UBND TỈNH ĐIỆN BIÊN
HỘI ĐỒNG PHỐI HỢP PHỔ BIẾN, GIÁO DỤC PHÁP LUẬT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

SỞ TƯ PHÁP

ĐỀ CƯƠNG GIỚI THIỆU, PHỔ BIẾN LUẬT AN NINH MẠNG NĂM 2025

(Tài liệu dành cho Báo cáo viên pháp luật cấp tỉnh, Tuyên truyền viên pháp luật trên địa bàn tỉnh Điện Biên)

Luật An ninh mạng số 116/2025/QH15 đã được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XV, kỳ họp thứ 10 thông qua ngày 10 tháng 12 năm 2025, có hiệu lực thi hành kể từ ngày 01/7/2026 *(Luật số 116/2025/QH15)*. Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14; Luật An ninh mạng số 24/2018/QH14 hết hiệu lực kể từ ngày 01/7/2026.

PHẦN I. NHỮNG VẤN ĐỀ CHUNG

I. SỰ CẦN THIẾT BAN HÀNH LUẬT AN NINH MẠNG

1. Cơ sở chính trị, pháp lý

- Nghị quyết số 29-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược Bảo vệ Tổ quốc trên không gian mạng.

- Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược an ninh mạng quốc gia.

- Nghị quyết số 51-NQ/TW ngày 05/9/2019 của Bộ Chính trị về Chiến lược bảo vệ an ninh quốc gia.

- Nghị quyết số 44-NQ/TW ngày 24/11/2023 của Ban Chấp hành Trung ương Đảng khóa XIII về Chiến lược bảo vệ Tổ quốc trong tình hình mới.

- Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về Đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

- Nghị quyết số 68-NQ/TW ngày 04/5/2025 của Bộ Chính trị về phát triển kinh tế tư nhân.

- Luật Ban hành văn bản quy phạm pháp luật năm 2025.

- Trong những năm qua, nhận thấy thực tế trùng lặp chức năng bảo vệ an ninh mạng giữa Bộ Công an và Bộ Thông tin và Truyền thông đã gây ra nhiều bất cập trong công tác quản lý, Quốc hội và Chính phủ Việt Nam đã quyết định điều chỉnh lại cơ cấu tổ chức, nhằm bảo đảm một cơ chế quản lý thống nhất và hiệu quả trong lĩnh vực an ninh mạng. Do vậy, ngày 19/02/2025, Quốc hội đã ban hành Nghị quyết số 190/2025/QH15 quy định về xử lý một số vấn đề liên quan đến sắp xếp tổ chức bộ máy nhà nước và theo Thông báo Kết luận số 04/TB-BCĐTKNQ18 ngày 12/01/2025 của Ban Chỉ đạo Chính phủ tại Phiên họp thứ 9

liên quan tới việc thống nhất điều chỉnh một số nhiệm vụ của các bộ, ngành về Bộ Công an, trong đó có nhiệm vụ bảo đảm an toàn thông tin mạng từ Bộ Thông tin và Truyền thông về Bộ Công an.

Như vậy, trên cơ sở những quan điểm, chỉ đạo của Đảng, Nhà nước ta thời gian qua, Quốc hội đã quyết định thông qua Luật An ninh mạng số 116/2025/QH15, trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) để bảo đảm hoàn thiện thể chế về an ninh mạng phù hợp và thống nhất.

2. Cơ sở thực tiễn

a) Thực tiễn Việt Nam cho thấy, công tác bảo vệ an ninh mạng thời gian qua đang phải đối mặt với nhiều nguy cơ, thách thức mới, ngày càng đan xen, phức tạp, chi phối trực tiếp đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân, tác động trực tiếp tới cả hoạt động bảo đảm an ninh mạng và bảo đảm an toàn thông tin mạng. Cụ thể như:

Thứ nhất, hoạt động tấn công mạng, gián điệp mạng và lộ, mất bí mật nhà nước tại Việt Nam diễn ra ngày càng phức tạp, ảnh hưởng nghiêm trọng đến an ninh quốc gia. Tin tặc sử dụng nhiều thủ đoạn tinh vi, không ngừng nâng cấp, cải tiến các dòng mã độc để tiến hành các chiến dịch tấn công mạng nhằm vào các cơ quan, tổ chức, doanh nghiệp của Việt Nam. Mục tiêu chủ yếu nhằm vào hệ thống mạng thông tin của các cơ quan Trung ương và các tập đoàn, doanh nghiệp quan trọng. Mục tiêu tấn công không chỉ nhằm thu thập thông tin tình báo, bí mật nhà nước, đặc biệt là các chủ trương, chính sách đối ngoại, an ninh, quốc phòng của Việt Nam mà còn chuẩn bị sẵn để tiến hành các hành động tình báo, phát động các cuộc tấn công phá hoại khi cần thiết. Hàng năm, Cục A05 phát hiện trên 2.600 trang/cổng thông tin điện tử của Việt Nam (có tên miền ".vn") bị tin tặc tấn công, thay đổi giao diện hoặc chèn tập tin; hàng chục vụ lộ tài liệu bí mật nhà nước với hàng trăm đầu tài liệu; hàng trăm terabyte (TB) dữ liệu của các bộ, ban, ngành, địa phương bị tin tặc chiếm đoạt, trong đó có nhiều tài liệu bí mật nhà nước. Một số cơ quan, đơn vị mặc dù đã được kiểm tra, cảnh báo về các nguy cơ gây mất an ninh mạng, lộ mất bí mật nhà nước, tình trạng này vẫn tiếp diễn tại một số cơ quan, đơn vị.

Thứ hai, việc kiểm soát, quản trị và bảo vệ dữ liệu chưa tương xứng với giá trị và mức độ khai thác, sử dụng dữ liệu trong nền kinh tế số, xã hội số. Dữ liệu cá nhân đang được khai thác, sử dụng, tạo ra giá trị thặng dư một cách tự do, thiếu nguyên tắc và sự quản lý, dẫn tới thực trạng lộ, lọt, mua bán, xâm phạm dữ liệu cá nhân diễn ra phổ biến, ngày càng nghiêm trọng, kéo theo gia tăng các loại tội phạm mạng, tội phạm lừa đảo chiếm đoạt tài sản.

Thứ ba, hoạt động phá hoại tư tưởng, chống đối trong nước nhằm từng bước chuyển hóa chế độ chính trị ở nước ta diễn ra mạnh mẽ. Hàng năm, A05 rà soát, phát hiện hơn 7.500 nguồn khởi phát thông tin xấu độc, thu hút hơn 83 triệu lượt tiếp cận, tương tác thông tin, tập trung công kích, chống phá.

