

QUỐC HỘI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Luật số: /2026/QH16

Dự thảo 28/9/2026

LUẬT
AN NINH DỮ LIỆU

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam đã được sửa đổi, bổ sung một số điều theo Nghị quyết số 203/2025/QH15;

Quốc hội ban hành Luật An ninh dữ liệu.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Luật này quy định về nguyên tắc, biện pháp bảo vệ an ninh dữ liệu; quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân và quản lý nhà nước về an ninh dữ liệu.

2. 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;
- Tổ chức, cá nhân nước ngoài ở ngoài lãnh thổ Việt Nam liên quan đến xử lý dữ liệu thuộc quyền tài phán của Việt Nam hoặc có hành vi xâm phạm an ninh dữ liệu của Việt Nam.

Điều 2. Giải thích từ ngữ

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

1. An ninh dữ liệu là sự bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của dữ liệu trong suốt vòng đời trước các mối đe dọa, nguy cơ xâm phạm; bảo đảm hoạt động xử lý dữ liệu không gây phương hại đến chủ quyền dữ liệu quốc gia, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Bảo vệ an ninh dữ liệu là việc áp dụng lực lượng, phương tiện và biện pháp theo quy định của pháp luật để phòng ngừa, phát hiện, ngăn chặn, xử lý nguy cơ, hành vi xâm phạm an ninh dữ liệu và khắc phục hậu quả do hành vi xâm phạm an ninh dữ liệu gây ra.

3. Dữ liệu thuộc quyền tài phán của Việt Nam là dữ liệu được tạo lập, thu thập trên lãnh thổ Việt Nam hoặc do cơ quan, tổ chức, cá nhân Việt Nam tạo lập, thu thập.

4. Chủ quyền dữ liệu quốc gia là quyền tối cao của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam ban hành chính sách, pháp luật, quản lý, kiểm soát và bảo vệ dữ liệu thuộc quyền tài phán của Việt Nam.

5. Rủi ro an ninh dữ liệu là khả năng xảy ra sự cố an ninh dữ liệu và thiệt hại có thể phát sinh từ sự cố đó.

6. Sự cố an ninh dữ liệu là sự việc bất ngờ xảy ra xâm phạm an ninh dữ liệu.

7. Cấp độ rủi ro an ninh dữ liệu là mức phân loại rủi ro an ninh dữ liệu theo quy định tại Điều 8 của Luật này.

8. Hoạt động xử lý dữ liệu có nguy cơ cao là hoạt động xử lý dữ liệu mà do tính chất, mục đích, quy mô, mức độ tích tụ, liên kết, suy diễn của dữ liệu hoặc công nghệ được sử dụng có khả năng trực tiếp gây hậu quả nghiêm trọng đối với an ninh dữ liệu.

9. Dữ liệu dẫn xuất là dữ liệu mới được tạo ra từ hoạt động phân tích, tổng hợp, suy luận, mô hình hóa, huấn luyện hoặc tinh chỉnh trên cơ sở một hoặc nhiều dữ liệu khác, bao gồm đặc trưng và tham số của mô hình được hình thành trong quá trình huấn luyện, tinh chỉnh.

10. Đầu độc dữ liệu là hành vi cố ý chen, sửa đổi, xóa hoặc làm sai lệch dữ liệu nhằm làm thay đổi chức năng, tạo lỗ hổng ẩn hoặc làm sai lệch kết quả xử lý của hệ thống thông tin, hệ thống trí tuệ nhân tạo.

11. Dữ liệu độc hại là dữ liệu chứa mã độc hoặc dữ liệu bị đầu độc được sử dụng nhằm phá hoại, làm sai lệch hoạt động của hệ thống thông tin, hệ thống trí tuệ nhân tạo.

12. Hạ tầng dữ liệu quốc gia trọng yếu là trung tâm dữ liệu, cơ sở dữ liệu quốc gia, nền tảng và hạ tầng mạng cấp quốc gia lưu trữ, xử lý dữ liệu Cấp độ 4, Cấp độ 5 mà khi bị xâm phạm gây tổn hại đặc biệt nghiêm trọng đến an ninh quốc gia hoặc hoạt động của lĩnh vực trọng yếu, thuộc danh mục do Thủ tướng Chính phủ ban hành.

13. Hệ thống vật lý - số là hệ thống tích hợp dữ liệu, phần mềm, mạng, cảm biến và thành phần vật lý để giám sát, điều khiển, tự động hóa hoặc thực hiện hành động trong môi trường vật lý.

14. Dữ liệu điều khiển là dữ liệu, lệnh, tham số, khóa mật mã, thông tin xác thực được sử dụng để giám sát, điều khiển, xác lập quyền điều khiển hoặc làm thay đổi trạng thái hoạt động của hệ thống vật lý - số.

15. Không gian mới gồm không gian vũ trụ, không gian tầm thấp, không gian ngầm, không gian biển và đại dương.

16. Nhật ký sự kiện an ninh là bản ghi thông tin kỹ thuật về trạng thái, cấu hình, hành vi truy cập và sự kiện phát sinh trong quá trình xử lý dữ liệu, bao gồm siêu dữ liệu an ninh và chỉ báo tấn công, không bao gồm nội dung của dữ liệu được xử lý.

17. Quyền truy cập đặc quyền là quyền truy cập cho phép quản trị hệ thống thông tin, thay đổi cấu hình, phân quyền hoặc thực hiện thao tác trích xuất, sửa đổi, xóa dữ liệu hàng loạt, làm thay đổi hoạt động của hệ thống thông tin.

18. Bên xử lý dữ liệu là cơ quan, tổ chức, cá nhân thực hiện việc xử lý dữ liệu thay mặt chủ quản dữ liệu, chủ sở hữu dữ liệu hoặc theo ủy quyền, thỏa thuận, hợp đồng với chủ thể đó.

19. Cơ quan chuyên trách bảo vệ an ninh dữ liệu là đơn vị thuộc lực lượng chuyên trách bảo vệ an ninh mạng tại Bộ Công an, Bộ Quốc phòng được giao nhiệm vụ bảo vệ an ninh dữ liệu.

21. Chuỗi cung ứng sản phẩm, dịch vụ dữ liệu là tập hợp tổ chức, cá nhân cung cấp sản phẩm phần mềm, hạ tầng lưu trữ, giải pháp xử lý dữ liệu và dịch vụ kỹ thuật có kết nối, tiếp cận hoặc tham gia vào quá trình xử lý dữ liệu của chủ quản dữ liệu.

Điều 3. Áp dụng pháp luật về an ninh dữ liệu

1. Trường hợp luật khác có quy định khác với Luật này về biện pháp quản lý, biện pháp kỹ thuật và thủ tục bảo đảm an ninh của dữ liệu thì áp dụng quy định của Luật này, trừ trường hợp quy định tại khoản 2 Điều này.

2. Việc áp dụng pháp luật đối với nội dung giao thoa được thực hiện như sau:

a) Nguyên tắc, điều kiện xử lý dữ liệu cá nhân, quyền của chủ thể dữ liệu cá nhân, trách nhiệm của bên kiểm soát, bên xử lý dữ liệu cá nhân thực hiện theo pháp luật về bảo vệ dữ liệu cá nhân; biện pháp bảo đảm an ninh đối với dữ liệu cá nhân theo cấp độ rủi ro thực hiện theo Luật này;

b) Bảo vệ an ninh mạng đối với hệ thống thông tin thực hiện theo pháp luật về an ninh mạng; bảo vệ an ninh đối với dữ liệu lưu trữ, xử lý trên hệ thống thông tin thực hiện theo Luật này;

c) Hoạt động xây dựng, quản trị, khai thác, chia sẻ và phân loại dữ liệu theo tính chất quan trọng thực hiện theo pháp luật về dữ liệu; công tác bảo vệ và quản trị an ninh dữ liệu thực hiện theo quy định của Luật này;

d) Bảo vệ bí mật nhà nước thực hiện theo pháp luật về bảo vệ bí mật nhà nước; việc sử dụng mật mã để bảo vệ dữ liệu bí mật nhà nước thực hiện theo quy định của Luật Cơ yếu và quy định của Luật này; trường hợp Luật Cơ yếu và Luật này cùng quy định về một vấn đề thì thực hiện theo quy định của Luật này;

đ) Quản lý rủi ro, thử nghiệm có kiểm soát, gắn nhãn, giám sát của con người đối với hệ thống trí tuệ nhân tạo; ứng dụng công nghệ số, giao dịch điện tử, lưu trữ thực hiện theo pháp luật về trí tuệ nhân tạo, công nghiệp công nghệ số, chuyển đổi số, giao dịch điện tử và lưu trữ; bảo đảm an ninh đối với dữ liệu được tạo lập, lưu trữ, xử lý trong các hoạt động đó thực hiện theo Luật này;

e) Trường hợp tập dữ liệu được chia sẻ, cung cấp, giao dịch hoặc chuyển nhượng có đồng thời dữ liệu cá nhân và dữ liệu khác thì từng phần dữ liệu thực hiện theo quy định tương ứng tại điểm a và điểm c khoản này; biện pháp bảo đảm an ninh đối với tập dữ liệu được áp dụng theo cấp độ rủi ro cao nhất của dữ liệu trong tập dữ liệu.

3. Trường hợp Luật này và luật khác cùng quy định thủ tục hành chính, đánh giá, thẩm định, kiểm tra, chứng nhận hoặc chế độ báo cáo đối với cùng một đối tượng, cùng một nội dung thì thực hiện như sau:

a) Cơ quan, tổ chức, cá nhân lập một bộ hồ sơ, thực hiện một thủ tục thông qua một đầu mối tiếp nhận; kết quả giải quyết được sử dụng chung cho các cơ quan có thẩm quyền;

b) Kết quả đánh giá, thẩm định, kiểm tra, kiểm toán, chứng nhận đã được thực hiện hợp pháp theo luật khác và còn hiệu lực thì được công nhận đối với nội dung tương ứng theo Luật này; cơ quan nhà nước không yêu cầu thực hiện lại;

c) Báo cáo sự cố đã gửi qua hệ thống điện tử thống nhất quy định tại khoản 4 Điều 26 của Luật này được coi là đã thực hiện nghĩa vụ báo cáo, thông báo cho Bộ Công an đối với cùng sự cố theo pháp luật về an ninh mạng và pháp luật về bảo vệ dữ liệu cá nhân; hệ thống điện tử thống nhất chuyển thông tin báo cáo sự cố đến cơ quan quản lý ngành, lĩnh vực có liên quan, cơ quan quản lý ngành, lĩnh vực không yêu cầu báo cáo lại cùng nội dung;

d) Đối với sự cố an ninh dữ liệu liên quan đến bí mật nhà nước, cơ quan tiếp nhận chuyển thông tin cho cơ quan quản lý bí mật nhà nước có liên quan theo quy định của Chính phủ;

đ) Cơ quan có thẩm quyền tự khai thác hồ sơ, kết quả đã có trên hệ thống điện tử thống nhất và cơ sở dữ liệu có liên quan; không yêu cầu cơ quan, tổ chức, cá nhân nộp lại hoặc chứng minh việc đã hoàn thành nghĩa vụ đã được cơ quan có thẩm quyền khác xác nhận.

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.

5. Trường hợp chủ sở hữu dữ liệu trực tiếp quản lý, vận hành, khai thác dữ liệu hoặc không giao chủ quản dữ liệu thì chủ sở hữu dữ liệu thực hiện nghĩa vụ của chủ quản dữ liệu theo quy định của Luật này.

6. Phần nội dung dữ liệu có trong nhật ký sự kiện an ninh được bảo vệ theo chế độ pháp lý áp dụng đối với dữ liệu tương ứng.

Điều 4. Nguyên tắc bảo vệ an ninh dữ liệu

1. Tuân thủ Hiến pháp và pháp luật; bảo vệ chủ quyền dữ liệu quốc gia, an ninh quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Bảo vệ an ninh dữ liệu là yêu cầu xuyên suốt trong chuyển đổi số quốc gia; gắn với bảo đảm lưu thông dữ liệu hợp pháp, phục vụ phát triển Chính phủ số, kinh tế số, xã hội số và hội nhập quốc tế.

3. Quản lý theo cấp độ rủi ro; biện pháp bảo vệ tương xứng với cấp độ rủi ro và mức độ rủi ro thực tế, không vượt quá yêu cầu tối thiểu theo cấp độ rủi ro do Chính phủ quy định, không cản trở hoạt động hợp pháp của cơ quan, tổ chức, cá nhân.

4. Bảo vệ an ninh dữ liệu được thực hiện chủ động từ khâu thiết kế và xuyên suốt vòng đời dữ liệu.

5. Chủ quản dữ liệu tự xác định cấp độ rủi ro, tự áp dụng biện pháp bảo vệ và chịu trách nhiệm trước pháp luật. Cơ quan nhà nước thực hiện hậu kiểm là chủ yếu; chỉ thực hiện tiền kiểm đối với dữ liệu, hệ thống có rủi ro cao theo quy định của Luật này.

6. Một đối tượng, một nội dung rủi ro chỉ đánh giá, thẩm định, kiểm tra một lần; kế thừa, công nhận kết quả đã thực hiện hợp pháp theo luật khác và theo tiêu chuẩn, chứng nhận quốc tế tương đương theo quy định của Luật này; chỉ yêu cầu đánh giá, thẩm định lại khi có thay đổi làm phát sinh hoặc gia tăng rủi ro an ninh dữ liệu, trừ kiểm toán định kỳ quy định tại khoản 4 và khoản 5 Điều 10 của Luật này.

7. Bảo đảm đồng bộ, liên thông giữa bảo vệ an ninh dữ liệu với bảo vệ an ninh mạng, bảo vệ dữ liệu cá nhân và bảo vệ bí mật nhà nước.

8. Không phân biệt đối xử giữa tổ chức, cá nhân trong nước và nước ngoài trong áp dụng biện pháp bảo vệ an ninh dữ liệu, trừ trường hợp luật quy định khác vì lý do quốc phòng, an ninh quốc gia.

9. 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 và quyền, lợi ích hợp pháp khác của cơ quan, tổ chức, cá nhân, trừ trường hợp luật có quy định khác.

Điều 5. Chính sách của Nhà nước và hợp tác quốc tế về an ninh dữ liệu

1. Nhà nước có trách nhiệm hoàn thiện đồng bộ thể chế và tổ chức thực hiện các mục tiêu, nhiệm vụ về an ninh dữ liệu trong Chiến lược bảo vệ an ninh mạng, an ninh dữ liệu và các chiến lược quốc gia có liên quan; bảo vệ chủ quyền dữ liệu quốc gia, an ninh quốc gia, an ninh con người, hoạt động của Nhà nước và dịch vụ thiết yếu.

