BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG KỈ NGUYÊN TRÍ TUỆ NHÂN TẠO KINH NGHIỆM CỦA CHÂU ÂU VÀ KIẾN NGHỊ HOÀN THIỆN PHÁP LUẬT VIỆT NAM

NGUYỄN THỊ THU TRANG *

Tóm tắt: *Sự phát triển của trí tuệ nhân tạo tác động tới nhiều mặt của đời sống xã hội. Tuy vậy, sự hình thành trí tuệ nhân tạo và ứng dụng trí tuệ nhân tạo trong cuộc sống có thể xâm phạm tới quyền về đời sống riêng tư nói chung và quyền bảo vệ dữ liệu cá nhân nói riêng. Bài viết đề cập Quy định chung về bảo vệ dữ liệu của châu Âu (GDPR) để thấy được những ưu điểm và bất cập trong việc bảo vệ dữ liệu cá nhân; tác động của GDPR tới trí tuệ nhân tạo, nền tảng công nghệ, an ninh mạng và pháp luật trên toàn cầu, từ đó rút ra bài học kinh nghiệm cho Việt Nam và kiến nghị hoàn thiện pháp luật nhằm bảo vệ hiệu quả dữ liệu cá nhân trong kỉ nguyên trí tuệ nhân tạo.*

Từ khóa: Dữ liệu cá nhân; quyền về đời sống riêng tư; trí tuệ nhân tạo

Nhận bài: 01/11/2021 Hoàn thành biên tập: 28/10/2022 Duyệt đăng: 28/10/2022

PERSONAL DATA PROTECTION IN THE AI AGE - EUROPEAN EXPERIENCE AND RECOMMENDATIONS TO IMPROVE THE LAW OF VIETNAM

Abstract: *The development of artificial intelligence affects many aspects of social life. However, the formation of artificial intelligence and the application of artificial intelligence in life may violate the right to privacy in general and the right to protect personal data in particular. The article mentions the European General Data Protection Regulation (GDPR) to see the advantages and disadvantages in protecting personal data; GDPR's impact on artificial intelligence, technology platform, cyber security and law globally, from which to experience lessons for Vietnam and propose to improve the law to effectively protect personal data in the era of artificial intelligence.*

Keywords: Personal data; right to privacy; Artificial Intelligence (AI)

Received: Nov 1st, 2021; Editing completed: Oct 28th, 2022; Accepted for publication: Oct 28th, 2022

Dẫn nhập

Quá trình chuyển đổi kĩ thuật số đang được thực hiện liên tục và một phần trong đó sử dụng trí tuệ nhân tạo (Artificial Intelligence - AI)[1]. Đây là một công nghệ liên ngành nhằm mục đích sử dụng các tập dữ liệu lớn (Big Data), khả năng tính toán phù hợp với các quy trình phân tích và ra quyết định cụ thể theo thứ tự để cho phép máy tính hoàn thành các nhiệm vụ gần đúng với khả năng của con người và thậm chí vượt quá khả năng của con người ở một số khía cạnh nhất định[2]. Theo đó, AI được ứng dụng trong nhiều lĩnh vực khác nhau của đời sống xã hội, cụ thể: 1) AI ứng

* **Tiến sĩ, Trường Đại học Kinh tế-Luật, Đại học Quốc gia Thành phố Hồ Chí Minh**
E-mail: ntttrang@uel.edu.vn

[1] Hoffmann-Riem, W. (2020), "Artificial Intelligence as a Challenge for Law and Regulation", *In: Regulating Artificial Intelligence (Wischmeyer T., Rademacher T. (eds))*, Springer, Cham, p. 2.

[2] Kaplan, J. (2016), *Artificial intelligence*, Oxford University Press, New York.

dụng trong công việc: ứng dụng trong kinh doanh[3], y tế[4], giáo dục[5], giao thông vận tải[6], sản xuất[7];... 2) AI ứng dụng trong đời sống hàng ngày: AI được sử dụng trong các thiết bị công nghệ như Siri, Bixby, Cortana... giúp cho cuộc sống của con người trở nên tiện lợi và thoải mái hơn. AI được ứng dụng trong "trợ lí ảo": hỗ trợ trong quá trình làm việc[8]; hỗ trợ học sinh tìm đường đến trường[9]; hỗ trợ khách hàng[10]; ...

Bên cạnh những lợi ích nêu trên, sự phát triển AI kéo theo sự xâm phạm tới dữ liệu cá nhân. Bởi vì, khối nhà nước và khối tư nhân đều có nhu cầu thu thập dữ liệu cá nhân phục vụ cho mục đích của mình. *Thứ nhất*, đối với khối tư nhân: dữ liệu đại diện cho một giá trị tiền tệ nhất định[11]. Khối tư nhân thu thập dữ liệu không có cấu trúc để trích xuất thông tin xác định các đặc điểm giới tính, hành vi hoặc tinh thần, sở thích mua sắm, lịch trình hoặc thói quen hàng ngày của một người nhất định. Dựa trên dữ liệu cá nhân đó, khối tư nhân đã đưa ra quyết định kinh doanh phù hợp. *Thứ hai*, đối với khối nhà nước: dữ liệu đại diện cho sức mạnh. Khối nhà nước tập hợp dữ liệu không có cấu trúc để trích xuất thông tin xác định các đặc điểm nhân khẩu học, địa lí xã hội, sức khoẻ, quan điểm chính trị, cư trú hoặc di chuyển của của công dân hoặc của người đang cư trú trên lãnh thổ quốc gia. Nhà nước dựa trên dữ liệu cá nhân để: 1) Quản lí về cư trú, nhân khẩu, thu nhập công dân, quan điểm chính trị của dân cư,...; 2) Quyết định về tính điểm công dân, dịch tễ, giao thông, an sinh xã hội...

Quyền về đời sống riêng tư nói chung và quyền được bảo vệ dữ liệu cá nhân nói riêng là quyền cơ bản của con người. Theo đó, tại tại Điều 12 Tuyên ngôn Nhân quyền quốc tế năm 1948 (Universal Declaration of Human Rights - UDHR) như sau: *"Không ai phải chịu sự can thiệp một cách tuỳ tiện vào cuộc*

[3] Soni, N. & Sharma, E. & Singh, N. & Kapoor, A. (2020), "Artificial Intelligence in Business: From Research and Innovation to Market Deployment", *Procedia Computer Science*, 167, p. 2200 - 2210.

[4] Bhattad, P. & Jain, V. (2020), "Artificial Intelligence in Modern Medicine - The Evolving Necessity of the Present and Role in Transforming the Future of Medical Care", *Cureus*, 12(5), p.e8041.

[5] Roll, I.; Wylie, R. (2016), "Evolution and revolution in artificial intelligence in education", *Int. J. Artif. Intell. Education*, 26, p. 582 – 599.

[6] Woschank, M.; Rauch, E.; Zsifkovits, H. (2020), "A Review of Further Directions for Artificial Intelligence, Machine Learning, and DeepLea rning in Smart Logistics", *Sustainability*, 12, p. 3760.

