HOÀN THIỆN KHUNG PHÁP LÝ VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN KHÔNG GIAN MẠNG: KINH NGHIỆM TỪ CHÂU ÂU

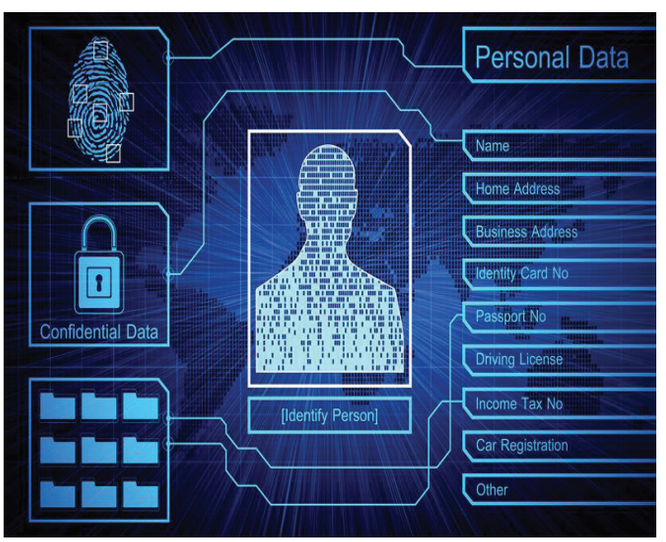
Đàm Trung Việt[1], Phí Công Thường[2]

[1]Trường Đại học Kinh tế, Đại học Đà Nẵng
[2]Bộ Khoa học và Công nghệ

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ trên toàn cầu, việc bảo vệ dữ liệu cá nhân không chỉ là yêu cầu pháp lý, mà còn là nền tảng để xây dựng niềm tin số, đảm bảo quyền công dân và thúc đẩy kinh tế số phát triển bền vững. Tại Việt Nam, hai Nghị quyết trọng điểm của Bộ Chính trị là Nghị quyết số 52-NQ/TW ngày 27/9/2019 và Nghị quyết số 57-NQ/TW 22/12/2024 đã xác lập những định hướng chiến lược đầy tham vọng, mở đường cho việc hoàn thiện hệ thống pháp luật về bảo vệ dữ liệu cá nhân. Những phân tích của bài báo sẽ góp phần hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân trên không gian mạng từ kinh nghiệm quốc tế.

Thực trạng khung pháp lý về bảo vệ dữ liệu cá nhân trên không gian mạng tại Việt Nam

Dữ liệu cá nhân 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 thể, hoặc giúp xác định một con người cụ thể. Bảo vệ dữ liệu cá nhân bao gồm bảo vệ dữ liệu cá nhân cơ bản và bảo vệ dữ liệu cá nhân nhạy cảm.



Tổng quan về dữ liệu cá nhân.

Hiện nay, Việt Nam đã có các quy định về bảo vệ dữ liệu cá nhân trên không gian mạng và đã được thực thi. Tuy nhiên, vẫn còn tồn tại không ít bất cập cần được quan tâm khắc phục trong thời gian tới, cụ thể là:

Thứ nhất, hiệu lực pháp lý của văn bản còn thấp. Hiện nay, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân (Nghị định số 13/2023/NĐ-CP) đang là văn bản pháp luật điều chỉnh chuyên biệt về bảo vệ dữ liệu cá nhân, nhưng về hiệu lực pháp lý thì đây mới chỉ là văn bản dưới luật. Trong khi đó, thế giới số vẫn đang vận hành và xâm nhập vào đời sống thường nhật, việc Nghị định số 13/2023/NĐ-CP điều chỉnh lâu dài trong đời sống kinh tế - xã hội là chưa phù hợp. Phần lớn các nước trên thế giới và trong khu vực đã có "văn bản luật" để điều chỉnh về bảo vệ dữ liệu cá nhân, tuy vậy ở nước ta hiện nay mới chỉ đang là Nghị định.

