# BẢO VỆ DỮ LIỆU CÁ NHÂN TẠI VIỆT NAM - THỰC TRẠNG VÀ GIẢI PHÁP

**ĐOÀN MẠNH HỒNG**
**TRẦN THANH TÙNG**
**Trường Đại học Kinh tế và Quản trị kinh doanh, Đại học Thái Nguyên**

*Nhận bài ngày 20/4/2025. Sửa chữa xong 28/4/2025. Duyệt đăng 10/5/2025.*

***Abstract***

*Personal data is a critical asset across economic, social, and governance sectors. While rapid technological advancements and digital transformation offer significant opportunities, they also present serious privacy challenges. This study analyzes the current state of personal data protection in Vietnam, focusing on the legal framework, types of data breaches, underlying causes, consequences, public awareness, and the effectiveness of existing measures. The article also proposes solutions to strengthen legal regulations and apply technological innovations to improve data protection in the context of ongoing digital transformation.*

***Keywords:*** *Personal data, legal framework, data breach, privacy, cybersecurity, digital transformation.*

**1. Đặt vấn đề**

Tại Việt Nam, quốc gia có tốc độ phát triển và ứng dụng Internet cao, dữ liệu của hàng triệu người dân đang được thu thập, lưu trữ, xử lý và chia sẻ trên không gian mạng dưới nhiều hình thức. Tuy nhiên, tình trạng lộ, lọt, mua bán trái phép dữ liệu cá nhân (DLCN) diễn ra ngày càng phổ biến và phức tạp, gây ra những hậu quả nghiêm trọng về kinh tế - xã hội và an ninh quốc gia. Nhận thức được tầm quan trọng cấp bách của vấn đề, Chính phủ Việt Nam đã ban hành Nghị định số 13/2023/NĐ-CP về bảo vệ DLCN (sau đây gọi là Nghị định 13), có hiệu lực từ ngày 01/7/2023. Đây được coi là văn bản pháp lý chuyên sâu và toàn diện đầu tiên của Việt Nam trong lĩnh vực này, đánh dấu một bước tiến quan trọng trong việc xây dựng hành lang pháp lý bảo vệ DLCN, tiệm cận với các tiêu chuẩn quốc tế. Tuy nhiên, việc triển khai và thực thi Nghị định 13 vẫn còn đối mặt với nhiều thách thức, từ việc diễn giải các quy định còn chung chung, sự thiếu hụt nguồn lực và nhận thức của doanh nghiệp đến sự cần thiết phải hài hòa với các quy định quốc tế như Luật bảo vệ dữ liệu của Liên minh Châu Âu (General Data Protection Regulation - GDPR). Trong nghiên cứu này, tác giả tập trung vào một số nội dung sau: 1) Phân tích khung pháp lý hiện hành về bảo vệ DLCN tại Việt Nam, đặc biệt là Nghị định 13 và Luật An ninh mạng, đồng thời so sánh với GDPR để làm rõ bối cảnh pháp lý; 2) Đánh giá thực trạng vi phạm DLCN tại Việt Nam và trên thế giới thông qua số liệu thống kê và các vụ việc điển hình; 3) Xác định các nguyên nhân, phương thức tấn công phổ biến và phân tích tác động của vi phạm DLCN; 4) Đánh giá mức độ nhận thức và thực hành bảo vệ DLCN của người dân và tổ chức; 5) Phân tích hiệu quả và hạn chế của các biện pháp bảo vệ hiện có; 6) Đề xuất một số giải pháp nhằm tăng cường hiệu quả bảo vệ DLCN tại Việt Nam.