[7] Chaudhry, I. A. & Shami, M. & Khan, A. (2004), "Manufacturing Applications of Artificial Intelligence", *Journal of Engineering and Applied Sciences*, 23, p. 29 - 33.

[8] Arora, S. & Athavale, V. & Maggu, H. & Agarwal, A. (2021), "Artificial Intelligence and Virtual Assistant - Working Model", *Mobile Radio Communications and 5G Networks (Nikhil Marriwala, C. C. Tripathi, Dinesh Kumar, Shruti Jain Edn)*, Springer, p. 163 - 171.

[9] Page, L. C., & Gehlbach, H. (2017), "How an Artificially Intelligent Virtual Assistant Helps Students Navigate the Road to College", *AERA Open*, 3(4), p. 1 - 12.

[10] Brill, T. & Munoz, L. & Miller, R. (2019), "Siri, Alexa, and other digital assistants: a study of customer satisfaction with artificial intelligence applications", *Journal of Marketing Management*, 35, DOI: 10.1080/0267257X.2019.1687571.

[11] Mazurek, G. & Małagocka, K. (2019), "Are we down to zero-one code? Perception of privacy and data protection in the context of the development of artificial intelligence", *Journal of Management Analytics*, Vol.6 (4), p. 344.

sống riêng tư,... Mọi người đều được pháp luật bảo vệ chống lại sự xúc phạm và can thiệp như vậy". Tiếp đến, tại Công ước quốc tế về các quyền Dân sự và Chính trị (International Covenant on Civil and Political Rights - ICCPR) năm 1966 một lần nữa khẳng định tại Điều 17 không ai có thể can thiệp tuỳ tiện hoặc bất hợp pháp vào quyền riêng tư đối với dữ liệu cá nhân. Ngoài ra, các điều ước quốc tế, khu vực, song phương và pháp luật của các quốc gia đã cụ thể hoá các quy định nêu trên nhằm đảm bảo quyền về đời sống riêng tư nói chung và bảo vệ dữ liệu cá nhân nói riêng.

Như đã nêu ở trên, với sự phát triển mạnh mẽ của AI, với mục đích khác nhau của khối tư nhân cũng như nhà nước, dữ liệu cá nhân của con người đã, đang và sẽ bị xâm phạm. Vì vậy, xây dựng hành lang pháp lí ở quốc gia, khu vực và toàn cầu nhằm bảo vệ dữ liệu cá nhân trong kỉ nguyên AI là thực sự cần thiết. Trong phạm vi bài viết, tác giả đề cập quy định về bảo vệ dữ liệu cá nhân của EU, để thấy được điểm phù hợp và bất cập, từ đó có cơ sở để đề xuất những giải pháp, kiến nghị nhằm bảo vệ hiệu quả dữ liệu cá nhân và giúp hoàn thiện pháp luật Việt Nam về vấn đề này.

1. Bảo vệ dữ liệu cá nhân của châu Âu - Quy định và tác động

1.1. Quy định về bảo vệ dữ liệu cá nhân của châu Âu

Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation - GDPR) - Luật bảo vệ dữ liệu mới của EU có hiệu lực từ ngày 25/5/2018. GDPR áp dụng cho các tổ chức thuộc EU và ngoài EU sử dụng hoặc xử lí dữ liệu cá nhân về những người sống ở EU[12]. Các quy định của GDPR được điều chỉnh để phù hợp với những thay đổi trong công nghệ; nhóm thông tin được sử dụng để giao dịch trên kênh ảo; tính chất xuyên biên giới của việc thu thập, xử lí và sử dụng cơ sở dữ liệu[13]. Nhiệm vụ chính của GDPR là đảm bảo quyền về đời sống riêng tư của các thể nhân, với quy định cụ thể sau:

Thứ nhất, đối tượng được bảo vệ

Luật bảo vệ dữ liệu của EU bảo vệ các cá nhân (thể nhân - không phải là các tổ chức) - "chủ thể dữ liệu", liên quan đến việc xử lí dữ liệu cá nhân của họ (các điều 1.1, 1.2, 4.1). Trong đó, GDPR quy định về dữ liệu cá nhân liên quan và việc xử lí dữ liệu cá nhân (Điều 4.1, 4.2). GDPR đưa ra các quyền cá nhân thiết thực đối với chủ thể dữ liệu[14], cụ thể: 1) EU quan tâm tới bảo vệ dữ liệu của cá nhân (chủ thể dữ liệu); 2) Dữ liệu cá nhân không đơn thuần là các dữ liệu về tên và số nhận dạng như trước đây. Thay vào đó, dữ liệu cá nhân được mở rộng hơn rất nhiều so với quan điểm truyền thống. Dữ liệu cá nhân được EU bảo vệ còn có cả bản sắc thể chất, sinh lí, di truyền, tinh thần, kinh tế, văn hoá hoặc xã hội của thể nhân đó

[12] Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR], Art. 3(1) and 3(2).

[13] Mazurek, G. & Małagocka, K., tlđd, p. 351.

[14] Bendiek, A.t & Römer, M. (2019), "Externalizing Europe: the global effects of European data protection", *Digital Policy, Regulation and Governance*, Vol. 21, Iss. 1, p. 35.

(Điều 4.1). Điều này cho thấy, chủ thể dữ liệu được bảo vệ tương đối toàn diện về dữ liệu cá nhân của họ. 3) Những hoạt động xử lí dữ liệu cá nhân được GDPR dự liệu là khá rộng và đầy đủ. Với tốc độ phát triển công nghệ nói chung và AI nói riêng như hiện nay, việc dự liệu các hoạt động xử lí dữ liệu thuộc đối tượng điều chỉnh của GDPR là thực sự kịp thời. Qua đó, dữ liệu cá nhân của chủ thể dữ liệu sẽ được bảo vệ tốt hơn.

