# BẢO VỆ DỮ LIỆU CÁ NHÂN NHẠY CẢM THEO QUY ĐỊNH CHUNG VỀ BẢO VỆ DỮ LIỆU CỦA LIÊN MINH CHÂU ÂU (GDPR) VÀ GIÁ TRỊ THAM KHẢO CHO VIỆT NAM

***Đào Kim Anh****

**Tóm tắt:** *Bài viết phân tích quy định về dữ liệu cá nhân nhạy cảm theo Quy định chung của Liên minh châu Âu (GDPR) và so sánh với các quy định trong Nghị định số 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân của Việt Nam. Bài viết chỉ rằng, mặc dù Nghị định số 13/2023/NĐ-CP đã bước đầu ghi nhận sự cần thiết phải bảo vệ đặc biệt đối với dữ liệu cá nhân nhạy cảm nhưng các quy định hiện nay còn mang tính hình thức và thiếu hiệu quả, chưa có sự phân biệt rõ ràng về thu thập và xử lý dữ liệu cá nhân nhạy cảm so với các dữ liệu cá nhân thông thường. Trên cơ sở phân tích các quy định của GDPR, bài viết đưa ra một số khuyến nghị hoàn thiện các quy định pháp luật về bảo vệ dữ liệu cá nhân nhạy cảm, đặc biệt trong bối cảnh Việt Nam đang xây dựng Luật Bảo vệ dữ liệu cá nhân.*

**Abstract:** *The article analyzes the provisions on sensitive personal data under the European Union's General Data Protection Regulation (GDPR) and compares them with the provisions in Vietnam's Decree No. 13/2023/ND-CP. It argues that although Decree 13 has initially acknowledged the necessity of special protection for sensitive personal data, the current provisions are still formalistic and ineffective, lacking a clear distinction between the collection and processing of sensitive personal data and other personal data. Based on the analysis of GDPR provisions, the article offers several recommendations for improving the legal regulations on the protection of sensitive personal data, especially in the context of Vietnam's efforts to develop a Personal Data Protection Law.*

## 1. Đặt vấn đề

Với sự phát triển nhanh chóng của khoa học công nghệ trong thời đại hiện nay, dữ liệu cá nhân được coi là nguồn tài nguyên quốc gia cần được bảo vệ[1]. Trong dữ liệu cá nhân, có những dữ liệu rất nhạy cảm, gắn liền với quyền riêng tư và các quyền cơ bản của cá nhân mà việc xâm phạm có thể gây ra những hậu quả nghiêm trọng, thậm chí không thể khắc phục[2]. Ví dụ về các dữ liệu này có thể kể tới dữ liệu về sinh trắc học, dữ liệu về đời sống tình dục, dữ liệu về sức khỏe và đời tư của cá nhân… Vì tính chất đặc thù này mà các dữ liệu nhạy cảm đang trở thành mục tiêu tấn công hấp dẫn của các nhóm tội phạm công nghệ cao. Ví dụ, vào năm 2019, vụ rò rỉ dữ liệu về sinh trắc học quy mô lớn, bao gồm hơn 27 triệu dữ liệu nhận diện khuôn mặt và vân tay trên hệ thống Biostar 2 gây ảnh hưởng nghiêm trọng tới hàng nghìn tổ chức và cá nhân,

* TS., Giảng viên, Khoa Luật, trường Đại học Ngoại thương.

[1] Trần Thị Thu Phương, *Quy định chung của Liên minh châu Âu về bảo vệ dữ liệu cá nhân và một số khuyến nghị đến Quốc hội, Chính phủ và doanh nghiệp Việt Nam*, Tạp chí Nghiên cứu lập pháp, số 23 (447), năm 2021, tr.42.

[2] Paul Quinn và Gianclaudio Malgieri, *The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework*, German Law Journal, Vol 22, Issue 8, December 2021, p.1584.

trong đó có cả Cảnh sát hoàng gia London[3]. Vào năm 2023, dữ liệu của hơn 815 triệu người Ấn Độ bị rao bán bởi tin tặc, trong đó có cả các thông tin bản sao dấu vân tay của người dân làm dấy lên nhiều lo ngại, gây mất niềm tin đối với việc cung cấp dữ liệu sinh trắc học và nhận dạng cá nhân của người dân đối với các cơ quan chức năng[4].

Tại Việt Nam, một báo cáo gần đây của Bộ Công an cũng chỉ ra rằng hoạt động mua bán dữ liệu cá nhân, dữ liệu nhạy cảm đang diễn ra ngày càng phổ biến, diễn biến phức tạp với hình thức thủ đoạn tinh vi[5]. Chính vì vậy, vấn đề bảo vệ dữ liệu nhạy cảm đang đặt ra những thách thức lớn đối với các quốc gia, trong đó có Việt Nam. Những dữ liệu cá nhân nào được coi là nhạy cảm và cần có quy định gì để bảo vệ các dữ liệu này là những nội dung quan trọng, không thể thiếu trong xây dựng và hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân.

Để trả lời các câu hỏi này, bài viết tập trung phân tích các quy định về dữ liệu cá nhân nhạy cảm theo Quy định chung của Liên minh Châu Âu (General Data Protection Regulation – GDPR)[6] và so sánh với các quy định trong Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân (Nghị định 13) của Việt Nam. Thông qua những phân tích này, bài viết chỉ rằng, mặc dù Nghị định 13 đã bước đầu ghi nhận sự cần thiết phải bảo vệ pháp lý đặc biệt đối với các dữ liệu cá nhân nhạy cảm, các quy định hiện nay còn nhiều điểm chưa rõ ràng và thiếu hiệu quả, chưa có sự phân biệt rõ ràng về thu thập và xử lý dữ liệu cá nhân nhạy cảm so với các dữ liệu cá nhân thông thường. Các quy định này cần được tiếp tục xem xét và hoàn thiện, đặc biệt trong quá trình soạn thảo và ban hành Luật Bảo vệ dữ liệu cá nhân, nhằm tăng cường cơ chế bảo vệ hiệu quả đối với các dữ liệu cá nhân nhạy cảm. Trên cơ sở phân tích các quy định của GDPR, bài viết cũng đưa ra một số khuyến nghị nhằm hoàn thiện các quy định về bảo vệ dữ liệu cá nhân nhạy cảm trong pháp luật Việt Nam.

