

MỘT SỐ VẤN ĐỀ PHÁP LÝ VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG ĐÔ THỊ THÔNG MINH TẠI VIỆT NAM^(*)

BÙI THỊ NGUYỆT THU^(**)

Ngày nhận bài: 08/5/2024

Ngày thẩm định: 15/5/2024

Ngày duyệt đăng: 20/6/2024

Tóm tắt: Trong quá trình xây dựng đô thị thông minh, việc sử dụng công nghệ thông tin nhằm tăng hiệu quả và hiệu suất cung cấp dịch vụ công, đã đặt ra vấn đề về tính minh bạch trong việc thu thập và sử dụng dữ liệu cá nhân. Công chúng lo ngại dữ liệu cá nhân thu thập được sẽ bị lạm dụng, rò rỉ và khai thác sai mục đích. Bài viết đề cập đến một số vấn đề cần khắc phục trong khung pháp lý về bảo vệ dữ liệu cá nhân khi xây dựng đô thị thông minh, nhằm góp phần phát triển đô thị thông minh bền vững ở Việt Nam.

Từ khóa: bảo vệ dữ liệu cá nhân; đô thị thông minh; pháp lý

1. Quan niệm về đô thị thông minh và yêu cầu bảo vệ dữ liệu cá nhân

1.1. - Đô thị thông minh
Hiện chưa có định nghĩa cụ thể về “đô thị thông minh” được chấp nhận rộng rãi trên thế giới, cũng như không có hình mẫu chung cho “mô hình đô thị thông minh”, mặc dù mô hình phát triển đô thị thông minh đã xuất hiện từ năm 2010 và có những kết quả nhất định. Cách tiếp cận phát triển đô thị thông minh cũng rất đa dạng giữa các quốc gia. Năm 2016, Liên minh Viễn thông thế giới (ITU) đã tổng kết khoảng 116 định nghĩa về đô thị thông minh từ nhiều nguồn khác nhau nhằm đưa ra một định nghĩa chung. Theo đó: “Đô thị thông minh phát triển bền vững là đô thị đổi mới sáng tạo, sử dụng ICT và các phương tiện

khác để cải thiện chất lượng cuộc sống, hiệu quả quản lý vận hành, cung cấp dịch vụ và mức độ cạnh tranh của đô thị, trong khi vẫn đảm bảo đáp ứng những nhu cầu của các thể hệ hiện tại và tương lai về mọi khía cạnh kinh tế, môi trường, văn hóa và xã hội”⁽¹⁾.

Đô thị thông minh được giải thích tại tiêu mục 3.4 Mục 3 Tiêu chuẩn quốc gia TCVN ISO 37122:2020 (ISO 37122:2019) như sau: “Đô thị thông minh là đô thị gia tăng sự phát triển từ đó mang lại những kết quả mang tính bền vững về xã hội, kinh tế và môi trường. Các đô thị thông minh đáp ứng những thách thức như biến đổi khí hậu, gia tăng dân số và bất ổn chính trị và kinh tế bằng cách cải thiện về cơ bản cách thức thu hút xã hội, áp dụng các phương pháp lãnh đạo cộng tác, làm việc theo nguyên tắc và hệ thống của đô thị và sử dụng thông tin dữ liệu và công nghệ hiện đại để cung cấp dịch vụ tốt hơn và chất lượng cuộc sống cho mọi người trong đô thị (cư dân, doanh nghiệp, khách vãng lai), hiện tại và trong tương lai gần mà không gây ra sự không

^(*) Bài viết trong khuôn khổ thực hiện đề tài cấp Bộ năm 2024: “Bảo mật và bảo vệ dữ liệu cá nhân trong quá trình xây dựng và thực thi pháp luật ở Việt Nam hiện nay” do TS. Bùi Thị Nguyệt Thu làm chủ nhiệm

^(**) TS, Học viện Chính trị khu vực II, Học viện Chính trị quốc gia Hồ Chí Minh

công bằng của những người khác hoặc sự suy thoái của môi trường tự nhiên”⁽²⁾.