Thứ hai, nguyên tắc xử lí dữ liệu cá nhân

1) Dữ liệu cá nhân được xử lí hợp pháp, công bằng và minh bạch (Điều 5.1.a). GDPR đã nhấn mạnh việc xử lí dữ liệu cá nhân phải được thực hiện theo "phương pháp minh bạch - in a transparent manner". Cho thấy, phương pháp xử lí dữ liệu cần được thể hiện rõ ràng. Nguyên tắc này đặc biệt quan trọng bởi vì quá trình xử lí dữ liệu thông qua AI là kĩ thuật xử lí vốn rất phức tạp. 2) Nguyên tắc giới hạn mục đích (Điều 5.1.b): Dữ liệu cá nhân được thu thập cho các mục đích cụ thể, rõ ràng và hợp pháp và không được xử lí thêm theo cách không phù hợp với các mục đích đó. Chính nguyên tắc này giúp chủ thể xác định được mục đích thu thập dữ liệu và biết được giới hạn của hành vi thu thập dữ liệu. 3) Nguyên tắc giảm thiểu dữ liệu (Điều 5.1.c): Bên xử lí dữ liệu không được thu thập nhiều hơn những dữ liệu cần thiết phục vụ cho mục đích xử lí. Điều này giúp hạn chế, kiểm soát việc thu thập dữ liệu để phục vụ cho những mục đích không chính đáng. 4) Nguyên tắc chính xác (Điều 5.1.d): Nguyên tắc này giúp hạn chế những dữ liệu cá nhân không chính xác được lưu trữ và xử lí sẽ ảnh hưởng tới lợi ích của chủ thể dữ liệu, chủ thể sử dụng dữ liệu và bên liên quan. 5) Nguyên tắc giới hạn lưu trữ (Điều 5.1.e): Nguyên tắc này giúp hạn chế và kiểm soát thời gian lưu trữ dữ liệu cá nhân và tránh trường hợp chủ thể lưu trữ, xử lí dữ liệu sử dụng dữ liệu vào mục đích không chính đáng. 6) Nguyên tắc tính toàn vẹn và bảo mật (Điều 5.1.f): Nguyên tắc này đưa ra nhằm ràng buộc chủ thể thu thập, lưu trữ và xử lí dữ liệu cần phản đảm bảo tính toàn vẹn và bảo mật dữ liệu của các chủ thể dữ liệu. 7) Nguyên tắc giải trình (Điều 5.2): Nguyên tắc này giúp nâng cao trách nhiệm giải trình của chủ thể thu thập, lưu trữ và xử lí dữ liệu cá nhân. Nhìn chung, hệ thống các nguyên tắc của GDPR được xây dựng đầy đủ, phù hợp và mang tính hiện đại.

Thứ ba, điều kiện xử lí dữ liệu hợp pháp

Việc xử lí dữ liệu sẽ hợp pháp khi và chỉ khi thuộc phạm vi áp dụng ít nhất một trong những điều sau được ghi nhận tại Điều 6.1 GDPR. GDPR khi xác định tính hợp pháp của xử lí dữ liệu dựa trên các yếu tố khác nhau: *Một là,* tôn trọng ý chí và lợi ích của chủ thể dữ liệu; *Hai là,* ghi nhận nghĩa vụ của người kiểm soát; *Ba là,* tôn trọng quyền lợi của bên thứ ba và lợi ích công cộng. Rõ ràng việc xác định các trường hợp xử lí dữ liệu hợp pháp đã được liệt kê tương đối toàn diện dựa trên góc nhìn về quyền và nghĩa vụ của các chủ thể khác nhau. Một trong những điểm tiến bộ của GDPR chính là xác định tính hợp pháp của dữ liệu đã quan tâm tới quyền lợi của chủ thể đặc biệt là trẻ em bởi trẻ em là chủ thể chưa có khả năng thể hiện ý chí, xác định mục đích, nhu cầu như người trưởng thành.

Thứ tư, quyền của chủ thể dữ liệu

Một là, quyền truy cập dữ liệu cá nhân: Chủ thể dữ liệu sẽ có quyền nhận được xác nhận từ người kiểm soát về việc dữ liệu cá nhân liên quan đến họ có đang được xử lí hay không và có quyền truy cập vào dữ liệu cá nhân, các thông tin tại Điều 15.1 GDPR. Qua quy định trên của GDPR cho thấy chủ thể dữ liệu hoàn toàn có quyền truy cập những thông tin về mục đích, nội dung, đích đến, thời gian lưu trữ, cải chính, xoá, quyết định tự động của nguồn dữ liệu sơ cấp và nguồn dữ liệu thứ cấp. Nhờ quyền truy cập dữ liệu này giúp chủ thể dữ liệu có được thông tin liên quan để có thể bảo vệ quyền lợi chính đáng của mình.

Hai là, quyền cải chính: Theo quy định tại Điều 16 GDPR, *"chủ thể dữ liệu sẽ có quyền được người kiểm soát sửa chữa dữ liệu cá nhân không chính xác liên quan đến họ một cách không chậm trễ. Có tính đến các mục đích của việc xử lí, chủ thể dữ liệu có quyền hoàn thiện dữ liệu cá nhân chưa hoàn chỉnh của mình, bao gồm cả việc cung cấp một báo cáo bổ sung".*

Ba là, quyền xoá - lãng quên: Chủ thể dữ liệu sẽ có quyền yêu cầu người kiểm soát xoá dữ liệu cá nhân liên quan đến họ mà không bị chậm trễ quá mức và người kiểm soát sẽ có nghĩa vụ xoá dữ liệu cá nhân không chậm trễ quá mức nếu thuộc một trong các căn cứ tại Điều 17.1 GDPR. Rõ ràng, việc xoá dữ liệu phụ thuộc vào ý chí của chủ thể dữ liệu nhằm bảo vệ quyền lợi của chủ thể hoặc vào ý chí của nhà nước nhằm bảo vệ lợi ích công cộng. Quyền được "lãng quên" (right to be forgotten) lần đầu tiên được chính thức ghi nhận trong GDPR là điểm tiến bộ nhằm bảo vệ quyền bí mật cá nhân và quyền tự do của chủ thể dữ liệu. Nói rộng hơn, quyền "lãng quên" là quyền cơ bản của con người[15].

Bốn là, quyền hạn chế xử lí: Chủ thể dữ liệu sẽ có quyền tiếp nhận giới hạn xử lí của bộ điều khiển khi áp dụng một trong các điều tại Điều 18(1) GDPR. GDPR đã dự liệu khá đầy đủ các trường hợp để chủ thể dữ liệu giới hạn xử lí dữ liệu của bộ điều khiển. Việc quy định này nhằm bảo vệ lợi ích của chủ thể dữ liệu khi họ có sự phản đối, không thừa nhận hoặc chờ xác minh hoặc lưu trữ để phục vụ cho vấn đề pháp lí.

Năm là, quyền đối với tính khả chuyển của dữ liệu: Chủ thể dữ liệu sẽ có quyền nhận dữ liệu cá nhân liên quan đến mình mà họ đã cung cấp cho người kiểm soát (ở định dạng có cấu trúc, được sử dụng phổ biến và máy có thể đọc được) và có quyền truyền những dữ liệu đó đến người kiểm soát khác mà không bị cản trở khi: theo quy định của GDPR và việc xử lí được thực hiện bằng các phương tiện tự động (Điều 20.1). Quy định này cho thấy chủ thể dữ liệu có quyền quyết định giao dữ liệu của mình cho các chủ thể khác nhau hay nói cách khác là chuyển dữ liệu lưu trữ cho người kiểm soát khác nhau. Tuy vậy, quyền này không phải là quyền tuyệt đối. Theo đó, việc chuyển dữ liệu cần phải tôn trọng lợi ích công cộng,

[15] Judgment of the Court (Grand Chamber), 13 May 2014. Case C-131/12: Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, EUR-Lex - 62012CJ0131 - EN - EUR-Lex (europa.eu), truy cập 15/8/2022.

lợi ích của người khác và việc thực thi quyền lực nhà nước (Điều 20.3, 20.4). Quy định này vừa đảm bảo quyền lợi của chủ thể dữ liệu mà vẫn hài hòa với lợi ích của các chủ thể liên quan.

