NÂNG CAO NĂNG LỰC BẢO VỆ AN NINH DỮ LIỆU, AN NINH MẠNG CỦA LỰC LƯỢNG CÔNG AN NHÂN DÂN

NGUYỄN THỊ HOÀI THU*

Chuyển đổi số và sự bùng nổ của kinh tế dữ liệu đang tạo ra những thay đổi sâu sắc trong phương thức quản trị quốc gia, tổ chức đời sống xã hội và vận hành các hoạt động kinh tế. Bên cạnh những tác động tích cực, như: nâng cao hiệu quả quản lý, mở rộng không gian dịch vụ số và gia tăng năng lực kết nối, chia sẻ thông tin, tiến trình số hóa cũng đặt ra những thách thức. Trong bối cảnh đó, lực lượng Công an nhân dân có vai trò đặc biệt quan trọng trong phòng ngừa, phát hiện, đấu tranh với tội phạm mạng; đồng thời, bảo vệ an ninh dữ liệu và bảo đảm môi trường số an toàn, lành mạnh. Nâng cao năng lực bảo vệ an ninh dữ liệu, an ninh mạng của lực lượng Công an nhân dân vừa là yêu cầu khách quan của quá trình phát triển đất nước trong kỷ nguyên số, vừa là đòi hỏi mang tính chiến lược nhằm củng cố sức đề kháng cho an ninh quốc gia trước các rủi ro phi truyền thống.

Từ khóa: *An ninh mạng; an ninh dữ liệu; công an nhân dân; cách mạng 4.0; an toàn thông tin.*

Digital transformation and the rapid growth of the data economy are driving profound shifts in national governance, social organization, and economic activities. Although digitalization enhances administrative efficiency and information-sharing capacity, it simultaneously introduces sophisticated security vulnerabilities. In this landscape, the People's Public Security Forces serve as the vanguard in preventing, detecting, and combating cybercrime, while safeguarding data sovereignty and ensuring a secure digital ecosystem. Elevating their data security and cybersecurity capabilities is not only an objective necessity for national development in the digital era but also a strategic imperative to fortify national security against non-traditional threats.

Keywords: *Cybersecurity; data security; People's Public Security forces; Fourth Industrial Revolution; information security.*

NGÀY NHẬN: 20/12/2025 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 20/4/2026 NGÀY DUYỆT: 18/5/2026

DOI: https://doi.org/10.59394/qlnn.364.2026.1505

1. Đặt vấn đề

Không gian mạng được nhìn nhận như một môi trường xã hội - chính trị - kinh tế mới, nơi con người thực hiện hành vi xã hội không bị giới hạn bởi thời gian, không gian, vì vậy, các nguy cơ trên không gian mạng có thể chuyển hóa rất nhanh thành rủi ro an ninh truyền thống. Điều 2 *Luật An ninh mạng* năm 2018 xác định: an ninh mạng là sự bảo đảm 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

* *TS, Học viện Chính trị Công an nhân dân*

quan, tổ chức, cá nhân. Đồng thời, coi bảo vệ an ninh mạng là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng. Trong khi đó, an ninh dữ liệu có thể hiểu là trạng thái và năng lực bảo đảm dữ liệu (đặc biệt dữ liệu quan trọng, dữ liệu cá nhân và dữ liệu phục vụ hoạt động thiết yếu) được quản trị an toàn trong toàn bộ vòng đời: thu thập - xử lý - lưu trữ - chia sẻ - khai thác - hủy bỏ nhằm ngăn ngừa truy cập trái phép, sửa đổi, phá hủy, rò rỉ hoặc sử dụng sai mục đích. Khi dữ liệu trở thành "tư liệu sản xuất" và nền tảng cho quyết định quản trị thì một sự cố dữ liệu không chỉ là mất thông tin mà có thể là mất năng lực điều hành và mất niềm tin.

Do vậy, bảo vệ an ninh mạng, an ninh dữ liệu là yêu cầu trực tiếp để bảo vệ an ninh quốc gia và giữ vững trật tự, an toàn xã hội trong điều kiện xuất hiện ngày càng nhiều mối đe dọa phi truyền thống.