Như vậy, có thể hiểu, đô thị thông minh (smart city) là đô thị gia tăng sự phát triển, từ đó, đưa lại những kết quả mang tính bền vững về xã hội, kinh tế và môi trường. Đây là một mô hình phát triển của đô thị. Nó đáp ứng những thách thức, như biến đổi khí hậu, gia tăng dân số và bất ổn chính trị và kinh tế, bằng cách cải thiện về cơ bản cách thức thu hút xã hội, áp dụng các phương pháp lãnh đạo cộng tác, làm việc theo nguyên tắc và hệ thống của đô thị; sử dụng thông tin dữ liệu và công nghệ hiện đại để cung cấp dịch vụ tốt hơn, nâng cao chất lượng cuộc sống hiện tại và tương lai cho mọi người trong đô thị (cư dân, doanh nghiệp, khách vãng lai).

- Yêu cầu về bảo vệ dữ liệu cá nhân trong quá trình xây dựng đô thị thông minh

Để phát triển đô thị thông minh, ngày 01/8/2018, Thủ tướng Chính phủ đã ban hành Quyết định số 950/QĐ-TTg phê duyệt Đề án phát triển đô thị thông minh bền vững Việt Nam giai đoạn 2018 - 2025 và định hướng đến năm 2030. Đề án đã chỉ ra mục tiêu và lộ trình 03 giai đoạn phát triển đô thị thông minh ở Việt Nam (giai đoạn đến năm 2020; giai đoạn đến năm 2025; định hướng đến năm 2030). Đề án cũng xác định 07 quan điểm và nguyên tắc phát triển đô thị thông minh, trong đó có nguyên tắc “bảo đảm an ninh mạng và bảo vệ dữ liệu”. Ngày 01/7/2023, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân cũng chính thức có hiệu lực thi hành. Nghị định nêu rõ, cơ quan chuyên trách bảo vệ dữ liệu cá nhân là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an), có trách nhiệm giúp Bộ Công an thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân.

Việc ứng dụng công nghệ thông tin, xây dựng, thiết kế, quản lý cơ sở hạ tầng đô

thị và bảo vệ dữ liệu cá nhân là một trong những nội dung quan trọng mà chính quyền một số tỉnh, thành áp dụng trong quá trình chuyển đổi đô thị thông minh. Tính đến nay, có 46/63 địa phương ở Việt Nam đã quy hoạch và triển khai dự án đô thị thông minh⁽³⁾. Để phát triển đô thị thông minh, các tỉnh/thành tập trung: quy hoạch đô thị thông minh, xây dựng và quản lý đô thị thông minh, cung cấp các tiện ích hạ tầng kỹ thuật của đô thị thông minh.

Đến nay, nhiều địa phương đã hoàn thành xây dựng và đưa vào sử dụng trung tâm giám sát điều hành đô thị thông minh, với mục tiêu là giám sát và vận hành các dịch vụ của đô thị thông minh, cung cấp các tiện ích của đô thị thông minh. Với bốn chức năng chính: giám sát, báo cáo, điều hành và hỗ trợ chỉ đạo, trung tâm giám sát điều hành đô thị thông minh triển khai các dịch vụ đô thị, như: giám sát chỉ tiêu kinh tế - xã hội; giám sát hành chính công; giám sát thông tin môi trường mạng internet; giám sát thông tin dịch bệnh COVID-19; giám sát an ninh, an toàn thông tin; giám sát chất lượng môi trường; giám sát an ninh, trật tự và an toàn giao thông (qua hệ thống camera); giám sát hoạt động công nghiệp; giám sát tài nguyên; giám sát các lĩnh vực chuyên ngành; tương tác, giao tiếp phục vụ công dân; quản lý dữ liệu dịch vụ dùng chung.

