BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC PHAN THIẾT

TRỊNH VÕ HOÀNG

HOÀN THIỆN PHÁP LUẬT VỀ TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA KHÁCH HÀNG

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ
LUẬT KINH TẾ

Lâm Đồng – 2026

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC PHAN THIẾT

TRỊNH VÕ HOÀNG

HOÀN THIỆN PHÁP LUẬT VỀ TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA KHÁCH HÀNG

NGÀNH LUẬT KINH TẾ

MÃ SỐ: 8380107

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. **TS. Phạm Thị Hồng Tâm**
2. **TS. Nguyễn Thành Luân**

Lâm Đồng – 2026

NHẬN XÉT CỦA HỘI ĐỒNG XÉT DUYỆT

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Lâm Đồng, ngày tháng năm 2026

Hội đồng xét duyệt

LỜI CẢM ƠN

Trong quá trình học tập, nghiên cứu và thực hiện đề án "Hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng", tôi đã nhận được sự quan tâm, hướng dẫn và hỗ trợ quý báu từ quý Thầy, Cô, gia đình, bạn bè và các cá nhân có liên quan.

Trước hết, tôi xin bày tỏ lòng biết ơn sâu sắc đến TS. Phạm Thị Hồng Tâm và TS. Nguyễn Thành Luân đã tận tình hướng dẫn, định hướng khoa học, góp ý và hỗ trợ tôi trong suốt quá trình thực hiện đề án. Những ý kiến, chỉ dẫn của quý Thầy, Cô là cơ sở quan trọng giúp tôi hoàn thiện nội dung nghiên cứu một cách nghiêm túc và phù hợp hơn.

Tôi xin chân thành cảm ơn Ban Giám hiệu Trường Đại học Phan Thiết, quý Thầy, Cô Khoa Luật và các Thầy, Cô đã tham gia giảng dạy, truyền đạt kiến thức, tạo điều kiện thuận lợi cho tôi trong suốt quá trình học tập và nghiên cứu tại Trường.

Tôi cũng xin gửi lời cảm ơn đến gia đình, bạn bè và đồng nghiệp đã luôn động viên, chia sẻ và hỗ trợ tôi về tinh thần trong thời gian học tập và hoàn thành đề án này.

Mặc dù đã có nhiều cố gắng, nhưng do giới hạn về thời gian, kiến thức và kinh nghiệm nghiên cứu, đề án khó tránh khỏi những thiếu sót. Tôi rất mong nhận được sự góp ý của quý Thầy, Cô và Hội đồng để đề án được hoàn thiện hơn.

Xin trân trọng cảm ơn!

Học viên

Trịnh Võ Hoàng

LỜI CAM ĐOAN

Tôi xin cam đoan đề án "Hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng" là công trình nghiên cứu của riêng tôi, được thực hiện dưới sự hướng dẫn khoa học của giảng viên hướng dẫn.

Các nội dung nghiên cứu, nhận xét, đánh giá và kiến nghị trong đề án là kết quả của quá trình tìm hiểu, phân tích và tổng hợp từ các nguồn tài liệu có liên quan. Những thông tin, số liệu, vụ việc và tài liệu tham khảo được sử dụng trong đề án đều có nguồn gốc rõ ràng, được trích dẫn theo đúng quy định.

Tôi xin chịu hoàn toàn trách nhiệm về tính trung thực, chính xác của nội dung đề án và cam kết rằng đề án này chưa từng được sử dụng để bảo vệ hoặc công bố trong bất kỳ công trình nghiên cứu nào khác.

Học viên

Trịnh Võ Hoàng

TÓM TẮT TIẾNG VIỆT

Đề án "Hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng" nghiên cứu trách nhiệm pháp lý của doanh nghiệp trong quá trình thu thập, xử lý, lưu trữ, sử dụng, chia sẻ và bảo vệ dữ liệu cá nhân của khách hàng trong hoạt động kinh doanh. Trong bối cảnh chuyển đổi số và phát triển kinh tế số, dữ liệu cá nhân ngày càng trở thành nguồn tài nguyên quan trọng, giúp doanh nghiệp nâng cao hiệu quả quản trị, cải thiện chất lượng dịch vụ và gia tăng lợi thế cạnh tranh. Tuy nhiên, việc khai thác dữ liệu cá nhân cũng làm phát sinh nhiều nguy cơ xâm phạm quyền riêng tư, quyền nhân thân và quyền được bảo vệ dữ liệu của khách hàng, nhất là trước thực trạng rò rỉ, mua bán, sử dụng trái phép dữ liệu cá nhân trong các lĩnh vực như thương mại điện tử, tài chính – ngân hàng, viễn thông và dịch vụ số.

Mục tiêu của đề án là làm rõ cơ sở lý luận và pháp lý về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng; phân tích thực trạng quy định pháp luật Việt Nam và thực tiễn áp dụng; từ đó đề xuất các giải pháp hoàn thiện pháp luật và nâng cao hiệu quả thực hiện trách nhiệm của doanh nghiệp. Đề án tập trung nghiên cứu trong phạm vi pháp luật Việt Nam, chủ yếu dưới góc độ trách nhiệm dân sự và trách nhiệm hành chính; trách nhiệm hình sự được đề cập ở mức độ liên quan. Về thời gian, đề án tập trung vào giai đoạn 2023–2025, gắn với sự phát triển của Nghị định số 13/2023/NĐ-CP, Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định 356/2025/NĐ-CP.

Về nội dung, đề án gồm ba chương. Chương 1 hệ thống hóa các vấn đề lý luận và pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, bao gồm khái niệm, đặc điểm, các yếu tố ảnh hưởng, nguyên tắc pháp luật và nội dung trách nhiệm của doanh nghiệp trong từng giai đoạn xử lý dữ liệu. Chương này cũng tham khảo kinh nghiệm pháp luật của Liên minh châu Âu, Hoa Kỳ và Singapore để rút ra bài học cho Việt Nam.

Chương 2 phân tích thực trạng pháp luật và thực tiễn thực hiện trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng. Nội dung tập trung

vào trách nhiệm của doanh nghiệp khi thu thập dữ liệu, xử lý – lưu trữ – bảo mật dữ liệu, chia sẻ hoặc chuyển giao dữ liệu cho bên thứ ba, cũng như trách nhiệm khi xảy ra vi phạm và chế tài áp dụng. Thông qua một số vụ việc điển hình như rò rỉ dữ liệu cá nhân, thu thập – mua bán dữ liệu trái phép và chia sẻ dữ liệu sai quy định, đề án chỉ ra rằng pháp luật Việt Nam đã bước đầu hình thành khung pháp lý quan trọng nhưng vẫn còn nhiều hạn chế: quy định còn mang tính nguyên tắc, thiếu tiêu chuẩn kỹ thuật cụ thể, cơ chế giám sát chưa mạnh, chế tài chưa thật sự đủ sức răn đe và trách nhiệm giải trình của doanh nghiệp chưa được cụ thể hóa đầy đủ.

Chương 3 đề xuất định hướng và giải pháp hoàn thiện pháp luật theo hướng xây dựng cơ chế quản trị dữ liệu chủ động, lấy doanh nghiệp làm trung tâm của trách nhiệm tuân thủ. Các giải pháp chính gồm: bổ sung quy định cụ thể về trách nhiệm giải trình của doanh nghiệp; hoàn thiện cơ chế giám sát và thực thi pháp luật; quy định rõ các yêu cầu về tổ chức thực hiện, kỹ thuật bảo mật, quản trị dữ liệu và hệ thống an toàn thông tin; đồng thời bảo đảm tốt hơn quyền của người tiêu dùng đối với dữ liệu cá nhân. Bên cạnh đó, đề án đề xuất doanh nghiệp cần xây dựng chương trình tuân thủ nội bộ, thực hiện đánh giá tác động xử lý dữ liệu, chỉ định nhân sự phụ trách bảo vệ dữ liệu, áp dụng công nghệ tăng cường quyền riêng tư và nâng cao văn hóa tuân thủ. Đối với cơ quan quản lý nhà nước, cần tăng cường hướng dẫn, thanh tra, kiểm tra chuyên đề, tuyên truyền pháp luật và phối hợp liên ngành trong quản lý dữ liệu cá nhân.

Tóm lại, đề án khẳng định rằng hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là yêu cầu cấp thiết trong bối cảnh kinh tế số. Việc hoàn thiện này không chỉ góp phần bảo vệ quyền riêng tư và quyền lợi hợp pháp của khách hàng, mà còn nâng cao trách nhiệm xã hội của doanh nghiệp, củng cố niềm tin của người tiêu dùng và thúc đẩy môi trường kinh doanh minh bạch, an toàn, bền vững tại Việt Nam.

TÓM TẮT TIẾNG ANH

The project “Improving the Law on Corporate Responsibility in Protecting Customers’ Personal Data” examines the legal responsibilities of enterprises in the process of collecting, processing, storing, using, sharing, and protecting customers’ personal data in business activities. In the context of digital transformation and the development of the digital economy, personal data has become an increasingly valuable resource, enabling businesses to improve management efficiency, enhance service quality, and strengthen their competitive advantage. However, the exploitation of personal data also gives rise to numerous risks of infringing upon customers’ privacy, personal rights, and the right to personal data protection, especially amid the growing occurrence of data leakage, illegal trading, and unauthorised use of personal data in areas such as e-commerce, finance and banking, telecommunications, and digital services.

The objective of the project is to clarify the theoretical and legal foundations of corporate responsibility in protecting customers’ personal data; analyse the current state of Vietnamese legal regulations and their practical application; and propose solutions to improve the law and enhance the effectiveness of corporate compliance. The project focuses on Vietnamese law, mainly from the perspectives of civil and administrative liability, while criminal liability is discussed where relevant. In terms of time scope, the project focuses on the period from 2023 to 2025, associated with the development of Decree No. 13/2023/ND-CP, the 2024 Data Law, the 2025 Personal Data Protection Law, and Decree No. 356/2025/ND-CP.

In terms of structure, the project consists of three chapters. Chapter 1 systematises theoretical and legal issues concerning corporate responsibility in protecting customers’ personal data, including concepts, characteristics, influencing factors, legal principles, and corporate obligations at each stage of data processing. This chapter also examines legal experiences from the European Union, the United States, and Singapore in order to draw lessons for Vietnam.

Chapter 2 analyses the current legal framework and practical implementation of corporate responsibility in protecting customers' personal data. It focuses on corporate obligations in data collection, processing, storage, security, sharing or transfer to third parties, as well as liability and sanctions in cases of violation. Through typical cases such as personal data leakage, illegal data collection and trading, and unlawful data sharing, the project shows that Vietnam has initially established an important legal framework. However, several limitations remain, including regulations that are still general in nature, a lack of specific technical standards, weak supervision mechanisms, insufficient deterrent sanctions, and an underdeveloped corporate accountability mechanism.

Chapter 3 proposes directions and solutions for improving the law by building a proactive data governance mechanism, with enterprises placed at the centre of compliance responsibility. Key solutions include supplementing specific regulations on corporate accountability, improving supervision and law enforcement mechanisms, clarifying requirements on organisational implementation, technical security, data governance, and information security systems, while better ensuring consumers' rights over their personal data. In addition, the project proposes that enterprises should establish internal compliance programs, conduct data processing impact assessments, appoint personnel in charge of data protection, apply privacy-enhancing technologies, and promote a culture of compliance. For state management agencies, it is necessary to strengthen guidance, inspections, specialised audits, legal awareness campaigns, and inter-agency coordination in personal data management.

In conclusion, the project affirms that improving the law on corporate responsibility in protecting customers' personal data is an urgent requirement in the digital economy. Such improvement not only contributes to protecting customers' privacy and legitimate rights but also enhances corporate social responsibility, strengthens consumer trust, and promotes a transparent, safe, and sustainable digital business environment in Vietnam.

MỤC LỤC

PHẦN MỞ ĐẦU 12

1. Tính cấp thiết của đề tài 12

2. Tình hình nghiên cứu của đề tài 13

3. Đối tượng, phạm vi nghiên cứu 17

3.1. Đối tượng nghiên cứu 17

3.2. Phạm vi nghiên cứu 17

3.2. Phạm vi nghiên cứu 17

4. Mục tiêu, nhiệm vụ nghiên cứu 19

4.1. Mục tiêu tổng quát 19

4.2. Nhiệm vụ nghiên cứu 19

4.3. Câu hỏi nghiên cứu và giả thuyết nghiên cứu 19

5. Phương pháp nghiên cứu 20

6. Ý nghĩa khoa học của nghiên cứu 22

7. Kết cấu của đề án 23

CHƯƠNG 1. MỘT SỐ VẤN ĐỀ LÝ LUẬN VÀ PHÁP LUẬT VỀ TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA KHÁCH HÀNG 23

1.1. Một số vấn đề lý luận về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 24

1.1.1. Một số khái niệm nền tảng về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 24

1.1.2. Đặc điểm về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 28

1.1.3. Các yếu tố ảnh hưởng đến trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 31

1.2. Một số vấn đề lý luận pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 34
1.2.1. Khái niệm pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 34
1.2.2. Nguyên tắc pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 35
1.2.3. Nội dung pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 38
1.3. Pháp luật một số quốc gia về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng và kinh nghiệm cho Việt Nam 40
1.3.1. Pháp luật Liên minh châu Âu về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 40
1.3.2. Pháp luật Hoa Kỳ về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 42
1.3.3. Pháp luật Singapore về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 43
1.3.4. Kinh nghiệm cho Việt Nam 44
TIỂU KẾT CHƯƠNG 1 46
CHƯƠNG 2. THỰC TRẠNG PHÁP LUẬT VỀ TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA KHÁCH HÀNG VÀ THỰC TIỄN THỰC HIỆN 47
2.1. Thực trạng quy định pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 47
2.1.1. Trách nhiệm khi thu thập dữ liệu 47
2.1.2. Trách nhiệm khi xử lý, lưu trữ và bảo mật 48
2.1.3. Trách nhiệm khi chia sẻ/chuyển giao cho bên thứ ba 50
2.1.4. Trách nhiệm khi xảy ra vi phạm và chế tài 51
2.2. Thực tiễn thực hiện pháp luật thông qua một số vụ việc điển hình 52
2.2.1. Vi phạm nghĩa vụ bảo mật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 52

2.2.2. Thu thập, sử dụng trái phép về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 59
2.2.3. Chia sẻ/chuyển giao trái quy định về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 65
2.3. Đánh giá thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 72
2.3.1. Kết quả đạt được trong thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 72
2.3.2. Hạn chế, bất cập trong thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 75
2.3.3. Nguyên nhân và vấn đề đặt ra 77
TIỂU KẾT CHƯƠNG 2 79
3.1. Định hướng hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 80
3.2. Kiến nghị hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 82
3.2.1. Hoàn thiện, pháp luật cần bổ sung các quy định cụ thể về trách nhiệm giải trình của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 83
3.2.2. Hoàn thiện cơ chế giám sát và thực thi pháp luật về bảo vệ dữ liệu cá nhân của khách hàng 84
3.2.3. Hoàn thiện quy định về tổ chức thực hiện và kỹ thuật của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 85
Về mặt kỹ thuật, cần bổ sung các quy định yêu cầu doanh nghiệp áp dụng các biện pháp bảo mật tối thiểu đối với dữ liệu cá nhân. Cụ thể, có thể quy định tại cấp luật nguyên tắc bắt buộc về: 86
3.2.4. Hoàn thiện quy định về quản trị dữ liệu và hệ thống bảo mật thông tin của nhiều doanh nghiệp 86
3.2.5. Hoàn thiện quy định về nghĩa vụ của doanh nghiệp và quyền bảo vệ dữ liệu cá nhân của người tiêu dùng 87

3.3. Kiến nghị nâng cao hiệu quả thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng 88
3.3.1. Giải pháp từ phía doanh nghiệp 88
3.3.2. Giải pháp từ phía cơ quan quản lý nhà nước 90
TIỂU KẾT CHƯƠNG 3 93
KẾT LUẬN 94
TÀI LIỆU THAM KHẢO 96

PHẦN MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong bối cảnh chuyển đổi số và phát triển không ngừng của nền kinh tế số, dữ liệu cá nhân ngày càng trở thành một nguồn tài nguyên quan trọng trong hoạt động kinh doanh của doanh nghiệp. Thông qua việc thu thập, xử lý và khai thác dữ liệu cá nhân của khách hàng, doanh nghiệp có thể nâng cao hiệu quả quản lý, phát triển sản phẩm, cung cấp dịch vụ và gia tăng lợi thế cạnh tranh trên thị trường. Tuy nhiên, cùng với những lợi ích kinh tế mang lại, việc sử dụng dữ liệu cá nhân cũng tiềm ẩn nhiều nguy cơ xâm phạm quyền và lợi ích hợp pháp của khách hàng, đặc biệt là quyền riêng tư và quyền được bảo vệ dữ liệu cá nhân. Thực tiễn cho thấy, tình trạng rò rỉ, mua bán, sử dụng trái phép dữ liệu cá nhân của khách hàng diễn ra ngày càng phổ biến trong nhiều lĩnh vực kinh doanh như thương mại điện tử, lĩnh vực tài chính - ngân hàng, ngành viễn thông và dịch vụ số. Nhiều hành vi vi phạm xuất phát từ chính doanh nghiệp hoặc từ bên thứ ba có liên quan đến quá trình xử lý dữ liệu, gây ra những hậu quả nghiêm trọng đối với khách hàng và làm suy giảm niềm tin của xã hội đối với môi trường kinh doanh. Vấn đề này đã đặt ra yêu cầu cấp thiết phải xác định rõ trách nhiệm pháp lý của doanh nghiệp trong việc bảo vệ dữ liệu cá nhân của khách hàng. Các quy định liên quan đến trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân còn phân tán, thiếu tính đồng bộ và chưa làm rõ ranh giới trách nhiệm pháp lý của doanh nghiệp trong từng giai đoạn xử lý dữ liệu, từ thu thập, lưu trữ đến sử dụng và chia sẻ dữ liệu cá nhân của khách hàng. Thực tiễn áp dụng pháp luật cũng cho thấy còn nhiều khó khăn trong việc xác định trách nhiệm và áp dụng chế tài đối với doanh nghiệp khi xảy ra vi phạm.

Bên cạnh đó, trong khoa học pháp lý, vấn đề bảo vệ dữ liệu cá nhân của khách hàng hiện tại chủ yếu được nghiên cứu dưới góc độ quyền riêng tư hoặc bảo vệ thông tin cá nhân nói chung, trong khi các nghiên cứu chuyên về trách nhiệm pháp lý của doanh nghiệp trong hoạt động kinh doanh vẫn còn một số hạn chế. Do đó, việc nghiên cứu một cách có hệ thống về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng không chỉ có ý nghĩa về mặt lý luận mà còn có giá trị thực tiễn cao.

Xuất phát từ những lý do nêu trên, việc lựa chọn đề tài **"Hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng"** là cần thiết, có ý nghĩa khoa học và mang tính thời sự, góp phần làm rõ cơ sở lý luận, đánh giá thực trạng pháp luật và đề xuất các giải pháp nhằm hoàn thiện khung pháp lý, nâng cao hiệu quả bảo vệ dữ liệu cá nhân trong bối cảnh phát triển nền kinh tế số tại Việt Nam hiện nay.

2. Tình hình nghiên cứu của đề tài

Trong bối cảnh chuyển đổi số và sự phát triển mạnh mẽ của nền kinh tế số, vấn đề bảo vệ dữ liệu cá nhân ngày càng thu hút sự quan tâm của giới nghiên cứu trong và ngoài nước. Nhiều công trình khoa học đã tiếp cận vấn đề này dưới các góc độ khác nhau như quyền con người, an ninh mạng, thương mại điện tử và quản trị doanh nghiệp.

2.1. Về các công trình nước ngoài

Thông qua Báo cáo Data Privacy Benchmark Study 2025, Cisco (2025) cho thấy trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng ngày càng được nhìn nhận như một yếu tố cốt lõi của quản trị doanh nghiệp và xây dựng niềm tin thị trường. Kết quả khảo sát toàn cầu chỉ ra rằng các doanh nghiệp đầu tư nghiêm túc vào việc tuân thủ pháp luật về bảo vệ dữ liệu cá nhân, thông qua xây dựng quy trình nội bộ, kiểm soát truy cập dữ liệu và bảo đảm tính minh bạch đối với khách hàng, không chỉ góp phần giảm thiểu rủi ro pháp lý mà còn nâng cao uy tín và lợi thế cạnh tranh. Nghiên cứu nhấn mạnh vai trò của trách nhiệm chủ động và trách nhiệm giải trình của doanh nghiệp trong toàn bộ quá trình xử lý dữ liệu cá nhân của khách hàng.

Báo cáo của Global Privacy Benchmarks Report 2024 tiếp cận trách nhiệm của doanh nghiệp từ góc độ quản trị tuân thủ nội bộ. Kết quả nghiên cứu cho thấy các doanh nghiệp thực hiện tốt nghĩa vụ bảo vệ dữ liệu cá nhân thường tập trung xây dựng và vận hành các chương trình quản trị dữ liệu cá nhân, bao gồm ban hành chính sách bảo vệ dữ liệu, đào tạo nhân sự, kiểm soát hoạt động xử lý dữ liệu và giám sát việc tuân thủ của các bên thứ ba. Nghiên cứu này khẳng định hiệu quả bảo vệ dữ liệu

cá nhân phụ thuộc lớn vào mức độ chủ động và năng lực quản trị của doanh nghiệp (TrustArc. (2025).

Bổ sung cho hai hướng tiếp cận trên, nghiên cứu của tác giả Zhang et al. (2023) thông qua phân tích thực nghiệm các chính sách quyền riêng tư của doanh nghiệp theo chuẩn GDPR cho thấy, mặc dù nhiều doanh nghiệp đã công bố chính sách bảo vệ dữ liệu cá nhân, nhưng mức độ tuân thủ thực chất đối với các yêu cầu về minh bạch, giới hạn mục đích và trách nhiệm giải trình còn chưa cao. Nghiên cứu nhấn mạnh rằng trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng không chỉ dừng lại ở việc ban hành chính sách, mà còn phải bảo đảm nội dung và việc thực thi chính sách phản ánh đầy đủ các nghĩa vụ pháp lý theo quy định về bảo vệ dữ liệu cá nhân. Tương tự, tác giả Negi (2023) trong nghiên cứu GDPR Literature Review đã tổng hợp hơn 160 nghiên cứu về GDPR, chỉ ra khoảng trống nghiên cứu về thực thi và tuân thủ trong doanh nghiệp.

Tác giả Mondschein & Monda (2019) đã phân tích cơ chế pháp lý và nguyên tắc cốt lõi của GDPR, đặc biệt là việc xử lý dữ liệu trong nghiên cứu khoa học và yêu cầu tuân thủ pháp luật. Trong khi, European Data Protection Board (EDPB, 2023) nghiên cứu về việc sử dụng dữ liệu cá nhân cho mục đích thứ cấp và các yêu cầu bảo đảm tuân thủ GDPR trong bối cảnh nghiên cứu và chia sẻ dữ liệu. Hoặc, Amaral và cộng sự (2021) trong nghiên cứu AI-enabled Automation for Privacy Policy Compliance đã ứng dụng trí tuệ nhân tạo để kiểm tra mức độ tuân thủ GDPR của chính sách bảo mật, cho thấy khả năng tự động hóa kiểm soát tuân thủ pháp luật.

2.2. Về các công trình trong nước

- Về sách, giáo trình

Cuốn sách "Quyền riêng tư và bảo vệ dữ liệu cá nhân trong pháp luật Việt Nam" do PGS.TS Nguyễn Thị Quế Anh chủ biên là tài liệu nghiên cứu chuyên sâu về quyền nhân thân và khung pháp lý trong kỷ nguyên số. Tác phẩm tập trung phân tích các khoảng trống pháp lý và thách thức trước sự bùng nổ của công nghệ thông tin.