**2. Phương pháp nghiên cứu**

Trong nghiên cứu này, tác giả chủ yếu sử dụng phương pháp phân tích định tính, kết hợp với một số kỹ thuật sau: - Phân tích văn bản pháp luật: Nghiên cứu, diễn giải và phân tích sâu các quy định trong Nghị định 13/2023/NĐ-CP, Luật An ninh mạng 2018, Luật Bảo vệ dữ liệu của Liên minh Châu Âu (GDPR) và các văn bản hướng dẫn liên quan; - Phân tích so sánh: Đối chiếu, so sánh các nội dung của Nghị định 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu của Liên minh Châu Âu (GDPR); - Tổng hợp và phân tích dữ liệu

*Email: manhhong@tueba.edu.vn*

thứ cấp: Thu thập, tổng hợp và phân tích số liệu thống kê, báo cáo từ các cơ quan nhà nước, tổ chức an ninh mạng, công ty tư vấn và các nguồn tin uy tín về tình hình vi phạm DLCN; - Nghiên cứu các trường hợp cụ thể: Phân tích các vụ vi phạm dữ liệu lớn và điển hình tại Việt Nam để minh họa các phương thức tấn công, hậu quả và bài học kinh nghiệm; - Phân tích chuyên gia: Tham khảo các bài phân tích, bình luận, góp ý của các chuyên gia.

**3. Bảo vệ dữ liệu cá nhân của một số quốc gia trên thế giới**

***3.1. Về pháp lý***

Hiện nay, luật pháp quốc tế vẫn chưa phát triển kịp so với công nghệ, điều này dẫn đến việc bảo vệ DLCN còn gặp rất nhiều khó khăn. Do sự phát triển nhanh chóng của công nghệ, đặc biệt là trí tuệ nhân tạo nên việc bảo vệ DLCN trong môi trường số càng trở nên cấp thiết hơn. Do đó, nhiều quốc gia trên thế giới đã ban hành đạo luật về bảo vệ DLCN. Cụ thể, đã có hơn 80 quốc gia ban hành văn bản quy phạm pháp luật về vấn đề này, tiêu biểu phải kể đến pháp luật của Liên minh Châu Âu (EU) và Hoa Kỳ.

Luật của liên minh Châu Âu (GDPR) có hiệu lực từ 25/5/2018 được xây dựng để cung cấp cho công dân của các quốc gia thành viên EU có quyền kiểm soát dữ liệu cá nhân nhiều hơn. GDPR yêu cầu các doanh nghiệp phải tuân thủ các quy định cụ thể, rõ ràng về cách thu thập thông tin cá nhân, địa điểm lưu trữ dữ liệu, loại hình dữ liệu được phép chia sẻ, các công ty nằm ngoài lãnh thổ Châu Âu cũng phải chấp hành các quy định này. Doanh nghiệp nào vi phạm sẽ bị phạt lên tới 20 triệu Euro hoặc 4% doanh thu toàn cầu hàng năm. Ngoài ra, để phù hợp hơn trong việc áp dụng các quy tắc của GDPR, nhiều quốc gia thành viên đã thay đổi luật của nước mình để áp dụng và tuân thủ các yêu cầu của GDPR như Pháp ban hành Luật số 2018-493 (FDPA) ngày 20/6/2018 về bảo vệ DLCN, vương quốc Anh thông qua Luật Bảo vệ dữ liệu quốc gia mới (DPA) có hiệu lực vào ngày 25/5/2018,... [1]. Hoa Kỳ không ban hành đạo luật riêng để quy định về vấn đề này nhưng các quy định về bảo vệ DLCN được quy định cụ thể tại các văn bản pháp luật như: phụ huynh có quyền kiểm soát đối với thông tin mà các trang web thu thập thông tin từ con cái của họ (Luật Bảo vệ quyền về sự riêng tư trực tuyến của trẻ em - COPPA), đảm bảo tính bí mật về các thông tin của bệnh nhân về thông tin liên quan đến sức khỏe,...