Trung tâm giám sát điều hành đô thị thông minh giúp chính quyền phương giám sát, kiểm soát các hoạt động xã hội của người dân và dự đoán xu hướng xã hội. Tuy nhiên, giám sát đô thị thông qua cảm biến camera có khả năng dẫn đến việc dữ liệu cá nhân bị lạm dụng, tiết lộ, rò rỉ và khai thác sai mục đích. Điều này bắt nguồn từ những nguyên nhân: (1) Các cơ quan, tổ chức, doanh nghiệp chưa có biện pháp bảo vệ thông tin thống nhất, hiệu quả; (2) Hệ thống lưu trữ và xử lý dữ liệu cá nhân hiện nay có những lỗ hổng có thể bị tin tặc khai thác để tấn công, gây ra tổn thất đáng kể; (3) Chưa có cơ chế hữu hiệu bảo vệ dữ liệu cá nhân.

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

Trước khi Nghị định số 13/2023/NĐ-CP ra đời, trong các bản văn pháp luật của Việt Nam tồn tại cả 02 thuật ngữ: “thông tin cá nhân” và “dữ liệu cá nhân”. Tuy nhiên, xét về bản chất, cả hai thuật ngữ trên đều có nội hàm như nhau, đều gắn chặt với quyền bất khả xâm phạm về đời sống riêng tư - một quyền cơ bản của con người.

Hiến pháp năm 2013 đưa ra những nguyên tắc chung là mọi người đều có quyền bất khả xâm phạm về đời tư, bí mật cá nhân, bí mật gia đình và có quyền bảo vệ danh dự, uy tín của mình. Thông tin liên quan đến bí mật đời tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo vệ an toàn⁽⁴⁾. Tiếp đến là các bộ luật, luật chuyên ngành và nhiều văn bản dưới luật khác quy định liên quan đến bảo vệ dữ liệu cá nhân. Điều 72 Luật Công nghệ thông tin năm 2006 quy định thông tin cá nhân hợp pháp của tổ chức, cá nhân được trao đổi, truyền đưa hoặc lưu trữ trên môi trường mạng phải được bảo mật theo quy định của pháp luật. Luật An toàn thông tin mạng năm 2015 quy định nguyên tắc bảo vệ thông tin cá nhân trên internet (Điều 16) và quy định tổ chức, cá nhân xử lý thông tin cá nhân phải thực hiện các biện pháp quản lý, kỹ thuật phù hợp để bảo vệ thông tin cá nhân do mình thu thập, lưu trữ và tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn thông tin mạng (Điều 19). Tuy nhiên, liên quan đến các quy định pháp luật về bảo vệ dữ liệu cá nhân trong quá trình xây dựng đô thị thông minh, **còn nhiều vấn đề cần được bổ sung, làm rõ:**

Một là, chưa thống nhất về thuật ngữ liên quan đến dữ liệu cá nhân dùng trong hệ thống các văn bản pháp luật

Tại Điều 3 Nghị định số 52/2013/NĐ-CP ngày 16/5/2013 của Chính phủ về thương mại điện tử khẳng định: “Thông tin cá nhân trong Nghị định này không bao gồm thông tin liên hệ công việc và những thông tin mà cá nhân đã tự công bố trên các phương tiện

truyền thông”⁽⁵⁾, trong khi đó, Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng quy định: “thông tin cá nhân là thông tin gắn liền với việc xác định danh tính, nhân thân của cá nhân bao gồm tên, tuổi, địa chỉ, số chứng minh nhân dân, số điện thoại, địa chỉ thư điện tử và thông tin khác theo quy định của pháp luật”⁽⁶⁾ bất kể nó đã được công bố hay chưa. Nghị định số 13/2023/NĐ-CP xác định “dữ liệu cá nhân cơ bản” bao gồm: “Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có); ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích; giới tính; nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ; quốc tịch; hình ảnh của cá nhân; số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế; tình trạng hôn nhân; thông tin về mối quan hệ gia đình (cha mẹ, con cái); thông tin về tài khoản số của cá nhân; dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng; các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể”⁽⁷⁾.