Trong khi, Nghị định là văn bản quy phạm pháp luật được Chính phủ ban hành trong quá trình hành pháp, chứ không phải là văn bản quy phạm pháp luật được Quốc hội thông qua. Điều này thể hiện rằng, Nghị định số 13/2023/NĐ-CP chưa được tiếp cận, thông

qua trước toàn thể đại biểu, cử tri cả nước giống như một "văn bản luật" trong các kỳ họp. Điều này làm ảnh hưởng tới hiệu quả chấp pháp, gây sai lệch việc trong tuân thủ pháp luật về bảo vệ dữ liệu cá nhân của nhân dân, cử tri cả nước.

Thứ hai, chưa có quy định điều chỉnh công nghệ trí tuệ nhân tạo (AI). AI trong kỷ nguyên số được coi là sự phát triển vượt bậc về công nghệ. Chúng ta sử dụng công nghệ AI để bảo vệ dữ liệu cá nhân, thì tội phạm mạng cũng có thể sử dụng nó để đánh cắp, trao đổi, mua bán, lưu trữ, sử dụng, xử lý trái phép dữ liệu cá nhân. Hơn nữa, công nghệ AI không phải là những thực thể sinh ra đã có sẵn những tri thức, mà được hình thành, phát triển từ tri thức nhân loại, từ những dữ liệu mà người sử dụng (chủ thể dữ liệu) cung cấp. Hiện nay, theo quy định tại Nghị định số 13/2023/NĐ-CP, bảo vệ dữ liệu cá nhân chỉ giới hạn ở "cơ quan, tổ chức, cá nhân có liên quan", chưa đề cập chủ thể "AI", vì AI không phải là chủ thể nên chưa có quy định điều chỉnh; đồng thời, cũng không phải là một thực thể "có thật", được định danh hay có thể định danh.

Thứ ba, chế tài xử lý đối với hành vi vi phạm là chưa đủ rõ ràng và chưa đủ sức răn đe. Hầu hết các hành vi "nhờn luật" hiện nay, đều xuất phát từ việc chế tài chưa đủ sức răn đe. Bên cạnh đó, các doanh nghiệp, tổ chức, cơ quan cũng "tạo điều kiện" cho các tội phạm mạng tiếp cận dữ liệu một cách dễ dàng, vì các cơ quan, tổ chức này cũng không chấp hành nghiêm chỉnh những quy định về bảo vệ dữ liệu cá nhân trên không gian mạng. Dù đã có các quy định về tội phạm trong Bộ luật Hình sự và một số chế tài xử phạt hành chính tại Nghị định số 15/2020/NĐ-CP ngày 3/2/2020 của Chính phủ về 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. Tuy nhiên vẫn chưa thể làm rõ được cách thức vận hành và định danh, định tội đối với các hành vi, tội phạm xâm phạm dữ liệu cá nhân do chưa có một bộ tiêu chí cụ thể để xác định hành vi nào thì xử phạt hành chính, hành vi nào là tội phạm hình sự.

Dữ liệu cá nhân bị cấm mua bán.