Thứ tư, hoạt động sử dụng công nghệ cao để thực hiện hành vi phạm tội, xâm phạm trật tự, an toàn xã hội diễn ra ngày càng phức tạp, gây bức xúc trong xã hội, gây thiệt hại lớn về tài sản cho người dân, nhất là hoạt động lừa đảo, chiếm đoạt tài sản, đánh bạc và tổ chức đánh bạc, truyền bá văn hóa phẩm đồi trụy, mua bán vũ khí, vật liệu nổ, ma túy, bằng cấp giả. Đặc biệt, các nhóm tội phạm người nước ngoài có xu hướng dịch chuyển sang địa bàn Việt Nam để thực hiện hành vi phạm tội với nhiều thủ đoạn hoạt động mới tinh vi hơn, tập trung ở các tỉnh, thành phố lớn, khu du lịch, vùng ven biển có vị trí chiến lược, thiết yếu về an ninh quốc phòng như thành phố Hồ Chí Minh, Hải Phòng, Quảng Ninh, Nha Trang, Đà Nẵng... Một số đối tượng người Trung Quốc còn móc nối, cấu kết với đối tượng người Việt Nam để lừa đảo, lôi kéo người Việt Nam sang Campuchia phạm tội sử dụng công nghệ cao, dưới hình thức giới thiệu "việc nhẹ, lương cao".

Thực tế, trong 06 tháng đầu năm 2025, A05 phát hiện 25 vụ việc liên quan hệ thống thông tin của một số cơ quan, đơn vị tồn tại điểm yếu, lỗ hổng bảo mật nghiêm trọng, xảy ra tình trạng lây nhiễm mã độc; lộ mất tài khoản quản trị, tài khoản người dùng; 56 vụ việc liên quan hoạt động quảng cáo, rao bán thông tin, dữ liệu cá nhân trên các diễn đàn hội nhóm, trang mạng tin tặc với gần 110 triệu bản ghi. Triển khai Đề án 06 của Chính phủ, A05 tiến hành kiểm tra, đánh giá an ninh mạng hệ thống thông tin tại 07 ban, bộ, ngành, địa phương kết nối Cơ sở dữ liệu quốc gia về dân cư và hệ thống định danh xác thực điện tử VNeID, phát hiện 1.315 lỗ hổng bảo mật mức độ nghiêm trọng, 4.095 lỗ hổng bảo mật mức độ cao tại các máy chủ hệ thống. Một trong những nguyên nhân dẫn đến thực trạng trên là do sự bất cập, thiếu đồng bộ trong hệ thống chính sách, pháp luật về lĩnh vực an ninh mạng.

Bối cảnh và tình hình trên đã đặt ra yêu cầu cấp bách là tiếp tục nhanh chóng hoàn thiện thể chế, chính sách pháp luật làm nền tảng vững chắc để thực hiện công tác quản lý nhà nước trên lĩnh vực an ninh mạng, đấu tranh phòng, chống tội phạm mạng, tội phạm sử dụng công nghệ cao, tội phạm xâm phạm dữ liệu cá nhân. Đặc biệt, theo tinh thần Nghị quyết số 18-NQ/TW ngày 25/10/2017 về một số vấn đề tiếp tục đổi mới, sắp xếp tổ chức bộ máy của hệ thống chính trị tinh gọn, hoạt động hiệu lực, hiệu quả và thực hiện Đề án tiếp nhận chức năng, nhiệm vụ bảo đảm an toàn thông tin mạng từ Bộ Thông tin và Truyền thông về Bộ Công an, công tác rà soát, đồng bộ hệ thống chính sách pháp luật trong lĩnh vực an ninh mạng, an toàn thông tin mạng là hết sức cần thiết để ổn định hoạt động của bộ máy bảo đảm thông suốt, không gián đoạn, góp phần bảo vệ an ninh mạng hiệu quả, toàn diện, thống nhất.

b) Thực tế, về bản chất công nghệ, an toàn thông tin mạng là một phần của an ninh mạng, nên hai vấn đề này thực sự có nhiều điểm tương đồng nhau, cụ thể: (1) Mục tiêu chính: Cả hai đều nhắm tới mục đích bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa và tấn công. (2) Phương pháp: Đều sử dụng các biện pháp kỹ thuật và quy trình để đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của thông tin và hệ thống. (3) Kiểm soát truy cập: Áp dụng các biện pháp kiểm soát truy cập nhằm đảm bảo chỉ những người có quyền mới được truy cập vào các tài nguyên và thông tin. (4) Phát hiện và ngăn chặn: Cả hai lĩnh vực đều triển khai các giải pháp nhằm

phát hiện và ngăn chặn các mối đe dọa từ bên ngoài và bên trong. (5) Đào tạo và nhận thức: Cả an toàn thông tin mạng và an ninh mạng đều chú trọng vào việc nâng cao nhận thức và đào tạo người dùng về các biện pháp bảo mật và cách phòng tránh các rủi ro bảo mật. (6) Cùng thực hiện chức năng quản lý nhà nước đối với thông tin, dữ liệu và hệ thống thông tin. Cùng thực hiện thanh tra, kiểm tra trên cùng một hệ, loại đối tượng, doanh nghiệp. Điều này khiến phát sinh nhiều mâu thuẫn, trùng lặp trong khi triển khai công tác thực tế.

Nhìn vào thực tiễn hiện nay, Việt Nam đang thực hiện cuộc cách mạng số với rất nhiều yếu tố thuận lợi về thể chế chính trị, kinh tế, xã hội, khoa học công nghệ để đưa đất nước bứt phá, bước vào kỷ nguyên vươn mình giàu mạnh. Bên cạnh đó, nước ta là quốc gia được đánh giá có tốc độ phát triển và ứng dụng Internet cao nhất thế giới, đứng đầu khu vực Đông Nam Á về số lượng tên miền quốc gia; có ngành công nghiệp thông tin có thứ hạng cao trong khu vực và trên thế giới; cơ sở hạ tầng số phát triển nhanh, cơ sở hạ tầng dữ liệu và mạng lưới trung tâm dữ liệu đang được cải thiện; Chính phủ điện tử dần toàn diện; dân số trẻ, có trình độ học vấn, tỷ lệ người dân dùng điện thoại thông minh và sử dụng các ứng dụng, dịch vụ trên không gian mạng, nhất là mạng xã hội ở mức cao.

Như vậy, từ các cơ sở thực tiễn trên, việc hợp nhất là cần thiết, phù hợp với yêu cầu hoàn thiện thể chế và thống nhất quản lý nhà nước về an ninh mạng.

II. MỤC ĐÍCH, QUAN ĐIỂM CHỈ ĐẠO XÂY DỰNG LUẬT AN NINH MẠNG

1. Mục đích xây dựng Luật

Việc xây dựng, ban hành Luật An ninh mạng năm 2025 nhằm thống nhất hệ thống pháp luật, thay thế và hợp nhất các quy định của Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018. Luật nhằm giải quyết những bất cập, chồng chéo trong quản lý, tạo hành lang pháp lý đồng bộ để bảo vệ hệ thống thông tin, dữ liệu và người dân trước các nguy cơ an ninh mạng ngày càng gia tăng, cụ thể như sau:

- Bảo đảm tính thống nhất, đồng bộ của hệ thống pháp luật, loại bỏ sự chồng chéo, mâu thuẫn giữa hai luật hiện hành, tạo khung pháp lý rõ ràng, minh bạch, đáp ứng yêu cầu quản lý và bảo vệ không gian mạng.