## 2. Sự cần thiết của cơ chế bảo vệ đặc biệt dành cho dữ liệu cá nhân nhạy cảm

Trong các dữ liệu cá nhân, tồn tại một số loại dữ liệu nhạy cảm mà do tính chất đặc thù mà việc xử lý có thể gây ra những rủi ro đáng kể đối với các quyền và tự do cơ bản của con người, ví dụ như dữ liệu về chủng tộc, nguồn gốc dân tộc, quan điểm tôn giáo, dữ liệu về sức khỏe, di truyền, sinh trắc vân tay, dữ liệu về đời sống tình dục… So với các dữ liệu cá nhân thông thường, việc lạm dụng những dữ liệu này có thể gây hậu quả nghiêm trọng hơn đối với các quyền cơ bản của con người, như quyền riêng tư và quyền không bị phân biệt đối xử[7].

Ở quy mô lớn hơn, lịch sử loài người đã cho thấy rằng, việc lạm dụng dữ liệu nhạy cảm (ví dụ dữ liệu về chủng tộc hoặc tôn giáo) có thể tạo điều kiện cho các vi phạm

[3] The Guardian, *Major breach found in biometrics system used by banks, UK police and defence firms,* https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms, công bố ngày 14/08/2019, truy cập ngày 20/5/2024.

[4] The Indian Express, *ICMR data leak: Four held, claim to have stolen FBI, Pak's CNIC info too*, https://indianexpress.com/article/india/icmr-data-leak-four-held-claim-to-have-stolen-fbi-paks-cnic-info-too-9072200/, công bố ngày 18/12/2023, truy cập ngày 22/5/2024.

[5] Bộ Công an, *Dự thảo Báo cáo đánh giá tác động của chính sách trong đề nghị xây dựng Luật Bảo vệ dữ liệu cá nhân*, https://bocongan.gov.vn/giao-duc-pho-bien-phap-luat/van-ban/Pages/du-thao.aspx?ItemID=430#parentHorizontalTab4, công bố ngày 1/3/2024 , truy cập ngày 19/5/2024.

[6] *General Data Protection Regulation*, https://gdpr-info.eu/, truy cập ngày 11/4/2024.

[7] Christopher Kuner (chủ biên), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 369.

nhân quyền nghiêm trọng. Seltzer và Anderson thông qua một cuộc xem xét sơ bộ về lịch sử các cuộc diệt chủng và cưỡng bức di cư trong hai thế kỷ qua đã chỉ ra một số trường hợp rõ ràng là hậu quả của việc lạm dụng dữ liệu cá nhân về chủng tộc hoặc tôn giáo[8]. Những trường hợp này bao gồm cuộc diệt chủng người Do thái do chế độ Đức Quốc xã thực hiện trong Thế chiến II; việc giam giữ người Mỹ gốc Nhật trong cùng thời kỳ; việc di dời cưỡng bức người Mỹ bản địa khỏi đất đai lãnh thổ của họ ở Hoa Kỳ vào thế kỷ XIX, hay cuộc diệt chủng Rwanda nhắm tới nhóm sắc tộc Tutsi năm 1994[9].

Ngoài ra, một số dữ liệu nhạy cảm (ví dụ: Một số loại dữ liệu sinh trắc học) tạo ra sự thay đổi không thể đảo ngược trong mối quan hệ giữa cơ thể và danh tính vì chúng biến các đặc điểm cơ thể con người trở thành dữ liệu có thể đọc được bởi máy móc (machinerable) và có thể sử dụng mãi mãi[10]. Vì vậy, trong thời đại công nghệ số, khi dữ liệu nhạy cảm trở nên dễ bị tổn thương hơn bao giờ hết thì sự bảo vệ đặc biệt đối với nhóm dữ liệu này là hết sức cần thiết.

Mặt khác, việc xử lý dữ liệu nhạy cảm cũng có thể mang lại những lợi ích vô cùng to lớn. Một ví dụ điển hình là việc xử lý dữ liệu y tế trong nghiên cứu để tạo ra các phương pháp chẩn đoán mới hoặc các phương pháp điều trị đột phá. Nói cách khác, sự phát triển nhanh chóng của công nghệ vừa đặt ra rủi ro cho việc xử lý dữ liệu nhạy cảm, vừa tạo ra những cơ hội mới để mang lại lợi ích cho không chỉ cá nhân mà toàn xã hội nói chung.

Chính vì tính chất đặc thù dẫn tới những rủi ro cao đồng thời với tiềm năng to lớn mà việc xử lý dữ liệu cá nhân nhạy cảm có thể mang lại, pháp luật cần có sự đối xử đặc biệt đối với nhóm dữ liệu này[11]. Tuy nhiên, sự đối xử đặc biệt này nên được "luật hóa" như thế nào là một vấn đề còn gây nhiều tranh cãi. Làm thế nào để các quy định về dữ liệu nhạy cảm đồng thời đáp ứng hai mục tiêu, vừa đảm bảo sự bảo vệ đầy đủ nhưng lại không hạn chế quá mức tiềm năng của chúng, vẫn là một câu hỏi khó cho các nhà lập pháp. Phần tiếp theo đây sẽ phân tích cách tiếp cận của Liên minh châu Âu đối với vấn đề này, cụ thể thông qua các quy định về bảo vệ dữ liệu nhạy cảm trong GDPR.

## 3. Bảo vệ dữ liệu cá nhân nhạy cảm theo GDPR

GDPR dành riêng một điều khoản (Điều 9) để quy định về việc xử lý các nhóm dữ liệu cá nhân đặc biệt (dữ liệu cá nhân nhạy cảm). Quy định này không phải xuất hiện lần đầu tiên trong GDPR mà kế thừa quy định trước đó tại Điều 8 trong Chỉ thị Bảo vệ dữ liệu (Data Protection Directive) được EU ban hành từ năm 1995. Ngay từ thời điểm ban hành Chỉ thị Bảo vệ dữ liệu, các nhà lập pháp EU đã cho rằng cần có cơ chế riêng điều chỉnh việc xử lý một số nhóm dữ liệu đặc biệt. Tiếp tục cách tiếp cận này, Điều 9 GDPR quy định việc xử lý các dữ liệu cá nhân nhạy cảm, trong đó đưa ra định nghĩa dữ liệu cá nhạy cảm và các điều kiện cụ thể về việc xử lý các dữ liệu này.

