

BẢO VỆ DỮ LIỆU SINH TRẮC HỌC TRONG KỶ NGUYÊN SỐ THEO PHÁP LUẬT MỘT SỐ QUỐC GIA VÀ KINH NGHIỆM CHO VIỆT NAM

ĐÀM THỊ DIỄM HẠNH* - NGUYỄN HUỖNH NHƯ -
NGUYỄN PHẠM TUỆ TÂM - QUẢN PHẠM ANH THƯƠNG**

Tóm tắt: Trong kỷ nguyên số, dữ liệu sinh trắc học (vân tay, khuôn mặt, mống mắt, giọng nói...) ngày càng được ứng dụng rộng rãi trong lĩnh vực tài chính, y tế, thương mại điện tử và quản lý Nhà nước. Tại Việt Nam, mặc dù Luật An ninh mạng năm 2018; Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân và mới đây là Luật Bảo vệ dữ liệu cá nhân được Quốc hội thông qua ngày 26/6/2025, sẽ có hiệu lực vào 01/01/2026 đã bước đầu điều chỉnh khung pháp lý về bảo vệ cá nhân nói chung nhưng chưa đủ để bảo vệ dữ liệu sinh trắc học - một loại dữ liệu cá nhân đặc biệt. Bài viết nghiên cứu pháp luật bảo vệ dữ liệu sinh trắc học của một số quốc gia, từ đó đề xuất bài học cho Việt Nam.

Từ khóa: Dữ liệu sinh trắc học; bảo mật; kỷ nguyên số

Ngày nhận bài: 07/3/2025; Biên tập xong: 12/8/2025; Duyệt đăng: 22/8/2025

PROTECTING BIOMETRICAL DATA IN THE DIGITAL AGE UNDER THE LAWS OF SEVERAL COUNTRIES AND LESSONS FOR VIETNAM

Abstract: In the digital era, biometric data - such as fingerprints, facial features, iris patterns, and voice - is increasingly utilized in finance, healthcare, e-commerce, and public administration. In Vietnam, although legal instruments including the 2018 Law on Cybersecurity, the 2023 Decree on Personal Data Protection, and most recently the Law on Personal Data Protection, enacted by the National Assembly on June 26, 2025 and effective from January 1, 2026, have established an initial framework for personal data protection in general, they are not enough to protect biometric data, which is a special type of personal data. This paper examines the legal frameworks governing biometric data protection in selected countries, thereby proposing recommendations for Vietnam.

Keywords: Biometric data; security; digital era

Received: Mar 07, 2025; **Editing completed:** Aug 12, 2025; **Accepted for publication:** Aug 22, 2025

Đặt vấn đề

Dữ liệu sinh trắc học là những thông tin chi tiết về bộ phận cơ thể của một người, loại dữ liệu này mang khả năng chứng minh, nhận dạng được người đó là ai. Dữ liệu sinh trắc học được chia thành hai loại: Sinh trắc học vật lý và sinh trắc học hành vi. Bài viết chỉ đề cập đến sinh trắc học vật lý.

Với khả năng nhận diện tuyệt đối, chức năng bảo mật cao, lợi thế trong việc lưu trữ dữ liệu gốc, tiết kiệm thời gian khi sử dụng, dữ liệu sinh trắc học đang ngày một được ưa chuộng, là sự ưu tiên đối với “sự chạy đua” phát triển của lĩnh vực công nghệ trong kỷ nguyên số ngày nay. Tuy nhiên, các chủ thể thu thập, sử dụng dữ liệu này cần phải nhìn nhận một vấn đề: Dữ liệu sinh trắc học là loại dữ liệu gắn bó mật thiết với quyền nhân thân, quyền riêng tư của mỗi chủ thể hơn hết tất cả các loại dữ liệu khác. Các loại dữ liệu như mật khẩu chữ/số có thể thay đổi để chấm dứt hệ lụy của việc bị xâm phạm, nhưng dữ liệu sinh trắc học lại gắn liền một cách vật lý với cơ thể của chủ nhân dữ liệu. Với tốc độ lan

truyền mà môi trường Internet mang lại, cùng các mảnh khé, thủ thuật đánh cắp tinh vi trong thời đại công nghệ thì trong trường hợp dữ liệu sinh trắc học không được bảo đảm an toàn, rò rỉ, bị đánh cắp thì hậu quả sẽ vô cùng nghiêm trọng. Do đó, bảo mật dữ liệu sinh trắc học là một vấn đề cần được, coi trọng trong thời đại kỷ nguyên số hiện nay.

