Định danh IP và chi phí “10% ngân sách”: Hai chính sách đột phá thay đổi an ninh mạng Việt Nam

17/11/2025 08:26

QUANG MINH

Trong bối cảnh tội phạm mạng ngày càng tinh vi và nguy hiểm, an ninh mạng không còn là chi phí tùy chọn mà đã trở thành chiến lược bắt buộc để bảo vệ chủ quyền số quốc gia. Dự thảo Luật An ninh mạng mới đang được giới chuyên môn đánh giá cao bởi hai nội dung được xem là then chốt, có khả năng thay đổi cục diện an ninh mạng Việt Nam: Yêu cầu Định danh địa chỉ IP và quy định tối thiểu 10% ngân sách cho an ninh mạng.

Siết chặt quản lý: Đưa "căn cước" cho không gian mạng

Trong không gian mạng, địa chỉ IP (Internet Protocol) được ví như "địa chỉ địa lý" đơn nhất, là căn cước bắt buộc cho phép các thiết bị điện tử liên lạc, trao đổi thông tin. Việc xác định được IP giống như xác định thông tin cư trú, cho phép lực lượng chức năng truy vết địa điểm, thời gian và thông tin thuê bao sử dụng.

Tuy nhiên, việc quản lý IP hiện nay đang tồn tại những bất cập lớn. Mặc dù Bộ Khoa học và Công nghệ (thông qua VNNIC) quản lý cấp phát các khối IP, nhưng chính các nhà cung cấp dịch vụ Internet (ISP) mới là chủ thể định danh, quản lý và cấp phát IP cho khách hàng. Các địa chỉ này thường xuyên thay đổi mà chưa có cơ quan chức năng nào quản lý về an ninh trật tự.

Thực tiễn cho thấy, việc khai thác thông tin IP để phục vụ công tác bảo đảm an ninh quốc gia và an toàn xã hội đang gặp nhiều khó khăn. Tỷ lệ tra cứu địa chỉ IP có thông tin thuê bao rất thấp, và thời gian tra cứu rất chậm, gây khó khăn lớn cho công tác nghiệp vụ và đấu tranh phòng chống tội phạm. Lực lượng chức năng phải

phụ thuộc hoàn toàn vào mức độ phối hợp của doanh nghiệp thông qua cơ chế "xin - cho".

Sự phụ thuộc này đã làm phát sinh các hành vi tiêu cực tại một số doanh nghiệp như: mua bán thông tin, cơ chế riêng trong việc cung cấp thông tin, dẫn đến nguy cơ bị lộ lọt thông tin và hoạt động nghiệp vụ của lực lượng công an.

Về mặt kỹ thuật, việc định danh, quản lý toàn bộ địa chỉ IP cấp phát là hoàn toàn khả thi, bởi các doanh nghiệp vốn đã chủ động thực hiện việc này để tính cước và thu phí. Tuy nhiên, họ lại không chủ động cung cấp thông tin phục vụ an ninh trật tự, thậm chí từ chối giải pháp kỹ thuật API (giao diện lập trình ứng dụng) cho phép lực lượng công an kết nối chủ động tra cứu.

Để khắc phục triệt để, Dự thảo Luật An ninh mạng quy định các doanh nghiệp cung cấp dịch vụ Internet tại Việt Nam có trách nhiệm: Định danh, quản lý tập trung thông tin sử dụng địa chỉ IP và cung cấp thông tin này cho lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Công an theo cơ chế kỹ thuật nhanh chóng, chuẩn hóa (API).

Luật sư Trương Anh Tú, Chủ tịch TAT Law Firm, nhận định yêu cầu định danh và quản lý tập trung IP là bước nâng chuẩn an ninh số, phù hợp với thông lệ quốc tế, đồng thời là nền tảng để điều tra, truy vết và ứng phó kịp thời với tấn công mạng có tổ chức.

Tuy nhiên, Đại biểu Chu Thị Hồng Thái, Đại biểu Quốc hội đoàn Đại biểu tỉnh Lạng Sơn đã góp ý rằng việc quy định doanh nghiệp cung cấp thông tin khi có yêu cầu bằng “văn bản hoặc thư điện tử, điện thoại hoặc một hình thức trao đổi khác đã được xác nhận” là quá rộng và không rõ ràng, tiềm ẩn rủi ro bị lạm dụng.

Đại biểu đề nghị việc cung cấp thông tin phải được thực hiện bằng văn bản điện tử có xác thực hoặc hệ thống kết nối chính thức giữa doanh nghiệp và cơ quan nhà nước, đảm bảo nguyên tắc bảo vệ dữ liệu cá nhân.

Luật hóa 10% ngân sách: An ninh là chi phí bắt buộc

Chính sách quan trọng thứ hai là việc luật hóa quy định kinh phí bảo vệ an ninh mạng của cơ quan, tổ chức, doanh nghiệp nhà nước và tổ chức chính trị phải bảo đảm tối thiểu 10% trong tổng kinh phí triển khai các dự án công nghệ thông tin.

