BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG PHÁP LUẬT TRUNG QUỐC – KINH NGHIỆM CHO VIỆT NAM

Nguyễn Phúc Thiện*

Tóm tắt: *Bài viết tập trung nghiên cứu khái quát các quy định về bảo vệ dữ liệu cá nhân tại Trung Quốc trước và sau khi ban hành Bộ luật Dân sự (BLDS) Trung Quốc năm 2020, nghiên cứu sâu các quy định về bảo vệ thông tin cá nhân (TTCN) theo Luật Bảo vệ thông tin cá nhân Trung Quốc năm 2021 (PIPL). Từ đó, nghiên cứu đối sánh các quy định tương ứng trong Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ Việt Nam về bảo vệ dữ liệu cá nhân (DLCN) (Nghị định 13/2023/NĐ-CP) và đưa ra một số kiến nghị.*

Abstract: *This article provides an overview of personal data protection regulations in China before and after the enactment of the 2020 Chinese Civil Code, and offers an in-depth analysis of the 2021 Personal Information Protection Law of China (PIPL). It compares these regulations with the corresponding provisions in Vietnam's Decree No. 13/2023/NĐ-CP, dated 17th April 2023, on personal data protection, and offers suggestions for improving Vietnam's legal framework in this area.*

1. Pháp luật Trung Quốc về bảo vệ dữ liệu cá nhân

Trong phạm vi nghiên cứu này, đối với phần pháp luật Trung Quốc, tác giả không phân biệt "dữ liệu" với "thông tin" và sử dụng chúng thay thế cho nhau. Bởi lẽ, "thông tin cá nhân" theo quy định của pháp luật Trung Quốc có nội hàm tương đồng với thuật ngữ "dữ liệu cá nhân" trong bối cảnh của châu Âu và tiệm cận với "dữ liệu cá nhân" theo Nghị định số 13/2023/NĐ-CP của Việt Nam, nên có thể đặt vào cùng một bối cảnh để nghiên cứu.

Lấy thời điểm ban hành BLDS Trung Quốc năm 2020 làm mốc chuẩn, mục này được phân tích theo hai giai đoạn: (i) Giai đoạn trước khi ban hành BLDS Trung Quốc năm 2020 và; (ii) Từ khi ban hành BLDS Trung Quốc năm 2020.

1.1. Giai đoạn trước khi ban hành Bộ luật Dân sự Trung Quốc năm 2020

Trước khi BLDS Trung Quốc năm 2020 được ban hành thì quy định bảo vệ DLCN nằm rải rác trong hơn 30 văn bản luật theo lĩnh vực, các diễn giải tư pháp liên quan và các quy định hành chính. Mục này phân tích mang tính đại diện các quy phạm bảo vệ DLCN[1] tại: (i) Luật Bảo vệ quyền và lợi ích người tiêu dùng; (ii) Quy định của Toà án nhân dân tối cao về một số vấn đề liên quan đến việc áp dụng pháp luật trong xét xử các vụ án tranh chấp dân sự về xâm phạm quyền và lợi ích cá nhân qua mạng thông tin; (iii) Luật An ninh mạng.

* ThS., Khoa Luật - Trường Đại học Mở Tp. Hồ Chí Minh.

[1] Ngoài các văn bản này thì pháp luật hình sự Trung Quốc cũng điều chỉnh rất sớm đối với các vi phạm liên quan đến dữ liệu cá nhân. Mặc dù các biện pháp trừng phạt do Luật Hình sự áp đặt thực sự đủ nghiêm khắc nhưng ngưỡng dẫn đến trách nhiệm hình sự lại tương đối cao so với trường hợp của luật tư.

1.1.1. Luật Bảo vệ quyền và lợi ích người tiêu dùng[2]

Luật này điều chỉnh mối quan hệ giữa người tiêu dùng và nhà điều hành doanh nghiệp. Điều 29 quy định khi thu thập và sử dụng TTCN của người tiêu dùng, các nhà kinh doanh phải tuân theo các nguyên tắc hợp pháp, chính đáng và cần thiết, nêu rõ mục đích, phương pháp, phạm vi thu thập và sử dụng thông tin và được sự đồng ý của người tiêu dùng. Ngoài ra, các nhà điều hành và nhân viên của họ phải giữ bí mật tuyệt đối TTCN đã thu thập của người tiêu dùng và không được tiết lộ, bán hoặc cung cấp bất hợp pháp thông tin đó cho người khác. Bên cạnh đó, theo Điều 50 thì người tiêu dùng có thể kiện nhà điều hành doanh nghiệp nếu quyền của người tiêu dùng đối với DLCN bị vi phạm[3].

1.1.2. Quy định của Tòa án nhân dân tối cao về một số vấn đề liên quan đến áp dụng pháp luật trong xét xử các vụ án tranh chấp dân sự xâm phạm quyền, lợi ích cá nhân do sử dụng mạng thông tin[4]

Thuật ngữ *"tranh chấp dân sự về các vụ việc xâm phạm quyền, lợi ích cá nhân do sử dụng mạng thông tin"* nêu trong quy định này là để chỉ các tranh chấp phát sinh từ việc sử dụng mạng thông tin xâm phạm quyền có họ, tên, uy tín, danh dự của người khác, chân dung và quyền riêng tư[5]. Toà án nhân dân tối cao cũng khẳng định rằng, việc tiết lộ trái pháp luật TTCN sẽ làm phát sinh trách nhiệm pháp lý, nhưng cũng ghi nhận các quy định loại trừ trách nhiệm dân sự của việc tiết lộ TTCN mà không có sự đồng ý của chủ thể thông tin (quy tắc sử dụng hợp lý), bao gồm việc tiết lộ trong phạm vi cần thiết để thúc đẩy lợi ích công cộng, tiết lộ thông tin ẩn danh cho nghiên cứu học thuật hoặc thống kê, tiết lộ TTCN công khai hợp pháp mà không vi phạm đạo đức xã hội, lợi ích công cộng hoặc lợi ích cá nhân quan trọng và việc tiết lộ được pháp luật hoặc quy định hành chính cho phép[6].

