

NÂNG CAO HIỆU QUẢ THỰC THI PHÁP LUẬT VỀ BẢO ĐẢM AN NINH THÔNG TIN TRƯỚC NHỮNG THÁCH THỨC MỚI CỦA KHOA HỌC DỮ LIỆU TRONG KỶ NGUYÊN SỐ

HÀ THỊ KHÁNH HUYỀN
Khoa Luật, Học viện Cảnh sát nhân dân

Nhận bài ngày 22/7/2026. Sửa chữa xong 25/8/2026. Duyệt đăng 27/8/2026.

Abstract

In the context of digital transformation and the rapid development of data science, ensuring information security is essential to safeguarding national digital sovereignty and protecting the legitimate rights and interests of agencies, organizations, and individuals. However, emerging technologies such as artificial intelligence, big data, and cloud computing have also increased the risks of cyberattacks, data breaches, and privacy violations. This article examines the challenges posed by data science in the digital era, analyzes the current enforcement of laws on information security in Vietnam, and proposes solutions to improve enforcement effectiveness, thereby contributing to the development of a secure, trustworthy, and sustainable digital environment.

Keywords: Cyberspace security, data protection, data science, digital era, information security.

1. Đặt vấn đề

Sự phát triển mạnh mẽ của khoa học dữ liệu (KHDL), trí tuệ nhân tạo (AI) và chuyển đổi số đang tạo ra những biến đổi sâu sắc trong đời sống xã hội, thúc đẩy tăng trưởng kinh tế, nâng cao hiệu quả quản trị quốc gia và chất lượng cuộc sống. Trong bối cảnh đó, dữ liệu trở thành nguồn tài nguyên chiến lược, giữ vai trò quan trọng trong quản lý nhà nước, hoạt động sản xuất, kinh doanh và cung cấp dịch vụ. Tuy nhiên, cùng với những lợi ích to lớn, các nguy cơ đối với an ninh thông tin cũng gia tăng với tính chất ngày càng phức tạp. Tình trạng lộ lọt dữ liệu, tấn công mạng, đánh cắp thông tin, phát tán tin giả và xâm phạm quyền riêng tư diễn biến phổ biến, tác động tiêu cực đến an ninh quốc gia, trật tự an toàn xã hội và quyền, lợi ích hợp pháp của tổ chức, cá nhân. Mặc dù Việt Nam đã ban hành nhiều quy định quan trọng về an ninh, an toàn thông tin, song trước sự phát triển nhanh chóng của KHDL và công nghệ số, hệ thống pháp luật vẫn bộc lộ những hạn chế nhất định. Vì vậy, việc nghiên cứu thực trạng và đề xuất giải pháp nâng cao hiệu quả thực thi pháp luật về bảo đảm an ninh thông tin trước các thách thức mới của KHDL có ý nghĩa lý luận và thực tiễn cấp thiết hiện nay.

2. Nội dung nghiên cứu

2.1. Một số vấn đề về khoa học dữ liệu và bảo đảm an ninh thông tin trong kỷ nguyên số

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ trên phạm vi toàn cầu, KHDL đang trở thành một trong những nền tảng công nghệ cốt lõi thúc đẩy sự phát triển của kinh tế số, xã hội số và quản trị số. Việc thu thập, xử lý, phân tích và khai thác dữ liệu không chỉ giúp nâng cao hiệu quả hoạt động quản lý nhà nước, tối ưu hóa hoạt động sản xuất, kinh doanh mà còn góp phần hỗ trợ quá trình ra quyết định trong nhiều lĩnh vực khác nhau của đời sống xã hội. Dữ liệu vì vậy ngày càng được xem là tài nguyên chiến lược của quốc gia trong kỷ nguyên số.

Về phương diện lý luận, KHDL được hiểu là lĩnh vực liên ngành kết hợp giữa công nghệ thông tin, toán học, thống kê và AI nhằm thu thập, xử lý, phân tích và khai thác dữ liệu phục vụ các mục tiêu quản lý, dự báo và hỗ trợ ra quyết định. Đặc trưng nổi bật của KHDL là khả năng xử lý khối lượng dữ liệu lớn

