QUYỀN RIÊNG TƯ TRONG CHĂM SÓC SỨC KHỎE TẠI VIỆT NAM – THÁCH THỨC VÀ GIẢI PHÁP

TS NGUYỄN HỒ BÍCH HẰNG*
Khoa Luật, Đại học Đông Phần Lan
School of Law, University of Eastern Finland,
Email: nhbhang@hcmulaw.edu.vn
TS TRẦN NGỌC TUẤN
Khoa Luật Dân sự, Trường Đại Học Luật TP. Hồ Chí Minh
Faculty of Civil Law, Ho Chi Minh City University of Law
Email: tntuan@hcmulaw.edu.vn

Tóm tắt

Trong bối cảnh chuyển đổi số và ứng dụng công nghệ vào chăm sóc sức khỏe, quyền riêng tư tại Việt Nam, đặc biệt là quyền riêng tư trong chăm sóc sức khỏe ở lĩnh vực y tế, vẫn chưa được bảo vệ và chú trọng một cách toàn diện. Bài viết tập trung phân tích các quy định pháp luật hiện hành của Việt Nam liên quan đến quyền riêng tư trong chăm sóc sức khỏe, đồng thời so sánh với quy định pháp luật của châu Âu, Nhật Bản và Singapore. Từ đó, bài viết đúc kết kinh nghiệm và đưa ra các kiến nghị hoàn thiện các quy định pháp luật nhằm nâng cao hiệu quả bảo vệ quyền riêng tư của cá nhân, thúc đẩy một môi trường y tế an toàn, bền vững tại Việt Nam.

Từ khóa: *chăm sóc sức khỏe, dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm, Quy định chung về bảo vệ dữ liệu, quyền riêng tư*

Abstract

In the era of digital transformation and technology integration into healthcare, privacy protection in Vietnam, particularly in healthcare, requires urgent and greater attention. This article examines the current Vietnamese legal framework governing privacy in healthcare and compares it with advanced legal systems in the European Union, Japan, and Singapore. Through this comparative analysis, the study highlights essential lessons and proposes recommendations to strengthen Vietnam's regulations, enhance personal privacy protection, and foster a secure, sustainable healthcare environment.

Keywords: *General Data Protection Regulation, healthcare, personal data, privacy, sensitive data*
DOI: https://doi.org/10.70236/khplvn.604
Ngày nhận bài: 05/02/2025 **Ngày duyệt đăng: 08/04/2026**

1. Khái quát về quyền riêng tư trong chăm sóc sức khỏe tại Việt Nam

Quyền riêng tư[1] trong chăm sóc sức khỏe (hay còn gọi là quyền riêng tư y tế) là một trong những quyền của người bệnh được bảo vệ bí mật riêng tư về tình trạng sức khỏe của mình và các vấn đề khác có liên quan trong lĩnh vực y tế. Theo quy định tại Luật Khám bệnh, chữa bệnh năm 2023 (Luật KCB năm 2023),[2] người bệnh có quyền được tôn trọng danh dự, bảo vệ sức khỏe và tôn trọng bí mật riêng tư trong quá trình khám, chữa bệnh.[3] Người bệnh được tôn trọng về tuổi tác, giới tính, dân tộc, tôn giáo, tín ngưỡng, tình trạng sức khỏe, điều kiện kinh tế và địa vị xã hội. Mọi thông tin trong hồ sơ bệnh án và các thông tin đời tư cung cấp trong quá trình khám, chữa bệnh phải được giữ bí mật, trừ khi người bệnh đồng ý hoặc theo quy định pháp luật.[4] Đây là luật chuyên ngành đầu tiên tại Việt Nam ghi nhận trực tiếp quyền riêng tư trong chăm sóc sức khỏe, đặt nền tảng pháp lý quan trọng trong việc bảo vệ dữ liệu cá nhân nhạy cảm trong lĩnh vực chăm sóc sức khỏe hiện nay.

* Bài viết thuộc phạm vi công trình nghiên cứu khoa học cấp Trường trọng điểm năm 2026 của Trường Đại học Luật TP. Hồ Chí Minh, đề tài "Trách nhiệm bồi thường thiệt hại do ứng dụng trí tuệ nhân tạo trong chăm sóc y tế tại Việt Nam", chủ nhiệm đề tài: TS. Nguyễn Xuân Quang theo Quyết định số 246/QĐ-ĐHL ngày 24/02/2026.

1 Trong phạm vi bài viết này, quyền riêng tư được tiếp cận như một khái niệm bao trùm, trong đó bí mật riêng tư là một nội dung cấu thành.

2 Luật Khám bệnh, chữa bệnh năm 2023 được thông qua ngày 09/01/2023.

3 Điều 10 Luật KCB năm 2023.

4 Khoản 3 và khoản 4 Điều 69 Luật KCB năm 2023.

Quyền riêng tư trong chăm sóc sức khỏe là một loại của quyền riêng tư.[5] Điểm khác biệt của quyền này là có tính nhạy cảm và bí mật cao hơn so với quyền riêng tư thông thường. Quyền riêng tư trong chăm sóc sức khỏe thông thường được thể hiện qua hồ sơ bệnh án.[6] Nếu quyền riêng tư trong chăm sóc sức khỏe bị tiết lộ, cá nhân đó có thể dễ dàng bị người khác đánh giá, dẫn đến hành vi phân biệt đối xử trong công việc hoặc sinh hoạt hàng ngày.[7]

Ngoài ra, nếu quyền riêng tư trong chăm sóc sức khỏe không được bảo vệ đầy đủ và có nguy cơ bị tiết lộ, người bệnh có thể phát sinh tâm lý che giấu các thông tin y tế liên quan đến tình trạng thể chất và tâm lý của mình khi điều trị hoặc tránh né một số kiểm tra y tế.[8] Khi đó, bác sĩ sẽ không có đủ thông tin y tế để đưa ra các quyết định điều trị chính xác, làm sai lệch kết quả chẩn đoán và phát sinh tranh chấp y tế, gây ra tình trạng bất lợi cho các bên. Tuy nhiên, trong một số trường hợp, việc giữ bí mật thông tin của người bệnh và tôn trọng quyền riêng tư của người bệnh còn có thể xung đột với lợi ích của bên thứ ba, thậm chí là cả cộng đồng,[9] đòi hỏi phải có những giới hạn nhất định đối với quyền này. Chính vì vậy, quyền riêng tư trong chăm sóc sức khỏe không chỉ cần được bảo vệ ở mức độ cao hơn so với quyền riêng tư thông thường[10] mà còn phải được điều chỉnh theo nguyên tắc cân bằng với các lợi ích hợp pháp khác trong xã hội.

Trên thực tế, tại Việt Nam, tình trạng các cơ sở y tế bị tin tặc tấn công ngày càng gia tăng.[11] Khi xảy ra sự cố tấn công bằng mã độc mã hóa dữ liệu nhằm mục đích tống tiền, hoạt động khám chữa bệnh tại các bệnh viện, cơ sở y tế sẽ tê liệt, chưa kể thông tin của người bệnh có thể bị đánh cắp, rao bán.[12] Cụ thể, "tháng 11/2023, website của Bệnh viện Chợ Rẫy bị tin tặc tấn công cài mã độc, chiếm quyền điều khiển. Tháng 12/2023, dữ liệu của Bệnh viện Đa khoa Trung tâm tỉnh An Giang bị mã hóa. Mới đây nhất, tháng 3/2024, website lấy số khám bệnh trực tuyến của Bệnh viện Tim TP. Hồ Chí Minh bị tấn công, làm ngưng trệ hoạt động của hệ thống."[13] Tình trạng này phổ biến tại các quốc gia trên thế giới, có thể kể đến các vụ việc gần đây tại Thái Lan[14]

5 Trần Ngọc Tuấn, "Bảo vệ quyền riêng tư của bệnh nhân đối với hình ảnh y tế thông qua công nghệ blockchain", *Tạp chí Khoa học xã hội Việt Nam*, số 11, 2022, tr. 80-81.

6 Khoản 17 Điều 2 Luật KCB năm 2023.

7 Trong vụ việc giữa *I v. Finland* do Tòa án Nhân quyền châu Âu phán quyết năm 2008, sau khi hồ sơ HIV dương tính của nguyên đơn bị bộc lộ khiến cho những đồng nghiệp tại nơi làm việc biết, cô đã không được gia hạn hợp đồng với nơi làm việc, buộc cô phải tìm kiếm một công việc khác, xem *ECHR I v. Finland*, No. 20511/03, 2008, https://www.5rb.com/case/i-v-finland/, truy cập ngày 8/11/2025.