Cuốn sách "Pháp luật về bảo vệ dữ liệu cá nhân – Kinh nghiệm quốc tế và gợi mở cho Việt Nam" do TS. Nguyễn Văn Cương chủ biên (xuất bản năm 2023) là một

tài liệu nghiên cứu chuyên sâu về khung pháp lý bảo vệ dữ liệu cá nhân (DLCN). Trong bối cảnh Việt Nam đã thông qua Luật Bảo vệ dữ liệu cá nhân năm 2025 (có hiệu lực từ 01/01/2026), các nghiên cứu như của TS. Nguyễn Văn Cương đóng vai trò quan trọng trong việc cung cấp cơ sở khoa học để thực thi luật mới hiệu quả.

Giáo trình Luật Dân sự Việt Nam (Tập 1) của Trường Đại học Luật Hà Nội (2022), quyền nhân thân và đời sống riêng tư được xác lập là nền tảng pháp lý cốt lõi cho việc bảo vệ dữ liệu cá nhân. Giáo trình nhấn mạnh rằng khi xã hội số phát triển, việc bảo vệ dữ liệu cá nhân chính là cách hiện thực hóa quyền nhân thân trong không gian mạng. Mọi hành vi xử lý dữ liệu mà không có sự cho phép hoặc vượt quá phạm vi cho phép đều vi phạm các nguyên tắc cơ bản của Luật Dân sự.

Công trình "Bình luận khoa học Bộ luật Dân sự năm 2015" (Viện Khoa học pháp lý – Bộ Tư pháp) đã phân tích chi tiết các quy định về quyền nhân thân, trong đó có quyền về đời sống riêng tư và bí mật cá nhân – là cơ sở pháp lý quan trọng cho việc bảo vệ dữ liệu cá nhân trong thực tiễn.

- Về luận văn, luận án

Tác giả Nguyễn Đăng Khoa (2024) với luận văn Bảo vệ dữ liệu cá nhân trong hoạt động thương mại điện tử theo pháp luật Việt Nam tại Trường Đại học Ngân hàng TP. Hồ Chí Minh. Công trình tập trung phân tích việc thu thập, xử lý và sử dụng dữ liệu cá nhân trong môi trường thương mại điện tử, qua đó chỉ ra những rủi ro pháp lý trong hoạt động kinh doanh. Tuy nhiên, nghiên cứu chủ yếu giới hạn trong lĩnh vực thương mại điện tử, chưa làm rõ trách nhiệm pháp lý tổng thể của doanh nghiệp trong các lĩnh vực khác.

Luận văn của Nguyễn Thị Thu Hương (2022) về Pháp luật về bảo vệ thông tin cá nhân của người tiêu dùng tại Việt Nam, Trường Đại học Luật Hà Nội. Luận văn làm rõ các quy định pháp luật liên quan đến bảo vệ thông tin cá nhân của người tiêu dùng và nghĩa vụ của tổ chức, cá nhân kinh doanh. Tuy nhiên, nghiên cứu tiếp cận chủ yếu dưới góc độ quyền người tiêu dùng, chưa phân tích sâu trách nhiệm giải trình và quản trị dữ liệu của doanh nghiệp.

Luận án của tác giả Lê Thị Hồng Nhung (2023) về Bảo vệ dữ liệu cá nhân theo pháp luật Việt Nam trong bối cảnh chuyển đổi số, Đại học Quốc gia Hà Nội. Luận án

tiếp cận toàn diện vấn đề bảo vệ dữ liệu cá nhân, có phân tích pháp luật và đề xuất định hướng hoàn thiện trong bối cảnh chuyển đổi số. Tuy nhiên, nội dung chưa tập trung chuyên sâu vào trách nhiệm pháp lý của doanh nghiệp trong mối quan hệ với khách hàng.

- Về tạp chí

Tác giả Phạm Việt Tuấn (2022) đã tổng hợp, phân tích và trình bày các quy định về bảo vệ dữ liệu cá nhân trong pháp luật Việt Nam dựa trên cách tiếp cận đối với quyền của chủ thể dữ liệu và hệ thống lại các quy định, đồng thời, đưa ra một số kiến nghị, đề xuất với hy vọng góp phần hoàn thiện các quy định về bảo vệ dữ liệu cá nhân trong pháp luật Việt Nam. Cùng hướng nghiên cứu, tác giả Phạm Thị Hiền và Nguyễn Thu Dung (2021) đã nghiên cứu về pháp luật về bảo vệ dữ liệu cá nhân trong nền kinh tế số ở Việt Nam hiện nay, tác giả đã nêu khái quát những quy định của pháp luật Việt Nam hiện hành về bảo vệ dữ liệu cá nhân. Qua đó, tác giả làm rõ một số vấn đề pháp lý còn tồn tại trong thực tiễn bảo vệ dữ liệu cá nhân gắn với phát triển kinh tế số và đưa ra những giải pháp khuyến nghị.

Tác giả Nguyễn Thị Long (2022) tập trung phân tích thực trạng quy định pháp luật Việt Nam hiện hành về bảo vệ dữ liệu cá nhân, cụ thể: Đánh giá những quy định chung về dữ liệu cá nhân; quy định về quyền và nghĩa vụ của các chủ thể liên quan đến dữ liệu cá nhân; các phương thức bảo vệ dữ liệu cá nhân theo quy định pháp luật Việt Nam hiện hành.

Tác giả Vũ Công Giao và Lê Trần Như Tuyên (2020) phân tích sự tác động của kỹ thuật số đến quyền đối với dữ liệu cá nhân; đánh giá các quy định của pháp luật quốc tế và pháp luật ở một số quốc gia về việc bảo vệ quyền này trong bối cảnh mới và nêu ra một số giá trị mà Việt Nam có thể tham khảo. Tương tự, nghiên cứu của tác giả Trần Thị Thu Phương (2021) về quy định chung của Liên minh châu Âu về bảo vệ dữ liệu cá nhân và một số khuyến nghị cho Việt Nam đã làm rõ các nguyên tắc bảo vệ dữ liệu và đề xuất hướng hoàn thiện pháp luật trong nước, nghiên cứu tập trung vào so sánh pháp luật Việt Nam với chuẩn mực quốc tế, đặc biệt là GDPR của Liên minh châu Âu. Tác giả Trần Thị Thanh Bích và Đào Thị Anh Thư (2025) đã đưa ra một số giải pháp hoàn thiện khung pháp lý nhằm cân bằng giữa bảo vệ dữ liệu

cá nhân và thúc đẩy đổi mới sáng tạo là yêu cầu cấp thiết hiện nay, không chỉ giúp tăng cường bảo vệ quyền riêng tư mà còn tạo điều kiện thuận lợi để Việt Nam hội nhập sâu rộng vào nền kinh tế số toàn cầu.

Cụ thể hơn, tác giả Lê Thị Thuỳ Trang (2017), nghiên cứu một số quy định về bảo vệ thông tin cá nhân trên thế giới và tại Việt Nam, trong khi, tác giả Chu Thị Hoa (2021) cho rằng cần coi dữ liệu cá nhân là một loại tài sản phi truyền thống và đề xuất hai nhóm nguyên tắc lập quy nhằm cân bằng lợi ích giữa các chủ thể, đồng thời đề xuất sửa đổi, bổ sung các quy định pháp luật hiện hành theo hướng thống nhất ghi nhận quyền nhân thân đối với thông tin cá nhân, tách bạch cơ chế điều chỉnh giữa quan hệ xử lý dữ liệu cá nhân với dữ liệu công nghiệp, trung hòa xung đột thông qua cơ chế quy chuẩn, kiểm định, đánh giá tín nhiệm số đối với các chủ thể xử lý dữ liệu.

Nhìn chung, các công trình nghiên cứu chủ yếu tiếp cận vấn đề dữ liệu cá nhân dưới góc độ quyền cá nhân hoặc bảo vệ người tiêu dùng nói chung, chưa có nhiều nghiên cứu chuyên sâu tập trung trực tiếp vào trách nhiệm pháp lý của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng trong hoạt động kinh doanh, đặc biệt là các nghiên cứu gắn với phân tích tình huống và thực tiễn áp dụng pháp luật. Đây chính là khoảng trống nghiên cứu mà Đề án hướng tới làm rõ và bổ sung.

3. Đối tượng, phạm vi nghiên cứu

3.1. Đối tượng nghiên cứu

Đối tượng nghiên cứu là các quy định pháp luật và thực tiễn áp dụng pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng trong hoạt động kinh doanh, bao gồm các nghĩa vụ pháp lý của doanh nghiệp và các hình thức trách nhiệm pháp lý phát sinh khi có hành vi vi phạm.

3.2. Phạm vi nghiên cứu

3.2. Phạm vi nghiên cứu

Về nội dung, Đề án tập trung nghiên cứu trách nhiệm pháp lý của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng trong hoạt động kinh doanh. Trọng tâm nghiên cứu không phải là toàn bộ vấn đề bảo vệ dữ liệu cá nhân nói chung, mà là việc xác định nghĩa vụ pháp lý của doanh nghiệp và các hình thức trách nhiệm pháp lý

phát sinh khi doanh nghiệp không thực hiện, thực hiện không đúng hoặc thực hiện không đầy đủ nghĩa vụ bảo vệ dữ liệu cá nhân của khách hàng.

Trong phạm vi này, Đề án tập trung làm rõ trách nhiệm của doanh nghiệp trong các giai đoạn chủ yếu của quá trình xử lý dữ liệu cá nhân, bao gồm: thu thập dữ liệu; xử lý, lưu trữ và bảo mật dữ liệu; chia sẻ, chuyển giao dữ liệu cho bên thứ ba; xử lý sự cố và khắc phục hậu quả khi xảy ra hành vi xâm phạm dữ liệu cá nhân của khách hàng. Các hình thức trách nhiệm pháp lý được nghiên cứu chủ yếu là trách nhiệm dân sự và trách nhiệm hành chính. Trách nhiệm hình sự chỉ được đề cập ở mức độ liên quan nhằm làm rõ tính đầy đủ của cơ chế xử lý vi phạm, không phải là trọng tâm nghiên cứu chính của Đề án.

Về chủ thể, Đề án tập trung nghiên cứu doanh nghiệp với tư cách là chủ thể thu thập, xử lý, lưu trữ, sử dụng hoặc chia sẻ dữ liệu cá nhân của khách hàng trong hoạt động kinh doanh. Đề án không đi sâu nghiên cứu trách nhiệm của cơ quan nhà nước, tổ chức chính trị - xã hội, cá nhân riêng lẻ hoặc các chủ thể xử lý dữ liệu không nhằm mục đích kinh doanh, trừ trường hợp các chủ thể này có liên quan đến việc phân tích cơ chế pháp lý chung.

Về không gian, Đề án tập trung nghiên cứu trong phạm vi pháp luật Việt Nam và thực tiễn áp dụng tại Việt Nam. Pháp luật của Liên minh châu Âu, Hoa Kỳ và Singapore chỉ được đề cập ở mức độ tham khảo, nhằm rút ra một số kinh nghiệm có giá trị cho quá trình hoàn thiện pháp luật Việt Nam, không phải là đối tượng nghiên cứu độc lập hoặc so sánh toàn diện.

Về thời gian, Đề án tập trung nghiên cứu các quy định pháp luật và thực tiễn áp dụng trong giai đoạn 2023–2025. Đây là giai đoạn pháp luật Việt Nam về bảo vệ dữ liệu cá nhân có nhiều chuyển biến quan trọng, gắn với Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định số 356/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân. Việc lựa chọn giai đoạn này nhằm phản ánh sự chuyển biến của khung pháp lý và thực tiễn áp dụng pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng tại Việt Nam.

Ngoài ra, Đề án không đi sâu nghiên cứu các khía cạnh kỹ thuật chuyên ngành về an toàn thông tin, an ninh mạng hoặc công nghệ bảo mật dữ liệu, mà chỉ đề cập các vấn đề này ở mức độ cần thiết nhằm làm rõ nghĩa vụ và trách nhiệm pháp lý của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

4. Mục tiêu, nhiệm vụ nghiên cứu

4.1. Mục tiêu tổng quát

Đề án được thực hiện nhằm làm rõ cơ sở lý luận và cơ sở pháp lý về trách nhiệm của doanh nghiệp trong việc bảo vệ dữ liệu cá nhân của khách hàng trong hoạt động kinh doanh; qua đó, phân tích và đánh giá một cách toàn diện các quy định pháp luật hiện hành cũng như thực tiễn áp dụng pháp luật ở Việt Nam và đề xuất các giải pháp và kiến nghị có cơ sở khoa học nhằm hoàn thiện pháp luật và nâng cao hiệu quả thực hiện trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng trong bối cảnh phát triển kinh tế số hiện nay.

4.2. Nhiệm vụ nghiên cứu

Để đạt được mục tiêu, Đề án tập trung vào các mục tiêu cụ thể sau:

Thứ nhất, làm rõ các vấn đề lý luận cơ bản về dữ liệu cá nhân, bảo vệ dữ liệu cá nhân và trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

Thứ hai, phân tích và đánh giá các quy định pháp luật hiện hành của Việt Nam về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

Thứ ba, đánh giá thực tiễn áp dụng pháp luật thông qua hoạt động của doanh nghiệp và một số vụ việc điển hình.

Cuối cùng, đề xuất các giải pháp nhằm hoàn thiện pháp luật và nâng cao hiệu quả thực hiện trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

4.3. Câu hỏi nghiên cứu và giả thuyết nghiên cứu

Trên cơ sở mục tiêu và nhiệm vụ nghiên cứu đã xác định, Đề án tập trung trả lời các câu hỏi nghiên cứu sau:

Thứ nhất, trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng được hiểu như thế nào và cần phân biệt ra sao với nghĩa vụ của doanh nghiệp trong quá trình thu thập, xử lý, lưu trữ, sử dụng, chia sẻ và bảo vệ dữ liệu cá nhân?

Thứ hai, pháp luật Việt Nam hiện hành quy định như thế nào về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, đặc biệt là trách nhiệm dân sự, trách nhiệm hành chính và trách nhiệm pháp lý phát sinh khi xảy ra hành vi vi phạm?

Thứ ba, thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng hiện nay còn tồn tại những hạn chế, bất cập nào, nhất là trong việc xác định căn cứ phát sinh trách nhiệm, hình thức trách nhiệm, cơ chế xử lý vi phạm và biện pháp khắc phục hậu quả?

Thứ tư, cần hoàn thiện pháp luật theo định hướng nào để nâng cao hiệu quả thực hiện trách nhiệm của doanh nghiệp, bảo vệ tốt hơn quyền và lợi ích hợp pháp của khách hàng trong bối cảnh chuyển đổi số và phát triển kinh tế số?

Từ các câu hỏi nghiên cứu trên, Đề án đặt ra giả thuyết nghiên cứu như sau: mặc dù pháp luật Việt Nam đã từng bước hình thành khung pháp lý về bảo vệ dữ liệu cá nhân, đặc biệt thông qua Nghị định số 13/2023/NĐ-CP, Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định số 356/2025/NĐ-CP, nhưng các quy định về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng vẫn cần tiếp tục được hoàn thiện. Những hạn chế chủ yếu thể hiện ở việc pháp luật còn thiên về quy định nghĩa vụ tuân thủ, trong khi cơ chế xác định trách nhiệm pháp lý, trách nhiệm giải trình, trách nhiệm kiểm soát bên thứ ba, trách nhiệm khắc phục hậu quả và trách nhiệm bồi thường thiệt hại chưa được cụ thể hóa đầy đủ.

Do đó, Đề án cho rằng việc hoàn thiện pháp luật cần chuyển từ cách tiếp cận chỉ nhấn mạnh nghĩa vụ của doanh nghiệp sang cách tiếp cận đầy đủ hơn về trách nhiệm pháp lý của doanh nghiệp. Theo đó, doanh nghiệp không chỉ phải tuân thủ các yêu cầu về bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu, mà còn phải chịu hậu quả pháp lý rõ ràng khi vi phạm, bao gồm trách nhiệm dân sự, trách nhiệm hành chính, biện pháp khắc phục hậu quả và trong trường hợp nghiêm trọng có thể phát sinh trách nhiệm hình sự đối với chủ thể có liên quan.

5. Phương pháp nghiên cứu

Đề án được thực hiện trên cơ sở phương pháp luận của chủ nghĩa duy vật biện chứng và duy vật lịch sử, bảo đảm việc nhận thức và phân tích các vấn đề pháp lý

trong mối liên hệ với bối cảnh kinh tế - xã hội và sự phát triển của hoạt động kinh doanh. Trên nền tảng đó, Đề án sử dụng tổng hợp các phương pháp nghiên cứu khoa học pháp lý nhằm làm rõ nội dung và đạt được mục tiêu nghiên cứu đã đặt ra.

Trong đó, phương pháp phân tích và tổng hợp được sử dụng xuyên suốt để nghiên cứu, hệ thống hóa và làm rõ các quy định pháp luật hiện hành về bảo vệ dữ liệu cá nhân và trách nhiệm của doanh nghiệp, đồng thời đánh giá mức độ đầy đủ, thống nhất và khả thi của các quy định này.

Phương pháp so sánh pháp luật được sử dụng nhằm đối chiếu pháp luật Việt Nam với pháp luật của một số quốc gia và khu vực, qua đó rút ra những giá trị tham khảo phục vụ cho việc hoàn thiện pháp luật trong nước.

Đặc biệt, Đề án nhấn mạnh việc sử dụng phương pháp nghiên cứu tình huống (case study) như một công cụ quan trọng để đánh giá thực tiễn áp dụng pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng. Thông qua việc phân tích một số vụ việc điển hình liên quan đến hành vi vi phạm bảo vệ dữ liệu cá nhân trong hoạt động kinh doanh, Đề án làm rõ cách thức các quy định pháp luật được áp dụng trên thực tế, những khó khăn, vướng mắc trong việc xác định trách nhiệm pháp lý của doanh nghiệp, cũng như những khoảng trống và bất cập của pháp luật hiện hành. Trên cơ sở đó, các nghiên cứu tình huống không chỉ đóng vai trò minh họa mà còn là căn cứ thực tiễn quan trọng để Đề án đánh giá hiệu quả điều chỉnh của pháp luật và đề xuất các giải pháp hoàn thiện pháp luật một cách phù hợp và khả thi.

Bên cạnh đó, phương pháp lịch sử – logic cũng được sử dụng nhằm làm rõ quá trình hình thành và phát triển của các quy định pháp luật về bảo vệ dữ liệu cá nhân, qua đó góp phần lý giải xu hướng hoàn thiện pháp luật trong bối cảnh chuyển đổi số và hội nhập quốc tế.

Đề án còn sử dụng phương pháp hệ thống hóa pháp luật nhằm sắp xếp, phân loại và làm rõ mối quan hệ giữa các quy định pháp luật có liên quan, đặc biệt là các quy định về bảo vệ dữ liệu cá nhân và trách nhiệm của doanh nghiệp đang được quy định rải rác trong nhiều văn bản khác nhau. Trên cơ sở đó, Đề án góp phần nhận diện mức độ thống nhất, đồng bộ cũng như những điểm chồng chéo, mâu thuẫn (nếu có) trong hệ thống pháp luật hiện hành.

Phương pháp phân tích quy phạm pháp luật được sử dụng để đi sâu làm rõ nội dung, phạm vi điều chỉnh, đối tượng áp dụng cũng như điều kiện phát sinh trách nhiệm pháp lý của doanh nghiệp theo từng quy định cụ thể. Thông qua đó, Đề án đánh giá tính rõ ràng, minh bạch và khả năng áp dụng trên thực tế của các quy phạm pháp luật, đồng thời chỉ ra những hạn chế, bất cập trong cách thiết kế quy định pháp luật hiện hành.

Đồng thời, Đề án kết hợp phương pháp tổng kết thực tiễn thông qua việc thu thập, chọn lọc và phân tích các tài liệu, báo cáo, vụ việc điển hình và thông tin từ thực tiễn áp dụng pháp luật liên quan đến bảo vệ dữ liệu cá nhân. Việc vận dụng phương pháp này nhằm làm rõ cách thức pháp luật được thực thi trong thực tế, những khó khăn, vướng mắc phát sinh trong quá trình áp dụng, cũng như khoảng cách giữa quy định pháp luật và thực tiễn triển khai. Trên cơ sở đó, Đề án có cơ sở thực tiễn để đề xuất các kiến nghị hoàn thiện pháp luật phù hợp và khả thi hơn.

6. Ý nghĩa khoa học của nghiên cứu

Dưới góc độ nghiên cứu, Đề án góp phần hệ thống hóa và làm rõ cơ sở lý luận và pháp lý về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, qua đó bổ sung, làm phong phú thêm các nghiên cứu pháp lý về bảo vệ dữ liệu cá nhân trong bối cảnh phát triển kinh tế số. Việc tiếp cận vấn đề thông qua phương pháp nghiên cứu tình huống cho phép Đề án gắn kết chặt chẽ giữa lý luận và thực tiễn, làm rõ cách thức pháp luật được áp dụng trong các tình huống cụ thể và đánh giá hiệu quả điều chỉnh của pháp luật hiện hành.

Dưới góc độ thực tiễn, kết quả nghiên cứu của Đề án có thể được sử dụng làm tài liệu tham khảo cho các cơ quan nhà nước có thẩm quyền trong quá trình xây dựng và hoàn thiện chính sách, pháp luật về bảo vệ dữ liệu cá nhân; đồng thời cung cấp cơ sở khoa học giúp doanh nghiệp nâng cao nhận thức và thực hiện tốt hơn trách nhiệm pháp lý của mình trong việc bảo vệ dữ liệu cá nhân của khách hàng trong hoạt động kinh doanh.

Bên cạnh đó, nghiên cứu cũng có những giới hạn nhất định. Do phạm vi nghiên cứu tập trung chủ yếu vào trách nhiệm pháp lý của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng theo pháp luật Việt Nam, nên Đề án chưa có điều kiện đi sâu

phân tích toàn diện các mô hình điều chỉnh pháp luật của nhiều quốc gia khác. Việc nghiên cứu tình huống trong Đề án chủ yếu dựa trên các vụ việc điển hình đã được công bố, vì vậy chưa phản ánh đầy đủ mọi dạng vi phạm và mọi khía cạnh của thực tiễn áp dụng pháp luật về bảo vệ dữ liệu cá nhân trong hoạt động kinh doanh.

7. Kết cấu của đề án

Ngoài phần Mở đầu, Kết luận và Danh mục tài liệu tham khảo, Đề án gồm 03 chương:

Chương 1: Một số vấn đề lý luận và pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

Chương 2: Thực trạng pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng và thực tiễn áp dụng

Chương 3: Giải pháp hoàn thiện pháp luật và nâng cao hiệu quả thực hiện trách nhiệm của doanh nghiệp.

CHƯƠNG 1. MỘT SỐ VẤN ĐỀ LÝ LUẬN VÀ PHÁP LUẬT VỀ TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA KHÁCH HÀNG

1.1. Một số vấn đề lý luận về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

1.1.1. Một số khái niệm nền tảng về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Trong bối cảnh chuyển đổi số và phát triển kinh tế số, dữ liệu cá nhân của khách hàng ngày càng trở thành đối tượng được doanh nghiệp thu thập, xử lý, lưu trữ, khai thác và chia sẻ trong quá trình cung cấp hàng hóa, dịch vụ. Vì vậy, để làm rõ trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, trước hết cần xác định một số khái niệm nền tảng, bao gồm dữ liệu cá nhân, bảo vệ dữ liệu cá nhân, trách nhiệm pháp lý của doanh nghiệp và các hình thức trách nhiệm pháp lý có thể phát sinh khi doanh nghiệp vi phạm.

