấp độ rủi ro;

b) Mã hóa dữ liệu bằng giải pháp mật mã cơ yếu, mật mã an ninh, mật mã dân sự, mật mã kháng lượng tử và các giải pháp mật mã khác;

c) Biện pháp giám sát, cảnh báo sớm và kiểm toán an ninh;

d) Biện pháp thẩm định an ninh hệ thống và đánh giá tác động;

đ) Biện pháp ứng phó, khắc phục sự cố;

e) Biện pháp kỹ thuật khẩn cấp;

g) Các biện pháp chế tài hành chính, dân sự, hình sự theo quy định của pháp luật.

2. Việc áp dụng 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 của tổ chức, cá nhân.

3. Chính phủ quy định chi tiết thẩm quyền, trình tự, thủ tục áp dụng các biện pháp quy định tại khoản 1 Điều này.

CHƯƠNG II.
HỆ THỐNG BẢO ĐẢM AN NINH THEO CẤP ĐỘ VÀ TRONG TOÀN BỘ VÒNG ĐỜI DỮ LIỆU

MỤC 1. HỆ THỐNG BẢO ĐẢM AN NINH DỮ LIỆU

Điều 9. Hệ thống bảo đảm an ninh dữ liệu

1. Hệ thống bảo đảm an ninh dữ liệu là tập hợp các chính sách, quy trình, biện pháp kỹ thuật, biện pháp quản lý và nguồn lực nhằm bảo đảm tính bí mật, tính toàn vẹn, tính sẵn sàng, tính xác thực và khả năng chống chịu của dữ liệu.

2. Cơ quan, tổ chức thuộc đối tượng áp dụng của Luật này có trách nhiệm thiết lập, duy trì và cải tiến hệ thống bảo đảm an ninh dữ liệu phù hợp với quy mô hoạt động, tính chất dữ liệu và mức độ rủi ro.

3. Hệ thống bảo đảm an ninh dữ liệu phải được rà soát, cập nhật định kỳ hoặc khi có thay đổi đáng kể về hệ thống, công nghệ, mô hình hoạt động hoặc mức độ rủi ro.

4. Việc xây dựng hệ thống bảo đảm an ninh dữ liệu phải tuân thủ các nguyên tắc sau đây:

a) Quản lý theo mức độ rủi ro.

b) Áp dụng biện pháp bảo vệ tương ứng với cấp độ an ninh dữ liệu.

c) Bảo đảm an ninh trong toàn bộ vòng đời của dữ liệu.

d) Kết hợp biện pháp quản lý, kỹ thuật và tổ chức.

đ) Bảo đảm khả năng giám sát, truy vết và kiểm tra.

e) Bảo đảm tính liên tục của hoạt động.

Điều 10. Đánh giá rủi ro định kỳ, đột xuất và chứng nhận hợp quy

1. Chủ quản hệ thống thông tin xử lý dữ liệu Cốt lõi, dữ liệu Quan trọng có trách nhiệm tự tổ chức đánh giá rủi ro an ninh dữ liệu định kỳ hằng năm và báo cáo Bộ Công an. Bộ Công an có thẩm quyền yêu cầu thực hiện đánh giá đột xuất khi phát hiện nguy cơ mất an ninh dữ liệu nghiêm trọng.

2. Sản phẩm, dịch vụ công nghệ thông tin chuyên dùng phục vụ bảo vệ, mã hóa, giám sát an ninh dữ liệu phải được chứng nhận hợp quy trước khi lưu thông trên thị trường.

3. Việc đánh giá rủi ro phải được thực hiện:

a) Định kỳ;

b) Trước khi đưa hệ thống dữ liệu mới vào vận hành;

c) Khi thay đổi đáng kể hệ thống;

d) Sau khi xảy ra sự cố nghiêm trọng;

đ) Theo yêu cầu của cơ quan có thẩm quyền.

4. Hồ sơ đánh giá rủi ro bao gồm: Danh mục dữ liệu; mức độ quan trọng của dữ liệu; danh mục nguy cơ; kết quả phân tích rủi ro; kế hoạch xử lý rủi ro; kết quả theo dõi và cập nhật.

5. Chính phủ quy định chi tiết tần suất đánh giá, nội dung báo cáo, điều kiện, trình tự cấp chứng nhận hợp quy đối với sản phẩm công nghệ an ninh dữ liệu.

6. Hồ sơ đánh giá rủi ro quy định tại Điều này được xây dựng trên cơ sở kết quả kiểm kê, lập bản đồ dữ liệu quy định tại Điều 11 và có thể được sử dụng làm một phần của hồ sơ đánh giá tác động an ninh dữ liệu quy định tại Điều 12 và Điều 15 đối với cùng một hệ thống

thông tin, không yêu cầu chủ quản dữ liệu phải lập nhiều bộ hồ sơ riêng biệt cho cùng một nội dung đánh giá.

Điều 11. Kiểm kê và lập bản đồ dữ liệu

1. Chủ quản dữ liệu phải thực hiện kiểm kê dữ liệu thường xuyên nhằm xác định:

a) Loại dữ liệu;

b) Vị trí lưu trữ;

c) Nơi xử lý;

d) Chủ sở hữu;

đ) Đơn vị quản lý;

e) Mức độ quan trọng.

2. Dữ liệu quan trọng, dữ liệu cốt lõi phải được lập bản đồ dữ liệu.

3. Bản đồ dữ liệu phải phản ánh: Vị trí dữ liệu; luồng dữ liệu; điểm truy cập; điểm kết nối; hệ thống liên quan; phụ thuộc vào bên thứ ba.

Điều 12. Đánh giá tác động an ninh dữ liệu

1. Đánh giá tác động an ninh dữ liệu là việc phân tích ảnh hưởng của hoạt động xử lý dữ liệu đối với an ninh quốc gia, lợi ích công cộng và an ninh của hệ thống dữ liệu.

2. Đánh giá tác động phải được thực hiện trước khi:

a) Triển khai hệ thống dữ liệu mới;

b) Xử lý dữ liệu trọng yếu;

c) Thay đổi kiến trúc hệ thống;

d) Chuyển dữ liệu ra ngoài phạm vi quản lý;

đ) Sử dụng công nghệ mới có nguy cơ ảnh hưởng đến an ninh dữ liệu.

3. Nội dung đánh giá tác động

a) Mô tả hoạt động xử lý.

b) Mục đích xử lý.

c) Dữ liệu bị tác động.

d) Nguy cơ đối với an ninh dữ liệu.

đ) Biện pháp giảm thiểu.

e) Kế hoạch giám sát.

MỤC 2. BẢO ĐẢM AN NINH TOÀN BỘ VÒNG ĐỜI DỮ LIỆU

Điều 13. Quản lý danh mục và trách nhiệm bảo đảm an ninh dữ liệu

1. Bộ Công an chủ trì, phối hợp với các Bộ, cơ quan ngang Bộ xây dựng, trình Thủ tướng Chính phủ ban hành và cập nhật Danh mục dữ liệu quốc gia nhằm bảo đảm an ninh dữ liệu.

2. Cơ quan, tổ chức, cá nhân có hoạt động xử lý dữ liệu thuộc Danh mục quy định tại khoản 1 Điều này có trách nhiệm kiểm kê, phân loại, khai báo danh mục và thực hiện các biện pháp bảo đảm an ninh dữ liệu trong toàn bộ vòng đời và tương ứng với cấp độ rủi ro.

3. Đối với các 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.

4. Chính phủ quy định chi tiết về tiêu chí, trình tự, thủ tục lập, thẩm định, ban hành, đăng ký và cập nhật Danh mục dữ liệu quốc gia; quy định nội dung quản trị rủi ro tối thiểu tương ứng với từng cấp độ dữ liệu và các nghĩa vụ bảo vệ vòng đời dữ liệu theo quy định tại khoản 2 Điều này.

Điều 14. Kiểm soát an ninh trong thu thập, khởi tạo và thiết kế hệ thống dữ liệu

1. Tổ chức, cá nhân khi phát triển, sản xuất, cung cấp hoặc sử dụng các hệ thống thông tin, thiết bị phần cứng, phần mềm, ứng dụng và công nghệ để thu thập, khởi tạo dữ liệu phải tích hợp các biện pháp an ninh, bảo mật ngay từ giai đoạn thiết kế, phát triển và trong suốt vòng đời sản phẩm.

2. Tổ chức, doanh nghiệp, cá nhân kinh doanh chỉ được phép thu thập đúng, đủ những trường thông tin thực sự cần thiết để thực hiện mục đích đã tuyên bố.