- Nâng cao hiệu quả của hoạt động bảo đảm an ninh mạng, kết hợp chặt chẽ các biện pháp bảo vệ hệ thống thông tin, dữ liệu cá nhân, phòng chống tấn công mạng với các giải pháp bảo đảm an ninh quốc gia trên không gian mạng.

- Tạo điều kiện thuận lợi cho tổ chức, doanh nghiệp và cá nhân trong việc tuân thủ pháp luật, giảm thiểu thủ tục hành chính, đồng thời bảo vệ quyền lợi hợp pháp, thúc đẩy môi trường số an toàn, phát triển kinh tế số bền vững.

- Hoàn thiện cơ chế phòng thủ, giám sát, cảnh báo và ứng phó với các nguy cơ, sự cố an ninh mạng, bảo vệ hệ thống thông tin quan trọng quốc gia, tăng cường năng lực phòng ngừa và khắc phục hậu quả của các cuộc tấn công mạng.

- Đáp ứng yêu cầu hội nhập quốc tế, phù hợp với các cam kết, chuẩn mực quốc tế về an ninh mạng, thúc đẩy nghiên cứu, phát triển công nghệ và nâng cao năng lực cạnh tranh của Việt Nam trong lĩnh vực an ninh mạng.

2. Quan điểm xây dựng Luật

- Khẳng định sự lãnh đạo tuyệt đối của Đảng và sự quản lý thống nhất của Nhà nước đối với công tác an ninh mạng; xác định bảo vệ an ninh mạng là nhiệm vụ quan trọng, thường xuyên của cả hệ thống chính trị và toàn dân, trong đó lực lượng chuyên trách giữ vai trò nòng cốt.

- Kiên định bảo vệ chủ quyền, quyền tài phán và lợi ích quốc gia trên không gian mạng; yêu cầu mọi hoạt động trên không gian mạng tuân thủ Hiến pháp và pháp luật Việt Nam, kiên quyết đấu tranh làm thất bại các hành vi lợi dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

- Chuyển đổi tư duy từ phòng vệ sang chủ động và tự chủ trong bảo vệ an ninh mạng; chủ động phòng ngừa, phát hiện, đấu tranh và vô hiệu hóa các mối đe dọa khi cần thiết, đồng thời ưu tiên đầu tư phát triển khoa học, công nghệ, nâng cao năng lực tự chủ an ninh mạng quốc gia, khuyến khích sử dụng sản phẩm, dịch vụ an ninh mạng trong nước, sản phẩm "Make in Vietnam".

- Kết hợp hài hòa giữa bảo vệ an ninh mạng với phát triển kinh tế - xã hội; bảo đảm quyền con người, quyền công dân, tạo môi trường thuận lợi cho chuyển đổi số quốc gia, phát triển kinh tế số và xã hội số.

- Lấy dữ liệu và con người làm trọng tâm trong bảo vệ an ninh mạng; xác định an ninh dữ liệu là trụ cột mới cần được bảo vệ toàn diện, đồng thời ưu tiên nguồn lực cho yếu tố con người thông qua cơ chế, chính sách đặc thù về đào tạo, thu hút, sử dụng nhân lực chất lượng cao và nâng cao nhận thức an ninh mạng trong toàn xã hội.

PHẦN II. GIỚI THIỆU VĂN BẢN

I. Bố cục

Luật An ninh mạng năm 2025 gồm 08 chương với 45 điều, quy định về an ninh mạng, bảo vệ an ninh mạng, quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân, cụ thể như sau:

Chương I. Những quy định chung

Gồm 07 điều, từ Điều 1 đến Điều 7 quy định về: (1) Phạm vi điều chỉnh và đối tượng áp dụng; (2) Giải thích từ ngữ; (3) Chính sách của Nhà nước về an ninh mạng; (4) Nguyên tắc bảo vệ an ninh mạng; (5) Biện pháp bảo vệ an ninh mạng; (6) Hợp tác quốc tế về an ninh mạng; (7) Các hành vi bị nghiêm cấm về an ninh mạng.

Chương II. Bảo vệ an ninh mạng đối với hệ thống thông tin

Gồm 05 điều, từ Điều 8 đến Điều 12 quy định về: (1) Phân loại cấp độ hệ thống thông tin; (2) Hệ thống thông tin quan trọng về an ninh quốc gia; (3) Nhiệm vụ, biện pháp và trách nhiệm bảo vệ đối với từng loại hệ thống; (4) Trách nhiệm

bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; (5) Kiểm tra an ninh mạng đối với hệ thống thông tin không thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Chương III. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng

Gồm 10 điều, từ Điều 13 đến Điều 22 quy định về: (1) Các thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng; (2) Phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng; (3) Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; (4) Phòng, chống xâm hại trẻ em trên không gian mạng; (5) Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại; (6) Phòng, chống tấn công mạng; (7) Phòng, chống khủng bố mạng; (8) Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; (9) Đấu tranh bảo vệ an ninh mạng; (10) Ngăn chặn xung đột thông tin trên không gian mạng.

Chương IV. Hoạt động bảo vệ an ninh mạng

Gồm 04 điều, từ Điều 23 đến Điều 26 quy định về: (1) Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội ở trung ương và địa phương; (2) Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế; (3) Bảo đảm an ninh thông tin mạng; (4) Bảo đảm an ninh dữ liệu.

Chương V. Tiêu chuẩn, quy chuẩn kỹ thuật, sản phẩm, dịch vụ an ninh mạng

Gồm 03 điều, từ Điều 27 đến Điều 29 quy định về: (1) Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng; (2) Sản phẩm, dịch vụ an ninh mạng; (3) Kinh doanh sản phẩm, dịch vụ an ninh mạng.

Chương VI. Lực lượng, điều kiện bảo đảm an ninh mạng

Gồm 09 điều, từ Điều 30 đến Điều 38 quy định về: (1) Lực lượng bảo vệ an ninh mạng; (2) Bảo đảm nguồn nhân lực bảo vệ an ninh mạng; (3) Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; (4) Giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; (5) Tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng; (6) Phổ biến kiến thức về an ninh mạng; (7) Nghiên cứu, phát triển an ninh mạng; (8) Nâng cao năng lực tự chủ về an ninh mạng; (9) Kinh phí bảo vệ an ninh mạng.

Chương VII. Trách nhiệm của cơ quan, tổ chức, cá nhân về an ninh mạng

Gồm 04 điều, từ Điều 39 đến Điều 42 quy định về: (1) Trách nhiệm quản lý nhà nước về an ninh mạng; (2) Trách nhiệm của chủ quản hệ thống thông tin trong bảo vệ an ninh mạng; (3) Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng; (4) Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng.

Chương VIII. Điều khoản thi hành

Gồm 03 điều, từ Điều 43 đến Điều 45 quy định về: (1) Sửa đổi, bổ sung một số điều của các luật có liên quan; (2) Hiệu lực thi hành; (3) Điều khoản chuyển tiếp.