Thứ nhất, về dữ liệu cá nhân.

Dữ liệu cá nhân có thể được hiểu là thông tin gắn liền với một cá nhân cụ thể hoặc có khả năng giúp xác định một cá nhân cụ thể. Dữ liệu cá nhân có thể tồn tại dưới nhiều hình thức khác nhau như chữ viết, chữ số, hình ảnh, âm thanh, ký hiệu hoặc các dạng dữ liệu điện tử khác. Trong quan hệ giữa doanh nghiệp và khách hàng, dữ liệu cá nhân thường bao gồm họ tên, số điện thoại, địa chỉ, thông tin tài khoản, lịch sử giao dịch, thông tin thanh toán, vị trí, hành vi tiêu dùng, thói quen truy cập, dữ liệu sinh trắc học hoặc các thông tin khác có khả năng nhận diện khách hàng.

Dưới góc độ pháp lý, dữ liệu cá nhân không chỉ là một loại thông tin phục vụ hoạt động quản trị và kinh doanh của doanh nghiệp, mà còn gắn liền với quyền nhân thân, quyền riêng tư và quyền được bảo vệ đời sống cá nhân của chủ thể dữ liệu. Do đó, mọi hoạt động thu thập, xử lý và khai thác dữ liệu cá nhân của khách hàng đều phải được đặt trong giới hạn pháp luật, bảo đảm tính hợp pháp, minh bạch, đúng mục đích và an toàn.

Thứ hai, về bảo vệ dữ liệu cá nhân.

Bảo vệ dữ liệu cá nhân là tổng thể các biện pháp pháp lý, kỹ thuật, tổ chức và quản trị nhằm bảo đảm dữ liệu cá nhân không bị thu thập, xử lý, sử dụng, tiết lộ, chia sẻ, chuyển giao, truy cập, sửa đổi, phá hủy hoặc khai thác trái pháp luật. Bảo vệ dữ liệu cá nhân không chỉ là việc bảo mật thông tin bằng các giải pháp kỹ thuật, mà còn bao gồm việc thiết lập quy trình xử lý dữ liệu hợp pháp, bảo đảm quyền của chủ thể dữ liệu, kiểm soát mục đích sử dụng dữ liệu và phòng ngừa rủi ro phát sinh trong suốt vòng đời của dữ liệu.

Đối với doanh nghiệp, bảo vệ dữ liệu cá nhân của khách hàng bao gồm việc xây dựng chính sách bảo vệ dữ liệu, thông báo rõ ràng cho khách hàng về mục đích và phạm vi xử lý dữ liệu, xin sự đồng ý hợp lệ khi pháp luật yêu cầu, áp dụng biện pháp bảo mật phù hợp, kiểm soát việc truy cập nội bộ, quản lý việc chia sẻ dữ liệu cho bên thứ ba, xử lý kịp thời sự cố dữ liệu và khắc phục hậu quả khi xảy ra vi phạm.

Thứ ba, về trách nhiệm pháp lý của doanh nghiệp.

Trách nhiệm pháp lý của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là hậu quả pháp lý bất lợi mà doanh nghiệp phải gánh chịu khi không thực hiện, thực hiện không đúng hoặc thực hiện không đầy đủ các nghĩa vụ pháp luật liên quan đến bảo vệ dữ liệu cá nhân, làm phát sinh nguy cơ hoặc hậu quả xâm phạm quyền và lợi ích hợp pháp của khách hàng.

Khái niệm này cần được phân biệt với nghĩa vụ của doanh nghiệp. Nghĩa vụ là những yêu cầu xử sự bắt buộc mà pháp luật đặt ra cho doanh nghiệp trong quá trình xử lý dữ liệu cá nhân, chẳng hạn như nghĩa vụ thông báo, xin sự đồng ý, bảo mật dữ liệu, xử lý dữ liệu đúng mục đích, bảo đảm quyền của chủ thể dữ liệu và kiểm soát bên thứ ba. Trong khi đó, trách nhiệm pháp lý phát sinh khi doanh nghiệp vi phạm các nghĩa vụ đó. Nói cách khác, nghĩa vụ là yêu cầu phải thực hiện, còn trách nhiệm pháp lý là hậu quả phải gánh chịu khi vi phạm nghĩa vụ.

Trong lĩnh vực bảo vệ dữ liệu cá nhân, trách nhiệm pháp lý của doanh nghiệp có thể bao gồm trách nhiệm dân sự, trách nhiệm hành chính và trong trường hợp nghiêm trọng có thể phát sinh trách nhiệm hình sự đối với cá nhân hoặc pháp nhân thương mại có liên quan.

Thứ tư, về trách nhiệm dân sự của doanh nghiệp.

Trách nhiệm dân sự của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là hậu quả pháp lý phát sinh khi hành vi vi phạm của doanh nghiệp gây thiệt hại đến quyền và lợi ích hợp pháp của khách hàng. Trách nhiệm này thường gắn với việc bồi thường thiệt hại, khôi phục quyền lợi cho khách hàng, xin lỗi, cải chính công khai hoặc thực hiện các biện pháp khác nhằm khắc phục hậu quả do hành vi xâm phạm dữ liệu cá nhân gây ra.

Trong thực tiễn, trách nhiệm dân sự có thể phát sinh khi doanh nghiệp thu thập dữ liệu trái pháp luật, sử dụng dữ liệu sai mục đích, tiết lộ thông tin khách hàng, làm rò rỉ dữ liệu, chuyển giao dữ liệu cho bên thứ ba không đúng quy định hoặc không áp dụng biện pháp bảo mật phù hợp dẫn đến thiệt hại cho khách hàng. Trách nhiệm dân sự có ý nghĩa quan trọng vì trực tiếp hướng đến việc bảo vệ và khôi phục quyền lợi của chủ thể dữ liệu bị xâm phạm.

Thứ năm, về trách nhiệm hành chính của doanh nghiệp.

Trách nhiệm hành chính của doanh nghiệp là hậu quả pháp lý do cơ quan nhà nước có thẩm quyền áp dụng khi doanh nghiệp vi phạm các quy định quản lý nhà nước về bảo vệ dữ liệu cá nhân. Trách nhiệm này thể hiện thông qua các hình thức xử phạt vi phạm hành chính và biện pháp khắc phục hậu quả như phạt tiền, buộc chấm dứt hành vi vi phạm, buộc xóa hoặc hủy dữ liệu thu thập trái pháp luật, buộc cải chính thông tin, buộc thực hiện biện pháp bảo đảm an toàn dữ liệu hoặc các biện pháp khác theo quy định pháp luật.

Khác với trách nhiệm dân sự vốn hướng đến việc bồi thường và khôi phục quyền lợi cho chủ thể bị thiệt hại, trách nhiệm hành chính chủ yếu nhằm bảo đảm trật tự quản lý nhà nước, phòng ngừa vi phạm và răn đe các hành vi xâm phạm dữ liệu cá nhân trong hoạt động kinh doanh.

Thứ sáu, về trách nhiệm hình sự.

Trách nhiệm hình sự là hình thức trách nhiệm pháp lý nghiêm khắc nhất, có thể phát sinh khi hành vi xâm phạm dữ liệu cá nhân có tính chất nguy hiểm cho xã hội, gây hậu quả nghiêm trọng hoặc đủ yếu tố cấu thành tội phạm theo quy định của pháp luật hình sự. Trong lĩnh vực bảo vệ dữ liệu cá nhân, trách nhiệm hình sự có thể được đặt ra đối với cá nhân hoặc pháp nhân thương mại có liên quan nếu có hành vi như

truy cập trái phép, thu thập, mua bán, sử dụng, phát tán hoặc chiếm đoạt dữ liệu cá nhân trái pháp luật với mức độ nghiêm trọng.

Tuy nhiên, trong phạm vi Đề án này, trách nhiệm hình sự chỉ được đề cập ở mức độ liên quan nhằm làm rõ tính đầy đủ của các hình thức trách nhiệm pháp lý. Trọng tâm nghiên cứu của Đề án vẫn là trách nhiệm dân sự và trách nhiệm hành chính của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

Từ các khái niệm trên, có thể hiểu rằng trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là tổng thể các hậu quả pháp lý mà doanh nghiệp phải gánh chịu khi vi phạm nghĩa vụ bảo vệ dữ liệu cá nhân trong quá trình thu thập, xử lý, lưu trữ, sử dụng, chia sẻ, chuyển giao hoặc bảo mật dữ liệu của khách hàng. Trách nhiệm này không chỉ nhằm xử lý hành vi vi phạm, mà còn có chức năng phòng ngừa rủi ro, bảo vệ quyền của khách hàng, nâng cao trách nhiệm giải trình của doanh nghiệp và bảo đảm môi trường kinh doanh an toàn, minh bạch trong nền kinh tế số.

Bên cạnh đó, cần phân biệt rõ "nghĩa vụ" và "trách nhiệm" của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

Nghĩa vụ của doanh nghiệp là những yêu cầu xử sự bắt buộc mà pháp luật đặt ra đối với doanh nghiệp trong quá trình thu thập, xử lý, lưu trữ, sử dụng, chia sẻ, chuyển giao và bảo vệ dữ liệu cá nhân của khách hàng. Các nghĩa vụ này có thể bao gồm nghĩa vụ thông báo cho khách hàng, xin sự đồng ý hợp lệ của chủ thể dữ liệu, xử lý dữ liệu đúng mục đích, bảo mật dữ liệu, bảo đảm quyền của khách hàng, kiểm soát việc chuyển giao dữ liệu cho bên thứ ba và áp dụng các biện pháp kỹ thuật, tổ chức cần thiết để bảo vệ dữ liệu cá nhân.

Trong khi đó, trách nhiệm của doanh nghiệp là hậu quả pháp lý bất lợi phát sinh khi doanh nghiệp không thực hiện, thực hiện không đúng hoặc thực hiện không đầy đủ các nghĩa vụ nói trên, làm phát sinh nguy cơ hoặc hậu quả xâm phạm quyền, lợi ích hợp pháp của khách hàng. Nói cách khác, nghĩa vụ là yêu cầu pháp luật buộc doanh nghiệp phải thực hiện trước và trong quá trình xử lý dữ liệu cá nhân, còn trách nhiệm pháp lý phát sinh khi doanh nghiệp vi phạm các nghĩa vụ đó.

Sự phân biệt này có ý nghĩa quan trọng đối với phạm vi nghiên cứu của Đề án. Đề án không chỉ dừng lại ở việc xác định doanh nghiệp có những nghĩa vụ gì trong

bảo vệ dữ liệu cá nhân của khách hàng, mà tập trung làm rõ khi doanh nghiệp vi phạm các nghĩa vụ đó thì phải chịu những hậu quả pháp lý nào. Các hậu quả này có thể bao gồm trách nhiệm dân sự như bồi thường thiệt hại, xin lỗi, cải chính, khôi phục quyền lợi cho khách hàng; trách nhiệm hành chính như bị xử phạt vi phạm hành chính, buộc chấm dứt hành vi vi phạm, buộc xóa hoặc hủy dữ liệu thu thập trái pháp luật, buộc khắc phục hậu quả; và trong trường hợp nghiêm trọng có thể phát sinh trách nhiệm hình sự đối với cá nhân hoặc pháp nhân thương mại có liên quan theo quy định pháp luật.

Từ đó, có thể hiểu rằng nghĩa vụ là cơ sở pháp lý ban đầu để xác định hành vi đúng hoặc sai của doanh nghiệp, còn trách nhiệm pháp lý là cơ chế xử lý khi doanh nghiệp vi phạm nghĩa vụ. Vì vậy, khi nghiên cứu trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, cần phân tích đồng thời hai phương diện: một là các nghĩa vụ pháp lý mà doanh nghiệp phải tuân thủ; hai là các hình thức trách nhiệm pháp lý phát sinh khi doanh nghiệp không tuân thủ hoặc tuân thủ không đầy đủ các nghĩa vụ đó.

1.1.2. Đặc điểm về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là một dạng trách nhiệm pháp lý đặc thù, phát sinh trong quá trình doanh nghiệp thu thập, xử lý, lưu trữ, sử dụng, chia sẻ, chuyển giao và bảo vệ dữ liệu cá nhân của khách hàng. Trách nhiệm này không chỉ thể hiện ở việc doanh nghiệp phải tuân thủ các nghĩa vụ pháp luật đặt ra, mà còn bao gồm việc doanh nghiệp phải gánh chịu hậu quả pháp lý khi không thực hiện, thực hiện không đúng hoặc thực hiện không đầy đủ các nghĩa vụ đó. Có thể khái quát một số đặc điểm cơ bản sau:

Thứ nhất, trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là trách nhiệm pháp lý gắn với hoạt động kinh doanh. Trong quan hệ giữa doanh nghiệp và khách hàng, doanh nghiệp thường là chủ thể trực tiếp thu thập, quản lý, khai thác hoặc quyết định mục đích và phương thức xử lý dữ liệu cá nhân. Do đó, trách nhiệm của doanh nghiệp không chỉ xuất phát từ quan hệ hợp đồng hoặc quan hệ tiêu dùng, mà còn phát sinh từ yêu cầu bảo vệ quyền riêng tư, quyền nhân thân và

quyền được bảo vệ dữ liệu cá nhân của khách hàng. Điều này làm cho trách nhiệm của doanh nghiệp trong lĩnh vực này mang tính pháp lý rõ rệt, chịu sự điều chỉnh của nhiều nhóm quy phạm pháp luật khác nhau như pháp luật dân sự, pháp luật bảo vệ quyền lợi người tiêu dùng, pháp luật an ninh mạng, pháp luật dữ liệu và pháp luật về bảo vệ dữ liệu cá nhân.

Thứ hai, trách nhiệm của doanh nghiệp phát sinh trong toàn bộ vòng đời xử lý dữ liệu cá nhân. Trách nhiệm của doanh nghiệp không chỉ đặt ra tại thời điểm thu thập dữ liệu cá nhân, mà còn kéo dài trong suốt quá trình xử lý, lưu trữ, sử dụng, chia sẻ, chuyển giao, chỉnh sửa, xóa, hủy dữ liệu và xử lý sự cố liên quan đến dữ liệu cá nhân. Vì vậy, doanh nghiệp không thể chỉ dừng lại ở việc xin sự đồng ý ban đầu của khách hàng, mà còn phải bảo đảm dữ liệu cá nhân được xử lý đúng mục đích, đúng phạm vi, được bảo mật an toàn và được kiểm soát trong suốt quá trình sử dụng. Khi doanh nghiệp để xảy ra rò rỉ, mất mát, truy cập trái phép hoặc sử dụng dữ liệu sai mục đích, trách nhiệm pháp lý có thể phát sinh tùy theo tính chất, mức độ và hậu quả của hành vi vi phạm.

Thứ ba, trách nhiệm của doanh nghiệp bao gồm cả trách nhiệm phòng ngừa và trách nhiệm gánh chịu hậu quả pháp lý khi xảy ra vi phạm. Ở khía cạnh phòng ngừa, doanh nghiệp phải xây dựng chính sách bảo vệ dữ liệu cá nhân, thiết lập quy trình xử lý dữ liệu, áp dụng biện pháp kỹ thuật bảo mật, phân quyền truy cập, đào tạo nhân sự, kiểm soát bên thứ ba và đánh giá rủi ro trong hoạt động xử lý dữ liệu. Tuy nhiên, nếu doanh nghiệp không thực hiện hoặc thực hiện không đầy đủ các yêu cầu này dẫn đến việc dữ liệu cá nhân của khách hàng bị xâm phạm, doanh nghiệp có thể phải chịu các hậu quả pháp lý bất lợi như chấm dứt hành vi vi phạm, xóa hoặc hủy dữ liệu thu thập trái pháp luật, khắc phục hậu quả, bồi thường thiệt hại, bị xử phạt vi phạm hành chính hoặc bị xem xét trách nhiệm pháp lý nghiêm khắc hơn trong trường hợp có đủ căn cứ theo quy định pháp luật.

Thứ tư, trách nhiệm của doanh nghiệp có tính đa dạng về hình thức pháp lý. Tùy thuộc vào hành vi vi phạm và hậu quả phát sinh, doanh nghiệp có thể phải chịu nhiều hình thức trách nhiệm khác nhau. Trách nhiệm dân sự có thể phát sinh khi hành vi vi phạm gây thiệt hại đến quyền và lợi ích hợp pháp của khách hàng, làm phát sinh

nghĩa vụ bồi thường thiệt hại, xin lỗi, cải chính hoặc khôi phục quyền lợi cho chủ thể dữ liệu. Trách nhiệm hành chính có thể được áp dụng khi doanh nghiệp vi phạm các quy định quản lý nhà nước về bảo vệ dữ liệu cá nhân, an toàn thông tin, an ninh mạng hoặc bảo vệ quyền lợi người tiêu dùng. Trong trường hợp hành vi vi phạm có tính chất nghiêm trọng, gây hậu quả lớn hoặc có dấu hiệu tội phạm, trách nhiệm hình sự có thể được xem xét đối với cá nhân hoặc pháp nhân thương mại có liên quan theo quy định của pháp luật.

Thứ năm, trách nhiệm của doanh nghiệp gắn liền với trách nhiệm giải trình. Trong bối cảnh kinh tế số, doanh nghiệp không chỉ có nghĩa vụ tuân thủ pháp luật mà còn phải chứng minh được việc tuân thủ đó. Trách nhiệm giải trình đòi hỏi doanh nghiệp phải lưu giữ hồ sơ xử lý dữ liệu, chứng minh căn cứ pháp lý của việc thu thập và sử dụng dữ liệu, thiết lập quy trình tiếp nhận và xử lý yêu cầu của khách hàng, kiểm soát việc chia sẻ dữ liệu với bên thứ ba, đồng thời có khả năng giải thích và chứng minh các biện pháp bảo vệ dữ liệu đã được áp dụng. Đây là đặc điểm quan trọng, cho thấy trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân không chỉ là trách nhiệm thụ động khi xảy ra vi phạm, mà còn là trách nhiệm chủ động trong quản trị rủi ro và bảo đảm tuân thủ pháp luật.

Thứ sáu, trách nhiệm của doanh nghiệp có thể phát sinh cả trong trường hợp vi phạm do bên thứ ba có liên quan đến quá trình xử lý dữ liệu. Trong thực tiễn kinh doanh, doanh nghiệp thường chia sẻ, chuyển giao hoặc thuê bên thứ ba xử lý dữ liệu cá nhân của khách hàng, chẳng hạn như đối tác công nghệ, đơn vị lưu trữ dữ liệu, đơn vị tiếp thị, trung gian thanh toán hoặc nhà cung cấp dịch vụ số. Trong các trường hợp này, nếu doanh nghiệp không lựa chọn, kiểm soát, giám sát hoặc ràng buộc trách nhiệm của bên thứ ba một cách phù hợp, doanh nghiệp vẫn có thể phải chịu trách nhiệm khi dữ liệu cá nhân của khách hàng bị sử dụng, tiết lộ hoặc chuyển giao trái pháp luật. Do đó, trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân không chỉ giới hạn trong phạm vi hoạt động nội bộ của doanh nghiệp, mà còn mở rộng đến việc kiểm soát các chủ thể có liên quan trong chuỗi xử lý dữ liệu.

Từ những đặc điểm trên có thể thấy, trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng không đồng nhất với việc liệt kê các nghĩa vụ tuân

thủ. Nghĩa vụ là những yêu cầu xử sự mà pháp luật đặt ra cho doanh nghiệp trong quá trình xử lý dữ liệu, còn trách nhiệm pháp lý là hậu quả bất lợi mà doanh nghiệp phải gánh chịu khi vi phạm các nghĩa vụ đó. Vì vậy, khi nghiên cứu trách nhiệm của doanh nghiệp, cần làm rõ cả hai phương diện: các nghĩa vụ pháp lý mà doanh nghiệp phải thực hiện và các hình thức trách nhiệm pháp lý phát sinh khi doanh nghiệp không thực hiện đúng các nghĩa vụ đó.

1.1.3. Các yếu tố ảnh hưởng đến trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Việc thực hiện trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân không chỉ phụ thuộc vào ý chí tuân thủ của doanh nghiệp mà còn chịu tác động bởi nhiều yếu tố khác nhau. Các yếu tố này có thể chia thành nhóm yếu tố pháp lý, kinh tế – công nghệ, tổ chức – quản trị nội bộ và nhận thức tuân thủ pháp luật.

Thứ nhất, yếu tố pháp lý.

Đây là yếu tố nền tảng và có ảnh hưởng trực tiếp đến mức độ thực hiện trách nhiệm bảo vệ dữ liệu cá nhân của doanh nghiệp. Một hệ thống pháp luật đầy đủ, rõ ràng và thống nhất không chỉ giúp doanh nghiệp nhận diện chính xác các nghĩa vụ pháp lý của mình mà còn tạo cơ sở để triển khai các biện pháp bảo vệ dữ liệu phù hợp trong thực tiễn hoạt động kinh doanh. Ngược lại, nếu các quy định pháp luật còn chồng chéo, thiếu đồng bộ hoặc chưa có hướng dẫn cụ thể, doanh nghiệp sẽ gặp khó khăn trong việc xác định phạm vi trách nhiệm cũng như cách thức tuân thủ, đặc biệt trong các hoạt động xử lý dữ liệu phức tạp như chuyển dữ liệu xuyên biên giới, chia sẻ dữ liệu với bên thứ ba hoặc xử lý dữ liệu cá nhân nhạy cảm.

Bên cạnh đó, hiệu quả thực thi pháp luật cũng là một khía cạnh quan trọng của yếu tố pháp lý. Việc tăng cường hoạt động thanh tra, kiểm tra và áp dụng các chế tài xử phạt đối với hành vi vi phạm về bảo vệ dữ liệu cá nhân có tác động trực tiếp đến ý thức tuân thủ của doanh nghiệp. Khi cơ chế thực thi nghiêm minh, minh bạch và có tính răn đe cao, doanh nghiệp sẽ có xu hướng chủ động xây dựng và duy trì các biện pháp bảo vệ dữ liệu cá nhân một cách bài bản hơn, từ đó góp phần nâng cao hiệu quả bảo vệ dữ liệu cá nhân của khách hàng trong thực tiễn.

Thứ hai, yếu tố kinh tế – công nghệ.

Trong bối cảnh nền kinh tế số phát triển mạnh mẽ, dữ liệu cá nhân ngày càng trở thành nguồn tài nguyên quan trọng, gắn liền với hoạt động sản xuất, kinh doanh và cung cấp dịch vụ của doanh nghiệp. Việc khai thác dữ liệu cá nhân giúp doanh nghiệp nâng cao hiệu quả quản trị, tối ưu hóa trải nghiệm khách hàng và gia tăng lợi thế cạnh tranh trên thị trường. Tuy nhiên, chính sự phụ thuộc ngày càng lớn vào dữ liệu cũng đặt ra những thách thức đáng kể đối với doanh nghiệp trong việc thực hiện trách nhiệm bảo vệ dữ liệu cá nhân.