8 Năm 2021, Bộ Công an khởi tố vụ án một cá nhân mắc ung thư nhưng che giấu bệnh án để mua 19 hợp đồng bảo hiểm từ 15 công ty. Người này hợp pháp hóa hồ sơ bệnh án và yêu cầu chi trả, nhận 4 tỷ đồng từ 5 công ty, Xem Bông Mai, "Đổi tên khi khám bệnh, giấu ung thư để mua 19 hợp đồng bảo hiểm", *Báo Tuổi Trẻ*, 2024, http:// https://tuoitre.vn/doi-ten-khi-kham-benh-giau-ung-thu-de-mua-19-hop-dong-bao-hiem-20240906104537847.htm, truy cập ngày 8/11/2025.

9 Phạm Thị Anh Đào, Đặng Ngọc Huyền Vy, "Quyền bảo mật thông tin của người nhiễm HIV/AIDS ở Việt Nam hiện nay", *Tạp Chí Khoa học Kiểm sát*, số 7(91), 2025, tr. 56, DOI: https://doi.org/10.59554/tckhks.v7i91.588

10 Adebayo Yusuf Balogun, "Strengthening compliance with data privacy regulations in US healthcare cybersecurity", *Asian Journal of Research in Computer Science*, Vol. 18(1), 2025, tr. 154-173, DOI: https://doi.org/10.9734/ajrcos/2025/v18i1555

11 Tăng Thị Bích Diễm, "Trách nhiệm dân sự trong xử lý dữ liệu cá nhân theo Điều 82 Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu – Kinh nghiệm cho Việt Nam", *Tạp chí Khoa học pháp lý Việt Nam,* số 05 (189), 2025, tr. 15.

12 Trọng Đạt, "Bệnh viện có thể tê liệt vì hacker mã hoá dữ liệu tống tiền", *Báo VietNamNet*, 2024, https://vietnamnet.vn/benh-vien-co-the-te-liet-vi-hacker-ma-hoa-du-lieu-tong-tien-2273268.html, truy cập ngày 8/11/2025.

13 Trọng Đạt, *tlđd*.

14 Thái Lan, tháng 01/2022 thông tin của 39 triệu người bệnh được cho là từ bệnh viện Siriraj tại Bangkok bị đánh cắp và rao bán trên một diễn đàn chia sẻ dữ liệu trên internet. Xem: Suchit Leesa-Nguansuk, "Claim on huge data leak", *Bangkok Post PCL.*, 2022, https://www.bangkokpost.com/thailand/general/2245063/claim-on-huge-patient-data-leak, truy cập ngày 8/11/2025.

hoặc tại Hoa Kỳ.[15] Tuy nhiên, những vụ việc nêu trên chỉ dừng lại ở mức độ tin tặc tấn công đơn vị y tế và người bệnh chưa ghi nhận thiệt hại trực tiếp. Tại Phần Lan, năm 2020, cơ sở điều trị sức khỏe tâm thần, bị tin tặc tấn công, làm lộ thông tin 30.000 bệnh án do không mã hóa dữ liệu. Tin tặc tống tiền cả bệnh viện và người bệnh, gây hậu quả nghiêm trọng đến đời sống riêng tư và tâm lý nạn nhân.[16] Những tác động tâm lý phát sinh từ vụ tấn công này sẽ gây ra những hệ lụy lâu dài đối với nạn nhân. Phần Lan, ngoài việc triển khai các biện pháp pháp lý có liên quan đến việc bảo mật dữ liệu cá nhân còn triển khai một loạt các hoạt động xã hội, tôn giáo nhằm hỗ trợ những nạn nhân trong vụ việc nói trên.[17] Do đó, việc hoàn thiện các quy định liên quan đến quyền riêng tư trong chăm sóc sức khỏe không chỉ bảo đảm quyền lợi của người bệnh mà còn góp phần nâng cao chất lượng dịch vụ y tế, tạo niềm tin cho cộng đồng.

2. Quyền riêng tư trong chăm sóc sức khỏe gắn liền với dữ liệu cá nhân nhạy cảm

Ngay từ năm 425 trước Công nguyên, bác sĩ phẫu thuật Hippocrates (460BC-380BC) đã đưa ra Lời thề (*The Hippocratic Oath*), tuyên bố nguyên tắc bảo mật quyền riêng tư của người bệnh.[18] Lời thề Hippocrates đã thiết lập cam kết bảo vệ bí mật của người bệnh, đánh dấu sự khởi đầu cho nguyên tắc bảo mật thông tin trong lĩnh vực y khoa.[19] Với sự phát triển của công nghệ và dữ liệu lớn (*big data*), quyền riêng tư trong chăm sóc sức khỏe ngày càng đối mặt với thách thức từ việc trao đổi thông tin và ứng dụng công nghệ trong y tế. Trong bối cảnh đó, nhằm tăng cường cơ chế bảo vệ dữ liệu cá nhân trước những rủi ro mới phát sinh, pháp luật một số quốc gia đã phân biệt dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm, nhằm cung cấp sự bảo vệ tốt hơn cho từng loại dữ liệu.

2.1. Quy định về dữ liệu cá nhân nhạy cảm

2.1.1. Quy định của Liên minh châu Âu

Dữ liệu cá nhân nhạy cảm được quy định dưới dạng hạng mục dữ liệu cá nhân đặc biệt trong Quy định chung về bảo vệ dữ liệu (*General Data Protection Regulation*, GDPR), bao gồm thông tin về chủng tộc, quan điểm chính trị, tín ngưỡng, thành viên công đoàn, dữ liệu di truyền, sinh trắc học, sức khỏe, đời sống tình dục hoặc khuynh hướng tình dục.[20] GDPR cấm xử lý loại dữ liệu này, trừ trường hợp ngoại lệ được quy định. Một số trường hợp ngoại lệ cho phép xử lý dữ liệu cá nhân đặc biệt, bao gồm có sự đồng thuận từ chủ thể dữ liệu, để bảo vệ quyền lợi cá nhân, để phục vụ công tác y tế dự phòng và y tế nghiệp vụ, hoặc vì lợi ích công cộng. Bên cạnh đó, khoản 4 Điều 9 quy định rằng: "Các quốc gia thành viên có thể duy trì hoặc đưa ra các điều kiện bổ sung, bao gồm các hạn chế, liên quan đến việc xử lý dữ liệu di truyền, dữ liệu sinh trắc

15 Ngày 22/4/2024, United Health Group thông báo tin tặc đã đánh cắp lượng lớn dữ liệu tại Change Healthcare, đơn vị xử lý 50% yêu cầu bảo hiểm y tế Mỹ, gây gián đoạn nghiêm trọng trong thanh toán ngành y tế. Xem Mannas Mishra & Zeba Siddiqui, "United Health says hackers possibly stole large number of Americans' data", *Reuters*, 2024, https://www.reuters.com/technology/cybersecurity/unitedhealth-says-hack-could-impact-data-substantial-proportion-americans-2024-04-22/, truy cập ngày 8/11/2025.

16 Cyber Peace Institute, "Vastaamo data breach - Attack on human security, dignity and equity", *Cyber Peace Institute*, 2020, https://cyberpeaceinstitute.org/news/2020-10-28-vastaamo-data-breach-attack-on-human-security-dignity-and-equity/, truy cập ngày 8/11/2025.

17 Nguyễn Hồ Bích Hằng, "Bình luận về những quy định liên quan đến dữ liệu cá nhân theo quy định của pháp luật Việt Nam", *Tạp chí Khoa học Pháp lý Việt Nam*, số 08 (180), 2024, tr. 34 - 47.

18 The Hippocratic Oath, "Greeek Medicine", 2012, https://www.congress.gov/117/meeting/house/114995/documents/HHRG-117-IF02-20220719-SD007.pdf, truy cập ngày 8/11/2025.