II. Những nội dung mới trong Luật An ninh mạng

1. Hoàn thiện và thống nhất hệ thống khái niệm làm nền tảng cho quản lý và bảo vệ an ninh mạng

Luật An ninh mạng năm 2025 đã có bước đổi mới quan trọng về kỹ thuật lập pháp thông qua việc chuẩn hóa, thống nhất hệ thống khái niệm cơ bản làm nền tảng cho quản lý nhà nước về an ninh mạng. Đây là thay đổi có ý nghĩa căn bản, khắc phục tình trạng phân tán, thiếu thống nhất giữa các khái niệm về "an toàn thông tin mạng" và "an ninh mạng" trong hệ thống pháp luật giai đoạn trước, qua đó tạo cơ sở pháp lý rõ ràng, đồng bộ cho việc tổ chức thi hành Luật. Cụ thể:

- Thống nhất cách hiểu và phạm vi của khái niệm "an ninh mạng": Tại khoản 1 Điều 2, Luật định nghĩa "*An ninh mạng là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân*". Cách định nghĩa này giúp thống nhất nhận thức và mở rộng phạm vi điều chỉnh của Luật phù hợp với yêu cầu thực tiễn.

- Phân định rõ khái niệm "an ninh thông tin mạng" với tư cách là trụ cột kỹ thuật của an ninh mạng: Theo khoản 2 Điều 2, "*An ninh thông tin mạng là sự bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của thông tin trên không gian mạng, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội*". Việc làm rõ nội hàm này giúp tách bạch giữa yêu cầu bảo vệ về mặt kỹ thuật - công nghệ với các yêu cầu bảo vệ an ninh mạng mang tính tổng thể về chính trị, pháp lý, xã hội, qua đó tạo thuận lợi cho việc xây dựng và áp dụng các biện pháp kỹ thuật bảo vệ hạ tầng thông tin.

- Bổ sung và luật hóa khái niệm "an ninh dữ liệu" đáp ứng yêu cầu của kỷ nguyên số: Lần đầu tiên, Luật An ninh mạng năm 2025 ghi nhận "an ninh dữ liệu" là một khái niệm pháp lý độc lập tại khoản 3 Điều 2. Theo đó, *"An ninh dữ liệu là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội*". Đây là điểm mới thể hiện sự thay đổi tư duy quản lý, coi dữ liệu là tài nguyên chiến lược cần được bảo vệ và khai thác hiệu quả.

- Khẳng định chủ quyền số thông qua khái niệm "không gian mạng quốc gia": Tại khoản 6 Điều 2, Luật xác lập khái niệm "*Không gian mạng quốc gia là phần không gian mạng thuộc chủ quyền, quyền tài phán và quyền kiểm soát của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam*", qua đó khẳng định cơ sở pháp lý cho việc thực thi chủ quyền, quyền tài phán và quyền kiểm soát của Nhà nước Việt Nam đối với phần không gian mạng thuộc chủ quyền quốc gia. Quy định này

có ý nghĩa đặc biệt quan trọng trong bối cảnh hội nhập quốc tế sâu rộng và sự gia tăng của các hoạt động xuyên biên giới trên không gian mạng.

Việc chuẩn hóa và thống nhất hệ thống khái niệm nêu trên đã giúp xác định rõ phạm vi điều chỉnh và đối tượng áp dụng của Luật An ninh mạng năm 2025, khắc phục tình trạng chồng chéo, mâu thuẫn trong quản lý nhà nước, đồng thời tạo nền tảng pháp lý thống nhất, xuyên suốt cho việc áp dụng và thực thi pháp luật về an ninh mạng trong tình hình mới.

2. Bổ sung, cụ thể hóa các hành vi bị nghiêm cấm gắn với sự phát triển của khoa học, công nghệ và các phương thức hoạt động mới trên không gian mạng

Luật An ninh mạng năm 2025 đã kịp thời cập nhật và luật hóa nhiều hành vi vi phạm mới phát sinh trong quá trình ứng dụng công nghệ cao, khắc phục khoảng trống pháp lý của các quy định trước đây, tạo cơ sở pháp lý đầy đủ cho công tác phòng ngừa, đấu tranh và xử lý vi phạm trên không gian mạng.

- Kiểm soát chặt chẽ việc lạm dụng trí tuệ nhân tạo và công nghệ mới (Deepfake, AI): Trước thực trạng tội phạm sử dụng công nghệ trí tuệ nhân tạo để giả mạo hình ảnh, giọng nói, video nhằm lừa đảo, chiếm đoạt tài sản hoặc xâm phạm danh dự, nhân phẩm của người khác, Luật đã bổ sung quy định nghiêm cấm hành vi sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái pháp luật tại điểm g khoản 2 Điều 7. Quy định này tạo cơ sở pháp lý trực tiếp để xử lý các hành vi lừa đảo qua cuộc gọi video giả mạo, cũng như các hành vi bôi nhọ, vu khống bằng công nghệ ghép hình, ghép video.

- Nhận diện và phòng, chống các phương thức xâm phạm an ninh kinh tế trên không gian mạng: Luật đã cụ thể hóa các hành vi bị nghiêm cấm liên quan đến lĩnh vực tài chính, tiền tệ và thị trường số. Theo điểm d khoản 1 Điều 7, hành vi đưa thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, kinh doanh đa cấp, chứng khoán, trái phiếu… gây hoang mang dư luận và thiệt hại cho nền kinh tế bị nghiêm cấm. Đồng thời, tại điểm e khoản 4 Điều 13, Luật xác định hành vi thiết lập, cung cấp dịch vụ trái phép cho các sàn giao dịch tài sản số, tiền ảo hoặc tổ chức hoạt động kinh doanh đa cấp trái phép trên không gian mạng là hành vi xâm phạm an ninh quốc gia.

- Tăng cường bảo vệ danh tính số và dữ liệu cá nhân: Đáp ứng yêu cầu cấp thiết trong bối cảnh dữ liệu cá nhân bị khai thác, mua bán trái phép tràn lan, Luật nghiêm cấm tuyệt đối hành vi thu thập, sử dụng, phát tán, trao đổi, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân theo quy định tại điểm h khoản 2 Điều 7. Bên cạnh đó, các hành vi sử dụng danh tính giả, giấy tờ giả để đăng ký tài khoản ngân hàng, tài khoản số hoặc tạo lập "tài khoản rác" phục vụ hoạt động phạm tội cũng được xác định là hành vi xâm phạm trật tự, an toàn xã hội tại điểm g khoản 4 Điều 13, qua đó góp phần ngăn chặn các hành vi lừa đảo, rửa tiền trên không gian mạng.

Những quy định nêu trên đã mở rộng đáng kể phạm vi điều chỉnh của Luật An ninh mạng năm 2025, tạo cơ sở pháp lý vững chắc để các lực lượng chức năng

chủ động phòng ngừa, phát hiện và xử lý kịp thời các nguy cơ an ninh mạng mới phát sinh, đáp ứng yêu cầu bảo vệ an ninh quốc gia, trật tự, an toàn xã hội trong bối cảnh chuyển đổi số toàn diện.