2. Nhà nước có chính sách ưu tiên phát triển điện toán đám mây chủ quyền, hạ tầng dữ liệu và trung tâm dữ liệu an toàn, xanh, tiết kiệm năng lượng, có khả năng chống chịu, phục hồi; có chính sách khuyến khích phát triển Việt Nam thành địa điểm lưu trữ, xử lý dữ liệu quốc tế an toàn, tin cậy trên cơ sở bảo đảm chủ quyền dữ liệu, năng lực kiểm soát và quản trị rủi ro.

3. Nhà nước áp dụng chính sách hỗ trợ, ưu đãi theo pháp luật về đầu tư, thuế, khoa học, công nghệ và đổi mới sáng tạo đối với nghiên cứu, phát triển, chuyển giao công nghệ bảo vệ an ninh dữ liệu, mật mã an ninh, mật mã kháng lượng tử, mật mã lượng tử, công nghệ tăng cường quyền riêng tư, công nghệ lỗi và trung tâm dữ liệu xanh. Trung tâm dữ liệu xanh là trung tâm dữ liệu đã công bố hợp quy theo quy chuẩn kỹ thuật quốc gia về hiệu quả sử dụng năng lượng; Chính phủ quy định lộ trình hỗ trợ trung tâm dữ liệu đang hoạt động chuyển đổi.

4. Chi phí đầu tư, tài trợ hợp pháp cho bảo vệ an ninh dữ liệu, nghiên cứu phát triển công nghệ mật mã, mật mã kháng lượng tử, trung tâm dữ liệu xanh được tính vào chi phí được trừ khi xác định thu nhập chịu thuế theo quy định của pháp luật về thuế thu nhập doanh nghiệp.

5. Cơ quan nhà nước có trách nhiệm nâng cao năng lực tự chủ, khả năng kiểm chứng, thay thế công nghệ và nhà cung cấp; đánh giá và có phương án giảm mức độ phụ thuộc chiến lược đối với dữ liệu, công nghệ, điện toán đám mây, tín hiệu định vị, dẫn đường, đồng bộ thời gian, hạ tầng truyền dẫn và nguồn lực nằm ngoài khả năng kiểm soát.

6. Nhà nước có trách nhiệm phát triển nguồn nhân lực chất lượng cao; 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.

7. Nhà nước có trách nhiệm phát triển hệ sinh thái và công nghiệp an ninh dữ liệu tự chủ, tin cậy, hiện đại, hội nhập; khuyến khích hợp tác công - tư, đặt hàng, thử nghiệm, kiểm định, công nhận, mua sắm và triển khai sản phẩm, dịch vụ trên cơ sở tiêu chuẩn mở, khả năng kiểm chứng, cạnh tranh bình đẳng và khả năng thay thế. Cơ quan có thẩm quyền ưu tiên hình thành năng lực nghiên cứu, phòng thử nghiệm, doanh nghiệp công nghệ nòng cốt và sản phẩm lưỡng dụng trong nước; không được áp dụng biện pháp tạo vị trí độc quyền cho một sản phẩm, nhà cung cấp.

8. Giải pháp, công nghệ bảo vệ an ninh dữ liệu và mô hình xử lý, chuyển dữ liệu mới được thử nghiệm có kiểm soát theo pháp luật về khoa học, công nghệ và đổi mới sáng tạo. Trong phạm vi, thời hạn thử nghiệm, tổ chức tham gia được miễn, giảm một phần nghĩa vụ theo Luật này theo quy định của Chính phủ; không miễn, giảm nghĩa vụ đối với dữ liệu Cấp độ 5, dữ liệu chứa bí mật nhà nước và nghĩa vụ báo cáo sự cố. Bộ Công an tham gia đánh giá nội dung an ninh dữ liệu trong quá trình thử nghiệm.

9. Hợp tác quốc tế về an ninh dữ liệu được thực hiện trên nguyên tắc tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi; tuân thủ pháp luật Việt Nam và điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên. Nội dung hợp tác gồm phòng ngừa, phát hiện, cảnh báo, ứng phó sự cố; đấu tranh với hành vi xâm phạm an ninh dữ liệu; nghiên cứu, đào tạo; tiêu chuẩn, đánh giá sự phù hợp; mật mã; an ninh chuỗi cung ứng, an ninh dữ liệu trong các không gian mới và chuyển, xử lý dữ liệu xuyên biên giới an toàn, tin cậy.

10. Bộ Công an chủ trì, phối hợp với Bộ Ngoại giao, Bộ Quốc phòng và cơ quan có liên quan thực hiện hợp tác quốc tế về an ninh dữ liệu theo thẩm quyền.

Điều 6. Các hành vi bị nghiêm cấm

1. Chiếm đoạt, mua bán, trao đổi, thu thập, truy cập, trích xuất, làm lộ, làm mất, làm sai lệch, phá hủy dữ liệu trái phép; cản trở trái phép việc truy cập, xử lý dữ liệu hợp pháp.

2. Đầu độc dữ liệu; lợi dụng dữ liệu, thuật toán và hệ thống trí tuệ nhân tạo để tổ chức các chiến dịch thao túng thông tin, xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

3. Lợi dụng hoạt động bảo vệ an ninh dữ liệu để truy cập, thu thập, khai thác, sử dụng dữ liệu trái pháp luật hoặc để trục lợi.

4. Che giấu sự cố an ninh dữ liệu hoặc không báo cáo, thông báo trong trường hợp Luật này hoặc pháp luật có liên quan quy định phải báo cáo, thông báo.

5. Tiết lộ, chuyển giao trái pháp luật khóa mật mã, thông tin xác thực hoặc tham số an ninh làm suy giảm an ninh dữ liệu.

6. Cố ý cung cấp thông tin sai sự thật, che giấu rủi ro đã phát hiện, chia tách dữ liệu, xác định không đúng quy mô tích tụ, liên kết, suy diễn hoặc cố ý xác định dữ liệu ở cấp độ thấp hơn mức phải xác định theo quy định của Luật này nhằm tránh áp dụng yêu cầu bảo vệ tương ứng.

7. Cung cấp hoặc cho phép tiếp cận dữ liệu từ Cấp độ 3 trở lên theo yêu cầu của cơ quan, tòa án nước ngoài hoặc tổ chức nước ngoài thực hiện yêu cầu đó khi không có căn cứ quy định tại khoản 1 Điều 20 của Luật này.

8. Sản xuất, kinh doanh, cung cấp, sử dụng công cụ, phần mềm, thiết bị có chứa mã độc, tính năng ẩn, cổng hậu nhằm thu thập, trích xuất, phá hoại dữ liệu trái pháp luật.

9. Sử dụng trái pháp luật dữ liệu chứa bí mật nhà nước, dữ liệu cốt lõi để huấn luyện mô hình trí tuệ nhân tạo hoặc chuyển giao cho bên thứ ba.

10. Giả mạo sản phẩm mật mã an ninh; kinh doanh sản phẩm, dịch vụ mật mã an ninh không thuộc Danh mục quy định tại khoản 3 Điều 16 của Luật này; tiết lộ trái pháp luật thông tin về sản phẩm, giải pháp mật mã an ninh hoặc thông tin về cơ quan, tổ chức, cá nhân sử dụng mật mã an ninh.

11. Cản trở trái pháp luật hoạt động của cơ quan, người có thẩm quyền.

Điều 7. Biện pháp bảo vệ an ninh dữ liệu

1. Biện pháp bảo vệ an ninh dữ liệu bao gồm:

a) Biện pháp quản lý: xác định cấp độ rủi ro, đánh giá tác động, giám sát tuân thủ, kiểm toán, thẩm định, thanh tra, kiểm tra, bố trí nhân sự phụ trách an ninh dữ liệu;

b) Biện pháp kỹ thuật: mã hóa dữ liệu, quản lý truy cập, định danh, sao lưu, phục hồi dữ liệu, tiêu hủy dữ liệu an toàn, kiểm thử an ninh dữ liệu;

c) Bảo vệ an ninh vật lý đối với thiết bị, hạ tầng lưu trữ, xử lý dữ liệu;

d) Đánh giá sự phù hợp, chứng nhận theo tiêu chuẩn, quy chuẩn kỹ thuật về an ninh dữ liệu;

đ) Ứng phó, khắc phục sự cố an ninh dữ liệu;

e) Đào tạo, tuyên truyền, diễn tập bảo vệ an ninh dữ liệu;

g) Ngăn chặn, vô hiệu hóa dữ liệu độc hại, yêu cầu xóa bỏ dữ liệu, loại bỏ dữ liệu độc hại;

h) Xử lý vi phạm pháp luật về an ninh dữ liệu.

2. Chủ quản dữ liệu áp dụng biện pháp bảo vệ an ninh dữ liệu tương xứng với cấp độ rủi ro theo quy định của Luật này. Việc thẩm định, thanh tra, kiểm tra,

ngăn chặn, vô hiệu hóa dữ liệu độc hại và xử lý vi phạm do cơ quan, người có thẩm quyền thực hiện theo quy định của Luật này và pháp luật có liên quan.

3. Chính phủ quy định chi tiết Điều này.

Chương II

BẢO VỆ AN NINH DỮ LIỆU THEO CẤP ĐỘ RỦI RO VÀ VÒNG ĐỜI DỮ LIỆU

Điều 8. Cấp độ rủi ro an ninh dữ liệu

1. Cấp độ rủi ro an ninh dữ liệu được xác định dựa trên khả năng xảy ra sự cố và mức độ thiệt hại đối với quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân, bao gồm 05 cấp độ từ thấp đến cao như sau:

a) Cấp độ 1: khả năng xảy ra và hậu quả ở mức thấp, ít gây tổn hại đến quyền, lợi ích hợp pháp của tổ chức, cá nhân; không xâm hại an ninh quốc gia, trật tự, an toàn xã hội; bao gồm dữ liệu công khai, dữ liệu mở theo quy định của pháp luật;

b) Cấp độ 2: khả năng xảy ra và hậu quả ở mức trung bình, gây tổn hại nghiêm trọng đến quyền, lợi ích hợp pháp của tổ chức, cá nhân hoặc đe dọa trật tự, an toàn xã hội; bao gồm dữ liệu lưu hành nội bộ, dữ liệu kinh doanh và dữ liệu cá nhân không thuộc điểm c khoản này;

c) Cấp độ 3: khả năng xảy ra và hậu quả ở mức cao, gây tổn hại rất nghiêm trọng đến quyền, lợi ích hợp pháp của tổ chức, cá nhân, gây tổn hại đến trật tự, an toàn xã hội và đe dọa phương hại an ninh quốc gia; bao gồm dữ liệu quan trọng không thuộc dữ liệu cốt lõi, dữ liệu cốt lõi quy định tại khoản 3 Điều này và dữ liệu cá nhân nhạy cảm được xử lý đạt ngưỡng quy mô lớn theo quy định của Chính phủ;

d) Cấp độ 4: khả năng xảy ra và hậu quả ở mức rất cao, gây tổn hại đặc biệt nghiêm trọng đến quyền, lợi ích hợp pháp của tổ chức, cá nhân, gây tổn hại nghiêm trọng trật tự, an toàn xã hội và gây phương hại an ninh quốc gia; bao gồm dữ liệu cốt lõi, trừ dữ liệu thuộc điểm đ khoản này và dữ liệu cốt lõi quy định tại khoản 3 Điều này;

đ) Cấp độ 5: hậu quả ở mức đặc biệt nghiêm trọng, trực tiếp xâm phạm an ninh quốc gia; bao gồm dữ liệu cốt lõi thuộc lĩnh vực quốc phòng, an ninh và dữ liệu cốt lõi về vận hành, điều khiển công trình quan trọng đặc biệt liên quan đến an ninh quốc gia theo tiêu chí do Chính phủ quy định.

2. Cấp độ rủi ro an ninh dữ liệu không thay thế việc phân loại dữ liệu theo pháp luật về dữ liệu; không làm thay đổi quyền sở hữu, quyền quản lý, quyền khai thác, sử dụng dữ liệu.

3. Dữ liệu được xác định là dữ liệu cốt lõi chỉ do đạt ngưỡng về số lượng chủ thể dữ liệu hoặc khối lượng dữ liệu thì được xác định là Cấp độ 3, trừ dữ liệu thuộc lĩnh vực quốc phòng, an ninh, cơ yếu, đối ngoại; dữ liệu trong cơ sở dữ liệu quốc gia, cơ sở dữ liệu của cơ quan nhà nước; dữ liệu sinh trắc học, dữ liệu di truyền; dữ

liệu vận hành hạ tầng dữ liệu quốc gia trọng yếu. Khi có căn cứ việc xâm phạm tập dữ liệu đó trực tiếp đe dọa an ninh quốc gia, cơ quan chuyên trách bảo vệ an ninh dữ liệu thực hiện theo quy định tại khoản 9 Điều này.

4. Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đã được phê duyệt theo pháp luật về an ninh mạng được sử dụng để xác định cấp độ rủi ro an ninh dữ liệu đối với nội dung tương ứng; chủ quản dữ liệu chỉ bổ sung nội dung chưa có.

5. Chủ quản dữ liệu đánh giá lại cấp độ khi thay đổi quy mô, mục đích, công nghệ xử lý, bên thứ ba tham gia xử lý, khi tích tụ, liên kết, suy diễn dữ liệu làm dữ liệu đáp ứng tiêu chí của cấp độ khác hoặc trước khi thực hiện hoạt động xử lý dữ liệu có nguy cơ cao; trường hợp dữ liệu thuộc Cấp độ 3 trở lên thì thực hiện đánh giá tác động theo quy định tại khoản 4 Điều 10 của Luật này; hoàn thành việc áp dụng biện pháp bảo vệ theo cấp độ mới trong thời hạn do Chính phủ quy định. Hệ thống chuyển lên Cấp độ 4, Cấp độ 5 phải được thẩm định theo quy định tại khoản 6 Điều 11 của Luật này.

6. Dữ liệu đáp ứng tiêu chí dữ liệu quan trọng, dữ liệu cốt lõi nhưng chưa có tên trong danh mục thì chủ quản dữ liệu kiến nghị cơ quan có thẩm quyền cập nhật danh mục và áp dụng biện pháp bảo vệ tương ứng trong thời gian chờ cập nhật.

7. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng và bộ quản lý ngành, lĩnh vực rà soát định kỳ tiêu chí xác định cấp độ; kiến nghị cơ quan có thẩm quyền sửa đổi tiêu chí, cập nhật danh mục dữ liệu quan trọng, dữ liệu cốt lõi.

8. Cơ quan chuyên trách bảo vệ an ninh dữ liệu công bố công cụ tự xác định cấp độ và hướng dẫn chủ quản dữ liệu khi có đề nghị. Chủ quản dữ liệu thực hiện theo văn bản hướng dẫn không bị xử lý vi phạm do xác định sai cấp độ đối với nội dung đã được hướng dẫn.

9. Khi có căn cứ xác định dữ liệu được xác định cấp độ thấp hơn mức phải xác định, cơ quan chuyên trách bảo vệ an ninh dữ liệu yêu cầu bằng văn bản chủ quản dữ liệu xác định lại; hết thời hạn ghi trong văn bản mà chủ quản dữ liệu không thực hiện thì cơ quan chuyên trách bảo vệ an ninh dữ liệu quyết định cấp độ. Chủ quản dữ liệu có quyền giải trình, khiếu nại, khởi kiện theo quy định của pháp luật.

10. Dữ liệu chứa bí mật nhà nước được xác định độ mật và bảo vệ theo pháp luật về bảo vệ bí mật nhà nước. Hệ thống thông tin lưu trữ, xử lý dữ liệu chứa bí mật nhà nước độ Mật, Tối mật, Tuyệt mật phải đáp ứng yêu cầu bảo vệ không thấp hơn yêu cầu tối thiểu đối với dữ liệu Cấp độ 3, Cấp độ 4 và Cấp độ 5 tương ứng với độ mật cao nhất của dữ liệu mà hệ thống lưu trữ, xử lý; trường hợp Luật này và pháp luật về bảo vệ bí mật nhà nước có yêu cầu khác nhau về cùng một nội dung thì áp dụng yêu cầu cao hơn.

11. Việc cung cấp, chuyển giao dữ liệu chứa bí mật nhà nước cho cơ quan, tổ chức, cá nhân trong nước và nước ngoài, kể cả theo yêu cầu quy định tại Điều 20 của Luật này, thực hiện theo pháp luật về bảo vệ bí mật nhà nước. Quy định tại

các khoản 5, 6, 7, 8 và 9 Điều này, điểm b khoản 7 Điều 10, Điều 19, khoản 1 và khoản 2 Điều 20 của Luật này không áp dụng đối với dữ liệu chứa bí mật nhà nước.

12. Chính phủ quy định chi tiết tiêu chí, phương pháp xác định cấp độ rủi ro an ninh dữ liệu; ngưỡng quy mô lớn; tiêu chí xác định dữ liệu cốt lõi thuộc Cấp độ 5 và dữ liệu cốt lõi quy định tại khoản 3 Điều này; bảng tương ứng giữa cấp độ rủi ro an ninh dữ liệu và cấp độ an toàn hệ thống thông tin; thời hạn áp dụng biện pháp bảo vệ theo cấp độ mới, chu kỳ rà soát tiêu chí, thời hạn trả lời kiến nghị cập nhật danh mục và trình tự xác định lại cấp độ quy định tại các khoản 5, 6, 7, 8 và 9 Điều này.

Điều 9. Bảo vệ an ninh dữ liệu theo vòng đời dữ liệu

1. Dữ liệu được bảo vệ an ninh trong suốt vòng đời, từ khâu thiết kế, tạo lập, thu thập, lưu trữ, xử lý, truyền đưa, chia sẻ, giao dịch, sao lưu, khôi phục cho đến khi tiêu hủy, bảo đảm tương thích với cấp độ rủi ro của dữ liệu.

2. Chủ quản dữ liệu từ Cấp độ 3 trở lên có trách nhiệm tuân thủ các nguyên tắc bảo vệ an ninh trong từng khâu vòng đời dữ liệu như sau:

a) Tích hợp giải pháp bảo vệ an ninh ngay từ khâu thiết kế hệ thống; hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5 phải được thẩm định theo quy định tại Điều 11 của Luật này;

b) Kiểm tra nguồn gốc và tính nguyên vẹn của dữ liệu tiếp nhận từ bên ngoài; ngăn chặn việc tích hợp dữ liệu không rõ nguồn gốc hoặc có dấu hiệu xâm nhập;

c) Áp dụng tiêu chuẩn, quy chuẩn kỹ thuật mã hóa và kiểm soát truy cập trong lưu trữ, xử lý, truyền đưa và chia sẻ dữ liệu; không giao dịch dữ liệu Cấp độ 5;

d) Thực hiện sao lưu dữ liệu tách biệt với hệ thống vận hành, bảo đảm bản sao lưu không bị xóa, mã hóa đồng thời khi hệ thống vận hành bị xâm phạm; bảo đảm tính nguyên vẹn, khả năng khôi phục và tuân thủ pháp luật về giao dịch điện tử;

đ) Tiêu hủy dữ liệu bảo đảm dữ liệu không thể khôi phục và ghi nhật ký sự kiện an ninh.

3. Chủ quản dữ liệu Cấp độ 1, Cấp độ 2 tự quyết định phương án bảo vệ phù hợp với yêu cầu quản trị của mình.

4. Việc sử dụng dữ liệu từ Cấp độ 3 trở lên cho mục đích nghiên cứu, huấn luyện trí tuệ nhân tạo, xử lý dữ liệu dẫn xuất hoặc điều khiển hệ thống vật lý - số phải tuân thủ các giới hạn về phạm vi, mục đích, áp dụng cơ chế khử nhận dạng hoặc dữ liệu tổng hợp, đồng thời duy trì khả năng truy xuất nguồn gốc và lịch sử thay đổi của dữ liệu. Trường hợp dữ liệu đã khử nhận dạng, dữ liệu tổng hợp không đáp ứng mục đích sử dụng, tổ chức, cá nhân được sử dụng dữ liệu thực khi có căn cứ pháp lý, giới hạn mục đích, phạm vi, thời hạn sử dụng, áp dụng biện pháp bảo vệ theo cấp độ rủi ro của dữ liệu và tiêu hủy dữ liệu khi kết thúc mục đích sử dụng.

5. Chủ quản dữ liệu từ Cấp độ 3 trở lên chỉ cấp quyền truy cập đặc quyền ở mức tối thiểu cần thiết, ghi nhận đầy đủ nhật ký thao tác và thu hồi quyền ngay khi

thay đổi nhiệm vụ hoặc chấm dứt quan hệ công tác; lưu giữ nhật ký sự kiện an ninh, bảo đảm tính nguyên vẹn, không bị sửa đổi, xóa trái phép.

6. Chủ quản dữ liệu Cấp độ 4, Cấp độ 5 đánh giá mức độ tin cậy của nhân sự trước khi cấp quyền truy cập đặc quyền; đối với dữ liệu Cấp độ 5, áp dụng tiêu chí, chu kỳ đánh giá nghiêm ngặt hơn và cơ chế nhiều người có thẩm quyền cùng xác nhận đối với thao tác trọng yếu. Nhân sự tiếp cận dữ liệu chứa bí mật nhà nước thực hiện theo pháp luật về bảo vệ bí mật nhà nước.

7. Chủ quản dữ liệu Cấp độ 4, Cấp độ 5 và hạ tầng dữ liệu quốc gia trọng yếu phải xây dựng phương án vận hành dự phòng, phương án ứng phó khi đứt gãy kết nối hoặc gián đoạn nhà cung cấp; duy trì bản sao lưu được cách ly để không thể bị sửa đổi, xóa hoặc mã hóa từ hệ thống đang vận hành và định kỳ kiểm tra khả năng khôi phục; đánh giá mức độ phụ thuộc chiến lược về dữ liệu trong kỳ kiểm toán an ninh dữ liệu. Phương án vận hành dự phòng, phương án kỹ thuật quy định tại khoản 10 Điều 23 của Luật này và phương án ứng phó sự cố theo pháp luật về an ninh mạng được xây dựng thành một phương án.

8. Trường hợp tổ chức, doanh nghiệp chấm dứt hoạt động, giải thể hoặc phá sản, việc xử lý dữ liệu được thực hiện như sau:

a) Dữ liệu được bàn giao cho chủ thể kế thừa hợp pháp theo quy định của pháp luật;

b) Trường hợp không có chủ thể kế thừa, dữ liệu cốt lõi, dữ liệu phát sinh từ việc thực hiện nhiệm vụ do Nhà nước giao được chuyển giao cho cơ quan nhà nước có thẩm quyền; dữ liệu cá nhân được xử lý theo quy định của pháp luật về bảo vệ dữ liệu cá nhân; dữ liệu khác được tiêu hủy hoặc xử lý theo quy định của pháp luật về doanh nghiệp, pháp luật về phá sản;

c) Việc bàn giao, chuyển giao, tiêu hủy dữ liệu từ Cấp độ 3 trở lên phải được lập biên bản;

d) Người đại diện theo pháp luật, quản tài viên, doanh nghiệp quản lý, thanh lý tài sản hoặc người được giao quản lý, thanh lý tài sản chịu trách nhiệm tổ chức thực hiện quy định tại khoản này.

9. Chính phủ quy định chi tiết Điều này.

Điều 10. Đánh giá tác động, kiểm toán và chứng nhận an ninh dữ liệu

1. Chủ quản dữ liệu Cấp độ 1 không phải lập hồ sơ, thực hiện thủ tục hành chính về an ninh dữ liệu theo quy định của Luật này, trừ nghĩa vụ ứng phó, báo cáo sự cố quy định tại khoản 5 và khoản 6 Điều 22 của Luật này.

2. Chủ quản dữ liệu Cấp độ 2 xây dựng phương án bảo vệ an ninh dữ liệu theo mẫu rút gọn do Bộ Công an công bố; phương án được thể hiện trong quy chế, hồ sơ bảo vệ dữ liệu cá nhân hoặc hồ sơ bảo đảm an toàn hệ thống thông tin đã có và được lưu giữ để phục vụ thanh tra, kiểm tra.

3. Hộ kinh doanh, doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ, doanh nghiệp khởi nghiệp sáng tạo không phải lập phương án quy định tại khoản 2 Điều này; áp dụng biện pháp bảo vệ cơ bản theo hướng dẫn do Bộ Công an công bố.

4. Chủ quản dữ liệu từ Cấp độ 3 trở lên có trách nhiệm thiết lập danh mục dữ liệu từ Cấp độ 3 trở lên thuộc phạm vi quản lý, thực hiện đánh giá tác động an ninh dữ liệu và tổ chức kiểm toán an ninh dữ liệu định kỳ theo cấp độ rủi ro; kết quả đánh giá và kiểm toán phải được lưu giữ hoặc tích hợp vào hồ sơ thẩm định theo quy định của pháp luật.

5. Kiểm toán đối với dữ liệu Cấp độ 4, Cấp độ 5 bao gồm kiểm thử xâm nhập. Chủ quản dữ liệu Cấp độ 4, Cấp độ 5 gửi báo cáo kết quả kiểm toán qua hệ thống điện tử thống nhất quy định tại khoản 4 Điều 26 của Luật này.

6. Hoạt động kiểm toán an ninh dữ liệu được thực hiện bởi chính chủ quản dữ liệu, tổ chức độc lập hoặc tổ chức cung cấp dịch vụ đánh giá an ninh mạng đủ điều kiện theo quy định của pháp luật; hoạt động kiểm toán này không thay thế cho hoạt động thanh tra, kiểm tra của cơ quan nhà nước có thẩm quyền.

7. Việc đánh giá tác động và chứng nhận an ninh dữ liệu được thực hiện theo nguyên tắc tích hợp và công nhận lẫn nhau:

a) Hồ sơ đánh giá tác động an ninh dữ liệu được tích hợp chung với hồ sơ bảo vệ dữ liệu cá nhân, hồ sơ an ninh mạng hoặc hồ sơ đánh giá rủi ro trí tuệ nhân tạo;

b) Các chứng nhận hợp pháp theo tiêu chuẩn quốc tế hoặc quốc gia thuộc danh mục do cơ quan có thẩm quyền công bố được sử dụng để thay thế các nội dung đánh giá, kiểm toán tương ứng; chủ quản dữ liệu chỉ phải bổ sung những nội dung mà chứng nhận chưa bao quát hết.

8. Sản phẩm, dịch vụ chuyên dùng bảo vệ an ninh dữ liệu sử dụng cho hệ thống Cấp độ 4, Cấp độ 5 phải đáp ứng quy chuẩn kỹ thuật quốc gia, được xem xét tích hợp trong hồ sơ thẩm định chung, không thiết lập thủ tục chứng nhận hoặc kiểm định độc lập theo Luật này.

9. Chính phủ quy định chi tiết nội dung, hồ sơ đánh giá tác động, chế độ kiểm toán định kỳ, đột xuất theo từng cấp độ rủi ro, chu kỳ kiểm thử xâm nhập, thời hạn gửi báo cáo kết quả kiểm toán và tiêu chí công nhận các tiêu chuẩn, chứng nhận quy định tại Điều này.

Điều 11. Thẩm định an ninh dữ liệu

1. Hồ sơ thiết kế hệ thống thông tin để lưu trữ, xử lý dữ liệu Cấp độ 4, Cấp độ 5 phải được thẩm định an ninh dữ liệu trước khi triển khai xây dựng hệ thống. Cấp độ được xác định theo dữ liệu mà hệ thống dự kiến lưu trữ, xử lý nêu trong hồ sơ thiết kế. Hệ thống chỉ được đưa vào vận hành chính thức sau khi có văn bản kết quả thẩm định đạt yêu cầu.

2. Thẩm quyền thẩm định được quy định như sau:

a) Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, Ban Cơ yếu Chính phủ thẩm định về an ninh dữ liệu đối với hệ thống xử lý dữ liệu Cấp độ 5, trừ trường hợp quy định tại điểm c khoản này;

b) Bộ Công an thẩm định về an ninh dữ liệu đối với hệ thống xử lý dữ liệu Cấp độ 4, trừ trường hợp quy định tại điểm c khoản này;

c) Bộ Quốc phòng thẩm định an ninh dữ liệu đối với hệ thống thông tin quân sự; Ban Cơ yếu Chính phủ thẩm định an ninh dữ liệu đối với hệ thống thông tin cơ yếu.