19 Lois N. Magner & Oliver Kim, *A history of medicine*, CRC press, 2017, DOI: https://doi.org/10.1201/9781315113814

20 Khoản 1 Điều 9, GDPR.

học hoặc dữ liệu liên quan đến sức khỏe". Do đó, các quốc gia thành viên có thể tùy theo điều kiện, hoàn cảnh mà có thể giới hạn dữ liệu cá nhân đặc biệt liên quan đến lĩnh vực sức khỏe. Ngoài ra, Điều 16 GDPR quy định rằng chủ thể dữ liệu có quyền yêu cầu sửa đổi dữ liệu cá nhân nếu thông tin không chính xác hoặc chưa đầy đủ, nhằm bảo đảm dữ liệu được xử lý một cách chính xác và phù hợp với mục đích. Hơn nữa, Điều 17 quy định quyền xóa dữ liệu cá nhân hay "quyền được lãng quên", cho phép chủ thể yêu cầu xóa dữ liệu cá nhân mà không chậm trễ trong các trường hợp như dữ liệu không còn cần thiết, chủ thể rút lại sự đồng ý, dữ liệu được xử lý bất hợp pháp, hoặc cần xóa để tuân thủ pháp luật. Tuy nhiên, quyền này không áp dụng trong một số trường hợp ngoại lệ, chẳng hạn như bảo vệ quyền tự do ngôn luận, thực hiện nghĩa vụ pháp lý, phục vụ lợi ích công cộng, nghiên cứu khoa học hoặc bảo vệ pháp lý.

Hơn nữa, ngày 24.4.2024 các thành viên của quốc hội châu Âu đã thông qua cơ chế thiết lập Không gian Dữ liệu Y tế châu Âu (*European Health Data Space - EHDS*) là một hệ sinh thái cụ thể về sức khỏe bao gồm các quy định, tiêu chuẩn và thực hành chung, cơ sở hạ tầng và khuôn khổ quản trị nhằm mục tiêu (i) tăng cường quyền lợi cho cá nhân thông qua việc tăng cường truy cập kỹ thuật số và kiểm soát dữ liệu y tế cá nhân điện tử ở cấp quốc gia và trên toàn Liên minh châu Âu (EU); (ii) khuyến khích một thị trường thống nhất về hồ sơ y tế điện tử, các thiết bị y tế liên quan và các hệ thống trí tuệ nhân tạo có rủi ro cao; (iii) cung cấp một cơ cấu đáng tin cậy và hiệu quả cho việc sử dụng dữ liệu y tế cho nghiên cứu, đổi mới, hoạch định chính sách.[21]

EHDS cùng với GDPR sẽ tạo điều kiện cho phép cá nhân trên khắp EU có quyền kiểm soát dữ liệu sức khỏe của mình một cách hiệu quả. EHDS sẽ trao quyền cho người bệnh trong việc tiếp cận dữ liệu sức khỏe của mình dưới định dạng điện tử, bao gồm việc truy cập các thông tin này từ quốc gia thành viên của EU khác với quốc gia mà người đó đang sinh sống, và cho phép chuyên gia y tế tham khảo hồ sơ y tế của người bệnh khi có sự đồng ý của người bệnh từ một quốc gia khác. Những hồ sơ sức khỏe điện tử sẽ bao gồm các bản tóm tắt bệnh án, đơn thuốc điện tử, hình ảnh y tế và kết quả xét nghiệm.[22] Với EHDS, cá nhân tại EU có thể truy cập và kiểm soát dữ liệu sức khỏe dễ dàng hơn, đồng thời hỗ trợ chuyên gia y tế tiếp cận lịch sử y tế xuyên biên giới, nâng cao hiệu quả chẩn đoán và điều trị. Chẳng hạn, một người Thụy Điển du lịch tại Áo có thể được bác sĩ tại Áo truy cập dữ liệu y tế của người Thụy Điển để điều trị thích hợp. Những lợi ích của EHDS không chỉ dừng lại ở đó, mà còn có tác dụng đối với các đơn vị cung cấp dịch vụ y tế, các nhà nghiên cứu, nhà hoạch định chính sách, và cả đối với ngành công nghiệp liên quan đến y tế, sức khỏe.[23] Đây là quy định mang tính đột phá của EU trong bảo vệ dữ liệu y tế, đặc biệt quan trọng trước tình trạng gia tăng tấn công mạng vào cơ sở y tế nhằm chiếm đoạt và cưỡng đoạt tài sản của cơ sở y tế và/hoặc người bệnh.[24]

Bên cạnh các văn bản nêu trên, liên quan đến dữ liệu y tế, EU còn có Quy định (EU) 2021/2281.[25] Quy định này góp phần nâng cao năng lực cung cấp các công nghệ

21 EHDS, "European Health Data Space (EHDS) - Updates", https://www.european-health-data-space.com, truy cập ngày 8/11/2025.
22 EHD, *tlđd*.
23 European Commission, Questions and Answers on the European Health Data Space, 24/4/2024, tr. 1.
24 David Fåhraeus, Jane Reichel, Santa Slokenberg, "The European Health Data Space: Challenges and Opportunities", *Swedish Institute for European Policy Studies*, 2024, tr. 16.
25 Quy định (EU) 2021/2281 của Nghị viện và Hội đồng châu Âu ngày 15/12/2021 về đánh giá công nghệ y tế và sửa đổi Chỉ thị 2011/24/EU (Quy định (EU) 2021/2281).

tiên tiến trong lĩnh vực y tế cho người bệnh EU, chẳng hạn như thuốc và một số thiết bị y tế. Quy định này bảo đảm sử dụng hiệu quả các nguồn lực và tăng cường chất lượng đánh giá công nghệ y tế trên toàn Liên minh. Để tạo điều kiện thuận lợi cho công việc chung và trao đổi thông tin giữa các quốc gia thành viên trong EU về đánh giá công nghệ y tế, một nền tảng công nghệ thông tin sẽ được thành lập trên cơ sở dữ liệu và chức năng của các cơ quan chuyên môn. Nền tảng công nghệ thông tin này sẽ phải liên kết chặt chẽ với EHDS. Mặc dù vậy, Quy định (EU) 2021/2281 chỉ sẽ được áp dụng từ ngày 12/1/2025 và có hiệu lực đối với toàn bộ các quốc gia thành viên của châu Âu.[26]

Như vậy, sự kết hợp giữa GDPR, EHDS và các quy định liên quan thể hiện nỗ lực của EU trong việc cân bằng quyền lợi cá nhân và lợi ích cộng đồng, đồng thời thúc đẩy sự phát triển bền vững và hiện đại hóa hệ thống y tế trên toàn EU.

2.1.2. Quy định của Nhật Bản

Luật Bảo vệ thông tin cá nhân Nhật Bản năm 2003 (*Act on the Protection of Personal Information,* APPI)[27] được ban hành nhằm bảo vệ quyền, lợi ích cá nhân và bảo đảm quản lý thông tin cá nhân hiệu quả trong các tổ chức hành chính, cùng với các mục tiêu liên quan khác. Đạo luật này thiết lập các nguyên tắc xử lý thông tin, chính sách cơ bản, trách nhiệm của chính phủ và nghĩa vụ của doanh nghiệp, cùng việc thành lập Ủy ban Bảo vệ thông tin cá nhân trong bối cảnh xã hội số phát triển.[28] Trong đạo luật này, "thông tin cá nhân nhạy cảm"[29] là thông tin cá nhân liên quan đến chủng tộc, tín ngưỡng, địa vị xã hội, lịch sử y tế, hồ sơ phạm tội, việc từng bị thiệt hại bởi một tội phạm, hoặc các yếu tố nhận dạng khác (hoặc tương đương) được quy định bởi Lệnh của Nội các, với yêu cầu đặc biệt phải cẩn trọng để không gây ra sự phân biệt đối xử bất công, thành kiến hoặc các bất lợi khác đối với cá nhân đó.