Hai là, chưa quy định rõ các trường hợp xử lý dữ liệu mà không cần có sự đồng ý của chủ thể dữ liệu cũng như giới hạn xử lý và cơ quan có thẩm quyền xử lý

Hiện nay, Nghị định số 13/2023/NĐ-CP đưa ra nguyên tắc chung yêu cầu: Bên kiểm soát và xử lý dữ liệu/Bên xử lý dữ liệu khi tiến hành bất kỳ hoạt động xử lý dữ liệu nào đều phải được sự đồng ý của chủ thể dữ liệu và trong tất cả các quy trình xử lý (Điều 11); và trước khi tiến hành hoạt động xử lý dữ liệu phải thông báo cho chủ thể dữ liệu cá nhân (Điều 13). Trong một số trường hợp cụ thể, cơ quan công quyền có thể thực hiện xử lý dữ liệu mà không cần có sự đồng ý của chủ thể dữ liệu: (1)

Các trường hợp khẩn cấp, cần thiết để bảo vệ tính mạng và sức khỏe của chủ thể dữ liệu hoặc những người khác; (2) Tiết lộ công khai dữ liệu cá nhân theo yêu cầu của pháp luật; (3) Phòng ngừa và kiểm soát bạo loạn, khủng bố, tội phạm và vi phạm pháp luật theo quy định của pháp luật; (4) Thực hiện các nghĩa vụ theo hợp đồng giữa chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của pháp luật; (5) Phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật chuyên ngành⁽⁸⁾. Tuy nhiên, lại chưa quy định rõ phạm vi, giới hạn cũng như thẩm quyền xử lý, nên có thể dẫn đến việc lạm dụng các quy định về ngoại lệ để xâm phạm dữ liệu cá nhân.

Ba là, mức xử phạt chưa đủ răn đe

Các hình phạt hành chính liên quan đến bảo vệ dữ liệu cá nhân nằm rải rác trong nhiều văn bản pháp luật. Mức phạt từ 2.000.000 đồng đến 70.000.000 đồng đối với một số hành vi xâm nhập thông tin cá nhân, như lưu giữ thông tin của người dùng trong thời gian vượt quá thời hạn lưu giữ theo quy định của pháp luật hoặc do hai bên thỏa thuận; thu thập, xử lý và sử dụng thông tin của các tổ chức hoặc cá nhân khác mà không có sự đồng ý của họ hoặc cho các mục đích bất hợp pháp; mua bán, trao đổi trái phép thông tin riêng của người sử dụng dịch vụ viễn thông.

Bộ luật Hình sự năm 2015 quy định về “Tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác” tại Điều 159 và “Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông” tại Điều 288. Mức phạt cao nhất là 07 năm tù và phạt tiền từ 20.000.000 đồng đến 200.000.000 đồng.

Bốn là, một số quy định liên quan đến bảo vệ dữ liệu cá nhân trong các văn bản luật và dưới luật chưa thống nhất

Chẳng hạn, Điều 3 Luật An toàn thông tin mạng năm 2015 quy định: “Xử lý thông tin cá

nhân là việc thực hiện một hoặc một số hoạt động thu thập, chỉnh sửa, sử dụng, lưu trữ, cung cấp, chia sẻ hoặc phát tán thông tin cá nhân trên không gian mạng nhằm mục đích thương mại”. Định nghĩa này rộng hơn quy định tại Điều 21 và Điều 22 Luật Công nghệ thông tin năm 2006, loại trừ việc “thu thập” và “sử dụng” thông tin cá nhân. Luật Công nghệ thông tin năm 2006 yêu cầu các cá nhân và tổ chức phải thông báo cho chủ thể thông tin cá nhân về phạm vi, mục đích, hình thức và địa điểm thu thập và sử dụng thông tin cá nhân trước khi thực hiện, trong khi Luật An toàn thông tin mạng năm 2015 chỉ yêu cầu phải thông báo phạm vi và mục đích. Gần đây, tại khoản 2 Điều 3 và khoản 1 Điều 9 Nghị định số 13/2023/NĐ-CP quy định chủ thể có quyền được biết về việc xử lý dữ liệu cá nhân của mình, trừ trường hợp luật khác có quy định khác; hay tại khoản 2 Điều 9 quy định chủ thể có quyền không đồng ý xử lý dữ liệu cá nhân của mình; chủ thể có quyền xóa, truy cập, yêu cầu hạn chế xử lý dữ liệu, phản đối xử lý dữ liệu, trừ trường hợp luật khác có quy định khác.