3. Chủ quản hệ thống thông tin xử lý dữ liệu Cấp độ 3 tự đánh giá, áp dụng biện pháp bảo vệ và lưu giữ hồ sơ theo quy định tại khoản 4 Điều 10 của Luật này, không phải thông báo.

4. Thẩm định an ninh dữ liệu được thực hiện một lần, đồng thời với thẩm định an ninh mạng trong một bộ hồ sơ, một quy trình theo pháp luật về an ninh mạng; cơ quan thẩm định ban hành một văn bản kết quả chung; thời hạn thẩm định an ninh dữ liệu không vượt quá thời hạn thẩm định an ninh mạng đối với cùng hệ thống. Hồ sơ đánh giá tác động quy định tại khoản 4 Điều 10, việc đánh giá sự phù hợp của sản phẩm, dịch vụ quy định tại khoản 8 Điều 10 và việc chuyển dữ liệu ra nước ngoài theo thiết kế của hệ thống được xem xét trong cùng hồ sơ thẩm định.

5. Trước khi đưa hệ thống vào vận hành chính thức, chủ quản hệ thống thông tin kiểm thử an ninh dữ liệu theo thiết kế đã được thẩm định và lưu giữ kết quả để xuất trình khi thanh tra, kiểm tra.

6. Hệ thống đang vận hành phải được thẩm định trong các trường hợp sau đây: dữ liệu được xác định lại lên Cấp độ 4, Cấp độ 5; nâng cấp, thay đổi trọng yếu làm thay đổi nơi lưu trữ, xử lý, nhà cung cấp hạ tầng, cơ chế quản lý khóa mật mã hoặc quyền truy cập từ bên ngoài đối với dữ liệu Cấp độ 4, Cấp độ 5. Đối với thay đổi khác, chủ quản hệ thống thông tin cập nhật hồ sơ, kiểm thử an ninh dữ liệu và lưu giữ kết quả. Hệ thống không phải tạm dừng vận hành trong thời gian thẩm định, trừ trường hợp quy định tại khoản 8 Điều này.

7. Cơ quan, người thực hiện thẩm định, kiểm tra có trách nhiệm bảo mật thông tin kỹ thuật, bí mật kinh doanh, bí mật công nghệ của tổ chức, cá nhân; không được yêu cầu bàn giao mã nguồn, trọng số mô hình trí tuệ nhân tạo, trừ trường hợp phục vụ khởi tố, điều tra vụ án hình sự theo pháp luật về tố tụng hình sự.

8. Chủ quản hệ thống thông tin có trách nhiệm khai báo trung thực cấp độ rủi ro, cung cấp đầy đủ hồ sơ và thực hiện kết luận thẩm định. Trường hợp có ý khai báo sai cấp độ nhằm né tránh thẩm định hoặc đưa hệ thống vào vận hành khi chưa có văn bản kết quả thẩm định đạt yêu cầu, cơ quan có thẩm quyền thẩm định quyết định bằng văn bản tạm dừng vận hành phần hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5 chưa được thẩm định cho đến khi hoàn thành thẩm định; không tạm dừng phần hệ thống không liên quan.

9. Chính phủ quy định chi tiết thành phần hồ sơ thiết kế, hồ sơ hiện trạng, danh mục thay đổi trọng yếu, trình tự, thủ tục, thời hạn thẩm định quy định tại Điều này.

Chương III

BẢO VỆ AN NINH DỮ LIỆU TRONG CHUYỂN ĐỔI SỐ, HẠ TẦNG SỐ, KHÔNG GIAN MỚI, CÔNG NGHỆ MỚI VÀ HOẠT ĐỘNG XUYỀN BIÊN GIỚI

Điều 12. Bảo vệ an ninh dữ liệu trong chuyển đổi số

1. Cơ quan, tổ chức chủ trì chương trình, dự án, nhiệm vụ chuyển đổi số, hệ thống số có trách nhiệm xác định cấp độ rủi ro của dữ liệu được xử lý và phương án bảo vệ an ninh dữ liệu từ khâu thiết kế; thực hiện quy định tại Điều 10 và Điều 11 của Luật này trước khi đưa hệ thống vào vận hành chính thức.

2. Cấp độ rủi ro của hệ thống số, nền tảng số được xác định theo dữ liệu có cấp độ rủi ro cao nhất được xử lý trên hệ thống, nền tảng đó; trường hợp dữ liệu được phân vùng, cách ly theo tiêu chuẩn, quy chuẩn kỹ thuật thì xác định theo từng phân vùng.

3. Dữ liệu hình thành từ việc số hóa hồ sơ, tài liệu được bảo vệ theo cấp độ rủi ro của hồ sơ, tài liệu gốc.

4. Cơ quan, tổ chức sử dụng hạ tầng dùng chung đạt mức bảo đảm theo cấp độ rủi ro của dữ liệu không phải đầu tư hạ tầng riêng.

5. Chính phủ quy định chi tiết yêu cầu bảo đảm an ninh dữ liệu từ khâu thiết kế quy định tại khoản 1 và yêu cầu kỹ thuật về phân vùng, cách ly dữ liệu quy định tại khoản 2 Điều này.

Điều 13. Bảo vệ an ninh dữ liệu đối với hạ tầng số, hệ thống vật lý - số và không gian mới

1. Doanh nghiệp cung cấp dịch vụ viễn thông, Internet, viễn thông vệ tinh, trung tâm dữ liệu, điện toán đám mây có trách nhiệm sau đây:

a) Bảo đảm an ninh dữ liệu trong phạm vi dịch vụ và theo phân định trách nhiệm tại hợp đồng với khách hàng;

b) Bảo đảm khách hàng nhận lại, di chuyển dữ liệu khi chấm dứt hợp đồng; không lưu giữ bản sao dữ liệu của khách hàng sau thời hạn chuyển giao dữ liệu theo hợp đồng, trừ trường hợp pháp luật có quy định khác;

c) Không truy cập nội dung dữ liệu của khách hàng, trừ trường hợp được khách hàng đồng ý, để khắc phục sự cố kỹ thuật hoặc theo yêu cầu của cơ quan có thẩm quyền theo quy định của pháp luật;

d) Phối hợp bảo toàn nhật ký sự kiện an ninh, chứng cứ điện tử và ứng phó sự cố;

đ) Đối với dữ liệu Cấp độ 5 lưu trữ, xử lý trên hạ tầng của doanh nghiệp, bảo đảm khóa giải mã do chủ quản dữ liệu quản lý tại Việt Nam; doanh nghiệp không nắm giữ, không có khả năng truy cập khóa giải mã và nội dung dữ liệu; không cung cấp, không cho phép tiếp cận dữ liệu theo yêu cầu của cơ quan, tổ chức nước ngoài, kể cả yêu cầu theo pháp luật nước ngoài có hiệu lực ngoài lãnh thổ.

2. Trách nhiệm của doanh nghiệp quy định tại khoản 1 Điều này được giới hạn trong phạm vi kiểm soát kỹ thuật được xác định trong hợp đồng dịch vụ. Chủ quản dữ liệu chịu trách nhiệm xác định cấp độ rủi ro, mục đích xử lý và biện pháp bảo vệ đối với nội dung dữ liệu.

3. Thủ tướng Chính phủ ban hành danh mục hạ tầng dữ liệu quốc gia trọng yếu theo đề nghị của Bộ Công an; đối với hạ tầng thuộc lĩnh vực quốc phòng, theo đề nghị của Bộ Quốc phòng.

4. Cơ quan, tổ chức quản lý, vận hành hạ tầng dữ liệu quốc gia trọng yếu thực hiện thẩm định an ninh dữ liệu theo quy định tại Điều 11, kiểm soát chuỗi cung ứng theo quy định tại Điều 18, chủ động giám sát, phát hiện nguy cơ theo quy định tại khoản 1 Điều 22, bảo đảm khả năng chống chịu, phục hồi theo quy định tại khoản 7 Điều 9 của Luật này và tổ chức diễn tập ứng phó sự cố hằng năm. Doanh nghiệp cung cấp dịch vụ trung tâm dữ liệu, điện toán đám mây cho hạ tầng dữ liệu quốc gia trọng yếu tham gia diễn tập, chia sẻ thông tin sự cố với cơ quan, tổ chức quản lý hạ tầng đó trong phạm vi dịch vụ.

5. Bộ Công an chủ trì, phối hợp với bộ quản lý ngành, lĩnh vực đánh giá khả năng chống chịu, phục hồi của hạ tầng dữ liệu quốc gia trọng yếu theo kế hoạch hằng năm, cùng đợt kiểm tra định kỳ quy định tại khoản 11 Điều 26 của Luật này; Bộ Quốc phòng chủ trì đối với hạ tầng thuộc lĩnh vực quốc phòng. Cơ quan đánh giá sử dụng kết quả kiểm toán, diễn tập đã thực hiện hợp lệ, không yêu cầu thực hiện lại.

6. Trường hợp hạ tầng dữ liệu quốc gia trọng yếu đồng thời là công trình quan trọng liên quan đến an ninh quốc gia thì việc bảo vệ công trình thực hiện theo pháp luật về bảo vệ công trình quan trọng liên quan đến an ninh quốc gia, việc bảo vệ an ninh dữ liệu thực hiện theo Luật này; kết quả thẩm định, kiểm tra được sử dụng chung, không thực hiện lại đối với cùng một nội dung.

7. Chủ quản hệ thống vật lý - số, hệ thống điều khiển tự động vận hành lưới điện, nhà máy, giao thông và hạ tầng thiết yếu khác theo tiêu chí do Chính phủ quy định có trách nhiệm áp dụng biện pháp kiểm soát tính nguyên vẹn, xác thực nguồn gốc đối với dữ liệu điều khiển, dữ liệu cảm biến, tham số hệ thống; phát hiện, ngăn chặn hành vi quy định tại khoản 1 và khoản 2 Điều 6 của Luật này.

8. Chủ quản hệ thống quy định tại khoản 7 Điều này và chủ quản dữ liệu đo xa, điều khiển, định vị, dẫn đường, đồng bộ thời gian phải xác thực nguồn dữ liệu và lệnh điều khiển; kiểm soát quyền truy cập đặc quyền, khóa mật mã và thay đổi cấu hình; khi chuyển giao quyền điều khiển, thay đổi chủ thể vận hành hoặc loại bỏ hệ thống phải thu hồi quyền truy cập và thu hồi, vô hiệu hóa hoặc chuyển giao khóa mật mã. Nghĩa vụ quy định tại khoản 7 và khoản này được áp dụng không phụ thuộc cấp độ rủi ro của dữ liệu khi việc dữ liệu bị giả mạo, làm sai lệch có khả năng trực tiếp làm mất quyền điều khiển hoặc làm sai lệch vị trí, thời gian, trạng thái vận hành của hệ thống.

9. Dữ liệu đo xa, theo dõi, điều khiển, định vị, dẫn đường, đồng bộ thời gian phát sinh từ hoạt động trong không gian mới thuộc quyền tài phán của Việt Nam

được bảo vệ theo cấp độ rủi ro; việc chuyển dữ liệu này ra nước ngoài thực hiện theo quy định tại Điều 19 của Luật này. Quy định tại khoản này không thay thế quản lý chuyên ngành về phương tiện bay, vệ tinh, tần số vô tuyến điện và không làm phát sinh giấy phép, đăng ký hoặc thủ tục chuyên ngành mới.

10. Việc xử lý dữ liệu trên vệ tinh, phương tiện tự động hoặc nền tảng đặt ngoài lãnh thổ Việt Nam không miễn trừ nghĩa vụ theo Luật này đối với chủ thể thuộc phạm vi áp dụng quy định tại Điều 1 của Luật này. Chủ quản hệ thống quản lý rủi ro tại giao diện giữa thành phần không gian, mặt đất, trung tâm điều khiển, hạ tầng điện toán đám mây và bên thứ ba theo quy định tại Điều 18 của Luật này.

11. Chính phủ quy định chi tiết Điều này, bao gồm thời gian phục hồi tối đa đối với hạ tầng dữ liệu quốc gia trọng yếu, tiêu chí nhận diện lĩnh vực trọng yếu, hệ thống vật lý - số; không làm phát sinh thủ tục hành chính ngoài thủ tục quy định tại Luật này.

Điều 14. Bảo vệ an ninh dữ liệu trong xử lý dữ liệu quy mô lớn

1. Xử lý dữ liệu quy mô lớn là việc xử lý tập dữ liệu đạt ngưỡng về số lượng chủ thể dữ liệu, dung lượng hoặc tần suất xử lý do Chính phủ quy định.

2. Tổ chức, cá nhân xử lý dữ liệu quy mô lớn có trách nhiệm sau đây:

a) Trường hợp dữ liệu có dữ liệu cá nhân, sử dụng hồ sơ đánh giá tác động xử lý dữ liệu cá nhân theo pháp luật về bảo vệ dữ liệu cá nhân, không lập hồ sơ riêng theo Luật này; trường hợp dữ liệu từ Cấp độ 3 trở lên, thực hiện đánh giá tác động theo quy định tại Điều 10 của Luật này;

b) Mã hóa, khử nhận dạng hoặc giả danh hóa dữ liệu có khả năng định danh chủ thể trước khi kết hợp dữ liệu từ nhiều nguồn, trừ trường hợp việc định danh là mục đích hợp pháp của hoạt động xử lý;

c) Kiểm soát quyền truy cập, lưu giữ nhật ký sự kiện an ninh đối với quá trình xử lý;

d) Đánh giá lại cấp độ rủi ro theo quy định tại khoản 5 Điều 8 của Luật này khi kết hợp các tập dữ liệu tạo thành tập dữ liệu từ Cấp độ 3 trở lên.

3. Quy mô xử lý không làm thay đổi cấp độ rủi ro của dữ liệu kinh doanh nội bộ, dữ liệu kỹ thuật vận hành không chứa dữ liệu cá nhân nhạy cảm, không thuộc danh mục dữ liệu quan trọng, dữ liệu cốt lõi.

4. Chính phủ quy định chi tiết ngưỡng xác định xử lý dữ liệu quy mô lớn quy định tại khoản 1 Điều này.

Điều 15. Bảo vệ an ninh dữ liệu đối với công nghệ mới và trí tuệ nhân tạo

1. Công nghệ mới là công nghệ đang được nghiên cứu, thử nghiệm hoặc bắt đầu ứng dụng, làm phát sinh nguy cơ mới đối với an ninh dữ liệu, thuộc danh mục do Chính phủ quy định.