Sáu là, quyền phản đối: Dựa trên cơ sở liên quan đến tình huống cụ thể của mình, chủ thể dữ liệu sẽ có quyền phản đối bất cứ lúc nào đối với việc xử lí dữ liệu cá nhân liên quan đến họ khi dữ liệu được xử lí nhằm đảm bảo lợi ích công cộng, người kiểm soát, hoặc bên thứ ba hoặc việc thực thi được trao quyền cho người kiểm soát (các điều 21.1., 6.1.e, 6.1.f). Rõ ràng, để bảo vệ dữ liệu cá nhân của mình, chủ thể dữ liệu hoàn toàn có quyền phản đối việc xử lí dữ liệu của họ khi dùng để tiếp thị trực tiếp, nghiên cứu, thống kê và xử lí nhằm đảm bảo lợi ích công cộng, người kiểm soát và bên thứ ba. Đây là một "phương thức" đưa ra nhằm đảm bảo cho chủ thể dữ liệu thể hiện ý chí của mình khi dữ liệu cá nhân của họ được xử lí vào những mục đích khác nhau.

Bảy là, quyền không ràng buộc với quyết định được hình thành tự động: Chủ thể dữ liệu sẽ có quyền không ràng buộc với một quyết định chỉ dựa trên quá trình xử lí tự động (bao gồm cả việc lập hồ sơ), mà quyết định này tạo ra những ảnh hưởng pháp lí liên quan đến chủ thể hoặc ảnh hưởngtương tự đáng kể đến chủ thể đó (Điều 22.1). Với công nghệ số nói chung và AI nói riêng phát triển mạnh mẽ, những quyết định được hình thành tự động thường xuyên xuất hiện. GDPR dự liệu và trao cho chủ thể dữ liệu có quyền "không ràng buộc" với quyết định hình thành tự động là thực sự cần thiết bởi vì những quyết định được hình thành tự động có thể không thể hiện đúng ý chí của chủ thể dữ liệu.

Thứ năm, nghĩa vụ của các bên liên quan tới dữ liệu cá nhân

Một là, người kiểm soát: Người kiểm soát phải thực hiện các biện pháp kỹ thuật và phương thức phù hợp để đảm bảo và có thể chứng minh rằng quá trình xử lí được thực hiện theo đúng quy định (Điều 24.1). Song song với các hoạt động xử lí dữ liệu, người kiểm soát phải thực hiện các chính sách bảo vệ dữ liệu thích hợp (Điều 24.2). Ngoài ra, người kiểm soát phải tuân thủ các quy tắc ứng xử đã được phê duyệt nêu tại Điều 40 hoặc các cơ chế chứng nhận đã được phê duyệt nêu tại Điều 42 GDPR (Điều 24.3). Người kiểm soát là chủ thể đóng vai trò quan trọng trong việc bảo vệ dữ liệu cá nhân. Vì vậy, việc quy định rõ trách nhiệm của chủ thể này là cần thiết, cụ thể về: biện pháp kĩ thuật, phương thức xử lí; chính sách bảo mật; quy tắc ứng xử và cơ chế chứng nhận. Theo đó, trách nhiệm của người kiểm soát càng cao; quy định về nghĩa vụ càng rõ ràng, chi tiết thì dữ liệu cá nhân càng được bảo vệ tốt.

Hai là, người xử lí: Người xử lí không được giao kết với người xử lí khác mà không có sự cho phép trước bằng văn bản cụ thể hoặc chung của người kiểm soát (Điều 28.1). Trong trường hợp được sự cho phép bằng văn bản chung, người xử lí phải thông báo cho người kiểm soát về bất kì dự kiến thay đổi nào liên quan đến việc bổ sung hoặc thay thế người xử lí để tạo cơ hội cho người kiểm soát phản đối những thay đổi đó (Điều 28.2).

Việc xử lí dữ liệu sẽ ràng buộc người xử lí đối với người kiểm soát về: đối tượng và thời gian xử lí, bản chất và mục đích của quá trình xử lí, loại dữ liệu cá nhân và các dạng chủ thể dữ liệu và nghĩa vụ và quyền của người kiểm soát (Điều 28.3). Rõ ràng, người xử lí tham gia vào quá trình xử lí dữ liệu bằng các biên pháp kĩ thuật và phương thức xử lí phù hợp nên đây là một mắt xích quan trọng trong việc bảo vệ dữ liệu cá nhân. Tóm lại, GDPR quy định về trường hợp nào cần người xử lí; quyền và nghĩa vụ của người xử lí; thay thế người xử lí. Những quy định này gián tiếp tác động tới bảo vệ dữ liệu cá nhân.

Ba là, nhân viên bảo vệ dữ liệu: Nhân viên bảo vệ dữ liệu được người kiểm soát và người xử lí chỉ định để bảo vệ dữ liệu trong các trường hợp được ghi nhận tại Điều 37.1. Nhân viên bảo vệ dữ liệu phải có ít nhất một trong các nhiệm vụ ghi nhận tại Điều 39.1. Nhân viên bảo vệ dữ liệu trong quá trình thực hiện nhiệm vụ của mình phải xem xét rủi ro liên quan đến hoạt động xử lí, có tính đến bản chất, phạm vi, bối cảnh và mục đích của việc xử lí (Điều 39.2). Để tránh việc dữ liệu cá nhân bị vi phạm trong quá trình xử lí bởi cơ quan công quyền hoặc xử lí dữ liệu trên quy mô lớn hoặc xử lí dữ liệu trong các hạng mục đặc biệt, việc tham gia của người bảo vệ dữ liệu là cần thiết. Rõ ràng, nhân viên bảo vệ dữ liệu là bên thứ ba khách quan thực hiện nhiều hoạt động khác nhau như giám sát, tư vấn, thông báo, hợp tác nhằm bảo vệ dữ liệu của chủ thể dữ liệu trong quá trình các cơ quan công quyền, người xử lí, người giám sát và những người liên quan.

Bốn là, cơ quan giám sát độc lập: Mỗi quốc gia thành viên sẽ quy định cho một hoặc nhiều cơ quan công quyền độc lập chịu trách nhiệm giám sát việc áp dụng Quy định này (Điều 51.1). Mỗi cơ quan giám sát có các quyền và nghĩa vụ sau: quyền điều tra, quyền uỷ quyền và tư vấn; quyền điều chỉnh quy định (Điều 58.1, 58.2, 58.3); nghĩa vụ báo cáo hoạt động hằng năm (Điều 59). Các báo cáo đó sẽ được chuyển đến Quốc hội, Chính phủ và các cơ quan chức năng khác theo chỉ định của pháp luật quốc gia thành viên và sẽ được cung cấp cho công chúng, cho Uỷ ban và cho Hội đồng châu Âu. Cơ quan giám sát - cơ quan bảo vệ dữ liệu và xử lí mọi vấn đề liên quan đến vi phạm dữ liệu do một công ti báo cáo, dàn xếp các yêu cầu truy cập chủ thể dữ liệu và cung cấp hướng dẫn giải thích các điều khoản GDPR cụ thể[16]. Cơ quan giám sát độc lập cũng tiến hành điều tra các công ti có trụ sở chính trong phạm vi quyền hạn của họ (Điều 77). GDPR có hạn chế khi chưa có quy định về cơ quan giám sát độc lập nào có thẩm quyền điều tra đối với công ti vi phạm ảnh hưởng tới nhiều chủ thể dữ liệu tại nhiều quốc gia thành viên.