***3.2. Về vi phạm dữ liệu cá nhân***

Theo số liệu của công ty an ninh mạng Surfshark, năm 2024 có hơn 5,5 tỷ tài khoản bị xâm phạm, gấp gần 8 lần so với năm 2023 (khoảng 730 triệu). Trung Quốc, Nga và Mỹ là các điểm nóng chính, chiếm 46% tổng số tài khoản bị xâm phạm. Châu Á là khu vực bị ảnh hưởng thứ hai. Chi phí trung bình toàn cầu cho một vụ vi phạm dữ liệu năm 2024 là 4,88 triệu USD. Chi phí trung bình trên mỗi bản ghi là 165 USD. Ngành Y tế tiếp tục là ngành có chi phí vi phạm cao nhất (trung bình 9,77 triệu USD/vụ năm 2024). Các vụ vi phạm quy mô lớn (mega-breach) ngày càng tốn kém, với chi phí trung bình cho vụ vi phạm 50-60 triệu bản ghi là 375 triệu USD năm 2024. Trung bình mất 194 ngày để xác định và 64 ngày để ngăn chặn một vụ vi phạm dữ liệu vào năm 2024. Các vụ vi phạm liên quan đến thông tin đăng nhập bị đánh cắp mất nhiều thời gian nhất để giải quyết (trung bình 292 ngày vòng đời) [2].

**4. Bảo vệ dữ liệu cá nhân tại Việt Nam**

***4.1. Nhận thức của người dân và doanh nghiệp***

Mặc dù tình trạng vi phạm DLCN và lừa đảo trực tuyến gia tăng mạnh nhưng nhận thức của người dân về tầm quan trọng và các biện pháp tự bảo vệ DLCN vẫn còn hạn chế. Khảo sát cho thấy tỷ lệ lớn người dùng thừa nhận thông tin của họ từng bị sử dụng trái phép và nhiều người vẫn trở thành nạn nhân của các chiêu thức lừa đảo tinh vi. Nhiều người cho biết là họ sẵn sàng cung cấp thông tin cá nhân để đổi lấy những tiện ích công nghệ. Nhiều doanh nghiệp, đặc biệt là doanh nghiệp nhỏ và vừa chưa nhận thức đầy đủ về tầm quan trọng của việc bảo vệ DLCN hoặc gặp khó khăn trong việc hiểu và diễn giải các quy định phức tạp của hệ thống văn bản quy phạm pháp luật. Tuy nhiên, cũng có những chuyển biến tích cực trong nhận thức về an ninh mạng tại các doanh nghiệp sau các vụ tấn công nghiêm trọng gần đây. Khảo sát của Hiệp hội An ninh mạng quốc gia năm 2024 cho thấy 75,68% doanh nghiệp đã tiến hành đào tạo nhận thức về an ninh mạng cho nhân viên [3].

***4.2. Về pháp lý***

Hiện tại, pháp luật của Việt Nam vẫn chưa có một đạo luật riêng để quy định về việc bảo vệ DLCN. Các quy định về bảo vệ DLCN nằm rải rác trong các văn bản pháp luật khác nhau như Hiến pháp năm 2013, Luật An toàn thông tin mạng năm 2015, Luật Tiếp cận thông tin năm 2016, Bộ luật Dân sự năm 2015, Luật Bảo vệ quyền lợi người tiêu dùng năm 2010, Luật Công nghệ thông tin năm 2006,... Tuy nhiên, những quy định này được quy định không thống nhất, chồng chéo và gây khó khăn trong việc tra cứu. Nghị định 13/2023/NĐ-CP, ban hành ngày 17/4/2023 và có hiệu lực từ 01/7/2023, là văn bản pháp lý chuyên sâu đầu tiên của Việt Nam về bảo vệ DLCN. Nghị định này áp dụng cho mọi tổ chức, cá nhân trong và ngoài nước có liên quan đến xử lý DLCN tại Việt Nam, kể cả khi việc xử lý diễn ra bên ngoài lãnh thổ Việt Nam. Một số điều khoản trong Nghị định 13 còn được diễn đạt chung chung, gây khó khăn trong việc diễn giải và áp dụng thống nhất. Thiếu hướng dẫn chi tiết từ Bộ Công an cũng là một trở ngại.

*So sánh Nghị định 13/2023/NĐ-CP với Luật Bảo vệ dữ liệu của liên minh Châu Âu (GDPR):*

*Phạm vi áp dụng:* GDPR có phạm vi ngoài lãnh thổ rộng hơn, áp dụng cho bất kỳ tổ chức nào xử lý dữ liệu của cá nhân trong EU, bất kể địa điểm của tổ chức đó. Nghị định 13 tập trung hơn vào các hoạt động xử lý DLCN tại Việt Nam hoặc liên quan đến xử lý DLCN tại Việt Nam, dù có yếu tố nước ngoài.

