SƠ LƯỢC VỀ LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA VIỆT NAM

Luật sư Nguyễn Đức Hiếu, bà Phạm Thanh Mai, ông Đỗ Phương Khoa
Global Vietnam Lawyers Law LLC

I. Giới thiệu

"Dữ liệu cá nhân" thu hút nhiều sự chú ý và đang là chủ đề của nhiều cuộc tranh biện pháp lý trên toàn thế giới.

Nếu việc bảo vệ dữ liệu cá nhân bị lơi lỏng sẽ tạo điều kiện cho hành vi trộm cắp danh tính, gian lận, lừa đảo, v.v., nhưng bảo vệ quá chặt chẽ sẽ gây khó khăn cho sự phát triển doanh nghiệp và cũng sẽ ngăn cản Việt Nam đạt được các mục tiêu xã hội có ích, như trong lĩnh vực an toàn, y tế, nghiên cứu khoa học[1]. Khi pháp luật Việt Nam về bảo vệ dữ liệu cá nhân vẫn còn ở giai đoạn sơ khởi và dường như đang tiến theo con đường của EU, cùng với nhiều sự thay đổi lớn sắp diễn ra, các doanh nghiệp có thể sẽ cần phải thường xuyên cập nhật vấn đề pháp lý trong lĩnh vực này.

Mục tiêu của bài viết này là cập nhật cho các doanh nghiệp nắm bắt sự tiến triển của các quy định pháp luật liên quan, với trọng tâm là Nghị định 13/2023 về bảo vệ dữ liệu cá nhân, được Chính phủ Việt Nam ban hành vào ngày 17 tháng 4 năm 2023 ("**Nghị định 13/2023**). Đây là văn bản pháp lý mới nhất tính đến thời điểm hiện tại của bài viết này, mà từ văn bản này các doanh nghiệp có thể tìm hiểu dữ liệu cá nhân ở Việt Nam đang được bảo vệ như thế nào.

II. Tóm tắt về cách hoạt động của pháp luật bảo vệ dữ liệu cá nhân

Nghị định 13/2023 đã được soạn thảo để tập trung vào cách thức bảo vệ dữ liệu cá nhân trong suốt quá trình thu thập, xử lý, lưu trữ, sử dụng và thậm chí xóa dữ liệu trên không gian mạng. Do đó, bài viết này sẽ nêu tóm tắt về các đối tượng, mà không phải là chủ thể dữ liệu (như được định nghĩa bên dưới), có liên quan đến và phải tuân thủ Nghị định 13/2023 và nêu đặc điểm của bảo vệ dữ liệu cá nhân theo Nghị định này là gì.

1. Đối tượng nào phải tuân thủ theo Nghị định 13/2023?

Nghị định 13/2023 có lẽ được truyền cảm hứng và phát triển từ Quy Định Chung Về Bảo Vệ Dữ Liệu Của EU ("**GDPR**"), mặc dù ở một mức độ nào đó, nó được điều chỉnh để phù hợp với bối cảnh và điều kiện kinh tế - xã hội của Việt Nam. Vì vậy, những đối

[1] Orly Lobel, "The Problem With Too Much Data Privacy" (Time, 2022) <https://time.com/6224484/data-privacy-problem/>, truy cập ngày 26 tháng 3 năm 2024.

tượng được quy định tại GDPR cũng có thể được tìm thấy trong Nghị định 13/2023, cụ thể là:

- "**Chủ thể dữ liệu**" đề cập đến một cá nhân được dữ liệu cá nhân phản ánh[2]. Trong ngữ cảnh của một doanh nghiệp / kinh doanh, chủ thể dữ liệu có thể là nhân viên, ứng viên tìm việc, khách hàng của doanh nghiệp, và đối tác kinh doanh; người sử dụng lao động là một cá nhân cũng có thể được coi là một "chủ thể dữ liệu". Khi dữ liệu cá nhân được thu thập, ghi, sao chép, chia sẻ, tiết lộ hoặc bất kỳ hoạt động tương tự nào, nó được coi là "**xử lý dữ liệu cá nhân**".

- "**Bên kiểm soát dữ liệu cá nhân**" đề cập đến một tổ chức hoặc cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân (ví dụ: doanh nghiệp lưu trữ dữ liệu cá nhân hợp pháp được thu thập từ khách hàng của họ).