3. Hoàn thiện cơ chế bảo vệ an ninh mạng theo cấp độ đối với hệ thống thông tin

Luật An ninh mạng năm 2025 đã thể chế hóa cách tiếp cận quản lý an ninh mạng dựa trên mức độ rủi ro và tầm quan trọng của hệ thống thông tin, thay thế mô hình áp dụng biện pháp bảo vệ mang tính dàn trải, cào bằng. Theo đó, nguồn lực được ưu tiên tập trung bảo vệ các hệ thống thông tin quan trọng, có phạm vi và mức độ ảnh hưởng lớn đến an ninh quốc gia, trật tự, an toàn xã hội. Cơ chế này được quy định cụ thể như sau:

- Phân loại hệ thống thông tin theo 05 cấp độ an ninh mạng: Khoản 1 Điều 8 quy định hệ thống thông tin được phân loại thành 05 cấp độ, căn cứ vào mức độ tổn hại có thể xảy ra đối với an ninh quốc gia, trật tự, an toàn xã hội và quyền, lợi ích hợp pháp của tổ chức, cá nhân khi hệ thống bị xâm phạm hoặc gặp sự cố. Việc phân loại từ cấp độ 1 (chỉ gây ảnh hưởng trong phạm vi tổ chức, cá nhân quản lý) đến cấp độ 5 (gây tổn hại đặc biệt nghiêm trọng đến an ninh quốc gia) là căn cứ pháp lý để xác định yêu cầu và trách nhiệm bảo vệ tương ứng.

- Áp dụng biện pháp bảo vệ an ninh mạng phù hợp với từng cấp độ hệ thống: Trên cơ sở phân loại theo cấp độ, Điều 10 quy định trách nhiệm bảo vệ an ninh mạng theo hướng tương xứng với mức độ rủi ro:

+ Đối với hệ thống thông tin cấp độ 1 và cấp độ 2, chủ quản hệ thống được chủ động lựa chọn và áp dụng các biện pháp bảo vệ phù hợp với nhu cầu, điều kiện và khả năng thực tế.

+ Đối với hệ thống thông tin cấp độ 3 và cấp độ 4 (không thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia), bắt buộc phải triển khai một số biện pháp bảo vệ cơ bản, bao gồm ban hành quy định nội bộ; áp dụng tiêu chuẩn, quy chuẩn kỹ thuật; xây dựng tường lửa; tổ chức sao lưu dữ liệu; thực hiện giám sát và ứng phó sự cố. Quy định này vừa bảo đảm yêu cầu an ninh mạng, vừa góp phần tối ưu hóa chi phí tuân thủ đối với doanh nghiệp, nhất là doanh nghiệp nhỏ và vừa.

- Thiết lập chế độ bảo vệ nghiêm ngặt đối với hệ thống thông tin quan trọng về an ninh quốc gia: Đối với nhóm hệ thống thông tin có vai trò đặc biệt quan trọng (như hệ thống quân sự, an ninh, tài chính – ngân hàng, năng lượng, giao thông…), Luật quy định các yêu cầu bảo vệ ở mức cao nhất, bao gồm:

+ Phải được thẩm định an ninh mạng và chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng.

+ Thực hiện giám sát an ninh mạng thường xuyên; tự kiểm tra an ninh mạng định kỳ hằng năm và thông báo kết quả kiểm tra bằng văn bản cho lực lượng chuyên trách trước tháng 10 hằng năm.

+ Xây dựng cơ chế tự cảnh báo, phương án ứng phó và khắc phục sự cố, đồng thời phối hợp chặt chẽ với Bộ Công an, Bộ Quốc phòng trong giám sát và xử lý các tình huống liên quan đến an ninh mạng.

Cơ chế bảo vệ an ninh mạng theo cấp độ nêu trên tạo điều kiện để Nhà nước và xã hội tập trung, sử dụng hiệu quả nguồn lực nhằm bảo vệ vững chắc các hạ tầng trọng yếu, bảo đảm sự an toàn, ổn định và khả năng vận hành liên tục của các hệ thống thông tin quan trọng về an ninh quốc gia trước các nguy cơ, thách thức trên không gian mạng.

4. Tăng cường trách nhiệm của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam

Luật An ninh mạng năm 2025 đánh dấu sự chuyển đổi quan trọng trong cách tiếp cận quản lý nhà nước đối với doanh nghiệp cung cấp dịch vụ trên không gian mạng, theo đó chuyển từ cơ chế phối hợp mang tính tự nguyện sang xác lập nghĩa vụ pháp lý bắt buộc, áp dụng thống nhất đối với cả doanh nghiệp trong nước và doanh nghiệp nước ngoài hoạt động tại Việt Nam. Việc quy định rõ các trách nhiệm cụ thể nhằm bảo đảm tính nghiêm minh, hiệu lực và hiệu quả trong công tác quản lý nhà nước về an ninh mạng, cụ thể như sau:

- Quy định rõ thời hạn bắt buộc trong việc xử lý thông tin vi phạm: Luật đã khắc phục tình trạng chậm trễ trong việc ngăn chặn, gỡ bỏ thông tin xấu, độc trên không gian mạng thông qua việc xác lập thời hạn thực hiện cụ thể. Theo điểm b khoản 2 Điều 25, Doanh nghiệp trong nước và nước ngoài khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin, gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm quy định của Luật này chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và lưu nhật ký hệ thống để phục vụ xác minh, điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của pháp luật; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, yêu cầu ngăn chặn, xóa bỏ thông tin chậm nhất là 06 giờ, bảo đảm khả năng phản ứng nhanh trước các tình huống đột xuất.

- Yêu cầu doanh nghiệp chủ động triển khai biện pháp phòng ngừa bằng kỹ thuật và quản lý: Luật không chỉ dừng lại ở yêu cầu xử lý theo đề nghị của cơ quan có thẩm quyền, mà còn đặt ra nghĩa vụ chủ động đối với doanh nghiệp. Theo khoản 1 Điều 14, chủ quản hệ thống thông tin và doanh nghiệp cung cấp dịch vụ phải triển khai các biện pháp quản lý và kỹ thuật cần thiết nhằm phòng ngừa, phát hiện, ngăn chặn và gỡ bỏ kịp thời các thông tin có nội dung vi phạm pháp luật, như tuyên truyền chống Nhà nước, kích động bạo loạn, phá rối an ninh, trật tự hoặc xâm phạm quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- Thiết lập chế tài ngừng cung cấp dịch vụ đối với trường hợp vi phạm nghiêm trọng: Để xử lý triệt để nguồn phát tán thông tin vi phạm, Luật quy định rõ trách nhiệm của doanh nghiệp trong việc không cung cấp hoặc ngừng cung cấp dịch vụ đối với các tổ chức, cá nhân đăng tải thông tin có nội dung vi phạm nghiêm

trọng khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.

Các quy định nêu trên góp phần nâng cao vai trò và trách nhiệm xã hội của doanh nghiệp trong môi trường số, khẳng định doanh nghiệp không chỉ là chủ thể kinh doanh vì lợi nhuận mà còn là một mắt xích quan trọng trong hệ thống bảo vệ an ninh mạng quốc gia, hướng tới xây dựng không gian mạng an toàn, lành mạnh và bền vững cho người sử dụng.