### *3.1. Định nghĩa dữ liệu cá nhân nhạy cảm*

Điều 9(1) quy định dữ liệu cá nhân nhạy cảm bao gồm "bất kỳ dữ liệu nào tiết lộ chủng tộc hoặc nguồn gốc dân tộc, quan điểm chính trị, đức tin tôn giáo, quan niệm triết lý, thành viên công đoàn", "dữ liệu di

[8] William Seltzer và Margo Anderson, *The Dark Side of Numbers: The Role of Population Data Systems in Human Right Abuses,* Social Research, Vol 68, No 2, Numbers (Summer 2001), p.485–486.

[9] William Seltzer và Margo Anderson, tlđd, p. 486–487.

[10] Christopher Kuner, tlđd, p. 370.

[11] Paul Quinn và Gianclaudio Malgieri, tlđd, p. 1586.

truyền và sinh trắc học" hoặc "dữ liệu liên quan đến sức khỏe, đời sống tình dục và xu hướng tình dục" của cá nhân. Đây đều là những dữ liệu đặc biệt quan trọng đối với các quyền cơ bản của con người hoặc có thể gây ảnh hưởng lớn tới đời sống của cá nhân. Ví dụ, việc bảo vệ dữ liệu về quan điểm chính trị được cho là cần thiết để đảm bảo quyền tự do biểu đạt – một quyền cơ bản được ghi nhận tại Điều 11 trong Hiến chương Liên minh châu Âu về những Quyền cơ bản và Điều 10 Công ước châu Âu về quyền con người. Tương tự như vậy, việc cấm xử lý dữ liệu liên quan tới đời sống tình dục hay xu hướng tình dục nhằm bảo vệ cuộc sống riêng tư, gia đình của cá nhân theo Điều 7 Hiến chương Liên minh châu Âu về những Quyền cơ bản và Điều 8 Công ước châu Âu về quyền con người.

Trước tiên, có thể dễ dàng nhận thấy cách quy định tại Điều 9(1) đó là đưa ra danh sách dữ liệu nhạy cảm dưới dạng đóng, tức là ngoài các dữ liệu đã liệt kê thì không thể thêm các loại dữ liệu khác. Cách quy định này có thể khiến nhiều người cho là làm hẹp phạm vi áp dụng của Điều này. Tuy nhiên, quan điểm này không hoàn toàn đúng, bởi nếu phân tích kỹ sẽ thấy Điều 9(1) có phạm vi áp dụng khá rộng. Danh sách nhóm dữ liệu nhạy cảm tại Điều này không chỉ bao gồm các nhóm thông tin trực tiếp mà còn bao gồm cả các thông tin mang tính chỉ dẫn, có thể được sử dụng để gián tiếp dẫn tới dữ liệu nhạy cảm của cá nhân. Cụ thể là Điều 9(1) các nhà lập pháp sử dụng cách diễn đạt "bất kỳ dữ liệu nào *tiết lộ (revealing)* chủng tộc…", thay vì "dữ liệu *về* chủng tộc,…" Minh chứng cho lập luận này, trong báo cáo về vụ bê bối dữ liệu Facebook – Cambrige Analytica[12], Ủy ban Thông tin của Vương quốc Anh (Information Commissioner's Office) đã nêu rõ rằng, công ty Cambrige Analytica đã xử lý dữ liệu cá nhân thu được từ người dùng Facebook để dự đoán về khuynh hướng và quan điểm chính trị của họ, và dữ liệu như vậy nên được coi là dữ liệu nhạy cảm trong bối cảnh đó[13].

Việc quy định dữ liệu nhạy cảm bao gồm cả các thông tin trực tiếp và thông tin gián tiếp dẫn tới dữ liệu là phù hợp để đảm bảo tính hiệu quả của cơ chế bảo vệ đặc biệt dành cho nhóm dữ liệu này. Nhờ sự phát triển của công nghệ thông tin trong bối cảnh xã hội ngày nay, việc thu thập dữ liệu cá nhân thông qua xử lý thông tin gián tiếp là không hề khó khăn. Do đó, quy định về bảo vệ dữ liệu cá nhân nhạy cảm sẽ kém hiệu quả nếu chỉ hướng tới bảo vệ các thông tin trực tiếp.

Tuy nhiên, cách quy định rộng như vậy về dữ liệu nhạy cảm cũng có thể dẫn tới nhiều vấn đề trong quá trình áp dụng và diễn giải luật. Ví dụ, một bức ảnh của cá nhân có thể chỉ ra chủng tộc của người đó (dựa trên màu da của họ) hoặc tôn giáo (nếu họ đang mặc trang phục tôn giáo), nhưng việc áp dụng Điều 9 GDPR cho tất cả bức

[12] Vụ bê bối dữ liệu Facebook–Cambridge Analytica liên quan đến việc thu thập thông tin nhận dạng cá nhân của 87 triệu người sử dụng Facebook mà Cambridge Analytica bắt đầu thu thập vào năm 2014. Dữ liệu này được sử dụng để gây ảnh hưởng đến ý kiến cử tri thay mặt các chính khách thuê họ. Sau khi phát hiện ra, làn sóng người dùng giận dữ và tẩy chay xảy ra trên phạm vi toàn cầu (The Atlantic, *The Cambridge Analytica Scandal, in Three Paragraphs*, https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/, công bố ngày 20/03/2018, truy cập ngày 23/5/2024).

[13] Information Commission's Office, *Investigation into the use of data analytics in political campaigns: A report to Parliament*, 6 November 2018, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf, công bố ngày 6/11/2018, truy cập ngày 22/5/2024, tr. 36.

ảnh cá nhân có vẻ quá rộng[14]. Chính vì vậy, trong các đoạn giải thích, GDPR cũng làm rõ rằng, các bức ảnh chỉ được coi là dữ liệu nhạy cảm khi chúng thỏa mãn định nghĩa về dữ liệu sinh trắc học[15]. Bên cạnh đó, Ủy ban Bảo vệ dữ liệu châu Âu (EDPB) đã hướng dẫn rằng các hình ảnh, video không tự nó được coi là loại dữ liệu cá nhân đặc biệt, nhưng nếu hình ảnh, video đó được xử lý để suy luận ra dữ liệu nhạy cảm thì Điều 9 sẽ được áp dụng. Để làm rõ ý này, EDPB đưa ra ví dụ rằng, quan điểm chính trị của cá nhân có thể được suy luận từ hình ảnh cho thấy cá nhân đó có thể nhận diện tham gia vào một sự kiện tôn giáo, chính trị hay tham gia đình công... Trong trường hợp đó, hình ảnh ghi lại được sẽ thuộc dữ liệu nhạy cảm theo Điều 9[16]. Như vậy, việc xác định một dữ liệu có thuộc phạm vi điều chỉnh của Điều 9 hay không sẽ phụ thuộc vào bối cảnh thu thập và xử lý dữ liệu đó.