Điều 12 Quy định này cũng xác định thông tin di truyền, hồ sơ bệnh án, dữ liệu khám sức khỏe, tiền án, địa chỉ nhà riêng, hoạt động riêng tư... là quyền riêng tư. Trong nghiên cứu của mình, Xu Duoye nhận định: "*Sự hiểu biết của công chúng cũng như thẩm phán về sự khác biệt giữa TTCN và quyền riêng tư có thể không giống như ngày nay, quyền riêng tư trong Quy định này có thể không có nghĩa giống như quyền riêng tư trong Bộ luật Dân sự. Việc giải thích luật pháp và tư pháp trong tương lai sẽ làm rõ phạm vi của DLCN*[7]".

Sau khi BLDS Trung Quốc năm 2020 được ban hành, Toà án nhân dân tối cao đã

[2] Được thông qua tại kỳ họp thứ tư Ủy ban thường vụ Đại hội Đại biểu Nhân dân Toàn quốc khóa VIII ngày 31/10/1993, theo "Quyết định sửa đổi một số luật" tại Kỳ họp thứ mười Ủy ban thường vụ Đại hội Đại biểu Nhân dân Toàn quốc khóa XI ngày 27/8/2009. Bản sửa đổi đầu tiên dựa trên bản sửa đổi thứ hai của "Quyết định sửa đổi Luật Bảo vệ Người tiêu dùng của Cộng hòa Nhân dân Trung Hoa" tại phiên họp thứ năm của Ủy ban Thường vụ Đại hội Đại biểu Nhân dân Toàn quốc khóa XII vào ngày 25/10/2013.

[3] Điều 50. Trường hợp nhà kinh doanh xâm phạm nhân phẩm của người tiêu dùng, xâm phạm quyền tự do cá nhân của người tiêu dùng hoặc xâm phạm quyền của người tiêu dùng đối với thông tin cá nhân được pháp luật bảo vệ, họ phải chấm dứt hành vi xâm phạm, khôi phục uy tín, loại bỏ ảnh hưởng, đưa ra lời xin lỗi, và bù đắp thiệt hại.

[4] Được thông qua tại kỳ họp thứ 1621 của Ủy ban Tư pháp Tòa án nhân dân tối cao ngày 23/6/2014 và có hiệu lực kể từ ngày 10/10/2014.

[5] Điều 1 của Quy định.

[6] Điều 12 của Quy định.

[7] Xu Duoye, *The Civil Code and the Private Law protection of personal information*, Tsinghua China Law Review [Vol. 13:187], tr.193-194.

thay thế Quy định này bằng cách bỏ các điều khoản liên quan đến DLCN trong Quy định[8].

1.1.3. Luật An ninh mạng[9]

Luật An ninh mạng đưa ra định nghĩa về DLCN *"là các thông tin khác nhau được ghi lại bằng phương thức điện tử hoặc bằng các cách khác có thể xác định danh tính cá nhân của một thể nhân, độc lập hoặc kết hợp với các thông tin khác, bao gồm nhưng không giới hạn ở tên, ngày sinh, số chứng minh nhân dân, sinh trắc học cá nhân của thể nhân đó, thông tin, địa chỉ, số điện thoại*[10]*..."*.

Ngoài ra, Luật này còn quy định về thu thập và sử dụng DLCN (Điều 41), cung cấp DLCN cho các bên khác (Điều 42 và Điều 44), thông báo và báo cáo rò rỉ (Điều 42), và quyền yêu cầu xoá hoặc chỉnh sửa của chủ thể dữ liệu (Điều 43). Luật An ninh mạng cũng quy định nghĩa vụ bảo mật của cơ quan quản lý mạng và nhân viên của họ (Điều 45). Về tổng thể, Luật An ninh mạng chủ yếu bao gồm các quy định pháp lý điều chỉnh hành vi của "các nhà khai thác mạng". Nó thiết lập một khuôn khổ để bảo vệ DLCN trong bối cảnh các hoạt động trực tuyến[11]. Điều 74 Luật An ninh mạng quy định: *"Người nào vi phạm các quy định của luật này mà gây thiệt hại cho người khác thì phải chịu trách nhiệm dân sự theo quy định của luật"*. Đây là quy định đáng được chú ý, bởi lẽ phần lớn trách nhiệm pháp lý theo Luật An ninh mạng là trách nhiệm hành chính. Quy định này và Điều 50 Luật Bảo vệ quyền và lợi ích người tiêu dùng nói trên là cơ sở chính để khởi kiện trong lĩnh vực luật tư trước khi BLDS Trung Quốc năm 2020 có hiệu lực.

Từ các phân tích trên, có thể kết luận rằng, hệ thống pháp luật điều chỉnh việc bảo vệ DLCN trước khi BLDS Trung Quốc năm 2020 ra đời tồn tại những hạn chế nhất định như sau: (i) Cách tiếp cận theo ngành, rời rạc, chủ yếu bao gồm các nguồn luật công; (ii) Bản chất pháp lý của việc bảo vệ DLCN không được xác định; (iii) Trước khi BLDS được ban hành, các khái niệm về quyền riêng tư và DLCN không được phân định rõ ràng về ranh giới quy chuẩn tương ứng của chúng[12].

1.2. Bảo vệ thông tin cá nhân theo quy định của Bộ luật Dân sự Trung Quốc năm 2020

BLDS Trung Quốc năm 2020 được ban hành đánh dấu mốc quan trọng trong lịch sử lập pháp của quốc gia này. Các quy tắc bảo vệ TTCN trong BLDS nhìn chung được mô phỏng theo các quy tắc trong Luật An ninh mạng nhưng phạm vi điều chỉnh được mở rộng đáng kể, với một số điểm phát triển quan trọng[13]. Về nguyên tắc, BLDS đưa ra sự khác biệt giữa bảo vệ TTCN (thường được gọi là "bảo vệ dữ liệu" theo cách tiếp cận của châu Âu) và quyền riêng tư, coi đây là hai khái niệm đan xen nhưng khác biệt[14]. Các quy định về bảo vệ TTCN trong BLDS hầu hết được quy định tại Chương 6

[8] Toà án nhân dân tối cao nước Cộng hoà Nhân dân Trung Hoa, *Quy định một số vấn đề về xét xử các tranh chấp dân sự liên quan đến việc sử dụng mạng thông tin xâm phạm quyền, lợi ích cá nhân*, http://gongbao.court.gov.cn/Details/9d03333660865fc33f62695cd87b84.html, truy cập ngày 19/4/2023.

[9] Thông qua tại Phiên họp thứ 24 của Ủy ban Thường vụ Đại hội Đại biểu Nhân dân Toàn quốc khóa XII vào ngày 7/11/2016.