5. Khẳng định bảo đảm an ninh dữ liệu là bộ phận quan trọng của bảo vệ an ninh mạng

Luật An ninh mạng năm 2025 thể hiện sự thay đổi căn bản trong tư duy quản lý nhà nước về an ninh mạng, từ cách tiếp cận chủ yếu tập trung bảo vệ hạ tầng kỹ thuật sang bảo vệ dữ liệu - tài nguyên số có giá trị cốt lõi của nền kinh tế số và xã hội số. Lần đầu tiên, khái niệm "an ninh dữ liệu" được luật hóa một cách đầy đủ, xác lập vị trí độc lập trong hệ thống pháp luật, với các nội dung trọng tâm sau đây:

- Xác lập an ninh dữ liệu như một khái niệm pháp lý độc lập và toàn diện. Khác với các quy định trước đây chỉ đề cập rải rác đến bảo vệ dữ liệu dưới góc độ an toàn thông tin, Luật An ninh mạng năm 2025 đã đưa ra định nghĩa riêng về "an ninh dữ liệu" tại khoản 3 Điều 2. Theo đó, an ninh dữ liệu không chỉ dừng lại ở việc phòng, chống truy cập trái phép, phá hoại hoặc đánh cắp dữ liệu, mà còn bao gồm yêu cầu bảo đảm tính toàn vẹn, độ chính xác, tính sẵn sàng và khả năng khai thác hiệu quả của dữ liệu nhằm phục vụ phát triển kinh tế - xã hội và chuyển đổi số quốc gia. Quy định này đặt nền tảng pháp lý cho việc bảo vệ chất lượng và giá trị sử dụng của dữ liệu, coi dữ liệu là nguồn lực chiến lược của quốc gia.

- Thiết lập hành lang pháp lý toàn diện để bảo đảm an ninh dữ liệu. Tại Điều 26, Luật quy định cụ thể các biện pháp bảo đảm an ninh dữ liệu, bao gồm việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật; sử dụng mật mã bảo vệ dữ liệu; kiểm soát nhân sự tham gia xử lý dữ liệu; và thực hiện đánh giá rủi ro an ninh dữ liệu một cách định kỳ. Đáng chú ý, Luật lần đầu tiên đặt ra yêu cầu kiểm tra, đánh giá việc chuyển dữ liệu xuyên biên giới, qua đó tăng cường năng lực quản lý nhà nước đối với dòng chảy dữ liệu, nhất là dữ liệu quan trọng, dữ liệu cốt lõi, nhằm ngăn ngừa nguy cơ thất thoát hoặc bị lợi dụng gây phương hại đến lợi ích quốc gia.

- Tăng cường chế tài xử lý vi phạm dữ liệu tại Việt Nam. Nhằm xử lý triệt để tình trạng thu thập, mua bán, trao đổi dữ liệu trái phép, Luật quy định rõ tại điểm h khoản 2 Điều 7 hành vi thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân là hành vi bị nghiêm cấm. Đây là cơ sở pháp lý quan trọng để tăng cường khả năng kiểm soát, thanh tra, xử lý vi phạm và bảo vệ quyền, lợi ích hợp pháp của người dùng Việt Nam.

Thông qua các quy định nêu trên, Luật An ninh mạng năm 2025 đã hình thành khung pháp lý tương đối đầy đủ về an ninh dữ liệu, tạo nền tảng cho việc phòng ngừa, phát hiện và xử lý các hành vi xâm phạm dữ liệu, qua đó góp phần

bảo vệ an ninh quốc gia, trật tự, an toàn xã hội và củng cố niềm tin của người dân, doanh nghiệp trong môi trường số.

6. Bổ sung, tăng cường các quy định về bảo vệ trẻ em trên không gian mạng, đồng thời mở rộng yêu cầu bảo vệ đối với người cao tuổi và người có khó khăn trong nhận thức, làm chủ hành vi

Luật An ninh mạng năm 2025 tiếp tục khẳng định quan điểm nhất quán của Nhà nước trong việc bảo vệ con người làm trung tâm của quá trình chuyển đổi số, đặc biệt là trẻ em và các nhóm đối tượng dễ bị tổn thương trên không gian mạng. Luật không chỉ tăng cường các biện pháp bảo vệ trẻ em, mà còn mở rộng yêu cầu bảo vệ đối với người cao tuổi và người có khó khăn trong nhận thức, làm chủ hành vi. Các quy định này được thiết kế theo hướng xác định rõ trách nhiệm của các chủ thể liên quan, bảo đảm sự phối hợp đồng bộ giữa gia đình, nhà trường và doanh nghiệp cung cấp dịch vụ trên không gian mạng.

- Luật hóa trách nhiệm của gia đình trong việc quản lý, giám sát hoạt động của trẻ em trên không gian mạng. Nhằm khắc phục tình trạng trẻ em tự ý đăng ký, sử dụng các dịch vụ mạng xã hội, trò chơi trực tuyến và các dịch vụ giá trị gia tăng khác mà không có sự kiểm soát, khoản 2 Điều 16 quy định rõ cha, mẹ hoặc người giám hộ có trách nhiệm quản lý, giám sát việc trẻ em truy cập, sử dụng thông tin và dịch vụ trên không gian mạng. Trường hợp trẻ em sử dụng các dịch vụ yêu cầu đăng ký tài khoản, cha, mẹ hoặc người giám hộ phải đứng tên đăng ký và chịu trách nhiệm đối với việc sử dụng tài khoản đó. Quy định này nhằm gắn trách nhiệm pháp lý cụ thể của gia đình với hành vi của trẻ em, qua đó tăng cường hiệu quả phòng ngừa từ sớm.

- Xác lập nghĩa vụ chủ động của doanh nghiệp trong việc phòng ngừa và xử lý nội dung xâm hại trẻ em. Luật chuyển cách tiếp cận từ yêu cầu xử lý bị động sang yêu cầu doanh nghiệp phải chủ động bảo vệ người sử dụng, nhất là trẻ em. Theo quy định tại khoản 3 Điều 16 và khoản 2 Điều 25, doanh nghiệp cung cấp dịch vụ trên không gian mạng có trách nhiệm triển khai các biện pháp kỹ thuật và biện pháp quản lý cần thiết để phát hiện, ngăn chặn, gỡ bỏ kịp thời các thông tin có nội dung xâm hại trẻ em, kích động bạo lực, khiêu dâm, đồi trụy hoặc lôi kéo trẻ em tham gia các hành vi vi phạm pháp luật. Đồng thời, doanh nghiệp phải thiết lập cơ chế, công cụ thuận tiện để người sử dụng phản ánh, tố giác nhanh chóng các nội dung xấu, độc liên quan đến trẻ em.