Trước hết, việc tuân thủ các yêu cầu về bảo vệ dữ liệu đòi hỏi doanh nghiệp phải đầu tư đáng kể vào hạ tầng công nghệ thông tin và các giải pháp kỹ thuật như bảo mật hệ thống, mã hóa dữ liệu, kiểm soát truy cập, giám sát và lưu vết hoạt động xử lý dữ liệu. Những khoản đầu tư này có thể tạo ra áp lực tài chính, đặc biệt đối với các doanh nghiệp vừa và nhỏ, từ đó ảnh hưởng đến mức độ và hiệu quả thực hiện trách nhiệm bảo vệ dữ liệu cá nhân trong thực tế. Bên cạnh đó, sự phát triển nhanh chóng của các công nghệ mới như điện toán đám mây, trí tuệ nhân tạo, phân tích dữ liệu lớn và các nền tảng số làm gia tăng khối lượng, tốc độ và phạm vi xử lý dữ liệu cá nhân. Điều này không chỉ làm tăng nguy cơ rò rỉ, mất mát dữ liệu mà còn khiến doanh nghiệp gặp khó khăn trong việc kiểm soát toàn bộ vòng đời của dữ liệu, đặc biệt trong các trường hợp chia sẻ dữ liệu với bên thứ ba hoặc xử lý dữ liệu xuyên biên giới. Do đó, yếu tố kinh tế – công nghệ vừa là động lực, vừa là thách thức lớn đối với việc thực hiện trách nhiệm bảo vệ dữ liệu cá nhân của doanh nghiệp.

Thứ ba, yếu tố tổ chức, quản trị doanh nghiệp

Đây là yếu tố có vai trò quyết định đến năng lực thực thi trách nhiệm bảo vệ dữ liệu cá nhân của doanh nghiệp trong thực tế. Một doanh nghiệp có cơ cấu tổ chức hợp lý, phân công trách nhiệm rõ ràng và thiết lập được hệ thống kiểm soát nội bộ hiệu quả sẽ có điều kiện thuận lợi để triển khai các biện pháp bảo vệ dữ liệu một cách đồng bộ và nhất quán. Ngược lại, nếu cơ chế quản trị nội bộ còn lỏng lẻo, thiếu sự phối hợp giữa các bộ phận hoặc chưa xác định rõ trách

nhiệm của từng cá nhân, bộ phận trong quá trình xử lý dữ liệu, việc thực hiện các nghĩa vụ pháp lý về bảo vệ dữ liệu cá nhân sẽ gặp nhiều khó khăn.

Trong thực tiễn, nhiều doanh nghiệp chưa xây dựng được bộ phận chuyên trách về bảo vệ dữ liệu cá nhân, thiếu các quy trình nội bộ thống nhất trong thu thập, xử lý và lưu trữ dữ liệu, cũng như chưa thiết lập hệ thống quản trị rủi ro đối với hoạt động xử lý dữ liệu. Đặc biệt, trong trường hợp doanh nghiệp sử dụng dịch vụ của bên thứ ba hoặc hợp tác với các đối tác công nghệ, nếu không có cơ chế kiểm soát chặt chẽ và các thỏa thuận bảo mật rõ ràng, nguy cơ vi phạm dữ liệu cá nhân sẽ gia tăng đáng kể. Khi đó, mặc dù hành vi vi phạm có thể phát sinh từ bên thứ ba, doanh nghiệp vẫn có thể phải chịu trách nhiệm pháp lý do không thực hiện đầy đủ nghĩa vụ kiểm soát và giám sát theo quy định của pháp luật. Do đó, việc xây dựng một hệ thống quản trị nội bộ hiệu quả, bao gồm cơ cấu tổ chức phù hợp, quy trình xử lý dữ liệu rõ ràng và cơ chế kiểm soát rủi ro chặt chẽ, là điều kiện quan trọng để doanh nghiệp thực hiện đầy đủ trách nhiệm bảo vệ dữ liệu cá nhân của khách hàng trong thực tiễn.

Thứ tư, yếu tố nhận thức và tuân thủ pháp luật

Nhận thức và văn hóa tuân thủ pháp luật của doanh nghiệp là yếu tố mang tính quyết định đến hiệu quả thực hiện trách nhiệm bảo vệ dữ liệu cá nhân trong thực tiễn. Khi doanh nghiệp nhận thức đầy đủ rằng dữ liệu cá nhân không chỉ là nguồn lực phục vụ hoạt động kinh doanh mà còn là đối tượng được pháp luật bảo vệ, gắn liền với quyền riêng tư và quyền nhân thân của khách hàng, doanh nghiệp sẽ có xu hướng chủ động xây dựng chiến lược bảo vệ dữ liệu một cách bài bản. Điều này thể hiện ở việc ban hành các chính sách nội bộ rõ ràng, thiết lập quy trình xử lý dữ liệu chặt chẽ, cũng như đầu tư đào tạo nhân sự nhằm nâng cao năng lực tuân thủ pháp luật. Ngược lại, nếu doanh nghiệp chỉ coi việc bảo vệ dữ liệu cá nhân là nghĩa vụ mang tính hình thức hoặc thực hiện đối phó nhằm tránh chế tài, thì việc tuân thủ thường mang tính thụ động, thiếu bền vững. Trong trường hợp này, nguy cơ xảy ra vi phạm sẽ gia tăng, đặc biệt là

các vi phạm xuất phát từ yếu tố con người như truy cập trái phép, tiết lộ dữ liệu, sử dụng dữ liệu sai mục đích hoặc thiếu kỹ năng xử lý sự cố. Những vi phạm này không chỉ gây thiệt hại cho khách hàng mà còn ảnh hưởng tiêu cực đến uy tín, thương hiệu và trách nhiệm pháp lý của doanh nghiệp.

Bên cạnh đó, mức độ hiểu biết pháp luật của người lao động, khả năng cập nhật kịp thời các quy định pháp luật mới, cũng như ý thức chấp hành trong quá trình thực hiện công việc có ảnh hưởng trực tiếp đến hiệu quả triển khai các biện pháp bảo vệ dữ liệu cá nhân trong doanh nghiệp. Trong bối cảnh hệ thống pháp luật về bảo vệ dữ liệu cá nhân còn đang trong quá trình hoàn thiện, việc doanh nghiệp chủ động nâng cao nhận thức pháp lý và xây dựng văn hóa tuân thủ không chỉ giúp giảm thiểu rủi ro vi phạm mà còn tạo nền tảng cho việc thực hiện đầy đủ và hiệu quả trách nhiệm pháp lý trong bảo vệ dữ liệu cá nhân của khách hàng.

1.2. Một số vấn đề lý luận pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

1.2.1. Khái niệm pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Trong khoa học pháp lý, pháp luật được hiểu là hệ thống các quy tắc xử sự chung do Nhà nước ban hành hoặc thừa nhận, bảo đảm thực hiện nhằm điều chỉnh các quan hệ xã hội theo định hướng nhất định. Các quy phạm pháp luật mang tính bắt buộc chung, được bảo đảm thực hiện bằng quyền lực nhà nước và là công cụ chủ yếu để Nhà nước quản lý xã hội.

Trên cơ sở đó, pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng có thể được hiểu là tổng thể các quy phạm pháp luật do Nhà nước ban hành nhằm quy định quyền, nghĩa vụ và trách nhiệm pháp lý của doanh nghiệp trong quá trình thu thập, xử lý, lưu trữ, sử dụng, chia sẻ và bảo vệ dữ liệu cá nhân của khách hàng. Theo đó, pháp luật không chỉ xác định các nghĩa vụ cụ thể của doanh nghiệp như bảo mật dữ liệu, bảo đảm sự đồng ý của chủ thể dữ liệu, mà còn

thiết lập cơ chế kiểm soát, giám sát và xử lý vi phạm nhằm bảo đảm các nghĩa vụ này được thực thi trong thực tế.

Pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng vừa mang đầy đủ đặc điểm của pháp luật nói chung, vừa thể hiện tính đặc thù trong việc điều chỉnh các quan hệ phát sinh từ hoạt động xử lý dữ liệu trong môi trường số, qua đó góp phần bảo vệ quyền riêng tư của cá nhân và bảo đảm trật tự, an toàn trong hoạt động kinh doanh.

Từ những phân tích trên, có thể hiểu rằng pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là tổng thể các quy phạm pháp luật do Nhà nước ban hành nhằm điều chỉnh các quan hệ phát sinh trong quá trình doanh nghiệp thu thập, xử lý, lưu trữ và sử dụng dữ liệu cá nhân của khách hàng, đồng thời quy định nghĩa vụ, trách nhiệm và chế tài áp dụng đối với doanh nghiệp khi vi phạm các quy định về bảo vệ dữ liệu cá nhân. Hệ thống pháp luật này đóng vai trò quan trọng trong việc bảo đảm quyền riêng tư của cá nhân, tăng cường trách nhiệm của doanh nghiệp và góp phần xây dựng môi trường kinh doanh minh bạch, an toàn trong bối cảnh chuyển đổi số hiện nay.

1.2.2. Nguyên tắc pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Việc xác lập các nguyên tắc pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng có ý nghĩa quan trọng trong việc định hướng xây dựng và thực thi các quy định pháp luật liên quan đến bảo vệ dữ liệu cá nhân. Các nguyên tắc này không chỉ là cơ sở để xác định nghĩa vụ của doanh nghiệp trong quá trình thu thập, xử lý và sử dụng dữ liệu cá nhân mà còn là tiêu chuẩn để đánh giá mức độ tuân thủ pháp luật của doanh nghiệp. Trong bối cảnh kinh tế số và sự phát triển mạnh mẽ của công nghệ thông tin, việc bảo vệ dữ liệu cá nhân của khách hàng ngày càng trở thành yêu cầu thiết yếu nhằm bảo đảm quyền riêng tư của cá nhân cũng như duy trì sự minh bạch và an toàn trong hoạt động kinh doanh. Trên cơ sở nghiên cứu pháp luật quốc tế và kinh nghiệm lập pháp của nhiều quốc gia, có thể khái quát một số nguyên tắc cơ bản của pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng như sau:

Thứ nhất, nguyên tắc hợp pháp, công bằng và minh bạch trong xử lý dữ liệu cá nhân[1]. Theo nguyên tắc này, doanh nghiệp chỉ được phép thu thập và xử lý dữ liệu cá nhân của khách hàng khi có căn cứ pháp lý hợp lệ, đặc biệt là sự đồng ý của chủ thể dữ liệu hoặc các căn cứ pháp lý khác theo quy định của pháp luật. Quá trình xử lý dữ liệu phải được thực hiện một cách công bằng, không gây phương hại đến quyền và lợi ích hợp pháp của khách hàng. Đồng thời, doanh nghiệp có nghĩa vụ thông báo rõ ràng cho khách hàng về mục đích thu thập dữ liệu, phạm vi sử dụng, thời gian lưu trữ và các chủ thể có thể tiếp cận dữ liệu. Việc bảo đảm tính minh bạch trong xử lý dữ liệu cá nhân giúp tăng cường sự tin cậy của khách hàng đối với doanh nghiệp và góp phần hạn chế các hành vi lạm dụng dữ liệu cá nhân.

Thứ hai, nguyên tắc giới hạn mục đích xử lý dữ liệu[2]. Theo nguyên tắc này, dữ liệu cá nhân của khách hàng chỉ được thu thập và sử dụng cho những mục đích cụ thể, rõ ràng và hợp pháp đã được thông báo cho khách hàng trước khi tiến hành thu thập dữ liệu. Doanh nghiệp không được sử dụng dữ liệu cá nhân cho các mục đích khác với mục đích ban đầu nếu không có sự đồng ý của khách hàng hoặc không có căn cứ pháp lý theo quy định của pháp luật. Nguyên tắc này nhằm ngăn chặn việc sử dụng dữ liệu cá nhân một cách tùy tiện hoặc vượt quá phạm vi cần thiết cho hoạt động kinh doanh của doanh nghiệp.

Thứ ba, nguyên tắc tối thiểu hóa dữ liệu[3]. Theo đó, doanh nghiệp chỉ được thu thập và xử lý những dữ liệu cá nhân thực sự cần thiết cho việc cung cấp sản phẩm hoặc dịch vụ cho khách hàng. Việc thu thập dữ liệu phải phù hợp với mục đích đã xác định và không được vượt quá phạm vi cần thiết. Nguyên tắc tối thiểu hóa dữ liệu góp phần hạn chế nguy cơ lạm dụng thông tin cá nhân cũng như giảm thiểu rủi ro rò rỉ hoặc xâm phạm dữ liệu cá nhân trong quá trình xử lý dữ liệu.

---

[1] Theo Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu (GDPR), dữ liệu cá nhân phải được xử lý "một cách hợp pháp, công bằng và minh bạch đối với chủ thể dữ liệu" (European Parliament and Council, 2016, Article 5). Nguyên tắc này cũng được thừa nhận trong nhiều khuôn khổ pháp lý quốc tế như Hướng dẫn của OECD về bảo vệ quyền riêng tư và Khung bảo vệ dữ liệu cá nhân của ASEAN. Tại Việt Nam, Nghị định số 13/2023/NĐ-CP cũng ghi nhận các nguyên tắc tương tự trong việc xử lý dữ liệu cá nhân.

[2] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Article 5(1)(b); OECD. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

[3] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Article 5(1)(c).

Thứ tư, nguyên tắc bảo đảm an toàn và bảo mật dữ liệu cá nhân[4]. Doanh nghiệp có trách nhiệm áp dụng các biện pháp kỹ thuật và biện pháp quản lý phù hợp nhằm bảo đảm an toàn cho dữ liệu cá nhân của khách hàng trong suốt quá trình thu thập, lưu trữ và xử lý dữ liệu. Các biện pháp này có thể bao gồm mã hóa dữ liệu, kiểm soát truy cập, thiết lập hệ thống quản lý an toàn thông tin và thường xuyên kiểm tra, đánh giá các nguy cơ rủi ro liên quan đến bảo mật dữ liệu. Việc bảo đảm an toàn và bảo mật dữ liệu cá nhân không chỉ là nghĩa vụ pháp lý của doanh nghiệp mà còn là yếu tố quan trọng nhằm bảo vệ quyền riêng tư của khách hàng và duy trì uy tín của doanh nghiệp trên thị trường.

Thứ năm, nguyên tắc trách nhiệm giải trình của doanh nghiệp[5]. Theo nguyên tắc này, doanh nghiệp phải chịu trách nhiệm trước pháp luật về toàn bộ hoạt động thu thập, xử lý và bảo vệ dữ liệu cá nhân của khách hàng. Doanh nghiệp cần thiết lập các cơ chế quản lý nội bộ, quy trình kiểm soát và hệ thống giám sát nhằm bảo đảm việc xử lý dữ liệu cá nhân được thực hiện đúng quy định của pháp luật. Khi có yêu cầu từ cơ quan quản lý nhà nước hoặc khi xảy ra sự cố liên quan đến dữ liệu cá nhân, doanh nghiệp phải có khả năng chứng minh việc tuân thủ các quy định về bảo vệ dữ liệu cá nhân.

Thứ sáu, nguyên tắc bảo đảm quyền của chủ thể dữ liệu[6]. Pháp luật về bảo vệ dữ liệu cá nhân phải bảo đảm cho khách hàng – với tư cách là chủ thể dữ liệu – được thực hiện các quyền cơ bản đối với dữ liệu cá nhân của mình, bao gồm quyền được biết, quyền truy cập, quyền yêu cầu chỉnh sửa hoặc xóa dữ liệu, quyền hạn chế xử lý dữ liệu và quyền phản đối việc xử lý dữ liệu trong một số trường hợp nhất định. Việc bảo đảm các quyền này góp phần tăng cường sự kiểm soát của cá nhân đối với dữ liệu cá nhân của mình, đồng thời tạo cơ chế pháp lý để bảo vệ khách hàng trước các hành vi xâm phạm dữ liệu cá nhân.

---

[4] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Articles 5 and 32; OECD. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;* Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân (*Điều 26 – Bảo đảm an toàn dữ liệu cá nhân)

[5] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Article 5(2); Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân (*Điều 38, Điều 39)

[6] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Articles 12–22; Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân (Điều 9-* Quyền của chủ thể dữ liệu)

Như vậy, các nguyên tắc pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng đóng vai trò nền tảng trong việc định hướng xây dựng hệ thống pháp luật và tổ chức thực thi các quy định về bảo vệ dữ liệu cá nhân. Việc bảo đảm tuân thủ các nguyên tắc này không chỉ góp phần bảo vệ quyền riêng tư của khách hàng mà còn thúc đẩy sự phát triển bền vững của nền kinh tế số và nâng cao trách nhiệm xã hội của doanh nghiệp trong bối cảnh chuyển đổi số hiện nay.

1.2.3. Nội dung pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng là tổng thể các quy phạm pháp luật quy định nghĩa vụ của doanh nghiệp trong quá trình thu thập, xử lý, lưu trữ và sử dụng dữ liệu cá nhân của khách hàng. Những quy định này nhằm bảo đảm quyền riêng tư của cá nhân, đồng thời thiết lập cơ chế pháp lý để kiểm soát việc khai thác và sử dụng dữ liệu cá nhân trong hoạt động kinh doanh. Trong bối cảnh kinh tế số và sự phát triển mạnh mẽ của công nghệ thông tin, dữ liệu cá nhân ngày càng trở thành nguồn tài nguyên quan trọng đối với doanh nghiệp. Tuy nhiên, việc thu thập và sử dụng dữ liệu cá nhân nếu không được kiểm soát chặt chẽ có thể dẫn đến nguy cơ xâm phạm quyền riêng tư của khách hàng. Vì vậy, pháp luật của nhiều quốc gia đã xây dựng hệ thống quy định nhằm xác định rõ trách nhiệm của doanh nghiệp trong việc bảo vệ dữ liệu cá nhân. Về cơ bản, nội dung của pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng có thể được khái quát trên một số phương diện chủ yếu sau đây:

Trước hết, pháp luật quy định trách nhiệm của doanh nghiệp trong việc thu thập dữ liệu cá nhân của khách hàng. Theo đó, doanh nghiệp chỉ được phép thu thập dữ liệu cá nhân khi có căn cứ pháp lý hợp lệ, đặc biệt là sự đồng ý của khách hàng hoặc các trường hợp khác do pháp luật quy định[7]. Việc thu thập dữ liệu phải được thực hiện một cách minh bạch và đúng mục đích, đồng thời doanh nghiệp phải thông báo cho khách hàng về loại dữ liệu được thu thập, mục đích sử dụng dữ liệu, phạm vi sử dụng và thời gian lưu trữ dữ liệu. Quy định này nhằm bảo đảm rằng khách hàng

[7] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Articles 6, 13; Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân (Điều 11-Sự đồng ý của chủ thể dữ liệu)*

có đầy đủ thông tin và có quyền quyết định đối với việc cung cấp dữ liệu cá nhân của mình.

Hai là, pháp luật quy định trách nhiệm của doanh nghiệp trong việc xử lý và sử dụng dữ liệu cá nhân của khách hàng. Sau khi thu thập dữ liệu, doanh nghiệp có trách nhiệm xử lý và sử dụng dữ liệu cá nhân đúng với mục đích đã thông báo cho khách hàng và không được sử dụng dữ liệu cho các mục đích khác nếu chưa có sự đồng ý của chủ thể dữ liệu hoặc không có căn cứ pháp lý theo quy định của pháp luật[8]. Bên cạnh đó, việc chia sẻ hoặc chuyển giao dữ liệu cá nhân cho bên thứ ba cũng phải tuân thủ các điều kiện chặt chẽ nhằm bảo đảm dữ liệu cá nhân của khách hàng không bị lạm dụng hoặc sử dụng trái phép.

Ba là, pháp luật quy định trách nhiệm của doanh nghiệp trong việc bảo đảm an toàn và bảo mật dữ liệu cá nhân của khách hàng. Theo đó, doanh nghiệp phải áp dụng các biện pháp kỹ thuật và biện pháp quản lý phù hợp nhằm bảo vệ dữ liệu cá nhân trước nguy cơ truy cập trái phép, mất mát, phá hủy hoặc rò rỉ dữ liệu. Các biện pháp này có thể bao gồm việc thiết lập hệ thống bảo mật thông tin, kiểm soát quyền truy cập dữ liệu, mã hóa dữ liệu và xây dựng quy trình quản lý an toàn thông tin[9]. Trong trường hợp xảy ra sự cố rò rỉ dữ liệu, doanh nghiệp có trách nhiệm thông báo cho cơ quan có thẩm quyền và cho chủ thể dữ liệu theo quy định của pháp luật.

Bốn là, pháp luật quy định trách nhiệm của doanh nghiệp trong việc bảo đảm quyền của chủ thể dữ liệu[10]. Doanh nghiệp phải tạo điều kiện để khách hàng thực hiện các quyền của mình đối với dữ liệu cá nhân, bao gồm quyền được biết về việc xử lý dữ liệu, quyền truy cập dữ liệu, quyền yêu cầu chỉnh sửa hoặc xóa dữ liệu, quyền hạn chế xử lý dữ liệu và quyền phản đối việc xử lý dữ liệu trong một số trường hợp nhất định. Việc bảo đảm các quyền này góp phần tăng cường sự kiểm soát của cá nhân đối

---

[8] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Articles 5, 6, 28, 44–49; Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân (Điều 3, 11, 22, 23)*

[9] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Articles 5, 32, 33; Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân (Điều 26, 23)*

[10] European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*, Articles 12–21; Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân (*Điều 9 – Quyền của chủ thể dữ liệu)

với dữ liệu cá nhân của mình và nâng cao tính minh bạch trong hoạt động xử lý dữ liệu của doanh nghiệp.

Năm là, pháp luật quy định trách nhiệm pháp lý của doanh nghiệp khi vi phạm các quy định về bảo vệ dữ liệu cá nhân. Trong trường hợp doanh nghiệp vi phạm nghĩa vụ bảo vệ dữ liệu cá nhân của khách hàng, doanh nghiệp có thể phải chịu các hình thức trách nhiệm pháp lý khác nhau, bao gồm trách nhiệm hành chính, trách nhiệm dân sự và trong một số trường hợp nghiêm trọng có thể phát sinh trách nhiệm hình sự[11]. Việc quy định các chế tài xử lý vi phạm nhằm tăng cường tính răn đe, đồng thời bảo đảm việc tuân thủ pháp luật trong lĩnh vực bảo vệ dữ liệu cá nhân.

Như vậy, nội dung pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng bao gồm hệ thống các quy định điều chỉnh toàn bộ quá trình từ thu thập, xử lý, lưu trữ đến bảo vệ và sử dụng dữ liệu cá nhân. Các quy định này không chỉ nhằm bảo vệ quyền và lợi ích hợp pháp của khách hàng mà còn góp phần xây dựng môi trường kinh doanh minh bạch, an toàn và phù hợp với yêu cầu phát triển của nền kinh tế số.

1.3. Pháp luật một số quốc gia về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng và kinh nghiệm cho Việt Nam

Việc bảo vệ thông tin riêng cũng như thông tin cá nhân là vấn đề nóng không chỉ ở Việt Nam mà còn ở nhiều nước trên thế giới. Hiện nay, có khoảng 40 quốc gia đã ban hành các quy định pháp luật về bảo vệ thông tin cá nhân trên mạng.

1.3.1. Pháp luật Liên minh châu Âu về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR) áp dụng từ ngày 25/5/2018 và có phạm vi áp dụng rất rộng, không chỉ đối với doanh nghiệp đặt tại EU mà còn đối với doanh nghiệp ngoài EU nếu có hoạt động cung cấp hàng hóa, dịch vụ cho chủ thể dữ liệu ở EU hoặc theo dõi hành vi của họ. Cách thiết kế này cho

[11] European Parliament and Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Articles 82–84; Điều 288, Bộ luật Hình sự 2015 (sửa đổi 2017); Điều 38, Bộ luật Dân sự 2015; Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân

thấy trách nhiệm của doanh nghiệp được xác lập không đơn thuần theo nơi đặt trụ sở mà theo mức độ tham gia vào quá trình xử lý dữ liệu cá nhân của khách hàng[12].