- "**Bên xử lý dữ liệu cá nhân**" đề cập đến một tổ chức hoặc cá nhân xử lý dữ liệu cá nhân thay mặt cho bên kiểm soát dữ liệu cá nhân thông qua một thỏa thuận (ví dụ: nhà cung cấp dịch vụ lưu trữ dữ liệu đám mây). Bên xử lý dữ liệu cá nhân cũng có thể đảm nhận vai trò của "người kiểm soát dữ liệu cá nhân" và bên xử lý dữ liệu đó được gọi là "**Bên kiểm soát và xử lý dữ liệu cá nhân**" (ví dụ: các doanh nghiệp đảm nhận các chức năng lưu trữ và xử lý). Khái niệm về bên có vai trò kép này khác biệt so với GDPR, nhưng chưa rõ tại sao Nghị định 13/2023 lại đưa khái niệm nào vào.

2. Bảo vệ dữ liệu cá nhân được quy định như thế nào theo Nghị định 13/2023?

Dưới đây là một số đặc điểm quan trọng:

(a) Quyền của chủ thể dữ liệu

Chủ thể dữ liệu có quyền (i) được biết về hoạt động xử lý dữ liệu cá nhân của mình, (ii) đồng ý cho phép xử lý, (iii) truy cập dữ liệu cá nhân, (iv) rút lại sự đồng ý, (v) xóa dữ liệu cá nhân, (vi) hạn chế xử lý dữ liệu, (vii) yêu cầu cung cấp dữ liệu cá nhân của riêng họ, (viii) phản đối việc xử lý, (ix) khiếu nại, tố cáo và khởi kiện, (x) yêu cầu bồi thường thiệt hại và (xi) tự bảo vệ.[3]

---

[2] "**Dữ liệu cá nhân**", được định nghĩa là " *thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể.* " Nghị định 13/2023 phân loại "dữ liệu cá nhân" thành 02 nhóm như Điều 9 và 10 của GDPR: "**dữ liệu cá nhân cơ bản**" (ví dụ: tên, ngày &; nơi sinh, số điện thoại, số chứng minh nhân dân, số định danh cá nhân, v.v.) và "**dữ liệu cá nhân nhạy cảm**" (ví dụ: thông tin sức khỏe, thông tin về đặc điểm di truyền, thông tin về tội phạm, thông tin liên quan đến ngân hàng và vị trí cá nhân).

[3] - Điều 9 Nghị định 13/2023

Nghị định 13/2023 nhấn mạnh về cơ chế đồng ý. Đối với các doanh nghiệp, việc tìm kiếm sự đồng ý minh thị và chính xác từ các chủ thể dữ liệu cho bất kỳ giai đoạn nào mà dữ liệu cá nhân của họ được xử lý là cần thiết. Tuy nhiên, phương thức mà qua đó sự đồng ý có thể được đưa ra hoặc được tiếp nhận một cách đúng đắn lại không đơn giản như thoạt nhìn, không phải vì các doanh nghiệp không có đủ năng lực để thiết kế một hệ thống khả thi, mà là vì chưa có tiêu chuẩn tuân thủ rõ ràng trong Nghị định 13/2023.

Nghị định 13/2023 cũng quy định một số trường hợp ngoại lệ khi không cần sự đồng ý của chủ thể dữ liệu: (i) trong trường hợp khẩn cấp hoặc theo yêu cầu của pháp luật, (ii) dữ liệu cá nhân được thu thập từ hoạt động ghi âm, ghi hình tại nơi công cộng.[4] Đối với (i) dữ liệu cá nhân của người bị tuyên bố mất tích hoặc đã chết và (ii) dữ liệu cá nhân của trẻ em, Nghị định 13/2023 cũng yêu cầu phải có sự đồng ý của (các) thành viên gia đình của các đối tượng này khi xử lý dữ liệu cá nhân của họ.[5]

Một lần nữa, cần có một bộ tiêu chuẩn cho cơ chế đồng ý hoạt động và hi vọng sẽ được các nhà làm luật quy định trong tương lai. Trong khi đó, các doanh nghiệp nên chủ động trong việc đưa ra một nền tảng tương tác dễ truy cập để các chủ thể dữ liệu tương tác với các doanh nghiệp, theo đó cơ chế đồng ý có thể diễn ra. GDPR là văn bản có ảnh hưởng đến các nhà làm luật và các cơ quan quản lý Việt Nam cũng như được lấy làm tiêu chuẩn, vì vậy sẽ là hợp lý nếu các doanh nghiệp tạo ra cơ chế đồng ý phù hợp với các tiêu chuẩn liên quan được quy định tại GDPR, dù cơ chế này đang hiện hữu hay được áp dụng cho Việt Nam.

(b) Yêu cầu thông báo

Bên Kiểm soát và/hoặc Bên Xử lý Dữ liệu Cá nhân có nghĩa vụ thực hiện yêu cầu này khi phát hiện ra sự cố hoặc hành vi vi phạm dữ liệu cá nhân. Trong trường hợp này, phải thông báo bằng văn bản (bản cứng hoặc bản mềm), cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) về hành vi vi phạm, sự cố đó trong vòng 72 giờ (hoặc muộn hơn nếu có lý do).