Email: hahuyenk34@gmail.com

với tốc độ cao và phạm vi rộng, từ đó tạo ra những giá trị mới phục vụ phát triển kinh tế - xã hội. Tuy nhiên, chính sự phụ thuộc ngày càng lớn vào dữ liệu và công nghệ số cũng làm gia tăng nguy cơ mất an toàn thông tin, lộ lọt dữ liệu, xâm phạm quyền riêng tư và các hành vi tấn công mạng. Trong điều kiện hiện nay, an ninh thông tin không còn chỉ được hiểu theo nghĩa bảo vệ hệ thống kỹ thuật hay hạ tầng công nghệ mà còn bao gồm việc bảo đảm tính bí mật, tính toàn vẹn của dữ liệu, thông tin trong môi trường số. Đây là yêu cầu có ý nghĩa đặc biệt quan trọng đối với hoạt động quản lý nhà nước, bảo vệ chủ quyền quốc gia trên không gian mạng cũng như bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân. Do đó, bảo đảm an ninh thông tin cần được nhìn nhận như một bộ phận cấu thành quan trọng của an ninh quốc gia trong thời đại số hóa. Thực tiễn cho thấy, cùng với sự phát triển của KHDL, các phương thức, thủ đoạn xâm phạm an ninh thông tin ngày càng tinh vi và khó kiểm soát hơn. Các hành vi tấn công mạng, đánh cắp dữ liệu, phát tán mã độc, chiếm đoạt thông tin cá nhân, thao túng dữ liệu hay sử dụng công nghệ AI để thực hiện hành vi vi phạm pháp luật đang đặt ra nhiều thách thức mới đối với công tác quản lý nhà nước và thực thi pháp luật. Điều này đòi hỏi hệ thống pháp luật về bảo đảm an ninh thông tin phải thường xuyên được hoàn thiện theo hướng đồng bộ, hiện đại và phù hợp với sự phát triển của công nghệ số.

Từ góc độ nghiên cứu, việc làm rõ những vấn đề lý luận về KHDL và bảo đảm an ninh thông tin có ý nghĩa quan trọng trong việc xác định đúng bản chất, phạm vi và yêu cầu điều chỉnh pháp luật đối với lĩnh vực này. Đồng thời, đây cũng là cơ sở để đánh giá thực trạng pháp luật hiện hành, nhận diện những hạn chế, bất cập và đề xuất các giải pháp nâng cao hiệu quả thực thi pháp luật về bảo đảm an ninh thông tin trong kỷ nguyên số hiện nay.

2.2. Quy định của pháp luật về bảo đảm an ninh thông tin ở Việt Nam hiện nay

2.2.1. Hệ thống pháp luật về bảo đảm an ninh thông tin

Trong những năm gần đây, cùng với quá trình chuyển đổi số quốc gia và sự phát triển mạnh mẽ của công nghệ thông tin, Việt Nam đã từng bước xây dựng và hoàn thiện hệ thống pháp luật về bảo đảm an ninh thông tin tương đối đồng bộ. Hệ thống quy định pháp luật hiện hành đã tạo cơ sở pháp lý quan trọng cho hoạt động quản lý nhà nước, phòng ngừa, phát hiện và xử lý các hành vi xâm phạm an ninh thông tin trong môi trường mạng. Hiến pháp năm 2013 chưa trực tiếp sử dụng thuật ngữ bảo vệ dữ liệu cá nhân và chưa xây dựng một cơ chế bảo vệ dữ liệu cá nhân một cách độc lập, nhưng đã đặt nền tảng hiến định quan trọng cho quyền này thông qua việc ghi nhận và bảo vệ quyền về đời sống riêng tư, bí mật cá nhân và bí mật gia đình. Cụ thể, Hiến pháp năm 2013 khẳng định: *“Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình.”* (Quốc hội, 2014, Điều 21).

Một trong những văn bản pháp luật có ý nghĩa nền tảng là Luật An ninh mạng năm 2025. Luật đã quy định tương đối toàn diện về bảo vệ an ninh quốc gia trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an ninh mạng; phòng ngừa, xử lý hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội và quyền, lợi ích hợp pháp của tổ chức, cá nhân. Đặc biệt đã làm rõ *“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”* (Quốc hội, 2025a, Điều 2), ngoài ra Luật An ninh mạng cũng đặt ra cơ chế quản lý dữ liệu, yêu cầu lưu trữ dữ liệu tại Việt Nam đối với một số loại hình dịch vụ và tăng cường trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng. Các quy định này góp phần hình thành cơ chế bảo vệ dữ liệu và bảo đảm an toàn cho hệ thống thông tin trong hoạt động của cơ quan nhà nước, tổ chức và doanh nghiệp. Bên cạnh các đạo luật chuyên ngành điều chỉnh trực tiếp lĩnh vực an ninh mạng và an toàn thông tin, hệ thống pháp luật Việt Nam còn từng bước được hoàn thiện thông qua việc ban hành các quy định chuyên biệt về bảo vệ dữ liệu cá nhân. Trong đó, Luật Bảo vệ dữ liệu cá nhân năm 2025 đánh dấu bước phát triển quan trọng trong việc xây dựng khuôn khổ pháp lý thống nhất nhằm bảo vệ quyền và lợi ích