2. Tổ chức, cá nhân nghiên cứu, phát triển, cung cấp, triển khai công nghệ mới, hệ thống trí tuệ nhân tạo xử lý dữ liệu từ Cấp độ 3 trở lên có trách nhiệm sau đây:

- a) Tích hợp biện pháp bảo vệ an ninh dữ liệu từ khâu thiết kế;
- b) Bảo đảm dữ liệu huấn luyện, dữ liệu kiểm thử có nguồn gốc hợp pháp; kiểm soát tính nguyên vẹn, phòng, chống đầu độc dữ liệu;
- c) Áp dụng biện pháp kỹ thuật ngăn chặn việc trích xuất, suy ngược, tái tạo trái phép dữ liệu huấn luyện thông qua truy vấn, khai thác mô hình;
- d) Kiểm soát quyền truy cập, lưu giữ nhật ký sự kiện an ninh đối với dữ liệu huấn luyện;
- đ) Cô lập, khắc phục và báo cáo sự cố theo quy định tại Điều 22 của Luật này;
- e) Đối với hệ thống trí tuệ nhân tạo được cấp quyền tự động lập kế hoạch, quyết định hoặc thực hiện hành động trên hệ thống xử lý dữ liệu từ Cấp độ 3 trở lên mà không cần phê duyệt của con người đối với từng hành động: định danh riêng hệ thống, phân quyền ở mức tối thiểu để thực hiện nhiệm vụ được giao, giới hạn phạm vi hành động, ghi nhật ký sự kiện an ninh và bảo đảm con người có thể can thiệp, tạm dừng, thu hồi quyền;
- g) Kiểm thử an ninh dữ liệu trước khi triển khai và khi có thay đổi trọng yếu theo tiêu chí do Chính phủ quy định đối với hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5; kết quả kiểm thử hợp lệ theo pháp luật về trí tuệ nhân tạo được sử dụng lại.

3. Đánh giá an ninh dữ liệu đối với hệ thống trí tuệ nhân tạo được tích hợp trong hồ sơ đánh giá rủi ro theo pháp luật về trí tuệ nhân tạo; không lập hồ sơ riêng, không tổ chức thẩm định riêng. Bộ Công an tham gia về nội dung an ninh dữ liệu trong quy trình kiểm thử, thử nghiệm có kiểm soát do cơ quan có thẩm quyền theo pháp luật về trí tuệ nhân tạo chủ trì đối với hệ thống xử lý dữ liệu từ Cấp độ 3 trở lên.

4. Dữ liệu dẫn xuất được tạo ra từ dữ liệu từ Cấp độ 3 trở lên, bao gồm trọng số mô hình, tham số thuật toán, dữ liệu tổng hợp, được bảo vệ theo quy định tại khoản 4 Điều 9 của Luật này; trường hợp dữ liệu gốc chứa dữ liệu cốt lõi, bí mật nhà nước thì dữ liệu dẫn xuất được bảo vệ theo cấp độ của dữ liệu gốc. Việc chuyển các sản phẩm này ra nước ngoài thực hiện theo quy định tại Điều 19 của Luật này.

5. Trường hợp hệ thống trí tuệ nhân tạo bị đầu độc dữ liệu dẫn đến kết quả đầu ra đe dọa trực tiếp an ninh quốc gia, chủ quyền, lãnh thổ của Việt Nam, cơ quan chuyên trách bảo vệ an ninh dữ liệu yêu cầu bằng văn bản tổ chức, cá nhân khắc phục trong thời hạn không quá 72 giờ; hết thời hạn mà không khắc phục thì áp dụng biện pháp kỹ thuật khẩn cấp theo quy định tại Điều 23 của Luật này. Việc kiểm tra thực hiện theo quy định tại khoản 11 Điều 26 của Luật này.

6. Hệ thống trí tuệ nhân tạo phục vụ hoạt động quốc phòng, an ninh, cơ yếu phải đáp ứng các yêu cầu sau đây, không phụ thuộc cấp độ rủi ro của dữ liệu được xử lý:

- a) Con người giám sát, kiểm soát và chịu trách nhiệm cuối cùng đối với quyết định, hành động của hệ thống; hệ thống không được tự quyết định việc áp dụng biện pháp hạn chế quyền con người, quyền công dân hoặc biện pháp cưỡng chế;

b) Không vận hành trên hệ thống, dịch vụ trí tuệ nhân tạo công cộng hoặc hạ tầng của bên thứ ba, trừ trường hợp được Bộ Công an, Bộ Quốc phòng cho phép theo phạm vi quản lý và có biện pháp bảo vệ theo cấp độ rủi ro của dữ liệu được xử lý;

c) Mô hình, công cụ, thư viện, dữ liệu có nguồn gốc nước ngoài hoặc không kiểm chứng được nguồn gốc phải được đánh giá khả năng chứa chức năng ẩn, bị đầu độc dữ liệu và khả năng truyền dữ liệu ra ngoài phạm vi kiểm soát trước khi sử dụng;

d) Được đánh giá an ninh dữ liệu trước khi đưa vào sử dụng và khi có thay đổi làm gia tăng rủi ro; tham số mô hình được huấn luyện, tinh chỉnh từ dữ liệu chứa bí mật nhà nước được quản lý theo chế độ bảo vệ bí mật nhà nước tương ứng, trừ trường hợp kết quả đánh giá kỹ thuật xác định tham số không còn khả năng tái tạo, suy diễn ngược hoặc làm lộ dữ liệu đó.

7. Bộ Công an hướng dẫn, kiểm tra việc thực hiện khoản 6 Điều này đối với hoạt động phục vụ an ninh quốc gia, trật tự, an toàn xã hội; Bộ Quốc phòng thực hiện đối với hoạt động quốc phòng và hoạt động cơ yếu; Ban Cơ yếu Chính phủ tổ chức thực hiện trong phạm vi quản lý.

8. Chính phủ quy định chi tiết danh mục công nghệ mới và yêu cầu kỹ thuật quy định tại Điều này.

Điều 16. Mật mã an ninh

1. Mật mã an ninh là hệ thống sản phẩm, giải pháp kỹ thuật mã hóa do Bộ Công an quản lý để bảo vệ dữ liệu, bí mật nhà nước phục vụ bảo đảm an ninh quốc gia và trật tự, an toàn xã hội.

2. Nhà nước ưu tiên nguồn lực đầu tư nghiên cứu, phát triển, thử nghiệm và làm chủ công nghệ mật mã an ninh nhằm nâng cao năng lực tự chủ quốc gia về mật mã.

3. Mật mã an ninh bảo vệ dữ liệu không thuộc phạm vi bí mật nhà nước được thực hiện theo cơ chế tự nguyện; cơ quan, tổ chức, doanh nghiệp, cá nhân được tự lựa chọn sử dụng các sản phẩm, dịch vụ mật mã an ninh thuộc Danh mục do Bộ Công an công bố để bảo vệ dữ liệu và hệ thống thông tin theo nhu cầu.

4. Mật mã an ninh bảo vệ bí mật nhà nước được thực hiện như sau:

a) Bộ Công an sử dụng mật mã an ninh bảo vệ dữ liệu bí mật nhà nước thuộc thẩm quyền quản lý, hệ thống thông tin nghiệp vụ và cơ sở dữ liệu chuyên ngành phục vụ công tác bảo đảm an ninh, trật tự theo lộ trình;

b) Bộ Công an chủ trì, phối hợp với các cơ quan liên quan đánh giá hiệu quả, tính an toàn, khả năng tương thích, lấy ý kiến bằng văn bản của Bộ Quốc phòng và báo cáo Thủ tướng Chính phủ xem xét, quyết định việc mở rộng phạm vi sử dụng mật mã an ninh bảo vệ bí mật nhà nước ngoài phạm vi Công an nhân dân.

5. Chính phủ quy định chi tiết Điều này.

Điều 17. Mật mã kháng lượng tử và mật mã lượng tử

1. Mật mã kháng lượng tử là giải pháp mật mã được thiết kế để bảo đảm dữ liệu an toàn trước các phương pháp tấn công bằng máy tính lượng tử. Nhà nước ưu

tiên đầu tư nghiên cứu, làm chủ công nghệ và định hướng lộ trình chuyển đổi sang mật mã kháng lượng tử phù hợp với sự phát triển công nghệ.

2. Việc ưu tiên chuyển đổi sang mật mã kháng lượng tử hoặc áp dụng mô hình mã hóa kết hợp được áp dụng đối với hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống xử lý dữ liệu từ Cấp độ 3 trở lên của cơ quan nhà nước, lực lượng vũ trang và các hệ thống quản lý dữ liệu có thời hạn bảo mật dài hạn. Hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5 đầu tư mới hoặc nâng cấp phải bảo đảm khả năng thay thế linh hoạt thành phần mật mã mà không phải thay thế toàn bộ hệ thống.

3. Chủ quản hệ thống quy định tại khoản 2 Điều này có trách nhiệm duy trì danh mục cấu phần mật mã phục vụ quản trị rủi ro; không phải thực hiện thủ tục đăng ký hoặc báo cáo định kỳ cho cơ quan nhà nước, chỉ cung cấp thông tin liên quan theo yêu cầu bằng văn bản khi xảy ra sự cố hoặc khi thanh tra, kiểm tra.

4. Nhà nước khuyến khích tổ chức, doanh nghiệp, đặc biệt là các lĩnh vực tài chính, ngân hàng, thương mại điện tử và dịch vụ xác thực điện tử chủ động áp dụng mật mã kháng lượng tử; có chính sách hỗ trợ kỹ thuật cho doanh nghiệp nhỏ và vừa, đồng thời bảo đảm kinh phí từ ngân sách nhà nước đối với hệ thống của cơ quan nhà nước theo phân cấp.

5. Việc triển khai ứng dụng mật mã lượng tử chính thức phải thông qua quá trình kiểm thử, đánh giá độc lập về mức độ an toàn, khả năng tương thích và vận hành.

6. Chính phủ quy định chi tiết danh mục hệ thống thuộc diện chuyển đổi, lộ trình, yêu cầu kỹ thuật và thời hạn thực hiện theo từng giai đoạn trên cơ sở năng lực công nghệ và đánh giá chi phí - lợi ích; bảo đảm không buộc chuyển đổi đồng loạt khi chưa đủ điều kiện kỹ thuật.

Điều 18. Bảo vệ an ninh dữ liệu trong chuỗi cung ứng sản phẩm, dịch vụ dữ liệu

1. Chủ quản dữ liệu chịu trách nhiệm kiểm soát an ninh dữ liệu trong chuỗi cung ứng sản phẩm, dịch vụ dữ liệu tương ứng với cấp độ rủi ro của dữ liệu.

2. Chủ quản dữ liệu giao bên xử lý dữ liệu thực hiện xử lý dữ liệu vẫn chịu trách nhiệm đối với nghĩa vụ thuộc phạm vi quản lý, quyết định của mình. Bên xử lý dữ liệu chịu trách nhiệm đối với nghĩa vụ, hành vi thuộc phạm vi được giao hoặc do mình trực tiếp thực hiện. Trách nhiệm của các bên được phân định theo quy định của Luật này và hợp đồng.

3. Sản phẩm, dịch vụ dữ liệu khi đưa vào chuỗi cung ứng phải bảo đảm các yêu cầu an ninh dữ liệu sau đây:

a) Không chứa tính năng ẩn, công hậu hoặc mã độc để tự động trích xuất, sao chép hoặc phát tán dữ liệu trái phép;

b) Dữ liệu từ Cấp độ 3 trở lên lưu trữ, truyền tải trong chuỗi cung ứng phải được mã hóa, phân quyền truy cập và ghi nhật ký sự kiện an ninh;

c) Sản phẩm, dịch vụ kết nối, tiếp cận dữ liệu từ Cấp độ 3 trở lên đã được đánh giá, kiểm tra an ninh mạng theo quy định của pháp luật về an ninh mạng trước khi kết nối vào hệ thống dữ liệu.

4. Chủ quản dữ liệu từ Cấp độ 3 trở lên có trách nhiệm sau đây:

a) Xác định phạm vi dữ liệu, giới hạn quyền truy cập và đánh giá rủi ro an ninh dữ liệu đối với bên cung cấp sản phẩm, dịch vụ dữ liệu trước khi kết nối;

b) Quy định cụ thể nghĩa vụ bảo mật dữ liệu, phạm vi xử lý dữ liệu và chế tài xử lý khi để rò rỉ dữ liệu trong hợp đồng, thỏa thuận cung cấp dịch vụ;

c) Giám sát việc truy cập dữ liệu của bên cung cấp; dừng kết nối và thu hồi ngay quyền truy cập dữ liệu khi phát hiện nguy cơ hoặc sự cố an ninh dữ liệu;

d) Đối với hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5, việc truy cập từ xa của bên cung cấp phải được chủ quản dữ liệu phê duyệt, giám sát, ghi nhận ký và không cho phép sao chép, trích xuất dữ liệu; bên cung cấp ở nước ngoài không được truy cập trực tiếp hệ thống xử lý dữ liệu cấm chuyển ra nước ngoài quy định tại khoản 5 Điều 19 của Luật này; việc truy cập từ nước ngoài làm tiếp cận nội dung dữ liệu thực hiện theo quy định tại Điều 19 của Luật này.

5. Chủ quản dữ liệu Cấp độ 1, Cấp độ 2 tự thỏa thuận với bên cung cấp về biện pháp bảo vệ; khi phát hiện nguy cơ, sự cố an ninh dữ liệu thì dừng kết nối, thu hồi quyền truy cập của bên cung cấp.

6. Bên cung cấp sản phẩm, dịch vụ dữ liệu có trách nhiệm sau đây:

a) Chỉ xử lý dữ liệu đúng phạm vi, mục đích đã thỏa thuận trong hợp đồng;

b) Bàn giao hoặc tiêu hủy toàn bộ dữ liệu, không lưu bản sao dưới bất kỳ hình thức nào khi kết thúc hợp đồng, thỏa thuận cung cấp dịch vụ, trừ trường hợp pháp luật có quy định khác;

c) Thông báo ngay cho chủ quản dữ liệu khi phát hiện hành vi truy cập trái phép hoặc nguy cơ lộ, rò rỉ dữ liệu thuộc phạm vi sản phẩm, dịch vụ cung cấp;

d) Chỉ giao cho bên thứ ba xử lý dữ liệu từ Cấp độ 3 trở lên khi được chủ quản dữ liệu đồng ý bằng văn bản và ràng buộc bên thứ ba nghĩa vụ bảo vệ không thấp hơn nghĩa vụ của mình.