*Phân loại dữ liệu:* Nghị định 13 phân loại rõ ràng DLCN thành cơ bản và nhạy cảm trong khi GDPR không phân loại như vậy mà coi mọi DLCN đều cần bảo vệ, với một số "hạng mục đặc biệt" (special categories) yêu cầu biện pháp bảo vệ nghiêm ngặt hơn (tương tự DLCN nhạy cảm của Việt Nam).

*Chuyển dữ liệu xuyên biên giới:* GDPR cho phép chuyển dữ liệu ra ngoài EU nếu quốc gia tiếp nhận đảm bảo mức độ bảo vệ tương đương hoặc có các biện pháp bảo vệ phù hợp (SCCs, BCRs). Nghị định 13 yêu cầu quy trình lập và nộp hồ sơ TIA phức tạp hơn và có thể tiềm ẩn yêu cầu lưu trữ dữ liệu tại chỗ (data localization) theo Luật An ninh mạng và Nghị định 53/2022/NĐ-CP (yêu cầu lưu trữ tối thiểu 24 tháng đối với một số loại dữ liệu nhất định).

*Cơ sở pháp lý cho xử lý:* Cả hai đều coi trọng sự đồng ý nhưng GDPR liệt kê 6 cơ sở pháp lý bình đẳng (bao gồm lợi ích hợp pháp), trong khi Nghị định 13 nhấn mạnh sự đồng ý là chủ yếu và liệt kê các trường hợp ngoại lệ cụ thể.

*Cơ quan quản lý và chế tài:* GDPR được thực thi bởi các Cơ quan bảo vệ dữ liệu (DPA) độc lập tại mỗi quốc gia thành viên EU, với quyền lực điều tra và phạt tiền rất lớn. Tại Việt Nam, Bộ Công an (cụ thể là A05) là cơ quan chủ trì thực hiện Nghị định 13, tập trung nhiều vào khía cạnh an ninh mạng. Mức phạt theo Nghị định 13 hiện thấp hơn nhiều so với GDPR.

*Vai trò Bên kiểm soát/xử lý:* Nghị định 13 giới thiệu vai trò "Bên kiểm soát và xử lý DLCN", một khái niệm không có trong GDPR nhưng ý nghĩa và tác động thực tế của vai trò kép này chưa hoàn toàn rõ ràng.

Do còn có những khác biệt nên các tổ chức, cá nhân đã tuân thủ GDPR không được mặc nhiên coi là tuân thủ Nghị định 13.

***4.3. Về vi phạm dữ liệu cá nhân***

Theo số liệu khảo sát của Hiệp hội An ninh mạng quốc gia (NCA), năm 2023 ghi nhận khoảng 13.900 vụ tấn công mạng vào các hệ thống tại Việt Nam, tăng 9,5% so với năm 2022. Trung bình mỗi tháng có 1.160 vụ tấn công. Thiệt hại do mất an toàn thông tin mạng ước tính khoảng 21.200 tỷ đồng trong năm 2022. Trong năm 2024, có tới 46,15% cơ quan, doanh nghiệp bị tấn công mạng ít nhất 1 lần, với tổng số hơn 659.000 vụ. 14,5 triệu tài khoản bị rò rỉ, chiếm 12% tổng số toàn cầu. Thiệt hại do lừa đảo trực tuyến ước tính 18.900 tỷ đồng. 66,24% người dùng Internet xác nhận thông tin của họ từng bị sử dụng trái phép [4]. Mặc dù số lượng sự cố được báo cáo có xu hướng giảm vào cuối năm 2024, tuy nhiên, theo các chuyên gia, mức độ tinh vi và nghiêm trọng của các cuộc tấn công lại gia tăng, đặc biệt là các cuộc tấn công bằng mã độc (ransomware) nhắm vào các ngành trọng yếu như viễn thông, năng lượng, chứng khoán, logistics.