Vấn đề bảo mật dữ liệu sinh trắc học đã được một số quốc gia đặc biệt chú trọng. Họ đã xây dựng nên những khung pháp lý quy định các cơ chế bảo mật dữ liệu sinh trắc học như: Chủ thể thực hiện bảo vệ, công nghệ phục vụ cho việc bảo vệ, quy trình phương pháp tiến hành bảo mật dữ liệu, trách nhiệm pháp lý khi vi phạm nghĩa vụ bảo mật... Một số quốc gia tiên phong trong việc bảo mật dữ liệu sinh trắc học như Nga, Brazil, Trung Quốc và Hoa Kỳ. Tại Việt Nam, dữ liệu sinh trắc học đã được đề cập đến trong một số văn bản pháp luật, nhưng về vấn đề bảo mật lại chưa được cụ thể, chúng

* Email: Dtdhanh@hou.edu.vn

Tiến sĩ, Trường Đại học Mô Hà Nội

** Sinh viên Trường Đại học Luật Hà Nội

ta vẫn phải tiếp cận trên phương diện bảo mật chung về thông tin cá nhân. Trước những hậu quả khi dữ liệu này không được đảm bảo trong khâu bảo mật, việc đặt ra các quy định pháp lý liên quan đến việc bảo mật là điều vô cùng cần thiết để Việt Nam có thể khai thác được những lợi ích của dữ liệu sinh trắc học trong thời đại kỷ nguyên mới ngày nay.

1. Hạn chế, vướng mắc đối với việc bảo vệ dữ liệu sinh trắc học tại Việt Nam

Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 được Quốc hội thông qua trong bối cảnh nhu cầu bảo vệ quyền riêng tư ngày càng gia tăng tại Việt Nam. Đây là văn bản pháp lý đầu tiên có hiệu lực cao nhất điều chỉnh toàn diện về xử lý dữ liệu cá nhân. Tuy nhiên, bên cạnh những đóng góp tích cực, Luật vẫn còn tồn tại một số hạn chế nhất định, đặc biệt là ở tính khái quát của khung pháp lý và việc phân định chưa rõ ràng trách nhiệm giữa các cơ quan quản lý.

Thứ nhất, theo quy định của Luật Bảo vệ dữ liệu cá nhân năm 2025, dữ liệu sinh trắc học vẫn chưa có sự ưu tiên trong hệ thống bảo mật thông tin của quốc gia. Những hệ quả từ việc xâm phạm dữ liệu sinh trắc học không thể chấm dứt ngay lập tức giống như các loại dữ liệu thông tin dạng số/chữ khác. Do đó, cần phải đặt việc ưu tiên thực hiện bảo vệ dữ liệu sinh trắc học lên hàng đầu để có thể đối phó với những hành vi xâm phạm tinh vi đang phát triển song song với công nghệ cao. Thực tế ở một số quốc gia có tỷ lệ tội phạm mạng cao như Hoa Kỳ đã đặc biệt chú trọng và ưu tiên bảo vệ dữ liệu sinh trắc học trong hệ thống thông tin cá nhân. Điều đó cho thấy, từ thực tế của xã hội công nghệ hóa ngày nay, nếu chúng ta không coi trọng việc bảo vệ dữ liệu sinh trắc học thì khả năng gánh chịu những hậu quả từ hành vi xâm nhập, đánh cắp dữ liệu sinh trắc học là không thể tránh khỏi.

Thứ hai, việc đánh giá tác động của hệ thống bảo mật vẫn chưa được chú ý đến. Để đảm bảo rằng việc thực hiện bảo mật dữ liệu sinh trắc học sẽ mang lại hiệu quả thì việc đánh giá trước và trong quá trình bảo mật là điều vô cùng cần thiết. Thực tế, không có một hệ thống bảo mật “một lần và mãi mãi” nào có thể đối phó hiệu quả với các mối đe dọa an ninh mạng đang không ngừng tiến hóa. Việc giữ mãi một chương trình bảo vệ cố định giống như xây dựng một pháo đài chỉ để chống lại những cuộc tấn công đã biết trong quá khứ. Trong khi đó, các con đường xâm nhập và truy cập bất hợp pháp đang ngày càng đa dạng, tinh vi hơn. Nếu không có sự đánh giá định kỳ và điều chỉnh liên tục, hệ thống bảo mật sẽ nhanh

chóng trở nên bị động trước tội phạm công nghệ cao. Khả năng ứng phó trước các cuộc xâm nhập sẽ trở nên khó khăn, thậm chí là bất khả thi, dẫn đến những hậu quả không thể chấm dứt ngay lập tức đối với loại dữ liệu đặc biệt nhạy cảm này.