### *3.2. Quy định về xử lý dữ liệu cá nhân nhạy cảm*

Về việc xử lý dữ liệu cá nhân nhạy cảm, Điều 9(1) quy định việc xử lý này, về nguyên tắc, là bị cấm. Tuy nhiên, Điều 9(2) cũng đưa ra một danh sách các trường hợp ngoại lệ mà Điều 9(1) sẽ không áp dụng (tức là việc xử lý dữ liệu là có thể thực hiện). Cách tiếp cận này tạo ra một "hàng rào" bảo vệ rất cao đối với dữ liệu cá nhân nhạy cảm. Một mặt, quy định này khẳng định tầm quan trọng đặc biệt mà GDPR dành cho các dữ liệu nhạy cảm. Nguyên tắc cấm xử lý dữ liệu cá nhân nhạy cảm khiến cho bên kiểm soát dữ liệu hoặc bên xử lý phải hết sức thận trọng khi có ý định xử lý nhóm dữ liệu này. Mặt khác, vì các quy định tại Điều 9(2) cho phép xử lý dữ liệu cá nhân nhạy cảm là các ngoại lệ, nên về nguyên tắc, sẽ được diễn giải theo hướng hẹp. Điều này một lần nữa hạn chế rủi ro đối với chủ thể dữ liệu[17].

Theo Điều 9(2), việc xử lý dữ liệu cá nhân nhạy cảm có thể thực hiện nếu thuộc một trong 10 trường hợp ngoại lệ sau đây.

Thứ nhất là, xử lý dữ liệu nhạy cảm khi có sự đồng ý rõ ràng (explicit consent) của chủ thể dữ liệu (Điều 9(2)(a)). Quy định này cần được so sánh với quy định về xử lý dữ liệu thông thường tại Điều 6(1)(a) GDPR, trong đó yêu cầu có sự đồng ý của chủ thể dữ liệu nhưng không có điều kiện sự đồng ý này phải "rõ ràng". Quy định "sự đồng ý rõ ràng" tại Điều 9(2) đưa ra một điều kiện cao hơn, đòi hỏi một mức độ chính xác và minh thị hơn trong tuyên bố đồng ý, cũng như một mô tả chính xác về các mục đích xử lý thông tin[18]. Ngoài ra, bên kiểm soát dữ liệu cũng cần tạo điều kiện để chủ thể dữ liệu thông tin được rút lại sự đồng ý bất cứ lúc nào trước khi việc xử lý dữ liệu nhạy cảm được thực hiện[19].

Thứ hai là, việc xử lý dữ liệu là cần thiết để thực hiện các nghĩa vụ và thực hiện các quyền cụ thể của bên kiểm soát dữ liệu hoặc chủ thể dữ liệu trong lĩnh vực pháp luật lao động hoặc pháp luật về an sinh xã hội (Điều 9(2)(b)). Ngoại lệ này bao gồm trường hợp nhà tuyển dụng cần xử lý dữ liệu nhạy cảm của nhân viên nhằm tuân thủ các nghĩa vụ của họ theo pháp luật lao động và an sinh xã hội. Ví dụ như khi các công ty ở Đức cần thu thập dữ liệu về tôn giáo của nhân viên để khấu trừ thuế nhà thờ (church tax), hoặc việc thu thập dữ liệu sinh trắc học để sử dụng trong các hệ thống kiểm soát ra vào tại nơi làm việc.

[14] Christopher Kuner, tlđd, p. 374.
[15] GDPR, Recital 51.
[16] EDPB, *Guidelines 3/2019 on processing of personal data through video devices, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf,* công bố ngày 29/01/2020, truy cập ngày 13/5/2024, p. 17-18.
[17] Christopher Kuner, tlđd, p. 375.
[18] Điều 4(11) GDPR.
[19] Điều 13(2)(c) và 14(2)(d) GDPR.

Thứ ba là, việc xử lý dữ liệu nhằm bảo vệ lợi ích thiết yếu của chủ thể dữ liệu hoặc của người khác khi chủ thể dữ liệu vì các lý do pháp lý hoặc thể chất mà không thể đưa ra sự đồng ý (Điều 9(2)(c)). Theo hướng dẫn trong GDPR thì những "lợi ích thiết yếu" của cá nhân bao gồm "tính toàn vẹn về thể chất hoặc sự sống", vì vậy ngoại lệ này áp dụng khi việc xử lý dữ liệu liên quan đến sức khỏe và sự an toàn của các cá nhân[20]. Ví dụ như khi việc xử lý dữ liệu nhạy cảm cần thiết cho việc điều trị y tế (dù là điều trị để cứu sống, hay điều trị cho một tình trạng y tế nghiêm trọng nhưng không nguy hiểm đến tính mạng, như gãy xương). Để ngoại lệ này áp dụng, chủ thể dữ liệu phải ở trong tình huống không thể đưa ra sự đồng ý vì lý do về thể chất (ví dụ như khi họ bị bệnh nặng) hoặc về mặt pháp lý (ví dụ như khi họ là người chưa thành niên)[21].

Thứ tư là, xử lý dữ liệu nhạy cảm do một tổ chức phi lợi nhuận có mục tiêu chính trị, triết học, tôn giáo hoặc công đoàn thực hiện trong quá trình hoạt động hợp pháp của tổ chức này và với điều kiện là phải có các biện pháp bảo vệ dữ liệu thích đáng. GDPR có hướng dẫn rằng, ngoại lệ này chỉ áp dụng với các tổ chức có mục đích nhằm cho phép "việc thực hiện các quyền tự do cơ bản"[22]. Do đó, không phải mọi tổ chức phi chính phủ hoặc tổ chức phi lợi nhuận đều được viện dẫn ngoại lệ này. Ngoài ra, ngoại lệ chỉ áp dụng cho việc xử lý dữ liệu liên quan đến các mục đích của tổ chức (ví dụ như việc xử lý dữ liệu bởi một tổ chức tôn giáo nhằm mục đích quảng cáo sẽ không được áp dụng ngoại lệ này). Điều 9(2)(d) quy định rằng, ngoại lệ này chỉ áp dụng đối với việc xử lý dữ liệu nội bộ bởi tổ chức, và không áp dụng cho việc chuyển dữ liệu cho các bên thứ ba.