Năm là, thiếu chế tài xử phạt trong pháp luật về bảo vệ dữ liệu cá nhân

- Thiếu hình phạt đối với việc bán dữ liệu cá nhân: Theo Thông tư liên tịch số 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC về việc áp dụng quy định của Bộ luật Hình sự đối với một số tội phạm liên quan đến công nghệ thông tin và viễn thông, hành vi mua bán thông tin cá nhân sẽ không cấu thành tội phạm nếu không có bằng chứng “gây hậu quả nghiêm trọng”. Việc chứng minh tội phạm đề phù hợp với các yếu tố cấu thành tội phạm này hiện đang rất khó khăn. Việc công bố, rao bán hơn 17.000 dữ liệu về căn cước công dân là ví dụ điển hình⁽⁹⁾. Do vậy, trong nhiều năm qua, mặc dù Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) đã thực hiện nhiều cuộc điều tra liên quan đến việc mua bán thông tin cá nhân trên mạng,

nhưng do vướng mắc pháp lý nên thường chuyển sang sở thông tin và truyền thông để xử lý vi phạm hành chính.

- Thiếu quy định về trách nhiệm hình sự đối với hành vi xâm phạm quyền được bảo vệ đối với dữ liệu cá nhân: Điều 159 Bộ luật Hình sự năm 2015 quy định về “tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác”; Điều 288 Bộ luật này cũng quy định “tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông”. Tuy nhiên, cả hai điều khoản này đều chưa được cập nhật các hành vi bất hợp pháp hiện tại liên quan đến bảo vệ dữ liệu cá nhân, chẳng hạn tài khoản mạng xã hội bị đánh cắp, trộm cắp dữ liệu cá nhân và giao dịch bất hợp pháp cũng như thu thập và sử dụng dữ liệu cá nhân mà không cần thông báo hoặc cơ chế bảo vệ người dùng.

3. Khuyến nghị một số giải pháp nhằm hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân trong xây dựng đô thị thông minh ở Việt Nam

Một là, ban hành Luật Bảo vệ dữ liệu cá nhân

Việc hệ thống hóa các quy định bảo vệ dữ liệu cá nhân nằm rải rác trong nhiều văn bản pháp luật là hết sức cấp thiết, luật mới cần thể hiện rõ những nội dung, như tên gọi là Luật Bảo vệ dữ liệu cá nhân theo cách đặt tên của nhiều quốc gia. Việc xác định phạm vi của luật cần được xem xét và tính toán kỹ lưỡng để tránh sự trùng lặp với các văn bản pháp luật chuyên ngành khác. Luật này cần làm rõ, cụ thể hóa các khái niệm cơ bản về dữ liệu cá nhân, quyền và nghĩa vụ của chủ thể dữ liệu cá nhân, nghĩa vụ của chủ thể bảo vệ dữ liệu cá nhân, các nguyên tắc bảo vệ dữ liệu cá nhân, phương thức và trình tự thủ tục bảo vệ dữ liệu cá nhân, quy định về giới hạn của bảo vệ dữ liệu cá nhân trong các lĩnh vực khác nhau, các môi trường thông tin khác nhau trong đời sống.