- Mở rộng phạm vi bảo vệ đối với người cao tuổi và người có khó khăn trong nhận thức, làm chủ hành vi. Xuất phát từ thực tiễn cho thấy người cao tuổi và người có hạn chế về nhận thức, khả năng làm chủ hành vi là nhóm đối tượng dễ trở thành nạn nhân của các hành vi lừa đảo, chiếm đoạt tài sản trên không gian mạng, khoản 5 Điều 16 đã bổ sung quy định yêu cầu cơ quan nhà nước có thẩm quyền và doanh nghiệp cung cấp dịch vụ trên không gian mạng phải có cơ chế hỗ trợ phù hợp, cảnh báo sớm các nguy cơ, đồng thời ưu tiên tiếp nhận, xử lý các phản ánh, khiếu nại, tố giác liên quan đến hành vi lừa đảo mạng đối với nhóm đối tượng này.

Các quy định trên đã thiết lập một hành lang pháp lý tương đối toàn diện, buộc các chủ thể liên quan cùng tham gia trách nhiệm bảo vệ trẻ em và các nhóm yếu thế trên không gian mạng. Trọng tâm của các quy định không chỉ là xử lý vi phạm, mà là phòng ngừa, ngăn chặn từ sớm, qua đó góp phần xây dựng môi trường số an toàn, lành mạnh và nhân văn.

7. Khuyến khích nghiên cứu, phát triển và ứng dụng khoa học, công nghệ trong lĩnh vực an ninh mạng; ưu tiên đầu tư hạ tầng, sản phẩm và dịch vụ an ninh mạng trong nước

Luật An ninh mạng năm 2025 thể hiện tầm nhìn chiến lược dài hạn của Nhà nước trong lĩnh vực an ninh mạng, theo đó xác định an ninh mạng không chỉ là nhiệm vụ bảo vệ mang tính kỹ thuật đơn thuần, mà là quá trình xây dựng năng lực tự chủ về công nghệ, hình thành nền công nghiệp an ninh mạng trong nước, từng bước bảo đảm chủ quyền số quốc gia. Quan điểm này được cụ thể hóa thông qua hệ thống các cơ chế ưu đãi, hỗ trợ và đầu tư đồng bộ nhằm thúc đẩy nghiên cứu, phát triển và ứng dụng khoa học, công nghệ trong lĩnh vực an ninh mạng, cụ thể như sau:

- Xác lập công nghiệp an ninh mạng là ngành, nghề đặc biệt ưu đãi đầu tư. Tại Điều 37, Luật quy định hoạt động đầu tư, kinh doanh sản phẩm, dịch vụ an ninh mạng và xây dựng hạ tầng kỹ thuật bảo vệ an ninh mạng thuộc danh mục ngành, nghề đặc biệt ưu đãi đầu tư. Trên cơ sở đó, Nhà nước áp dụng các chính sách ưu đãi cao về thuế, đất đai và thủ tục hành chính nhằm khuyến khích tổ chức, doanh nghiệp trong và ngoài nước đầu tư vào nghiên cứu, phát triển công nghệ an ninh mạng. Đây là cơ sở pháp lý quan trọng để hình thành các trung tâm nghiên cứu và phát triển, khu công nghiệp chuyên ngành an ninh mạng và các phòng thí nghiệm trọng điểm phục vụ nghiên cứu, thử nghiệm và làm chủ công nghệ bảo mật.

- Thiết lập cơ chế ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng sản xuất trong nước. Nhằm tạo thị trường ổn định cho doanh nghiệp công nghệ trong nước, khoản 4 Điều 3 quy định rõ cơ quan, tổ chức nhà nước ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng được sản xuất trong nước khi đáp ứng yêu cầu về kỹ thuật, chất lượng và an ninh. Quy định này không mang tính áp đặt, mà đóng vai trò định hướng thị trường, tạo động lực để các doanh nghiệp trong nước mạnh dạn đầu tư nghiên cứu, phát triển sản phẩm, từng bước thay thế các giải pháp nhập khẩu và nâng cao năng lực cạnh tranh của ngành công nghiệp an ninh mạng Việt Nam.

- Bảo đảm nguồn lực tài chính ổn định cho hoạt động đổi mới sáng tạo trong an ninh mạng. Khắc phục tình trạng thiếu nguồn lực đầu tư cho công tác bảo vệ an ninh mạng trong quá trình chuyển đổi số, khoản 1 Điều 38 của Luật quy định cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội và các đơn vị sự nghiệp công lập do ngân sách nhà nước bảo đảm phải bố trí kinh phí bảo vệ an ninh mạng trong dự toán chi thực hiện nhiệm vụ chuyển đổi số, ứng dụng công nghệ thông tin hàng năm của cơ quan, tổ chức, đơn vị mình; bố trí tối thiểu 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin để bảo vệ an ninh mạng. Quy định này tạo cơ sở tài chính bền vững để triển khai đồng bộ các giải pháp bảo mật,

đồng thời thúc đẩy việc nghiên cứu, ứng dụng các công nghệ mới như trí tuệ nhân tạo, dữ liệu lớn và chuỗi khối trong công tác phòng ngừa, phát hiện và xử lý tấn công mạng.

Thông qua các chính sách nêu trên, Luật An ninh mạng năm 2025 từng bước hình thành hệ sinh thái công nghiệp an ninh mạng trong nước, nâng cao năng lực làm chủ công nghệ, giảm dần sự phụ thuộc vào các giải pháp công nghệ nước ngoài, qua đó góp phần bảo đảm an ninh mạng quốc gia theo hướng độc lập, tự chủ và bền vững trong dài hạn.

8. Quy định việc bố trí nguồn lực phù hợp cho bảo đảm an ninh mạng trong các chương trình, đề án, dự án đầu tư chuyển đổi số và ứng dụng công nghệ thông tin

Luật An ninh mạng năm 2025 thể hiện quan điểm xuyên suốt và mang tính thực tiễn cao của Nhà nước trong lĩnh vực an ninh mạng, theo đó xác định bảo đảm an ninh mạng là yêu cầu bắt buộc, phải được đặt ra ngay từ khâu thiết kế, lập dự toán và triển khai các chương trình, đề án, dự án chuyển đổi số và ứng dụng công nghệ thông tin. Lần đầu tiên, pháp luật quy định cụ thể, định lượng về nguồn lực tài chính dành cho bảo vệ an ninh mạng, qua đó khắc phục tình trạng coi nhẹ hoặc cắt giảm chi phí bảo mật trong quá trình đầu tư công nghệ.

Thứ nhất, luật hóa tỷ lệ kinh phí tối thiểu dành cho bảo đảm an ninh mạng. Tại khoản 1 Điều 38, Luật quy định rõ các cơ quan, tổ chức sử dụng ngân sách nhà nước khi lập dự toán cho các chương trình, đề án, dự án chuyển đổi số hoặc ứng dụng công nghệ thông tin phải bố trí tối thiểu 15% tổng kinh phí thực hiện để đầu tư cho hạng mục bảo vệ an ninh mạng. Quy định này tạo cơ sở pháp lý bắt buộc, bảo đảm an ninh mạng không bị xem là hạng mục phụ hoặc bị cắt giảm khi cân đối ngân sách.