Liên minh châu Âu là hình mẫu bảo hộ dữ liệu cá nhân với GDPR có tầm ảnh hưởng đến nhiều quốc gia và khu vực, đặc biệt là các tổ chức xử lý bất kỳ dữ liệu cá nhân nào của công dân EU và mức phạt lên đến 20 triệu EUR, cao hơn nữa là 4% doanh thu toàn cầu nếu một doanh nghiệp nào đó vi phạm về việc bảo vệ dữ liệu cá nhân[13]. Ngày nay, với những quy định quốc tế về kiểm soát an ninh và bảo vệ dữ liệu, tương lai sẽ còn tiếp tục xuất hiện các quy định khắt khe hơn, chế tài mạnh hơn và tổn hại danh tiếng nhiều hơn đối với chủ thể cố tình không tuân thủ.

Về nội dung, GDPR xây dựng một hệ thống trách nhiệm rất chặt chẽ đối với doanh nghiệp. Trước hết, doanh nghiệp phải tuân thủ các nguyên tắc cốt lõi của xử lý dữ liệu, gồm tính hợp pháp, công bằng và minh bạch; giới hạn mục đích; tối thiểu hóa dữ liệu; tính chính xác; giới hạn lưu trữ; và bảo đảm tính toàn vẹn, bảo mật dữ liệu. Đồng thời, GDPR đặt ra nguyên tắc trách nhiệm giải trình, theo đó bên kiểm soát dữ liệu phải chịu trách nhiệm và có khả năng chứng minh sự tuân thủ các nguyên tắc này. Đây là điểm tiến bộ nổi bật vì pháp luật không chỉ yêu cầu "làm đúng" mà còn yêu cầu doanh nghiệp "chứng minh được là mình làm đúng".

Bên cạnh đó, GDPR quy định tương đối toàn diện các nghĩa vụ của doanh nghiệp trong từng công đoạn xử lý dữ liệu. Doanh nghiệp phải có căn cứ pháp lý khi xử lý dữ liệu; phải cung cấp thông tin minh bạch cho chủ thể dữ liệu; trong một số trường hợp phải chỉ định cán bộ bảo vệ dữ liệu (DPO); phải thực hiện đánh giá tác động bảo vệ dữ liệu đối với các hoạt động xử lý có rủi ro cao; phải áp dụng các biện pháp kỹ thuật và tổ chức phù hợp nhằm bảo đảm an ninh xử lý dữ liệu; và phải thông báo vi phạm dữ liệu cá nhân cho cơ quan giám sát có thẩm quyền khi xảy ra sự cố. Đồng thời, GDPR trao cho chủ thể dữ liệu nhiều quyền mạnh như quyền được thông

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[13] Regulation (EU) 2016/679 (GDPR), Article 83

tin, quyền truy cập, quyền cải chính, quyền xóa dữ liệu, quyền hạn chế xử lý, quyền phản đối và quyền di chuyển dữ liệu.

Từ kinh nghiệm của Liên minh châu Âu có thể thấy, trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân được thiết kế theo hướng toàn diện, phòng ngừa rủi ro từ sớm và nhấn mạnh mạnh mẽ đến nghĩa vụ giải trình, quản trị nội bộ và trách nhiệm pháp lý khi có vi phạm.

1.3.2. Pháp luật Hoa Kỳ về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Hoa Kỳ hiện vẫn vận hành chủ yếu theo mô hình phân tán, kết hợp giữa luật liên bang theo ngành và luật bang. Trong số đó, California là bang có ảnh hưởng lớn nhất với Đạo luật Quyền riêng tư người tiêu dùng California (CCPA), được sửa đổi, bổ sung mạnh mẽ bởi CPRA. Theo thông tin chính thức của bang California, CCPA áp dụng đối với một số doanh nghiệp vì lợi nhuận hoạt động tại California và đạt một trong các ngưỡng nhất định, như doanh thu hằng năm trên 25 triệu USD, hoặc mua, bán, chia sẻ thông tin cá nhân của từ 100.000 cư dân/hộ gia đình trở lên, hoặc có từ 50% doanh thu hằng năm trở lên đến từ việc bán thông tin cá nhân của cư dân California[14].

Điểm nổi bật của mô hình California là tập trung mạnh vào các quyền của người tiêu dùng và nghĩa vụ minh bạch của doanh nghiệp. Theo hướng dẫn của Văn phòng Tổng chưởng lý California, người tiêu dùng có quyền biết doanh nghiệp đã thu thập những loại thông tin nào, nguồn thu thập, mục đích sử dụng, loại bên thứ ba được tiết lộ hoặc bán dữ liệu; có quyền yêu cầu xóa; quyền yêu cầu không bán hoặc không chia sẻ dữ liệu; quyền yêu cầu sửa thông tin không chính xác; và quyền giới hạn việc sử dụng, tiết lộ thông tin nhạy cảm. Doanh nghiệp còn có nghĩa vụ thông báo cho người tiêu dùng trước hoặc tại thời điểm thu thập về loại dữ liệu được thu thập và cách sử dụng dữ liệu đó.

So với GDPR, mô hình California ít nhấn mạnh vào hệ thống nguyên tắc tổng quát cho toàn bộ vòng đời xử lý dữ liệu, nhưng lại đặc biệt mạnh ở cơ chế bảo đảm

[14] *California Consumer Privacy Act of 2018*. https://leginfo.legislature.ca.gov/

quyền cá nhân và minh bạch hóa hoạt động thu thập, chia sẻ, kinh doanh dữ liệu. Kinh nghiệm của Hoa Kỳ vì vậy cho thấy một hướng tiếp cận khác: đặt trách nhiệm doanh nghiệp gắn chặt với nghĩa vụ công khai thông tin, đáp ứng yêu cầu của người tiêu dùng và kiểm soát việc thương mại hóa dữ liệu cá nhân. Mô hình này đặc biệt đáng tham khảo trong bối cảnh thị trường số phát triển nhanh, nơi dữ liệu khách hàng thường bị sử dụng cho mục đích quảng cáo, phân tích hành vi và chuyển giao cho nhiều bên trung gian.

1.3.3. Pháp luật Singapore về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

So với GDPR, hệ thống của Singapore có xu hướng thực dụng hơn nhưng vẫn đặt ra các nghĩa vụ cụ thể đối với doanh nghiệp. Theo hướng dẫn chính thức của PDPC, doanh nghiệp phải tuân thủ một chuỗi nghĩa vụ gồm: nghĩa vụ giải trình; nghĩa vụ thông báo; nghĩa vụ có sự đồng ý; nghĩa vụ giới hạn mục đích; nghĩa vụ bảo đảm tính chính xác; nghĩa vụ bảo vệ; nghĩa vụ giới hạn lưu giữ; nghĩa vụ hạn chế chuyển giao ra nước ngoài; nghĩa vụ cho phép tiếp cận và chỉnh sửa; và nghĩa vụ thông báo vi phạm dữ liệu. Đặc biệt, PDPA yêu cầu doanh nghiệp chỉ được thu thập, sử dụng hoặc tiết lộ dữ liệu cho các mục đích mà cá nhân đã đồng ý; không được ép cá nhân đồng ý vượt quá những gì hợp lý để cung cấp sản phẩm, dịch vụ; và phải bổ nhiệm nhân sự phụ trách bảo vệ dữ liệu, công khai thông tin liên hệ của người này.

Một điểm đáng chú ý của Singapore là việc gắn trách nhiệm bảo vệ dữ liệu với quản trị vận hành của doanh nghiệp. Doanh nghiệp phải có các "các biện pháp an ninh hợp lý" để ngăn ngừa truy cập, thu thập, sử dụng hoặc tiết lộ trái phép; phải chấm dứt lưu giữ hoặc tiêu hủy dữ liệu khi không còn cần thiết cho mục đích kinh doanh hoặc pháp lý; và chỉ được chuyển dữ liệu ra nước ngoài khi bảo đảm mức độ bảo vệ tương đương với chuẩn của PDPA, trừ trường hợp được miễn trừ. Khi xảy ra vi phạm dữ liệu mà có khả năng gây tổn hại đáng kể cho cá nhân hoặc có quy mô đáng kể, doanh nghiệp phải thông báo cho PDPC và cho những cá nhân bị ảnh hưởng trong thời gian sớm nhất có thể.

Kinh nghiệm của Singapore cho thấy một mô hình pháp luật tương đối phù hợp với các quốc gia châu Á: quy định không quá đồ sộ nhưng đủ rõ để buộc doanh

nghiệp phải nội luật hóa nghĩa vụ bảo vệ dữ liệu vào quy trình quản trị nội bộ. Từ đó, trách nhiệm của doanh nghiệp không chỉ tồn tại trên bình diện pháp lý mà còn được chuyển hóa thành các yêu cầu vận hành cụ thể như chỉ định DPO, quy trình tiếp nhận yêu cầu của chủ thể dữ liệu, chính sách lưu giữ dữ liệu và cơ chế phản ứng khi có vi phạm.

1.3.4. Kinh nghiệm cho Việt Nam

Từ việc nghiên cứu pháp luật của Liên minh châu Âu, Singapore và Hoa Kỳ, có thể rút ra một số kinh nghiệm quan trọng cho Việt Nam trong việc hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

Thứ nhất, Việt Nam cần xây dựng mô hình pháp luật theo hướng quản trị dữ liệu chủ động, lấy doanh nghiệp làm trung tâm của trách nhiệm tuân thủ. Kinh nghiệm từ GDPR cho thấy trách nhiệm của doanh nghiệp không chỉ phát sinh khi có vi phạm mà được thiết kế xuyên suốt toàn bộ vòng đời xử lý dữ liệu, từ thu thập, sử dụng đến lưu trữ và xóa bỏ dữ liệu. Điều này thể hiện sự chuyển dịch từ mô hình bảo vệ dữ liệu thụ động sang mô hình quản trị dữ liệu chủ động, trong đó doanh nghiệp phải tự đánh giá rủi ro, thiết lập cơ chế kiểm soát nội bộ và chịu trách nhiệm về toàn bộ hoạt động xử lý dữ liệu. Do đó, Việt Nam cần định hướng hoàn thiện pháp luật theo mô hình này, thay vì chỉ tập trung vào xử lý vi phạm, nhằm nâng cao tính phòng ngừa và hiệu quả thực thi trong thực tiễn.

Thứ hai, Việt Nam cần tiếp tục cụ thể hóa và hoàn thiện các quy định về nghĩa vụ của doanh nghiệp trong từng giai đoạn xử lý dữ liệu cá nhân. Kinh nghiệm từ EU và Singapore cho thấy pháp luật càng quy định rõ ràng, chi tiết thì khả năng tuân thủ và giám sát càng cao. Các nghĩa vụ của doanh nghiệp cần được xác định cụ thể ở từng khâu như thu thập dữ liệu, thông báo và xin ý kiến đồng ý của chủ thể dữ liệu, sử dụng đúng mục đích, bảo mật, lưu giữ, chia sẻ với bên thứ ba và chuyển dữ liệu ra nước ngoài. Việc quy định rõ các nghĩa vụ này không chỉ giúp doanh nghiệp dễ dàng áp dụng mà còn tạo cơ sở pháp lý vững chắc cho cơ quan quản lý trong việc thanh tra, kiểm tra và xử lý vi phạm.

Thứ ba, Việt Nam cần tăng cường ghi nhận và thực thi nguyên tắc trách nhiệm giải trình của doanh nghiệp. Một điểm tiến bộ nổi bật của GDPR và PDPA là yêu cầu

doanh nghiệp không chỉ tuân thủ mà còn phải chứng minh được việc tuân thủ thông qua hệ thống quản trị nội bộ. Điều này bao gồm việc xây dựng chính sách bảo vệ dữ liệu, phân công nhân sự phụ trách, thực hiện đánh giá tác động xử lý dữ liệu, lưu trữ hồ sơ và thiết lập cơ chế kiểm tra định kỳ. Do đó, pháp luật Việt Nam cần thể chế hóa rõ hơn nguyên tắc này, qua đó thúc đẩy doanh nghiệp chuyển từ trạng thái tuân thủ hình thức sang tuân thủ thực chất và có trách nhiệm.

Thứ tư, Việt Nam cần hoàn thiện cơ chế bảo đảm thực thi quyền của chủ thể dữ liệu theo hướng "quyền có thể thực hiện được". Kinh nghiệm từ Hoa Kỳ (đặc biệt là bang California) cho thấy việc bảo vệ dữ liệu cá nhân gắn chặt với việc bảo đảm các quyền của người tiêu dùng, như quyền được biết, quyền yêu cầu xóa, quyền từ chối chia sẻ dữ liệu và quyền hạn chế sử dụng dữ liệu nhạy cảm. Tuy nhiên, các quyền này chỉ có ý nghĩa khi được thiết kế kèm theo quy trình thực thi cụ thể. Vì vậy, Việt Nam cần quy định rõ về trình tự, thủ tục thực hiện quyền của chủ thể dữ liệu, thời hạn phản hồi, nghĩa vụ giải trình của doanh nghiệp và cơ chế khiếu nại, xử lý vi phạm khi quyền này không được bảo đảm.

Thứ năm, Việt Nam cần tăng cường cơ chế thực thi pháp luật và hệ thống chế tài đủ mạnh để bảo đảm tính răn đe. Một trong những yếu tố làm nên hiệu quả của GDPR là hệ thống chế tài nghiêm khắc, với mức xử phạt lớn và cơ chế bồi thường thiệt hại rõ ràng. Điều này tạo áp lực buộc doanh nghiệp phải tuân thủ pháp luật một cách nghiêm túc. Bên cạnh đó, vai trò của cơ quan giám sát độc lập trong việc thanh tra, kiểm tra và xử lý vi phạm cũng là yếu tố quan trọng. Do đó, Việt Nam cần tiếp tục hoàn thiện hệ thống chế tài theo hướng tương xứng với mức độ vi phạm, đồng thời nâng cao năng lực thực thi của cơ quan quản lý nhà nước nhằm bảo đảm các quy định pháp luật được áp dụng hiệu quả trong thực tiễn.

TIỂU KẾT CHƯƠNG 1

Chương 1 đã xây dựng cơ sở lý luận và pháp lý nền tảng cho việc nghiên cứu trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng. Thông qua việc tiếp cận đa chiều, từ góc độ lý luận đến pháp lý, Chương đã làm rõ bản chất của dữ liệu cá nhân cũng như xác định trách nhiệm của doanh nghiệp như một chế định pháp lý tổng hợp, bao trùm toàn bộ quá trình xử lý dữ liệu. Qua đó cho thấy, trách nhiệm của doanh nghiệp không chỉ dừng lại ở việc tuân thủ các quy định pháp luật mà còn gắn liền với yêu cầu bảo đảm quyền riêng tư, quyền nhân thân của khách hàng trong bối cảnh phát triển kinh tế số.

Bên cạnh đó, việc phân tích các nguyên tắc pháp luật cơ bản và nội dung trách nhiệm của doanh nghiệp theo từng giai đoạn xử lý dữ liệu đã góp phần làm rõ cấu trúc và phạm vi điều chỉnh của pháp luật trong lĩnh vực này. Đồng thời, các yếu tố ảnh hưởng đến việc thực hiện trách nhiệm của doanh nghiệp cũng được nhận diện, cho thấy tính chất đa chiều và phức tạp của vấn đề, đòi hỏi sự kết hợp giữa quy định pháp luật, năng lực công nghệ, tổ chức quản trị và ý thức tuân thủ của doanh nghiệp.

Đặc biệt, thông qua việc nghiên cứu kinh nghiệm pháp luật của một số quốc gia và khu vực tiêu biểu, Chương 1 đã chỉ ra xu hướng chung của pháp luật hiện đại là chuyển từ mô hình quản lý thụ động sang mô hình quản trị dữ liệu chủ động, nhấn mạnh trách nhiệm giải trình và vai trò trung tâm của doanh nghiệp trong bảo vệ dữ liệu cá nhân. Những kinh nghiệm này không chỉ có giá trị tham khảo mà còn là cơ sở quan trọng để định hướng hoàn thiện pháp luật Việt Nam trong thời gian tới.

Tóm lại, Chương 1 đã hình thành khung lý luận và pháp lý làm nền tảng cho việc phân tích thực trạng và đề xuất giải pháp ở các chương tiếp theo, góp phần bảo đảm tính logic và tính hệ thống của toàn bộ Đề án.

CHƯƠNG 2. THỰC TRẠNG PHÁP LUẬT VỀ TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA KHÁCH HÀNG VÀ THỰC TIỄN THỰC HIỆN

2.1. Thực trạng quy định pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

2.1.1. Trách nhiệm khi thu thập dữ liệu

Pháp luật Việt Nam hiện hành quy định doanh nghiệp chỉ được thu thập dữ liệu cá nhân khi có căn cứ pháp lý hợp lệ, trong đó phổ biến nhất là sự đồng ý của chủ thể dữ liệu hoặc các trường hợp được pháp luật cho phép. Đồng thời, doanh nghiệp có nghĩa vụ thông báo rõ ràng cho khách hàng về loại dữ liệu được thu thập, mục đích thu thập, phạm vi sử dụng, thời hạn lưu trữ và quyền của khách hàng đối với dữ liệu cá nhân của mình[15].

Các yêu cầu này hiện được ghi nhận trong Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15), trong đó Điều 5 quy định nguyên tắc xử lý dữ liệu cá nhân phải bảo đảm tính hợp pháp, minh bạch và đúng mục đích, còn Điều 6 quy định sự đồng ý của chủ thể dữ liệu phải được thể hiện rõ ràng, tự nguyện và có thể chứng minh. Trên cơ sở đó, Nghị định số 356/2025/NĐ-CP đã cụ thể hóa tại Điều 7 và Điều 9, quy định chi tiết về điều kiện thu thập dữ liệu và hình thức thể hiện sự đồng ý, đồng thời yêu cầu doanh nghiệp phải lưu trữ và cung cấp chứng cứ chứng minh sự đồng ý khi cần thiết.

Tuy nhiên, các quy định hiện hành vẫn bộc lộ một số hạn chế. Trước hết, yêu cầu về minh bạch chưa đi kèm với tiêu chuẩn cụ thể về cách thức cung cấp thông tin, dẫn đến tình trạng doanh nghiệp thực hiện nghĩa vụ này mang tính hình thức, đặc biệt trong môi trường trực tuyến. Thông tin thường được trình bày dài, phức tạp hoặc tích hợp nhiều mục đích xử lý trong một lần chấp thuận, gây khó khăn cho người dùng trong việc nhận biết và kiểm soát dữ liệu của mình. Bên cạnh đó, pháp luật chưa có quy định rõ ràng để kiểm soát hiệu quả các hình thức "đồng ý mặc định" hoặc "đồng ý gộp", làm suy giảm ý nghĩa thực chất của cơ chế đồng ý.

[15] Điều 3 và Điều 4 của Luật Bảo vệ dữ liệu cá nhân 2025.

So với pháp luật của Liên minh châu Âu - Quy định chung về bảo vệ dữ liệu (GDPR), pháp luật Việt Nam còn thiếu các tiêu chuẩn chi tiết về sự đồng ý, như yêu cầu sự đồng ý phải "tự do, cụ thể, được thông báo và rõ ràng" (freely given, specific, informed and unambiguous)[16]. Đồng thời, GDPR còn cho phép chủ thể dữ liệu rút lại sự đồng ý một cách dễ dàng, trong khi quy định của Việt Nam chưa làm rõ đầy đủ cơ chế này. Tương tự, pháp luật Singapore cũng yêu cầu doanh nghiệp phải chứng minh được căn cứ hợp pháp của việc thu thập và chịu trách nhiệm giải trình trong toàn bộ quá trình xử lý dữ liệu.

Như vậy, có thể thấy pháp luật Việt Nam đã bước đầu thiết lập khung pháp lý tương đối đầy đủ về trách nhiệm của doanh nghiệp trong giai đoạn thu thập dữ liệu cá nhân. Tuy nhiên, để nâng cao hiệu quả thực thi, cần tiếp tục hoàn thiện theo hướng tăng cường tính thực chất của cơ chế đồng ý, cụ thể hóa nghĩa vụ minh bạch và thiết lập các tiêu chuẩn rõ ràng hơn trong hoạt động thu thập dữ liệu.

2.1.2. Trách nhiệm khi xử lý, lưu trữ và bảo mật

Sau khi thu thập, doanh nghiệp tiếp tục phát sinh trách nhiệm trong quá trình xử lý, lưu trữ và bảo mật dữ liệu cá nhân của khách hàng. Theo Luật An toàn thông tin mạng năm 2015 (số 86/2015/QH13), các tổ chức, doanh nghiệp tham gia hoạt động trên môi trường mạng có nghĩa vụ áp dụng biện pháp bảo đảm an toàn thông tin, phòng ngừa hành vi xâm nhập, đánh cắp, phá hoại dữ liệu.

Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định 356/2025/NĐ-CP[17] tiếp tục cụ thể hóa trách nhiệm của doanh nghiệp theo hướng yêu cầu bảo đảm an toàn dữ liệu trong toàn bộ vòng đời xử lý. Theo đó, doanh nghiệp phải xây dựng và duy trì các biện pháp kỹ thuật và tổ chức phù hợp nhằm bảo vệ dữ liệu cá nhân khỏi nguy cơ bị truy cập trái phép, bị sửa đổi, bị rò rỉ hoặc bị hủy hoại. Trách nhiệm này bao gồm việc thiết lập cơ chế phân quyền truy cập dữ liệu trong nội bộ doanh nghiệp; áp dụng các biện pháp mã hóa, kiểm soát truy cập, lưu vết hoạt động xử lý dữ liệu; cũng như tổ chức đào tạo nhân sự nhằm hạn chế rủi ro phát sinh từ yếu tố con người. Ngoài ra, doanh nghiệp có nghĩa vụ bảo đảm dữ liệu cá nhân chỉ được xử lý trong phạm vi mục đích

[16] Điều 4 và Điều 7 GDPR

[17] Khoản 7 Điều 20; Khoản 7 Điều 21; Khoản 4 Điều 22; Khoản 3 Điều 33; Khoản 4 Điều 38 của Luật Bảo vệ dữ liệu cá nhân 2025

đã công bố và được khách hàng chấp thuận[18]. Việc sử dụng dữ liệu cá nhân vượt quá mục đích ban đầu, hoặc kéo dài thời gian lưu trữ không cần thiết, có thể làm phát sinh nguy cơ vi phạm quyền của khách hàng và trách nhiệm pháp lý tương ứng. Đồng thời, doanh nghiệp phải bảo đảm quyền của khách hàng trong việc yêu cầu truy cập, chỉnh sửa hoặc xóa dữ liệu cá nhân theo quy định pháp luật, qua đó thể hiện trách nhiệm tôn trọng quyền kiểm soát dữ liệu của chủ thể dữ liệu[19]. Xét về ưu điểm, các quy định này đã bước đầu tiếp cận với chuẩn mực quốc tế khi nhấn mạnh các nguyên tắc như mục đích cụ thể, tối thiểu hóa dữ liệu và bảo mật thông tin. Điều này góp phần tạo hành lang pháp lý quan trọng trong bối cảnh chuyển đổi số, đồng thời nâng cao ý thức của tổ chức, cá nhân trong việc bảo vệ dữ liệu, đặc biệt là dữ liệu cá nhân. Bên cạnh đó, việc kết hợp giữa quy định về kỹ thuật và trách nhiệm pháp lý giúp tăng tính ràng buộc và khả năng thực thi trên thực tế.

Tuy nhiên, các quy định hiện hành vẫn còn một số hạn chế. Trước hết, nhiều nội dung còn mang tính nguyên tắc chung, chưa có hướng dẫn chi tiết về tiêu chuẩn kỹ thuật cụ thể (ví dụ: mức độ mã hóa, chuẩn an ninh bắt buộc), dẫn đến khó khăn trong áp dụng thống nhất. Ngoài ra, cơ chế giám sát và chế tài xử lý vi phạm tuy đã có nhưng chưa thật sự mạnh và đồng bộ, đặc biệt trong môi trường số xuyên biên giới. Việc phân định rõ trách nhiệm giữa các chủ thể (bên kiểm soát, bên xử lý dữ liệu) trong một số trường hợp thực tế vẫn còn chưa rõ ràng.