Hai là, bảo đảm tính minh bạch trong việc thu thập và sử dụng dữ liệu cá nhân tại các đô thị thông minh

Cần cân bằng giữa nhu cầu thu thập, xử lý thông tin, dữ liệu của người dân để vận hành đô thị thông minh và nhu cầu bảo đảm quyền riêng tư. Để đạt được mục tiêu này, pháp luật cần quy định các thủ tục thu thập và chia sẻ dữ liệu cá nhân.

Việc xử lý dữ liệu cá nhân phải được thực hiện với sự minh bạch đối với các chủ thể dữ liệu. Mọi người đều có quyền biết dữ liệu cá nhân của mình được thu thập, sử dụng, lưu trữ và chia sẻ như thế nào, đồng thời có quyền chỉnh sửa và sửa đổi thông tin của mình, phản đối việc sử dụng dữ liệu không đúng cách theo quy định của pháp luật, có quy trình khiếu nại hành chính và khiếu kiện tư pháp giúp bảo đảm quyền minh bạch. Đặc biệt, cần thúc đẩy việc minh bạch hóa các vi phạm về dữ liệu cá nhân trong các cơ quan nhà nước ở tất cả các cấp. Chủ thể dữ liệu có quyền nhận thông báo trong trường hợp sự cố lộ lọt dữ liệu xảy ra. Bên cạnh đó, các cơ quan nhà nước cần thường xuyên tiến hành đánh giá tác động quyền riêng tư và công khai thông tin kết quả đánh giá trên các nền tảng trực tuyến. Tính minh bạch về vi phạm dữ liệu và công bố đánh giá tác động quyền riêng tư cần được chính thức coi như một nội dung trong chứng nhận bảo mật do Trung tâm Giám sát an toàn không gian mạng quốc gia, Bộ Thông tin và Truyền thông cấp⁽¹⁰⁾.

Ba là, quy định cụ thể các hành vi bị nghiêm cấm trong việc thu thập và xử lý dữ liệu cá nhân

Pháp luật Việt Nam ghi nhận nguyên tắc chung là cấm cung cấp, mua bán, chuyển giao, lưu trữ, sử dụng thông tin vi phạm các quy định về an toàn, an ninh thông tin, nhưng các văn bản pháp luật hiện hành đều tập trung vào việc bảo vệ bí mật quốc gia và quân sự. Vì vậy, luật mới cần quy định cụ thể các hành vi bị nghiêm cấm trong việc thu thập và xử lý dữ liệu cá nhân để tạo cơ sở pháp lý đưa

ra các hình phạt, tập trung các nội dung về quyền và nghĩa vụ của các bên liên quan đến dữ liệu cá nhân, trong đó có quyền của chủ thể dữ liệu; nghĩa vụ của Chính phủ và các đối tượng thu thập, xử lý dữ liệu; nghĩa vụ của bên thứ ba; các hành vi bị nghiêm cấm,...

Bốn là, quy định rõ các trường hợp xử lý dữ liệu mà không cần có sự đồng ý của chủ thể dữ liệu cũng như giới hạn xử lý và cơ quan có thẩm quyền xử lý

Quy định chung của Liên minh châu Âu về bảo vệ dữ liệu (GDPR) cung cấp các điều khoản rất chi tiết về các trường hợp và điều kiện mà dữ liệu có thể được xử lý mà không cần sự đồng ý của chủ thể dữ liệu so với Nghị định số 13/2023/NĐ-CP của Việt Nam. Điều 6 của GDPR nêu rõ các cơ sở pháp lý để xử lý dữ liệu cá nhân mà không cần sự đồng ý. Điều này bao gồm quá trình xử lý cần thiết để thực hiện hợp đồng, tuân thủ nghĩa vụ pháp lý, bảo vệ lợi ích thiết yếu, nhiệm vụ được thực hiện vì lợi ích công cộng.