2. Pháp luật của một số quốc gia về việc bảo vệ dữ liệu sinh trắc học

Tại Hoa Kỳ, Illinois và Texas là 02 tiểu bang đi đầu trong các quy định về dữ liệu sinh trắc học. Việc bảo vệ dữ liệu sinh trắc học tại 02 tiểu bang này được chú trọng với các khía cạnh linh hoạt và ưu tiên, cụ thể:

Với Illinois, Biometric Information Privacy Act (BIPA) - “Đạo luật bảo vệ thông tin dữ liệu sinh trắc học” của bang Illinois¹ đặt việc bảo vệ dữ liệu sinh trắc học phải được thực hiện phù hợp với từng ngành, lĩnh vực đã thu thập dữ liệu sinh trắc học². Đồng thời, dữ liệu sinh trắc học phải được ưu tiên bảo vệ hơn so với các loại dữ liệu khác³. Trong từng ngành nghề, dữ liệu sinh trắc học sẽ đóng vai trò quan trọng nhất định, đồng thời khả năng thực hiện, phương pháp được sử dụng cho việc bảo vệ sẽ có sự chênh lệch giữa các lĩnh vực hoạt động. Một doanh nghiệp thực hiện việc kinh doanh các công thức của chương trình máy tính sẽ có khả năng bảo vệ khác với một trường tiểu học. Hơn nữa, mức độ ảnh hưởng của công nghệ số trong từng môi trường cũng sẽ có sự khác biệt. Do đó, cơ chế linh hoạt trong việc bảo vệ dữ liệu sinh trắc học cũng cần được lưu ý trong việc thực hiện hoạt động này.

Với Texas, tiểu bang này sẽ sử dụng cơ chế ưu tiên việc bảo vệ dữ liệu sinh trắc học⁴, tức là việc thực hiện các biện pháp để bảo vệ dữ liệu sinh trắc học mà họ đã thu thập phải là tối ưu nhất trong khả năng vận hành và hoạt động của họ. Ở một góc độ nào đó, có thể hiểu là trong cùng một điều kiện thì phải sử dụng tài nguyên cho việc bảo vệ đến khi đảm bảo được dữ liệu sinh trắc học được bảo vệ một cách an toàn nhất.

Đối với Trung Quốc, quá trình bảo vệ đã được xây dựng thành một hệ thống quy định chi tiết hóa và toàn diện. Trung Quốc đã đưa ra các quy định cụ thể về những việc cần làm⁵ nhằm đảm bảo việc bảo vệ dữ liệu sinh trắc

¹ BIPA, <https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57>, truy cập ngày 16/02/2025.

² BIPA §15,(e)(1).

³ BIPA §15,(e)(2).

⁴ Capture or Use of Biometric Identifier Act §503.001,(c),(2) - Mục 503.001 (c),(2) Chương 503 quy định về các đặc điểm dữ liệu sinh trắc học, Bộ luật Kinh doanh và Thương mại, Bang Texas, Hoa Kỳ.

⁵ Điều 63 Luật Bảo vệ thông tin cá nhân của Trung Quốc - Personal Information Protection Law (PIPL).