Năm là, Hội đồng bảo vệ dữ liệu được thành lập như một cơ quan của Liên minh và có tư cách pháp nhân[17]. Hội đồng hoạt động độc lập với các nhiệm vụ: giám sát và đảm

[16] Daigle, B. and Khan, M. (2020), "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities", *Journal of International Commerce and Economics,* https://www.usitc.gov/journals, truy cập 16/8/2022.

[17] GDPR, Art. 68(1).

bảo việc áp dụng đúng GDPR; tư vấn cho Uỷ ban châu Âu; ban hành các hướng dẫn, khuyến nghị; kiểm tra theo yêu cầu của một trong các thành viên hoặc theo yêu cầu của Uỷ ban; đưa ra hướng dẫn cho các cơ quan giám sát;... (các điều 69.1, 70.1). Bên cạnh đó, Hội đồng sẽ lập một báo cáo hằng năm về việc bảo vệ các thể nhân liên quan đến khiếu nại trong Liên minh, ở các nước thứ ba và các tổ chức quốc tế nếu có liên quan. Báo cáo sẽ được công bố rộng rãi và được chuyển đến Nghị viện châu Âu, Hội đồng châu Âu và Uỷ ban châu Âu (Điều 71.1). Hội đồng bảo vệ dữ liệu được tạo ra để phân xử các quyết định mâu thuẫn giữa các cơ quan bảo vệ dữ liệu thành viên EU, đưa ra ý kiến và hướng dẫn về các điều khoản GDPR cụ thể và để giám sát rằng GDPR đang được áp dụng nhất quán trong EU[18]. Hội đồng bảo vệ dữ liệu là cơ quan sẽ giúp giải quyết những mâu thuẫn có thể phát sinh giữa EU với quốc gia thứ ba. Chính vì lẽ đó, Hội đồng là cơ quan quan trọng tham gia vào việc bảo vệ dữ liệu tại EU.

Thứ sáu, trách nhiệm pháp lí của chủ thể vi phạm

Một là, trách nhiệm bồi thường (Điều 82): Bất kì người nào bị thiệt hại vật chất hoặc phi vật chất do hành vi vi phạm GDPR đều có quyền được người kiểm soát hoặc người xử lí bồi thường thiệt hại. Bất kì người kiểm soát nào tham gia vào quá trình xử lí dữ liệu sẽ phải chịu trách nhiệm về thiệt hại do quá trình xử lí vi phạm GDPR này. Bên nhận gia công chỉ phải chịu trách nhiệm đối với thiệt hại do quá trình xử lí không tuân thủ các nghĩa vụ của GDPR đối với bên nhận gia công hoặc khi có hành vi vượt quá hoặc trái với hướng dẫn hợp pháp của người kiểm soát. Trường hợp có nhiều người kiểm soát và người xử lí tham gia và gây thiệt hại cho chủ thể dữ liệu, người kiểm soát và người xử lí phải chịu trách nhiệm bồi thường toàn bộ thiệt hại nhằm đảm bảo việc bồi thường hiệu quả cho chủ thể dữ liệu. Người đã bồi thường toàn bộ thiệt hại có quyền yêu cầu những người kiểm soát và người xử lí còn lại chịu trách nhiệm phần bồi thường tương ứng.

Hai là, xử phạt hành chính: Đối với người kiểm soát hoặc người xử lí cố ý hoặc do sơ xuất vi phạm một số quy định của GDPR thì bị phạt hành chính. Theo GDPR, tiền phạt cho các vi phạm nghiêm trọng nhất có thể lên tới 20 triệu euro (22 triệu đô la) hoặc 4% doanh thu toàn cầu (hoặc doanh thu hàng năm của một công ti trên toàn thế giới)[19]. Các quốc gia thành viên quy định xử phạt hành chính đối với hành vi vi phạm bảo vệ dữ liệu cá nhân và thông báo cho Uỷ ban Châu Âu. Trường hợp quốc gia thành viên không có quy định về phạt vi phạm hành chính, điều khoản xử phạt hành chính của GDPR có thể được áp dụng theo cách thức phạt tiền do cơ quan giám sát có thẩm quyền khởi xướng và do tòa án quốc gia có thẩm

[18] European Commission, "What is the European Data Protection Board (EDPB)?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en, truy cập 16/8/2022.

[19] Điều 83.5, 83.6 GDPR; Daigle, B. & Khan, M., tlđd.

quyền áp dụng, đồng thời đảm bảo rằng các biện pháp pháp lí đó có hiệu lực và có tác dụng tương đương với mức phạt hành chính của cơ quan giám sát (Điều 83.9).

Ba là, hình phạt (Điều 84): Các quốc gia thành viên sẽ đưa ra quy định về các hình phạt khác áp dụng đối với các hành vi vi phạm GDPR, cụ thể là các hành vi vi phạm không bị phạt hành chính theo Điều 83. Các quốc gia sẽ thực hiện tất cả các biện pháp cần thiết để đảm bảo rằng hình phạt được thực hiện. Các hình phạt như vậy sẽ có hiệu lực, tương xứng và có tính răn đe. Mỗi quốc gia thành viên sẽ thông báo cho Uỷ ban châu Âu các quy định của pháp luật quốc gia về hình phạt và bất kì sửa đổi tiếp theo nào ảnh hưởng đến chúng.