2. Vai trò của lực lượng Công an nhân dân trong việc bảo vệ an ninh dữ liệu, an ninh mạng

Trong bối cảnh công nghệ số toàn cầu, việc bảo vệ an ninh mạng và an ninh dữ liệu là điều kiện để bảo đảm hoạt động thông suốt của hệ thống cơ quan nhà nước, dịch vụ công và các hệ thống thông tin quan trọng, qua đó, giữ vững năng lực quản trị quốc gia trong môi trường số. Điều 5 *Luật An ninh mạng* năm 2018 đặt ra yêu cầu áp dụng các biện pháp bảo vệ (thẩm định, đánh giá, kiểm tra, giám sát, ứng phó sự cố, đấu tranh bảo vệ, sử dụng mật mã để bảo vệ thông tin mạng…) và nhấn mạnh tính chủ động trong phòng ngừa, phát hiện, ngăn chặn các nguy cơ đe dọa an ninh mạng. Yêu cầu này càng trở nên cấp bách trong bối cảnh Chính phủ thúc đẩy chính phủ số, đô thị thông minh, dữ liệu lớn (Big Data), trí tuệ nhân tạo (AI)… với mức độ liên thông càng cao và mức độ rủi ro lan truyền cũng càng lớn.

Đối với phát triển khoa học, công nghệ, bảo vệ an ninh mạng, an ninh dữ liệu là điều kiện an ninh của phát triển khoa học, công nghệ và đổi mới sáng tạo. Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030, nhấn mạnh định hướng chủ động ứng phó với thách thức từ không gian mạng; đồng thời, coi việc nâng cao năng lực phòng ngừa, giám sát, cảnh báo, ứng phó là trụ cột quan trọng để bảo vệ tiến trình chuyển đổi số. Thực tế, nếu thiếu một "lá chắn" đủ mạnh, các sáng kiến số có thể trở thành "điểm hở" mới, khi đó công nghệ mới bị lợi dụng để gia tăng rủi ro và thành quả đổi mới sáng tạo có thể bị triệt tiêu bởi sự cố an ninh. Trong bối cảnh đó, lực lượng Công an nhân dân có vai trò đặc biệt quan trọng, được nhận diện ở cả phương diện pháp lý lẫn phương diện thực tiễn quản trị an ninh quốc gia.

Thứ nhất, về phương diện pháp lý, Luật An ninh mạng năm 2018 đặt ra nguyên tắc huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; đồng thời, nhấn mạnh phát huy vai trò nòng cốt của Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an. Lực lượng này có chức năng thẩm định an ninh mạng và thực hiện nhiều hoạt động bảo đảm an toàn đối với hệ thống thông tin quan trọng về an ninh quốc gia. Bên cạnh đó, Nghị định số 52/2022/NĐ-CP ngày 15/8/2022 của Chính phủ cũng đã cụ thể hóa nhiều biện pháp bảo vệ, tạo cơ sở để triển khai đồng bộ từ thẩm định, đánh giá, kiểm tra, giám sát đến ứng phó, khắc phục sự cố và các cơ chế liên quan. *Về phương diện thực tiễn*, vai trò của Lực lượng Công an nhân dân thể hiện ở vai trò "lá chắn an ninh" đối với các nguy cơ đe dọa an ninh quốc gia và trật tự an toàn xã hội trên không gian mạng. Lực lượng Công an nhân dân vừa chủ động nắm tình hình, nhận diện phương thức, thủ đoạn mới, vừa tổ chức lực lượng, phương tiện để phòng ngừa và ngăn chặn từ sớm, từ xa; đồng thời, bảo đảm xử lý nghiêm minh hành vi vi phạm, qua đó, răn đe và củng cố kỷ cương.

Thứ hai, trực tiếp đảm nhận vai trò tác chiến nghiệp vụ số trong phòng, chống tội phạm công nghệ cao. Điểm khác biệt của đấu tranh tội phạm mạng là chứng cứ chủ yếu tồn tại dưới dạng điện tử; dấu vết có thể bị xóa nhanh; đối tượng phạm tội có thể ở ngoài lãnh thổ. Do vậy, năng lực điều tra số, thu thập - bảo toàn - giám định dữ liệu, phân tích kỹ thuật và phối hợp liên ngành trở thành yêu cầu cốt lõi. Nếu không nâng cấp năng lực theo hướng hiện đại, việc xử lý sẽ rơi vào tình thế đuổi theo xử lý sự cố, vừa tốn kém nguồn lực vừa khó tạo hiệu quả bền vững.