Thứ năm là, dữ liệu nhạy cảm có thể được xử lý khi những dữ liệu này đã được công khai rõ ràng bởi chính chủ thể dữ liệu (Điều 9(2)(e) GDPR). Trong trường hợp này, "công khai" được hiểu bao gồm việc đăng dữ liệu trên các phương tiện truyền thông đại chúng, đưa lên các nền tảng mạng xã hội trực tuyến hoặc các hành động tương tự. Tuy nhiên, sự công khai này phải rõ ràng, điều này yêu cầu một hành động xác nhận từ phía chủ thể dữ liệu và có sự nhận thức của họ về hậu quả của hành động[23]. Ví dụ, EDPB hướng dẫn rằng, trong trường hợp giám sát bằng camera, ngay cả khi có thông báo trước về việc lắp đặt camera tại khu vực giám sát thì bên kiểm soát dữ liệu cũng không thể viện dẫn Điều 9(2)(e) để xử lý dữ liệu nhạy cảm thu thập được (nếu có). Theo Cơ quan này thì việc chỉ đơn giản là đi vào phạm vi hoạt động của camera giám sát không thể được hiểu rằng chủ thể dữ liệu có ý định công khai các dữ liệu nhạy cảm có liên quan tới họ mà camera có thể ghi lại[24]. Ngoài ra, ngoại lệ này cũng không áp dụng nếu việc công khai dữ liệu trước đó là bất hợp pháp.

Thứ sáu là, xử lý dữ liệu nhạy cảm để chứng minh hoặc thực hiện các khiếu kiện, yêu cầu pháp lý hoặc bất cứ tình huống nào khi tòa án thực thi chức năng tư pháp của mình (Điều 9(2)(f)). Ngoại lệ này áp dụng cho các thủ tục tố tụng tại tòa án, dù là được viện dẫn nguyên đơn hay bị đơn cũng như trong các thủ tục tố tụng tương tự (ví dụ như tại trọng tài).

Thứ bảy là, khi việc xử lý dữ liệu nhạy cảm phục vụ "lợi ích công cộng đáng kể" (substantial public interest). Trong quá trình soạn thảo GDPR, khi thảo luận về ngoại lệ này, có nhiều quan ngại rằng, một quy định chung chung, thiếu cụ thể về lợi ích công

[20] GDPR, Recital 112.
[21] Christopher Kuner, tlđd, p. 378.
[22] GDPR, Recital 51.
[23] Christopher Kuner, tlđd, p. 378.
[24] EDPB, tlđd, p. 17-19.

cộng có thể tạo ra lỗ hổng dẫn tới việc lạm dụng[25]. Để tránh tình trạng này, Điều 9(2)(f) quy định rằng việc xử lý dữ liệu trong trường hợp này phải dựa trên luật của EU hoặc quốc gia thành viên và luật đó phải "tương xứng với mục tiêu theo đuổi, tôn trọng bản chất của quyền bảo vệ dữ liệu và đưa ra các biện pháp phù hợp và cụ thể để bảo vệ các quyền cơ bản và lợi ích của chủ thể dữ liệu". Việc xác định lợi ích công cộng đáng kể yêu cầu một sự cân bằng giữa lợi ích công cộng và các rủi ro đối với chủ thể dữ liệu. Để xử lý dữ liệu nhạy cảm, lợi ích công cộng được viện dẫn phải là "đáng kể" – điều kiện này cao hơn so với điều kiện xử lý dữ liệu cá nhân thông thường vì lợi ích công cộng theo Điều 6(1)(e). GDPR đưa ra một số ví dụ cho trường hợp ngoại lệ này, bao gồm việc xử lý dữ liệu là cần thiết cho các mục đích nhân đạo, như giám sát dịch bệnh và sự lây lan của chúng hoặc trong các tình huống khẩn cấp nhân đạo, đặc biệt là trong các thảm họa tự nhiên và do con người gây ra[26]. Có thể thấy, GDPR đặt ra điều kiện rất cao để viện dẫn ngoại lệ này.

Thứ tám là, việc xử lý dữ liệu là cần thiết cho các mục đích điều trị hoặc phòng ngừa y tế, bao gồm cả cung cấp dịch vụ y tế, chăm sóc sức khỏe, quản lý hệ thống y tế và sức khỏe xã hội theo quy định của luật EU hoặc của quốc gia thành viên (Điều 9(2)(h)). Để ngoại lệ được áp dụng thì cần đáp ứng thêm các điều kiện tại Điều 9(3), yêu cầu dữ liệu nhạy cảm phải được xử lý "bởi hoặc dưới trách nhiệm của một chuyên gia chịu sự ràng buộc của nghĩa vụ bảo mật chuyên môn" như bác sĩ, nha sĩ, nhà tâm lý học, bệnh viện và công ty bảo hiểm.

Thứ chín là, việc xử lý dữ liệu vì lợi ích công cộng trong lĩnh vực sức khỏe cộng đồng (Điều 9(2)(i)). Điều 9(2)(i) cũng làm rõ rằng, ngoại lệ này áp dụng đặc biệt trong các trường hợp "bảo vệ chống lại các mối đe dọa nghiêm trọng xuyên biên giới đối với sức khỏe hoặc đảm bảo tiêu chuẩn cao về chất lượng và an toàn của chăm sóc sức khỏe và của các sản phẩm y tế hoặc thiết bị y tế". Ngoại lệ này chỉ cho phép việc xử lý dữ liệu phải "dựa trên luật của Liên minh hoặc Quốc gia thành viên cung cấp các biện pháp thích hợp và cụ thể để bảo vệ các quyền của chủ thể dữ liệu, đặc biệt là bảo mật chuyên môn".

Thứ mười là, việc xử lý dữ liệu nhằm mục đích lưu trữ vì lợi ích công cộng, nghiên cứu khoa học hoặc lịch sử hoặc mục đích thống kê (Điều 9(2)(j)). Theo đó, việc xử lý dữ liệu nhạy cảm phải tương xứng với mục tiêu theo đuổi, tôn trọng bản chất của quyền bảo vệ dữ liệu và cung cấp các biện pháp thích hợp và cụ thể để bảo vệ các quyền cơ bản và lợi ích của chủ thể dữ liệu. Tính tương xứng trong ngữ cảnh này thường yêu cầu rằng, dữ liệu chỉ được xử lý đến mức cần thiết nhất[27].