2.1.3. Quy định của Singapore

Mục đích của Đạo luật Bảo vệ dữ liệu cá nhân năm 2012 (*Personal Data Protection Act 2012*, PDPA)[30] Singapore là điều chỉnh việc thu thập, sử dụng và tiết lộ dữ liệu cá nhân bởi các tổ chức theo cách công nhận cả quyền của cá nhân trong việc bảo vệ dữ liệu cá nhân của họ và nhu cầu của các tổ chức trong việc thu thập, sử dụng hoặc tiết lộ dữ liệu cá nhân cho các mục đích mà một người hợp lý sẽ coi là phù hợp trong hoàn cảnh. Đạo luật này không phân loại dữ liệu cá nhân thành các nhóm khác nhau, bao gồm cả dữ liệu cá nhân nhạy cảm. Theo nguyên tắc, khi xử lý dữ liệu được xem là nhạy cảm, cần phải có sự đồng ý rõ ràng từ chủ thể dữ liệu, nhằm bảo đảm tính minh bạch và quyền riêng tư.[31] Các nhà lập pháp cho rằng việc không thiết lập một danh mục riêng đối với dữ liệu cá nhân nhạy cảm trong khuôn khổ PDPA Singapore xuất phát một phần từ tính chất còn tương đối mới của hệ thống pháp luật này, cũng như định hướng xây dựng các khung pháp lý chuyên ngành để điều chỉnh những loại dữ liệu đặc

26 Khoản 2 Điều 36 Quy định (EU) 2021/2281.

27 Luật Bảo vệ Thông tin Cá nhân Nhật Bản (APPI - *Act on the Protection of Personal Information*) có hiệu lực ngày 1/4/2005. Luật đã được sửa đổi nhiều lần, lần sửa đổi lớn gần đây nhất có hiệu lực vào 1/4/2022 để phù hợp hơn với các tiêu chuẩn quốc tế như GDPR.

28 Điều 1 APPI Nhật Bản.

29 Khoản 3 Điều 2 APPI Nhật Bản.

30 PDPA Singapore năm 2012 được sửa đổi, bổ sung năm 2020.

31 Report On A Model Data Protection Code For The Private Sector, Prepared by The National Internet Advisory Committee Legal Subcommittee, Mục 4.3.6 (Implementation and Operational Guidelines), https://isomer-user-content.by.gov.sg/109/73098a1a-4443-4342-b468-d49a8f9435a8/report-on-a-model-data-protection-code-for-the-private-sector-.pdf, truy cập ngày 8/11/2025.

thù. Theo đó, các lĩnh vực cụ thể như ngân hàng hoặc y tế có thể được điều chỉnh bởi các quy định chuyên biệt, ví dụ như Đạo luật Ngân hàng và các bộ quy tắc hiện hành dành cho các chuyên gia y tế,[32] được xem là các loại dữ liệu nhạy cảm.[33]

2.1.4. Quy định của Việt Nam

Theo quy định tại Luật Bảo vệ dữ liệu cá nhân năm 2025[34] thì dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân, khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp đến quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.[35] Nghị định số 356/2025/NĐ-CP[36] đã liệt kê dữ liệu nhạy cảm gồm: Dữ liệu tiết lộ nguồn gốc chủng tộc, nguồn gốc dân tộc; Quan điểm về chính trị, tôn giáo, tín ngưỡng; Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình; Tình trạng sức khỏe; Dữ liệu sinh trắc học, đặc điểm di truyền; Dữ liệu tiết lộ đời sống tình dục, xu hướng tình dục của cá nhân; Dữ liệu về tội phạm, vi phạm pháp luật được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật; Vị trí của cá nhân được xác định qua dịch vụ định vị; …[37] So với danh mục dữ liệu cá nhân nhạy cảm được quy định tại Nghị định số 13/2023/NĐ-CP thì danh mục dữ liệu cá nhân nhạy cảm được Nghị định số 356/2025/NĐ-CP quy định chi tiết và cụ thể hơn, đặc biệt là đối với các thông tin liên quan đến tài chính, ngân hàng của cá nhân. Ngoài ra, Nghị định này cũng quy định "trong quá trình xử lý dữ liệu cá nhân nhạy cảm, cơ quan tổ chức phải thiết lập quy định phân quyền giới hạn truy cập, quy trình xử lý và các biện pháp bảo mật".[38] Quy định này mở ra các khả năng cho việc xử lý các thông tin liên quan đến sức khỏe của cá nhân một cách riêng biệt.

Theo quy định tại Điều 9 Luật Bảo vệ dữ liệu cá nhân năm 2025 thì chủ thể dữ liệu có quyền được biết về hoạt động xử lý dữ liệu và đồng ý hoặc không đồng ý cho phép xử lý thông tin cá nhân, trừ trường hợp pháp luật quy định khác. Cá nhân được quyền truy cập để xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu nếu có sai sót, và quyền rút lại sự đồng ý khi không muốn tiếp tục cho phép xử lý thông tin của mình. Ngoài ra, chủ thể dữ liệu có quyền xóa hoặc yêu cầu xóa dữ liệu cá nhân nếu không còn cần thiết hoặc vi phạm quy định, cũng như quyền hạn chế xử lý dữ liệu trong một số trường hợp nhất định.

Bên cạnh đó, Luật Dữ liệu năm 2024[39] quy định nguyên tắc trong phát triển, ứng dụng công nghệ trong xử lý, quản trị, quản lý, sử dụng, khai thác dữ liệu là tôn trọng quyền và lợi ích hợp pháp của người khác, không được gây nguy hiểm cho sức khỏe thể chất và tâm lý của người khác, không được xâm phạm quyền và lợi ích của người khác về chân dung, uy tín, danh dự, quyền riêng tư hoặc thông tin cá nhân. Đối với việc công khai dữ liệu, trong quá trình thực hiện chức năng, nhiệm vụ, quyền hạn của mình, người đứng đầu cơ quan nhà nước quyết định việc cung cấp dữ liệu liên quan đến bí mật kinh doanh, đời sống riêng tư, bí mật cá nhân, bí mật gia đình trong trường

32 Singapore Parliament Reports (Hansard) (16 September 2010), Vol, 87, column 1215 (RAdm Lui Tuck Yew, Acting Minister for Information, Communication and the Arts).
33 Report on a Model Data Protection Code for the Private Sector, Mục 4.3.3, *tlđd*.
34 Luật Bảo vệ dữ liệu cá nhân năm 2025 được thông qua vào ngày 26/6/2025 và có hiệu lực từ 1/1/2026.
35 Khoản 3 Điều 2 Luật Bảo vệ dữ liệu cá nhân năm 2025.
36 Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân (Nghị định số 356/2025/NĐ-CP).
37 Khoản 1 Điều 4 Nghị định số 356/2025/NĐ-CP.
38 Khoản 2 Điều 4 Nghị định số 356/2025/NĐ-CP.
39 Luật Dữ liệu năm 2024, được thông qua ngày 30/10/2024, có hiệu lực ngày 01/7/2025.

hợp cần thiết vì lợi ích công cộng, sức khỏe của cộng đồng theo quy định của luật có liên quan mà không cần có sự đồng ý của chủ thể dữ liệu.

Bên cạnh đó, Nghị định số 69/2024/NĐ-CP[40] đã thiết lập nền tảng pháp lý cho định danh và xác thực điện tử, trong đó quy định mọi thông tin danh tính điện tử, bao gồm dữ liệu y tế, phải được lưu trữ vĩnh viễn trong hệ thống định danh.[41] Quy định này bảo đảm tính minh bạch, chính xác và bảo mật khi quản lý thông tin điện tử, đồng thời tạo tiền đề cho việc tích hợp dữ liệu y tế trên quy mô toàn quốc. Ngoài ra, Quyết định số 1332/QĐ-BYT[42] ban hành thí điểm "Sổ sức khỏe điện tử", được tạo lập và ký số bởi các cơ sở khám, chữa bệnh để tích hợp lên ứng dụng VNeID. Quyết định này mở rộng phạm vi áp dụng tại tất cả các cơ sở y tế công lập và tư nhân, cho phép người dân quản lý thông tin sức khỏe cá nhân một cách đồng bộ và tiện lợi. Để triển khai cụ thể, Quyết định số 2733/QĐ-BYT[43] đưa ra hướng dẫn thí điểm việc thực hiện Sổ sức khỏe điện tử VNeID. Hướng dẫn này quy định rõ phạm vi áp dụng cho các cơ sở khám, chữa bệnh được cấp phép và các loại hình dịch vụ y tế, bao gồm khám ngoại trú, nội trú, điều trị ban ngày, kê đơn thuốc và khám chữa bệnh từ xa. Quyết định này bảo đảm rằng các cơ sở y tế có khung hướng dẫn cụ thể để đồng bộ dữ liệu và cung cấp dịch vụ y tế hiện đại. Như vậy, các quy định trên đã tạo nền tảng cho việc chuyển đổi số trong lĩnh vực y tế tại Việt Nam, đồng thời nâng cao hiệu quả quản lý thông tin sức khỏe cá nhân.