Kinh nghiệm từ châu Âu

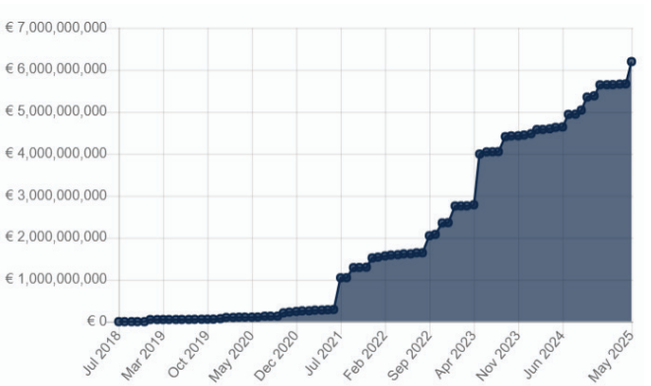
Quy định Bảo vệ dữ liệu chung của Liên minh châu Âu (sau đây gọi tắt là Quy định) tác động đến công nghệ AI thông qua việc hạn chế phạm vi ứng dụng. Tại Khoản 3 Điều 13 của Quy định, trường hợp bên kiểm soát dữ liệu dự định xử lý thêm cho mục đích khác so với mục đích ban đầu khi thu thập dữ liệu, thì trước đó phải tiến hành thông báo, cung cấp thông tin cho chủ thể dữ liệu về mục đích mới. Điều này đặt ra hạn chế đối với AI là không được phép tự ý xử lý dữ liệu cá nhân ngoài mục đích ban đầu được chủ thể dữ liệu cho phép, nếu vẫn muốn sử dụng thì phải được chủ thể dữ liệu cho phép (thông qua thông báo, cung cấp thông tin cho chủ thể dữ liệu từ trước đó). Mặt khác, Quy định này đặt ra thêm trách nhiệm cho bên kiểm soát trong việc bảo vệ dữ liệu cá nhân của chủ thể dữ liệu, nhằm hạn chế các hành vi "vượt quyền" của bên kiểm soát dữ liệu.

Quy định Bảo vệ dữ liệu chung (General Data Protection Regulation).

Tại Điều 83 của Quy định nêu điều kiện chung để áp dụng xử phạt hành chính, dựa vào các hành vi sau: (i) Bản chất, mức độ nghiêm trọng, thời gian vi phạm hay mục đích vi phạm, số lượng chủ thể dữ liệu bị ảnh hưởng và mức độ thiệt hại; (ii) Tính chất vô ý hoặc cố ý; (iii) Hành động nhằm giảm thiểu thiệt hại của bên kiểm soát dữ liệu và bên xử lý dữ liệu; (iv) Mức độ trách nhiệm của bên kiểm soát bảo vệ dữ liệu cá nhân và bên xử lý bảo vệ dữ liệu cá nhân liên quan đến các biện pháp kỹ thuật và tổ chức do họ thực hiện; (v) Những vi phạm trước đó của bên kiểm soát dữ liệu và bên xử lý dữ liệu; (vi) Mức độ hợp tác với cơ quan giám sát nhằm khắc phục vi phạm và giảm thiểu những tác động tiêu cực có thể xảy ra; (vii) Các loại bảo vệ dữ liệu cá nhân bị ảnh hưởng; (viii) Cách thức hành vi vi phạm được phát hiện bởi cơ quan giám sát, đặc biệt là việc bên kiểm soát bảo vệ dữ liệu cá nhân hoặc bên xử lý bảo vệ dữ liệu cá nhân có tự nguyện thông báo về hành vi vi phạm hay không, và nếu có thì ở mức độ nào; (ix) Việc tuân thủ các biện pháp đã được cơ quan giám sát ra lệnh đối với bên kiểm soát bảo vệ dữ liệu cá nhân hoặc bên xử lý bảo vệ dữ liệu cá nhân liên quan đến cùng một vấn đề; (x) Việc tuân thủ các quy tắc ứng xử được phê duyệt hoặc cơ chế chứng nhận được phê duyệt; (xi) Bất kỳ yếu tố tăng nặng hoặc giảm nhẹ nào khác có liên quan đến hoàn cảnh cụ thể của vụ việc.

Dựa vào các điều kiện này, mức phạt tiền tùy thuộc vào mức độ gây nguy hiểm cho xã hội, cao nhất là 20 triệu euro (tương đương gần 567 tỷ đồng) đối với cá nhân hoặc 4% tổng mức doanh thu theo năm tài chính trên toàn thế giới đối với doanh nghiệp. Từ khi Quy định có hiệu lực, đã tác động tích cực đến bảo vệ dữ liệu cá nhân và thu được số tiền phạt khá lớn, tính đến tháng 5/2025 đạt gần 6 tỷ Euro (hình 1).