3. Nhân sự tham gia quản trị, vận hành, tiếp cận các hệ thống xử lý dữ liệu Cốt lõi phải được sàng lọc, đánh giá năng lực, cam kết bảo mật thông tin và chịu sự giám sát, phân quyền truy cập tối thiểu theo quy định.

4. Các thiết bị công nghệ, sản phẩm trí tuệ nhân tạo và chuỗi cung ứng công nghệ phục vụ việc thu thập dữ liệu từ cấp độ 3 trở lên phải được kiểm tra, chứng nhận hợp quy và đánh giá rủi ro an ninh mạng trước khi đưa vào vận hành.

5. Đối với hệ thống thông tin thuộc phạm vi điều chỉnh của Luật này và 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 quy định tại Điều này được thực hiện đồng thời, tích hợp trong cùng một hồ sơ, một quy trình thẩm định do Bộ Công an chủ trì, phối hợp với cơ quan có thẩm quyền theo pháp luật về an ninh mạng để ra văn bản chấp thuận duy nhất.

6. Chính phủ quy định chi tiết về tiêu chuẩn kỹ thuật an ninh theo thiết kế, nghĩa vụ quản lý lỗ hổng bảo mật của nhà sản xuất và quy trình kiểm soát nhân sự; kiểm soát an ninh chuỗi cung ứng công nghệ và quy trình đánh giá rủi ro an ninh đối với hệ thống, thiết bị thu thập dữ liệu tự động.

Điều 15. Bảo đảm an ninh trong lưu trữ, truyền dẫn và xử lý dữ liệu

1. Hoạt động lưu trữ dữ liệu từ cấp độ 3 tại các trung tâm dữ liệu hoặc thông qua dịch vụ của bên thứ ba phải đáp ứng các tiêu chuẩn kỹ thuật bắt buộc về an ninh vật lý, an ninh mạng, quản lý khóa mật mã và cơ chế sao lưu, phục hồi dữ liệu khẩn cấp.

2. Dữ liệu từ cấp độ 3 khi truyền dẫn phải được áp dụng các biện pháp mã hóa và xác thực. Luồng truyền dẫn dữ liệu dữ liệu Cốt lõi giữa các cơ quan nhà nước và hạ tầng thông tin quan trọng về an ninh quốc gia phải được thực hiện trên kênh truyền chuyên biệt, giám sát liên tục.

3. Hoạt động xử lý dữ liệu phải tuân thủ đúng mục đích được xác định. Bên kiểm soát và bên xử lý dữ liệu phải thực hiện đánh giá tác động bảo vệ dữ liệu khi tiến hành các hoạt động xử lý dữ liệu quy mô lớn, dữ liệu có nguy cơ cao ảnh hưởng đến an ninh quốc gia hoặc xử lý dữ liệu bằng trí tuệ nhân tạo.

4. Chính phủ quy định chi tiết Điều này.

Điều 16. Bảo đảm an ninh trong chia sẻ, cung cấp và giao dịch dữ liệu

1. Việc chia sẻ, cung cấp dữ liệu phải dựa trên cơ sở pháp lý, được đánh giá tác động an ninh trước khi thực hiện và áp dụng các biện pháp kỹ thuật bảo vệ dữ liệu thích hợp. Nghiêm cấm chia sẻ dữ liệu của cơ quan nhà nước cho tổ chức, cá nhân khác nếu có nguy cơ gây phương hại đến an ninh quốc gia.

2. Nghiêm cấm mọi hành vi mua bán dữ liệu Cốt lõi hoặc 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, điều hành khẩn cấp trừ những trường hợp đặc biệt được Chính phủ cho phép. Việc giao dịch, mua bán dữ liệu là hoạt động kinh doanh có điều kiện và phải được cơ quan nhà nước có thẩm quyền cấp phép.

3. Tổ chức, cá nhân hoạt động môi giới, cung cấp sàn dữ liệu phải đăng ký hoạt động, bảo đảm năng lực kỹ thuật, tiêu chuẩn an ninh, xác minh nguồn gốc hợp pháp của dữ liệu và lưu trữ đầy đủ lịch sử giao dịch trong thời gian quy định để phục vụ thanh tra, kiểm tra.

4. Chính phủ quy định chi tiết Điều này.

Điều 17. Bảo đảm an ninh trong tiêu hủy dữ liệu

1. Khi dữ liệu hết thời hạn lưu trữ theo quy định của pháp luật hoặc theo thỏa thuận, hoặc khi chủ thể dữ liệu yêu cầu xóa bỏ, chủ thể quản lý dữ liệu phải tiến hành tiêu hủy dữ liệu.

2. Dữ liệu từ cấp độ 3 khi hết thời hạn lưu trữ hoặc không còn mục đích xử lý hợp pháp phải được tiêu hủy triệt để bằng các biện pháp kỹ thuật chuyên dụng, bảo đảm không thể khôi phục lại dưới mọi hình thức.

3. Bên kiểm soát dữ liệu và bên xử lý dữ liệu có trách nhiệm thiết lập quy trình tiêu hủy dữ liệu chặt chẽ, lập và lưu trữ hồ sơ, chứng từ tiêu hủy để sẵn sàng cung cấp cho cơ quan chức năng khi có yêu cầu.

4. Tổ chức cung cấp dịch vụ tiêu hủy dữ liệu phải đáp ứng các điều kiện về năng lực hành nghề, tuân thủ tiêu chuẩn kỹ thuật, an ninh và chịu trách nhiệm pháp lý đối với mọi hành vi làm rò rỉ dữ liệu trong quá trình tiêu hủy.

5. Chính phủ quy định chi tiết tiêu chuẩn kỹ thuật, an ninh, phương pháp tiêu hủy dữ liệu an toàn và quy trình kiểm tra việc thực hiện tiêu hủy dữ liệu đối với từng loại hình lưu trữ dữ liệu.

MỤC 3. BẢO ĐẢM AN NINH THEO CẤP ĐỘ DỮ LIỆU

Điều 18. Bảo vệ dữ liệu Thông thường

1. Cơ quan, tổ chức, cá nhân xử lý dữ liệu Thông thường có trách nhiệm chủ động áp dụng biện pháp bảo mật theo tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an ninh mạng; bảo đảm tính sẵn sàng và ngăn chặn hành vi giả mạo, xuyên tạc dữ liệu.

2. Nhà nước khuyến khích tổ chức, doanh nghiệp áp dụng các tiêu chuẩn an ninh dữ liệu quốc tế tiên tiến nhằm nâng cao năng lực cạnh tranh và thực hiện liên thông dữ liệu xuyên biên giới theo Điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

3. Khi phát hiện sự cố mất an ninh hoặc rò rỉ dữ liệu Thông thường có nguy cơ ảnh hưởng đến quyền và lợi ích hợp pháp của các bên liên quan, chủ thể xử lý dữ liệu phải kịp thời thông báo cho người sử dụng và áp dụng ngay biện pháp kỹ thuật ngăn chặn, giảm thiểu thiệt hại.

4. Hoạt động xử lý dữ liệu Thông thường phải tuân thủ các nguyên tắc bảo đảm an ninh trong toàn bộ vòng đời dữ liệu quy định tại Mục 2 Chương này.

Điều 19. Bảo vệ dữ liệu Nội bộ

1. Yêu cầu về hạ tầng và lưu trữ:

a) Dữ liệu Nội bộ phải được lưu trữ, xử lý trong các hệ thống thông tin đáp ứng tiêu chuẩn theo quy định của pháp luật;

b) Chủ quản hệ thống thông tin chứa dữ liệu Nội bộ phải bảo đảm tính sẵn sàng cao của hệ thống; xây dựng phương án và hạ tầng dự phòng thảm họa, bảo đảm khả năng khôi phục dữ liệu khi xảy ra sự cố nghiêm trọng.

2. Chủ quản hệ thống thông tin chứa dữ liệu Nội bộ phải triển khai các giải pháp kỹ thuật chủ động ngăn chặn, giảm thiểu thiệt hại từ các cuộc tấn công mạng; thiết lập hàng rào kỹ thuật phòng, chống, quét kiểm tra và bóc gỡ mã độc định kỳ nhằm bảo đảm an ninh hệ thống và dữ liệu được lưu trữ.

3. Dữ liệu cá nhân và bí mật doanh nghiệp thuộc phân loại dữ liệu Nội bộ trong quá trình xử lý phải được hệ thống sao lưu tự động, định kỳ; chủ quản hệ thống có trách nhiệm kiểm tra tính toàn vẹn, tính bảo mật của các bản sao lưu tối thiểu một tuần một lần để sẵn sàng ứng phó với các kịch bản tấn công mã hóa dữ liệu tống tiền.