1.2. Tác động của pháp luật bảo vệ dữ liệu cá nhân của châu Âu

GDPR hướng tới bảo vệ công dân EU nhưng tác động của nó mang tính chất toàn cầu và ảnh hưởng đến bất kì tổ chức nào nhắm mục tiêu đến thị trường châu Âu hoặc cung cấp dịch vụ và có nhận dạng thông tin cá nhân về cư dân EU[20]. GDPR quy định rằng các tổ chức nên nhận được sự đồng ý của người dùng để thu thập dữ liệu và "thực hiện các biện pháp tổ chức và kỹ thuật phù hợp" để bảo vệ dữ liệu cá nhân của cư dân EU[21]. Với mục đích bảo vệ thông tin cá nhân của công dân EU, GDPR có tác động tới sự phát triển nền tảng công nghệ, AI và công nghệ mới, pháp luật và an ninh mạng trên phạm vi toàn cầu. Cụ thể: 1) GDPR tác động tới nền tảng công nghệ: Các công ti về công nghệ trên thế giới, muốn tiếp cận thị trường châu Âu cần tái cấu trúc lại các hệ thống hoặc nền tảng hiện có để giảm nguy cơ không tuân thủ GDPR[22]; 2) GDPR tác động tới AI: các công nghệ mới nổi như AI, chuỗi khối và điện toán đám mây là những phương tiện hữu hiệu để thúc đẩy hiệu suất và năng suất[23]. Tuy vậy, những quy định chặt chẽ của GDPR về xử lí dữ liệu có khả năng kìm hãm sự phát triển của công nghệ mới, ví dụ như: yêu cầu thuật toán ra quyết định phải được xem xét và giải thích bởi con người (Điều 13 và Điều 22) hoặc yêu cầu xoá dữ liệu (Điều 17). Bởi vì, quyết định là do AI tự ra quyết định và việc xoá dữ liệu sẽ ảnh hưởng tới các thuật toán của AI và có thể phá vỡ hoàn toàn AI đó. 3) GDPR xung đột với pháp luật các quốc gia ngoài EU mà dữ liệu chuyển qua: Các công ti công nghệ ở khắp nơi trên thế giới đang lưu trữ, xử lí lượng dữ liệu cá nhân lớn của công dân EU. Theo GDPR thì EU sẽ áp dụng luật riêng của mình trên lãnh thổ có chủ quyền của các nước khác[24]. Tuy vậy, pháp luật của các quốc gia nơi có dữ liệu được lưu trữ và xử lí có thể xung đột với GDPR. 4) GDPR ảnh hưởng đến an ninh mạng: GDPR dự kiến sẽ có tác động đến chính sách và thực tiễn an ninh mạng của các tổ chức vì nó yêu cầu các công ti thực

[20] Li, H. & Yu, L. & He, W. (2019), "The Impact of GDPR on Global Technology Development", *Journal of Global Information Technology Management*, Vol. 22(1), p. 1.

[21] Kaushik, S. & Wang, Y. (2018), "Data privacy: Demystifying the GDPR", https://ischool.syr.edu/data-privacy-demystifying-gdpr/, truy cập 16/8/2022.

[22] Li, H. & Yu, L. & He, W., tlđd, p. 2.

[23] Li, H. & Yu, L. & He, W., tlđd, p. 3.

[24] Bendiek, A. & Römer, M., tlđd, p. 40.

hiện các biện pháp phù hợp để bảo vệ dữ liệu cá nhân và quyền riêng tư của người tiêu dùng, đồng thời chống lại việc mất hoặc lộ dữ liệu[25]. Vì vậy, các công ti công nghệ cần đầu tư nhiều hơn vào các chương trình đào tạo và giáo dục an ninh mạng[26].

2. Pháp luật Việt Nam về bảo vệ dữ liệu cá nhân - Thực trạng và kiến nghị hoàn thiện

2.1. Thực trạng pháp luật Việt Nam về bảo vệ dữ liệu cá nhân

Ngày 26/01/2021, Việt Nam ban hành Quyết định số 127/QĐ-TTg về Chiến lược quốc gia về nghiên cứu, phát triển và ứng dụng AI đến năm 2030 với mục tiêu cụ thể như sau: Đến năm 2025, Việt Nam nằm trong nhóm 5 nước dẫn đầu trong khu vực ASEAN và nhóm 60 nước dẫn đầu trên thế giới về nghiên cứu, phát triển và ứng dụng AI (mục II.1). Đến năm 2030, Việt Nam nằm trong nhóm 4 nước dẫn đầu trong khu vực ASEAN và nhóm 50 nước dẫn đầu trên thế giới về nghiên cứu, phát triển và ứng dụng AI (mục II.2). Để đạt được mục tiêu phát triển AI này thì nguy cơ xâm phạm đến dữ liệu cá nhân ở Việt Nam sẽ cao.

Tuy vậy, đến nay Việt Nam chưa có đạo luật hoặc văn bản pháp lí riêng biệt quy định về bảo vệ dữ liệu cá nhân mà vấn đề này được ghi nhận rải rác ở các văn bản pháp luật riêng. Theo quy định tại Điều 21 Hiến pháp năm 2013, mọi người có quyền bất khả xâm phạm về đời sống riêng tư, trong đó bao gồm cả bí mật cá nhân, bí mật gia đình, bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác. Với quy định này, Hiến pháp Việt Nam xác định bảo vệ quyền về đời sống riêng tư cũng chứa đựng bảo vệ dữ liệu cá nhân. Các văn bản pháp luật khác đã cụ thể hoá về bảo vệ quyền về đời sống riêng tư như: Bộ luật Dân sự, Bộ luật Hình sự, Bộ luật Tố tụng hình sự, Bộ luật Tố tụng dân sự, Luật Xuất bản, Luật Phòng, chống HIV/AID,... Một số văn bản pháp luật của Việt Nam ghi nhận rõ hơn về bảo vệ dữ liệu cá nhân như Luật an toàn thông tin mạng, Luật an ninh mạng, Luật công nghệ thông tin,... Cụ thể:

Thứ nhất, về trách nhiệm của chủ thể xử lí thông tin trong việc bảo vệ dữ liệu cá nhân.

Một là, Luật An toàn thông tin mạng dành Mục 2 gồm 5 điều (từ điều 16 đến điều 22) để quy định về bảo vệ thông tin cá nhân. Theo đó, chủ thể xử lí thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lí; xây dựng và công bố công khai biện pháp xử lí, bảo vệ thông tin cá nhân (khoản 2, 3 Điều 16). Chủ thể xử lí thông tin cá nhân có trách nhiệm thu thập thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng thông tin đó; sử dụng thông tin đúng mục đích; không được cung cấp, chia sẻ, phát tán thông tin cá nhân mà mình đã thu thập, tiếp cận, kiểm soát cho bên thứ ba, trừ trường hợp luật có quy định khác (khoản 1 Điều 17). Ngoài ra, chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lí

[25] Li, H. & Yu, L. & He, W., tlđd, p. 3.

[26] Withey, V. (2018), "The impact of GDPR on the technology sector", https://www.grcworldforums.com/gdpr/the-impact-of-gdpr-on-the-technology-sector/152.article, truy cập 16/8/2022.

thông tin cá nhân cập nhật, sửa đổi, huỷ bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba (khoản 1 Điều 17). Tổ chức, cá nhân xử lí thông tin cá nhân phải huỷ bỏ thông tin cá nhân đã được lưu trữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ và thông báo cho chủ thể thông tin cá nhân biết, trừ trường hợp pháp luật có quy định khác (khoản 1 Điều 17). Các quy định nói trên của Luật An toàn thông tin mạng Việt Nam tương đồng với những quy định của GDPR về bảo vệ thông tin cá nhân.