hợp pháp của cá nhân đối với dữ liệu của mình. Luật đã xác lập các nguyên tắc cơ bản trong bảo vệ dữ liệu cá nhân, trong đó nhấn mạnh nguyên tắc: “Bảo vệ dữ liệu cá nhân gắn với bảo vệ lợi ích quốc gia, dân tộc, phục vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh và đối ngoại; bảo đảm hài hòa giữa bảo vệ dữ liệu cá nhân với bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân” (Quốc hội, 2025b, Điều 3), các quy định về bảo vệ dữ liệu cá nhân, quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông và công nghệ thông tin; các quy định của Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2025, mặc dù chưa quy định một tội danh độc lập với tên gọi “tội xâm phạm dữ liệu cá nhân”, nhưng đã hình sự hóa một số hành vi nguy hiểm cho xã hội xâm phạm đến an toàn thông tin. Đáng chú ý là “Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông” (Quốc hội, 2025c, Điều 288) có ý nghĩa trực tiếp trong việc bảo vệ thông tin của cá nhân trước các hành vi sử dụng, công khai hoặc khai thác trái phép trên môi trường mạng. Hệ thống quy định này từng bước đáp ứng yêu cầu đấu tranh phòng, chống các hành vi vi phạm pháp luật trong môi trường số.

Nhìn chung, hệ thống pháp luật về bảo đảm an ninh thông tin ở Việt Nam đã từng bước được hoàn thiện theo hướng tiếp cận với xu thế phát triển của công nghệ số và yêu cầu hội nhập quốc tế. Tuy nhiên, trước sự phát triển nhanh chóng của KHDH, AI và các công nghệ mới, nhiều quy định pháp luật vẫn cần tiếp tục được rà soát, sửa đổi và bổ sung nhằm bảo đảm tính đồng bộ, khả thi và phù hợp với thực tiễn.

Việc xây dựng và triển khai hệ thống pháp luật về bảo đảm an ninh thông tin trong thời gian qua đã đạt được nhiều kết quả tích cực. Trước hết, công tác quản lý nhà nước về an ninh thông tin ngày càng được tăng cường. Các cơ quan chức năng đã từng bước hoàn thiện cơ chế quản lý, giám sát không gian mạng; đẩy mạnh công tác kiểm tra, thanh tra và xử lý vi phạm trong lĩnh vực an toàn, an ninh thông tin. Cùng với đó, hoạt động đấu tranh phòng, chống tội phạm mạng và tội phạm sử dụng công nghệ cao đã đạt được nhiều kết quả quan trọng. Nhiều vụ việc tấn công mạng, lừa đảo qua mạng, đánh cắp dữ liệu hoặc chiếm đoạt tài sản trên không gian mạng đã được phát hiện, điều tra và xử lý nghiêm minh theo quy định của pháp luật. Điều này góp phần bảo đảm an ninh quốc gia, giữ gìn trật tự an toàn xã hội và nâng cao tính rắn đe đối với các hành vi vi phạm pháp luật trên môi trường mạng.

Nhận thức của cơ quan, tổ chức và người dân về bảo vệ dữ liệu và an toàn thông tin cũng từng bước được nâng cao. Các hoạt động tuyên truyền, phổ biến pháp luật về an ninh mạng, an toàn thông tin được triển khai rộng rãi; nhiều cơ quan, doanh nghiệp đã chú trọng đầu tư hạ tầng kỹ thuật, áp dụng các giải pháp bảo mật và xây dựng quy trình quản lý dữ liệu an toàn hơn. Bên cạnh đó, việc ứng dụng công nghệ trong quản lý an ninh mạng ngày càng được đẩy mạnh. Nhiều hệ thống giám sát, cảnh báo sớm nguy cơ mất an toàn thông tin đã được triển khai; các giải pháp ứng dụng AI và phân tích dữ liệu lớn bước đầu được sử dụng trong hoạt động phát hiện, phòng ngừa và xử lý các nguy cơ tấn công mạng. Đây là cơ sở quan trọng góp phần nâng cao hiệu quả bảo đảm an ninh thông tin trong bối cảnh chuyển đổi số hiện nay.