4. Bộ Công an có trách nhiệm giám sát, kiểm tra việc tuân thủ các biện pháp bảo vệ dữ liệu Nội bộ; xử lý nghiêm các hành vi buông lỏng quản lý gây mất mát, rò rỉ dữ liệu hoặc tự ý thu thập, mua bán, chuyển giao dữ liệu trái phép theo quy định của pháp luật.

5. Hoạt động xử lý dữ liệu Nội bộ phải tuân thủ các biện pháp bảo đảm an ninh trong toàn bộ vòng đời dữ liệu quy định tại Mục 2 Chương này.

Điều 20. Bảo vệ dữ liệu Quan trọng

1. Yêu cầu về tổ chức và hạ tầng:

a) 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 theo quy định của pháp luật;

b) Cơ quan, tổ chức xử lý dữ liệu từ Quan trọng 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.

2. Chủ quản dữ liệu Quan trọng phải thiết lập hệ thống quản trị rủi ro; thực hiện lưu vết và bảo vệ an toàn nhật ký hệ thống (log) tối thiểu là sáu tháng để phục vụ công tác điều tra, ứng cứu sự cố và truy vết hành vi xâm phạm an ninh quốc gia.

3. Chủ quản hệ thống thông tin chứa dữ liệu Quan trọng phải áp dụng các biện pháp xác thực đa yếu tố, cơ chế phân quyền truy cập tối thiểu, mã hóa dữ liệu trong cả trạng thái lưu trữ và truyền dẫn theo tiêu chuẩn, quy chuẩn kỹ thuật quốc gia.

4. Bộ Công an chủ trì, phối hợp với các Bộ, ngành quản lý chuyên ngành thực hiện giám sát từ xa, kiểm tra định kỳ hoặc đột xuất việc tuân thủ các quy định về bảo vệ dữ liệu Quan trọng; trường hợp phát hiện nguy cơ rò rỉ hoặc mất an ninh dữ liệu nghiêm trọng, Bộ Công an có quyền yêu cầu tạm dừng hoạt động xử lý dữ liệu để khắc phục sự cố.

5. Hoạt động xử lý dữ liệu Quan trọng phải tuân thủ các biện pháp bảo đảm an ninh trong toàn bộ vòng đời dữ liệu quy định tại Mục 2 Chương này.

6. Nhân sự phụ trách an ninh dữ liệu quy định tại điểm b khoản 1 Điều này phải được bảo đảm tính độc lập trong hoạt động chuyên môn, có quyền báo cáo trực tiếp cho người đứng đầu cơ quan, tổ chức và không bị xử lý bất lợi khi thực hiện đúng chức trách.

Điều 21. Bảo vệ dữ liệu Cốt lõi

1. Dữ liệu Cốt lõi phải được lưu trữ, xử lý trong hệ thống thông tin cấp độ 4, 5 theo quy định của pháp luật; Dữ liệu Cốt lõi liên quan đến an ninh, quốc phòng, hạ tầng trọng yếu được áp dụng các biện pháp cách ly vật lý hoặc phân vùng an ninh đặc biệt với mạng Internet công cộng, 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.

2. Bảo đảm an ninh mật mã và cơ chế kiểm soát truyền dẫn dữ liệu:

a) Hoạt động lưu trữ, truyền dẫn dữ liệu Cốt lõi phải áp dụng các giải pháp mã hóa chuyên biệt;

b) Hoạt động truyền dẫn thông tin nhật ký hệ thống và siêu dữ liệu kiểm toán từ hệ thống thông tin lưu trữ dữ liệu Cốt lõi về Hệ thống giám sát an ninh dữ liệu tập trung quốc gia phải áp dụng giải pháp kỹ thuật truyền dữ liệu một chiều vật lý, bảo đảm duy trì nguyên tắc cách ly vật lý. Nghiêm cấm thiết lập luồng truyền tín hiệu điều khiển hoặc dịch chuyển luồng dữ liệu trái phép từ không gian mạng công cộng vào phân vùng lưu trữ dữ liệu Cốt lõi.

3. Việc tiếp cận, trích xuất hoặc thao tác đối với dữ liệu Cốt lõi phải được phê duyệt trực tiếp bằng văn bản bởi người đứng đầu cơ quan chủ quản hệ thống thông tin và chịu sự giám sát, kiểm soát của lực lượng chuyên trách bảo đảm an ninh dữ liệu.

4. Bộ Công an chủ trì, phối hợp với các đơn vị chức năng thực hiện thanh tra, kiểm tra, giám sát định kỳ hoặc đột xuất việc tuân thủ quy chuẩn kỹ thuật mật mã, cấu hình an ninh hệ thống và kiểm soát nguy cơ di chuyển, phát tán hoặc rò rỉ dữ liệu Cốt lõi.

5. Hoạt động xử lý dữ liệu Cốt lõi phải tuân thủ các biện pháp bảo đảm an ninh trong toàn bộ vòng đời dữ liệu quy định tại Mục 2 Chương này.

CHƯƠNG III.
BẢO ĐẢM AN NINH DỮ LIỆU TRONG PHÁT TRIỂN KINH TẾ SỐ VÀ CHÍNH PHỦ SỐ

Điều 22. Bảo đảm an ninh dữ liệu đối với hạ tầng số và dịch vụ viễn thông, Internet

1. Doanh nghiệp cung cấp dịch vụ viễn thông, dịch vụ Internet (ISP), dịch vụ mạng lõi và doanh nghiệp cung cấp hạ tầng dữ liệu tại Việt Nam có trách nhiệm:

a) Áp dụng các biện pháp quản lý và giải pháp kỹ thuật tương xứng nhằm bảo đảm an ninh dữ liệu, tính toàn vẹn và tính sẵn sàng của luồng dữ liệu truyền dẫn phù hợp với cấp độ an ninh hệ thống thông tin quy định tại Luật này;

b) Triển khai hệ thống kỹ thuật tự động rà quét, phát hiện, ngăn chặn và khắc phục kịp thời các sự cố mất an ninh dữ liệu, tấn công mạng, rò rỉ dữ liệu xuyên biên giới trên hạ tầng do mình quản lý, vận hành;

c) Thiết lập cơ chế xác thực, quản lý định danh người dùng và lưu trữ đầy đủ nhật ký truyền dẫn dữ liệu mạng (IP log) trong thời gian quy định để phục vụ công tác điều tra, truy vết hành vi vi phạm pháp luật về an ninh dữ liệu của cơ quan có thẩm quyền;

d) Thực hiện ngăn chặn khẩn cấp, chặn lọc luồng truy cập hoặc bóc gỡ các tập dữ liệu độc hại, dữ liệu xâm phạm an ninh quốc gia ngay khi có yêu cầu bằng văn bản hoặc lệnh điều phối kỹ thuật của Bộ Công an

2. Doanh nghiệp nước ngoài cung cấp dịch vụ viễn thông, Internet xuyên biên giới có hoạt động xử lý dữ liệu của người dùng tại Việt Nam hoặc tác động đến an ninh dữ liệu quốc gia Việt Nam có nghĩa vụ:

a) Thực hiện lưu trữ dữ liệu và thành lập chi nhánh hoặc văn phòng đại diện tại Việt Nam theo quy định của Luật này và pháp luật có liên quan;

b) Thiết lập cổng kết nối kỹ thuật an ninh và tuân thủ các yêu cầu phối hợp, xử lý thông tin, dữ liệu độc hại tương tự như các doanh nghiệp quy định tại khoản 1 Điều này.

3. Biện pháp chế tài kỹ thuật đối với doanh nghiệp vi phạm: Doanh nghiệp cung cấp dịch vụ quy định tại khoản 1 và khoản 2 Điều này nếu vi phạm pháp luật về an ninh dữ liệu, không tuân thủ lệnh điều phối ứng phó khẩn cấp hoặc buông lỏng quản lý để xảy ra rò rỉ dữ liệu quy mô lớn, tùy theo tính chất và mức độ vi phạm sẽ bị áp dụng các biện pháp cưỡng chế kỹ thuật bao gồm:

a) Giới hạn hoặc điều tiết băng thông kết nối mạng;

b) Tạm ngừng hoặc đình chỉ có thời hạn quyền truy cập, lưu chuyển luồng dữ liệu liên quan trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam;

c) Đình chỉ hoạt động hoặc thu hồi giấy phép cung cấp dịch vụ viễn thông, Internet theo quy định của pháp luật.