học một cách hiệu quả. Khung pháp lý này bao gồm việc phân định rõ ràng nhiệm vụ, trách nhiệm của từng cơ quan⁶ thực hiện và quy định sự phối hợp liên ngành⁷. Các biện pháp kỹ thuật trong xử lý được triển khai cụ thể là: Xây dựng hệ thống quản lý nội bộ và quy trình hoạt động, quản lý thông tin cá nhân theo phân loại, thực hiện các biện pháp bảo vệ kỹ thuật tương ứng như mã hóa và xóa nhận dạng, xác định hợp lý thẩm quyền xử lý thông tin và tiến hành giáo dục và đào tạo về an ninh cho nhân viên một cách thường xuyên, xây dựng và tổ chức thực hiện các phương án ứng phó khẩn cấp đối với các sự cố an ninh thông tin⁸. Song song với thực hiện các biện pháp bảo vệ, Trung Quốc còn đặt ra yêu cầu đánh giá tác động bảo vệ thông tin⁹ bao gồm: Mục đích và phương pháp xử lý thông tin, quyền lợi của chủ thể dữ liệu, các biện pháp được sử dụng. Có thể thấy sự cụ thể, chi tiết, rõ ràng trong quá trình sử dụng và lưu trữ của Trung Quốc đối với việc bảo vệ dữ liệu sinh trắc học là điều cần thiết đối với vị trí của quốc gia này trong thời đại kỷ nguyên số.

Chính phủ Liên bang Nga đã thiết lập quy trình pháp lý toàn diện nhằm đảm bảo an toàn dữ liệu sinh trắc học và điều chú trọng ở đây mà Nga đặt ra chính là “đánh giá hiệu quả của các biện pháp được thực hiện để đảm bảo tính bảo vệ của dữ liệu cá nhân trước khi đưa vào hoạt động hệ thống lưu trữ dữ liệu cá nhân”¹⁰. Từ giai đoạn thu thập, trước khi đưa dữ liệu vào hệ thống thông tin, cần phải xác định những mối đe dọa đối với dữ liệu sinh trắc học, xem xét các biện pháp, kỹ thuật, phương tiện phục vụ cho việc bảo vệ các dữ liệu sinh trắc học được đưa vào hệ thống thông tin¹¹. Trong thời đại mà công nghệ kỹ thuật không ngừng phát triển, việc đánh giá hiệu quả bảo vệ là hoạt động hết sức cần thiết và thiết thực, vì một hệ thống bảo vệ có thể được duy trì cố định, nhưng các hành vi xâm nhập phá hoại, truy cập trái phép, ăn cắp thông tin... lại ngày càng đa dạng, tinh vi, mang tính thủ thuật cao, khó có thể lường trước. Ngoài ra, chủ thể¹² thực hiện bảo vệ cũng được Nga quy định một cách cụ thể.

⁶ Điều 61 PIPL.

⁷ Điều 60, Điều 62 PIPL.

⁸ Điều 51 PIPL.

⁹ Điều 55 PIPL.

¹⁰ Điều 19.2.4 Luật liên bang số 152-FZ ngày 27/7/2006 về dữ liệu cá nhân, với các sửa đổi và bổ sung ngày 25/11, ngày 27/12/2009, ngày 28/6, ngày 27/7, ngày 29/11, ngày 23/12/2010, ngày 04/6, ngày 25/7/2011, ngày 05/4, ngày 23/7, ngày 21/12/2013, ngày 04/6/2014, (Luật liên bang số 152-FZ).

¹¹ Điều 19.2.1 và Điều 19.2.2 Luật liên bang số 152-FZ.

¹² Điều 7 Luật liên bang số 152-FZ.

Một quốc gia khác cũng cho thấy sự cần thiết đối với việc xây dựng khung pháp lý về bảo vệ dữ liệu sinh trắc học, là Brazil với Brazilian General Data Protection Law - LGPD¹³. Và tương tự như Trung Quốc, vấn đề bảo vệ được LGPD đặt ra cả trong quá trình sử dụng, nếu muốn sử dụng các dữ liệu sinh trắc học thì phải đảm bảo cho hệ thống vận hành sử dụng có khả năng đáp ứng được các yêu cầu bảo đảm sự an toàn cho dữ liệu sinh trắc học¹⁴. Trong quá trình bảo vệ dữ liệu, Brazil đã thiết lập cơ chế ứng phó khẩn cấp cho phép các cơ quan bảo vệ dữ liệu triển khai ngay lập tức các biện pháp kỹ thuật can thiệp khi phát hiện xâm nhập trái phép¹⁵. Quy định này có thể góp phần ngăn chặn kịp thời việc rò rỉ thông tin, đặc biệt là những thông tin quan trọng như dữ liệu sinh trắc học. Giả sử một khung pháp lý không đặt ra quy định này, nếu có sự cố xảy ra, cần phải đề xuất biện pháp vô hiệu hóa, sau đó chờ đợi các cơ quan có thẩm quyền phê duyệt, như vậy khả năng bảo đảm an toàn cho thông tin khi bị rò rỉ là rất thấp. Đây cũng có thể coi là một biện pháp đối phó kịp thời với các hành động tấn công dữ liệu trong thời đại kỷ nguyên số đang bao phủ cuộc sống hiện nay.