[10] Khoản 5 Điều 76 Luật An ninh mạng.

[11] Xu Duoye, tlđd (8), tr.191.

[12] Xem thêm: Raymond Yang Gao, *Personal Information Protection Under Chinese Civil Code: A Newly Established Private Right In The Digital Era*, Tsinghua China Law Review [Vol. 13:165], p.166.

[13] Xu Duoye, *tlđd (8)*, p.188.

[14] Raymond Yang Gao, *tlđd (13)*, p.178.

"Quyền riêng tư và bảo vệ TTCN" thuộc Quyển IV *"Quyền cá nhân"*.

Thứ nhất, BLDS Trung Quốc năm 2020 có sự định nghĩa và phân loại TTCN: (i) *"TTCN là các loại thông tin được ghi lại dưới dạng điện tử hoặc theo những cách khác để có thể nhận dạng một tự nhiên nhân cụ thể một cách độc lập hoặc kết hợp với các thông tin khác, bao gồm danh tính, ngày tháng sinh, số chứng minh nhân dân, thông tin sinh trắc học, chỗ ở, số điện thoại, thư điện tử, thông tin sức khoẻ, thông tin hành tung của tự nhiên nhân"* và quy định TTCN của thể nhân được pháp luật bảo vệ theo Điều 1034. (ii) Quyền riêng tư, theo BLDS Trung Quốc năm 2020 là *"an ninh đời sống tư nhân và không gian riêng tư bí mật, hoạt động riêng tư bí mật, tin tức riêng tư bí mật mà không muốn để người khác biết được của tự nhiên nhân*[15]*"*. Nhiều học giả Trung Quốc nhận xét rằng, quyền riêng tư, về bản chất, là một quyền phòng vệ được thiết kế để ngăn chặn sự xâm nhập, xâm phạm và tiết lộ của người khác, dù thực tế hay tiềm ẩn, và có thể yêu cầu bồi thường thiệt hại bằng tiền đối với những tổn thất đã gây ra. Ngược lại, bảo vệ TTCN thiết lập quyền kiểm soát của một cá nhân đối với TTCN của họ đang được đề cập. Tựu trung, theo BLDS Trung Quốc năm 2020 thì TTCN là khả năng nhận dạng, trong khi khái niệm về quyền riêng tư tập trung vào việc chủ thể không muốn bị làm phiền hoặc "bị biết" và việc bảo vệ quyền riêng tư mang tính thụ động và phòng thủ hơn. Tuy có sự phân biệt nhưng vì cả hai đều xuất phát từ việc bảo vệ phẩm giá con người và quyền tự do của một thể nhân đối với cuộc sống của họ nên chúng có liên quan và đan xen nhau, nói cách khác, TTCN và quyền riêng tư đều thể hiện lợi ích cá nhân cố hữu. Ngoài ra, BLDS Trung Quốc năm 2020 cũng phân biệt quyền riêng tư, TTCN với "TTCN riêng tư". Theo đó, TTCN riêng tư là phần chồng lấn giữa TTCN và quyền riêng tư. Do đó, TTCN riêng tư được bảo vệ theo cả quy tắc bảo vệ quyền riêng tư và quy tắc bảo vệ TTCN, cụ thể: *"Đối với TTCN riêng tư thì áp dụng quy định liên quan về quyền riêng tư, nếu không có quy định thì áp dụng quy định liên quan về bảo vệ TTCN*[16]*"*.

Thứ hai, bảo vệ TTCN theo BLDS Trung Quốc năm 2020 là một quyền dân sự độc lập: Mặc dù có nhiều tranh cãi xoay quanh việc bảo vệ TTCN là một quyền dân sự hay lợi ích hợp pháp[17] nhưng có thể nhận thấy rằng, BLDS Trung Quốc năm 2020 đã xác lập quyền bảo vệ TTCN với tư cách là một quyền nhân thân cụ thể song song với quyền riêng tư. Bất chấp nhiều lập luận ngược lại của các học giả Trung Quốc, mục đích lập pháp về vấn đề này đã được ưu tiên áp dụng[18]. BLDS Trung Quốc năm 2020 do Uỷ ban pháp luật của Đại hội đại biểu nhân dân toàn quốc chịu trách nhiệm soạn thảo, theo ý kiến của các thành viên chủ chốt của cơ quan lập pháp này, quyền TTCN của cá nhân thể hiện quyền quan trọng của công

[15] Điều 1032 BLDS Trung Quốc năm 2020.

[16] Điều 1034 BLDS Trung Quốc năm 2020.

[17] Những người ủng hộ cho rằng việc thiết lập một quyền dữ liệu cá nhân chung cho phép các chủ thể dữ liệu kiểm soát tốt hơn dữ liệu cá nhân của họ, trong khi các học giả phản đối quyền dữ liệu cá nhân tin rằng quyền kiểm soát tuyệt đối và độc quyền được cấp bởi quyền chung về dữ liệu cá nhân sẽ tạo ra rào cản lớn đối với việc lưu thông thông tin, vốn rất quan trọng đối với nền kinh tế kỹ thuật số. Theo hệ thống luật dân sự Trung Quốc, có sự phân biệt giữa quyền dân sự và lợi ích hợp pháp được luật pháp bảo vệ. Nhìn chung, quyền dân sự thường có thứ bậc cao hơn trong hệ thống luật dân sự Trung Quốc so với lợi ích hợp pháp, nhưng ranh giới giữa chúng không phải là bất biến, vì đôi khi lợi ích hợp pháp có thể phát triển lên thành một quyền dân sự độc lập theo thời gian.

[18] Yang Gao, *tlđd (13),* p.178.

dân trong xã hội hiện đại của kỷ nguyên số. Ngoài ra, trong phần mở đầu của PIPL, cũng chính cơ quan lập pháp chịu trách nhiệm ban hành BLDS Trung Quốc năm 2020 đã tuyên bố rằng: *"Khi soạn thảo BLDS [...] Đại hội Đại biểu Nhân dân Toàn quốc và Uỷ ban thường vụ [...] đã đặt ra các điều khoản để bảo vệ TTCN của một cá nhân như một quyền dân sự quan trọng*[19]*"*.