4. Chính phủ quy định chi tiết thời gian lưu trữ nhật ký truyền dẫn dữ liệu mạng, tiêu chí phân loại, danh mục hạ tầng số, dịch vụ Internet phải áp dụng biện pháp giám sát đặc biệt; quy trình, thủ tục phối hợp kỹ thuật giữa cơ quan chuyên trách bảo đảm an ninh dữ liệu quốc gia với các doanh nghiệp và trình tự áp dụng các biện pháp cưỡng chế kỹ thuật quy định tại Điều này.

Điều 23. Thẩm định an ninh hệ thống, hoạt động đầu tư và chuyển giao công nghệ

1. Hệ thống thông tin dự kiến lưu trữ, xử lý dữ liệu Cốt lõi, dữ liệu Quan trọng và dự án đầu tư, 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 vận hành hoặc phê duyệt.

2. Bộ Công an chủ trì, phối hợp với các đơn vị liên quan thực hiện thẩm định; văn bản thẩm định là căn cứ bắt buộc trong hồ sơ quyết định đầu tư, chuyển giao công nghệ liên quan.

3. Cơ quan nhà nước có thẩm quyền thực hiện thẩm định theo Điều này có trách nhiệm bảo mật tuyệt đối thông tin kỹ thuật, mã nguồn, tài liệu bí mật kinh doanh do tổ chức, cá nhân cung cấp trong quá trình thẩm định; chỉ sử dụng cho mục đích thẩm định an ninh dữ liệu. Mọi hành vi làm lộ, mất, sử dụng sai mục đích thông tin quy định tại khoản này bị xử lý nghiêm theo quy định của pháp luật.

4. Chính phủ quy định chi tiết nội dung, trình tự, thủ tục, thời hạn thẩm định và ngưỡng quy mô dữ liệu phải áp dụng thẩm định tại Điều này.

Điều 24. Bảo đảm an ninh dữ liệu trong phát triển Chính phủ số và các lĩnh vực quốc gia trọng yếu

1. Dữ liệu phục vụ hoạt động của cơ quan nhà nước, cung cấp dịch vụ công trực tuyến (Chính phủ số) và dữ liệu vận hành các hạ tầng kỹ thuật thuộc các lĩnh vực quốc gia trọng yếu bao gồm: Tài chính - Ngân hàng, Năng lượng, Y tế, Giáo dục, Viễn thông, Giao thông vận tải bắt buộc phải được phân loại và áp dụng các biện pháp bảo vệ ở mức độ tối thiểu là dữ liệu Quan trọng hoặc dữ liệu Cốt lõi.

2. Mọi hệ thống thông tin phục vụ Chính phủ số và các lĩnh vực trọng yếu quy định tại khoản 1 Điều này, khi kết nối, liên thông bắt buộc phải tích hợp giải pháp kỹ thuật giám sát kết nối theo thời gian thực với hệ thống giám sát an ninh dữ liệu tập trung của Bộ Công an. Đối với dữ liệu quân sự, quốc phòng tham gia vào các hạ tầng trọng yếu liên ngành, việc giám sát do Bộ Quốc phòng chủ trì thực hiện theo quy định tại Điều 51 Luật này.

3. Chủ quản hệ thống thông tin thuộc lĩnh vực trọng yếu quy định tại khoản 1 Điều này có trách nhiệm:

a) Thực hiện kiểm toán cấu hình an ninh, rà quét lỗ hổng bảo mật tối thiểu 02 lần một năm;

b) Xây dựng phương án dự phòng thảm họa, bảo đảm năng lực khôi phục dữ liệu sạch sau khi xảy ra sự cố.

4. Chính phủ quy định chi tiết Điều này.

Điều 25. Bảo đảm an ninh dữ liệu dài hạn

1. Dữ liệu Cốt lõi, Quan trọng có ý nghĩa chiến lược quốc gia, 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.

2. Chủ quản hệ thống thông tin liên quan có trách nhiệm 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.

3. Nhà nước có chính sách khuyến khích, ưu đãi đối với tổ chức, cá nhân nghiên cứu, đầu tư, đào tạo nhân lực, ứng dụng thành công giải pháp mật mã kháng lượng tử và bảo vệ chuyên gia phát hiện lỗ hổng bảo mật nghiêm trọng.

4. Chính phủ quy định chi tiết danh mục dữ liệu, lộ trình, tiêu chuẩn, quy chuẩn kỹ thuật mật mã kháng lượng tử, quản lý việc áp dụng mật mã kháng lượng tử để đảm bảo an ninh dữ liệu và cơ chế ưu đãi quy định tại Điều này.

Điều 26. Quản trị thuật toán và hệ thống trí tuệ nhân tạo

1. Tổ chức, doanh nghiệp nghiên cứu, phát triển, vận hành và cung cấp dịch vụ trí tuệ nhân tạo, đặc biệt là hệ thống trí tuệ nhân tạo tạo sinh tại Việt Nam phải:

a) Thiết lập quy trình kiểm chứng và làm sạch dữ liệu đào tạo, bảo đảm nguồn gốc dữ liệu hợp pháp, không vi phạm quyền sở hữu trí tuệ;

b) Tích hợp giải pháp gắn nhãn kỹ thuật số nội dung do trí tuệ nhân tạo tạo ra;

c) Xây dựng bộ lọc kỹ thuật chủ động ngăn chặn nội dung thông tin sai lệch, gây phương hại an ninh quốc gia, trật tự, an toàn xã hội.

2. 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.

3. Doanh nghiệp vận hành nền tảng trí tuệ nhân tạo phải thiết lập kênh tiếp nhận báo cáo vi phạm hoạt động liên tục; 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.

4. 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 thẩm quyền quyết định tạm ngừng cung cấp dịch vụ hoặc áp dụng các biện pháp ngăn chặn kỹ thuật đối với hệ thống đó theo quy định.

Điều 27. Đảm bảo an ninh đối với cơ chế thử nghiệm có kiểm soát giải pháp công nghệ về an ninh dữ liệu

1. Chính phủ ban hành quy chế về cơ chế thử nghiệm có kiểm soát đối với các giải pháp công nghệ về an ninh dữ liệu mới, trí tuệ nhân tạo, chuỗi khối và dữ liệu lớn trong các lĩnh vực chiến lược.

2. Tổ chức, doanh nghiệp tham gia cơ chế thử nghiệm có kiểm soát được áp dụng trình tự đánh giá rút gọn nhưng vẫn phải bảo đảm các nguyên tắc an ninh dữ liệu cốt lõi quy định tại Luật này.

3. Chính phủ quy định chi tiết điều kiện, phạm vi, thời hạn thử nghiệm và trách nhiệm giám sát.

Điều 28. Bảo đảm chủ quyền, lưu trữ dữ liệu trong hoạt động kinh doanh, giao dịch dữ liệu

1. Dữ liệu Cốt lõi và 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, điều hành khẩn cấp bắt buộc phải được lưu trữ tại trung tâm dữ liệu đặt trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa 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.

2. Tổ chức vận hành sàn dữ liệu tại Việt Nam phải thiết lập hạ tầng kỹ thuật đáp ứng tiêu chuẩn an ninh, kiểm toán nguồn gốc pháp lý dữ liệu; hoạt động mua bán, chuyển giao dữ liệu cá nhân và dữ liệu Quan trọng phải được đăng ký để phục vụ công tác quản lý, giám sát.

3. Doanh nghiệp nước ngoài cung cấp dịch vụ viễn thông, Internet xuyên biên giới có hành vi vi phạm pháp luật về an ninh dữ liệu hoặc bảo vệ dữ liệu cá nhân của Việt Nam mà không khắc phục sau khi đã được cảnh báo bằng văn bản thì bị áp dụng biện pháp cưỡng chế thiết lập hạ tầng, lưu trữ dữ liệu tại Việt Nam.

4. Doanh nghiệp nước ngoài vi phạm quy định tại khoản 3 Điều này, tùy theo tính chất và mức độ vi phạm, bị áp dụng biện pháp kỹ thuật ngăn chặn gồm: giới hạn băng thông kết nối, tạm ngừng hoặc đình chỉ quyền truy cập luồng dữ liệu trên lãnh thổ Việt Nam.

6. Chính phủ quy định chi tiết Điều này.

Điều 29. Quản lý hoạt động kinh doanh dịch vụ dữ liệu và bảo hộ tài sản dữ liệu

1. Kinh doanh dịch vụ xử lý, phân tích, môi giới, lưu trữ, tiêu hủy dữ liệu là ngành, nghề đầu tư kinh doanh có điều kiện về an ninh, trật tự; doanh nghiệp hoạt động trong lĩnh vực này phải đáp ứng tiêu chuẩn an ninh theo quy định.