Thứ ba, vai trò kiến tạo thể chế và chuẩn mực thực thi nhằm xây dựng môi trường số an toàn, lành mạnh. Điều này thể hiện ở việc tham gia hoàn thiện cơ chế, chính sách; ban hành và chuẩn hóa quy trình phối hợp; thúc đẩy nâng cao nhận thức cộng đồng về bảo vệ dữ liệu; đồng thời, tổ chức thanh tra, kiểm tra, xử lý vi phạm theo thẩm quyền trong lĩnh vực bảo vệ dữ liệu cá nhân.

3. Thực trạng công tác bảo vệ an ninh dữ liệu, an ninh mạng của lực lượng Công an nhân dân

3.1. Bối cảnh chuyển đổi số và cơ sở pháp lý về bảo vệ an ninh dữ liệu, an ninh mạng

Thời gian qua, các chương trình, chiến lược quốc gia về chuyển đổi số và chính phủ số đã thúc đẩy mạnh mẽ việc số hóa quy trình, liên thông - chia sẻ dữ liệu, mở rộng dịch vụ công trực tuyến. Qua đó, tạo ra động lực nâng cao hiệu lực quản trị, chất lượng phục vụ người dân và doanh nghiệp. Ngày 03/6/2020, Thủ tướng Chính phủ đã ban hành Quyết định số 749/QĐ-TTg phê duyệt Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030, tạo khung định hướng cho phát triển chính phủ số, kinh tế số, xã hội số; đồng thời, yêu cầu bảo đảm an toàn, an ninh trong toàn bộ hệ sinh thái số. Tiếp đó, Quyết định số 942/QĐ-TTg ngày 15/6/2021 phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030, tiếp tục nhấn mạnh yêu cầu phát triển gắn với quản trị dữ liệu và bảo đảm an toàn thông tin trong vận hành các hệ thống số của khu vực công.

Ngày 22/12/2024, Bộ Chính trị ban hành Nghị quyết số 57-NQ/TW về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia, xác định chuyển đổi số quốc gia là đột phá quan trọng, quyết định sự phát triển của quốc gia; đồng thời, đặt ra yêu cầu phải bảo đảm chủ quyền quốc gia trên không gian mạng; bảo đảm an ninh mạng, an ninh dữ liệu, an toàn thông tin của tổ chức và cá nhân. Chính phủ đã ban hành Nghị quyết số 03/NQ-CP ngày 09/01/2025 và Nghị quyết số 71/NQ-CP ngày 01/4/2025 cập nhật, bổ sung chương trình hành động, cụ thể hóa chủ trương của Nghị quyết số 57-NQ/TW. Qua đó, tạo cơ sở để tổ chức triển khai đồng bộ các nhiệm vụ về thể chế, hạ tầng, dữ liệu, nhân lực và an toàn, an ninh trong tiến trình chuyển đổi số.

Về hành lang pháp lý chuyên ngành, khuôn khổ bảo vệ an ninh mạng được xác lập bởi *Luật An ninh mạng* năm 2018 và Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 đã tạo nền tảng pháp lý cho hoạt động phòng ngừa, phát hiện, ngăn chặn và xử lý hành vi xâm phạm an ninh mạng. Đồng thời, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân cũng đã xác lập rõ trách nhiệm của các chủ thể xử lý dữ liệu và cơ chế tổ chức thực thi. Đặc biệt, *Luật Dữ liệu* năm 2024 và Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 quy định chi tiết một số điều và biện pháp thi hành *Luật Dữ liệu*, cùng Quyết định số 20/2025/QĐ-TTg ngày 01/7/2025 của Thủ tướng Chính phủ ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi đã bổ sung các tầng quản trị dữ liệu theo hướng coi dữ liệu là tài sản chiến lược cần được quản trị - bảo vệ - giảm thiểu rủi ro một cách hệ thống. Đây là nền tảng thuận lợi để lực lượng Công an nhân dân triển khai nhiệm vụ

dựa trên căn cứ pháp lý rõ ràng trong bối cảnh chuyển đổi số diễn ra mạnh mẽ.