Hai là, Luật Công nghệ thông tin: Tổ chức, cá nhân tham gia phát triển công nghệ thông tin có trách nhiệm bảo đảm quyền và lợi ích hợp pháp của chủ sở hữu cơ sở dữ liệu và không gây cản trở cho việc sử dụng cơ sở dữ liệu đó khi thực hiện hành vi tái sản xuất, phân phối, quảng bá, truyền đưa, cung cấp nội dung hợp thành cơ sở dữ liệu đó (điểm b khoản 2 Điều 9). Việc thu thập, xử lí va ứng dụng thông tin cá nhân trên môi trường mạng phải được sự đồng ý của cá nhân đó. Chủ thể thu thập, xử lí và ứng dung thông tin có trách nhiệm: Thông báo cho người đó biết về hình thức, phạm vi, địa điểm và mục đích của việc thu thập, xử lí và sử dụng thông tin cá nhân của người đó; sử dụng đúng mục đích thông tin cá nhân thu thập được và chỉ lưu trữ những thông tin đó trong một khoảng thời gian nhất định theo quy định của pháp luật hoặc theo thoả thuận giữa hai bên; tiến hành các biện pháp quản lí, kĩ thuật cần thiết để bảo đảm thông tin cá nhân không bị mất, đánh cắp, tiết lộ, thay đổi hoặc phá huỷ; tiến hành ngay các biện pháp cần thiết khi nhận được yêu cầu kiểm tra lại, đính chính hoặc huỷ bỏ theo quy định của pháp luật; không được cung cấp thông tin cá nhân của người khác cho bên thứ ba, trừ trường hợp pháp luật có quy định khác (khoản 2 Điều 21, khoản 2 Điều 22). Qua các quy định nêu trên cho thấy, Luật Công nghệ thông tin Việt Nam tương đồng với những quy định của GDPR về bảo vệ thông tin cá nhân.

Ba là, Luật An ninh mạng: Chủ quản hệ thống thông tin có trách nhiệm triển khai biện pháp quản lí, kĩ thuật để phòng ngừa, phát hiện, ngăn chặn, phối hợp xử lí hành vi gián điệp mạng, xâm phạm bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này (điểm b, c khoản 2 Điều 17). Doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm áp dụng các giải pháp kĩ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp xảy ra hoặc có nguy cơ xảy ra sự cố lộ, lọt, tổn hại hoặc mất dữ liệu thông tin người sử dụng, cần lập tức đưa ra giải pháp ứng phó, đồng thời thông báo đến người sử dụng (điểm c khoản 1 Điều 41). Những quy định này của Luật An ninh mạng Việt Nam tương đồng với quy định của GDPR về bảo vệ dữ liệu cá nhân.

Thứ hai, một số văn bản quy định về trách nhiệm pháp lí đối với chủ thể vi phạm dữ liệu cá nhân: 1) Trách nhiệm bồi thường thiệt hại: Chủ thể gây thiệt hại do vi phạm

quy định về bảo vệ quyền về đời sống riêng tư nói chung và dữ liệu cá nhân nói riêng được quy định trong Bộ luật Dân sự Việt Nam và các luật chuyên ngành liên quan; 2) Trách nhiệm hành chính: Theo Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử, mức phạt cao nhất là 70 triệu đồng đối với hành vi vi phạm quy định về bảo đảm an toàn thông tin cá nhân trên mạng (Điều 86); 3) Trách nhiệm hình sự: Đối với tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông, người phạm tội có thể bị phạt cao nhất đến 200 triệu đồng (Điều 288 Bộ luật Hình sự Việt Nam năm 2015, sửa đổi năm 2017). Rõ ràng, các loại trách nhiệm pháp lí được áp dụng đối với chủ thể vi phạm theo pháp luật Việt Nam là tương đồng với GDPR. Tuy vậy, mức phạt hành chính và hình sự áp dụng đối với chủ thể vi phạm là khá thấp so với quy định của GDPR (lên tới 20 triệu euro).

Tóm lại, quy định về bảo vệ dữ liệu cá nhân của Việt Nam khá tương đồng với quy định của GDPR. Tuy vậy, hệ thống các quy định của Việt Nam còn có những bất cập sau: *Một là*, các quy định nằm rải rác ở nhiều văn bản khác nhau nên thiếu tính hệ thống và chưa điều chỉnh một cách toàn diện những quan hệ phát sinh nhằm bảo vệ dữ liệu cá nhân[27]. Nói cách khác, Việt Nam chưa có văn bản pháp luật riêng về bảo vệ dữ liệu cá nhân. *Hai là*, các quy định của pháp luật Việt Nam hiện hành còn thiếu và chưa cụ thể. Có rất nhiều quy định chỉ mang tính nguyên tắc, định hướng nên gây khó khăn trong quá trình áp dụng[28]. *Ba là*, trách nhiệm pháp lí của chủ thể vi phạm về dữ liệu cá nhân theo pháp luật Việt Nam còn khá nhẹ, chưa đảm bảo tính răn đe[29]. *Bốn là,* Việt Nam chưa có quy định về thành lập và thẩm quyền của cơ quan giám sát bảo vệ dữ liệu cá nhân.

2.2. Giải pháp, kiến nghị hoàn thiện pháp luật Việt Nam về bảo vệ dữ liệu cá nhân

Với chiến lược phát triển AI đến năm 2030 của Việt Nam được nêu ở trên cho thấy Việt Nam đã, đang và sẽ phát triển AI mạnh mẽ. Sự phát triển AI sẽ kéo theo yêu cầu bảo vệ dữ liệu cá nhân. Hệ thống pháp luật Việt Nam hiện hành chưa quy định một cách toàn diện và phù hợp đối với chủ thể vi phạm dữ liệu cá nhân. Từ thực trạng pháp luật Việt Nam, so sánh và tham khảo quy định bảo vệ dữ liệu của châu Âu (GDPR), tác giả đề xuất một số giải pháp và kiến nghị sau:

Thứ nhất, hệ thống hóa thành một văn bản pháp luật riêng về bảo vệ dữ liệu cá nhân. Nên chăng, Việt Nam xây dựng Luật Bảo vệ dữ liệu với những nội dung chính tham khảo GDPR, cụ thể: 1) Chủ thể dữ liệu được bảo vệ: cá nhân công dân Việt Nam

[27] Vũ Công Giao, Lê Trần Như Tuyên (2020), "Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam", *Tạp chí Nghiên cứu lập pháp*, 9 (209), http://lapphap.vn/Pages/TinTuc/210546/Bao-ve-quyen-doi-voi-du-lieu-ca-nhan-trong-phap-luat-quoc-te--phap-luat-o-mot-so-quoc-gia-va-gia-tri-tham-khao-cho-Viet-Nam.html, truy cập 17/8/2022.

[28] Vũ Công Giao, Lê Trần Như Tuyên, tlđd.