Tại Điều 84 không trực tiếp đề cập đến các tội phạm hình sự về bảo vệ dữ liệu cá nhân, mà để các quốc gia thành viên tự quy định về nội dung này, thể hiện sự tôn trọng các thành tố "cấu thành tội phạm" của từng quốc gia. Điển hình, năm 2018, Meta (công ty mẹ của Facebook) đã để xảy ra một sự cố vi phạm bảo mật dữ liệu cá nhân, ảnh hưởng đến khoảng 29 triệu người dùng. Trước hành vi vi phạm nghiêm trọng này, Ủy ban Bảo vệ Dữ liệu Ireland (DPC) là cơ quan có thẩm quyền giám sát Meta tại châu Âu đã ra quyết định xử phạt hành chính với số tiền lên đến 251 triệu euro (tương đương 263,5 triệu USD).



Hình 1. Tiền phạt tích lũy do vi phạm quy định bảo vệ dữ liệu chung tính đến tháng 5/2025.

Một số gợi ý cho Việt Nam

Trước yêu cầu cấp bách về giải quyết hài hòa các quan hệ xã hội mới, quan hệ pháp luật mới. Dựa trên thực trạng khung pháp lý, thực tiễn xã hội và kinh nghiệm của Châu Âu, Việt Nam cần quan tâm tới một số vấn đề sau:

Thứ nhất, cần sớm ban hành văn bản luật bảo vệ dữ liệu cá nhân. Trong đó chú trọng điều chỉnh những vấn đề có tính thời sự, thời điểm của các quan hệ xã hội. Nghị định số 13/2023/NĐ-CP đã có những điều chỉnh đáng kể nhằm đáp ứng yêu cầu quản lý trong bối cảnh mới, tuy nhiên việc thiếu vắng một văn bản luật có tính nền tảng (luật gốc) điều chỉnh toàn diện lĩnh vực này đang đặt ra những bất cập cả về kỹ thuật lập pháp lẫn hiệu lực pháp lý. Hơn nữa, khi các quan hệ xã hội mới liên quan đến dữ liệu cá nhân tiếp tục phát sinh như một tất yếu khách quan của quá trình chuyển đổi số và phát triển kinh tế số, Nhà nước buộc phải ban hành các nghị định mới để thay thế các nghị định hiện hành, dẫn đến tình trạng "nghị định thay thế nghị định", thiếu ổn định và không bảo đảm tính hệ thống của pháp luật. Do đó, việc xây dựng và ban hành một văn bản luật chuyên ngành về bảo vệ dữ liệu cá nhân là yêu cầu cấp thiết, nhằm thiết lập khung pháp lý thống nhất, có hiệu lực cao hơn, bảo đảm tính ổn định lâu dài, cũng như đáp ứng yêu cầu hội nhập quốc tế về bảo vệ quyền riêng tư và dữ liệu cá nhân.

Meta bị phát hiện thu thập dữ liệu nhạy cảm của người dùng.

Hiện nay, các quốc gia trong khu vực Đông Nam Á và Trung Quốc đã có văn bản điều chỉnh về bảo vệ dữ liệu cá nhân.

Thứ hai, chú trọng việc khoanh vùng quyền hạn của AI trong bảo vệ dữ liệu cá nhân trên không gian mạng. AI đang trở thành một công cụ hỗ trợ hiệu quả công tác kiểm tra, giám sát trên nhiều lĩnh vực, bao gồm cả lĩnh vực bảo vệ dữ liệu cá nhân. Tuy nhiên, nguy cơ AI bị các đối tượng tội phạm mạng lợi dụng để xâm phạm dữ liệu cá nhân ngày càng gia tăng, với mức độ ngày càng tinh vi và có hệ thống. Trước thực trạng đó, pháp luật cần phải thiết lập những giới hạn chặt chẽ đối với các chủ thể tham gia vào quá trình xử lý dữ liệu cá nhân trên không gian mạng, đặc biệt là khi sử dụng AI. Cụ thể, cần quy định rõ ràng về trách nhiệm và phạm vi quyền hạn của bên kiểm soát dữ liệu và bên xử lý dữ liệu, hạn chế việc sử dụng AI để thu thập, phân tích hoặc khai thác dữ liệu cá nhân một cách tự động, thiếu minh bạch. Trong mọi trường hợp, nếu bên kiểm soát dữ liệu hoặc bên xử lý dữ liệu muốn ứng dụng AI để tự động hóa việc xử lý dữ liệu cá nhân thì phải tuân thủ nguyên tắc minh bạch và có được sự chấp thuận rõ ràng, tự nguyện của chủ thể dữ liệu sau khi đã cung cấp đầy đủ thông tin liên quan. Điều này xuất phát từ nguyên lý cốt lõi rằng dữ liệu cá nhân là tài sản số, thông tin gắn liền với nhân thân và thuộc quyền kiểm soát của chính chủ thể dữ liệu, chứ không phải của bất kỳ tổ chức hay cá nhân nào khác. Đồng thời, việc tôn trọng quyền tự quyết của chủ thể dữ liệu cũng là biểu hiện cụ thể của quyền con người trong kỷ nguyên số.