3.2. Kết quả bảo vệ an ninh dữ liệu, an ninh mạng của lực lượng Công an nhân dân

Một là, về phòng ngừa, đấu tranh với tội phạm mạng và rủi ro dữ liệu. Thực tiễn cho thấy, lực lượng Công an nhân dân đã triển khai nhiều biện pháp đồng bộ trong đấu tranh phòng, chống tội phạm sử dụng công nghệ cao, đặc biệt là tội phạm lừa đảo trực tuyến - tội phạm gắn với khai thác dữ liệu cá nhân bị lộ lọt và thao túng "niềm tin số" của người dân. Theo đó, lực lượng Công an nhân dân đã chủ động nắm tình hình, nhận diện phương thức, thủ đoạn mới, tăng cường điều tra cơ bản và quản lý địa bàn, đối tượng, qua đó, nâng cao khả năng phát hiện, ngăn chặn, xử lý sớm. Tính riêng trong 11 tháng năm 2025, tình hình tội phạm hình sự trên cả nước tiếp tục được kiềm chế, giảm hơn 24%; riêng tội phạm lừa đảo trực tuyến giảm trên 30%[1].

Ở góc độ kết quả xử lý vụ việc, trong năm 2024, lực lượng Công an nhân dân đã phát hiện, xử lý hơn 7.866 vụ lừa đảo chiếm đoạt tài sản (có hơn 4.100 vụ lừa đảo trên không gian mạng)[2]. Nhiều trường hợp được công an các địa phương kịp thời ngăn chặn, cảnh báo, qua đó, hạn chế thiệt hại cho người dân, góp phần củng cố trật tự, an toàn xã hội trong môi trường số. Tuy nhiên, thiệt hại do lừa đảo trực tuyến vẫn ở mức rất lớn, phản ánh tính "động" và khả năng biến hóa của tội phạm công nghệ cao. Thiệt hại do lừa đảo trực tuyến năm 2024 ước tính lên tới 18.900 tỷ đồng, tình trạng lộ lọt dữ liệu cá nhân vẫn ở mức báo động[3].

Hai là, về tổ chức lực lượng, cơ chế phối hợp và quy trình nghiệp vụ. Theo Nghị định số 13/2023/NĐ-CP, cơ quan chuyên trách bảo vệ dữ liệu cá nhân là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, có trách nhiệm giúp Bộ Công an thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân; định danh rõ đầu mối, tạo điều kiện chuẩn hóa quy trình nghiệp vụ, tăng tính thống nhất trong hướng dẫn, thanh tra, kiểm tra và xử lý vi phạm. Trong cơ chế phối hợp, do đặc trưng của bảo vệ an ninh dữ liệu, an ninh mạng không thể thực hiện theo mô hình một ngành có thể tự làm được. Vì vậy, trong đấu tranh với lừa đảo trực tuyến để thực sự hiệu quả cần phụ thuộc vào sự phối hợp với các chủ thể quản lý hạ tầng và dòng chảy dữ liệu, như: viễn thông, ngân hàng, trung gian thanh toán, nền tảng số hoặc phối hợp quốc tế khi tội phạm đặt máy chủ, điều hành đường dây từ ngoài lãnh thổ.

Nghị định số 47/2020/NĐ-CP ngày 25/5/2020 của Chính phủ về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước đã tạo khung pháp lý cho việc liên thông dữ liệu phục vụ điều hành, cung cấp dịch vụ công; đồng thời, đặt ra yêu cầu trách nhiệm, đầu mối phối hợp và tuân thủ quy định trong quá trình kết nối - chia sẻ dữ liệu. Điều này cho thấy, cơ chế phối hợp trong bảo vệ dữ liệu, an ninh mạng đang dần hình thành cả theo chiều ngang (liên ngành) và chiều dọc (từ trung ương tới địa phương). Tuy nhiên, vẫn cần tiếp tục chuẩn hóa thành quy trình phối hợp nhanh, rõ trách nhiệm, đặc biệt trong tình huống khẩn cấp (ứng cứu sự cố, phong tỏa dòng tiền, thu thập - bảo toàn chứng cứ số).

Ba là, về năng lực kỹ thuật, hạ tầng giám sát, cảnh báo, ứng cứu và sức ép từ thực tiễn xử lý sự cố. Quyết định số 964/QĐ-TTg phê duyệt Chiến lược An toàn, An ninh mạng quốc gia đến năm 2025, tầm nhìn 2030 được coi là khung định hướng quan trọng để thúc đẩy các năng lực ứng phó, ngăn chặn theo hướng chủ động, tổng thể và dài hạn. Tuy nhiên, sức ép từ thực tiễn về sự cố cũng đặt ra các yêu cầu cấp bách trong việc nâng cao năng lực của lực lượng Công an nhân dân. Hệ thống giám sát kỹ thuật của các cơ quan chuyên môn thời gian qua đã ghi nhận số lượng lớn điểm yếu, lỗ hổng an toàn thông tin; đồng thời, sự cố nghiêm trọng phải xử lý tăng gần 60% so với năm trước[4].