Năm là, tăng mức xử phạt để bảo đảm tính răn đe

Hiện nay, mức phạt hành chính tối đa đối với hành vi xâm phạm quyền riêng tư là 70.000.000 VNĐ (khoảng 3.000 USD) và mức phạt hình sự là 200.000.000 VNĐ (khoảng 8.600 USD). Các khoản tiền phạt này khá thấp so với mức phạt 04% tổng doanh thu năm hoặc 20 triệu Euro như được quy định trong GDPR. Chúng không tương ứng với mức độ nghiêm trọng của việc xâm phạm quyền riêng tư hoặc dữ liệu cá nhân

Tóm lại, đô thị thông minh là một hướng phát triển đúng của Việt Nam, phù hợp với xu thế cuộc Cách mạng công nghiệp lần thứ tư. Tuy nhiên, trong quá trình triển khai thực hiện còn nhiều bất cập, hệ thống pháp luật liên quan còn có lỗ hổng. Trong thời gian tới, việc xây dựng đô thị thông minh ở Việt Nam, bên cạnh bảo đảm phù hợp với quy hoạch tổng thể hệ thống đô thị Việt Nam và chương trình phát triển đô thị quốc gia, giải quyết được những tồn tại, khó khăn, thách thức

hướng đến các mục tiêu tăng trưởng xanh và bền vững, cần thiết phải nhanh chóng hoàn thiện hành lang pháp lý, các quy phạm pháp luật, quy chuẩn, tiêu chuẩn và những cơ chế khuyến khích đầu tư cho việc phát triển đô thị thông minh, đặc biệt là hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân, góp phần tạo nền tảng vững chắc cho quá trình xây dựng và phát triển đô thị thông minh □

⁽¹⁾ Bộ Tư pháp, *Cách mạng công nghiệp lần thứ tư và những vấn đề pháp lý đặt ra cho việc xây dựng, hoàn thiện hệ thống pháp luật Việt Nam* (Kỷ yếu Hội thảo học cấp Quốc gia), Nxb Tư pháp, Hà Nội, 2020, tr.357-358

⁽²⁾ <https://thuvienphapluat.vn/phap-luat/do-thi-thong-minh-la-giyeu-cau-ve-ty-le-phan-tram-dan-cu-cua-do-thi-thong-minh-su-dung-thanh-thao-n-116237.html>

⁽³⁾ [https://baochinhphu.vn/48-tinh-thanh-dang-trien-khai-phat-trien-do-thi-thong-minh-102231129113119274.htm#:~:text=\(Chinhphu.vn\)%20%2D%20Vi%E1%BB%87t,c%3%A1c%20%E1%BB%A9ng%20d%E1%BB%A5ng%20c%E1%BA%A3nh%20b%3%A1o,](https://baochinhphu.vn/48-tinh-thanh-dang-trien-khai-phat-trien-do-thi-thong-minh-102231129113119274.htm#:~:text=(Chinhphu.vn)%20%2D%20Vi%E1%BB%87t,c%3%A1c%20%E1%BB%A9ng%20d%E1%BB%A5ng%20c%E1%BA%A3nh%20b%3%A1o,) truy cập ngày 30/4/2024

⁽⁴⁾ Điều 21 Hiến pháp năm 2013

⁽⁵⁾ Khoản 13 Điều 3 Nghị định số 52/2013/NĐ-CP ngày 16/5/2023 của Chính phủ về *thương mại điện tử*

⁽⁶⁾ Khoản 16 Điều 3 Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về *quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng*

⁽⁷⁾ Khoản 3 Điều 2 Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về *bảo vệ dữ liệu cá nhân*

⁽⁸⁾ Điều 17 Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về *bảo vệ dữ liệu cá nhân*

⁽⁹⁾ <https://mic.gov.vn/che-tai-xu-ly-cac-hanh-vi-vi-pham-quy-dinh-bao-ve-du-lieu-ca-nhan-197149685.htm>, truy cập ngày 05/5/2024

⁽¹⁰⁾ *Báo cáo Đánh giá việc bảo vệ dữ liệu cá nhân trên các giao diện tương tác với người dân của chính quyền địa phương*, Nhóm Quản trị và Tham gia của UNDP Việt Nam thực hiện, tháng 7/2022, tr.44