7. Chính phủ quy định chi tiết Điều này.

Điều 19. Bảo vệ an ninh dữ liệu trong chuyển, xử lý dữ liệu xuyên biên giới

1. Các trường hợp sau đây không tính là hoạt động chuyển, xử lý dữ liệu xuyên biên giới:

a) Truyền dẫn qua hệ thống kỹ thuật mà bên ở nước ngoài không có quyền truy cập, lưu trữ;

b) Lưu trữ dữ liệu Cấp độ 3, Cấp độ 4 ở nước ngoài nhưng đã được mã hóa theo quy chuẩn kỹ thuật, trong đó khóa giải mã do chủ quản dữ liệu quản lý tại Việt Nam và bên nước ngoài không nắm giữ, không kiểm soát;

c) Mang dữ liệu ra nước ngoài hoặc truy cập từ nước ngoài theo quy định tại khoản 10 Điều này.

2. Việc chuyển, xử lý dữ liệu xuyên biên giới phải bảo đảm không xâm phạm 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 từ Cấp độ 3 trở lên phải được mã hóa, phân quyền truy cập và ghi nhật ký truyền dữ liệu theo quy chuẩn kỹ thuật về an ninh dữ liệu.

3. Việc quản lý chuyển, xử lý dữ liệu xuyên biên giới được thực hiện theo cấp độ rủi ro:

a) Dữ liệu Cấp độ 1 và Cấp độ 2 thực hiện theo pháp luật chuyên ngành có liên quan, không phải thực hiện thủ tục theo quy định của Luật này;

b) Chủ quản dữ liệu Cấp độ 3 tự đánh giá an ninh dữ liệu trước khi thực hiện và lưu giữ hồ sơ phục vụ công tác thanh tra, kiểm tra;

c) Chủ quản dữ liệu Cấp độ 4 và Cấp độ 5 chỉ được thực hiện sau khi có văn bản thẩm định, chấp thuận của cơ quan chuyên trách bảo vệ an ninh dữ liệu;

d) Dữ liệu cấm chuyển xuyên biên giới thực hiện theo quy định tại khoản 5 Điều này.

4. Việc thẩm định, chấp thuận chuyển, xử lý dữ liệu Cấp độ 4 và Cấp độ 5 xuyên biên giới thực hiện theo nguyên tắc: Cơ quan chuyên trách bảo vệ an ninh dữ liệu chủ trì thẩm định dựa trên mục đích, phạm vi, mức độ tác động đến quốc phòng, an ninh quốc gia, bên nhận và biện pháp bảo vệ dữ liệu; đối với dữ liệu Cấp độ 5, phải lấy ý kiến bằng văn bản của Bộ Quốc phòng hoặc Bộ Công an theo phân công quản lý. Văn bản chấp thuận có giá trị áp dụng đối với luồng dữ liệu đã được phê duyệt cho đến khi có thay đổi về mục đích, loại dữ liệu, bên nhận hoặc biện pháp bảo vệ.

5. Dữ liệu cấm chuyển xuyên biên giới được quản lý như sau:

a) Nghiêm cấm chuyển, xử lý xuyên biên giới, cung cấp hoặc cho phép bên nước ngoài truy cập đối với dữ liệu Cấp độ 5 đặc biệt quan trọng về quốc phòng, an ninh quốc gia, chủ quyền lãnh thổ theo danh mục cốt lõi do Thủ tướng Chính phủ quyết định trên cơ sở đề nghị của Bộ trưởng Bộ Công an và Bộ trưởng Bộ Quốc phòng;

b) Thủ tướng Chính phủ quyết định trường hợp đặc biệt vì lợi ích quốc phòng, an ninh quốc gia, đối ngoại hoặc thực hiện điều ước quốc tế, thỏa thuận hợp tác quốc phòng, an ninh đã được phê duyệt;

c) Chủ quản dữ liệu có trách nhiệm chấm dứt hoạt động chuyển, xử lý trái quy định ngay sau khi nhận được thông báo từ cơ quan có thẩm quyền.

6. Việc chuyển dữ liệu cá nhân xuyên biên giới tuân thủ pháp luật về bảo vệ dữ liệu cá nhân, được tích hợp gọn trong hồ sơ tự đánh giá an ninh (đối với Cấp độ 3) hoặc hồ sơ thẩm định chung (đối với Cấp độ 4, Cấp độ 5) qua hệ thống điện tử thống nhất.

7. Trường hợp chuyển dữ liệu Cấp độ 3 và Cấp độ 4 thực sự cần thiết trong tình huống khẩn cấp để bảo vệ tính mạng, sức khỏe, tài sản, hoặc để thực hiện quan hệ lao động, hợp đồng mà chủ thể dữ liệu là một bên thì được miễn thủ tục hành chính sơ bộ; chủ quản dữ liệu chỉ cần lưu giữ hồ sơ giải trình phục vụ thanh tra, kiểm tra.

8. Chủ quản dữ liệu trong hoạt động chuyển, xử lý dữ liệu xuyên biên giới có trách nhiệm:

a) Xác định đúng cấp độ rủi ro và áp dụng biện pháp bảo vệ tương ứng trước khi thực hiện;

b) Kiểm soát chặt chẽ luồng dữ liệu; chủ động tạm dừng khi phát hiện nguy cơ xâm phạm an ninh quốc gia hoặc sự cố an ninh dữ liệu và thực hiện chế độ báo cáo theo quy định;

c) Cung cấp thông tin kỹ thuật liên quan trực tiếp khi có yêu cầu bằng văn bản từ cơ quan chuyên trách bảo vệ an ninh dữ liệu.

9. Người đứng đầu cơ quan chuyên trách bảo vệ an ninh dữ liệu thuộc Bộ Công an, Bộ Quốc phòng có thẩm quyền quyết định tạm dừng hoặc đình chỉ việc chuyển, xử lý dữ liệu xuyên biên giới khi có vi phạm pháp luật, có nguy cơ trực tiếp đe dọa nghiêm trọng chủ quyền, an ninh quốc gia hoặc không khắc phục các yêu cầu bảo đảm an ninh dữ liệu. Quyết định tạm dừng, đình chỉ phải xác định rõ phạm vi, thời hạn và bảo đảm quyền giải trình, khiếu nại của tổ chức, cá nhân theo quy định pháp luật.

10. Việc mang dữ liệu ra nước ngoài trên thiết bị, phương tiện lưu trữ hoặc truy cập từ nước ngoài để phục vụ công tác chuyên môn, sản xuất, kinh doanh được phân cấp quản lý rõ ràng theo quy chế nội bộ (đối với Cấp độ 1, 2), sự cho phép của người đứng đầu (đối với Cấp độ 3, 4 và Cấp độ 5 không thuộc diện cấm) hoặc văn bản cho phép đặc thù đối với dữ liệu cấm, gắn liền với nghĩa vụ bảo mật, mã hóa và báo cáo sự cố khi thiết bị thất lạc.

11. Cơ quan đại diện nước Cộng hòa xã hội chủ nghĩa Việt Nam ở nước ngoài và các cơ quan, tổ chức Việt Nam hoạt động ở nước ngoài tự áp dụng phương án bảo đảm an ninh dữ liệu theo hướng dẫn của cơ quan quản lý chuyên ngành.

12. Chính phủ quy định chi tiết hồ sơ, trình tự thẩm định, chấp thuận; tiêu chí xác định dữ liệu cấm chuyển xuyên biên giới; quy trình tạm dừng, đình chỉ; quy chuẩn kỹ thuật về mã hóa và quản lý khóa mật mã; không quy định thêm thủ tục hoặc điều kiện hành chính đối với dữ liệu Cấp độ 1, Cấp độ 2 và Cấp độ 3 ngoài các nguyên tắc đã được Luật này quy định.

Điều 20. Yêu cầu cung cấp dữ liệu từ nước ngoài và dịch vụ xuyên biên giới

1. Việc cung cấp dữ liệu từ Cấp độ 3 trở lên thuộc quyền tài phán của Việt Nam theo yêu cầu của cơ quan tư pháp, cơ quan thực thi pháp luật nước ngoài phải tuân thủ pháp luật về tương trợ tư pháp hoặc điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

2. Tổ chức, cá nhân khi nhận được yêu cầu trực tiếp từ nước ngoài quy định tại khoản 1 Điều này không được tự ý cung cấp mà phải báo cáo cơ quan chuyên trách bảo vệ an ninh dữ liệu để được hướng dẫn, xử lý và giải quyết xung đột nghĩa vụ pháp lý. Việc từ chối cung cấp dữ liệu để tuân thủ quy định này không bị coi là vi phạm pháp luật Việt Nam.

3. Tổ chức, cá nhân nước ngoài cung cấp dịch vụ xuyên biên giới có hoạt động xử lý dữ liệu từ Cấp độ 3 trở lên thuộc quyền tài phán của Việt Nam phải chỉ định đại diện hợp pháp hoặc đầu mối liên lạc tại Việt Nam để thực hiện các nghĩa vụ bảo đảm an ninh dữ liệu theo quy định của Luật này; được sử dụng đại diện, đầu mối đã chỉ định theo pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân.

4. Biện pháp kỹ thuật hạn chế, tạm dừng dịch vụ xuyên biên giới được áp dụng đối với tổ chức, cá nhân vi phạm các quy định về an ninh dữ liệu sau khi đã được yêu cầu bằng văn bản nhưng không khắc phục; thời hạn khắc phục ghi trong văn bản yêu cầu không ít hơn 15 ngày. Thủ trưởng cơ quan chuyên trách bảo vệ an ninh dữ liệu quyết định hạn chế đối với chức năng, dịch vụ có vi phạm; Bộ trưởng Bộ Công an quyết định tạm dừng toàn bộ dịch vụ. Thời hạn áp dụng biện pháp không quá 90 ngày.

5. Việc áp dụng biện pháp quy định tại khoản 4 Điều này phải tuân thủ các nguyên tắc sau đây:

- a) Chỉ áp dụng đối với phạm vi dịch vụ, chức năng có hành vi vi phạm;
- b) Được rà soát định kỳ và phải chấm dứt ngay khi vi phạm đã được khắc phục;
- c) Tổ chức, cá nhân bị áp dụng được thông báo, có quyền giải trình trước khi quyết định và có quyền khiếu nại, khởi kiện theo quy định của pháp luật.

6. Chính phủ quy định chi tiết trình tự, thủ tục, chu kỳ rà soát biện pháp kỹ thuật quy định tại khoản 4 Điều này, thời hạn báo cáo và thời hạn xử lý báo cáo, cơ chế phối hợp đối với yêu cầu cung cấp dữ liệu từ nước ngoài quy định tại khoản 1 và khoản 2 Điều này.

Điều 21. Đánh giá an ninh dữ liệu trong đầu tư, chuyển giao công nghệ

1. Việc xem xét yếu tố an ninh dữ liệu trong các hoạt động đầu tư, chuyển giao công nghệ, mua bán, sáp nhập, chuyển nhượng vốn được tích hợp vào các thủ tục hành chính hiện hành theo pháp luật về đầu tư, doanh nghiệp, cạnh tranh và chuyển giao công nghệ; không thiết lập thủ tục thẩm định hoặc cấp phép độc lập theo Luật này.

2. Cơ quan giải quyết thủ tục có trách nhiệm lấy ý kiến Bộ Công an, Bộ Quốc phòng đối với các giao dịch làm thay đổi quyền kiểm soát trực tiếp hoặc gián tiếp đối với doanh nghiệp quản lý dữ liệu từ Cấp độ 4 trở lên, hệ thống thông tin quan trọng về an ninh quốc gia hoặc hạ tầng dữ liệu quốc gia trọng yếu, bao gồm cả giao dịch thực hiện ngoài lãnh thổ Việt Nam đáp ứng tiêu chí do Chính phủ quy định tại khoản 6 Điều này.

3. Nội dung đánh giá an ninh dữ liệu tập trung vào các yếu tố: quyền tiếp cận dữ liệu, quản trị hệ thống, khả năng kiểm soát khóa mật mã, công nghệ lõi, khả năng chuyển đổi nhà cung cấp và mức độ phụ thuộc chiến lược về dữ liệu.

4. Việc lấy ý kiến và xử lý kết quả đánh giá được thực hiện theo nguyên tắc sau đây:

a) Phải được tiến hành trong thời hạn giải quyết thủ tục chung, không làm kéo dài thời gian giải quyết; ý kiến bằng văn bản của cơ quan được lấy ý kiến là căn cứ bắt buộc để xem xét, quyết định;

b) Trường hợp cơ quan được lấy ý kiến kết luận giao dịch có nguy cơ trực tiếp, nghiêm trọng đối với an ninh quốc gia mà cơ quan giải quyết thủ tục dự kiến quyết định khác, phải báo cáo Thủ tướng Chính phủ quyết định;

c) Nhà đầu tư, doanh nghiệp có liên quan được thông báo nội dung kiến nghị và có quyền giải trình trước khi cơ quan có thẩm quyền ra quyết định, trừ trường hợp liên quan đến bí mật nhà nước.

5. Kết quả đánh giá an ninh dữ liệu còn hiệu lực được kế thừa; việc lấy ý kiến không làm phát sinh nghĩa vụ kê khai, nộp hồ sơ độc lập ngoài các quy định của thủ tục đang giải quyết.

6. Chính phủ quy định chi tiết tiêu chí nhận diện giao dịch quy định tại khoản 2 Điều này, thời hạn phối hợp lấy ý kiến và cơ chế giải quyết.

Chương IV **ỨNG PHÓ SỰ CỐ** **VÀ BIỆN PHÁP KỸ THUẬT KHẢN CẤP BẢO VỆ AN NINH DỮ LIỆU**

Điều 22. Theo dõi, cảnh báo và ứng phó sự cố an ninh dữ liệu

1. Việc theo dõi và cảnh báo an ninh dữ liệu được thực hiện phân theo cấp độ rủi ro, như sau:

a) Chủ quản dữ liệu Cấp độ 1 và Cấp độ 2 tự chủ quản lý, không bắt buộc tổ chức theo dõi chuyên trách;

b) Chủ quản dữ liệu Cấp độ 3 tự tổ chức theo phương án bảo vệ an ninh dữ liệu của mình;

c) Chủ quản dữ liệu Cấp độ 4, Cấp độ 5 và hạ tầng dữ liệu quốc gia trọng yếu tự tổ chức theo dõi thường xuyên hoặc sử dụng dịch vụ chuyên nghiệp; chia sẻ chỉ báo tấn công và thông tin sự cố qua hệ thống điện tử thống nhất.