3. Bài học kinh nghiệm cho Việt Nam

Ứng dụng dữ liệu sinh trắc học vào các hoạt động, lĩnh vực là một con đường giúp cho Việt Nam hòa nhập vào thời đại kỷ nguyên số ngày nay. Tuy nhiên, để có thể tận dụng, khai thác triệt để lợi ích song song với phòng ngừa, ngăn chặn tối đa hậu quả của sự tấn công, xâm nhập đối với dữ liệu sinh trắc học, Việt Nam cần có một khung pháp lý cụ thể đối với việc bảo vệ dữ liệu sinh trắc học. Việt Nam có thể tham khảo một số thành quả của các nước về pháp luật bảo vệ dữ liệu sinh trắc học, rút ra bài học kinh nghiệm thực tiễn để có thể xây dựng một khung pháp lý ưu việt đối với vấn đề bảo vệ dữ liệu sinh trắc học.

Đầu tiên, nên ưu tiên thực hiện việc bảo vệ dữ liệu sinh trắc học. Đây là một yếu tố thúc đẩy việc xây dựng khung pháp lý cụ thể để bảo vệ dữ liệu sinh trắc học. Như đã đề cập ở phần đặt vấn đề, sự ưu tiên xuất phát từ việc dữ liệu sinh trắc học là một thành phần gắn liền với cơ thể của mỗi con người, khả năng di chuyển vật lý các thành phần của dữ liệu sinh trắc học là rất thấp, trừ trường hợp can thiệp các biện pháp sinh học. Chính vì vậy, dữ liệu sinh trắc

¹³ Luật Bảo vệ dữ liệu chung - Lei Geral de Proteção de Dados (LGPD).

¹⁴ Điều 49 LGPD.

¹⁵ Điều 48 LGPD.

học nên được ưu tiên bảo vệ hơn so với các loại dữ liệu khác. Tuy nhiên, cần làm rõ sự ưu tiên ở đây có nghĩa là trong một điều kiện nhất định, các thiết bị, nguồn nhân lực phục vụ cho việc bảo vệ dữ liệu sinh trắc học cần được đầu tư cao hơn. Để làm rõ điều này, có thể tham khảo quy định “thực hiện các biện pháp để bảo vệ dữ liệu sinh trắc học mà họ đã thu thập phải là tối ưu nhất trong khả năng vận hành và hoạt động của họ”¹⁶ từ 02 tiểu bang của Hoa Kỳ.

Thứ hai, quy định về việc thực hiện đánh giá tác động bảo vệ với nội dung như: Mục đích, lĩnh vực thu thập và các lợi ích có liên quan. Khi xem xét mục đích và lĩnh vực bảo vệ sẽ dữ liệu được có nhất thiết phải thu thập hay không và trong lĩnh vực được thu thập có đủ điều kiện thực hiện các công tác bảo vệ dữ liệu hay không. Giả sử, một công ty muốn thu thập dữ liệu sinh trắc học khuôn mặt của người qua cầu để đảm bảo số tiền thu được sẽ tương thích với số người qua lại. Trong trường hợp này, cần xem xét xem công ty này có đủ khả năng đáp ứng các thiết bị bảo đảm an toàn cho dữ liệu sinh trắc học từ giai đoạn thu thập đến lúc xóa dữ liệu hay không? Đồng thời, đề xuất đánh giá một số biện pháp khác có thể thỏa mãn được nhu cầu của công ty này, ví dụ như lắp đặt camera ghi lại hình ảnh xe và người qua lại, hành động này cũng có thể kiểm soát được sự tương thích với số tiền mà không cần phải sử dụng đến dữ liệu sinh trắc học khuôn mặt. Như vậy, việc đánh giá tác động sẽ giúp loại bỏ một số trường hợp thu thập một cách không cần thiết, từ đó việc bảo vệ dữ liệu sinh trắc học sẽ được thực hiện một cách đúng việc, hợp lý hơn trong việc điều hành loại dữ liệu này.