[29] Vũ Công Giao, Lê Trần Như Tuyên, tlđd.

hoặc những người đang cư trú tại Việt Nam. 2) Đối tượng bảo vệ: dữ liệu vị trí, số nhận dạng trực tiếp và các dạng thông tin khác có thể được sử dụng để xác định chủ thể dữ liệu một cách trực tiếp hoặc gián tiếp, ngoài dữ liệu nhận dạng cổ điển như tên và số nhận dạng của cá nhân. 3) Các nguyên tắc bảo vệ dữ liệu: hợp pháp, công khai, minh bạch, đúng mục đích, giới hạn mục đích,... 4) Quyền chủ thể dữ liệu: truy cập, chuyển dữ liệu, điều chỉnh, xoá, lãng quên,... 5) Nhiệm vụ và quyền hạn của các chủ thể bảo vệ dữ liệu: người kiểm soát, người xử lí, người bảo vệ dữ liệu,... 6) Nhiệm vụ quyền hạn của cơ quan bảo vệ dữ liệu: Cơ quan giám sát bảo vệ giữ liệu quốc gia. 7) Trách nhiệm pháp lí do vi phạm bảo vệ dữ liệu: bồi thường thiệt hại, hành chính và hình phạt. 8) Các quy định liên quan khác.

Thứ hai, thành lập cơ quan giám sát xử lí dữ liệu (cơ quan bảo vệ dữ liệu) chuyên trách. Các quốc gia thuộc EU cũng thành lập các cơ quan chuyên trách để bảo vệ dữ liệu như: Latvia thành lập cơ quan thanh tra nhà nước về dữ liệu Latvia; Tây Ban Nha thành lập Cơ quan bảo vệ dữ liệu; Pháp thành lập Uỷ ban quốc gia về tin học và tự do; Bỉ thành lập Uỷ ban bảo mật dữ liệu,...[30] Việc thành lập cơ quan bảo vệ dữ liệu độc lập giúp hoạt động giám sát, bảo vệ dữ liệu trong nước đạt hiệu quả cao. Thêm vào đó, cơ quan bảo vệ dữ liệu này là đầu mối hợp tác với các cơ quan bảo vệ dữ liệu của các quốc gia khác trong việc giám sát xử lí dữ liệu ở nước ngoài nhưng liên quan đến dữ liệu của công dân quốc gia mình. Chính vì lẽ đó, Việt Nam nên thành lập cơ quan bảo vệ dữ liệu độc lập thuộc hệ thống cơ quan thanh tra hoặc thuộc Bộ khoa học công nghệ.

Thứ ba, những quy định về bảo vệ dữ liệu cá nhân hiện được quy định trong các luật như Luật An ninh mạng, Luật An toàn thông tin mạng, Luật Công nghệ thông tin, Luật Bảo vệ quyền lợi người tiêu dùng,... sẽ được pháp điển hoá vào quy định của Luật Bảo vệ dữ liệu Việt Nam.

Thứ tư, nâng mức xử phạt hành chính và hình sự đối với chủ thể có hành vi vi phạm dữ liệu cá nhân. Bởi vì, những vi phạm trong lĩnh vực công nghệ nói chung và AI nói riêng về bảo vệ dữ liệu cá nhân có tác động rất lớn đến đời sống của chủ thể dữ liệu và đến trật tự công cộng. Do đó, nâng mức xử phạt hành chính và hình sự đối với hành vi vi phạm này là thực sự cần thiết để trừng phạt đối với chủ thể vi phạm và răn đe đối với chủ thể khác./.

[30] European Data Protection Board - EDPB, "Our members", https://edpb.europa.eu/about-edpb/about-edpb/members_en, truy cập 17/8/2022.

TÀI LIỆU THAM KHẢO

1. Arora, S. & Athavale, V. & Maggu, H. & Agarwal, A. (2021), "Artificial Intelligence and Virtual Assistant - Working Model", *Mobile Radio Communications and 5G Networks (Nikhil Marriwala, C. C. Tripathi, Dinesh Kumar, Shruti Jain Edn)*, Springer.
2. Bendiek, A.t & Römer, M. (2019), "Externalizing Europe: the global effects of European data protection", *Digital Policy, Regulation and Governance*, Vol. 21, Iss. 1.
3. Bhattad, P. & Jain, V. (2020), "Artificial Intelligence in Modern Medicine - The

Evolving Necessity of the Present and Role in Transforming the Future of Medical Care", *Cureus*, 12(5).

4. Brill, T. & Munoz, L. & Miller, R. (2019), "Siri, Alexa, and other digital assistants: a study of customer satisfaction with artificial intelligence applications", *Journal of Marketing Management*, 35.2019, DOI: 10.1080/0267257X.2019.1687571.
5. Chaudhry, I. A. & Shami, M. & Khan, A. (2004), "Manufacturing Applications of Artificial Intelligence", *Journal of Engineering and Applied Sciences*, 23.
6. Daigle, B. and Khan, M. (2020), "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities", *Journal of International Commerce and Economics,* https://www.usitc.gov/journals
7. Hoffmann-Riem, W. (2020), "Artificial Intelligence as a Challenge for Law and Regulation", In: *Regulating Artificial Intelligence (Wischmeyer T., Rademacher T. (eds))*, Springer, Cham.
8. Kaplan, J. (2016), *Artificial intelligence*, Oxford University Press, New York.
9. Kaushik, S. & Wang, Y. (2018), "Data privacy: Demystifying the GDPR", 2018, https://ischool.syr.edu/data-privacy-demystifying-gdpr/
10. Li, H. & Yu, L. & He, W. (2019), "The Impact of GDPR on Global Technology Development", *Journal of Global Information Technology Management*, Vol. 22(1).
11. Mazurek, G. & Małagocka, K. (2019), "Are we down to zero-one code? Perception of privacy and data protection in the context of the development of artificial intelligence", *Journal of Management Analytics*, Vol.6 (4).
12. Page, L. C., & Gehlbach, H. (2017), "How an Artificially Intelligent Virtual Assistant Helps Students Navigate the Road to College", *AERA Open*, 3(4).
13. Soni, N. & Sharma, E. & Singh, N. & Kapoor, A. (2020), "Artificial Intelligence in Business: From Research and Innovation to Market Deployment", *Procedia Computer Science,* 167.
14. Roll, I.; Wylie, R. (2016), "Evolution and revolution in artificial intelligence in education", *Int. J. Artif. Intell. Education*, 26.
15. Vũ Công Giao, Lê Trần Như Tuyên (2020), "Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam", *Tạp chí Nghiên cứu lập pháp*, 9(209), http://lapphap.vn/Pages/TinTuc/210546/Bao-ve-quyen-doi-voi-du-lieu-ca-nhan-trong-phap-luat-quoc-te--phap-luat-o-mot-so-quoc-gia-va-gia-tri-tham-khao-cho-Viet-Nam.html
16. Withey, V. (2018), "The impact of GDPR on the technology sector", https://www.grcworldforums.com/gdpr/the-impact-of-gdpr-on-the-technology-sector/152.article
17. Woschank, M.; Rauch, E.; Zsifkovits, H. (2020), "A Review of Further Directions for Artificial Intelligence, Machine Learning, and DeepLea rning in Smart Logistics", *Sustainability*, 12.