2. Nhà nước công nhận, bảo hộ quyền sở hữu, khai thác tài sản dữ liệu hợp pháp của cơ quan, tổ chức, cá nhân; nghiêm cấm các hành vi chiếm đoạt dữ liệu, bí mật thương mại và tấn công phá hoại hạ tầng dữ liệu của doanh nghiệp.

3. Chính phủ quy định chi tiết điều kiện cấp phép và cơ chế bảo hộ tài sản dữ liệu.

Điều 30. Bảo đảm an ninh dữ liệu trong chuỗi cung ứng

1. Tổ chức, cá nhân vận hành, xử lý dữ liệu có trách nhiệm kiểm soát và bảo đảm an ninh dữ liệu trong suốt chuỗi cung ứng đối với các bên thứ ba tham gia trực tiếp hoặc gián tiếp, bao gồm:

a) Nhà cung cấp dịch vụ điện toán đám mây;

b) Nhà cung cấp dịch vụ trí tuệ nhân tạo;

c) Đơn vị vận hành trung tâm dữ liệu;

d) Bên môi giới dữ liệu;

đ) Bên nhận thuê ngoài xử lý dữ liệu;

e) Các bên thứ ba khác có quyền tiếp cận, lưu trữ hoặc xử lý dữ liệu của tổ chức, cá nhân.

2. Trước khi thiết lập quan hệ hợp tác và định kỳ hằng năm trong quá trình vận hành, tổ chức, cá nhân phải tiến hành đánh giá rủi ro an ninh dữ liệu đối với bên thứ ba. Nội dung đánh giá phải thể hiện rõ:

a) Năng lực kỹ thuật và biện pháp bảo vệ dữ liệu của bên thứ ba;

b) Các nguy cơ, lỗ hổng bảo mật có thể phát sinh trong quá trình chuyển giao, lưu trữ và xử lý dữ liệu;

c) Biện pháp giảm thiểu rủi ro và phương án ứng phó sự cố an ninh dữ liệu.

3. 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 điều khoản thỏa thuận bảo mật dữ liệu bắt buộc trong hợp đồng dịch vụ chính thức). Hợp đồng phải quy định rõ:

a) Phạm vi, mục đích xử lý dữ liệu và giới hạn quyền truy cập của bên thứ ba;

b) Trách nhiệm kỹ thuật và tổ chức nhằm bảo vệ dữ liệu;

c) Nghĩa vụ thông báo ngay lập tức (không quá 24 giờ) khi xảy ra hoặc có nguy cơ xảy ra sự cố rò rỉ dữ liệu;

d) Trách nhiệm bồi thường thiệt hại và chế tài xử lý khi vi phạm cam kết an ninh dữ liệu.

4. Tổ chức, cá nhân 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 để chứng minh khả năng tuân thủ các tiêu chuẩn an ninh dữ liệu đã cam kết.

Điều 31. Tuyên truyền, phổ biến pháp luật về an ninh dữ liệu và kỹ năng ứng dụng trí tuệ nhân tạo

1. Nhà nước tổ chức tuyên truyền, phổ biến pháp luật về an ninh dữ liệu và kỹ năng ứng dụng trí tuệ nhân tạo. Doanh nghiệp cung cấp dịch vụ công nghệ, dịch vụ trí tuệ nhân tạo có trách nhiệm tích hợp các thông điệp cảnh báo an ninh dữ liệu ngắn gọn, trực quan ngay trên giao diện, tương tác của người dùng.

2. Nội dung tuyên truyền gồm:

a) Quyền và nghĩa vụ của tổ chức, cá nhân;

b) Nhận diện nguy cơ mất an ninh dữ liệu;

c) Biện pháp bảo vệ dữ liệu;

d) Trách nhiệm khi xảy ra sự cố.

3. Khuyến khích cơ quan, tổ chức, cá nhân tham gia hoạt động nâng cao nhận thức cộng đồng trong bảo đảm an ninh dữ liệu.

CHƯƠNG IV.
LƯU CHUYỂN DỮ LIỆU XUYÊN BIÊN GIỚI VÀ HỢP TÁC QUỐC TẾ

Điều 32. Bảo đảm an ninh trong hoạt động lưu chuyển dữ liệu xuyên biên giới

1. Hoạt động chuyển dữ liệu ra nước ngoài được thực hiện theo nguyên tắc phân luồng rủi ro, bảo đảm tối ưu hóa lợi ích kinh tế và không xâm phạm an ninh quốc gia, chủ quyền số của Việt Nam.

2. Việc chuyển dữ liệu Quan trọng hoặc Cốt lõi ra nước ngoài được Bộ Công an thẩm định, cấp văn bản chấp thuận về an ninh trước khi thực hiện. Đối với dữ liệu Quan trọng hoặc Cốt lõi có tác động trực tiếp, tức thời đến quốc phòng, an ninh, an toàn xã hội, tài chính - ngân hàng, năng lượng, viễn thông, điều hành khẩn cấp thì thực hiện theo quy định tại Khoản 4 Điều 6 Luật này.

3. 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:

a) 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;

b) Các bên ký kết Hợp đồng tiêu chuẩn về bảo vệ dữ liệu theo mẫu do Bộ Công an ban hành;

c) Chủ thể chuyển giao đã được cấp Chứng nhận hợp quy về an ninh dữ liệu xuyên biên giới theo quy định của Luật này.

4. Tổ chức chuyển dữ liệu ra nước ngoài theo quy định tại khoản 3 Điều này phải tự lập hồ sơ đánh giá tác động an ninh dữ liệu và báo cáo định kỳ hằng năm về Bộ Công an. Bộ Công an thực hiện hậu kiểm và có quyền đình chỉ luồng truyền dữ liệu ra nước ngoài nếu phát hiện vi phạm cam kết bảo mật.

5. Bộ Công an có trách nhiệm công bố công khai và cập nhật định kỳ danh mục quốc gia, vùng lãnh thổ được công nhận có hệ thống pháp luật bảo vệ dữ liệu tương đương quy định tại điểm a khoản 3 Điều này.

6. Chính phủ quy định chi tiết Điều này.

Điều 33. Tương trợ tư pháp và hợp tác quốc tế về an ninh dữ liệu

1. Hợp tác quốc tế, tương trợ tư pháp về an ninh dữ liệu thực hiện trên nguyên tắc tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với Hiến pháp, pháp luật Việt Nam và Điều ước quốc tế mà Việt Nam là thành viên.

2. Nội dung tương trợ tư pháp bao gồm phối hợp thu thập, chia sẻ chứng cứ điện tử; dẫn độ, chuyển giao người phạm tội; phong tỏa, thu hồi tài sản số; công nhận và cho thi hành phán quyết của tòa án nước ngoài trên cơ sở có đi có lại.

3. Bộ Công an là cơ quan đầu mối tham mưu Chính phủ đàm phán, ký kết Điều ước quốc tế về an ninh dữ liệu và phòng, chống tội phạm về dữ liệu.

4. Cơ quan nhà nước có thẩm quyền của Việt Nam có quyền từ chối yêu cầu tương trợ tư pháp hoặc chia sẻ chứng cứ điện tử từ phía nước ngoài nếu việc thực hiện yêu cầu đó gây phương hại đến chủ quyền, an ninh quốc gia, lợi ích chiến lược tối cao của Việt Nam hoặc không phù hợp với các nguyên tắc loại trừ được ghi nhận tại điều ước quốc tế về phòng, chống tội phạm mạng mà Việt Nam là thành viên.

Điều 34. Cơ chế phối hợp truy vết và ứng cứu sự cố an ninh dữ liệu toàn cầu

1. Bộ Công an là đầu mối quốc gia phối hợp với các tổ chức thực thi pháp luật quốc tế và doanh nghiệp công nghệ xuyên quốc gia để truy vết, ứng cứu sự cố an ninh dữ liệu xuyên biên giới.

2. Bộ Công an thiết lập nền tảng chia sẻ thông tin an ninh dữ liệu quốc gia; khuyến khích cơ quan, tổ chức, doanh nghiệp tham gia chia sẻ thông tin về mối đe dọa an ninh dữ liệu trên cơ sở tự nguyện, bảo đảm ẩn danh và miễn trừ trách nhiệm cho bên chia sẻ có thiện chí.