2.2. Chế tài xử lý vi phạm dữ liệu cá nhân

GDPR quy định nghiêm ngặt các chế tài để xử lý vi phạm và bảo vệ dữ liệu cá nhân. Theo Điều 32, các bên kiểm soát và xử lý dữ liệu phải áp dụng biện pháp kỹ thuật và tổ chức phù hợp như mã hóa, bút danh hóa, và bảo đảm tính bảo mật, toàn vẹn, khả dụng của hệ thống xử lý, nhằm giảm thiểu rủi ro như mất mát hoặc truy cập trái phép. Điều 83 quy định mức phạt hành chính lên đến 20 triệu EUR hoặc 4% doanh thu toàn cầu đối với vi phạm nghiêm trọng, trong khi các vi phạm khác có thể bị phạt 10 triệu EUR hoặc 2% doanh thu toàn cầu. Khi xác định mức phạt, cần xem xét các yếu tố như tính chất, mức độ, thời gian vi phạm; số lượng chủ thể dữ liệu bị ảnh hưởng; mức độ thiệt hại; tính cố ý hoặc vô ý; các biện pháp giảm thiệt hại; mức độ tuân thủ các biện pháp kỹ thuật, tổ chức (Điều 25 và Điều 32); hợp tác với cơ quan giám sát; vi phạm trước đó; loại dữ liệu bị ảnh hưởng; cách phát hiện vi phạm; sự tuân thủ Điều 58(2); và việc thực hiện Điều 40 hoặc Điều 42. Ngoài ra, lợi ích tài chính thu được hoặc tổn thất tránh được từ vi phạm cũng được cân nhắc. Bên cạnh đó, các quốc gia thành viên phải quy định các chế tài khác áp dụng cho các vi phạm đối với Quy định này, đặc biệt là những vi phạm không thuộc phạm vi áp dụng phạt hành chính theo Điều 83 và phải thực hiện mọi biện pháp cần thiết để bảo đảm các chế tài này được thực thi. Các chế tài đó phải bảo đảm tính hiệu quả, tương xứng và có tính răn đe.

Theo Đạo luật APPI Nhật Bản, các chế tài xử lý vi phạm được quy định nghiêm ngặt nhằm bảo vệ thông tin cá nhân. Cụ thể, Điều 67 quy định nhân viên hoặc cựu nhân viên tiết lộ, sử dụng trái phép thông tin cá nhân có thể bị phạt tù tối đa 2 năm

40 Nghị định số 69/2024/NĐ-CP của Chính phủ về Định danh và xác thực điện tử ngày 25/6/2024 (Nghị định số 69/2024/NĐ-CP).
41 Điều 17 Nghị định số 69/2024/NĐ-CP.
42 Quyết định số 1332/QĐ-BYT của Bộ Y tế về việc ban hành sổ sức khỏe điện tử phục vụ tích hợp trên ứng dụng VNEID ngày 21 tháng 5 năm 2024 (Quyết định số 1332/QĐ-BYT).
43 Quyết định số 2733/QĐ-BYT của Bộ Y tế về ban hành hướng dẫn thí điểm thực hiện sổ sức khỏe điện tử phục vụ tích hợp trên ứng dụng VNEID ngày 17/9/2024 (Quyết định số 2733/QĐ-BYT).

hoặc phạt tiền 1 triệu yen. Điều 84 xử phạt hành vi thu thập thông tin trái phép với mức phạt tù tối đa 1 năm hoặc 500.000 yen. Điều 83 quy định cá nhân sử dụng cơ sở dữ liệu cá nhân để trục lợi có thể bị phạt tù tối đa 1 năm hoặc 500.000 yen, trong khi doanh nghiệp vi phạm bị phạt lên đến 100 triệu yen. Báo cáo sai lệch hoặc cung cấp thông tin không đúng, theo Điều 85, có thể bị phạt tới 500.000 yen, và các vi phạm nhỏ khác bị xử lý dân sự với mức phạt tối đa 100.000 yen.[44] Đối chiếu một vụ điển hình, vụ rò rỉ thông tin y tế nghiêm trọng đã xảy ra tại Bệnh viện Y, khi một y tá đã tiết lộ thông tin bệnh trạng của một người bệnh cho chồng mình. Thông tin này sau đó được người chồng lan truyền, bao gồm cả thông tin về thời gian sống còn lại của người bệnh, gây ra cú sốc tâm lý nặng nề cho mẹ của người bệnh. Vụ việc làm giảm niềm tin của gia đình người bệnh đối với bệnh viện, dẫn đến việc chuyển viện và sau đó người bệnh qua đời. Tòa án tối cao Fukuoka,[45] vào ngày 17/01/2019 kết luận rằng Bệnh viện Y đã không thực hiện đủ trách nhiệm giám sát nhân viên và bảo mật thông tin người bệnh. Tòa án yêu cầu bệnh viện bồi thường 1,1 triệu Yen cho mẹ của người bệnh vì tổn thất tinh thần, đồng thời chỉ trích các biện pháp xử lý nội bộ như cảnh cáo và cắt giảm lương y tá là không đủ để khắc phục hậu quả.

Trong khi đó, Điều 48D PDPA Singapore quy định rằng bất kỳ cá nhân nào tiết lộ hoặc gây ra việc tiết lộ dữ liệu cá nhân thuộc sở hữu hoặc quyền kiểm soát của tổ chức hoặc cơ quan công quyền mà không được phép, với ý thức biết rõ hoặc hành vi cẩu thả, sẽ bị coi là phạm tội. Hình phạt có thể là phạt tiền lên đến 5.000 đô la Singapore, hoặc phạt tù tối đa 2 năm, hoặc cả hai. Tuy nhiên, nếu người vi phạm có thể chứng minh rằng dữ liệu đã công khai hợp pháp, việc tiết lộ được pháp luật hoặc lệnh Tòa án cho phép, hoặc họ có lý do hợp lý tin rằng họ có quyền tiết lộ thì không được xem là vi phạm quy định tại Điều 17 nhưng phải trên cơ sở tuân thủ nghiêm ngặt các điều kiện kèm theo, bảo đảm rằng việc tiết lộ dữ liệu chỉ diễn ra trong phạm vi cần thiết và phù hợp với mục đích được quy định tại Phụ lục 1 và Phụ lục 2 PDPA Singapore. Quy định này không ảnh hưởng đến các nghĩa vụ khác theo luật pháp liên quan, và "vi phạm áp dụng" bao gồm các vi phạm cụ thể khác trong PDPA Singapore và các luật liên quan. Hơn nữa, cá nhân truy cập, chỉnh sửa hoặc chuyển dữ liệu của người khác mà không có sự cho phép có thể bị phạt tiền đến 5.000 đô la Singapore, phạt tù tối đa 12 tháng, hoặc cả hai. Tổ chức vi phạm có thể bị phạt đến 50.000 đô la Singapore hoặc 100.000 đô la Singapore cho vi phạm nghiêm trọng hơn. Điều 56 quy định mức phạt chung cho vi phạm không có hình phạt cụ thể, gồm phạt tiền tối đa 10.000 đô la Singapore, phạt tù tối đa 3 năm, hoặc cả hai, cùng mức phạt bổ sung 1.000 đô la Singapore mỗi ngày nếu vi phạm tiếp tục.[46]

Chẳng hạn, vào tháng 6/2018, một cuộc tấn công mạng đã xâm nhập hệ thống dữ liệu y tế của SingHealth,[47] làm lộ thông tin cá nhân của 1,5 triệu người bệnh, bao gồm Thủ tướng Lý Hiển Long. Đây được xem là vụ vi phạm dữ liệu lớn nhất trong lịch sử Singapore. Căn cứ vào quy định của PDPA Singapore, các tổ chức vi phạm phải chịu trách nhiệm với dữ liệu mà họ thu thập và quản lý, ngay cả khi đã ủy thác

44 Điều 176-185, Chương VIII, APPI Nhật Bản.

45 Bản án của Tòa án tối cao Fukuoka, số hiệu H24.1.17, https://fukuzaki-law.jp/iryouhoumu/65/, truy cập ngày 8/11/2025.

46 Điều 51 và Điều 56 PDPA Singapore.