Một số vụ việc điển hình tại Việt Nam trong năm 2024:

*VNDirect:* Công ty chứng khoán lớn bị tấn công ransomware vào tháng 3/2024 khiến toàn bộ hệ thống giao dịch ngừng hoạt động trong nhiều ngày. Vụ việc cho thấy mức độ nghiêm trọng và khả năng gây tê liệt của ransomware đối với các tổ chức tài chính [5].

*PVOIL:* Bị tấn công ransomware vào đầu tháng 4/2024, làm gián đoạn hệ thống công nghệ thông tin, bao gồm cả việc xuất hóa đơn điện tử tại các cửa hàng bán lẻ xăng dầu [5].

*Rò rỉ dữ liệu ngành Y tế và Giáo dục:* Rất nhiều phụ huynh cho biết họ nhận được các cuộc gọi từ người lạ, tự xưng là giáo viên thông báo con họ đang gặp nguy hiểm và yêu cầu chuyển tiền để làm thủ tục cấp cứu. Với ngành Y tế, mặc dù chưa có báo cáo chi tiết về các vụ cụ thể lớn tại Việt Nam trong năm 2024 nhưng nguy cơ là hiện hữu, điển hình là vụ tấn công vào hãng xét nghiệm Synnovis ở Anh.

**5. Nguyên nhân và phương thức tấn công**

Có nhiều nguyên nhân gây lộ, lọt thông tin cá nhân, từ đó tạo cơ hội cho các tin tặc sử dụng để tấn công. Một số nguyên nhân chủ yếu là:

*Lỗi do con người:* Các lỗi như gửi nhầm thông tin (misdelivery), cấu hình sai hệ thống bảo mật, mật khẩu yếu hoặc tái sử dụng (lỗi chiếm 28% các vụ vi phạm trong năm 2022).

*Vi phạm từ bên thứ ba:* Các vụ tấn công nhắm vào nhà cung cấp dịch vụ hoặc phần mềm bên thứ ba ngày càng gia tăng, ảnh hưởng đến nhiều khách hàng cùng lúc. Các vụ vi phạm liên quan đến bên thứ ba tăng 68% trong năm 2024.

*Mua bán dữ liệu trái phép:* Tình trạng mua bán DLCN diễn ra công khai trên không gian mạng, bao gồm cả sự tham gia của các công ty, tổ chức.

Về phương thức tấn công, ngày càng có những phương thức tấn công tinh vi. Một số phương thức tấn công chủ yếu hiện nay là:

*Tấn công có chủ đích (APT) và mã độc tống tiền (Ransomware):* Đây là hình thức tấn công phổ biến và gây hậu quả nghiêm trọng nhất trong năm 2024 tại Việt Nam. Ransomware chiếm gần 24% các sự cố sử dụng mã độc trên toàn cầu và cùng với các hình thức tống tiền khác chiếm tới 32% tổng số vụ vi phạm. Tin tặc mã hóa dữ liệu và đòi tiền chuộc, gây thiệt hại tài chính và gián đoạn hoạt động nghiêm trọng.

*Khai thác lỗ hổng bảo mật:* Việc khai thác các lỗ hổng phần mềm (bao gồm cả zero-day) đã tăng gấp ba lần trong năm 2024 và trở thành con đường chính để xâm nhập hệ thống, đặc biệt là thông qua các ứng dụng web.

*Tấn công phi kỹ thuật (Social Engineering):* Lừa đảo (phishing), lừa đảo qua tin nhắn (smishing) và các hình thức giả mạo (pretexting) vẫn là phương thức hiệu quả để đánh cắp thông tin đăng nhập và lừa người dùng tiết lộ thông tin nhạy cảm hoặc cài đặt mã độc. Yếu tố con người là nguyên nhân trong 68% các vụ vi phạm. Khoảng 20% người dùng nhấp vào liên kết trong các chiến dịch mô phỏng lừa đảo.

**6. Một số giải pháp nhằm nâng cao hiệu quả bảo vệ dữ liệu cá nhân**

Để giải quyết những thách thức và tăng cường hiệu quả bảo vệ DLCN tại Việt Nam cần triển khai đồng bộ các giải pháp trên nhiều phương diện: nhận thức cộng đồng, pháp lý và công nghệ.