Như vậy, có thể thấy GDPR dành một mức bảo vệ rất cao đối với các dữ liệu nhạy cảm quy định tại Điều 9, theo đó, việc xử lý dữ liệu nhạy cảm chỉ được phép trong một số trường hợp ngoại lệ nhất định. Các ngoại lệ này có thể vì lợi ích của cá nhân chủ thể dữ liệu, lợi ích của bên thứ ba, hoặc lợi ích công cộng, nhưng đều được quy định khá chi tiết, để đảm bảo những mục đích này phải tương xứng với mức độ xử lý dữ liệu và tôn trọng quyền được bảo vệ dữ liệu. Ngoài ra, cũng cần lưu ý thêm rằng, ngay cả

[25] Article 29 Data Protection Working Party, *Advice paper on special categories of data (sensitive data),* https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf, công bố ngày 04/4/2011, truy cập 10/5/2024.

[26] GDPR, Recital 46.

[27] Christopher Kuner, tlđd, p. 381.

khi việc xử lý dữ liệu thuộc một trong các ngoại lệ đã quy định tại Điều 9(2) thì bên xử lý dữ liệu vẫn phải đảm bảo tuân thủ đầy đủ các nghĩa vụ về bảo vệ dữ liệu quy định tại Điều 6 (các quy định về xử lý dữ liệu cá nhân thông thường).

**4. Bảo vệ dữ liệu cá nhân nhạy cảm theo Nghị định số 13/2023/NĐ-CP và một số kiến nghị hoàn thiện**

Ngày 17/4/2023, Chính phủ đã ban hành Nghị định số 13/2023/NĐ-CP (Nghị định 13) về bảo vệ dữ liệu cá nhân, đánh dấu bước tiến lớn trong nỗ lực xây dựng hành lang pháp lý nhằm bảo vệ dữ liệu cá nhân tại Việt Nam. Đây là được coi là văn bản nền móng, tiến tới xây dựng Luật Bảo vệ dữ liệu cá nhân[28]. Nghị định 13 phân loại dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm (Điều 2) và cũng dành một số điều khoản riêng quy định về dữ liệu cá nhân nhạy cảm. Điều này cho thấy các nhà làm luật Việt Nam cũng dành sự quan tâm đặc biệt đối với nhóm dữ liệu này.

Đầu tiên, Nghị định 13 đưa ra định nghĩa về dữ liệu cá nhân nhạy cảm kèm theo một danh mục các loại dữ liệu thuộc nhóm này. Cụ thể, khoản 4 Điều 2 quy định: "Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân" và bao gồm các nhóm dữ liệu sau:

a) Quan điểm chính trị, quan điểm tôn giáo;

b) Tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án

c) Thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc;

d) Thông tin về đặc điểm di truyền;

đ) Thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân;

e) Thông tin về đời sống tình dục, xu hướng tình dục của cá nhân;

g) Dữ liệu về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;

h) Thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, các tổ chức được phép khác, gồm: thông tin định danh khách hàng theo quy định của pháp luật, thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch, thông tin về tổ chức, cá nhân là bên bảo đảm tại tổ chức tín dụng, chi nhánh ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán;

i) Dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị;

k) Dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.

Từ quy định này có thể thấy, Nghị định 13 thừa nhận tầm quan trọng của một số dữ liệu đặc biệt, cần được bảo vệ ở mức độ cao hơn so với các dữ liệu thông thường. Đây là các dữ liệu gắn với quyền riêng tư của cá nhân và nếu bị xâm phạm sẽ có ảnh hưởng trực tiếp tới quyền và lợi ích của cá nhân đó. Hướng tiếp cận này có nhiều điểm tương đồng với tinh thần của GDPR về bảo vệ dữ liệu nhạy cảm.

Ngoài ra, thoạt nhìn thì có vẻ như định nghĩa dữ liệu cá nhân nhạy cảm tại khoản 4 Điều 2 Nghị định 13 có phạm vi rộng hơn so với quy định tương tự tại Điều 9(1) của

[28] Thực hiện chỉ đạo của Chính phủ về việc xây dựng Luật Bảo vệ dữ liệu cá nhân, đầu năm 2024, Bộ Công an đã trình đề nghị xây dựng Luật Bảo vệ dữ liệu cá nhân, https://chinhphu.vn/du-thao-vbqppl/ho-so-de-nghi-xay-dung-luat-bao-ve-du-lieu-ca-nhan-6312, công bố ngày 29/02/2024, truy cập ngày 18/5/2024.

GDPR. Cụ thể, khoản 4 Điều 2 từ điểm a tới điểm e liệt kê các dữ liệu cá nhân tương tự như các dữ liệu tại Điều 9(1) GDPR như dữ liệu về quan điểm chính trị, tôn giáo, tình trạng sức khỏe, thông tin về nguồn gốc chủng tộc, dân tộc, thông tin về di truyền, đặc điểm sinh học, đời sống tình dục, xu hướng tình dục... Ngoài ra, khoản 4 Điều 2 cũng liệt kê một số nhóm dữ liệu khác được coi là nhạy cảm bao gồm dữ liệu về tội phạm, hành vi phạm tội, thông tin khách hàng của tổ chức tín dụng, dữ liệu về vị trí của cá nhân. Quy định này thậm chí cũng "để mở" danh mục dữ liệu cá nhân nhạy cảm, bao gồm các dữ liệu đặc thù khác theo quy định pháp luật, từ đó, nhằm tạo ra sự linh hoạt nhất định để "dự phòng" những dữ liệu cá nhân khác có thể yêu cầu bảo vệ đặc biệt trong tương lai.