2. Cơ quan chuyên trách bảo vệ an ninh dữ liệu thực hiện phát hiện, cảnh báo sớm nguy cơ từ bên ngoài hệ thống; ban hành cảnh báo kịp thời theo tiêu chí do pháp luật quy định.

3. Chủ quản dữ liệu từ Cấp độ 3 trở lên có trách nhiệm khắc phục lỗ hổng, rủi ro đã được cảnh báo hoặc áp dụng biện pháp giảm thiểu thay thế, đồng thời lưu giữ kết quả để phục vụ công tác thanh tra, kiểm tra.

4. Thông tin thu thập từ hoạt động theo dõi, cảnh báo chỉ được sử dụng duy nhất cho mục đích bảo vệ an ninh dữ liệu, không được dùng làm căn cứ độc lập để xử phạt vi phạm hành chính hoặc hạn chế quyền hoạt động của tổ chức, cá nhân. Việc chia sẻ thông tin, báo cáo sự cố trung thực, đúng hạn là yếu tố được xem xét giảm nhẹ khi giải quyết vi phạm liên quan.

5. Khi phát hiện nguy cơ hoặc xảy ra sự cố an ninh dữ liệu, chủ quản dữ liệu phải lập tức kích hoạt biện pháp ngăn chặn, cô lập và khắc phục hậu quả nhằm bảo vệ tối đa tính bảo mật, tính nguyên vẹn và tính khả dụng của dữ liệu, đồng thời bảo vệ quyền lợi hợp pháp của chủ thể dữ liệu.

6. Chế độ báo cáo sự cố được thực hiện thông qua hệ thống điện tử thống nhất như sau:

a) Sự cố đối với dữ liệu từ Cấp độ 3 trở lên thực hiện báo cáo theo thời hạn do Chính phủ quy định phù hợp với mức độ nghiêm trọng;

b) Sự cố đối với dữ liệu Cấp độ 1 và Cấp độ 2 do chủ quản dữ liệu tự xử lý, lưu hồ sơ giải trình; trường hợp thuộc diện phải thông báo theo pháp luật về bảo vệ dữ liệu cá nhân thì thực hiện theo pháp luật chuyên ngành.

7. Trường hợp sự cố có khả năng ảnh hưởng trực tiếp đến quyền và lợi ích hợp pháp của tổ chức, cá nhân, chủ quản dữ liệu có trách nhiệm thông báo kịp thời về tính chất sự cố, loại dữ liệu bị ảnh hưởng và hướng dẫn biện pháp tự bảo vệ; bảo đảm không tiết lộ bí mật nhà nước hoặc làm lộ thêm dữ liệu. Việc thông báo cho chủ thể dữ liệu cá nhân tuân thủ pháp luật về bảo vệ dữ liệu cá nhân.

8. Công tác điều phối ứng cứu sự cố nghiêm trọng đe dọa an ninh dữ liệu quốc gia do cơ quan chuyên trách bảo vệ an ninh dữ liệu thuộc Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, Ban Cơ yếu Chính phủ và các cơ quan liên quan; trường hợp phát sinh vướng mắc liên ngành, báo cáo Thủ tướng Chính phủ quyết định.

9. Chính phủ quy định kế hoạch ứng phó sự cố an ninh dữ liệu quốc gia và tổ chức diễn tập liên ngành nhằm nâng cao năng lực ứng phó tổng thể.

10. Hoạt động truy vết, điều tra sự cố được thực hiện dựa trên cơ sở bảo đảm tính nguyên vẹn của nhật ký hệ thống và chứng cứ điện tử, không thay thế cho hoạt động điều tra theo pháp luật tố tụng hình sự.

11. Khi xử lý nguy cơ hoặc sự cố cụ thể, cơ quan chuyên trách được quyền yêu cầu cung cấp thông tin kỹ thuật liên quan trực tiếp. Thông tin cung cấp được bảo mật và chỉ dùng cho mục đích bảo vệ an ninh dữ liệu.

12. Sau khi kiểm soát sự cố, chủ quản dữ liệu chịu trách nhiệm kiểm tra toàn diện tính nguyên vẹn của dữ liệu trước khi đưa hệ thống trở lại vận hành bình thường.

13. Chính phủ quy định chi tiết việc phân loại cấp độ sự cố, tiêu chí nhận diện nguy cơ, chế độ báo cáo, trình tự yêu cầu thông tin và quy trình phục hồi dữ liệu.

Điều 23. Biện pháp kỹ thuật khẩn cấp

1. Biện pháp kỹ thuật khẩn cấp chỉ được áp dụng khi có một trong các căn cứ sau đây và việc chậm áp dụng sẽ gây thiệt hại khó khắc phục:

- a) Sự cố an ninh dữ liệu đang xảy ra làm lộ, mất, sai lệch dữ liệu Cấp độ 4, Cấp độ 5 hoặc làm gián đoạn hoạt động của hạ tầng dữ liệu quốc gia trọng yếu;
- b) Hành vi xâm phạm đang diễn ra đối với dữ liệu từ Cấp độ 3 trở lên, gây hoặc đe dọa trực tiếp gây thiệt hại đặc biệt nghiêm trọng đến an ninh quốc gia, trật tự, an toàn xã hội mà biện pháp của chủ quản dữ liệu không ngăn chặn được;
- c) Trường hợp quy định tại khoản 5 Điều 15 của Luật này.

2. Biện pháp kỹ thuật khẩn cấp bao gồm:

- a) Phong tỏa dữ liệu là việc giữ nguyên trạng, không cho sửa đổi, xóa, sao chép, di chuyển đối với tập dữ liệu xác định;
- b) Vô hiệu hóa quyền truy cập của tài khoản, thiết bị, kết nối xác định;
- c) Tạm dừng, ngăn chặn luồng truyền dữ liệu xác định;
- d) Tạm dừng vận hành một phần hoặc toàn bộ hệ thống thông tin, dịch vụ, mô hình trí tuệ nhân tạo bị xâm phạm hoặc bị đầu độc dữ liệu.

3. Biện pháp kỹ thuật khẩn cấp được áp dụng theo thứ tự từ biện pháp ít hạn chế quyền nhất; chỉ áp dụng đối với phần dữ liệu, hệ thống liên quan trực tiếp đến căn cứ áp dụng và chấm dứt ngay khi căn cứ áp dụng không còn. Không được áp dụng biện pháp kỹ thuật khẩn cấp để chuyển quyền sở hữu dữ liệu, xóa vĩnh viễn dữ liệu, thu giữ, phong tỏa tài sản hoặc đình chỉ toàn bộ hoạt động của tổ chức, cá nhân; cơ quan thực hiện không truy cập nội dung dữ liệu nếu không có căn cứ pháp luật riêng.

4. Thẩm quyền quyết định áp dụng được quy định như sau:

- a) Thủ trưởng cơ quan chuyên trách bảo vệ an ninh dữ liệu thuộc Bộ Công an, Bộ Quốc phòng quyết định áp dụng biện pháp quy định tại các điểm a, b và c khoản 2 Điều này;
- b) Bộ trưởng Bộ Công an, Bộ trưởng Bộ Quốc phòng quyết định áp dụng biện pháp quy định tại điểm d khoản 2 Điều này.

5. Quyết định áp dụng được thể hiện bằng văn bản, nêu rõ căn cứ; dữ liệu, hệ thống, tổ chức, cá nhân bị áp dụng; phạm vi, biện pháp và thời hạn áp dụng. Trường hợp cấp bách, người có thẩm quyền được ra lệnh bằng lời nói hoặc phương tiện điện tử và phải ban hành văn bản trong thời hạn 24 giờ kể từ khi ra lệnh.

6. Thời hạn áp dụng biện pháp kỹ thuật khẩn cấp không quá 30 ngày. Trường hợp căn cứ áp dụng vẫn còn, cấp trên trực tiếp của người ra quyết định được gia hạn không quá 02 lần, mỗi lần không quá 15 ngày.

7. Trong thời hạn 24 giờ kể từ khi quyết định áp dụng, người ra quyết định báo cáo bằng văn bản cấp trên trực tiếp.

8. Tổ chức, cá nhân bị áp dụng biện pháp kỹ thuật khẩn cấp có các quyền sau đây:

a) Được thông báo về quyết định áp dụng, trừ nội dung thuộc bí mật nhà nước, bí mật công tác điều tra; trường hợp phải hoãn thông báo để không làm vô hiệu biện pháp thì thông báo chậm nhất 72 giờ kể từ khi kết thúc biện pháp;

b) Kiến nghị bằng văn bản với người ra quyết định hoặc cấp trên trực tiếp; cơ quan nhận kiến nghị trả lời bằng văn bản trong thời hạn 05 ngày làm việc. Việc kiến nghị không làm tạm dừng thi hành quyết định;

c) Khiếu nại, khởi kiện và được bồi thường thiệt hại theo pháp luật về trách nhiệm bồi thường của Nhà nước trong trường hợp việc áp dụng trái pháp luật.

9. Trường hợp sự việc đồng thời là tình huống nguy hiểm về an ninh mạng thì áp dụng biện pháp theo pháp luật về an ninh mạng. Biện pháp quy định tại Điều này chỉ áp dụng đối với nội dung bảo đảm an ninh của bản thân dữ liệu mà biện pháp theo pháp luật về an ninh mạng không xử lý được, gồm phong tỏa tập dữ liệu, ngăn chặn luồng truyền dữ liệu xác định, vô hiệu hóa quyền truy cập dữ liệu hoặc tạm dừng mô hình trí tuệ nhân tạo bị đầu độc dữ liệu; không áp dụng đồng thời biện pháp theo Điều này và biện pháp theo pháp luật về an ninh mạng có cùng mục đích đối với cùng một đối tượng.

10. Chủ quản dữ liệu Cấp độ 4, Cấp độ 5 có trách nhiệm chuẩn bị phương án kỹ thuật để thực hiện biện pháp kỹ thuật khẩn cấp. Chủ quản dữ liệu chấp hành quyết định áp dụng biện pháp kỹ thuật khẩn cấp của người có thẩm quyền.

11. Chính phủ quy định chi tiết trình tự, thủ tục áp dụng, gia hạn, chấm dứt biện pháp kỹ thuật khẩn cấp.

Chương V

NGUỒN LỰC BẢO VỆ VÀ QUẢN LÝ NHÀ NƯỚC VỀ AN NINH DỮ LIỆU

Điều 24. Lực lượng bảo vệ an ninh dữ liệu

1. Lực lượng bảo vệ an ninh dữ liệu thuộc lực lượng bảo vệ an ninh mạng, bao gồm:

a) Lực lượng chuyên trách bảo vệ an ninh dữ liệu tại Bộ Công an, Bộ Quốc phòng; lực lượng cơ yếu đối với hệ thống thông tin cơ yếu;

b) Bộ phận, nhân sự phụ trách bảo vệ an ninh dữ liệu tại Bộ, cơ quan ngang Bộ, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý hệ thống thông tin quan trọng về an ninh quốc gia, cơ sở dữ liệu quốc gia;

c) Nhân sự phụ trách bảo vệ an ninh dữ liệu tại cơ quan, tổ chức, doanh nghiệp quản lý hệ thống xử lý dữ liệu từ Cấp độ 3 trở lên;

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

2. Lực lượng quy định tại điểm b và điểm c khoản 1 Điều này được bố trí trên cơ sở tổ chức, biên chế, nhân sự hiện có, theo chế độ kiêm nhiệm hoặc chuyên trách căn cứ quy mô, cấp độ rủi ro của dữ liệu; không làm phát sinh tổ chức, biên chế mới. Doanh nghiệp được sử dụng dịch vụ bảo vệ an ninh dữ liệu của tổ chức cung cấp dịch vụ để thực hiện nghĩa vụ quy định tại điểm c khoản 1 Điều này.

3. Chủ quản dữ liệu từ Cấp độ 3 trở lên chỉ định đầu mối phụ trách an ninh dữ liệu; đối với dữ liệu Cấp độ 4, Cấp độ 5 và hệ thống thông tin quan trọng về an ninh quốc gia, đầu mối là người có thẩm quyền quyết định biện pháp bảo vệ. Đầu mối phụ trách an ninh dữ liệu được kiêm nhiệm với bộ phận, nhân sự phụ trách an ninh mạng, bảo vệ dữ liệu cá nhân.

4. Khi xảy ra sự cố an ninh dữ liệu từ mức nghiêm trọng trở lên hoặc trên diện rộng, cơ quan nhà nước có thẩm quyền được huy động lực lượng, phương tiện, trang thiết bị kỹ thuật của cơ quan, tổ chức, cá nhân theo quy định của pháp luật; chi phí huy động được bồi hoàn theo quy định của pháp luật.

5. Chính phủ quy định chi tiết Điều này.

Điều 25. Nguồn lực xã hội, nhân lực và thông báo lỗ hổng an ninh dữ liệu

1. Nhà nước khuyến khích cơ quan, tổ chức, cá nhân nghiên cứu, phát triển công nghệ, cung cấp dịch vụ đánh giá, kiểm toán, ứng cứu sự cố an ninh dữ liệu; huy động chuyên gia, tổ chức xã hội - nghề nghiệp tham gia bảo đảm an ninh dữ liệu.

2. Nhà nước ưu tiên phát triển nguồn nhân lực chất lượng cao về an ninh dữ liệu và các công nghệ số cốt lõi; khuyến khích hợp tác giữa cơ quan nhà nước, cơ sở đào tạo, viện nghiên cứu và doanh nghiệp.

3. Tổ chức, cá nhân phát hiện, kiểm thử và thông báo lỗ hổng an ninh dữ liệu với thiện chí được bảo vệ danh tính, quyền, lợi ích hợp pháp. Việc xem xét tính thiện chí và loại trừ trách nhiệm pháp lý được căn cứ vào mục đích, phạm vi truy cập, mức độ tương xứng của kiểm thử với mục đích xác định lỗ hổng, việc hạn chế khai thác dữ liệu ngoài phạm vi kiểm thử, việc thông báo cho chủ quản dữ liệu hoặc cơ quan chuyên trách bảo vệ an ninh dữ liệu ngay sau khi phát hiện và không nhằm mục đích trục lợi, phá hoại hoặc gây thiệt hại.