3. Chính phủ quy định chi tiết cơ chế vận hành nền tảng chia sẻ thông tin quy định tại Điều này.

CHƯƠNG V.
GIÁM SÁT, PHÒNG NGỪA VÀ ỨNG PHÓ SỰ CỐ AN NINH DỮ LIỆU

Điều 35. Giám sát an ninh dữ liệu tập trung và cảnh báo sớm rủi ro quốc gia

1. Bộ Công an xây dựng, quản lý và vận hành Hệ thống giám sát an ninh dữ liệu tập trung quốc gia đặt tại Trung tâm Quản trị an ninh dữ liệu quốc gia, thực hiện chức năng giám sát, phân tích, cảnh báo sớm và hỗ trợ ngăn chặn hành vi xâm phạm dữ liệu trái phép.

2. Chủ quản hệ thống thông tin xử lý dữ liệu Cốt lõi thực hiện truyền nhật ký an ninh qua thiết bị một chiều; chủ quản dữ liệu Quan trọng có trách nhiệm kết nối kỹ thuật, chia sẻ thông tin cảnh báo an ninh về Hệ thống giám sát tập trung quốc gia theo quy chuẩn kỹ thuật.

3. Hoạt động giám sát phải bảo đảm bí mật nghiệp vụ; nghiêm cấm lợi dụng chức năng giám sát để can thiệp trái phép vào hoạt động bình thường của hệ thống hoặc nội dung dữ liệu được giám sát. Việc can thiệp, 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.

4. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng và các cơ quan liên quan xây dựng, vận hành Hệ thống cảnh báo sớm rủi ro an ninh dữ liệu quốc gia. Bộ Quốc phòng chủ trì vận hành hệ thống cảnh báo sớm trong phạm vi quản lý quân sự, quốc phòng và chia sẻ thông tin nguy cơ với Bộ Công an.

5. Chủ quản hệ thống thông tin lưu trữ, xử lý dữ liệu Cốt lõi và dữ liệu Quan trọng khi nhận được cảnh báo từ Hệ thống cảnh báo sớm quốc gia phải triển khai ngay biện pháp cô lập, chặn lọc hệ thống và báo cáo kết quả khắc phục. Nghiêm cấm hành vi che giấu hoặc không thực hiện lệnh điều phối ứng phó khẩn cấp.

6. Chính phủ quy định chi tiết quy chuẩn kỹ thuật kết nối, truyền nhật ký và chia sẻ thông tin cảnh báo an ninh quy định tại khoản 2 và khoản 5 Điều này.

Điều 36. Biện pháp kỹ thuật khẩn cấp bảo đảm an ninh dữ liệu quốc gia

1. Tình huống khẩn cấp đe dọa trực tiếp chủ quyền dữ liệu, an ninh quốc gia, Bộ Công an, Bộ Quốc phòng trong phạm vi thẩm quyền có quyền ban hành lệnh điều phối đặc biệt, áp dụng biện pháp kỹ thuật khẩn cấp đối với doanh nghiệp cung cấp hạ tầng, dịch vụ mạng liên quan.

2. Việc trưng dụng hạ tầng, tài sản, nhân lực trong tình huống khẩn cấp thực hiện theo quy định của pháp luật về trưng mua, trưng dụng tài sản.

3. Chính phủ quy định chi tiết thẩm quyền, trình tự, thủ tục ban hành và bãi bỏ các biện pháp quy định tại Điều này.

Điều 37. Xây dựng phương án và kịch bản ứng phó sự cố an ninh dữ liệu

1. Sự cố an ninh dữ liệu được phân loại từ cấp độ cục bộ đến khẩn cấp quốc gia. Chủ quản hệ thống thông tin xử lý dữ liệu Nội bộ, dữ liệu Quan trọng và dữ liệu Cốt lõi có nghĩa vụ xây dựng phương án ứng phó sự cố và tổ chức diễn tập định kỳ hằng năm.

2. Bộ Công an, Bộ Quốc phòng chủ trì xây dựng kịch bản mẫu quốc gia, chỉ huy điều phối khi sự cố vượt quá khả năng kiểm soát của Bộ, ngành, địa phương.

3. Chính phủ quy định chi tiết tiêu chí phân loại cấp độ sự cố và quy trình điều phối khẩn cấp.

Điều 38. Trách nhiệm báo cáo, thông báo sự cố an ninh dữ liệu

1. Chủ quản dữ liệu có trách nhiệm báo cáo kịp thời sự cố an ninh dữ liệu cho Bộ Công an (hoặc Bộ Quốc phòng đối với dữ liệu quân sự) và thông báo cho chủ thể dữ liệu bị ảnh hưởng khi sự cố xâm phạm đến quyền, lợi ích hợp pháp của họ.

2. Nghiêm cấm hành vi che giấu, báo cáo sai sự thật hoặc cản trở hoạt động ứng cứu sự cố của cơ quan nhà nước có thẩm quyền.

3. Thời hạn báo cáo như sau:

a) Đối với dữ liệu Cốt lõi yêu cầu đánh giá, báo cáo sau khi phát hiện sự cố trong vòng 02 giờ;

b) Đối với dữ liệu khác, thông báo ban đầu cho Bộ Công an (hoặc Bộ Quốc phòng) trong thời hạn 24 giờ kể từ khi phát hiện sự cố;

c) Báo cáo đầy đủ về phạm vi, nguyên nhân, biện pháp khắc phục trong thời hạn 72 giờ kể từ khi phát hiện sự cố;

d) Báo cáo tổng kết, đánh giá sau xử lý trong thời hạn 30 ngày kể từ khi sự cố được khắc phục.

Điều 39. Điều phối quốc gia về ứng cứu sự cố an ninh dữ liệu

1. Trung tâm Quản trị an ninh dữ liệu quốc gia thuộc Bộ Công an là đầu mối chỉ huy, điều phối ứng cứu sự cố an ninh dữ liệu trên phạm vi toàn quốc.

2. Bộ Công an chủ trì thiết lập lực lượng phản ứng nhanh về dữ liệu quốc gia; Bộ Quốc phòng chủ trì ứng cứu sự cố thuộc phạm vi quân sự, quốc phòng.

3. Chính phủ quy định chi tiết cơ chế điều phối, trưng tập chuyên gia và trách nhiệm phối hợp quy định tại Điều này.

Điều 40. Truy vết và điều tra hành vi vi phạm về an ninh dữ liệu

1. Cơ quan chuyên trách thuộc Bộ Công an, Bộ Quốc phòng có quyền thu thập chứng cứ điện tử, trích xuất dữ liệu nhật ký hệ thống phục vụ công tác truy vết, điều tra hành vi vi phạm pháp luật về an ninh dữ liệu.

2. Doanh nghiệp viễn thông, công nghệ thông tin có nghĩa vụ bảo đảm tính toàn vẹn của nhật ký hệ thống và cung cấp thông tin kịp thời khi có yêu cầu bằng văn bản của cơ quan điều tra có thẩm quyền.

3. Chính phủ quy định chi tiết quy chuẩn kỹ thuật bảo quản chứng cứ điện tử quy định tại Điều này.

Điều 41. Phục hồi dữ liệu sau sự cố

1. Sau khi sự cố được khống chế, chủ quản dữ liệu có trách nhiệm khôi phục hệ thống bảo đảm đã loại bỏ hoàn toàn mã độc, khắc phục triệt để lỗ hổng bảo mật trước khi đưa hệ thống trở lại vận hành chính thức.

2. Đối với hệ thống thông tin của cơ quan nhà nước và hạ tầng trọng yếu, việc khôi phục kết nối phải có văn bản xác nhận đủ điều kiện an ninh của Bộ Công an hoặc Bộ Quốc phòng.

3. Nhà nước xem xét bố trí nguồn lực hỗ trợ khắc phục thảm họa đối với hệ thống bị thiệt hại đặc biệt nghiêm trọng thuộc nhóm dữ liệu Quan trọng, dữ liệu Cốt lõi.

Điều 42. Diễn tập bảo vệ an ninh dữ liệu

1. Bộ Công an, Bộ Quốc phòng chủ trì tổ chức diễn tập bảo đảm an ninh dữ liệu quốc gia đối với hạ tầng dữ liệu quốc gia trọng yếu trong phạm vi quản lý.

2. Kết quả diễn tập là căn cứ để đánh giá năng lực bảo đảm an ninh dữ liệu của cơ quan, tổ chức. Cá nhân tham gia diễn tập thực hiện đúng kịch bản được phê duyệt được miễn trừ trách nhiệm đối với sự cố kỹ thuật phát sinh trong quá trình diễn tập.