So với Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR), có thể thấy pháp luật Việt Nam còn ở giai đoạn hoàn thiện. GDPR quy định rất chi tiết về trách nhiệm của từng chủ thể, nguyên tắc "trách nhiệm giải trình" (accountability), cũng như yêu cầu bắt buộc về đánh giá tác động xử lý dữ liệu (DPIA) và bổ nhiệm cán bộ bảo vệ dữ liệu (DPO). Đồng thời, chế tài của GDPR rất nghiêm khắc, có thể lên đến 4% doanh thu toàn cầu, tạo sức răn đe mạnh mẽ. Trong khi đó, pháp luật Việt Nam mới dừng ở mức định hướng và đang từng bước tiệm cận các chuẩn mực này. Tuy vậy, quy định của Việt Nam lại có ưu điểm là linh hoạt, phù hợp với điều kiện

[18] Khoản 2, khoản 3, Điều 3, Luật Bảo vệ dữ liệu cá nhân 2025
[19] Khoản 1-5, Điều 4, Luật Bảo vệ dữ liệu cá nhân 2025 - Quyền của chủ thể dữ liệu: biết, đồng ý/rút đồng ý, truy cập, sửa, xóa dữ liệu và quyền thực thi các quyền này.

phát triển kinh tế – xã hội trong nước, tránh gây áp lực quá lớn cho doanh nghiệp trong giai đoạn đầu.

2.1.3. Trách nhiệm khi chia sẻ, chuyển giao cho bên thứ ba

Theo Luật Bảo vệ dữ liệu cá nhân năm 2025[20] và Nghị định 356/2025/NĐ-CP[21], doanh nghiệp chỉ được chia sẻ hoặc chuyển giao dữ liệu cá nhân cho bên thứ ba khi có căn cứ pháp lý hợp lệ, bảo đảm mục đích xử lý phù hợp và đáp ứng điều kiện về quyền của chủ thể dữ liệu. Trong trường hợp pháp luật yêu cầu sự đồng ý của khách hàng, doanh nghiệp phải bảo đảm khách hàng được thông tin đầy đủ về bên nhận dữ liệu, phạm vi dữ liệu chuyển giao, mục đích sử dụng và thời hạn xử lý. Việc chuyển giao dữ liệu trong tình trạng thiếu minh bạch hoặc không có cơ chế kiểm soát có thể bị xem là hành vi xâm phạm dữ liệu cá nhân và làm phát sinh trách nhiệm pháp lý của doanh nghiệp.

Đồng thời, doanh nghiệp phải có trách nhiệm thiết lập cơ chế quản trị rủi ro đối với bên thứ ba, thông qua việc ký kết thỏa thuận xử lý dữ liệu, quy định rõ nghĩa vụ bảo mật, trách nhiệm bảo vệ dữ liệu và giới hạn mục đích sử dụng dữ liệu. Việc thiếu kiểm soát đối với đối tác hoặc nhà cung cấp dịch vụ có thể dẫn đến nguy cơ dữ liệu cá nhân bị mua bán trái phép hoặc bị sử dụng sai mục đích, và trong nhiều trường hợp doanh nghiệp vẫn phải chịu trách nhiệm pháp lý do không thực hiện đầy đủ nghĩa vụ kiểm soát trong chuỗi xử lý dữ liệu[22].

Như vậy, trách nhiệm của doanh nghiệp khi chia sẻ hoặc chuyển giao dữ liệu cá nhân cho bên thứ ba không chỉ là điều kiện hợp pháp của hành vi chuyển giao, mà

---

[20] Khoản 2, Điều 3, Luật Bảo vệ dữ liệu cá nhân 2025: "*Chỉ được thu thập, xử lý dữ liệu cá nhân đúng phạm vi, mục đích cụ thể, rõ ràng….*"

[21] Khoản 1 Điều 7, Nghị định 356/2025/NĐ-CP - Khi tổ chức/cá nhân chuyển giao dữ liệu cá nhân cho bên nhận theo các trường hợp được quy định trong Luật Bảo vệ dữ liệu cá nhân 2025 (ví dụ tại Điều 17 Luật Bảo vệ dữ liệu cá nhân 2025– xử lý dữ liệu với bên thứ ba), thì phải xác lập thỏa thuận chuyển giao và trong đó nêu rõ: Mục đích chuyển giao dữ liệu cá nhân, Đối tượng chủ thể và loại dữ liệu được chuyển giao phù hợp với mục đích, Thời hạn xử lý dữ liệu và yêu cầu xóa/hủy sau khi hoàn thành mục đích, Cơ sở pháp lý của việc chuyển giao dữ liệu cá nhân.

[22] Khoản 1, Điều 7, Nghị định 356/2025/NĐ-CP quy định rằng việc chuyển giao dữ liệu cá nhân cho bên thứ ba (thường được coi là bên xử lý dữ liệu hoặc bên nhận dữ liệu) phải đi kèm với thỏa thuận bằng văn bản nêu rõ ràng mục đích, phạm vi, thời hạn xử lý và cơ sở pháp lý của việc chia sẻ/chuyển giao này - nghĩa là doanh nghiệp phải thiết lập một cơ chế điều chỉnh quan hệ pháp lý và trách nhiệm giữa các bên để đảm bảo dữ liệu được xử lý đúng và an toàn.

còn bao gồm trách nhiệm giám sát, phòng ngừa rủi ro và bảo đảm dữ liệu không bị khai thác trái phép sau khi chuyển giao[23].

2.1.4. Trách nhiệm khi xảy ra vi phạm và chế tài

Trong trường hợp xảy ra vi phạm bảo vệ dữ liệu cá nhân, trách nhiệm của doanh nghiệp được xác định theo nhiều phương diện khác nhau, bao gồm trách nhiệm dân sự, trách nhiệm hành chính và trong một số trường hợp có thể phát sinh trách nhiệm hình sự đối với cá nhân có liên quan. Về phương diện dân sự, Bộ luật Dân sự năm 2015[24] là cơ sở để xác định nghĩa vụ bồi thường thiệt hại khi hành vi vi phạm quyền riêng tư hoặc xâm phạm dữ liệu cá nhân gây ra tổn thất cho khách hàng. Khi dữ liệu cá nhân bị lộ lọt, bị sử dụng trái phép hoặc gây thiệt hại về tài sản, danh dự, uy tín của khách hàng, doanh nghiệp có thể phải chịu trách nhiệm bồi thường theo quy định.

Về phương diện hành chính, các quy định về xử phạt vi phạm hành chính trong lĩnh vực an toàn thông tin mạng và bảo vệ dữ liệu cá nhân là căn cứ để áp dụng chế tài đối với doanh nghiệp khi có hành vi vi phạm. Trong thực tiễn, xử phạt hành chính là công cụ phổ biến nhằm tăng tính răn đe và buộc doanh nghiệp tuân thủ nghiêm túc nghĩa vụ bảo vệ dữ liệu cá nhân. Ngoài ra, Luật Bảo vệ quyền lợi người tiêu dùng[25] (sửa đổi 2023), Nghị định 15/2020/NĐ-CP của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ

---

[23] Song song với Nghị định, Luật Bảo vệ dữ liệu cá nhân 2025 đặt ra các nguyên tắc xử lý dữ liệu cá nhân, trong đó bao gồm việc: đảm bảo dữ liệu được xử lý đúng mục đích, trong phạm vi được cho phép và có sự đồng ý từ chủ thể dữ liệu; các bên liên quan trong chuỗi xử lý phải đảm bảo an toàn dữ liệu; chịu trách nhiệm nếu để xảy ra việc xử lý sai mục đích, thiếu minh bạch hoặc gây hại đến quyền của chủ thể dữ liệu.

[24] Điều 13 Bộ luật Dân sự 2015 - Bồi thường thiệt hại: "*Người có quyền dân sự bị xâm phạm được bồi thường toàn bộ thiệt hại do quyền đó bị xâm phạm, trừ trường hợp pháp luật có quy định khác*." (Nội dung này là nguyên tắc chung về bồi thường thiệt hại do xâm phạm quyền, được dùng làm căn cứ pháp lý khi dữ liệu cá nhân bị xử lý sai quy định dẫn đến thiệt hại cho chủ thể dữ liệu); Điều 584 Bộ luật Dân sự 2015 — Trách nhiệm bồi thường thiệt hại ngoài hợp đồng: "*Người gây thiệt hại do làm xâm phạm đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản, quyền sở hữu hoặc các quyền, lợi ích hợp pháp khác của người khác thì phải bồi thường, trừ trường hợp do lỗi của bị hại hoặc do tình thế cấp thiết*." (Nội dung này phản ánh nguyên tắc chung về trách nhiệm dân sự ngoài hợp đồng, áp dụng khi quyền riêng tư và dữ liệu cá nhân bị xâm phạm dẫn tới thiệt hại thật tế cho khách hàng). Như vậy, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định hướng dẫn (như Nghị định 356/2025/NĐ-CP) quy định trách nhiệm bảo vệ dữ liệu và báo cáo vi phạm, thì nghĩa vụ bồi thường thiệt hại do vi phạm quyền riêng tư và xâm phạm dữ liệu cá nhân về mặt dân sự vẫn được điều chỉnh theo các điều khoản chung của Bộ luật Dân sự 2015, đặc biệt là Điều 13 và Điều 584 nêu trên.

[25] Khoản 3, Điều 3, Luật Bảo vệ quyền lợi người tiêu dùng 2023 (Luật số 19/2023/QH15)

thông tin và giao dịch điện tử[26] cũng tạo cơ sở để xử lý hành vi xâm phạm thông tin người tiêu dùng, đặc biệt trong các giao dịch thương mại điện tử và cung cấp dịch vụ số.

Đáng chú ý, Luật Bảo vệ dữ liệu cá nhân năm 2025[27] và Nghị định 356/2025/NĐ-CP[28] đã nhấn mạnh yêu cầu về trách nhiệm giải trình và nghĩa vụ ứng phó khi xảy ra sự cố dữ liệu. Theo đó, doanh nghiệp có nghĩa vụ triển khai biện pháp khắc phục, hạn chế thiệt hại, đồng thời thực hiện cơ chế thông báo theo yêu cầu pháp luật đối với cơ quan quản lý và chủ thể dữ liệu bị ảnh hưởng. Nghĩa vụ này không chỉ giúp bảo vệ quyền lợi khách hàng mà còn góp phần nâng cao tính minh bạch, thúc đẩy doanh nghiệp tuân thủ và chịu trách nhiệm đối với dữ liệu mà mình xử lý.

Như vậy, cơ chế trách nhiệm và chế tài đối với doanh nghiệp khi xảy ra vi phạm được thiết lập theo hướng đa tầng, kết hợp giữa trách nhiệm dân sự, hành chính và các biện pháp quản lý chuyên ngành. Tuy nhiên, hiệu quả áp dụng trong thực tiễn vẫn phụ thuộc lớn vào năng lực giám sát, phát hiện vi phạm và mức độ tuân thủ thực chất của doanh nghiệp trong quá trình xử lý dữ liệu cá nhân.

2.2. Thực tiễn thực hiện pháp luật thông qua một số vụ việc điển hình

2.2.1. Vi phạm nghĩa vụ bảo mật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

(1) Mô tả vụ việc: Rò rỉ dữ liệu cá nhân quy mô lớn tại Trung tâm Thông tin Tín dụng Quốc gia Việt Nam (CIC) vào tháng 9 năm 2025[29].

---

[26] Khoản 1 và Khoản 2, Điều 1, Nghị định 15/2020/NĐ-CP

[27] Khoản 1, Điều 8, Luật Bảo vệ dữ liệu cá nhân năm 2025 quy định trách nhiệm đối với việc xử lý vi phạm và các biện pháp ứng phó được khái quát: tổ chức, cá nhân vi phạm có thể bị xử phạt hành chính, bị truy cứu trách nhiệm hình sự và phải bồi thường thiệt hại theo quy định của pháp luật; đồng thời Luật quy định trách nhiệm thực hiện các biện pháp bảo vệ dữ liệu phù hợp (mặc dù không quy định chi tiết thủ tục "thông báo sự cố"), và giao Chính phủ quy định chi tiết các nội dung này.

[28] Khoản 1, Điều 28, Nghị định 356/2025/NĐ-CP - Nội dung của thông báo vi phạm quy định bảo vệ dữ liệu cá nhân quy định nội dung bắt buộc phải có trong thông báo vi phạm, gồm mô tả bản chất sự cố, thời gian, địa điểm, tổ chức/cá nhân liên quan, loại và khối lượng dữ liệu bị ảnh hưởng, và các biện pháp đề xuất để khắc phục, giảm thiểu thiệt hại (Đây chính là quy định thể hiện nghĩa vụ doanh nghiệp phải báo cáo chi tiết về sự cố và kế hoạch khắc phục) và Điều 29 - Thông báo vi phạm dữ liệu vị trí và dữ liệu sinh trắc học (Đây là quy định cụ thể hóa nghĩa vụ ứng phó sự cố, thông báo cho cơ quan quản lý và chủ thể dữ liệu, và khắc phục thiệt hại)

[29] VnExpress. (2025). *Cảnh báo thủ đoạn lừa đảo mới, nếu dữ liệu cá nhân tại CIC bị lộ*. https://vnexpress.net/canh-bao-thu-doan-lua-dao-moi-neu-du-lieu-ca-nhan-tai-cic-bi-lo-4938185.html

Ngày 10/9/2025, Trung tâm Thông tin Tín dụng Quốc gia Việt Nam (CIC – một đơn vị thuộc Ngân hàng Nhà nước) xác nhận xảy ra một sự cố an ninh mạng nghiêm trọng, với các dấu hiệu xâm nhập, truy cập và chiếm đoạt dữ liệu cá nhân khách hàng trái phép. Đây là một trong những vụ lộ dữ liệu cá nhân lớn nhất trong lịch sử Việt Nam, ảnh hưởng đến hàng chục triệu hồ sơ thông tin tín dụng. Dữ liệu bị ảnh hưởng (theo thông tin ban đầu): họ và tên, ngày sinh, số điện thoại, địa chỉ, các thông tin liên quan tới hồ sơ tín dụng. Có dấu hiệu rằng dữ liệu đã bị truy cập trái phép và có thể bị chiếm đoạt, nhưng con số chính xác vẫn đang tiếp tục được thống kê. Cơ quan Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) đã tiếp nhận báo cáo, phối hợp cùng cơ quan chức năng và các nhà mạng để xác minh và ứng phó sự cố, đồng thời cảnh báo các tổ chức, cá nhân không tự ý tải/xử lý dữ liệu bị xâm phạm.

(2) Nghĩa vụ pháp lý của tổ chức xử lý dữ liệu cá nhân

Tại thời điểm xảy ra vụ việc rò rỉ dữ liệu tại CIC (tháng 9/2025), khung pháp lý điều chỉnh chủ yếu là Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, cùng với các quy định trong Luật An ninh mạng 2018 và Luật An toàn thông tin mạng 2015. Theo đó, Điều 26 Nghị định 13/2023/NĐ-CP đã quy định tổ chức xử lý dữ liệu phải áp dụng các biện pháp kỹ thuật và quản lý để bảo đảm an toàn dữ liệu, kiểm soát truy cập và ngăn chặn hành vi xâm phạm. Tuy nhiên, các quy định này còn mang tính nguyên tắc, chưa cụ thể hóa các tiêu chuẩn kỹ thuật bắt buộc, dẫn đến khó bảo đảm tính thống nhất và hiệu quả trong thực tiễn, đặc biệt đối với các hệ thống dữ liệu quy mô lớn và có độ nhạy cảm cao như CIC.

Sau đó, pháp luật Việt Nam đã có bước hoàn thiện quan trọng với việc ban hành Luật Dữ liệu 2024 (Luật số 60/2024/QD5) và Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15). Các văn bản này đã nâng cao trách nhiệm của tổ chức xử lý dữ liệu, trong đó Điều 5, Luật Dữ liệu 2024 quy định nguyên tắc bảo đảm an toàn, an ninh dữ liệu, còn Khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025 đã làm rõ trách nhiệm pháp lý, bao gồm xử phạt, bồi thường và truy cứu trách nhiệm đối với hành vi vi phạm. Tuy nhiên, các quy định này vẫn mang tính khung, chưa quy định cụ thể các tiêu chuẩn kỹ thuật và cơ chế kiểm soát chi tiết trong bảo mật dữ liệu.

Để khắc phục phần nào hạn chế đó, Nghị định 356/2025/NĐ-CP (31/12/2025) đã được ban hành nhằm hướng dẫn chi tiết thi hành, trong đó Điều 28 và Điều 29 đã quy định cụ thể hơn về nghĩa vụ thông báo vi phạm và trách nhiệm ứng phó sự cố dữ liệu. Tuy nhiên, các quy định này vẫn chủ yếu tập trung vào giai đoạn xử lý sau khi sự cố xảy ra, mà chưa thiết lập đầy đủ các cơ chế phòng ngừa như tiêu chuẩn bảo mật bắt buộc, kiểm tra an ninh định kỳ hoặc kiểm toán độc lập hệ thống dữ liệu.

Có thể thấy rằng, mặc dù hệ thống pháp luật hiện hành đã có sự bổ sung và hoàn thiện đáng kể, kết hợp giữa luật và nghị định hướng dẫn, nhưng vẫn chưa giải quyết triệt để các rủi ro về an toàn dữ liệu trong thực tiễn.

(3) Phân tích dấu hiệu vi phạm nghĩa vụ bảo mật dữ liệu

Từ các tình tiết của vụ việc rò rỉ dữ liệu tại Trung tâm Thông tin Tín dụng Quốc gia Việt Nam (CIC), có thể nhận thấy nhiều dấu hiệu vi phạm nghĩa vụ bảo mật dữ liệu cá nhân của tổ chức xử lý dữ liệu, đặc biệt liên quan đến trách nhiệm bảo đảm an ninh, an toàn hệ thống thông tin.

Trước đâu, Điều 26 Nghị định 13/2023/NĐ-CP, tổ chức xử lý dữ liệu cá nhân có nghĩa vụ áp dụng các biện pháp kỹ thuật và quản lý nhằm bảo đảm an ninh, an toàn dữ liệu, bao gồm việc kiểm soát truy cập, phòng ngừa và phát hiện các hành vi xâm nhập trái phép. Tuy nhiên, việc dữ liệu cá nhân của hàng triệu người dùng bị rò rỉ cho thấy hệ thống bảo mật có khả năng tồn tại lỗ hổng, đặc biệt trong việc kiểm soát truy cập và bảo vệ dữ liệu khỏi các hành vi tấn công hoặc khai thác trái phép. Điều 24 Nghị định 13/2023/NĐ-CP, tổ chức phải thực hiện đánh giá tác động xử lý dữ liệu nhằm nhận diện và kiểm soát rủi ro. Việc không phát hiện và ngăn chặn kịp thời sự cố cho thấy hoạt động đánh giá rủi ro chưa được thực hiện, hoặc được thực hiện nhưng không hiệu quả, từ đó dẫn đến vi phạm nghĩa vụ phòng ngừa rủi ro chứ không chỉ là vi phạm trong khâu xử lý sự cố.

Từ góc độ pháp luật hiện hành, nghĩa vụ bảo mật dữ liệu cá nhân của tổ chức xử lý dữ liệu không còn được quy định chi tiết theo từng biện pháp kỹ thuật như trước đây, mà được thể hiện thông qua các nguyên tắc và trách nhiệm pháp lý tổng quát. Cụ thể, theo Điều 5 Luật Dữ liệu 2024 (Luật số 60/2024/QH15), dữ liệu phải được bảo đảm an ninh, an toàn và toàn vẹn trong suốt quá trình xử lý, qua đó đặt ra yêu

cầu bảo mật mang tính xuyên suốt đối với tổ chức xử lý dữ liệu. Đồng thời, theo khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15), tổ chức phải chịu trách nhiệm pháp lý khi để xảy ra vi phạm, kể cả trong trường hợp vi phạm xuất phát từ việc không bảo đảm an toàn hệ thống. Nghị định 356/2025/NĐ-CP bổ sung các nghĩa vụ liên quan đến xử lý sự cố dữ liệu, đặc biệt tại Điều 28 và Điều 29, theo đó tổ chức phải thông báo và thực hiện các biện pháp khắc phục khi xảy ra vi phạm. Tuy nhiên, các quy định này chủ yếu mang tính hậu kiểm, phát sinh sau khi sự cố đã xảy ra, mà chưa thiết lập các yêu cầu cụ thể về tiêu chuẩn bảo mật hoặc cơ chế phòng ngừa tương ứng.

Như vậy, pháp luật hiện hành đã chuyển từ cách tiếp cận quy định cụ thể về biện pháp bảo mật sang việc nhấn mạnh nguyên tắc và trách nhiệm pháp lý của tổ chức. Tuy nhiên, sự thay đổi này cũng làm lộ rõ khoảng trống khi thiếu các quy định cụ thể về kiểm soát và phòng ngừa rủi ro, dẫn đến việc nghĩa vụ bảo mật trên thực tế phụ thuộc nhiều vào mức độ tuân thủ của tổ chức hơn là cơ chế pháp lý ràng buộc chặt chẽ.

(4) Hậu quả pháp lý và xã hội của vụ việc

Vụ việc rò rỉ dữ liệu cá nhân quy mô lớn tại Trung tâm Thông tin Tín dụng Quốc gia Việt Nam (CIC) không chỉ đặt ra vấn đề về vi phạm nghĩa vụ bảo mật mà còn kéo theo những hậu quả nghiêm trọng trên cả phương diện pháp lý và xã hội.

Trước hết, về mặt pháp lý, việc để xảy ra rò rỉ dữ liệu cá nhân đồng nghĩa với việc tổ chức xử lý dữ liệu không bảo đảm yêu cầu về an ninh, an toàn dữ liệu theo Điều 5 Luật Dữ liệu 2024 (Luật số 60/2024/QH15). Đây không chỉ là vi phạm nguyên tắc mà còn là căn cứ để xác định trách nhiệm pháp lý của tổ chức. Theo khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15), tổ chức phải chịu trách nhiệm khi để xảy ra vi phạm, kể cả trong trường hợp vi phạm xuất phát từ sự thiếu sót trong việc bảo đảm an toàn hệ thống. Điều này có thể dẫn đến các hậu quả pháp lý như xử phạt hành chính, nghĩa vụ bồi thường thiệt hại cho chủ thể dữ liệu, và trong trường hợp nghiêm trọng có thể bị xem xét trách nhiệm theo các quy định pháp luật có liên quan.

Bên cạnh đó, theo Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP, khi xảy ra sự cố rò rỉ dữ liệu, tổ chức có nghĩa vụ thông báo, phối hợp xử lý và thực hiện các biện pháp khắc phục hậu quả. Điều này đồng nghĩa với việc doanh nghiệp không chỉ chịu trách nhiệm pháp lý mà còn phải gánh chịu các chi phí đáng kể liên quan đến xử lý sự cố, khắc phục hệ thống, cũng như chi phí phát sinh từ việc bồi thường thiệt hại và phục hồi uy tín. Theo báo cáo của IBM (Cost of a Data Breach Report 2023), chi phí trung bình của một vụ rò rỉ dữ liệu trên toàn cầu lên tới khoảng 4,45 triệu USD[30], trong đó lĩnh vực tài chính - ngân hàng là một trong những ngành chịu thiệt hại lớn nhất. Đối với Việt Nam, theo cảnh báo của Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT), các vụ lộ lọt dữ liệu cá nhân trong lĩnh vực tài chính có nguy cơ bị lợi dụng cho các hành vi gian lận như mạo danh vay tín dụng, lừa đảo tài chính và chiếm đoạt tài sản[31].