***6.1. Nâng cao nhận thức và giáo dục cộng đồng***

Nâng cao hiệu quả công tác truyền thông: Chính phủ chủ trì, phối hợp với các hiệp hội (NCA, VNBA), các tổ chức xã hội và doanh nghiệp cần triển khai chiến dịch truyền thông quy mô lớn và bền vững để nâng cao nhận thức của người dân về quyền DLCN, các rủi ro trên không gian mạng và biện pháp tự bảo vệ cơ bản.

Tích hợp vào chương trình giáo dục: Đưa nội dung về an toàn thông tin, quyền riêng tư và bảo vệ DLCN vào chương trình giáo dục phổ thông và đại học như một kỹ năng số cơ bản. Trang bị cho học sinh, sinh viên kiến thức và kỹ năng để nhận biết rủi ro và bảo vệ bản thân trên môi trường mạng.

Xây dựng tài liệu hướng dẫn dễ hiểu: Cung cấp các tài liệu, cẩm nang hướng dẫn đơn giản, dễ hiểu cho người dân về cách quản lý cài đặt quyền riêng tư, tạo mật khẩu mạnh, nhận diện lừa đảo và thực hiện các quyền của mình theo quy định.

Thúc đẩy văn hóa quyền riêng tư: Khuyến khích sự tôn trọng quyền riêng tư như một giá trị xã hội, nơi mọi cá nhân và tổ chức đều có ý thức trách nhiệm trong việc bảo vệ DLCN của bản thân và của người khác.

***6.2. Cải thiện khung pháp lý và cơ chế thực thi***

Ban hành Luật Bảo vệ DLCN: Sớm ban hành Luật Bảo vệ DLCN để luật hóa các quy định của Nghị định 13, tạo cơ sở pháp lý vững chắc và thống nhất. Cần tham khảo kinh nghiệm quốc tế (đặc biệt là GDPR) và ý kiến đóng góp từ các bên liên quan (doanh nghiệp, hiệp hội, chuyên gia) để đảm bảo tính khả thi và hài hòa.

Ban hành quy định xử phạt cụ thể và rõ ràng: Cần sớm ban hành văn bản quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng. Mức phạt cần đủ sức răn đe, có thể tham khảo mức phạt của GDPR nhưng cần cân nhắc tính khả thi trong bối cảnh của Việt Nam.

Tăng cường năng lực thực thi: Nâng cao năng lực cho Bộ Công an (A05) và các cơ quan liên quan trong việc giám sát, thanh tra, kiểm tra và xử lý vi phạm. Cân nhắc thành lập một cơ quan chuyên trách về bảo vệ dữ liệu (tương tự DPA của EU) để đảm bảo tính độc lập, chuyên môn và hiệu quả trong thực thi, tách biệt khỏi các nhiệm vụ an ninh mạng thuần túy.

***6.3. Ứng dụng công nghệ tiên tiến***

Hiện nay, có nhiều công nghệ giúp người dân bảo vệ DLCN, nghiên cứu này đề xuất một số công nghệ như sau:

*6.3.1. Công nghệ tăng cường quyền riêng tư (PETs)*

Áp dụng các PETs để tối đa hóa việc sử dụng dữ liệu mà vẫn giảm thiểu rủi ro về quyền riêng tư. Các công nghệ này bao gồm: - *Mã hóa (Encryption):* Đặc biệt là mã hóa đồng cấu (Homomorphic Encryption - HE) cho phép tính toán trên dữ liệu đã mã hóa mà không cần giải mã; - *Ẩn danh hóa (Anonymisation) và giả danh hóa (Pseudonymisation):* Loại bỏ hoặc thay thế các yếu tố nhận dạng trực tiếp; - *Quyền riêng tư vi phân (Differential Privacy - DP):* Thêm nhiễu (noise) vào tập dữ liệu hoặc kết quả truy vấn để bảo vệ thông tin cá nhân trong khi vẫn cho phép phân tích thống kê; - *Tính toán đa bên an toàn (Secure Multi-Party Computation - SMPC):* Cho phép nhiều bên cùng tính toán một hàm trên dữ liệu riêng tư của họ mà không tiết lộ dữ liệu đầu vào cho nhau; - *Bằng chứng không tiết lộ thông tin (Zero-Knowledge Proofs - ZKP):* Cho phép một bên chứng minh tính đúng đắn của một tuyên bố mà không tiết lộ bất kỳ thông tin nào ngoài chính tuyên bố đó; - *Dữ liệu tổng hợp (Synthetic Data):* Tạo ra dữ liệu nhân tạo có các thuộc tính thống kê tương tự dữ liệu gốc nhưng không chứa thông tin cá nhân thực tế; - *Môi trường thực thi tin cậy (Trusted Execution Environments - TEEs):* Cung cấp một khu vực xử lý an toàn trong phần cứng để bảo vệ dữ liệu và mã lệnh khỏi sự truy cập trái phép. Cần giải quyết các thách thức trong việc áp dụng PETs như nhận thức thấp, thiếu tiêu chuẩn hóa và chi phí.

*6.3.2. Trí tuệ nhân tạo (AI)*

Ứng dụng AI để tăng cường khả năng phát hiện và ứng phó với các mối đe dọa an ninh mạng. AI có thể phân tích lượng lớn dữ liệu để phát hiện các hành vi bất thường, dự đoán các cuộc tấn công, tự động hóa phản ứng sự cố và ưu tiên các cảnh báo.

*6.3.3. Ngăn chặn mất mát dữ liệu (Data Loss Prevention - DLP)*

Triển khai các hệ thống DLP để giám sát, phát hiện và ngăn chặn việc truy cập, di chuyển hoặc rò rỉ DLCN trái phép. DLP hoạt động trên các điểm cuối (endpoint), mạng (network) và đám mây (cloud), sử dụng các kỹ thuật như phân loại dữ liệu, giám sát hành vi người dùng, mã hóa và cảnh báo.

*6.3.4. Kiến trúc Không tin cậy (Zero Trust Architecture - ZTA)*

Áp dụng mô hình ZTA, trong đó không có sự tin cậy mặc định nào được cấp cho bất kỳ người dùng hay thiết bị nào, dù ở bên trong hay bên ngoài mạng. Mọi yêu cầu truy cập tài nguyên (bao gồm dữ liệu) đều phải được xác thực, ủy quyền và kiểm tra liên tục dựa trên nguyên tắc đặc quyền tối thiểu.

**7. Kết luận**

Việc bảo vệ DLCN đã trở thành một yêu cầu cấp thiết và là một thách thức lớn đối với Việt Nam

trong bối cảnh hội nhập quốc tế và phát triển kinh tế số. Sự ra đời của Nghị định 13/2023/NĐ-CP là một bước tiến pháp lý quan trọng, tạo ra một khung khổ toàn diện hơn, tiệm cận với các tiêu chuẩn quốc tế như GDPR nhằm bảo vệ quyền lợi chính đáng của công dân trên không gian mạng. Tuy nhiên, phân tích thực trạng cho thấy, khung pháp lý vẫn cần hoàn thiện, làm rõ và bổ sung các quy định về chế tài xử phạt cụ thể, đủ sức răn đe. Tình hình vi phạm dữ liệu, đặc biệt là các cuộc tấn công tinh vi như ransomware vẫn diễn biến phức tạp, gây thiệt hại lớn về kinh tế và lòng tin. Nhận thức của cả người dân và tổ chức, đặc biệt là doanh nghiệp nhỏ và vừa về tầm quan trọng và cách thức bảo vệ DLCN còn hạn chế. Các doanh nghiệp đối mặt với nhiều khó khăn về nguồn lực, kỹ thuật và quy trình để tuân thủ đầy đủ các yêu cầu của Nghị định 13. Vì vậy, để vượt qua những thách thức này cần có một cách tiếp cận đa chiều và sự chung tay của toàn xã hội. Về mặt pháp lý, cần sớm ban hành Luật Bảo vệ DLCN. Về công nghệ, cần nghiên cứu và ứng dụng các giải pháp tiên tiến như PETs, AI, DLP và ZTA sẽ giúp nâng cao khả năng phòng thủ và ứng phó với các mối đe dọa ngày càng tinh vi. Về tổ chức, các doanh nghiệp cần chủ động xây dựng văn hóa bảo mật, áp dụng các chuẩn mực quản lý quốc tế, đầu tư vào đào tạo nhân viên và chuẩn bị sẵn sàng các kế hoạch ứng phó sự cố. Cuối cùng, việc nâng cao nhận thức và trang bị kỹ năng số cho cộng đồng thông qua các chiến dịch truyền thông và giáo dục sâu rộng là nền tảng vững chắc để mỗi cá nhân có thể tự bảo vệ mình và góp phần xây dựng môi trường số an toàn, đáng tin cậy.