Thứ ba, BLDS Trung Quốc năm 2020 thiết lập các nguyên tắc cơ bản điều chỉnh việc xử lý dữ liệu: Điều 1035 Bộ luật này quy định *"xử lý TTCN phải tuân theo nguyên tắc hợp pháp, chính đáng, thiết yếu, không được xử lý vượt quá giới hạn"*, bên cạnh đó cũng phải phù hợp với những điều kiện luật định. Những nguyên tắc cơ bản này đã tạo cơ sở pháp lý quan trọng cho các luật và quy định ban hành sau Bộ luật này được phát triển và hoàn thiện hơn.

Là một đạo luật mang tính bước ngoặt và là luật tư cơ bản điều chỉnh các lĩnh vực khác nhau của đời sống xã hội, BLDS Trung Quốc năm 2020 coi quyền bảo vệ TTCN là một quyền nhân thân cụ thể, dù rằng đóng vai trò chủ yếu là sự trình bày lại và hệ thống hoá các điều khoản hiện hành đã được tìm thấy trong các luật chuyên ngành đã có từ trước và các nguồn luật khác, nhưng Bộ luật này cũng đã mở rộng đáng kể phạm vi áp dụng, đưa việc bảo vệ TTCN vào cơ chế thi hành và thực thi luật tư, qua đó nâng cao mức độ bảo vệ chống lại các hành vi vi phạm pháp luật.

1.3. Bảo vệ thông tin cá nhân theo quy định của Luật Bảo vệ thông tin cá nhân năm 2021

Ngay sau khi ban hành BLDS Trung Quốc năm 2020, Dự thảo PIPL đã được đưa ra góp ý. PIPL được thông qua tại phiên họp thứ 30 của Ủy ban Thường vụ Đại hội Đại biểu Nhân dân Toàn quốc khóa XIII ngày 20/8/2021, có hiệu lực ngày 01/11/2021. PIPL là văn bản luật toàn diện đầu tiên của Trung Quốc quy định việc bảo vệ TTCN và được mô phỏng theo Quy định Bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR).

PIPL được thiết kế để bảo vệ quyền riêng tư và TTCN của công dân Trung Quốc, đồng thời sẽ yêu cầu các sáng kiến tuân thủ của các tổ chức Trung Quốc và công ty nước ngoài hoạt động tại Trung Quốc. PIPL được cấu trúc thành 08 chương với 74 điều. Tác giả sẽ phân tích trọng tâm một số vấn đề quan trọng để lấy cơ sở cho việc góp ý Nghị định 13/2023/NĐ-CP.

1.3.1. Phạm vi áp dụng Luật Bảo vệ thông tin cá nhân Trung Quốc năm 2021

Chương 1, Điều 3 quy định rằng PIPL áp dụng cho *"các hoạt động xử lý TTCN của các thể nhân trong biên giới của Cộng hòa Nhân dân Trung Hoa"*. Tuy nhiên, giống như GDPR và một số luật khác, nó cũng có phạm vi lãnh thổ rộng hơn, áp dụng cho việc xử lý TTCN của các cá nhân Trung Quốc bên ngoài biên giới Trung Quốc nếu: (i) Mục đích là cung cấp sản phẩm hoặc dịch vụ cho thể nhân bên trong biên giới; (ii) Khi "phân tích hoặc đánh giá các hoạt động của thể nhân bên trong biên giới" hoặc; (iii) Các trường hợp khác được quy định trong luật hoặc quy định hành chính. Tuy nhiên, sẽ không biết các cơ quan quản lý Trung Quốc áp dụng các điều khoản này rộng rãi như thế nào khi PIPL được thực thi. Bên cạnh đó, PIPL không có ngưỡng tuân thủ [(như Đạo luật bảo vệ người tiêu dùng California (CCPA)]. Vì vậy, đơn vị xử lý bắt buộc phải tuân thủ bất kể doanh thu của

[19] 中国人大网, *《中华人民共和国个人信息保护法(草案)》全文公布*, https://www.secrss.com/articles/26427, truy cập ngày 19/4/2023.

công ty là bao nhiêu hoặc họ xử lý bao nhiêu DLCN trong một năm nhất định[20].

1.3.2. Thông tin cá nhân và thông tin cá nhân nhạy cảm

Điều 4 PIPL quy định TTCN *"đề cập đến các thông tin khác nhau liên quan đến các thể nhân* ***được xác định*** *hoặc* ***có thể nhận dạng****, được ghi lại bằng điện tử hoặc theo các cách khác, không bao gồm thông tin ẩn danh*[21]*".*

Điều này khác với nhiều luật khác ở chỗ không cung cấp rõ ràng các thông tin như tên, địa chỉ email, số giấy phép lái xe, hồ sơ sức khỏe... nhưng với cách diễn đạt này, nó cung cấp phạm vi bao quát đủ rộng để không đặt ra yêu cầu phải cập nhật thường xuyên, ví dụ như khi công nghệ thay đổi. PIPL thông qua yếu tố *"được xác định"* và *"có thể nhận dạng"* mà không cần giải thích thêm. Cùng với việc xem xét định nghĩa *"bất kỳ thông tin nào có thể được sử dụng, riêng lẻ hoặc kết hợp với các thông tin khác, để nhận dạng một thể nhân cụ thể"* tại Điều 1034(2) BLDS Trung Quốc năm 2020 và Luật An ninh mạng, hai yếu tố này có thể được hiểu như sau: "được xác định" tương ứng với "được định vị trực tiếp" và "có thể nhận dạng" tương ứng với "có thể xác định được khi kết hợp với các thông tin khác". Từ quan điểm này, PIPL nhất quán với thông lệ chung đối với khái niệm cốt lõi này. Ngoài ra, Điều 4 PIPL loại trừ rõ ràng dữ liệu "ẩn danh" khỏi phạm vi điều chỉnh, nhưng chỉ khi định nghĩa trong Điều 73(4) PIPL được đáp ứng, thông tin ẩn danh được xử lý đến mức không thể xác định được một thể nhân cụ thể và không thể khôi phục về trạng thái ban đầu không phải là TTCN và do đó không phải tuân theo PIPL[22].