Điều 43. Bảo hiểm rủi ro an ninh dữ liệu

1. Doanh nghiệp là chủ quản dữ liệu được khuyến khích 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.

2. Chính phủ quy định chi tiết hạn mức, điều kiện, loại hình bảo hiểm và chính sách ưu đãi thuế liên quan quy định tại Điều này.

CHƯƠNG VI.
PHÁT TRIỂN NGUỒN NHÂN LỰC, CÔNG NGHỆ VÀ LỰC LƯỢNG AN NINH DỮ LIỆU

Điều 44. Lực lượng bảo vệ an ninh dữ liệu quốc gia

1. Lực lượng chuyên trách bảo vệ an ninh dữ liệu quốc gia bao gồm:

a) Lực lượng chuyên trách thuộc Bộ Công an (chủ trì, điều phối tổng thể);

b) Lực lượng chuyên trách thuộc Bộ Quốc phòng (chủ trì bảo vệ dữ liệu quân sự, quốc phòng);

c) Lực lượng bảo vệ an ninh dữ liệu được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin, cơ sở dữ liệu quan trọng về an ninh quốc gia;

d) Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh dữ liệu.

2. Nhà nước ưu tiên đầu tư xây dựng lực lượng chuyên trách tiến thẳng lên hiện đại; trang bị công nghệ tiên tiến phục vụ bảo vệ dữ liệu, chủ quyền quốc gia.

3. Chính phủ quy định chi tiết chức năng, nhiệm vụ, quyền hạn và cơ chế phối hợp của lực lượng chuyên trách.

Điều 45. Phát triển nguồn nhân lực và hệ thống chứng nhận chuyên môn an ninh dữ liệu

1. Nhà nước quy hoạch mạng lưới đào tạo nguồn nhân lực về an ninh dữ liệu, ban hành khung tiêu chuẩn năng lực quốc gia về an ninh dữ liệu tương thích với các tiêu chuẩn quốc tế.

2. Nhân sự vận hành trực tiếp hệ thống thông tin xử lý dữ liệu Quan trọng, dữ liệu Cốt lõi phải sở hữu chứng nhận chuyên môn về an ninh dữ liệu do cơ quan nhà nước có thẩm quyền cấp hoặc công nhận tương đương đối với các chứng chỉ quốc tế có uy tín.

3. Nhà nước áp dụng chính sách cấp học bổng, hỗ trợ đào tạo chuyên sâu đối với nhân lực an ninh dữ liệu chất lượng cao.

4. Chính phủ quy định chi tiết khung tiêu chuẩn năng lực dữ liệu quốc gia và điều kiện công nhận chứng chỉ quốc tế tương đương quy định tại khoản 1 và khoản 2 Điều này.

Điều 46. Chính sách thu hút và đãi ngộ tài năng về an ninh dữ liệu

1. Nhà nước áp dụng cơ chế đãi ngộ đặc biệt, thu hút, tuyển dụng đặc cách không qua thi tuyển đối với chuyên gia, nhà khoa học có thành tích xuất sắc về an ninh dữ liệu, bao gồm cả người Việt Nam định cư ở nước ngoài.

2. Nhà nước áp dụng hành lang pháp lý an toàn bảo vệ chuyên gia công nghệ độc lập thực hiện phát hiện, thông báo lỗi bảo mật theo đúng quy trình phối hợp công bố lỗ hổng có thiện chí.

3. Chính phủ quy định chi tiết cơ chế đãi ngộ, đặc thù, tuyển dụng đặc cách và hành lang pháp lý an ninh quy định tại khoản 1 và khoản 2 Điều này.

Điều 47. Quản lý hoạt động của tổ chức, cá nhân nước ngoài về dữ liệu tại Việt Nam

1. Cơ quan, tổ chức sử dụng chuyên gia, đối tác nước ngoài tham gia các dự án dữ liệu Cấp độ 3, Cấp độ 4 có trách nhiệm 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 họ truy cập hệ thống.

2. Tổ chức, cá nhân nước ngoài có hành vi vi phạm pháp luật về an ninh dữ liệu của Việt Nam thì bị xử lý nghiêm theo quy định của pháp luật, bao gồm tước quyền truy cập hệ thống hoặc trục xuất khỏi lãnh thổ Việt Nam.

Điều 48. Huy động nguồn lực xã hội và xã hội hóa tài chính trong bảo đảm an ninh dữ liệu

1. Nhà nước khuyến khích tổ chức, cá nhân phát hiện, thông báo lỗ hổng, rủi ro an ninh dữ liệu; đóng góp giải pháp công nghệ bảo vệ dữ liệu cho cơ quan nhà nước và tham gia đầu tư, tài trợ tài chính cho các hoạt động nghiên cứu, phát triển công nghệ, đào tạo nhân lực về an ninh dữ liệu.

2. Bảo đảm bí mật thông tin danh tính, áp dụng chính sách giảm nhẹ hoặc miễn trừ trách nhiệm pháp lý cho người phát hiện, thông báo lỗi bảo mật có thiện chí và không vì mục đích trục lợi bất chính.

3. Tổ chức, doanh nghiệp có chi phí đầu tư, tài trợ cho hoạt động bảo đảm an ninh dữ liệu quốc gia, nghiên cứu công nghệ mật mã thế hệ mới hoặc đào tạo nhân lực chất lượng cao về an ninh dữ liệu thì các khoản chi phí này được tính vào chi phí hợp lý được trừ khi xác định thu nhập chịu thuế thu nhập doanh nghiệp theo quy định của pháp luật về thuế.

4. Chính phủ quy định chi tiết cơ chế tiếp nhận thông tin, khen thưởng, bảo vệ người thông báo và các hình thức chính sách ưu đãi, hỗ trợ cụ thể đối với hoạt động xã hội hóa tài chính quy định tại Điều này.

CHƯƠNG VII.
QUẢN LÝ NHÀ NƯỚC VỀ AN NINH DỮ LIỆU

Điều 49. Nội dung quản lý nhà nước về an ninh dữ liệu

Chính phủ thống nhất quản lý nhà nước về an ninh dữ liệu trên phạm vi toàn quốc, bao gồm:

1. Xây dựng, ban hành chiến lược, chính sách, văn bản quy phạm pháp luật về an ninh dữ liệu gắn với chiến lược phát triển kinh tế số, xã hội số, Chính phủ số.

2. Thiết lập, quản lý hệ thống phân loại dữ liệu, danh mục dữ liệu quốc gia và hệ thống tiêu chuẩn, quy chuẩn kỹ thuật.

3. Quản lý hạ tầng giám sát an ninh dữ liệu tập trung, cơ chế thử nghiệm có kiểm soát và hoạt động chứng nhận hợp quy.

4. Tổ chức thanh tra, kiểm tra, xử lý vi phạm và điều phối hợp tác quốc tế về an ninh dữ liệu.

Điều 50. Trách nhiệm của Bộ Công an

Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh dữ liệu, là cơ quan chủ trì, điều phối tổng thể, có trách nhiệm:

1. Tham mưu Chính phủ ban hành chính sách, pháp luật về an ninh dữ liệu; chủ trì điều phối ứng phó các tình huống khẩn cấp về an ninh dữ liệu quốc gia.

2.Thành lập, vận hành Trung tâm Quản trị an ninh dữ liệu quốc gia và Hệ thống giám sát an ninh dữ liệu tập trung quốc gia.

3. Chủ trì, phối hợp nghiên cứu, ứng dụng mật mã an ninh, mật mã kháng lượng tử để bảo vệ dữ liệu quản lý theo chức năng, nhiệm vụ của Bộ Công an và các khối dữ liệu kinh tế - xã hội.

4. Chủ trì, thẩm định điều kiện an ninh đối với hoạt động đầu tư, chuyển giao công nghệ và hoạt động chuyển dữ liệu ra nước ngoài liên quan đến dữ liệu Quan trọng, dữ liệu Cốt lõi.

5. Tổ chức phòng ngừa, đấu tranh chống tội phạm mạng, tội phạm về dữ liệu; thực hiện công tác thanh tra, kiểm tra, xử lý vi phạm pháp luật về an ninh dữ liệu.

Điều 51. Trách nhiệm của Bộ Quốc phòng

Bộ Quốc phòng là cơ quan chủ trì bảo đảm an ninh dữ liệu quân sự, quốc phòng, có trách nhiệm:

1. Chủ trì bảo đảm an ninh dữ liệu đối với hệ thống thông tin quân sự, quốc phòng; phối hợp với Bộ Công an xây dựng danh mục dữ liệu Cốt lõi, dữ liệu Quan trọng liên quan đến quân sự, quốc phòng.