Thứ ba, điều chỉnh mức xử phạt hành chính và tội phạm hình sự đối với các đối tượng có hành vi xâm phạm bảo vệ dữ liệu cá nhân trên không gian mạng. Hiện nay, hành vi lợi dụng không gian mạng để xâm phạm dữ liệu cá nhân diễn ra với tần suất cao, mức độ ngày càng tinh vi, gây ảnh hưởng nghiêm trọng đến quyền riêng tư và an toàn thông tin của công dân. Trước thực trạng này, cần thiết phải có những giải pháp mang tính phòng ngừa và răn đe mạnh mẽ trong khuôn khổ pháp luật, nhằm triệt tiêu từ gốc các ý đồ, hành vi vi phạm, ngay từ trong nhận thức của các chủ thể có nguy cơ, có ý định thực hiện hành vi xâm phạm. Một trong những giải pháp trọng tâm là điều chỉnh mức xử phạt vi phạm hành chính theo hướng tăng nặng đối với các hành vi xâm phạm dữ liệu cá nhân trên không gian mạng, vì mức xử phạt hiện hành còn tương đối nhẹ, chưa đủ sức răn đe. Hơn nữa, cần nghiên cứu, bổ sung các quy định hình sự để xử lý đối với những hành vi có tính chất nghiêm trọng, có tổ chức hoặc gây hậu quả lớn, bởi không phải mọi trường hợp đều có thể xử lý theo hướng hành chính. Việc định danh tội phạm xâm phạm dữ liệu cá nhân trong Bộ luật Hình sự sẽ tạo cơ sở pháp lý vững chắc để bảo vệ hiệu quả quyền của chủ thể dữ liệu, đồng thời khẳng định thông điệp pháp lý rõ ràng về tính nghiêm minh của pháp luật trong kỷ nguyên số. Bên cạnh việc xử lý đối với các chủ thể vi phạm, pháp luật cũng cần bổ sung các chế tài đối với cán bộ, công chức trong cơ quan quản lý nhà nước nếu không thực hiện đúng chức trách, nhiệm vụ trong công tác bảo vệ dữ liệu cá nhân. Mặc dù hiện nay đã có quy định về trách nhiệm quản lý, giám sát trong lĩnh vực này, nhưng việc thiếu cơ chế xử lý cụ thể khi cán bộ vi phạm nghĩa vụ hoặc buông lỏng quản lý.

Thứ tư, xây dựng bộ tiêu chí về hành vi xâm phạm bảo vệ dữ liệu cá nhân trên không gian mạng. Bộ tiêu chí này cần cụ thể để xác định, định danh từng hành vi, tùy vào mức độ khắc phục, phối hợp để khắc phục và đưa ra cảnh cáo, xử phạt khác nhau, xác định đúng người, đúng tội, không xử oan sai, không phạt quá mức hành vi. Xây dựng bộ tiêu chí dựa trên các điều kiện về: Bản chất, thời gian, mức độ, vi phạm trước đó, cách khắc phục, v, v.