Điều 28 PIPL quy định: "*TTCN nhạy cảm là TTCN mà một khi bị tiết lộ hoặc sử dụng trái phép có thể dễ dàng dẫn đến việc xâm phạm nhân phẩm của thể nhân hoặc gây tổn hại đến an toàn cá nhân và tài sản, bao gồm sinh trắc học, niềm tin tôn giáo, danh tính cụ thể, chăm sóc y tế, tài khoản tài chính, nơi ở và các thông tin khác, cũng như TTCN của trẻ vị thành niên dưới mười bốn tuổi".*

Đối với khái niệm TTCN nhạy cảm, PIPL làm rõ ranh giới của nó bằng cách tích hợp mô tả chung và danh sách mở. Ngoài ra, PIPL ghi nhận *"theo dõi vị trí cá nhân"* trong phạm vi TTCN nhạy cảm. Ngoài việc thông báo về các vấn đề chung, việc xử lý dữ liệu nhạy cảm cần được thông báo đến cá nhân, nội dung bao gồm sự cần thiết của việc xử lý và các tác động bất lợi có thể xảy ra và cần nhận được sự đồng ý từ cá nhân. Điều này cũng quy định đối với thông tin của trẻ em dưới mười bốn tuổi phải có sự đồng ý rõ ràng, riêng biệt từ các cá nhân – hoặc cha mẹ/người giám hộ của trẻ – trước khi xử lý TTCN nhạy cảm. Điều 28 và 30 PIPL quy định phải có *"mục đích cụ thể và nhu cầu thực hiện rõ ràng"* cùng với *"các*

[20] Các công ty đáp ứng các ngưỡng sau phải tuân thủ các yêu cầu của CCPA: (i) Tổng doanh thu hàng năm vượt quá 25 triệu USD, hoặc; (ii) Nhận, mua hoặc bán thông tin cá nhân của 50.000 người tiêu dùng, hộ gia đình hoặc thiết bị trở lên hoặc; (iii) Kiếm được hơn một nửa doanh thu hàng năm từ việc bán thông tin cá nhân của người tiêu dùng. Tham khảo: Usercentrics, *California Consumer Privacy Act (CCPA) – an overview*, https://usercentrics.com/knowledge-hub/california-consumer-privacy-act/, truy cập ngày 19/4/2023.

[21] Về "thông tin ẩn danh" tham khảo thêm tại: Usercentrics, *Data Anonymization: The What, Why, and How of Data Anonymization*, https://usercentrics.com/knowledge-hub/data-anonymization/, truy cập ngày 19/4/2023.

[22] Điều 73(4) PIPL quy định: *"Ẩn danh đề cập đến quá trình thông tin cá nhân không thể xác định được một thể nhân cụ thể sau khi xử lý và không thể phục hồi".*

biện pháp bảo vệ nghiêm ngặt" cũng như tiết lộ bổ sung cho những cá nhân có TTCN nhạy cảm sẽ được xử lý.

1.3.3. Nguyên tắc xử lý thông tin cá nhân[23]

PIPL quy định bảy nguyên tắc xử lý TTCN bao gồm:

Thứ nhất, tính hợp pháp: TTCN phải được xử lý theo các nguyên tắc hợp pháp, chính đáng, cần thiết và thiện chí, và không gây hiểu lầm, lừa đảo hoặc ép buộc.

Thứ hai, mục đích đặc tả: Quá trình xử lý phải được tiến hành: (i) Cho một mục đích cụ thể và hợp lý; (ii) Cho một mục đích liên quan trực tiếp đến mục đích xử lý; và (iii) Theo hướng ít ảnh hưởng nhất đến quyền và lợi ích cá nhân.

Thứ ba, giảm thiểu dữ liệu: Việc thu thập TTCN phải được giới hạn ở phạm vi tối thiểu cần thiết để đạt được mục đích xử lý.

Thứ tư, giới hạn lưu trữ: Thời gian lưu trữ TTCN phải là khoảng thời gian tối thiểu cần thiết để đạt được mục đích xử lý, trừ khi có bất kỳ luật hoặc quy định hành chính hiện hành nào quy định khác.

Thứ năm, minh bạch: Việc xử lý phải được tiến hành theo các nguyên tắc công khai và minh bạch.

Thứ sáu, sự chính xác: Đơn vị xử lý TTCN phải đảm bảo chất lượng TTCN được xử lý, tránh mọi ảnh hưởng tiêu cực đến quyền và lợi ích cá nhân do TTCN được xử lý không chính xác hoặc không đầy đủ.

Thứ bảy, bảo mật dữ liệu: Người xử lý TTCN phải thực hiện các biện pháp cần thiết để đảm bảo tính bảo mật của TTCN được xử lý.

1.3.4. Quyền của chủ thể dữ liệu[24]

Thứ nhất, quyền được thông báo: Trước khi xử lý TTCN, người xử lý TTCN phải cung cấp thông báo cho các cá nhân về cách TTCN của họ sẽ được xử lý.

Thứ hai, quyền truy cập: Theo PIPL, cá nhân có quyền yêu cầu đơn vị xử lý TTCN tiếp cận TTCN của mình một cách hợp pháp.

Thứ ba, quyền cải chính: Theo quy định của PIPL, trong trường hợp TTCN có sai sót hoặc chưa đầy đủ, cá nhân có quyền yêu cầu đơn vị xử lý TTCN chỉnh sửa.

Thứ tư, quyền tẩy xoá (erasure): Theo PIPL, cá nhân có quyền yêu cầu đơn vị xử lý TTCN xóa TTCN của mình khi có một trong các điều kiện sau:

Một là, mục đích xử lý đã đạt được, không thể đạt được hoặc TTCN không còn cần thiết để đạt được mục đích xử lý;

Hai là, bên xử lý TTCN ngừng cung cấp sản phẩm hoặc dịch vụ hoặc thời gian lưu giữ đã hết;

Ba là, cá nhân hủy bỏ sự đồng ý;

Bốn là, nơi người xử lý TTCN đã xử lý TTCN vi phạm pháp luật, quy định hành chính hoặc thỏa thuận; hoặc

Năm là, các trường hợp khác do pháp luật hoặc quy định hành chính quy định.

Thứ năm, quyền phản đối (từ chối): Theo PIPL, cá nhân có quyền phản đối việc xử lý TTCN.

Thứ sáu, quyền đối với tính di động của dữ liệu: Theo PIPL, các cá nhân có thể yêu cầu người xử lý TTCN chuyển TTCN của họ cho người xử lý TTCN được chỉ định.