2. Phối hợp thẩm định điều kiện an ninh đối với hoạt động chuyển dữ liệu liên quan quân sự, quốc phòng ra nước ngoài; vận hành hệ thống giám sát an ninh dữ liệu quân sự.

3. Đồng chủ trì, phối hợp với Bộ Công an và Bộ Khoa học và Công nghệ triển khai các dự án chiến lược quốc gia về nghiên cứu, phát triển và làm chủ công nghệ mã hóa kháng lượng tử.

4. Đối với dữ liệu do các cơ quan, đơn vị, doanh nghiệp thuộc phạm vi quản lý của Bộ Quốc phòng khởi tạo, xử lý và quản lý nhưng không phải là dữ liệu quân sự hoặc bí mật quân sự, quốc phòng thì việc phân loại cấp độ rủi ro, áp dụng các biện pháp bảo đảm an ninh, kết nối giám sát tập trung, thanh tra, kiểm tra và điều phối do Bộ Công an chủ trì, thực hiện theo quy định tại Điều 50 của Luật này.

Điều 52. Trách nhiệm của Bộ Khoa học và Công nghệ

Bộ Khoa học và Công nghệ chịu trách nhiệm quản lý nhà nước về khoa học, công nghệ, đo lường, chất lượng trong bảo đảm an ninh dữ liệu, có trách nhiệm:

1. Thúc đẩy nghiên cứu phát triển công nghệ mật mã thế hệ mới, giải pháp bảo mật nội địa; phối hợp thiết lập vùng thử nghiệm có kiểm soát đối với các công nghệ dữ liệu mới.

2. Ban hành, hướng dẫn áp dụng hệ thống tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia về hạ tầng số và an ninh hệ thống trí tuệ nhân tạo.

Điều 53. Trách nhiệm của Ban Cơ yếu Chính phủ

Ban Cơ yếu Chính phủ chịu trách nhiệm quản lý nhà nước về cơ yếu, là lực lượng phối hợp bảo vệ an ninh dữ liệu bằng kỹ thuật mật mã cơ yếu, có trách nhiệm:

1. Quản lý, tổ chức hoạt động mật mã cơ yếu bảo vệ dữ liệu chứa bí mật nhà nước của cơ quan Đảng, Nhà nước.

2. Thẩm định, chứng nhận các sản phẩm mật mã cơ yếu; Chủ trì nghiên cứu giải pháp mật mã kháng lượng tử để bảo vệ thông tin chiến lược quốc gia.

Điều 54. Trách nhiệm của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân các cấp

1. Người đứng đầu cơ quan, tổ chức, địa phương chịu trách nhiệm trực tiếp về an ninh dữ liệu trong phạm vi quản lý của mình; tổ chức phân loại dữ liệu và báo cáo Bộ Công an.

2. Bố trí nguồn lực, kinh phí bảo đảm an ninh dữ liệu; ưu tiên mua sắm, sử dụng sản phẩm công nghệ bảo mật nội địa đã được chứng nhận hợp quy.

3. Chấp hành mệnh lệnh điều phối kỹ thuật khẩn cấp và tạo điều kiện thuận lợi cho hoạt động thanh tra, kiểm tra của lực lượng chuyên trách.

4. Việc mua sắm sản phẩm, dịch vụ an ninh dữ liệu nội địa đã được chứng nhận hợp quy, phục vụ trực tiếp hệ thống thông tin quốc gia trọng yếu quy định tại khoản 2 Điều này, được áp dụng hình thức chỉ định thầu hoặc mua sắm đặc cách theo quy định của pháp luật về đấu thầu đối với trường hợp mua sắm nhằm bảo đảm an ninh quốc gia; việc áp dụng bảo đảm tương thích với các điều ước quốc tế về mua sắm chính phủ mà Việt Nam là thành viên.

Điều 55. Nghĩa vụ và trách nhiệm của chủ quản dữ liệu

1. Thiết lập, vận hành hệ thống quản trị rủi ro an ninh dữ liệu tương xứng với cấp độ phân loại dữ liệu của cơ quan, tổ chức.

2. Chấp hành nghiêm chỉnh nghĩa vụ thẩm định, kiểm toán an ninh và thực hiện kết nối chia sẻ thông tin giám sát về Hệ thống giám sát tập trung quốc gia đối với dữ liệu Cấp độ 3 và Cấp độ 4.

3. Tự chịu trách nhiệm trước pháp luật về tính chính xác của hoạt động tự phân loại dữ liệu và tự chứng nhận tuân thủ đối với dữ liệu Cấp độ 1 và Cấp độ 2.

CHƯƠNG VIII.
THANH TRA, KIỂM TRA VÀ XỬ LÝ VI PHẠM

Điều 56. Thanh tra, kiểm tra an ninh dữ liệu

1. Thanh tra Bộ Công an, Thanh tra Bộ Quốc phòng chủ trì, phối hợp với các cơ quan chuyên trách thực hiện hoạt động thanh tra chuyên ngành về an ninh dữ liệu theo quy định của pháp luật về thanh tra.

2. Hoạt động kiểm tra kỹ thuật, đánh giá rủi ro định kỳ hoặc đột xuất của lực lượng chuyên trách phải bảo đảm đúng thẩm quyền, trình tự thủ tục và không gây cản trở trái phép hoạt động bình thường của chủ quản dữ liệu.

3. Chính phủ quy định chi tiết phương thức, trình tự thanh tra, kiểm tra về an ninh dữ liệu.

Điều 57. Xử lý vi phạm pháp luật về an ninh dữ liệu

1. Tổ chức, cá nhân có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

2. Áp dụng hình thức xử phạt tiền theo tỷ lệ phần trăm tổng doanh thu của năm tài chính liền kề trước đó đối với tổ chức có hành vi vi phạm đặc biệt nghiêm trọng quy định về bảo vệ dữ liệu Quan trọng, dữ liệu Cốt lõi; mức 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, Chính phủ quy định việc xem xét áp dụng mức phạt 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.

3. Chủ thể dữ liệu bị thiệt hại do hành vi vi phạm quy định của Luật này có quyền yêu cầu bồi thường thiệt hại theo quy định của pháp luật dân sự.

4. Chính phủ quy định chi tiết hành vi vi phạm, hình thức, mức xử phạt cụ thể và chính sách khoan hồng đối với các doanh nghiệp nhỏ, doanh nghiệp khởi nghiệp sáng tạo chủ động khắc phục hậu quả sự cố.

CHƯƠNG IX.
ĐIỀU KHOẢN THI HÀNH

Điều 58. Hiệu lực thi hành, điều khoản chuyển tiếp và tính tương thích

1. Luật này có hiệu lực thi hành kể từ ngày 01 tháng 12 năm 2027.

2. Các quy định về bảo đảm an ninh dữ liệu tại các văn bản quy phạm pháp luật ban hành trước ngày Luật này có hiệu lực thi hành mà trái với quy định của Luật này thì áp dụng theo quy định của Luật này.

3. Đối với các hệ thống thông tin, giấy phép kinh doanh dịch vụ dữ liệu đã được cấp trước ngày Luật này có hiệu lực, Chính phủ quy định lộ trình và điều kiện chuyển tiếp phù hợp để các cơ quan, tổ chức hoàn thiện hệ thống, bảo đảm không làm gián đoạn các dịch vụ công ích và kinh tế xã hội thiết yếu.

4. Kể từ ngày 01 tháng 01 năm 2035, toàn bộ các hệ thống thông tin lưu trữ, xử lý Dữ liệu Cốt lõi (Cấp độ 4) và Dữ liệu Quan trọng (Cấp độ 3) thuộc hệ thống cơ quan Đảng, Nhà nước, lực lượng vũ trang và lĩnh vực tài chính - ngân hàng, năng lượng, viễn thông, giáo dục bắt buộc phải hoàn thành lộ trình kiểm đếm, di cư dữ liệu, dịch chuyển hoàn toàn sang sử dụng giải pháp mật mã kháng lượng tử đã được cấp chứng nhận hợp quy; bảo đảm tính tương thích với các tiêu chuẩn an ninh dữ liệu quốc tế.

5. Việc xây dựng tiêu chuẩn kỹ thuật và đánh giá an ninh dữ liệu xuyên biên giới theo Luật này bảo đảm tính tương thích, hài hòa có chọn lọc với các khung pháp lý của quốc tế trên nguyên tắc không hạ thấp các yêu cầu về bảo vệ chủ quyền số và an ninh quốc gia của Việt Nam.