Đây không phải là quy định mới, mà là mức thông lệ chung trên thế giới và đã được nhắc đến tại nhiều văn bản quan trọng của Thủ tướng Chính phủ, nhằm cải thiện chỉ số xếp hạng an toàn, an ninh mạng quốc gia của Việt Nam.

Các luật sư, chuyên gia nhận định, trong nhiều năm qua, các cơ quan, tổ chức thường có xu hướng dồn phần lớn ngân sách vào việc phát triển hạ tầng, ứng dụng và chuyển đổi số (phần nhìn thấy được) nhưng lại coi an ninh mạng (phần phòng thủ) là chi phí tùy chọn hoặc không đáng kể. Sự chênh lệch này đã tạo ra những lỗ hổng lớn trong các hệ thống thông tin quan trọng của quốc gia.

Quy định 10% buộc các cơ quan phải thay đổi tư duy, xem an ninh mạng là một chi phí bắt buộc, không thể thiếu, tương tự như chi phí bảo hiểm, bảo trì hoặc phòng cháy chữa cháy đối với một tòa nhà. Nếu không có chi phí dự phòng và đầu tư thích đáng, thiệt hại khi bị tấn công mạng (như mất dữ liệu, tê liệt hệ thống, rò rỉ thông tin quốc gia) có thể lớn hơn gấp nhiều lần so với số tiền tiết kiệm được.

Việc luật hóa mức trích tối thiểu 10% mang lại ý nghĩa chiến lược quan trọng. Cụ thể, quy định này đảm bảo các hệ thống công nghệ thông tin quan trọng (Hệ thống thông tin cấp độ 4, 5) sẽ có nguồn lực tài chính ổn định để đầu tư vào các giải pháp chuyên sâu như giám sát, phòng thủ, mua sắm các thiết bị an ninh chuyên dụng, và nâng cấp định kỳ. Việc này giúp cải thiện chỉ số xếp hạng an toàn, an ninh mạng quốc gia của Việt Nam trên bản đồ thế giới, chứng minh cam kết mạnh mẽ của Chính phủ trong việc bảo vệ không gian mạng.

Mức 10% là động lực mạnh mẽ để khuyến khích các cơ quan nhà nước sử dụng sản phẩm, dịch vụ công nghiệp an ninh mạng của Việt Nam. Khi có nhu cầu

ngân sách ổn định, thị trường nội địa sẽ phát triển, tạo điều kiện cho các doanh nghiệp công nghệ trong nước đầu tư nghiên cứu, phát triển các giải pháp bảo mật "Make in Vietnam" chất lượng cao, từ đó nâng cao năng lực tự chủ công nghệ quốc gia trong lĩnh vực quan trọng này.

Trong kỷ nguyên Chuyển đổi số, dữ liệu là tài sản. Mức chi phí 10% đảm bảo rằng an ninh dữ liệu và quản trị rủi ro luôn được đặt ngang hàng với việc phát triển ứng dụng. Đây là yêu cầu cấp thiết để bảo vệ dữ liệu cá nhân, dữ liệu tổ chức và dữ liệu quốc gia khỏi các nguy cơ chiếm đoạt, tiêu hủy, hoặc khai thác trái phép.

Tóm lại, quy định 10% không chỉ là một con số, mà là tuyên bố chính sách: An ninh mạng phải đi trước một bước so với tốc độ phát triển, đảm bảo rằng mọi bước tiến trong công nghệ đều được bảo vệ bằng một "lá chắn số" vững vàng.

“Quy định này hoàn toàn cần thiết vì nhiều cơ quan, doanh nghiệp Việt Nam đầu tư mạnh vào hạ tầng nhưng lại đầu tư quá ít cho an ninh, tạo ra lỗ hổng lớn. An ninh dữ liệu và quản trị rủi ro phải được coi là chi phí bắt buộc, giống như chi phí phòng cháy chữa cháy để tránh thiệt hại hàng trăm tỷ đồng khi bị tấn công mạng”, Luật sư Trương Anh Tú, Chủ tịch TAT Law Firm nhận định.

Tuy nhiên, Đại biểu Đinh Thị Ngọc Dung, Đoàn đại biểu Quốc hội TP.Hải Phòng bày tỏ sự cân nhắc đối với quy định này, cho rằng việc tách bạch kinh phí bảo vệ an ninh mạng trong một dự án phát triển công nghệ thông tin là khó khăn vì phần vận hành và phần bảo mật thường đi kèm, phát triển cùng nhau.

Bên cạnh vấn đề ngân sách, Dự thảo Luật cũng yêu cầu người đứng đầu hoặc người phụ trách hệ thống thông tin quan trọng phải tham gia sát hạch và được cấp chứng chỉ về an ninh mạng, nhằm đảm bảo chất lượng nhân lực chuyên trách.

Với hai chính sách đột phá về quản lý IP và đảm bảo nguồn lực tài chính, Dự thảo Luật An ninh mạng mới được kỳ vọng sẽ tạo ra một bước nhảy vọt trong công

tác bảo đảm an ninh quốc gia trên không gian mạng, củng cố niềm tin và thúc đẩy quá trình chuyển đổi số bền vững của đất nước.