2.2.2. Những khó khăn, hạn chế và nguyên nhân

Bên cạnh những kết quả đạt được, việc thực thi pháp luật về bảo đảm an ninh thông tin ở Việt Nam vẫn còn tồn tại nhiều khó khăn, hạn chế. Trước hết, tốc độ phát triển của khoa học công nghệ, đặc biệt là KHDH và AI diễn ra rất nhanh trong khi hệ thống pháp luật còn chậm được sửa đổi, bổ sung. Điều này dẫn đến tình trạng một số quy định pháp luật chưa theo kịp thực tiễn, thiếu tính dự báo hoặc chưa bao quát đầy đủ các hành vi vi phạm mới phát sinh trên không gian mạng. Ngoài ra, hoạt động kiểm soát dữ liệu xuyên biên giới còn gặp nhiều khó khăn. Dữ liệu hiện nay được lưu trữ, chia sẻ và xử lý trên nhiều nền tảng số có phạm vi hoạt động toàn cầu, trong khi cơ chế phối hợp quốc tế và công cụ quản lý của Việt Nam còn hạn chế. Điều này gây khó khăn trong việc xác định chủ thể vi phạm, thu thập chứng cứ điện tử và xử lý các hành vi xâm phạm an ninh thông tin có yếu tố nước ngoài.

Một khó khăn khác là nguồn nhân lực chất lượng cao trong lĩnh vực an ninh mạng và KHDH còn thiếu cả về số lượng và trình độ chuyên môn. Nhiều cơ quan, tổ chức chưa có đội ngũ chuyên trách đủ năng lực để đáp ứng yêu cầu quản trị và bảo vệ hệ thống thông tin trong điều kiện công nghệ phát

triển nhanh chóng. Bên cạnh đó, nhận thức của một bộ phận người sử dụng không gian mạng về bảo vệ dữ liệu cá nhân và an toàn thông tin còn hạn chế. Tình trạng sử dụng thông tin cá nhân thiếu kiểm soát, mất cảnh giác trước các hành vi lừa đảo trên không gian mạng vẫn diễn ra phổ biến, làm gia tăng nguy cơ mất an toàn thông tin. Ngoài ra, cơ chế phối hợp giữa các cơ quan, tổ chức trong công tác quản lý, phòng ngừa và xử lý vi phạm về an ninh thông tin ở một số lĩnh vực còn chưa chặt chẽ, thiếu tính đồng bộ. Việc chia sẻ dữ liệu, phối hợp xử lý sự cố hoặc hỗ trợ điều tra trong một số trường hợp còn chậm, ảnh hưởng đến hiệu quả thực thi pháp luật.

Những khó khăn, hạn chế nêu trên cho thấy yêu cầu tiếp tục hoàn thiện hệ thống pháp luật, nâng cao hiệu quả quản lý nhà nước, tăng cường hợp tác quốc tế và phát triển nguồn nhân lực chất lượng cao nhằm đáp ứng yêu cầu bảo đảm an ninh thông tin trong bối cảnh phát triển mạnh mẽ của KHDL và chuyển đổi số hiện nay.

2.3. Giải pháp nâng cao hiệu quả thực thi pháp luật về bảo đảm an ninh thông tin trong kỷ nguyên số

Từ thực trạng pháp luật và những khó khăn, thách thức đặt ra trong quá trình bảo đảm an ninh thông tin hiện nay có thể thấy rằng, việc nâng cao hiệu quả thực thi pháp luật là yêu cầu cấp thiết nhằm đáp ứng yêu cầu phát triển của KHDL và quá trình chuyển đổi số quốc gia. Để thực hiện mục tiêu này cần triển khai đồng bộ nhiều giải pháp trên cả phương diện hoàn thiện pháp luật, nâng cao hiệu quả quản lý nhà nước, phát triển nguồn nhân lực và tăng cường ứng dụng công nghệ hiện đại trong công tác bảo đảm an ninh thông tin.