47 Personal Data Protection Commission, "PDPC Imposes Financial Penalty on Both IHIS and SingHealth", 2019, https://www.pdpc.gov.sg/news-and-events/press-room/2019/01/pdpc-imposes-financial-penalty-on-both-ihis-and-singhealth, truy cập ngày 8/11/2025.

cho bên thứ ba. SingHealth, với vai trò là chủ sở hữu hệ thống dữ liệu người bệnh, bị phạt 250.000 SGD, trong khi Hệ thống Thông tin Y tế Tích hợp (*Integrated Health Information Systems*, IHiS), đơn vị phụ trách công nghệ cho lĩnh vực y tế, chịu mức phạt cao nhất từ trước đến nay là 750.000 SGD.

So với các quốc gia khác thì Nghị định số 356/2025/NĐ-CP về bảo vệ dữ liệu cá nhân đóng vai trò quan trọng trong việc thiết lập các nguyên tắc và quy định cụ thể về thu thập, xử lý, và bảo vệ dữ liệu cá nhân, đặc biệt là dữ liệu cá nhân nhạy cảm. Tuy nhiên, Nghị định chỉ tập trung vào việc định nghĩa các nguyên tắc và hành vi vi phạm mà không quy định chi tiết về các hình thức xử phạt đối với vi phạm trong lĩnh vực này. Hiện nay, các chế tài xử phạt chủ yếu được áp dụng dựa trên Nghị định số 15/2020/NĐ-CP (sửa đổi bởi Nghị định số 14/2022/NĐ-CP) và Nghị định số 356/2025/NĐ-CP vốn mang tính chất chung, áp dụng cho nhiều lĩnh vực khác nhau, đồng thời các vấn đề xử lý hành vi vi phạm được quy định ở nhiều văn bản khác nhau dẫn đến hiện tượng chồng chéo các quy định, gây khó khăn trong quá trình áp dụng trên thực tế. Do đó, dự thảo Nghị định quy định vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân (Dự thảo 2026)[48] được đề xuất nhằm hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân, bổ sung các quy định xử phạt chi tiết, rõ ràng và trực tiếp hơn, giải quyết được bất cập nêu trên. Theo đó, các hành vi vi phạm nguyên tắc bảo vệ dữ liệu cá nhân, như xử lý, thu thập, lưu trữ hoặc bảo mật dữ liệu không đúng quy định, có thể bị phạt tiền từ 50 - 70 triệu đồng. Trường hợp vi phạm nghiêm trọng hơn, như mua bán, chiếm đoạt, cố ý làm lộ, làm mất dữ liệu cá nhân, mức phạt có thể lên đến từ 70 - 100 triệu đồng. Ngoài ra, cá nhân, tổ chức vi phạm còn có thể bị áp dụng các hình thức xử phạt bổ sung như tịch thu tang vật, phương tiện vi phạm hoặc đình chỉ hoạt động xử lý dữ liệu cá nhân có thời hạn, đồng thời phải thực hiện các biện pháp khắc phục hậu quả như buộc xóa dữ liệu, hoàn trả hoặc buộc nộp lại số lợi bất hợp pháp có được do thực hiện hành vi vi phạm hoặc công khai xin lỗi chủ thể dữ liệu (Điều 57).

Đối với các hành vi vi phạm quyền của chủ thể dữ liệu, mức phạt dao động từ 25 -100 triệu đồng, tùy theo tính chất và mức độ vi phạm (Điều 58, 59, 60, 61, 62). Các hành vi vi phạm bao gồm việc không bảo đảm thực hiện các quyền của chủ thể dữ liệu, không phản hồi hoặc không thực hiện yêu cầu của chủ thể dữ liệu về sự đồng ý, rút lại sự đồng ý, chỉnh sửa, và lưu trữ, xóa, hủy dữ liệu cá nhân. Ngoài hình thức phạt tiền, tổ chức, cá nhân vi phạm còn có thể bị áp dụng các hình thức xử phạt bổ sung như tước quyền sử dụng giấy phép hoạt động có liên quan, tịch thu tang vật, phương tiện vi phạm hoặc đình chỉ hoạt động xử lý dữ liệu cá nhân có thời hạn. Đồng thời, các biện pháp khắc phục hậu quả cũng được áp dụng, bao gồm buộc hủy, xóa dữ liệu cá nhân đến mức không thể khôi phục, buộc hoàn trả hoặc nộp lại số lợi bất hợp pháp và công khai xin lỗi chủ thể dữ liệu trên các phương tiện thông tin đại chúng.

Ngoài ra, đối với chế tài hình sự, Điều 288 Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung 2017) quy định các chế tài nghiêm khắc đối với hành vi đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông. Người vi phạm có thể bị phạt tiền từ 30 triệu đến 1 tỷ đồng, phạt cải tạo không giam giữ đến 3 năm, hoặc phạt tù từ 6 tháng đến 7 năm, tùy vào mức độ vi phạm và hậu quả gây ra. Hành vi vi phạm bao

48 Dự thảo 2026, https://bocongan.gov.vn/chinh-sach-phap-luat/lay-y-kien-du-thao/ho-so-du-thao-nghi-dinh-quy-dinh-xu-phat-vi-pham-hanh-chinh-trong-linh-vuc-an-ninh-mang-va-bao-ve-du-lieu-ca-nhan-1772531021?type=dang-lay-y-kien, truy cập ngày 22/04/2026.

gồm đưa thông tin trái pháp luật, mua bán, công khai dữ liệu cá nhân trái phép, hoặc gây thiệt hại nghiêm trọng. Bên cạnh đó, người phạm tội còn có thể bị phạt bổ sung như cấm đảm nhiệm chức vụ hoặc hành nghề từ 1 đến 5 năm. Quy định này nhằm bảo vệ quyền riêng tư, dữ liệu cá nhân và an ninh mạng một cách chặt chẽ.

3. Kiến nghị hoàn thiện quy định pháp luật

3.1. Kiến nghị hoàn thiện quy định về cơ sở dữ liệu y tế

Học tập mô hình EHDS, Việt Nam cần bổ sung, hoàn thiện quy định pháp luật theo hướng xây dựng một hệ thống cơ sở dữ liệu y tế tích hợp toàn quốc, cho phép thông tin y tế cá nhân được truy cập và sử dụng linh hoạt giữa các địa phương trên toàn quốc, gồm cả cơ sở y tế công và tư nhân. Điều này không chỉ nâng cao hiệu quả chăm sóc sức khỏe mà còn cải thiện khả năng ứng phó với các tình huống khẩn cấp, đồng thời hỗ trợ tối ưu hóa quy trình chăm sóc sức khỏe.

Việc mở rộng và nâng cấp nền tảng quản lý thông tin y tế cơ sở (V20) theo Quyết định 198/QĐ-BYT tích hợp chặt chẽ với Sổ sức khỏe điện tử VNeID được quy định tại Quyết định số 2733/QĐ-BYT, Quyết định số 1332/QĐ-BYT và Nghị định số 69/2024/NĐ-CP sẽ góp phần đồng bộ hóa dữ liệu y tế, hiện đại hóa quản lý thông tin và thúc đẩy chuyển đổi số trong lĩnh vực y tế. Hệ thống này sẽ đồng bộ hóa dữ liệu quan trọng như bệnh án điện tử, lịch sử tiêm chủng, kê đơn thuốc và các kết quả xét nghiệm, giúp thông tin y tế của người bệnh có thể được truy cập bởi bất kỳ các cơ sở y tế công và tư nhân nào khi cần thiết. Đây là bước tiến quan trọng nhằm bảo đảm tính liên thông và liền mạch trong chăm sóc sức khỏe.