3.3. Một số hạn chế, thách thức

(1) Sự gia tăng nhanh về quy mô, tần suất và tính chất "có chủ đích" của các loại tội

phạm mạng khiến nhiệm vụ phòng ngừa, phát hiện xử lý ngày càng nặng nề. Theo thống kê, riêng trong năm 2024, có 46,15% cơ quan, doanh nghiệp cho biết đã từng bị tấn công mạng ít nhất một lần. Tổng số vụ tấn công ước tính lên tới hơn 659.000 vụ. Báo cáo của đơn vị chuyên trách thuộc Bộ Công an, riêng nhóm đơn vị trọng yếu đã ghi nhận hơn 74.000 cảnh báo tấn công, trong đó có 83 chiến dịch tấn công APT[5]. Việc các chiến dịch APT gia tăng làm thay đổi đáng kể yêu cầu năng lực: từ xử lý sự cố đơn lẻ sang yêu cầu giám sát chủ động, cảnh báo sớm, phân tích tình báo mạng và săn tìm mối đe dọa theo thời gian thực.

(2) Những lỗ hổng, điểm yếu kỹ thuật phổ biến và xu hướng gia tăng sự cố nghiêm trọng tạo áp lực lớn lên năng lực ứng cứu và điều tra số. Hệ thống giám sát kỹ thuật của cơ quan chuyên môn đã ghi nhận 90.033 điểm yếu, lỗ hổng trong tháng 6/2024, và số sự cố nghiêm trọng phải xử lý tăng gần 60% so với năm 2023[6]. Điều này kéo theo nhu cầu lớn về năng lực kỹ thuật, năng lực phối hợp ứng cứu và năng lực chuẩn hóa quy trình bảo toàn chứng cứ điện tử để bảo đảm giá trị pháp lý trong tố tụng.

(3) Tình trạng lộ lọt và mua bán dữ liệu cá nhân diễn biến nhức nhối, làm gia tăng tội phạm khiến phòng ngừa xã hội trở nên khó khăn hơn. Thực tế điều tra, triệt phá các đường dây mua bán dữ liệu cho thấy, quy mô dữ liệu bị giao dịch rất lớn, điển hình: cơ quan Công an đã triệt phá chuyên án mua bán gần 56 triệu thông tin dữ liệu cá nhân của các đối tượng lợi dụng dấu hiệu buông lỏng quản lý ở một số tổ chức, doanh nghiệp; dữ liệu bị lợi dụng để phục vụ lừa đảo, tín dụng đen, giả mạo…[7]. Riêng trong năm 2024, thiệt hại do lừa đảo trực tuyến ước tính 18.900 tỷ đồng và tình trạng lộ lọt dữ liệu cá nhân vẫn ở mức báo động[8]. Đặc biệt, các vụ việc lộ dữ liệu lớn có thể còn dẫn tới làm tăng rủi ro lừa đảo trên diện rộng. Khi dữ liệu bị rò rỉ lan rộng, lực lượng Công an nhân dân dù đã chủ động tăng cường trấn áp vẫn phải đối mặt với đầu vào rủi ro lớn: tội phạm có thể tiếp cận dữ liệu thật, tạo kịch bản cá nhân hóa, nâng xác suất nạn nhân mắc bẫy và làm suy giảm hiệu quả phòng ngừa theo cách thức truyền thống.