**Tài liệu tham khảo**

[1] EUR-Lex (2022), *General data protection regulation (GDPR) - Quy định bảo vệ dữ liệu chung*, nguồn: https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html, truy cập ngày 10/4/2025.

[2] Surfshark (2025), *Data Breach Statistics & Trends for 2024: Recap - Thống kê vi phạm dữ liệu toàn cầu: tóm tắt năm 2024*, nguồn: https://surfshark.com/research/study/data-breach-recap-2024, truy cập ngày: 22/4/2025.

[3] NCS Group (2025), *Báo cáo an ninh mạng 2024*, nguồn: https://ncsgroup.vn/wp-content/uploads/2025/01/NCS-Bao-cao-an-ninh-mang-2024.pdf, truy cập ngày 22/4/2025.

[4] Công ty Cổ phần công nghệ an ninh mạng Quốc gia Việt Nam (2024), *Tổng kết An ninh mạng Việt Nam năm 2023 và dự báo 2024*, nguồn: https://ncsgroup.vn/tong-ket-an-ninh-mang-viet-nam-nam-2023-va-du-bao-2024/, truy cập ngày 15/4/2025.

[5] An An (2024), *Từ vụ VNDirect, PVOil,... bị hack trong năm 2024: "Cảnh báo đỏ" về ransomware*, nguồn: https://www.nguoiduatin.vn, ngày 29/12/2024.

[6] Chính phủ (2023), *Nghị định số 13/2023/NĐ-CP, ngày 17/4/2023 bảo vệ dữ liệu cá nhân.*

[7] Nguyễn Hương, Nguyễn Đức Hùng (2024), *Luật An ninh mạng và các văn bản hướng dẫn (cập nhật)*. Nguồn: https://luatvietnam.vn, ngày 02/10/2024.

[8] Duy Anh (2024), *Dữ liệu cá nhân của hơn 66% người dùng Internet bị sử dụng trái phép trong năm 2024*, nguồn: https://lsvn.vn, ngày 29/12/2024.

[9] Phan Anh (2024), *Hơn 61 triệu tài khoản, bản ghi thông tin cá nhân bị lộ lọt trong nửa đầu năm 2024*, nguồn: https://vneconomy.vn, ngày 13/8/2024.

[10] Hiệp hội An ninh mạng quốc gia - NCA (2025), *Báo cáo tổng kết An ninh mạng năm 2024 (khu vực cơ quan, doanh nghiệp)*, nguồn: https://www.nca.org.vn, ngày 23/12/2024.

[11] Quỳnh Anh (2025), *Luật Bảo vệ dữ liệu cá nhân: Đảm bảo quyền riêng tư trong thời đại số*, nguồn: https://kinhtedothi.vn, ngày 5/4/2025.

[12] Nguyễn Giang Trường (2024), *Thực trạng về vấn đề bảo vệ dữ liệu cá nhân, kinh nghiệm một số quốc gia, khu vực và đề xuất hoàn thiện pháp luật ở Việt Nam hiện nay*, Tạp chí Công thương, số 12 tháng 5.

[13] University of Pittsburgh Human Research Protection Office, *European Union (EU) General Data Protection Regulation (GDPR) - Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu*, nguồn: https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr, truy cập ngày 10/4/2025.