4. Chính phủ quy định chi tiết cơ chế tiếp nhận, phối hợp xử lý thông tin và bảo vệ chủ thể thực hiện thông báo thiện chí quy định tại khoản 3 Điều này.

Điều 26. Quản lý nhà nước về an ninh dữ liệu và xử lý vi phạm

1. Chính phủ thống nhất quản lý nhà nước về an ninh dữ liệu.

2. Nội dung quản lý nhà nước về an ninh dữ liệu bao gồm:

a) Xây dựng, ban hành, tổ chức thực hiện chiến lược, văn bản quy phạm pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật về an ninh dữ liệu;

b) Xác định, hướng dẫn xác định cấp độ rủi ro; thẩm định, chấp thuận, đánh giá sự phù hợp về an ninh dữ liệu;

- c) Giám sát, cảnh báo, điều phối ứng phó sự cố an ninh dữ liệu;
- d) Tuyên truyền, đào tạo, phát triển nguồn nhân lực về an ninh dữ liệu;
- đ) Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh dữ liệu;
- e) Hợp tác quốc tế về an ninh dữ liệu;
- g) Sơ kết, tổng kết, đánh giá việc thi hành pháp luật về an ninh dữ liệu.

3. Bộ Công an chịu trách nhiệm trước Chính phủ, chủ trì thực hiện quản lý nhà nước về an ninh dữ liệu, trừ trường hợp quy định tại khoản 6 Điều này; thống nhất quản lý nhà nước về mật mã an ninh theo quy định tại Điều 16 của Luật này; thực hiện quản lý nhà nước về an ninh dữ liệu đối với hoạt động dân sự, kinh tế của doanh nghiệp thuộc Bộ Quốc phòng.

4. Bộ Công an là cơ quan đầu mối tiếp nhận hồ sơ, thông báo, báo cáo theo quy định của Luật này qua hệ thống điện tử thống nhất do Bộ Công an xây dựng, quản lý, vận hành, kết nối với Cổng Dịch vụ công quốc gia và hệ thống của cơ quan có liên quan. Thông tin tiếp nhận qua hệ thống được bảo mật và chỉ sử dụng cho mục đích quản lý nhà nước về an ninh dữ liệu.

5. Hằng năm, Bộ Công an báo cáo Chính phủ tình hình an ninh dữ liệu và kết quả thi hành Luật này; công bố thông tin không thuộc bí mật nhà nước.

6. Bộ Quốc phòng thực hiện quản lý nhà nước về an ninh dữ liệu đối với dữ liệu, hệ thống thông tin quân sự và hệ thống thông tin cơ yếu. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về cơ yếu theo pháp luật về cơ yếu, chủ trì bảo vệ an ninh dữ liệu đối với hệ thống thông tin cơ yếu; phối hợp với Bộ Công an đánh giá việc ứng dụng mật mã an ninh theo quy định tại điểm b khoản 4 Điều 16 của Luật này và chia sẻ thông tin nguy cơ, sự cố với Bộ Công an.

7. Bộ Khoa học và Công nghệ phối hợp với Bộ Công an xây dựng tiêu chuẩn, quy chuẩn kỹ thuật về an ninh dữ liệu; chủ trì, phối hợp với Bộ Công Thương và cơ quan có liên quan ban hành quy chuẩn kỹ thuật quốc gia về hệ số sử dụng năng lượng, tỷ lệ năng lượng tái tạo và hiệu suất thiết bị của trung tâm dữ liệu.

8. Bộ, cơ quan ngang Bộ, Ủy ban nhân dân cấp tỉnh trong phạm vi nhiệm vụ, quyền hạn phối hợp với Bộ Công an, Bộ Quốc phòng thực hiện quản lý nhà nước về an ninh dữ liệu.

9. Người đứng đầu cơ quan của Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam, tổ chức chính trị - xã hội chịu trách nhiệm bảo đảm an ninh dữ liệu trong cơ quan, tổ chức mình; ban hành và tổ chức thực hiện quy chế bảo vệ an ninh dữ liệu của cơ quan, tổ chức.

10. Đối với dữ liệu, hệ thống thông tin có tính chất lưỡng dụng, Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng thực hiện thẩm định, kiểm tra một lần; không tổ chức hai lần thẩm định, kiểm tra đối với cùng một nội dung.

11. Thanh tra, kiểm tra về an ninh dữ liệu thực hiện theo quy định của pháp luật và được kết hợp với thanh tra, kiểm tra về an ninh mạng trong cùng một đợt. Kiểm tra định kỳ không quá 01 lần trong 01 năm đối với cùng một cơ quan, tổ chức, trừ trường hợp có dấu hiệu vi phạm pháp luật rõ ràng hoặc phục vụ ứng cứu, điều tra sự cố an ninh dữ liệu.

12. Cơ quan, tổ chức, cá nhân 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; gây thiệt hại thì phải bồi thường theo quy định của pháp luật. Một hành vi vi phạm hành chính đồng thời được quy định tại pháp luật về an ninh dữ liệu, an ninh mạng, bảo vệ dữ liệu cá nhân, dữ liệu chỉ bị xử phạt một lần theo quy định của pháp luật về xử lý vi phạm hành chính.

13. Việc tự phát hiện, báo cáo đúng thời hạn, chủ động khắc phục hậu quả, hợp tác với cơ quan có thẩm quyền là căn cứ xem xét giảm nhẹ; việc che giấu sự cố, cố ý xác định sai cấp độ, tái phạm là căn cứ xem xét tăng nặng khi quyết định hình thức, mức xử lý theo quy định của pháp luật về xử lý vi phạm hành chính và quy định của Chính phủ.

14. Chính phủ quy định chi tiết cơ chế phối hợp giữa Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ và các cơ quan có liên quan trong quản lý nhà nước về an ninh dữ liệu; việc xây dựng, vận hành, kết nối hệ thống điện tử thống nhất quy định tại khoản 4 Điều này; nội dung tối thiểu của quy chế bảo vệ an ninh dữ liệu của cơ quan nhà nước quy định tại khoản 9 Điều này.

Chương VI

ĐIỀU KHOẢN THI HÀNH

Điều 27. Sửa đổi, bổ sung một số điều của các luật có liên quan

1. Sửa đổi, bổ sung một số điều của Luật An ninh mạng số 116/2025/QH15 như sau:

a) Bãi bỏ khoản 3 Điều 2;

b) Sửa đổi, bổ sung khoản 20 Điều 2 như sau:

“20. Mật mã dân sự là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước nhằm bảo đảm an ninh thông tin cho cơ quan, tổ chức, cá nhân, trừ mật mã của cơ yếu và mật mã an ninh theo quy định của Luật An ninh dữ liệu.”;

c) Sửa đổi, bổ sung Điều 26 như sau:

“Điều 26. Bảo đảm an ninh dữ liệu

Việc bảo đảm an ninh dữ liệu thực hiện trong suốt vòng đời của dữ liệu theo quy định của Luật An ninh dữ liệu; việc bảo đảm an ninh mạng, an toàn hệ thống thông tin xử lý dữ liệu thực hiện theo quy định của Luật này và pháp luật có liên quan.”;

d) Bổ sung khoản 2a vào sau khoản 2 Điều 28 như sau:

“2a. Sản phẩm, dịch vụ mật mã an ninh theo quy định của Luật An ninh dữ liệu không thuộc phạm vi sản phẩm, dịch vụ an ninh mạng quy định tại khoản 1 và khoản 2 Điều này; trường hợp sản phẩm, dịch vụ có chức năng độc lập khác thuộc khoản 1 hoặc khoản 2 Điều này thì áp dụng quy định của Luật này đối với chức năng đó.”;

đ) Bổ sung khoản 2a vào sau khoản 2 Điều 29 như sau:

“2a. Tổ chức, doanh nghiệp nghiên cứu, phát triển, sản xuất, cung cấp sản phẩm, giải pháp mật mã an ninh theo quy định của Luật An ninh dữ liệu không phải cấp giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng theo quy định tại Điều này đối với chức năng mật mã an ninh; trường hợp sản phẩm, dịch vụ có chức năng độc lập khác quy định tại Điều 28 của Luật này thì áp dụng quy định về giấy phép đối với chức năng đó.”.

2. Sửa đổi, bổ sung một số điều của Luật Dữ liệu số 60/2024/QH15 như sau:

a) Sửa đổi, bổ sung khoản 1 Điều 22 như sau:

“1. Dữ liệu thuộc danh mục bí mật nhà nước phải được mã hóa bằng mật mã của cơ yếu khi lưu trữ, truyền, nhận, chia sẻ trên mạng máy tính, trừ trường hợp sử dụng mật mã an ninh theo quy định tại khoản 4 Điều 16 của Luật An ninh dữ liệu.”;

b) Sửa đổi, bổ sung khoản 4 Điều 23 như sau:

“4. Điều kiện, trình tự, thủ tục và biện pháp bảo đảm an ninh khi chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng xuyên biên giới quy định tại khoản 2 Điều này thực hiện theo quy định của Luật An ninh dữ liệu. Chính phủ quy định chi tiết các nội dung khác của Điều này.”;

c) Sửa đổi, bổ sung khoản 4 Điều 25 như sau:

“4. Việc đánh giá rủi ro, báo cáo và phối hợp bảo vệ an ninh đối với dữ liệu cốt lõi, dữ liệu quan trọng thực hiện theo quy định của Luật An ninh dữ liệu.”.

Điều 28. Hiệu lực thi hành

Luật này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2027.

Điều 29. Quy định chuyển tiếp

1. Hệ thống thông tin đã đưa vào vận hành trước ngày Luật này có hiệu lực thi hành thực hiện như sau:

a) Hệ thống xử lý dữ liệu từ Cấp độ 3 trở lên hoàn thành việc xác định cấp độ rủi ro theo quy định tại Điều 8, đánh giá tác động theo quy định tại khoản 4 Điều 10 của Luật này và tự khắc phục nội dung chưa đáp ứng yêu cầu trong thời hạn 24 tháng; đối với doanh nghiệp nhỏ và vừa, thời hạn là 36 tháng;

b) Hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5 thực hiện kiểm toán an ninh dữ liệu lần đầu theo quy định tại khoản 4 và khoản 5 Điều 10 của Luật này trong thời hạn 12 tháng, khắc phục rủi ro được phát hiện và lưu giữ kết quả để xuất trình khi thanh tra, kiểm tra;

c) Hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5 được thẩm định theo quy định tại khoản 6 Điều 11 của Luật này khi nâng cấp, thay đổi trọng yếu, khi kết quả thanh tra, kiểm tra xác định hệ thống không đáp ứng yêu cầu bảo vệ hoặc theo lộ trình do Chính phủ quy định, ưu tiên hạ tầng dữ liệu quốc gia trọng yếu, cơ sở dữ liệu quốc gia; hệ thống đã được thẩm định an ninh mạng còn hiệu lực chỉ bổ sung nội dung chưa được thẩm định;

d) Chủ quản dữ liệu Cấp độ 4, Cấp độ 5 tổ chức giám sát theo quy định tại điểm c khoản 1 Điều 22 của Luật này trong thời hạn 12 tháng và xây dựng phương án theo quy định tại khoản 7 Điều 9 của Luật này trong thời hạn 24 tháng;

đ) Thời hạn quy định tại các điểm a, b và d khoản này được tính từ ngày Luật này có hiệu lực thi hành.

2. Văn bản chấp thuận, kết quả đánh giá tác động chuyển dữ liệu ra nước ngoài đã được cơ quan có thẩm quyền cấp, tiếp nhận theo pháp luật về bảo vệ dữ liệu cá nhân, pháp luật về dữ liệu trước ngày Luật này có hiệu lực thi hành tiếp tục được sử dụng đối với luồng chuyển dữ liệu đã được đánh giá, chấp thuận cho đến khi thay đổi mục đích, loại dữ liệu, bên nhận, quốc gia, vùng lãnh thổ tiếp nhận hoặc biện pháp bảo vệ; trường hợp văn bản có ghi thời hạn thì được sử dụng đến hết thời hạn đó.

3. Hồ sơ, thủ tục đã được tiếp nhận trước ngày Luật này có hiệu lực thi hành tiếp tục được giải quyết theo quy định của pháp luật tại thời điểm tiếp nhận, trừ trường hợp tổ chức, cá nhân đề nghị áp dụng quy định của Luật này.

4. Chương trình, dự án, nhiệm vụ chuyển đổi số đã được cấp có thẩm quyền phê duyệt trước ngày Luật này có hiệu lực thi hành tiếp tục thực hiện theo quyết định đã phê duyệt; quy định tại khoản 1 và khoản 2 Điều 12 của Luật này được áp dụng khi điều chỉnh chương trình, dự án, nhiệm vụ.

5. Dữ liệu đã được xác định là dữ liệu quan trọng, dữ liệu cốt lõi theo pháp luật về dữ liệu trước ngày Luật này có hiệu lực thi hành được xác định cấp độ theo quy định tại khoản 1 và khoản 3 Điều 8 của Luật này, không phải thực hiện thủ tục xác định lại. Chủ quản dữ liệu không phải rà soát, phân loại lại toàn bộ dữ liệu; việc xác định cấp độ đối với dữ liệu khác được thực hiện khi thiết lập mới, nâng cấp, thay đổi hệ thống hoặc hoạt động xử lý dữ liệu.

6. Hệ thống xử lý dữ liệu Cấp độ 4, Cấp độ 5 đầu tư mới, nâng cấp kể từ ngày Luật này có hiệu lực thi hành phải đáp ứng yêu cầu về khả năng thay thế thuật toán, giao thức, thành phần mật mã quy định tại khoản 2 Điều 17 của Luật này; hệ thống đang vận hành thực hiện theo lộ trình quy định tại khoản 6 Điều 17 của Luật này.

7. Hệ thống trí tuệ nhân tạo phục vụ quốc phòng, an ninh, cơ yếu đang sử dụng trước ngày Luật này có hiệu lực thi hành được tiếp tục sử dụng và phải đáp ứng quy định tại khoản 6 Điều 15 của Luật này trong thời hạn 24 tháng kể từ ngày Luật này có hiệu lực thi hành.

8. Chủ quản dữ liệu Cấp độ 2 đã hoạt động trước ngày Luật này có hiệu lực thi hành hoàn thành việc lập phương án bảo vệ an ninh dữ liệu quy định tại khoản 2 Điều 10 của Luật này trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

Luật này được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XVI, kỳ họp thứ 2 thông qua ngày ... tháng ... năm 2026.

CHỦ TỊCH QUỐC HỘI

Trần Thanh Mẫn