(4) Thiếu hụt nhân lực chuyên sâu ảnh hưởng tới năng lực tác chiến số. Theo khảo sát của Hiệp hội An ninh mạng quốc gia, có tới hơn 20,06% đơn vị cho biết, hiện chưa có nhân sự chuyên trách về an ninh mạng, 35,56% cơ quan, doanh nghiệp chỉ bố trí được không quá 5 người phụ trách, con số này là rất nhỏ so với yêu cầu thực tế hiện nay. Trong khi theo mô hình giám sát tập trung SOC 24/7 (3 ca 4 kíp) cần tối thiểu 8 - 10 vị trí chuyên trách, nhưng hơn 20,06% đơn vị chưa có nhân sự chuyên trách an ninh mạng và tỷ lệ lớn chỉ bố trí quy mô rất nhỏ. Bên cạnh đó, chỉ có 56,53% đơn vị bố trí riêng cán bộ chuyên trách bảo vệ dữ liệu cá nhân; 43,47% không có chuyên trách hoặc kiêm nhiệm và 19,45% cơ quan, doanh nghiệp thừa nhận đang gặp khó khăn khi đáp ứng tuân thủ, trong đó vướng mắc lớn nhất là thủ tục/quy trình/pháp lý[9]. Thực trạng này khiến lực lượng Công an nhân dân phải đầu tư nhiều hơn cho việc hướng dẫn, thanh tra, kiểm tra; đồng thời, đòi hỏi chuẩn hóa bộ tiêu chí, quy trình đánh giá rủi ro và cơ chế trách nhiệm giải trình để đưa pháp luật vào cuộc sống. Ở phạm vi vĩ mô, tình trạng thiếu hụt chuyên gia an ninh mạng cũng đang tạo "rào cản lớn" trong bảo đảm an toàn thông tin[10].

(5) Tình trạng nhiễu loạn thông tin (tin giả về lộ dữ liệu, thổi phồng sự cố…) làm phân tán nguồn lực và gây khó khăn cho công tác kiểm chứng, xử lý. Trong điều kiện lực lượng thực thi vừa phải xử lý tội phạm, vừa phải bảo đảm ổn định xã hội, không gian thông tin lại phải trở thành mặt trận thứ hai: nếu thiếu cơ chế phối hợp truyền thông và phản ứng nhanh, hiệu quả phòng ngừa có thể suy giảm. Trong khi đó, mức độ tự chủ công nghệ và khả năng nội địa hóa công cụ an ninh mạng còn hạn chế, ảnh hưởng nhất định tới năng lực bảo vệ của lực lượng chức năng.

4. Giải pháp nâng cao năng lực bảo vệ an ninh dữ liệu, an ninh mạng của lực lượng Công an nhân dân

Thứ nhất, tiếp tục hoàn thiện thể chế nội bộ, chuẩn hóa quy trình quản trị rủi ro dữ liệu và tăng cường trách nhiệm giải trình.

Trước mắt đưa hoạt động quản trị rủi ro an ninh dữ liệu, an ninh mạng thành kỷ luật tổ chức trong toàn lực lượng, coi đây là điều kiện để chuyển đổi số an toàn theo quan điểm và yêu cầu xuyên suốt của Nghị quyết số 57-NQ/TW, *Luật An ninh mạng* năm 2018 đặt trọng tâm phòng ngừa - phát hiện - ngăn chặn và xử lý hành vi xâm phạm. Đồng thời, cụ thể hóa các nghị định về biện pháp bảo vệ theo *Luật*, nhất là Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Bên cạnh đó, *Luật Dữ liệu* năm 2024 và danh mục dữ liệu quan trọng, dữ liệu cốt lõi cũng được xác định là trục ưu tiên bảo vệ, giúp chuyển đổi tư duy từ bảo vệ dàn trải sang bảo vệ theo mức độ rủi ro.

Để việc triển khai các biện pháp bảo vệ theo hướng chuẩn hóa thống nhất, phân tầng rủi ro và đo lường được, cần xây dựng và ban hành Khung quản trị an ninh dữ liệu áp dụng cho toàn lực lượng, gồm: phân loại dữ liệu theo vòng đời; quy định tối thiểu về quyền truy cập, ghi vết, mã hóa, sao lưu - khôi phục. Cùng với đó, xây dựng cơ chế chia sẻ dữ liệu liên thông bảo đảm đúng mục đích - đúng thẩm quyền - đúng phạm vi.