Thông báo được thực hiện theo Mẫu số 03 tại Phụ lục của Nghị định 13/2023.

(c) Đánh giá tuân thủ

Doanh nghiệp được yêu cầu lập và lưu giữ hồ sơ phục vụ công tác kiểm tra/đánh giá của cơ quan có thẩm quyền. Có hai loại hồ sơ mà doanh nghiệp bắt buộc phải chuẩn bị và lưu giữ, đó là: (i) Hồ sơ đánh giá tác động xử lý dữ

[4] Điều 17, Điều 18 Nghị định 13/2023
[5] Điều 19, 20 Nghị định 13/2023

liệu cá nhân và (ii) Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài (áp dụng đối với trường hợp dữ liệu cá nhân được chuyển ra nước ngoài). Các Hồ sơ này phải luôn được chuẩn bị và có sẵn để nộp trong vòng 60 ngày kể từ ngày dữ liệu cá nhân được xử lý và bất cứ khi nào cơ quan có thẩm quyền yêu cầu.[6]

Đáng chú ý, doanh nghiệp được chuyển dữ liệu cá nhân của công dân Việt Nam ra nước ngoài với điều kiện đã (i) lập Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài, và (ii) thông báo cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) về việc chuyển dữ liệu và thông tin liên lạc của tổ chức, cá nhân phụ trách việc chuyển dữ liệu đó bằng văn bản sau khi việc chuyển dữ liệu diễn ra thành công.[7]

(d) Nhân viên bảo vệ dữ liệu ("DPO") tại doanh nghiệp

Thông tin liên hệ của DPO sẽ được đưa vào các hồ sơ đánh giá nộp cho cơ quan có thẩm quyền như đã nêu tại mục (c) ở trên.

Nghị định 13/2023 không yêu cầu DPO phải là nhân viên của doanh nghiệp, nhưng nếu có yêu cầu, doanh nghiệp sẽ cần có ít nhất một nhân viên đảm nhận vai trò của DPO.

3. Hậu quả của việc không tuân thủ là gì?

Bên cạnh các rủi ro kỹ thuật như rò rỉ dữ liệu và đánh cắp danh tính và rủi ro về tiền bạc như mã độc tống tiền, việc không tuân thủ các quy định về dữ liệu cá nhân cũng có thể gây khó khăn cho các doanh nghiệp. Tuy nhiên, hiện nay, chưa có chế tài và xử phạt hành chính đối với hành vi không tuân thủ Nghị định 13/2023 đã được đề cập, trong khi vấn đề này vẫn đang được thảo luận, xem xét.

Do các nhà làm luật Việt Nam vốn có xu hướng áp dụng mô hình dựa trên GDPR, nên có khả năng họ sẽ thiết kế các biện pháp phạt vi phạm hành chính tương đồng với GDPR ở một vài điểm.

III. Kết luận:

Dự đoán rằng các nhà làm luật Việt Nam sẽ tiếp tục cố gắng áp dụng các nguyên tắc của GDPR trong việc xây dựng khung pháp lý của riêng mình để bảo đảm và bảo vệ dữ liệu cá nhân cá nhân. Điều này có nghĩa là các doanh nghiệp đã quen thuộc với GDPR có thể sẽ thấy không quá khó khăn để tuân thủ các quy định bảo vệ dữ liệu cá nhân tại Việt Nam.

---

[6] Điều 24 và 25 Nghị định 13/2023

[7] - Điều 25 Nghị định 13/2023

Mặc dù vậy, sự xuất hiện của trí tuệ nhân tạo, thường được gọi là AI, đã đặt ra những thách thức mới đối với việc bảo vệ dữ liệu cá nhân. Vì AI hoạt động dựa trên cách dữ liệu được nhập vào, xử lý và tạo ra, để đưa ra kết quả theo yêu cầu của người dùng, điều này gây ra các lo ngại xung quanh việc liệu dữ liệu cá nhân có được sử dụng để "nuôi" máy AI mà chủ thể dữ liệu không biết, và nếu có, luật bảo vệ dữ liệu cá nhân sẽ giải quyết những lo ngại đó như thế nào. Có lẽ các nhà làm luật Việt Nam đã bắt đầu nghiên cứu soạn thảo và cập nhật các văn bản pháp lý để kiểm soát AI cùng với dữ liệu cá nhân như một nỗ lực thu hẹp khoảng cách giữa luật pháp và công nghệ, hứa hẹn những thay đổi đáng kể đối với pháp luật bảo vệ dữ liệu cá nhân của Việt Nam trong tương lai.