Thứ ba, bài học trong việc duy trì đánh giá khả năng bảo vệ của các hệ thống, phương tiện sử dụng cho việc bảo vệ dữ liệu sinh trắc học. Duy trì đánh giá là một cách thức để ta có thể sớm phát hiện ra những lỗ hổng bảo mật trong hệ thống bảo vệ dữ liệu, từ đó kịp thời khắc phục. Đồng thời, đánh giá xem hệ thống cũng như phương tiện có còn đáp ứng đủ yêu cầu bảo vệ trước tần suất truy cập dữ liệu sinh trắc học cũng như trước các nguy cơ xâm nhập hay không. Duy trì việc đánh giá khả năng bảo vệ như một biện pháp trực tiếp chống lại sự tấn công, xâm nhập, rò rỉ, đánh cắp dữ liệu sinh trắc học mà Việt Nam phải đối mặt khi ứng dụng loại dữ liệu này trong thời đại kỹ nguyên số này.

Thứ tư, hướng dẫn cụ thể một số biện pháp, hành động mà các cơ quan chuyên trách có thể thực hiện ngay khi phát hiện dữ liệu bị tấn công bất ngờ. Trong thời đại kỹ

nguyên số, thủ đoạn xâm nhập ngày càng được cải tiến, diễn ra một cách nhanh chóng. Do đó, cần dự trù trước một số biện pháp có thể thực hiện ngay lập tức nhằm ngăn chặn, cắt đứt hành động xâm nhập đánh cắp. Việc dự trù hành động này cũng là công việc mà các cơ quan Bộ ngành cùng phối hợp thực hiện để đảm bảo tính chất chuyên môn, tăng khả năng thành công chống lại các thủ đoạn xâm nhập.

Kết luận

Dù có bước đi pháp lý chậm hơn so với một số quốc gia trong việc đảm bảo quyền riêng tư khi tiếp cận dữ liệu sinh trắc học, song qua quá trình nghiên cứu các khung pháp lý, cùng với việc rút ra bài học kinh nghiệm từ những thành công và hạn chế khi áp dụng các quy định pháp luật vào thực tiễn về việc bảo vệ dữ liệu sinh trắc học của các quốc gia, Việt Nam sẽ tránh được những sai lầm, cũng như lường trước được một số rủi ro có thể xảy ra trong quá trình bảo vệ dữ liệu sinh trắc học. Từ đó, việc xây dựng khung pháp lý quy định về bảo vệ dữ liệu sinh trắc học sẽ có được một tầm nhìn xa hơn, đề phòng, dự đoán được những nguy cơ mà thời đại kỹ nguyên số, công nghệ hóa phát triển một cách cao độ đặt ra cho nước ta trong việc ứng dụng dữ liệu này. Đây sẽ là cơ sở cho việc xây dựng hệ thống pháp luật Việt Nam thêm chặt chẽ và nghiêm minh hơn, tạo hành lang pháp lý an toàn, tin cậy, thuận lợi. Từ đó, góp phần cho sự phát triển kinh tế - xã hội trong giai đoạn kỷ nguyên phát triển mới, kỷ nguyên vươn mình của dân tộc Việt Nam./

TÀI LIỆU THAM KHẢO

1. Luật Bảo vệ dữ liệu cá nhân năm 2025;
2. *Biometric Information Privacy Act* (BIPA), 740 ILCS 14/ *Biometric Information Privacy Act*, <https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57>, truy cập ngày 16/02/2025;
3. *Capture or Use of Biometric Identifier Act*, <https://statutes.capitol.texas.gov/docs/bc/htm/bc.503.htm>, truy cập ngày 16/02/2025;
4. Luật liên bang số 152-FZ ngày 27/7/2006 về dữ liệu cá nhân (với các sửa đổi và bổ sung ngày 25/11, ngày 27/12/2009, ngày 28/6, ngày 27/7, ngày 29/11, ngày 23/12/2010, ngày 04/6, ngày 25/7/2011, ngày 05/4, ngày 23/7, ngày 21/12/2013, ngày 04/6/2014), <https://ivo.garant.ru/#/document/12148567/paragraph/24880:0>;
5. *Geral de Proteção de Dados* (LGPD), <https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/>, truy cập ngày 16/02/2025;
6. *Personal Information Protection Law* (PIPL), <https://personalinformationprotectionlaw.com/chapter-i-general-provisions/>, truy cập ngày 16/02/2025.

¹⁶ BIPA §503.001 (c) (2).