Ngoài ra, cần bắt buộc áp dụng nguyên tắc an ninh ngay từ thiết kế cho mọi dự án số hóa/ứng dụng mới: thẩm định an ninh mạng, đánh giá rủi ro dữ liệu, nghiệm thu an toàn trước khi đưa vào vận hành, nhất là với hệ thống xử lý dữ liệu quan trọng, dữ liệu cốt lõi theo danh mục tại Quyết định số 20/2025/QĐ-TTg. Đặc biệt, cần hình thành chuỗi quy trình chuẩn cho các tình huống điển hình (lộ dữ liệu, ransomware, APT, tấn công chuỗi cung ứng, giả mạo định danh...), trong đó quy định rõ trách nhiệm chỉ huy - tham mưu - kỹ thuật - truyền thông - phối hợp đối tác nhằm giảm độ trễ trong quá trình ứng phó. Đồng thời, cần gắn yêu cầu quản trị rủi ro với trách nhiệm giải trình và đánh giá kết quả theo tinh thần "kết quả thực hiện là tiêu chí đánh giá hiệu quả thực hiện nhiệm vụ, đánh giá thi đua, khen thưởng hằng năm" như Nghị quyết số 57-NQ/TW đã đề ra.

Thứ hai, đầu tư đột phá về hạ tầng kỹ thuật nhằm nâng cao năng lực giám sát, cảnh báo sớm, ứng cứu sự cố, điều tra số và bảo vệ các hệ thống trọng yếu.

Giải pháp kỹ thuật cần hướng tới mục tiêu kép: (1) Chuyển từ bị động sang chủ động, cảnh báo sớm; (2) Tăng khả năng chống chịu và năng lực điều tra số, bảo đảm phù hợp với định hướng chiến lược an toàn, an ninh mạng quốc gia và quan điểm về phát triển hạ tầng số hiện đại, đồng bộ, an ninh, an toàn theo tinh thần Nghị quyết số 57-NQ/TW. Từ đó, ưu tiên phát triển mô hình SOC theo tầng (trung ương - địa phương - chuyên trách), bảo đảm có năng lực "nhận diện" đối với nhật ký hệ thống, lưu lượng mạng, hành vi truy cập dữ liệu; ưu tiên kết nối giám sát đối với hệ thống xử lý dữ liệu quan trọng, dữ liệu cốt lõi theo danh mục hiện hành. Nghiên cứu xây dựng nền tảng chia sẻ tình báo mối đe dọa và kho chỉ báo tấn công dùng chung trong lực lượng, ứng dụng phân tích dữ liệu lớn (Big Data/AI) để phát hiện bất thường nhằm giảm phụ thuộc vào phát hiện thủ công.

Về nâng cao năng lực ứng cứu sự cố an ninh mạng và pháp y số, cần chuẩn hóa chuỗi ứng cứu, từ phát hiện - phân loại - khoanh vùng - xử lý - khôi phục - rút kinh nghiệm, gắn với yêu cầu biện pháp bảo vệ theo Nghị định số 53/2022/NĐ-CP quy định chi tiết một số điều của *Luật An ninh mạng* năm 2018. Cần đầu tư phòng thí nghiệm pháp y số, công cụ thu thập - bảo toàn - giám định chứng cứ điện tử; chuẩn hóa kho lưu trữ chứng cứ số và quy trình bảo đảm tính toàn vẹn để nâng chất lượng hồ sơ điều tra, truy tố. Xây dựng năng lực diễn tập thường xuyên theo kịch bản (ransomware, lộ dữ liệu, APT, tấn công chuỗi cung ứng) để đo lường khả năng chống chịu và độ sẵn sàng chiến đấu.

Thứ ba, đào tạo và phát triển nhân lực chuyên trách về bảo vệ an ninh mạng, an ninh dữ liệu.

Tiếp tục nghiên cứu xây dựng hệ sinh thái nhân lực an ninh dữ liệu, an ninh mạng theo hướng: đúng người - đúng kỹ năng - đúng vị trí - đúng lộ trình nghề nghiệp. Theo đó, ban hành khung năng lực vị trí việc làm cho các nhóm chức danh cốt lõi, như: phân tích mã độc, giám sát, phân tích cảnh báo bảo mật, giám định số, điều tra số, quản trị an ninh dữ liệu, kiểm thử xâm nhập, quản trị định danh, quản trị rủi ro...

Tiến hành đào tạo, bồi dưỡng theo hướng phân tầng, như: (1) Tầng phổ cập cho toàn lực lượng (nhận diện lừa đảo, bảo vệ dữ liệu cá nhân, kỷ luật sử dụng thiết bị số); (2) Tầng chuyên sâu cho lực lượng chuyên trách (kỹ thuật, điều tra số, ứng cứu); (3) Tầng chuyên gia (R&D, thiết kế hệ thống, tình báo mạng) theo mô hình "đào tạo gắn liền với nhiệm vụ" dựa trên tình huống thực tiễn. Ngoài ra, xây dựng cơ chế đào tạo liên kết với học viện, trường đại học, doanh nghiệp công nghệ uy tín; mở rộng hình thức "học tập số" theo Nghị quyết số 57-NQ/TW.