Thứ bảy, quyền từ chối sự ra quyết định tự động: Theo PIPL, những người xử lý TTCN phải đảm bảo tính minh bạch và công bằng của việc ra quyết định tự động. Nghiêm cấm việc phân biệt đối xử về giá và các điều kiện giao dịch khác đối với các cá nhân. Trong trường hợp các cá nhân

[23] Chương II PIPL.
[24] Chương IV PIPL.

cho rằng việc ra quyết định tự động có tác động đáng kể đến lợi ích của họ, các cá nhân đó có quyền yêu cầu đơn vị xử lý TTCN giải thích lý do và có thể từ chối khi quyết định được đưa ra thông qua các phương tiện tự động. Nếu quy trình xử lý TTCN áp dụng việc ra quyết định tự động để tiến hành tiếp thị và nhắn tin, thì tùy chọn không hướng đến các tính năng cá nhân hoặc tùy chọn từ chối việc ra quyết định tự động cũng sẽ được cung cấp.

Thứ tám, các quyền khác: Theo PIPL, các cá nhân cũng có thể yêu cầu người xử lý TTCN sao chép TTCN của họ và hạn chế xử lý TTCN của họ. Đối với cá nhân đã chết, những người thân thích của họ có thể vì lợi ích hợp pháp, chính đáng của mình mà thực hiện các quyền tham khảo, sao chép, sửa chữa, xóa... những TTCN của người chết, trừ trường hợp cá nhân đã chết có sự sắp xếp khác trước khi chết.

1.3.5. Các nghĩa vụ chính của đơn vị xử lý thông tin[25]

Thứ nhất, yêu cầu về sự đồng ý: Trước khi thu thập hoặc xử lý TTCN của ai đó, đơn vị xử lý thông tin phải nhận được sự đồng ý tự nguyện, rõ ràng và có hiểu biết của chủ thể thông tin[26]. Người xử lý thông tin thu thập hoặc xử lý "TTCN nhạy cảm" - một danh mục bao gồm sinh trắc học, niềm tin tôn giáo, danh tính cụ thể, chăm sóc y tế, tài khoản tài chính, nơi ở và các thông tin khác, cũng như TTCN của trẻ vị thành niên dưới mười bốn tuổi. Ngoài ra, phải chỉ ra mục đích cụ thể và sự cần thiết của việc thu thập dữ liệu và tuân theo một số biện pháp bảo vệ dữ liệu nghiêm ngặt được chỉ định trong PIPL. Tuy nhiên, có một số trường hợp miễn trừ theo luật mà không cần phải có sự đồng ý trước, bao gồm, ví dụ, thực hiện nghĩa vụ theo hợp đồng hoặc theo luật định, ứng phó với trường hợp khẩn cấp liên quan đến tính mạng và tài sản, đưa tin về một vấn đề được công chúng quan tâm và nơi thông tin đã được tìm thấy trong phạm vi công cộng.

Thứ hai, yêu cầu bản địa hoá dữ liệu và xoá dữ liệu: PIPL quy định rằng, nếu khối lượng TTCN được xử lý bởi bộ xử lý dữ liệu đạt đến các ngưỡng nhất định, yêu cầu bản địa hóa dữ liệu có thể được kích hoạt và bộ xử lý dữ liệu cũng sẽ được yêu cầu chỉ định một nhân viên bảo vệ thông tin để giám sát việc xử lý và bảo vệ đúng cách của DLCN được thu thập. Người xử lý dữ liệu được yêu cầu xóa DLCN đã thu thập khi mục đích thu thập đã đạt được, khi thông tin không còn phục vụ mục đích được tiết lộ, khi dịch vụ không còn được cung cấp, khi hết thời gian lưu giữ, khi người dùng hủy bỏ sự đồng ý hoặc khi các hoạt động xử lý trái với pháp luật và các quy định có liên quan.

Thứ ba, hạn chế chuyển giao TTCN cho bên thứ ba và nước ngoài: Trước khi người xử lý dữ liệu có thể chuyển TTCN cho bên thứ ba, ở Trung Quốc hoặc nước ngoài, trước tiên họ phải có được sự đồng ý của chủ thể dữ liệu và đảm bảo rằng việc sử dụng dữ liệu và phương pháp xử lý dữ liệu của người nhận dữ liệu tuân thủ các điều khoản bảo vệ dữ liệu theo sự đồng ý của chủ thể dữ liệu. Đối với chuyển giao xuyên biên giới, bộ xử lý dữ liệu cũng phải đảm bảo rằng người nước ngoài nhận dữ liệu cần bảo vệ dữ liệu không kém nghiêm ngặt hơn các yêu cầu do PIPL áp đặt. Tùy thuộc vào phân loại của quá trình xử lý dữ liệu dựa trên độ nhạy và khối lượng dữ liệu mà nó sở hữu, có thể áp dụng các yêu cầu bổ sung. Ví dụ: Giám đốc thông tin (CIO) và các công ty sở hữu khối lượng lớn DLCN phải hoàn thành đánh giá bảo mật bắt buộc do Cơ quan quản lý không gian mạng Trung Quốc

[25] Chương V PIPL.
[26] Điều 13 PIPL.

thực hiện trước khi truyền bất kỳ dữ liệu nào ra nước ngoài.

Thứ tư, yêu cầu tuân thủ chung: PIPL yêu cầu các công ty xử lý DLCN tiến hành tự kiểm tra thường xuyên để đánh giá rủi ro bảo mật thông tin của họ và thực hiện các chính sách và biện pháp bảo vệ tương ứng. Các quy tắc ngày càng nghiêm ngặt hơn có thể được áp dụng tùy thuộc vào việc một công ty có đủ điều kiện là "nền tảng dịch vụ Internet lớn", có "số lượng lớn" người dùng và tham gia vào "các hoạt động kinh doanh phức tạp" hay không, nhưng những điều khoản đó không được định nghĩa trong luật. Các công ty sử dụng thuật toán và các chức năng ra quyết định tự động tương tự để phân tích TTCN của chủ thể dữ liệu phải tuân thủ các nguyên tắc "minh bạch" và "công bằng" nhất định được quy định trong PIPL nghiêm cấm một số loại hoạt động tiếp thị và định giá phân biệt đối xử dựa trên trạng thái cá nhân của chủ thể dữ liệu và các đặc điểm được bảo vệ.