Tuy nhiên, quy định tại khoản 4 Điều 2 có một số điểm cần làm rõ. Thứ nhất là, liệu quy định này có bao gồm các thông tin mang tính chất chỉ dẫn, thông tin gián tiếp, mà nếu xử lý có thể dẫn tới các dữ liệu nhạy cảm hay không. Khác với cách quy định tại Điều 9(1), cho phép phạm vi áp dụng của dữ liệu cá nhân nhạy cảm bao gồm cả thông tin trực tiếp và thông tin gián tiếp, khoản 4 Điều 2 dường như chỉ nhắm tới các nhóm thông tin trực tiếp. Điều này được ngầm hiểu thông qua cách sử dụng từ ngữ "quan điểm chính trị, quan điểm tôn giáo", "thông tin về đời sống tình dục"… Trên thực tế, dữ liệu cá nhân nhạy cảm có thể được tạo ra trên cơ sở kết hợp nhiều dữ liệu cá nhân cơ bản và bên kiểm soát hoặc bên xử lý dữ liệu có thể dựa trên các dữ liệu cơ bản này để tạo ra các nhóm dữ liệu và sau đó suy ra về dữ liệu nhạy cảm của các cá nhân như quan điểm chính trị, nguồn gốc chủng tộc hay khuynh hướng tình dục của chủ thể dữ liệu[29]. Trường hợp công ty Cambrige Analytica đã xử lý dữ liệu người dùng Facebook để dự đoán về khuynh hướng và quan điểm chính trị của họ, từ đó cung cấp thông tin cho các tổ chức chính trị để định hướng dư luận là một ví dụ điển hình. Do đó, việc bỏ sót các nhóm thông tin gián tiếp trong định nghĩa dữ liệu cá nhân nhạy cảm có thể hạn chế sự hiệu quả của quy định này.

Ngoài ra, danh mục dữ liệu cá nhân nhạy cảm tại Nghị định 13 bao gồm nhiều nhóm dữ liệu, trong đó có những nhóm dữ liệu khác nhau về bản chất và đòi hỏi cách thức bảo vệ khác nhau. Ví dụ dữ liệu về quan điểm chính trị, tôn giáo, nguồn gốc chủng tộc… là các dữ liệu gắn liền với các quyền cơ bản của cá nhân, do đó cần ưu tiên quyền kiểm soát của chủ thể dữ liệu đối với việc xử lý dữ liệu. Trong khi đó, đối với thông tin về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật thì việc xử lý dữ liệu cần được trao quyền nhất định cho các cơ quan thực thi, đảm bảo sự cân bằng giữa quyền riêng tư của cá nhân và sự cần thiết xử lý thông tin để thực thi pháp luật. Do đó, việc gộp các nhóm dữ liệu này vào chung một điều khoản để áp dụng chung một cơ chế bảo vệ là chưa thực sự phù hợp[30].

Thêm vào đó, cách quy định về phạm vi dữ liệu cá nhân nhạy cảm như trên cũng dẫn tới các quy định về cơ chế bảo vệ đối với nhóm dữ liệu này trong Nghị định 13 cũng

[29] Lý Vương Thảo, *Tăng cường cơ chế bảo vệ dữ liệu cá nhân nhạy cảm theo quy định của pháp luật Việt Nam hiện nay*, Tạp chí Tòa án nhân dân điện tử, https://tapchitoaan.vn/tang-cuong-co-che-bao-ve-du-lieu-ca-nhan-nhay-cam-theo-quy-dinh-cua-phap-luat-viet-nam-hien-nay10859.html, công bố ngày 08/5/2024, truy cập ngày 23/5/2024.

[30] Cách quy định hiện nay của khoản 4 Điều 2 trong Nghị định 13 có nhiều điểm tương đồng với quy định của Điều 8 trong Chỉ thị bảo vệ dữ liệu cá nhân của EU trước đây. Tuy nhiên, nhận thấy những bất cập trong cách quy định này, GDPR đã tách các nhóm dữ liệu có đặc thù khác nhau và điều chỉnh bằng các quy định riêng.

chưa thực sự rõ ràng và hiệu quả. Cụ thể, Nghị định quy định về xử lý và bảo vệ dữ liệu cá nhân nhạy cảm rải rác trong một số điều khoản, mà thiếu một nguyên tắc chung. Cụ thể, khoản 8 Điều 11 quy định rằng "Đối với xử lý dữ liệu cá nhân nhạy cảm, chủ thể dữ liệu phải được thông báo rằng dữ liệu cần xử lý là dữ liệu cá nhân nhạy cảm". Ngoài ra, Điều 28 quy định về bảo vệ dữ liệu cá nhân nhạy cảm, theo đó ngoài các biện pháp bảo vệ dữ liệu cá nhân nói chung (khoản 2 Điều 26) và bảo vệ dữ liệu cá nhân cơ bản (Điều 27) thì cần chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân, chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân và việc xử lý dữ liệu cá nhân nhạy cảm phải được thông báo cho chủ thể dữ liệu. Những quy định này chủ yếu về mặt hình thức, mà chưa thực sự tạo ra một "sự bảo vệ đặc biệt" nào.

Bên cạnh đó, về nghĩa vụ thông báo cũng như các điều kiện xử lý dữ liệu nhạy cảm trong Nghị định 13, nếu so sánh với các quy định áp dụng cho dữ liệu cá nhân thông thường thì chưa thấy sự khác biệt rõ rệt. Thứ nhất, cả hai loại dữ liệu này đều có thể được xử lý nếu có sự đồng ý của chủ thể dữ liệu (Điều 11). Nếu so sánh với quy định trong GDPR thì trường hợp xử lý dữ liệu cá nhân nhạy cảm sẽ cần phải có sự đồng ý 'rõ ràng', cụ thể hơn của chủ thể dữ liệu.

Thứ hai, Nghị định 13 cho phép xử lý dữ liệu cá nhân (bao gồm cả dữ liệu cá nhân nhạy cảm) thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng mà không cần thông báo với chủ thể dữ liệu (Điều 18). Trong GDPR thì đây không phải là một căn cứ để cho phép xử lý dữ liệu cá nhân nhạy cảm. Liên quan tới trường hợp này, EDPB giải thích cụ thể rằng trong trường hợp giám sát bằng camera, ngay cả khi có thông báo trước về việc lắp đặt camera tại khu vực giám sát thì bên kiểm soát dữ liệu cũng không được phép xử lý dữ liệu đối với các dữ liệu nhạy cảm thu thập được[31].