Thứ tư, tăng cường phối hợp liên ngành, huy động sự tham gia của xã hội và mở rộng hợp tác quốc tế nhằm nâng hiệu quả phòng ngừa.

Cần phối hợp liên ngành theo cơ chế tác nghiệp nhanh với ngân hàng, viễn thông, trung gian thanh toán và các nền tảng số. Theo đó, cần thiết lập cơ chế "một đầu mối - một quy trình - một thời hạn" để tiếp nhận và xử lý yêu cầu phong tỏa giao dịch nghi vấn, xác minh tài khoản, chặn kênh liên lạc, đường dẫn lừa đảo, thu thập log và bảo toàn chứng cứ số; giảm "khoảng trống thời gian vàng" khi nạn nhân vừa chuyển tiền. Xây dựng kho dữ liệu dùng chung về kịch bản lừa đảo, dấu hiệu nhận biết, số tài khoản/đầu số/đường dẫn rủi ro.

Đồng thời, huy động sự tham gia của xã hội để nâng cảnh giác và tạo "miễn dịch số", trong đó tổ chức các chiến dịch phối hợp giữa cơ quan chức năng và doanh nghiệp công nghệ nhằm nâng cao nhận thức, kỹ năng an toàn số, coi đây là hướng đi cần nhân rộng. Chú trọng thúc đẩy văn hóa tuân thủ bảo vệ dữ liệu trong doanh nghiệp, đặc biệt ở các lĩnh vực thu thập nhiều dữ liệu nhạy cảm (tài chính, giáo dục, y tế, thương mại điện tử). Ngoài ra, cũng cần tăng cường hợp tác quốc tế (chia sẻ thông tin, tương trợ tư pháp, truy vết dòng tiền xuyên biên giới, thu thập chứng cứ số ngoài lãnh thổ), vì nhiều đường dây lừa đảo và hạ tầng tấn công đặt ngoài Việt Nam.

5. Kết luận

Chuyển đổi số đang diễn ra sâu rộng, dữ liệu đã trở thành nguồn lực chiến lược của phát triển; đồng thời, cũng là môi trường dễ bị lợi dụng tấn công mạng, lộ lọt thông tin và tội phạm công nghệ cao tập trung khai thác. Trong bối cảnh đó, lực lượng Công an nhân dân tiếp tục khẳng định vai trò nòng cốt trong bảo vệ an ninh quốc gia, giữ gìn trật tự an toàn xã hội trên không gian mạng, vừa là chủ thể trực tiếp phòng ngừa, phát hiện, đấu tranh với tội phạm mạng, vừa là lực lượng quan trọng trong tổ chức thực thi pháp luật về an ninh mạng và bảo vệ dữ liệu, góp phần giữ vững ổn định xã hội và tạo nền tảng vững chắc cho phát triển đất nước gắn với bảo vệ chủ quyền số trong kỷ nguyên số❐

Chú thích:

1. *Bộ Công an tăng cường đấu tranh, ngăn chặn với tội phạm lừa đảo trên không gian mạng.* https://bocongan.gov.vn, ngày 23/12/2024.

2. *Chính sách, pháp luật.* https://bocongan.gov.vn, truy cập ngày 12/01/2026.

3, 8. *Thiệt hại do lừa đảo trực tuyến ước tính 18.900 tỷ đồng năm 2024.* https://baochinhphu.vn, ngày 16/12/2024.

4, 6. *Sự cố an toàn thông tin tại Việt Nam tăng tới 60%.* https://mst.gov.vn, ngày 26/7/2024.

5, 9. *Hơn 46 cơ quan doanh nghiệp bị tấn công mạng trong năm 2024.* https://thoibaonganhang.vn, ngày 23/12/2024.

7. *Triệt phá đường dây mua bán gần 56 triệu dữ liệu cá nhân.* https://cand.com.vn, ngày 21/02/2025.

10. *Thiếu hụt nhân lực: thách thức lớn nhất của an ninh mạng Việt Nam.* https://antoanthongtin.vn, ngày 04/7/2025.