Điều thú vị là, Điều 58 trực tiếp đề cập rõ ràng đến những bên xử lý TTCN cung cấp "các dịch vụ nền tảng Internet quan trọng" với số lượng người dùng lớn, có mô hình kinh doanh phức tạp và quy định cụ thể nghĩa vụ của họ[27]. Tuy nhiên, các nền tảng mạng xã hội như Facebook, YouTube và Instagram... có sự hiện diện với số lượng người dùng khổng lồ ở những nơi khác trên thế giới nhưng lại bị chặn ở Trung Quốc.

1.3.6. Miễn trừ tuân thủ Luật Bảo vệ thông tin cá nhân Trung Quốc năm 2021

Người xử lý có thể được miễn cung cấp thông báo rõ ràng và kịp thời cho các cá nhân trong một số trường hợp, chẳng hạn như trong các trường hợp khẩn cấp để bảo vệ tính mạng, sức khỏe hoặc an ninh của thể nhân và tài sản của họ. Tuy nhiên, khi tình trạng khẩn cấp kết thúc, người xử lý phải thông báo và cung cấp thông tin cần thiết.

Như đã lưu ý, thông tin ẩn danh không được phân loại theo cùng một cách hoặc tuân theo cùng cơ sở pháp lý và các yêu cầu khác, trong nhiều trường hợp, như TTCN vẫn có thể nhận dạng được.

1.3.7. Thiết lập các quy tắc cung cấp thông tin cá nhân xuyên biên giới

Quy định về cung cấp TTCN xuyên biên giới được quy định tại Chương 3, từ Điều 38 đến Điều 43 PIPL.

Nguyên tắc cốt lõi của cung cấp TTCN xuyên biên giới trong PIPL là đặc trưng của Trung Quốc. Trong các luật bảo vệ dữ liệu khác, chẳng hạn như GDPR, cơ sở cốt lõi để truyền dữ liệu xuyên biên giới là "mức độ bảo vệ tương đương". Cả cơ chế miễn trừ (chẳng hạn như danh sách trắng, quyết định thỏa đáng và BCR) và cơ chế kiến trúc giao thức (chẳng hạn như SCC) đều được thiết kế để xác nhận hoặc đảm bảo rằng người nhận cung cấp cơ chế bảo mật để bảo vệ TTCN tương đương với cơ chế của bộ xử lý và nhằm mục đích ngăn chặn rò rỉ thông tin, lạm dụng và các sự cố khác. Tuy nhiên, cơ sở cốt lõi của PIPL là "vượt qua đánh giá

[27] Điều 58 PIPL quy định: Đơn vị xử lý thông tin cá nhân cung cấp các dịch vụ quan trọng trên nền tảng Internet, có số lượng người dùng lớn, loại hình kinh doanh phức tạp phải thực hiện các nghĩa vụ sau: (1) Thiết lập và cải thiện hệ thống tuân thủ bảo vệ thông tin cá nhân theo quy định của quốc gia và thành lập một tổ chức độc lập chủ yếu bao gồm các thành viên bên ngoài để giám sát việc bảo vệ thông tin cá nhân; (2) Tuân thủ các nguyên tắc cởi mở, công bằng và khách quan, xây dựng các quy tắc nền tảng và làm rõ các tiêu chuẩn xử lý thông tin cá nhân và nghĩa vụ bảo vệ thông tin cá nhân của các nhà cung cấp sản phẩm hoặc dịch vụ trên nền tảng; (3) Ngừng cung cấp dịch vụ cho các nhà cung cấp sản phẩm hoặc dịch vụ trên nền tảng vi phạm nghiêm trọng pháp luật và các quy định hành chính trong việc xử lý thông tin cá nhân; (4) Thường xuyên phát hành các báo cáo trách nhiệm xã hội về bảo vệ thông tin cá nhân và chấp nhận sự giám sát của xã hội.

bảo mật và đạt được chứng nhận". Cả việc "vượt qua kỳ đánh giá an ninh do cơ quan quản lý không gian mạng quốc gia tổ chức" và "đạt được chứng nhận bảo vệ TTCN của một tổ chức chuyên nghiệp theo quy định của cơ quan quản lý không gian mạng quốc gia" đều nhằm đảm bảo an ninh thực chất do người nhận cung cấp. Mặc dù điều khoản này bắt nguồn từ bối cảnh tuân thủ quy định chặt chẽ của Trung Quốc, đánh giá thực chất này đối với người nhận đáng tin cậy hơn và hiệu quả hơn trong việc đảm bảo an toàn thông tin người dùng so với các yêu cầu tương đương của môi trường tuân thủ. Ngoài ra, để bù đắp những thiếu sót của hệ thống đánh giá và chứng nhận cũng như đáp ứng nhu cầu của hoạt động kinh doanh, PIPL tạo cơ sở pháp lý vững chắc hơn bằng cách bổ sung một thỏa thuận tiêu chuẩn như một trong những điều kiện.

Không giống như các điều khoản cung cấp thông tin xuyên biên giới ở các quốc gia khác, "không có điều khoản vi phạm nào được chỉ định" trong PIPL. Hầu hết các luật bảo vệ dữ liệu khác bao gồm các điều khoản vi phạm đối với các biện pháp bảo vệ, chẳng hạn như "sự đồng ý" và "cần thiết để thực hiện hợp đồng". Do đó, trong trường hợp không có các biện pháp bảo vệ thích hợp, vẫn có thể thực hiện chuyển thông tin với sự đồng ý rõ ràng của cá nhân nếu có các quy tắc ràng buộc của công ty. Theo PIPL, không có sự hạn chế nào đối với việc chuyển giao xuyên biên giới bất kể cơ sở pháp lý, vì vậy việc chuyển giao phải đáp ứng tất cả các điều kiện tiên quyết tương ứng, phản ánh nguyên tắc lập pháp của Trung Quốc về ưu tiên bảo mật dữ liệu quốc gia.

2. Bảo vệ dữ liệu cá nhân theo quy định của pháp luật Việt Nam

Tại Việt Nam, ngày 17/4/2023 Chính phủ ban hành Nghị định 13/2023/NĐ-CP có hiệu lực từ ngày 01/7/2023. Nghị định 13/2023/NĐ-CP có bố cục 04 chương với 44 điều quy định về: Những quy định chung (Chương I, từ Điều 1 đến Điều 8); hoạt động bảo vệ dữ liệu cá nhân (Chương II, từ Điều 9 đến Điều 31); trách nhiệm của cơ quan, tổ chức, cá nhân (Chương III, từ Điều 32 đến Điều 42) và điều khoản thi hành (Chương IV, từ Điều 43 đến Điều 44).