Ngoài ra, sự cố rò rỉ dữ liệu quy mô lớn còn làm suy giảm niềm tin của xã hội đối với các tổ chức nắm giữ và xử lý dữ liệu, đặc biệt là các tổ chức có vai trò trung gian quan trọng như CIC. Khi niềm tin vào khả năng bảo mật dữ liệu bị suy giảm, người dùng có xu hướng e ngại trong việc cung cấp thông tin, từ đó ảnh hưởng đến hiệu quả vận hành của toàn bộ hệ thống kinh tế số.

(5) So sánh với chuẩn pháp luật quốc tế

So với các chuẩn mực pháp lý quốc tế - Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR), cách tiếp cận của pháp luật Việt Nam đối với nghĩa vụ bảo mật dữ liệu cá nhân vẫn còn những khác biệt đáng kể, đặc biệt trong việc phòng ngừa và kiểm soát rủi ro.

Về bản chất nghĩa vụ bảo mật, GDPR quy định nghĩa vụ này không chỉ dừng lại ở việc bảo vệ dữ liệu, mà yêu cầu doanh nghiệp phải áp dụng các biện pháp kỹ thuật và tổ chức "phù hợp với mức độ rủi ro", bao gồm mã hóa, kiểm soát truy cập, và đặc biệt là nguyên tắc "bảo vệ dữ liệu theo thiết kế và theo mặc định" (privacy by design & by default). Điều này có nghĩa là nghĩa vụ bảo mật phải được tích hợp ngay

[30] Cost of a Data Breach Report 2023. Link truy cập: https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf?utm_source=chatgpt.com

[31] Tạp chí Thanh tra. (2025). *Vụ lộ dữ liệu cá nhân của CIC: VNCERT yêu cầu không khai thác trái phép*. Truy cập từ: https://thanhtra.com.vn/an-ninh-trat-tu-D718A18CA/vu-lo-du-lieu-ca-nhan-cua-cic-vncert-yeu-cau-khong-khai-thac-trai-phep-fd59bf7b6.html

từ giai đoạn thiết kế hệ thống, chứ không phải chỉ được thực hiện khi dữ liệu đã được xử lý. Trong khi luật Việt Nam hiện hành, thông qua Điều 5 Luật Dữ liệu 2024 và khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, chủ yếu xác lập nghĩa vụ bảo đảm an toàn dữ liệu và trách nhiệm pháp lý khi xảy ra vi phạm, nhưng chưa đặt ra yêu cầu cụ thể về việc tích hợp bảo mật ngay từ giai đoạn thiết kế hệ thống. Điều này cho thấy nghĩa vụ bảo mật trong pháp luật Việt Nam vẫn mang tính "kết quả" nhiều hơn là "quá trình".

Về cơ chế phòng ngừa rủi ro, GDPR yêu cầu doanh nghiệp phải thực hiện đánh giá tác động bảo vệ dữ liệu (DPIA) đối với các hoạt động xử lý có rủi ro cao, đồng thời phải duy trì cơ chế giám sát liên tục đối với hệ thống xử lý dữ liệu. Nghĩa vụ này nhằm phát hiện sớm và ngăn chặn các nguy cơ trước khi xảy ra vi phạm. Ngược lại, trước đây pháp luật Việt Nam có quy định về đánh giá rủi ro, nhưng trong khuôn khổ mới lại chưa cụ thể hóa đầy đủ cơ chế này, dẫn đến việc phòng ngừa rủi ro chủ yếu phụ thuộc vào ý thức tuân thủ của doanh nghiệp.

Về cơ chế xử lý vi phạm, GDPR thiết lập nghĩa vụ rất chặt chẽ trong trường hợp xảy ra rò rỉ dữ liệu, bao gồm việc thông báo cho cơ quan quản lý trong vòng 72 giờ và thông báo cho chủ thể dữ liệu nếu có nguy cơ cao[32]. Quan trọng hơn, việc vi phạm nghĩa vụ bảo mật không chỉ bị xử lý sau khi hậu quả xảy ra, mà còn bị đánh giá dựa trên việc doanh nghiệp có thực hiện đầy đủ nghĩa vụ phòng ngừa hay không. Trong khi đó, theo Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP, chủ yếu tập trung vào nghĩa vụ thông báo và khắc phục sau khi sự cố đã xảy ra, chưa đặt ra cơ chế đánh giá trách nhiệm dựa trên mức độ phòng ngừa trước đó.

(6) Nhận xét và vấn đề đặt ra đối với pháp luật Việt Nam

Từ việc phân tích vụ việc rò rỉ dữ liệu tại Trung tâm Thông tin Tín dụng Quốc gia Việt Nam (CIC) và đối chiếu với các quy định pháp luật hiện hành, có thể nhận thấy rằng pháp luật Việt Nam đã có những bước tiến quan trọng trong việc xác lập nghĩa vụ bảo vệ dữ liệu cá nhân. Các văn bản này đã chuyển trọng tâm từ việc quy

[32] *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…". https://eur-lex.europa.eu/eli/reg/2016/679/oj

định các biện pháp kỹ thuật cụ thể sang việc nhấn mạnh nguyên tắc quản trị dữ liệu và trách nhiệm pháp lý của tổ chức xử lý dữ liệu.

Theo quy định của pháp luật Việt Nam hiện hành, trách nhiệm của tổ chức xử lý dữ liệu cá nhân đã được quy định tương đối đầy đủ trên nhiều phương diện. Cụ thể, theo Khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, tổ chức vi phạm có thể bị xử phạt hành chính, bồi thường thiệt hại và trong trường hợp nghiêm trọng có thể bị truy cứu trách nhiệm hình sự. Đồng thời, Điều 26 Nghị định 13/2023/NĐ-CP cũng quy định nghĩa vụ áp dụng các biện pháp bảo đảm an ninh, an toàn dữ liệu cá nhân; trong khi Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP đã cụ thể hóa nghĩa vụ thông báo và xử lý khi xảy ra vi phạm dữ liệu. Tuy nhiên, các quy định này vẫn còn một số hạn chế nhất định. Trước hết, pháp luật chưa quy định rõ ràng về mức xử phạt cụ thể tương ứng với quy mô và mức độ vi phạm, đặc biệt đối với các vụ việc rò rỉ dữ liệu quy mô lớn như trường hợp tại CIC. Bên cạnh đó, các quy định về trách nhiệm hình sự đối với hành vi vi phạm dữ liệu cá nhân vẫn còn phân tán trong các tội danh chung, chưa có quy định riêng biệt, dẫn đến khó khăn trong việc áp dụng trên thực tế. Ngoài ra, nghĩa vụ phòng ngừa rủi ro như đánh giá an ninh hệ thống, kiểm tra định kỳ hay áp dụng tiêu chuẩn kỹ thuật vẫn mang tính nguyên tắc, chưa được cụ thể hóa thành yêu cầu bắt buộc, đồng thời, cách tiếp cận này vẫn mang tính hậu kiểm, tức là chỉ phát sinh trách nhiệm sau khi hậu quả đã xảy ra.

Chưa thiết lập được cơ chế phòng ngừa rủi ro mang tính bắt buộc, khi các quy định chủ yếu dừng ở nguyên tắc chung tại Điều 5 Luật Dữ liệu 2024 mà chưa cụ thể hóa thành các tiêu chuẩn kỹ thuật hoặc quy trình kiểm soát bắt buộc đối với doanh nghiệp. Điều này dẫn đến việc nghĩa vụ bảo mật phụ thuộc nhiều vào mức độ tuân thủ tự nguyện, thay vì được bảo đảm bằng cơ chế pháp lý chặt chẽ.

Một hạn chế quan trọng khác là pháp luật hiện hành chưa quy định đầy đủ nghĩa vụ bảo mật theo hướng xuyên suốt vòng đời dữ liệu, đặc biệt trong các giai đoạn thiết kế và vận hành hệ thống. So với chuẩn mực quốc tế như GDPR, nơi yêu cầu áp dụng nguyên tắc “bảo vệ dữ liệu theo thiết kế”, pháp luật Việt Nam vẫn chưa thiết lập nghĩa vụ tích hợp bảo mật ngay từ đầu, mà chủ yếu tập trung vào việc xử lý khi sự cố đã xảy ra.

Ngoài ra, cơ chế giám sát và kiểm tra việc tuân thủ nghĩa vụ bảo mật cũng chưa được quy định rõ ràng. Mặc dù, Nghị định 356/2025/NĐ-CP đã bổ sung các quy định về thông báo và xử lý vi phạm tại Điều 28 và Điều 29, nhưng vẫn chưa thiết lập cơ chế kiểm tra định kỳ, kiểm toán dữ liệu hoặc giám sát độc lập đối với hệ thống xử lý dữ liệu của doanh nghiệp. Điều này làm giảm khả năng phát hiện sớm các lỗ hổng bảo mật và các nguy cơ tiềm ẩn.

2.2.2. Thu thập, sử dụng trái phép về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

(1) Mô tả vụ việc: Thu thập, mua bán gần 56 triệu dữ liệu cá nhân

Đầu năm 2025, cơ quan chức năng Việt Nam đã phát hiện và triệt phá một đường dây thu thập, mua bán dữ liệu cá nhân quy mô lớn trên phạm vi toàn quốc, với số lượng lên tới gần 56 triệu thông tin dữ liệu cá nhân của công dân[33]. Các dữ liệu bị thu thập và rao bán bao gồm nhiều loại thông tin nhạy cảm như họ và tên, số điện thoại, địa chỉ, thông tin nghề nghiệp, cũng như dữ liệu liên quan đến hoạt động tài chính – tín dụng của người dùng.

Theo kết quả điều tra, các đối tượng đã sử dụng nhiều phương thức khác nhau để thu thập và khai thác dữ liệu, bao gồm việc truy cập trái phép vào hệ thống thông tin, lợi dụng quyền truy cập nội bộ hoặc sử dụng các tài khoản ảo trên không gian mạng để mua bán, trao đổi dữ liệu nhằm mục đích trục lợi. Dữ liệu sau khi bị thu thập được chuyển giao cho các tổ chức, cá nhân khác để phục vụ các hoạt động quảng cáo, chào mời dịch vụ tài chính hoặc thậm chí phục vụ các hành vi lừa đảo, chiếm đoạt tài sản.

Cơ quan điều tra xác định hành vi của các đối tượng là hành vi thu thập và sử dụng dữ liệu cá nhân trái phép, xâm phạm nghiêm trọng quyền của chủ thể dữ liệu. Các đối tượng liên quan đã bị khởi tố về tội "đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông" theo quy định của Bộ luật Hình sự, đồng thời các

[33] Công an Nhân dân. (2025). *Triệt phá đường dây mua bán gần 56 triệu dữ liệu cá nhân*. https://cand.com.vn/Ho-so-Interpol/triet-pha-duong-day-mua-ban-gan-56-trieu-du-lieu-ca-nhan-i759592/

hành vi vi phạm cũng đặt ra những vấn đề đáng chú ý về trách nhiệm của các tổ chức trong việc bảo vệ dữ liệu cá nhân trong quá trình thu thập, xử lý và lưu trữ dữ liệu.

(2) Nghĩa vụ pháp lý của tổ chức xử lý dữ liệu cá nhân

Tại thời điểm xảy ra vụ việc (năm 2025), khung pháp lý điều chỉnh chủ yếu là Nghị định 13/2023/NĐ-CP. Theo đó, doanh nghiệp chỉ được thu thập và sử dụng dữ liệu cá nhân khi có căn cứ pháp lý hợp lệ, đặc biệt là sự đồng ý của chủ thể dữ liệu theo quy định tại khoản 1 Điều 11 và Điều 17 Nghị định 13/2023/NĐ-CP, đồng thời phải bảo đảm việc xử lý dữ liệu đúng mục đích đã thông báo theo nguyên tắc tại Điều 11. Bên cạnh đó, doanh nghiệp có nghĩa vụ áp dụng các biện pháp kiểm soát nội bộ nhằm bảo vệ dữ liệu cá nhân, bao gồm việc kiểm soát truy cập và ngăn chặn hành vi sử dụng trái phép theo Điều 26 Nghị định 13/2023/NĐ-CP, cũng như thực hiện đánh giá tác động xử lý dữ liệu để kiểm soát rủi ro theo Điều 24 Nghị định này.

Tuy nhiên, Nghị định 13/2023/NĐ-CP vẫn chưa giải quyết triệt để vấn đề thu thập và sử dụng dữ liệu trái phép trong thực tiễn. Mặc dù khoản 1 và khoản 2 Điều 11 đã quy định nguyên tắc phải có sự đồng ý của chủ thể dữ liệu và xử lý đúng mục đích, đồng thời Điều 26 yêu cầu tổ chức phải áp dụng biện pháp bảo đảm an ninh, an toàn dữ liệu cá nhân, nhưng các quy định này chủ yếu mang tính nguyên tắc, chưa cụ thể hóa thành các nghĩa vụ kiểm soát nội bộ bắt buộc. Bên cạnh đó, dù Điều 24 Nghị định 13/2023/NĐ-CP đã quy định về nghĩa vụ đánh giá tác động xử lý dữ liệu cá nhân, nhưng chưa xác định rõ tiêu chí, tần suất và phương thức thực hiện, dẫn đến khó khăn trong việc kiểm soát rủi ro trên thực tế. Ngoài ra, pháp luật cũng chưa quy định cụ thể trách nhiệm của tổ chức trong việc giám sát hoạt động của nhân sự có quyền truy cập dữ liệu hoặc kiểm soát chặt chẽ việc chia sẻ dữ liệu cho bên thứ ba. Chính những hạn chế này đã tạo ra khoảng trống trong cơ chế kiểm soát, dẫn đến nguy cơ dữ liệu bị khai thác vượt quá mục đích ban đầu hoặc bị sử dụng trái phép mà không được phát hiện kịp thời trong thực tiễn.

Pháp luật Việt Nam đã có bước hoàn thiện với việc ban hành Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15) và Nghị định 356/2025/NĐ-CP. Theo đó, trách nhiệm pháp lý của tổ chức xử lý dữ liệu đã được quy định rõ ràng hơn, đặc biệt là quy định về xử phạt, bồi thường thiệt hại và trách nhiệm pháp lý đối với hành

vi vi phạm tại khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, cũng như nghĩa vụ thông báo và xử lý vi phạm dữ liệu theo Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP.

Mặc dù đã có sự bổ sung, có thể nhận thấy rằng pháp luật hiện hành vẫn chưa giải quyết triệt để vấn đề thu thập và sử dụng dữ liệu cá nhân trái phép. Cụ thể, các quy định vẫn chưa thiết lập đầy đủ các nghĩa vụ mang tính phòng ngừa như cơ chế kiểm soát truy cập nội bộ bắt buộc, tiêu chuẩn quản lý dữ liệu cụ thể đối với doanh nghiệp hoặc cơ chế giám sát chặt chẽ việc chia sẻ dữ liệu cho bên thứ ba. Điều này cho thấy pháp luật mới chỉ chuyển từ việc quy định nguyên tắc sang tăng cường trách nhiệm pháp lý, nhưng vẫn chưa xây dựng được một cơ chế kiểm soát toàn diện đối với hoạt động xử lý dữ liệu cá nhân trong thực tiễn.

(3) Phân tích dấu hiệu vi phạm pháp luật

Từ các tình tiết của vụ việc, có thể xác định hành vi của các đối tượng và tổ chức liên quan đã có dấu hiệu vi phạm nghiêm trọng các quy định của pháp luật về bảo vệ dữ liệu cá nhân, đặc biệt trong hoạt động thu thập và sử dụng dữ liệu.

Trước hết, hành vi thu thập dữ liệu cá nhân với quy mô lớn mà không có sự đồng ý của chủ thể dữ liệu đã vi phạm nguyên tắc xử lý dữ liệu cá nhân theo quy định tại khoản 1 Điều 11 Nghị định 13/2023/NĐ-CP, theo đó việc xử lý dữ liệu phải dựa trên sự đồng ý của chủ thể dữ liệu. Đồng thời, việc thu thập dữ liệu không thông báo rõ mục đích hoặc vượt quá phạm vi cần thiết cũng vi phạm nguyên tắc xử lý đúng mục đích tại khoản 2 Điều 11 Nghị định này. Bên cạnh đó, việc sử dụng và chuyển giao dữ liệu cá nhân cho các bên khác nhằm mục đích thương mại hoặc phục vụ các hành vi lừa đảo là hành vi sử dụng dữ liệu sai mục đích, tiếp tục vi phạm nguyên tắc xử lý dữ liệu theo Điều 11 Nghị định 13/2023/NĐ-CP. Dưới góc độ pháp luật hiện hành, hành vi này cũng không bảo đảm các nguyên tắc về quản trị và sử dụng dữ liệu theo quy định tại Điều 5 Luật Dữ liệu 2024 (Luật số 60/2024/QH15), trong đó yêu cầu việc xử lý dữ liệu phải bảo đảm tính hợp pháp, đúng mục đích và an toàn, bảo mật.

Ngoài ra, việc để dữ liệu cá nhân bị thu thập, khai thác và mua bán trái phép với quy mô lớn cho thấy các tổ chức liên quan đã không thực hiện đầy đủ nghĩa vụ

bảo đảm an ninh, an toàn dữ liệu theo Điều 26 Nghị định 13/2023/NĐ-CP, cũng như không bảo đảm yêu cầu về bảo vệ dữ liệu theo nguyên tắc tại khoản 3 và khoản 4 Điều 5 Luật Dữ liệu 2024, bao gồm việc bảo đảm tính toàn vẹn, an ninh, an toàn và bảo vệ dữ liệu một cách chặt chẽ trong suốt quá trình xử lý. Đồng thời, việc không phát hiện và ngăn chặn kịp thời hành vi khai thác dữ liệu trái phép cũng cho thấy nghĩa vụ đánh giá và kiểm soát rủi ro theo Điều 24 Nghị định 13/2023/NĐ-CP chưa được thực hiện hiệu quả. Điều này phản ánh hạn chế trong cơ chế quản trị dữ liệu của tổ chức, đặc biệt trong việc kiểm soát truy cập nội bộ và giám sát việc sử dụng dữ liệu.

Từ góc độ pháp luật hình sự, hành vi thu thập, mua bán và sử dụng trái phép dữ liệu cá nhân với quy mô lớn, gây hậu quả nghiêm trọng, có dấu hiệu cấu thành tội "đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông" theo quy định tại Điều 288 Bộ luật Hình sự 2015 (sửa đổi, bổ sung 2017). Như vậy, hành vi trong vụ việc không chỉ vi phạm các quy định cụ thể của Nghị định 13/2023/NĐ-CP mà còn không bảo đảm các nguyên tắc quản trị dữ liệu theo Luật Dữ liệu 2024, đồng thời có dấu hiệu vi phạm pháp luật hình sự, cho thấy mức độ nguy hiểm cao và tính chất nghiêm trọng của hành vi thu thập và sử dụng dữ liệu cá nhân trái phép trong thực tiễn.

(4) Hậu quả pháp lý và xã hội của vụ việc

Vụ việc thu thập, mua bán dữ liệu cá nhân quy mô lớn không chỉ đặt ra vấn đề về vi phạm pháp luật mà còn kéo theo nhiều hậu quả nghiêm trọng trên cả phương diện pháp lý và xã hội.

Về mặt pháp lý, hành vi thu thập và sử dụng dữ liệu cá nhân trái phép đã xâm phạm trực tiếp đến quyền của chủ thể dữ liệu, đồng thời làm phát sinh trách nhiệm pháp lý đối với các cá nhân và tổ chức liên quan. Theo quy định tại khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, các hành vi vi phạm có thể bị xử phạt hành chính, buộc bồi thường thiệt hại và trong trường hợp nghiêm trọng có thể bị truy cứu trách nhiệm hình sự. Ngoài ra, đối với các hành vi có tổ chức, quy mô lớn và có mục đích trục lợi, các đối tượng liên quan có thể bị xử lý theo Điều 288 Bộ luật Hình sự 2015

(sửa đổi, bổ sung 2017) về tội "đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông".

Đối với doanh nghiệp, việc để xảy ra lộ, lọt và khai thác trái phép dữ liệu khách hàng không chỉ dẫn đến trách nhiệm pháp lý mà còn ảnh hưởng nghiêm trọng đến uy tín và hoạt động kinh doanh. Doanh nghiệp có thể phải chịu nghĩa vụ bồi thường thiệt hại cho khách hàng nếu chứng minh được thiệt hại thực tế, đồng thời có nguy cơ bị xử phạt hành chính theo quy định của pháp luật về bảo vệ dữ liệu cá nhân. Bên cạnh đó, theo các nguyên tắc quản trị dữ liệu tại Điều 5 Luật Dữ liệu 2024 (Luật số 60/2024/QH15), việc không bảo đảm an toàn, bảo mật dữ liệu còn cho thấy sự vi phạm trong hoạt động quản trị và khai thác dữ liệu của tổ chức.

Về mặt xã hội, hậu quả của vụ việc là đặc biệt nghiêm trọng khi dữ liệu cá nhân bị rò rỉ có thể bị lợi dụng để thực hiện các hành vi lừa đảo, giả mạo danh tính và chiếm đoạt tài sản. Theo cảnh báo của cơ quan chức năng, dữ liệu cá nhân sau khi bị lộ thường được sử dụng cho các hoạt động như gọi điện lừa đảo, giả mạo tổ chức tín dụng hoặc thực hiện các giao dịch tài chính trái phép. Điều này không chỉ gây thiệt hại trực tiếp cho người dân mà còn làm gia tăng nguy cơ mất an toàn trong không gian mạng. Ngoài ra, các vụ việc rò rỉ dữ liệu quy mô lớn còn làm suy giảm niềm tin của người dân đối với doanh nghiệp và hệ thống quản lý dữ liệu.

(5) So sánh với chuẩn pháp luật quốc tế

So với pháp luật Việt Nam, các chuẩn mực pháp lý quốc tế, đặc biệt là Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR), có mức độ hoàn thiện và tính ràng buộc cao hơn trong việc kiểm soát hoạt động thu thập và sử dụng dữ liệu cá nhân.

Về điều kiện thu thập và xử lý dữ liệu, GDPR quy định rất chặt chẽ về cơ sở pháp lý của việc xử lý dữ liệu, trong đó sự đồng ý của chủ thể dữ liệu phải được thể hiện rõ ràng, cụ thể và có thể chứng minh được (nguyên tắc "accountability"). Trong khi đó, pháp luật Việt Nam, mặc dù đã quy định về sự đồng ý tại Điều 11 và Điều 17 Nghị định 13/2023/NĐ-CP, nhưng chưa đặt ra yêu cầu cụ thể về việc chứng minh sự đồng ý hoặc cơ chế kiểm tra tính hợp lệ của sự đồng ý trong thực tiễn.

Về kiểm soát hoạt động sử dụng dữ liệu, GDPR thiết lập cơ chế quản lý chặt chẽ thông qua việc phân định rõ vai trò giữa "data controller" (bên kiểm soát dữ liệu) và "data processor" (bên xử lý dữ liệu), kèm theo nghĩa vụ pháp lý cụ thể đối với từng chủ thể. Ngoài ra, GDPR còn yêu cầu doanh nghiệp phải thực hiện đánh giá tác động bảo vệ dữ liệu (DPIA) đối với các hoạt động xử lý có rủi ro cao. Trong khi đó, pháp luật Việt Nam mới chỉ quy định về đánh giá tác động tại Điều 24 Nghị định 13/2023/NĐ-CP, nhưng chưa cụ thể hóa đầy đủ nội dung, quy trình và tiêu chí đánh giá, dẫn đến khó khăn trong áp dụng.