Tuy nhiên, việc lưu trữ vĩnh viễn mọi thông tin danh tính điện tử, bao gồm dữ liệu y tế theo Điều 17 Nghị định số 69/2024/NĐ-CP nhằm bảo đảm tính liên tục và khả năng truy xuất, có thể gây mâu thuẫn với Nghị định số 356/2025/NĐ-CP, vốn quy định quyền cá nhân được yêu cầu xóa dữ liệu không cần thiết hoặc khi rút lại sự đồng ý. Điều này đặt ra thách thức pháp lý trong việc cân bằng giữa quản lý dữ liệu dài hạn vì lợi ích công và quyền kiểm soát dữ liệu cá nhân của chủ thể dữ liệu. Để giải quyết điểm bất cập này, cần học hỏi mô hình EHDS của EU, bằng cách phân loại rõ ràng dữ liệu bắt buộc lưu trữ lâu dài vì mục đích an ninh quốc gia hoặc lợi ích công cộng, trong khi cho phép xóa dữ liệu khác theo yêu cầu cá nhân. Sự đồng bộ và minh bạch trong các quy định sẽ không chỉ bảo đảm hiệu quả quản lý nhà nước mà còn bảo vệ quyền lợi chính đáng của người dân. Đồng thời, việc triển khai hệ thống y tế số hóa toàn diện sẽ nâng cao chất lượng dịch vụ y tế, bảo đảm mọi người dân, dù ở bất kỳ đâu, đều được tiếp cận dịch vụ y tế một cách công bằng và hiệu quả, thúc đẩy mạnh mẽ tiến trình chuyển đổi số quốc gia trong lĩnh vực y tế.

3.2. Đề xuất hoàn thiện hệ thống chế tài xử lý vi phạm

Hiện nay, các chế tài nhằm bảo vệ quyền riêng tư trong chăm sóc sức khỏe chưa phát huy được vai trò và chưa mang lại được hiệu quả.[49] Bên cạnh Nghị định số 356/2025/NĐ-CP, và Luật Dữ liệu năm 2024, thì Dự thảo 2026 đối với các chế tài xử lý vi phạm liên quan đến dữ liệu cá nhân nhạy cảm đã bước đầu được quy định rõ. Tuy nhiên, để bảo đảm hiệu quả hơn trong việc bảo vệ dữ liệu cá nhân, đặc biệt là bảo

49 Nguyen Ho Bich Hang, "Addressing fragmentation in Vietnam's Data Protection Laws: Recommendations for a unified legal framework", *Vietnamese Journal of Legal Sciences*, Vol. 11(2), 2024, tr. 24, DOI: https://doi.org/10.2478/vjls-2024-0008

đảm việc bảo vệ quyền riêng tư trong chăm sóc sức khỏe một cách có hiệu quả, các tác giả kiến nghị như sau:

a) Chế tài hành chính, hình sự

Đối với quy định tại Điều 59 về vi phạm quy định về sự đồng ý của chủ thể dữ liệu, tác giả đề xuất bổ sung khoản 2 Điều 59 Dự thảo 2026:

d) Không thông báo hoặc không thể hiện rõ cho chủ thể dữ liệu về việc xử lý dữ liệu cá nhân nhạy cảm, bao gồm mục đích, phạm vi và rủi ro liên quan.

Tương tự, đối với hành vi không chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân nhạy cảm (khoản 2 Điều 69 Dự thảo 2026), các tác giả đề xuất sửa đổi như sau:

2. Phạt tiền từ 70.000.000 đồng đến 90.000.000 đồng đối với hành vi không chỉ định hoặc không duy trì bộ phận có chức năng bảo vệ dữ liệu cá nhân nhạy cảm; không chỉ định hoặc không bảo đảm yêu cầu về chuyên môn đối với nhân sự phụ trách bảo vệ dữ liệu cá nhân nhạy cảm; hoặc không thực hiện việc cung cấp, cập nhật hoặc trao đổi thông tin về bộ phận và nhân sự phụ trách bảo vệ dữ liệu cá nhân nhạy cảm với Cơ quan chuyên trách bảo vệ dữ liệu cá nhân theo quy định.

Ngoài ra, đối với hành vi vi phạm quy định về thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân (Điều 66 Dự thảo 2026), nhóm tác giả nhận thấy các quy định hiện hành mới dừng ở việc xử lý các vi phạm mang tính thủ tục, chưa phân hóa rõ mức độ vi phạm, đặc biệt chưa có chế tài đủ mạnh đối với hành vi cố ý không thông báo hoặc che giấu vi phạm. Do đó, nhóm tác giả đề xuất bổ sung quy định như sau:

2. Phạt tiền từ 200.000.000 đồng đến 500.000.000 đồng đối với một trong các hành vi sau đây:

a) Cố ý không thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân nhằm che giấu vi phạm

b) Cố ý cung cấp thông tin sai lệch, không trung thực về sự cố vi phạm dữ liệu cá nhân

c) Cố ý trì hoãn việc phát hiện, báo cáo hoặc xử lý vi phạm nhằm giảm nhẹ trách nhiệm hoặc tránh sự kiểm tra của cơ quan có thẩm quyền.

Đối với các vụ việc rò rỉ thông tin nghiêm trọng, đặc biệt là việc mua bán và trao đổi trái phép dữ liệu cá nhân nhạy cảm với quy mô lên đến hàng triệu người, mức phạt cần mang tính răn đe cao hơn. Theo quy định tại khoản 5 Điều 83 GDPR, mức phạt có thể lên đến 20 triệu euro hoặc 4% tổng doanh thu toàn cầu của doanh nghiệp, tùy theo mức nào cao hơn. Điều này phản ánh sự cần thiết trong việc áp dụng chế tài tương xứng với mức độ vi phạm nhằm bảo vệ quyền lợi của chủ thể dữ liệu và bảo đảm tính nghiêm minh của pháp luật. Ngoài hình phạt chính, các tổ chức vi phạm còn phải thực hiện các biện pháp khắc phục hậu quả như công khai xin lỗi, cải thiện hệ thống bảo mật, hoặc đình chỉ hoạt động thu thập và xử lý dữ liệu trong thời gian nhất định.

Hơn nữa, Điều 56 PDPA của Singapore quy định cơ chế xử phạt chung cho các vi phạm không có hình phạt cụ thể, bao gồm mức phạt tiền tối đa 10.000 SGD, phạt tù tối đa 3 năm, hoặc áp dụng cả hai hình thức. Quy định này nổi bật với việc áp dụng mức phạt bổ sung 1.000 SGD mỗi ngày nếu vi phạm tiếp tục kéo dài, tạo áp lực kinh tế buộc cá nhân, tổ chức nhanh chóng khắc phục sai phạm. Cơ chế này không chỉ răn đe mà còn ngăn chặn hiệu quả các hành vi kéo dài, như việc không tuân thủ yêu cầu xóa dữ liệu cá nhân hay xử lý dữ liệu trái phép. Kinh nghiệm này là bài học quý báu cho Việt Nam trong việc xây dựng chế tài xử lý vi phạm dữ liệu cá nhân. Việc áp dụng mức phạt bổ sung theo ngày có thể khuyến khích các cá nhân, tổ chức nhanh chóng tuân thủ, đồng thời tăng cường bảo vệ quyền lợi cá nhân và nâng cao hiệu quả quản lý dữ

liệu. Do đó, việc áp dụng mức hình phạt tiền bổ sung theo từng ngày sẽ là cơ sở để cơ quan có thẩm quyền dễ dàng kích hoạt cơ chế xử phạt chung cho các vi phạm không có hình phạt cụ thể hoặc buộc tổ chức vi phạm nhanh chóng chấm dứt hành vi vi phạm.

b) Chế tài dân sự

Cần bổ sung, hoàn thiện quy định pháp luật về chế tài dân sự trong trường hợp vi phạm bảo vệ dữ liệu cá nhân theo hướng tăng cường khả năng tự bảo vệ của chủ thể dữ liệu. Cụ thể, cần quy định rõ quyền của chủ thể dữ liệu trong việc yêu cầu bồi thường thiệt hại, bao gồm cả thiệt hại vật chất và thiệt hại tinh thần phát sinh từ hành vi xâm phạm dữ liệu cá nhân. Đồng thời, cần làm rõ cơ chế xác định thiệt hại tinh thần trong các trường hợp vi phạm ảnh hưởng đến danh dự, uy tín, đời sống riêng tư của cá nhân, bảo đảm việc bồi thường được thực hiện toàn bộ và kịp thời.

Bên cạnh đó, cần bổ sung quy định về nghĩa vụ chứng minh và phân bổ gánh nặng chứng minh nhằm bảo vệ tốt hơn quyền lợi của chủ thể dữ liệu trong các tranh chấp dân sự liên quan đến dữ liệu cá nhân, trên cơ sở các quy định hiện hành về mối quan hệ nhân quả giữa thiệt hại xảy ra và hành vi xâm phạm[50].