Việc ban hành Nghị định 13/2023/NĐ-CP là phù hợp với xu hướng chung trong thời đại công nghệ kỹ thuật số, việc cân bằng lợi ích giữa chủ thể dữ liệu với sự phát triển kinh tế cần được xem xét đảm bảo một cách hài hoà.

Phần trên của bài viết này đã trình bày một cách tổng quát nhất về quá trình hình thành và phát triển của các quy định bảo vệ DLCN tại Trung Quốc – quốc gia đông dân nhất trên thế giới và nền công nghệ kỹ thuật, kinh tế thuộc hàng đầu thế giới. Một điều không thể phủ nhận, quan điểm lập pháp của Trung Quốc đi kèm với việc bảo đảm quyền của các cá nhân, đặc biệt là đối với dữ liệu của họ trong thời đại kinh tế kỹ thuật số. Dưới góc độ nghiên cứu của mình, tác giả đưa ra quan điểm cá nhân và nêu một số ý kiến sau đối với các quy định của Nghị định 13/2023/NĐ-CP:

Thứ nhất, về kỹ thuật lập pháp: Tại Trung Quốc, PIPL là văn bản luật thống nhất các quy định về bảo vệ DLCN trong thời đại kỹ thuật số và có ý nghĩa quan trọng trong việc bảo vệ tốt nhất DLCN. Thêm vào đó, PIPL là một văn bản luật được xây dựng căn cứ trên Hiến pháp, điều này tạo nên cơ sở pháp lý hết sức vững chắc.

Còn ở Việt Nam, quy định bảo vệ DLCN được xây dựng dưới hình thức văn bản dưới luật, cụ thể là cấp độ "Nghị định", và căn cứ để xây dựng Nghị định này là BLDS, Luật An ninh quốc gia, Luật An

ninh mạng và Luật Xử lý vi phạm hành chính. Theo tác giả, quyền được bảo vệ DLCN là một quyền tối quan trọng của cá nhân, đặc biệt là trong giai đoạn kinh tế kỹ thuật số như hiện nay, quyền này cũng phù hợp với Hiến pháp. Do đó, tác giả ủng hộ kỹ thuật lập pháp mang tính chặt chẽ và thống nhất của Trung Quốc khi thiết kế PIPL là một văn bản cấp độ luật thay vì một Nghị định như Việt Nam.

Thứ hai, về khái niệm DLCN: Khoản 1 Điều 2 Nghị định 13/2023/NĐ-CP quy định: "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 với một con người cụ thể hoặc giúp xác định một con người cụ thể". Và "Thông tin giúp xác định một con người cụ thể là thông tin hình thành từ hoạt động của cá nhân mà khi kết hợp với các dữ liệu, thông tin lưu trữ khác có thể xác định một con người cụ thể[28]".

Khái niệm này khái quát một cách tương đối DLCN là gì, so với Dự thảo thì khái niệm DLCN tại Nghị định 13/2023/NĐ-CP hoàn chỉnh hơn khi đã ghi nhận cách xác định DLCN. Tuy nhiên, Nghị định 13/2023/NĐ-CP hiện đã bỏ đi quy định về *"ẩn danh DLCN"* so với Dự thảo trước đó (khoản 14 Điều 2 Dự thảo). Không biết lý do vì sao cơ quan soạn thảo đã bỏ đi vấn đề này, theo ý kiến của tác giả thì có thể cơ quan soạn thảo vẫn chưa tìm được cách quy định hoàn chỉnh (vì bản thân Dự thảo cũng không làm được việc này, và Nghị định 13/2023/NĐ-CP đã bỏ hẳn). Tuy nhiên, việc không đề cập đến "ẩn danh DLCN" không làm biến mất vấn đề. Vấn đề được đề cập là, các dữ liệu ẩn danh (đề cập đến quá trình DLCN không thể xác định được một thể nhân cụ thể sau khi xử lý và không thể phục hồi) có còn là DLCN và có chịu sự điều chỉnh của Nghị định 13/2023/NĐ-CP hay không. Do đó, tác giả đề nghị cần phải nghiên cứu thêm vấn đề này, có thể dựa trên Điều 4 PIPL, nên ghi nhận theo hướng dữ liệu ẩn danh không phải là DLCN và do đó không thuộc phạm vi điều chỉnh của Nghị định 13/2023/NĐ-CP.

Thứ ba, DLCN cơ bản và DLCN nhạy cảm: Khoản 3 và khoản 4 Điều 2 Nghị định 13/2023/NĐ-CP lần lượt quy định về DLCN cơ bản và DLCN nhạy cảm, bằng cách liệt kê. Với cấu trúc của Nghị định 13/2023/NĐ-CP, tác giả hiểu rằng không có sự phân biệt về cách xử lý giữa hai loại thông tin này, có một số ít nội dung trong Nghị định 13/2023/NĐ-CP đề cập đến việc khi xử lý DLCN nhạy cảm cần phải đăng ký với Uỷ ban bảo vệ DLCN, sự đồng ý của chủ thể dữ liệu... Theo tác giả, quy định này tạo ra những "vùng chồng lấn" nhất định khi áp dụng. Để hạn chế vấn đề này, cần tách "xử lý TTCN nhạy cảm" thành một mục riêng trong Nghị định 13/2023/NĐ-CP sẽ hợp lý hơn khi áp dụng trên thực tế và cũng hạn chế sự chồng lấn về việc xử lý dữ liệu.

Bên cạnh đó, Điều 20 Nghị định 13/2023/NĐ-CP quy định về xử lý dữ liệu trẻ em, theo tác giả, dữ liệu trẻ em cũng bao gồm DLCN cơ bản và DLCN nhạy cảm. Tuy nhiên, trẻ em là đối tượng cần bảo vệ đặc biệt nên DLCN của trẻ em trong thời đại kỹ thuật số cũng cần được bảo vệ nghiêm ngặt. Kinh nghiệm từ PIPL cho thấy, Trung Quốc ghi nhận thông tin của trẻ em dưới mười bốn tuổi là TTCN nhạy cảm, do đó được xử lý dựa trên các nguyên tắc xử lý TTCN nhạy cảm. Đây là kinh nghiệm mà Việt Nam cũng cần học tập.

[28] Khoản 2 Điều 2 Nghị định 13/2023/NĐ-CP.