Thứ ba, Nghị định 13 đưa ra quy định về các trường hợp xử lý dữ liệu mà không cần sự đồng ý của chủ thể dữ liệu (Điều 17) áp dụng như nhau đối với dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm. Cụ thể, các trường hợp này bao gồm: Trường hợp khẩn cấp, cần xử lý ngay dữ liệu cá nhân có liên quan để bảo vệ tính mạng, sức khỏe của chủ thể dữ liệu hoặc người khác; việc công khai dữ liệu cá nhân theo quy định của luật; việc xử lý dữ liệu của cơ quan nhà nước có thẩm quyền trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng; để thực hiện nghĩa vụ theo hợp đồng của chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của luật; và phục vụ hoạt động của cơ quan nhà nước đã được quy định theo luật chuyên ngành. Các trường hợp ngoại lệ này được quy định khá rộng và chưa dành sự quan tâm cần thiết đối với quyền lợi của chủ thể dữ liệu khi dữ liệu nhạy cảm bị công khai. Điều này khá rõ nếu so sánh với các trường hợp ngoại lệ cho phép xử lý dữ liệu nhạy cảm theo Điều 9(2) trong GDPR. Theo GDPR, ngay cả khi việc xử lý dữ liệu nhạy cảm nhằm mục đích công cộng, thì việc xử lý phải ở mức độ cần thiết, tương xứng, tôn trọng bản chất của quyền bảo vệ dữ liệu của chủ thể và cần phải đi cùng với các biện pháp bảo vệ thích hợp. Có thể thấy, cách tiếp cận của GDPR đòi hỏi sự cân bằng giữa một bên là lợi ích mà việc xử lý dữ liệu có thể mang lại với một bên là những rủi ro cao có thể gây ra đối với chủ thể dữ liệu. Những vấn đề này, rất tiếc, còn bỏ ngỏ trong quy định của Nghị định 13.

[31] EDPB, tldđ, p. 17-19.

Như vậy, phân tích quy định về bảo vệ dữ liệu cá nhân nhạy cảm theo Nghị định 13 cho thấy các nhà soạn thảo đã ghi nhận tầm dữ liệu cá nhân nhạy cảm cần có sự bảo vệ đặc biệt (so với các dữ liệu cá nhân cơ bản) do tính chất đặc thù của nhóm dữ liệu này có ảnh hưởng lớn tới quyền lợi của chủ thể dữ liệu. Nghị định 13 cũng đã đưa ra định nghĩa về dữ liệu cá nhân nhạy cảm và bước đầu xây dựng những quy định riêng về việc bảo vệ. Tuy nhiên, phân tích nội dung các quy định này cho thấy cơ chế bảo vệ mà Nghị định 13 dành cho nhóm dữ liệu nhạy cảm chủ yếu mới dừng lại ở mặt hình thức, thiếu các biện pháp cụ thể, rõ ràng, do đó chưa đảm bảo sự bảo vệ thích đáng cần thiết cho nhóm dữ liệu đặc thù này.

## 5. Kết luận và một số khuyến nghị

Với sự phát triển ngày càng nhanh, mạnh của khoa học công nghệ, dữ liệu cá nhân trở thành nguồn tài nguyên to lớn cho sự phát triển xã hội, đồng thời cũng là đối tượng tấn công hấp dẫn của các nhóm tội phạm công nghệ cao.Trong bối cảnh các mối đe dọa tới an ninh mạng và quyền riêng tư ngày càng tăng, việc bảo vệ dữ liệu cá nhân, đặc biệt là các dữ liệu cá nhân nhạy cảm đặt ra thách thức lớn đối các nhà lập pháp. Dữ liệu cá nhân nhạy cảm, nếu bị xâm phạm, có thể ảnh hưởng rất lớn tới quyền cơ bản của chủ thể dữ liệu, gây ra những hậu quả nghiêm trọng mà đôi khi không thể khắc phục được. Mặt khác, các dữ liệu này cũng có tiềm năng khai thác to lớn, có thể tạo ra lợi ích không chỉ đối với cá nhân mà cho toàn xã hội. Do đó, cần có những quy định pháp luật riêng biệt và cụ thể đối với việc thu thập và xử lý các nhóm dữ liệu này.

Nghị định 13 bước đầu đã ghi nhận tính chất đặc thù của dữ liệu cá nhân nhạy cảm và xây dựng một số quy định riêng dành cho các dữ liệu này. Tuy nhiên, các quy định này còn tương đối chung chung, chưa có sự phân biệt rõ ràng giữa xử lý dữ liệu cá nhân nhạy cảm đối với các trường hợp xử lý dữ liệu cá nhân thông thường. Các quy định này chưa thiết lập được một cơ chế bảo vệ hiệu quả dành cho nhóm dữ liệu vốn rất nhạy cảm và đặc thù này. Trong khi đó, việc rò rỉ thông tin cá nhân trên không gian mạng tại Việt Nam, đặc biệt các thông tin nhạy cảm đang diễn ra ngày càng nghiêm trọng, dưới nhiều hình thức và quy mô khác nhau. Do đó, việc tăng cường bảo vệ dữ liệu cá nhân nhạy cảm thông qua hoàn thiện các quy định pháp luật là vô cùng cần thiết.

Để thực hiện điều này, việc nghiên cứu các quy định về bảo vệ dữ liệu cá nhân nhạy cảm trong GDPR có giá trị tham khảo đối với các nhà làm luật tại Việt Nam. Ví dụ, GDPR mở rộng phạm vi bảo vệ dữ liệu cá nhân nhạy cảm, không chỉ bao gồm các thông tin trực tiếp mà cả các thông tin gián tiếp – các dữ liệu thông thường nhưng có thể được thu thập và xử lý dẫn tới dữ liệu cá nhân nhạy cảm. Ngoài ra, cách tiếp cận của GDPR về bảo vệ dữ liệu cá nhân được xây dựng theo hướng đưa ra một nguyên tắc chung bao hàm kèm theo các trường hợp ngoại lệ cụ thể. Không chỉ quy định về các trường hợp được phép xử lý dữ liệu cá nhân nhạy cảm, GDPR cũng đưa ra các quy định cụ thể về mức độ xử lý dữ liệu cần thiết, đảm bảo sự cân bằng và tương xứng giữa mục đích xử lý (có thể vì lợi ích của chủ thể dữ liệu hoặc mục đích công cộng) với mục đích tôn trọng quyền bảo vệ dữ liệu của cá nhân. Hướng tiếp cận này có thể được tham khảo bởi các nhà làm luật Việt Nam, đặc biệt trong quá trình soạn thảo và xây dựng Luật Bảo vệ dữ liệu cá nhân trong thời gian tới.