Thứ hai, bảo đảm đầu tư đồng bộ giữa hệ thống công nghệ và giải pháp bảo vệ an ninh mạng. Theo quy định tại khoản 2 Điều 38, nguồn kinh phí dành cho bảo đảm an ninh mạng được sử dụng để đầu tư trang thiết bị kỹ thuật, mua sắm giải pháp bảo mật chuyên sâu, thuê dịch vụ giám sát, ứng cứu sự cố an ninh mạng, cũng như đào tạo, bồi dưỡng nhân lực chuyên trách. Cách tiếp cận này khắc phục tình trạng đầu tư hình thức, manh mún, đồng thời bảo đảm mỗi hệ thống thông tin khi đưa vào vận hành đều được trang bị đầy đủ các biện pháp bảo vệ tương xứng với quy mô và mức độ rủi ro ngay từ đầu.

Thứ ba, tạo nền tảng tài chính cho tính bền vững của quá trình chuyển đổi số. Việc quy định rõ và thống nhất về nguồn lực tài chính cho bảo đảm an ninh mạng thể hiện cam kết mạnh mẽ của Nhà nước trong việc gắn an ninh mạng với phát triển bền vững. Các hệ thống thông tin được bảo vệ đầy đủ sẽ vận hành ổn định, an toàn trước các nguy cơ, thách thức an ninh mạng ngày càng gia tăng, qua đó nâng cao hiệu quả đầu tư công, hạn chế rủi ro, thất thoát và bảo đảm tính liên tục của các hoạt động kinh tế - xã hội trong môi trường số.

Quy định này là cơ sở pháp lý quan trọng để các bộ, ngành, địa phương và chủ đầu tư có căn cứ lập, thẩm định và phê duyệt dự toán kinh phí; đồng thời nâng

cao trách nhiệm của người đứng đầu cơ quan, tổ chức trong việc bảo đảm nguồn lực cho công tác an ninh mạng, góp phần triển khai hiệu quả các mục tiêu chuyển đổi số quốc gia.

9. Tạo cơ sở pháp lý để mở rộng và tăng cường hợp tác quốc tế về an ninh mạng trên cơ sở tôn trọng độc lập, chủ quyền và lợi ích quốc gia; đồng thời nội luật hóa các nội dung cơ bản của Công ước Liên hợp quốc về phòng, chống tội phạm mạng (Công ước Hà Nội)

Luật An ninh mạng năm 2025 thể hiện rõ tư duy đối ngoại chủ động, tích cực của Việt Nam trong lĩnh vực an ninh mạng, xuất phát từ nhận thức rằng an ninh mạng là vấn đề mang tính toàn cầu, vượt qua biên giới quốc gia và không thể giải quyết một cách đơn lẻ. Trên cơ sở đó, Luật đã thiết lập khung pháp lý tương đối toàn diện, tạo điều kiện để Việt Nam tham gia sâu hơn, thực chất hơn vào các cơ chế hợp tác quốc tế về an ninh mạng, đồng thời bảo đảm vững chắc lợi ích quốc gia, dân tộc.

- Khẳng định nguyên tắc hợp tác quốc tế gắn với bảo vệ chủ quyền quốc gia. Tại khoản 1 Điều 6, Luật quy định việc hợp tác quốc tế về an ninh mạng phải tuân thủ các nguyên tắc tôn trọng độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của mỗi quốc gia; không can thiệp vào công việc nội bộ của nhau; bảo đảm bình đẳng, cùng có lợi và phù hợp với pháp luật Việt Nam. Quy định này xác lập rõ giới hạn pháp lý trong quá trình hợp tác, qua đó bảo đảm hội nhập quốc tế về an ninh mạng không làm phương hại đến an ninh quốc gia, đồng thời khẳng định vị thế, quyền bình đẳng của Việt Nam trong các cơ chế quản trị internet và không gian mạng toàn cầu.

- Nội luật hóa các cam kết quốc tế, đặc biệt là Công ước Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội). Luật An ninh mạng năm 2025 đã cập nhật, bổ sung các quy định nhằm bảo đảm tính tương thích với các điều ước quốc tế mà Việt Nam là thành viên, trong đó có Công ước Hà Nội. Theo quy định tại khoản 2 Điều 6, tạo cơ sở để thực hiện hợp tác quốc tế về phòng, chống tội phạm mạng theo điều ước quốc tế mà Việt Nam là thành viên và pháp luật Việt Nam, tạo cơ sở pháp lý để các cơ quan có thẩm quyền như Bộ Công an, Viện kiểm sát nhân dân thực hiện hiệu quả các hoạt động tương trợ tư pháp, dẫn độ, chuyển giao người phạm tội và thu thập, trao đổi chứng cứ điện tử xuyên biên giới theo đúng trình tự, thủ tục pháp luật.

- Thiết lập cơ chế hợp tác thực chất thông qua chia sẻ thông tin và phối hợp nghiệp vụ. Nhằm nâng cao hiệu quả phòng, chống các loại tội phạm mạng có tính chất xuyên quốc gia, khoản 3 Điều 6 quy định cụ thể các nội dung hợp tác quốc tế, bao gồm: thiết lập và duy trì kênh liên lạc trực tiếp với các tổ chức an ninh mạng quốc tế và cơ quan thực thi pháp luật nước ngoài; trao đổi, chia sẻ thông tin về nguy cơ, phương thức, thủ đoạn tấn công mạng; phối hợp tổ chức diễn tập, đào tạo, nâng cao năng lực cho lực lượng chuyên trách. Đây là cơ sở pháp lý để tăng cường khả năng phản ứng nhanh, xử lý kịp thời các sự cố và truy vết tội phạm mạng vượt ra ngoài phạm vi lãnh thổ quốc gia.

PHẦN III. TỔ CHỨC THỰC HIỆN

Để kịp thời triển khai thi hành Luật, ngày 16/3/2026, Thủ tướng Chính phủ ban hành Quyết định số 437/QĐ-TTg ban hành Kế hoạch triển khai thi hành Luật An ninh mạng năm 2025, các bộ, cơ quan ngang bộ, Ủy ban nhân dân các cấp và các cơ quan, tổ chức có liên quan ở trung ương và địa phương có trách nhiệm: Tổ chức tuyên truyền, phổ biến nội dung của Luật An ninh mạng và các điểm mới của Luật này bằng các hình thức đa dạng, phù hợp với điều kiện, tình hình thực tế; tổ chức thực hiện các chuyên mục, chương trình, tin, bài phổ biến Luật An ninh mạng, các văn bản quy phạm pháp luật quy định chi tiết Luật này trên các phương tiện thông tin đại chúng hoặc các hình thức khác theo quy định của pháp luật về phổ biến, giáo dục pháp luật.

Có thể khẳng định, việc thay thế, hợp nhất các quy định của Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 bằng Luật An ninh mạng năm 2025 không chỉ góp phần nâng cao vị thế và uy tín của Việt Nam trong hợp tác quốc tế về an ninh mạng, mà còn tạo cơ sở pháp lý để cơ quan có thẩm quyền phòng ngừa, phát hiện, xử lý hành vi vi phạm pháp luật trên không gian mạng một cách hiệu quả, đáp ứng yêu cầu bảo vệ an ninh quốc gia trong bối cảnh hội nhập sâu rộng trong tình hình mới./.