Các quy định về trách nhiệm liên đới giữa các bên tham gia thu thập, xử lý, và lưu trữ dữ liệu cá nhân cũng cần được bổ sung, đồng thời việc miễn trừ nghĩa vụ chỉ áp dụng khi các bên chứng minh đã thực hiện đầy đủ trách nhiệm bảo vệ dữ liệu.

Mức bồi thường cụ thể cần được chi tiết hóa hơn đối với thiệt hại tinh thần trong trường hợp các bên không có thỏa thuận. Theo đó, nhóm tác giả đề xuất mức bồi thường tối đa đối với chủ thể dữ liệu và người thân thích khi bị xâm phạm không quá ba mươi lần mức lương cơ sở do Nhà nước quy định. Trên cơ sở đó, có thể phân cấp bồi thường thiệt hại về tinh thần thành ba mức độ tương ứng với mức độ tổn thất do hành vi xâm phạm dữ liệu cá nhân nhạy cảm gây ra, gồm: (i) Thiệt hại về tinh thần ở mức độ chung, thể hiện sự khó chịu nghiêm trọng về tâm lý đối với chủ thể dữ liệu, với mức bồi thường tối đa không quá mười lần mức lương cơ sở; (ii) Thiệt hại về tinh thần nghiêm trọng, thể hiện ở những ảnh hưởng đáng kể đến đời sống hàng ngày và trạng thái làm việc, tình trạng suy nhược tinh thần hoặc rối loạn tâm thần của chủ thể dữ liệu, với mức bồi thường tối đa không quá hai mươi lần mức lương cơ sở; (iii) Thiệt hại về tinh thần đặc biệt nghiêm trọng, thể hiện ở trạng thái suy sụp tột độ, hành vi tự gây hại hoặc tự sát của người bị xâm phạm, với mức bồi thường tối đa không quá ba mươi lần mức lương cơ sở. [51]

Kết luận

Việt Nam là một quốc gia đang phát triển, đã có những bước tiến đáng kể trong việc bảo vệ dữ liệu cá nhân, điển hình là qua Nghị định số 356/2025/NĐ-CP chịu ảnh hưởng lớn từ GDPR của EU. Tuy nhiên, vẫn còn thiếu các quy định chuyên biệt để bảo vệ dữ liệu y tế, vốn là những dữ liệu cá nhân nhạy cảm cần sự bảo vệ nghiêm ngặt để ngăn ngừa rủi ro xâm phạm quyền riêng tư của người bệnh. Do đó, việc bổ sung các quy định này vào Luật KCB năm 2023, Luật Bảo hiểm Y tế, Nghị định số 69/2024/NĐ-CP, Luật Dữ liệu năm 2024 và các văn bản pháp luật liên quan là cần thiết. Trong

50 Khoản 1 Điều 2 Nghị quyết số 02/2022/NQ-HĐTP ngày 6/9/2022 của Hội đồng thẩm phán Tòa án nhân dân tối cao Hướng dẫn áp dụng một số quy định của Bộ luật Dân sự về trách nhiệm bồi thường thiệt hại ngoài hợp đồng.

51 Trần Ngọc Tuấn, *Quyền về đời sống riêng tư của cá nhân theo quy định pháp luật dân sự Việt Nam*, Luận án tiến sĩ Luật học, Trường Đại học Luật Thành phố Hồ Chí Minh, 2024, tr. 167.

đó cần ghi nhận các tiêu chuẩn bảo mật như mã hóa dữ liệu, hạn chế quyền truy cập, việc lưu trữ, xử lý dữ liệu cá nhân nhạy cảm và xác định rõ trách nhiệm của các cơ sở y tế. Việc hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân và dữ liệu y tế không chỉ nâng cao mức độ bảo vệ quyền riêng tư mà còn giúp Việt Nam hội nhập với các tiêu chuẩn bảo vệ dữ liệu quốc tế, đồng thời gia tăng uy tín của các tổ chức y tế Việt Nam. ●

Tài liệu tham khảo

[1] *ECHR I v. Finland*, No. 20511/03, 2008

[2] Adebayo Yusuf Balogun, "Strengthening compliance with data privacy regulations in US healthcare cybersecurity", *Asian Journal of Research in Computer Science*, Vol. 18(1), 2025, tr. 154-173, DOI: https://doi.org/10.9734/ajrcos/2025/v18i1555

[3] Cyber Peace Institute, "Vastaamo data breach - Attack on human security, dignity and equity", *Cyber Peace Institute*, 2020

[4] Tăng Thị Bích Diễm, "Trách nhiệm dân sự trong xử lý dữ liệu cá nhân theo Điều 82 Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu – Kinh nghiệm cho Việt Nam", *Tạp chí Khoa học pháp lý Việt Nam,* số 05 (189), 2025, [trans: Tang Thi Bich Diem, "Civil liability in the processing of personal data under Article 82 of the European Union's General Data Protection Regulation – Lessons for Vietnam", *Vietnam Journal of Legal Science*, No. 05 (189), 2025], DOI: https://doi.org/10.70236/tckhplvn.261

[5] Phạm Thị Anh Đào, Đặng Ngọc Huyền Vy, "Quyền bảo mật thông tin của người nhiễm HIV/AIDS ở Việt Nam hiện nay", *Tạp Chí Khoa học Kiểm sát*, 7(91), 2025, tr. 56. DOI: https://doi.org/10.59554/tckhks.v7i91.588 [trans: Pham Thi Anh Dao, Dang Ngoc Huyen Vy, "The right to confidentiality of people living with HIV/AIDS in Vietnam nowadays", *Journal of Prosecutorial Science*, Vol. 7(91), 2025]

[6] Trọng Đạt, "Bệnh viện có thể tê liệt vì hacker mã hoá dữ liệu tống tiền", *Báo VietNamNet*, 2024 [trans: Trong Dat, "A hospital could be paralyzed by hackers encrypting its data for ransom", *VietNamNet Newspaper*, 2024]

[7] David Fåhraeus, Jane Reichel, Santa Slokenberg, "The European Health Data Space: Challenges and Opportunities", *Swedish Institute for European Policy Studies*, 2024

[8] Nguyen Ho Bich Hang, "Addressing fragmentation in Vietnam's Data Protection Laws: Recommendations for a unified legal framework", *Vietnamese Journal of Legal Sciences*, Vol. 11(2), 2024, DOI: https://doi.org/10.2478/vjls-2024-0008

[9] Nguyễn Hồ Bích Hằng, "Bình luận về những quy định liên quan đến dữ liệu cá nhân theo quy định của pháp luật Việt Nam", *Tạp chí Khoa học Pháp lý Việt Nam*, số 08 (180), 2024 [trans: Nguyen Ho Bich Hang, "Commentary on provisions related to personal data according to Vietnamese law" *Vietnam Journal of Legal Science*, No. 08 (180), 2024]

[10] Mannas Mishra & Zeba Siddiqui, "United Health says hackers possibly stole large number of Americans' data", *Reuters*, 20

[11] Lois N. Magner & Oliver Kim, *A history of medicine*, CRC press, 2017, DOI: https://doi.org/10.1201/9781315113814

[12] Singapore Parliament Reports (Hansard) (16 September 2010) vol 87 1215 (RAdm Lui Tuck Yew, Acting Minister for Information, Communication and the Arts)

[13] Suchit Leesa-Nguansuk, "Claim on huge data leak", *Bangkok Post PCL.*, 2022

[14] Trần Ngọc Tuấn, *Quyền về đời sống riêng tư của cá nhân theo quy định pháp luật dân sự Việt Nam*, Luận án tiến sĩ Luật học, Trường Đại học Luật Thành phố Hồ Chí Minh, 2024 [trans: Tran Ngoc Tuan, *The right to private life according to the provisions of Vietnamese Civil Law*, Doctoral dissertation in Law, Ho Chi Minh City University of Law, 2024]

[15] Trần Ngọc Tuấn, "Bảo vệ quyền riêng tư của bệnh nhân đối với hình ảnh y tế thông qua công nghệ blockchain", *Tạp chí Khoa học xã hội Việt Nam*, số 11, 2022 [trans: Tran Ngoc Tuan, "Protecting patient privacy regarding medical images through blockchain technology", *Vietnam Journal of Social Sciences*, No. 11, 2022]