2.3.1. Hoàn thiện hệ thống pháp luật về bảo đảm an ninh thông tin

Hoàn thiện hệ thống pháp luật là giải pháp nền tảng nhằm nâng cao hiệu quả thực thi pháp luật về bảo đảm an ninh thông tin trong bối cảnh chuyển đổi số và sự phát triển nhanh chóng của KHDL. Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng đã làm rõ: “Các biện pháp bảo vệ an ninh mạng: thẩm định an ninh mạng; đánh giá điều kiện an ninh mạng; kiểm tra an ninh mạng; giám sát an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng; sử dụng mật mã để bảo vệ thông tin mạng; yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân...” (Chính phủ, 2022, Điều 1). Ngoài ra cần tiếp tục rà soát, sửa đổi, bổ sung và hoàn thiện các quy định của pháp luật về an ninh mạng, an toàn thông tin mạng, bảo vệ dữ liệu cá nhân và các lĩnh vực có liên quan theo hướng đồng bộ, thống nhất, minh bạch và phù hợp với yêu cầu phát triển của khoa học, công nghệ. Việc hoàn thiện pháp luật phải bảo đảm khả năng dự báo, kịp thời điều chỉnh các quan hệ xã hội và các hành vi vi phạm mới phát sinh trong môi trường số, đặc biệt là các hành vi lợi dụng AI, dữ liệu lớn (Big Data), điện toán đám mây, Internet vạn vật (IoT), công nghệ chuỗi khối (Blockchain) và các công nghệ số mới để xâm phạm an ninh thông tin, đánh cắp dữ liệu hoặc thực hiện các hành vi tấn công mạng.

Cùng với đó, cần tiếp tục hoàn thiện cơ chế pháp lý về quản trị dữ liệu quốc gia, thu thập, lưu trữ, khai thác, kết nối, chia sẻ và sử dụng dữ liệu theo nguyên tắc bảo đảm an toàn, an ninh, bảo vệ quyền riêng tư và quyền lợi hợp pháp của tổ chức, cá nhân. Pháp luật cần quy định rõ trách nhiệm của cơ quan nhà nước, doanh nghiệp cung cấp dịch vụ số, tổ chức quản lý hạ tầng thông tin và các chủ thể có liên quan trong việc bảo vệ dữ liệu người dùng, quản lý rủi ro, bảo đảm an toàn hệ thống thông tin và ứng phó với các sự cố an ninh mạng. Đồng thời, cần nghiên cứu xây dựng và hoàn thiện các quy định điều chỉnh hoạt động phát triển, ứng dụng AI, quản trị dữ liệu xuyên biên giới, định danh và xác thực điện tử cũng như xác định rõ trách nhiệm pháp lý của các nền tảng số và các nhà cung cấp dịch vụ xuyên biên giới nhằm khắc phục khoảng trống pháp lý trước sự phát triển nhanh của công nghệ số và các mô hình kinh doanh mới.

Bên cạnh việc hoàn thiện các quy định nội dung cần nâng cao tính khả thi của pháp luật thông qua việc kịp thời ban hành các văn bản hướng dẫn thi hành, hoàn thiện cơ chế phối hợp giữa các cơ quan quản lý nhà nước trong công tác bảo đảm an ninh thông tin và tăng cường tính thống nhất giữa các

quy định của pháp luật về an ninh mạng, công nghệ thông tin, viễn thông, giao dịch điện tử, chuyển đổi số và bảo vệ dữ liệu cá nhân. Đồng thời, cần đẩy mạnh nghiên cứu, tiếp thu có chọn lọc kinh nghiệm quốc tế, hài hòa với các chuẩn mực và thông lệ quốc tế về quản trị dữ liệu và an ninh thông tin, qua đó góp phần xây dựng hành lang pháp lý hiện đại, ổn định, có tính dự báo cao, đáp ứng yêu cầu bảo vệ chủ quyền số quốc gia và thúc đẩy phát triển kinh tế số, xã hội số trong giai đoạn mới..

2.3.2. Nâng cao hiệu quả quản lý nhà nước và cơ chế phối hợp giữa các cơ quan chức năng

Để nâng cao hiệu quả quản lý nhà nước là yêu cầu quan trọng nhằm bảo đảm thực thi hiệu quả pháp luật về an ninh thông tin trong bối cảnh chuyển đổi số. Theo đó, cần tiếp tục hoàn thiện cơ chế quản lý theo hướng phân định rõ chức năng, nhiệm vụ của các cơ quan có thẩm quyền; đồng thời tăng cường thanh tra, kiểm tra, giám sát việc chấp hành pháp luật về an ninh mạng, an toàn thông tin và bảo vệ dữ liệu cá nhân. Việc kịp thời phát hiện, ngăn chặn và xử lý nghiêm các hành vi vi phạm sẽ góp phần nâng cao hiệu lực, hiệu quả quản lý nhà nước và tính răn đe của pháp luật. Ngoài ra, cần xây dựng cơ chế phối hợp chặt chẽ giữa các cơ quan quản lý nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng, cơ quan thực thi pháp luật và doanh nghiệp cung cấp dịch vụ số trong chia sẻ thông tin, cảnh báo sớm nguy cơ, ứng cứu sự cố và xử lý các vụ việc tấn công mạng. Sự phối hợp đồng bộ giữa các chủ thể sẽ nâng cao năng lực phòng ngừa, phát hiện và ứng phó với các nguy cơ xâm phạm an ninh thông tin trong môi trường số.

Trong bối cảnh các hành vi tấn công mạng và xâm phạm dữ liệu ngày càng mang tính xuyên quốc gia cần tăng cường hợp tác quốc tế trong trao đổi thông tin, hỗ trợ điều tra, chia sẻ kinh nghiệm và chuyển giao công nghệ. Đồng thời, chủ động tham gia các cơ chế hợp tác đa phương, từng bước hài hòa với các chuẩn mực quốc tế về an ninh thông tin, góp phần nâng cao hiệu quả thực thi pháp luật, bảo vệ chủ quyền số quốc gia và đáp ứng yêu cầu hội nhập quốc tế...

2.3.3. Phát triển nguồn nhân lực chất lượng cao trong lĩnh vực an ninh thông tin và khoa học dữ liệu

Nguồn nhân lực là yếu tố có ý nghĩa quyết định đối với hiệu quả bảo đảm an ninh thông tin trong kỷ nguyên số. Do đó, cần chú trọng đào tạo và phát triển đội ngũ chuyên gia có trình độ cao về an ninh mạng, KHDL, AI và điều tra tội phạm công nghệ cao. Việc xây dựng nguồn nhân lực chất lượng cao không chỉ phục vụ yêu cầu quản lý nhà nước mà còn đáp ứng nhu cầu bảo vệ hệ thống thông tin của các doanh nghiệp và tổ chức trong quá trình chuyển đổi số. Đồng thời, cần tăng cường công tác đào tạo, bồi dưỡng kỹ năng bảo đảm an toàn thông tin cho đội ngũ cán bộ, công chức và người lao động trong các cơ quan, tổ chức. Đây là giải pháp quan trọng nhằm hạn chế các nguy cơ mất an toàn thông tin xuất phát từ yếu tố con người vốn là một trong những nguyên nhân phổ biến dẫn đến lộ lọt dữ liệu và sự cố an ninh mạng hiện nay. Ngoài ra, cần đẩy mạnh tuyên truyền, phổ biến kiến thức pháp luật và kỹ năng sử dụng không gian mạng an toàn cho người dân để nâng cao nhận thức xã hội về bảo vệ dữ liệu cá nhân và an ninh thông tin trong môi trường số.

2.3.4. Tăng cường ứng dụng công nghệ hiện đại trong bảo đảm an ninh thông tin

Trong bối cảnh KHDL phát triển mạnh mẽ, việc ứng dụng các công nghệ hiện đại vào hoạt động bảo đảm an ninh thông tin là yêu cầu tất yếu. Các cơ quan, tổ chức cần đầu tư xây dựng hệ thống giám sát, cảnh báo sớm và ứng cứu sự cố an ninh mạng; đẩy mạnh ứng dụng AI, phân tích dữ liệu lớn và học máy trong hoạt động phát hiện nguy cơ tấn công mạng và xử lý các hành vi xâm phạm an ninh thông tin. Bên cạnh đó, cần tăng cường đầu tư hạ tầng kỹ thuật và hệ thống bảo mật cho các cơ sở dữ liệu quốc gia, hệ thống thông tin quan trọng và nền tảng số phục vụ hoạt động quản lý nhà nước. Việc xây dựng môi trường số an toàn, ổn định và có khả năng chống chịu cao trước các nguy cơ tấn công mạng là điều kiện quan trọng để thúc đẩy phát triển chính phủ số, kinh tế số và xã hội số ở Việt Nam hiện nay. Việc triển khai đồng bộ các giải pháp nêu trên sẽ góp phần nâng cao hiệu quả thực thi pháp luật về bảo đảm an ninh thông tin, đáp ứng yêu cầu bảo vệ an ninh quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân trong bối cảnh phát triển mạnh mẽ của KHDL và chuyển đổi số hiện nay..

Xem tiếp trang 416