Về cơ chế bảo vệ và phòng ngừa rủi ro, GDPR yêu cầu doanh nghiệp phải áp dụng các biện pháp kỹ thuật và tổ chức phù hợp, bao gồm nguyên tắc "bảo vệ dữ liệu theo thiết kế và theo mặc định" (privacy by design & by default). Đây là cơ chế mang tính phòng ngừa, yêu cầu doanh nghiệp phải tích hợp bảo vệ dữ liệu ngay từ khi thiết kế hệ thống. Trong khi đó, pháp luật Việt Nam, dù đã có quy định về bảo đảm an toàn dữ liệu tại Điều 26 Nghị định 13/2023/NĐ-CP và nguyên tắc bảo vệ dữ liệu tại Điều 5 Luật Dữ liệu 2024, nhưng vẫn chưa quy định cụ thể các yêu cầu kỹ thuật bắt buộc hoặc tiêu chuẩn áp dụng.

Về chế tài xử lý vi phạm, GDPR có mức xử phạt rất nghiêm khắc, có thể lên tới 4% tổng doanh thu toàn cầu của doanh nghiệp hoặc 20 triệu euro[34], tùy theo mức nào cao hơn. Điều này tạo ra sức răn đe mạnh mẽ đối với các doanh nghiệp trong việc tuân thủ pháp luật. Ngược lại, pháp luật Việt Nam, mặc dù đã quy định về trách nhiệm pháp lý tại Khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, nhưng chưa có cơ chế xử phạt cụ thể và đủ mạnh để tương xứng với quy mô vi phạm trong các vụ việc lớn.

(6) Nhận xét và vấn đề đặt ra đối với pháp luật Việt Nam

Tại thời điểm xảy ra vụ việc (năm 2025), pháp luật Việt Nam về bảo vệ dữ liệu cá nhân chủ yếu được điều chỉnh bởi Nghị định 13/2023/NĐ-CP. Theo quy định này, hoạt động thu thập và sử dụng dữ liệu cá nhân của doanh nghiệp phải tuân thủ các nguyên tắc cơ bản, bao gồm việc phải có sự đồng ý của chủ thể dữ liệu và xử lý dữ liệu đúng mục đích theo khoản 1 và khoản 2 Điều 11, đồng thời phải bảo đảm an

[34] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), Article 83: "Infringements … shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher." https://eur-lex.europa.eu/eli/reg/2016/679/oj

ninh, an toàn dữ liệu theo Điều 26 và thực hiện đánh giá tác động xử lý dữ liệu theo Điều 24 Nghị định này. Nhìn chung, các quy định này đã bước đầu thiết lập khuôn khổ pháp lý nhằm kiểm soát hoạt động thu thập và sử dụng dữ liệu cá nhân của doanh nghiệp.

Từ thực tiễn vụ việc, các quy định pháp luật tại thời điểm này vẫn chưa giải quyết hiệu quả vấn đề thu thập và sử dụng dữ liệu cá nhân trái phép. Trước hết, các quy định trong Nghị định 13/2023/NĐ-CP còn mang tính nguyên tắc, chưa cụ thể hóa thành các nghĩa vụ mang tính bắt buộc đối với doanh nghiệp, đặc biệt trong việc kiểm soát truy cập nội bộ và giám sát hoạt động xử lý dữ liệu. Điều này dẫn đến việc doanh nghiệp có thể không thực hiện đầy đủ nghĩa vụ nhưng khó bị phát hiện trong thực tiễn. Cũng chưa quy định rõ trách nhiệm của doanh nghiệp trong trường hợp dữ liệu bị lạm dụng bởi nhân sự nội bộ hoặc bị chuyển giao cho bên thứ ba trái phép, dẫn đến khoảng trống trong việc xác định trách nhiệm pháp lý khi xảy ra vi phạm. Ngoài ra, nghĩa vụ đánh giá rủi ro theo Điều 24 Nghị định 13/2023/NĐ-CP cũng chưa được cụ thể hóa về tiêu chí, phương thức và tần suất thực hiện, khiến hiệu quả phòng ngừa rủi ro còn hạn chế.

Ngoài ra, một hạn chế khác là thiếu cơ chế giám sát và kiểm tra độc lập đối với hoạt động xử lý dữ liệu của doanh nghiệp. Pháp luật chủ yếu đặt ra nghĩa vụ tự tuân thủ, nhưng chưa có quy định cụ thể về kiểm toán dữ liệu, thanh tra định kỳ hoặc cơ chế giám sát bên ngoài, dẫn đến việc các hành vi vi phạm chỉ được phát hiện sau khi hậu quả đã xảy ra.

2.2.3. Chia sẻ/chuyển giao trái quy định về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

(1) Mô tả vụ việc: Công ty Cổ phần Tập đoàn VNG (Zalo) chia sẻ dữ liệu người dùng cho bên thứ ba.

Cuối năm 2025, ứng dụng Zalo đã gửi thông báo yêu cầu chủ tài khoản phải cập nhật điều khoản dịch vụ mới được tiếp tục sử dụng[35]. Trong đó có nhiều điều khoản đáng chú ý như: Zalo có quyền thu thập, chia sẻ dữ liệu cá nhân của người dùng, bao

[35] Giáo dục Thủ đô. (2025). *Zalo yêu cầu chia sẻ dữ liệu cá nhân, luật sư lo ngại sẽ tạo tiền lệ nguy hiểm*. https://giaoducthudo.giaoducthoidai.vn/zalo-yeu-cau-chia-se-du-lieu-ca-nhan-luat-su-lo-ngai-se-tao-tien-le-nguy-hiem-197118.html

gồm dữ liệu cơ bản (số điện thoại, họ và tên, giới tính, mối quan hệ gia đình, thông tin CCCD...) và dữ liệu cá nhân nhạy cảm. Nếu không đồng ý thỏa thuận, chủ tài khoản Zalo sẽ không được tiếp tục sử dụng, hệ thống sẽ tự động xóa tài khoản sau 45 ngày nếu người dùng không thay đổi quyết định. Người dùng đã phản đối các điều khoản này vì họ cho rằng, làm như vậy là vi phạm quyền dữ liệu riêng tư của người dùng. Điều này vấp phải phản ứng từ người dùng và Ủy ban Cạnh tranh Quốc gia (UBCQG) yêu cầu VNG phải rà soát, không được đặt người dùng vào thế "bắt buộc" chấp nhận, đồng thời bảo vệ quyền lợi người tiêu dùng theo Luật Bảo vệ dữ liệu cá nhân có hiệu lực từ 01/01/2026. UBCQG đã yêu cầu VNG không chuyển giao dữ liệu của những người đã đồng ý cho bên thứ ba và làm việc để đảm bảo sự tuân thủ pháp luật.

Việc áp dụng các điều khoản dịch vụ này đã gây ra nhiều tranh luận trong dư luận và cộng đồng người dùng, khi nhiều ý kiến cho rằng việc yêu cầu người dùng chấp nhận các điều khoản cho phép thu thập và chia sẻ dữ liệu cá nhân một cách rộng rãi có thể xâm phạm quyền riêng tư của người dùng. Trước phản ứng của dư luận, các cơ quan quản lý nhà nước đã tiến hành xem xét và yêu cầu doanh nghiệp rà soát lại các điều khoản liên quan đến việc xử lý dữ liệu cá nhân của người dùng nhằm bảo đảm tuân thủ quy định pháp luật.

(2) Nghĩa vụ pháp lý của doanh nghiệp trong việc chia sẻ dữ liệu cá nhân

Tại thời điểm trước khi các quy định mới có hiệu lực, hoạt động chia sẻ dữ liệu cá nhân của doanh nghiệp chủ yếu được điều chỉnh bởi Nghị định 13/2023/NĐ-CP. Theo đó, doanh nghiệp chỉ được phép chia sẻ dữ liệu cá nhân cho bên thứ ba khi có sự đồng ý của chủ thể dữ liệu theo khoản 1 Điều 11 và Điều 17, đồng thời phải bảo đảm việc sử dụng dữ liệu đúng mục đích theo khoản 2 Điều 11. Ngoài ra, doanh nghiệp có nghĩa vụ bảo đảm an ninh, an toàn dữ liệu theo Điều 26 và thực hiện đánh giá tác động xử lý dữ liệu theo Điều 24 Nghị định này.

Tuy nhiên, các quy định này bộc lộ nhiều bất cập trong thực tiễn. Thứ nhất, pháp luật chưa quy định rõ nghĩa vụ của doanh nghiệp trong việc kiểm soát dữ liệu sau khi đã chuyển giao cho bên thứ ba, dẫn đến tình trạng dữ liệu có thể tiếp tục bị sử dụng sai mục đích mà không xác định được trách nhiệm. Thứ hai, mặc dù có quy định

về sự đồng ý tại Điều 17, nhưng chưa làm rõ tính tự nguyện của sự đồng ý trong các trường hợp người dùng bị "buộc phải chấp nhận điều khoản" để sử dụng dịch vụ. Thứ ba, các quy định về bảo mật và đánh giá rủi ro tại Điều 26 và Điều 24 vẫn mang tính nguyên tắc, chưa thiết lập cơ chế giám sát và kiểm tra độc lập, dẫn đến hiệu quả kiểm soát còn hạn chế.

Sau đó, pháp luật Việt Nam đã có bước hoàn thiện với việc ban hành Luật Dữ liệu 2024 (Luật số 60/2024/QH15) và Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15) cùng với Nghị định 356/2025/NĐ-CP. Các văn bản này đã bổ sung theo hướng tăng cường quản trị và kiểm soát dữ liệu, trong đó nhấn mạnh nguyên tắc bảo đảm tính hợp pháp, minh bạch và an toàn trong hoạt động xử lý và chia sẻ dữ liệu theo Điều 5 Luật Dữ liệu 2024. Đồng thời, trách nhiệm pháp lý của doanh nghiệp trong trường hợp vi phạm cũng được quy định rõ hơn tại khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, cùng với nghĩa vụ thông báo và xử lý vi phạm dữ liệu theo Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP.

Dù đã có sự bổ sung, có thể thấy rằng pháp luật hiện hành vẫn chưa giải quyết triệt để các rủi ro phát sinh từ hoạt động chia sẻ dữ liệu cá nhân. Cụ thể, vẫn chưa có quy định rõ ràng về trách nhiệm liên đới giữa doanh nghiệp và bên thứ ba, cũng như chưa thiết lập cơ chế kiểm soát sau chuyển giao dữ liệu. Bên cạnh đó, các nguyên tắc quản trị dữ liệu theo Luật Dữ liệu 2024 mới dừng ở mức định hướng chung, chưa được cụ thể hóa thành các nghĩa vụ kỹ thuật và cơ chế thực thi bắt buộc trong hoạt động của doanh nghiệp.

(3) Phân tích dấu hiệu vi phạm nghĩa vụ bảo vệ dữ liệu cá nhân

Từ nội dung vụ việc, có thể nhận thấy hoạt động chia sẻ hoặc chuyển giao dữ liệu cá nhân của doanh nghiệp đã đặt ra nhiều dấu hiệu vi phạm nghĩa vụ pháp lý trong việc bảo vệ dữ liệu khách hàng, đặc biệt liên quan đến trách nhiệm kiểm soát dữ liệu khi cung cấp cho bên thứ ba.

Theo quy định tại khoản 1, Điều 11 và Điều 17, Nghị định 13/2023/NĐ-CP, việc chia sẻ dữ liệu cá nhân cho bên thứ ba phải dựa trên sự đồng ý hợp lệ của chủ thể dữ liệu. Tuy nhiên, trong trường hợp doanh nghiệp thiết lập cơ chế "chấp nhận điều khoản hoặc không được sử dụng dịch vụ", có thể đặt ra nghi vấn rằng sự đồng ý

này không bảo đảm tính tự nguyện. Dưới góc độ pháp luật hiện hành, vấn đề này tiếp tục được nhấn mạnh trong Luật Bảo vệ dữ liệu cá nhân 2025, khi yêu cầu việc xử lý dữ liệu phải bảo đảm tính hợp pháp và trách nhiệm của tổ chức theo khoản 1 Điều 8, qua đó củng cố yêu cầu về tính hợp lệ của sự đồng ý trong toàn bộ quá trình xử lý và chia sẻ dữ liệu.

Việc chia sẻ dữ liệu cho bên thứ ba nhưng không làm rõ phạm vi, mục đích và đối tượng nhận dữ liệu có thể vi phạm nguyên tắc xử lý đúng mục đích theo khoản 2 Điều 11 Nghị định 13/2023/NĐ-CP. Dưới góc độ pháp luật mới, hành vi này còn không phù hợp với các nguyên tắc quản trị dữ liệu theo Điều 5 Luật Dữ liệu 2024 (Luật số 60/2024/QH15), trong đó yêu cầu việc xử lý và khai thác dữ liệu phải bảo đảm tính minh bạch, hợp pháp và đúng mục đích.

Đặc biệt, dấu hiệu vi phạm rõ nét nhất nằm ở nghĩa vụ bảo vệ dữ liệu sau khi chuyển giao. Theo Điều 26 Nghị định 13/2023/NĐ-CP, doanh nghiệp phải bảo đảm an ninh, an toàn dữ liệu, bao gồm kiểm soát truy cập và ngăn chặn việc sử dụng trái phép. Tuy nhiên, nếu doanh nghiệp không thiết lập cơ chế kiểm soát đối với bên thứ ba sau khi dữ liệu được chia sẻ, thì việc chuyển giao dữ liệu có thể dẫn đến nguy cơ bị khai thác trái phép hoặc tiếp tục chuyển giao ngoài phạm vi kiểm soát. Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15) đã quy định trách nhiệm pháp lý của tổ chức xử lý dữ liệu tại khoản 1 Điều 8, nhưng các quy định này chủ yếu dừng ở việc xác định trách nhiệm khi có vi phạm, mà chưa thiết lập cơ chế kiểm soát cụ thể đối với hoạt động chia sẻ dữ liệu cho bên thứ ba.

Tương tư, theo Điều 12 Nghị định 356/2025/NĐ-CP, chủ thể dữ liệu có quyền yêu cầu hạn chế hoặc chấm dứt việc xử lý dữ liệu, bao gồm cả việc ngừng cung cấp dữ liệu cho bên thứ ba. Điều này gián tiếp đặt ra nghĩa vụ cho doanh nghiệp trong việc kiểm soát hoạt động xử lý dữ liệu sau khi đã chuyển giao. Tuy nhiên, các quy định này chủ yếu mang tính chất xử lý sau khi phát sinh vấn đề, mà chưa đặt ra các nghĩa vụ mang tính phòng ngừa như kiểm soát chặt chẽ việc sử dụng dữ liệu của bên thứ ba ngay từ thời điểm chuyển giao. Do đó, có thể thấy rằng, pháp luật hiện hành vẫn chưa thiết lập đầy đủ cơ chế kiểm soát đối với dữ liệu cá nhân sau khi được chia sẻ, cũng như chưa quy định rõ trách nhiệm liên đới giữa doanh nghiệp và bên thứ ba

nhận dữ liệu. Đây là khoảng trống pháp lý quan trọng, làm gia tăng nguy cơ dữ liệu bị sử dụng trái phép trong thực tiễn.

(4) Hậu quả pháp lý và xã hội của vụ việc

Hành vi chia sẻ hoặc chuyển giao dữ liệu cá nhân trái quy định không chỉ vi phạm nghĩa vụ pháp lý của doanh nghiệp mà còn gây ra những hậu quả nghiêm trọng trên cả phương diện pháp lý và xã hội.

Trước hết, về mặt pháp lý, việc chia sẻ dữ liệu cá nhân cho bên thứ ba không bảo đảm điều kiện hợp pháp có thể làm phát sinh trách nhiệm pháp lý đối với doanh nghiệp. Theo khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15), tổ chức vi phạm có thể bị xử phạt hành chính, buộc bồi thường thiệt hại, trong trường hợp nghiêm trọng có thể bị truy cứu trách nhiệm hình sự. Đối với trường hợp dữ liệu bị khai thác trái phép sau khi chuyển giao, việc không kiểm soát được bên thứ ba cũng có thể khiến doanh nghiệp phải chịu trách nhiệm liên quan đến hậu quả phát sinh.

Bên cạnh đó, theo Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP, khi xảy ra vi phạm dữ liệu, doanh nghiệp có nghĩa vụ thông báo, khắc phục hậu quả và phối hợp xử lý. Tuy nhiên, các nghĩa vụ này chủ yếu phát sinh sau khi vi phạm đã xảy ra, cho thấy rằng doanh nghiệp có thể phải đối mặt với các chi phí pháp lý, chi phí khắc phục và trách nhiệm bồi thường đáng kể nếu không kiểm soát tốt hoạt động chia sẻ dữ liệu ngay từ đầu.

Đối với doanh nghiệp, hậu quả không chỉ dừng lại ở trách nhiệm pháp lý mà còn ảnh hưởng trực tiếp đến uy tín và hoạt động kinh doanh. Việc để xảy ra tình trạng dữ liệu khách hàng bị chia sẻ hoặc khai thác trái phép có thể làm mất niềm tin của người dùng, ảnh hưởng đến khả năng duy trì và phát triển khách hàng trong dài hạn. Trong bối cảnh cạnh tranh số hiện nay, niềm tin vào khả năng bảo vệ dữ liệu cá nhân là yếu tố quan trọng đối với sự tồn tại của doanh nghiệp.

Về mặt xã hội, hậu quả của việc chia sẻ dữ liệu cá nhân trái phép là đặc biệt nghiêm trọng khi dữ liệu sau khi chuyển giao có thể tiếp tục bị khai thác cho nhiều mục đích khác nhau mà chủ thể dữ liệu không kiểm soát được. Dữ liệu cá nhân có thể bị sử dụng để thực hiện các hành vi lừa đảo, giả mạo danh tính, hoặc phục vụ các

hoạt động thương mại không mong muốn, gây thiệt hại trực tiếp cho người dân. Ngoài ra, việc thiếu kiểm soát trong hoạt động chia sẻ dữ liệu còn tạo ra nguy cơ lan truyền rủi ro trong toàn bộ hệ sinh thái số. Khi dữ liệu được chuyển giao qua nhiều bên khác nhau mà không có cơ chế kiểm soát chặt chẽ, nguy cơ rò rỉ và lạm dụng dữ liệu sẽ gia tăng theo cấp số nhân, làm suy giảm mức độ an toàn của môi trường số nói chung.

(5) So sánh với chuẩn pháp luật quốc tế

So với pháp luật quốc tế, cụ thể là Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR), pháp luật Việt Nam đã có bước phát triển đáng kể thông qua việc ban hành Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15) và Nghị định 356/2025/NĐ-CP, tuy nhiên vẫn còn tồn tại khoảng cách nhất định trong việc kiểm soát hoạt động chia sẻ và chuyển giao dữ liệu cá nhân.

Về điều kiện chia sẻ dữ liệu, GDPR yêu cầu sự đồng ý của chủ thể dữ liệu phải được thể hiện rõ ràng, cụ thể và có thể chứng minh được, đồng thời doanh nghiệp phải chịu trách nhiệm giải trình về tính hợp pháp của việc xử lý dữ liệu. Trong khi đó, pháp luật Việt Nam trước đây theo Nghị định 13/2023/NĐ-CP mới chỉ dừng lại ở việc quy định nguyên tắc phải có sự đồng ý tại khoản 1 Điều 11 và Điều 17, mà chưa đặt ra cơ chế kiểm chứng hoặc chứng minh sự đồng ý trong thực tiễn. Đến Luật Bảo vệ dữ liệu cá nhân 2025, mặc dù đã bổ sung trách nhiệm pháp lý của doanh nghiệp tại khoản 1 Điều 8, nhưng vẫn chưa quy định cụ thể cơ chế "trách nhiệm giải trình" tương tự GDPR.

Về trách nhiệm của doanh nghiệp đối với bên thứ ba, GDPR quy định rõ doanh nghiệp vẫn phải chịu trách nhiệm đối với dữ liệu cá nhân ngay cả sau khi chuyển giao, thông qua các cơ chế như hợp đồng xử lý dữ liệu và nghĩa vụ giám sát bên nhận dữ liệu. Trong khi đó, pháp luật Việt Nam, kể cả sau khi ban hành Luật 91/2025/QH15 và Nghị định 356/2025/NĐ-CP, vẫn chưa quy định rõ ràng trách nhiệm liên đới giữa doanh nghiệp và bên thứ ba nhận dữ liệu, dẫn đến khoảng trống trong việc kiểm soát sau chuyển giao.

Về cơ chế kiểm soát và giám sát dữ liệu, GDPR áp dụng cách tiếp cận quản lý toàn bộ vòng đời dữ liệu, bao gồm cả giai đoạn trước, trong và sau khi chuyển giao. Mặc dù Nghị định 356/2025/NĐ-CP đã bổ sung các quy định về xử lý vi phạm và

thực hiện quyền của chủ thể dữ liệu (như tại Điều 12, Điều 28 và Điều 29), nhưng các quy định này chủ yếu mang tính chất hậu kiểm, tức là xử lý sau khi phát sinh vi phạm, mà chưa thiết lập đầy đủ cơ chế kiểm soát chủ động đối với hoạt động chia sẻ dữ liệu ngay từ đầu.

Về chế tài xử lý vi phạm, GDPR có mức xử phạt rất nghiêm khắc, có thể lên tới 4% tổng doanh thu toàn cầu của doanh nghiệp, tạo ra sức răn đe mạnh mẽ. Trong khi đó, pháp luật Việt Nam, dù đã có bước tiến khi quy định rõ trách nhiệm pháp lý tại khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, nhưng vẫn chưa thiết lập cơ chế xử phạt cụ thể và đủ mạnh tương xứng với quy mô vi phạm trong các trường hợp chia sẻ dữ liệu quy mô lớn.

(6) Nhận xét và vấn đề đặt ra đối với pháp luật Việt Nam

Từ việc phân tích vụ việc và đối chiếu với các quy định pháp luật hiện hành, có thể nhận thấy rằng pháp luật Việt Nam về bảo vệ dữ liệu cá nhân đã có những bước phát triển đáng kể, đặc biệt với việc ban hành Luật Dữ liệu 2024 (Luật số 60/2024/QH15), Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15) và Nghị định 356/2025/NĐ-CP. Các văn bản này đã từng bước hoàn thiện khung pháp lý, chuyển từ việc quy định mang tính nguyên tắc sang việc xác lập rõ hơn trách nhiệm pháp lý của doanh nghiệp trong hoạt động xử lý và chia sẻ dữ liệu cá nhân.

Từ thực tiễn vụ việc, pháp luật Việt Nam vẫn chưa theo kịp yêu cầu kiểm soát hoạt động chia sẻ và chuyển giao dữ liệu cá nhân trong môi trường số. Trước hết, các quy định hiện hành vẫn chưa thiết lập đầy đủ cơ chế kiểm soát sau khi dữ liệu được chuyển giao cho bên thứ ba. Mặc dù pháp luật đã yêu cầu bảo đảm an toàn dữ liệu theo Điều 26 Nghị định 13/2023/NĐ-CP và bổ sung trách nhiệm pháp lý tại khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025, nhưng vẫn chưa quy định cụ thể về nghĩa vụ giám sát, kiểm tra hoặc kiểm soát việc sử dụng dữ liệu của bên nhận dữ liệu. Pháp luật hiện hành cũng chưa quy định rõ trách nhiệm liên đới giữa doanh nghiệp và bên thứ ba nhận dữ liệu, dẫn đến khó khăn trong việc xác định trách nhiệm khi dữ liệu bị lạm dụng hoặc tiếp tục bị chuyển giao trái phép. Điều này đặc biệt đáng chú ý trong bối cảnh dữ liệu cá nhân thường được chia sẻ qua nhiều chủ thể khác nhau trong hệ sinh thái số.

Tiếp đến, đối với cơ chế bảo đảm sự đồng ý của chủ thể dữ liệu vẫn chưa thực sự hiệu quả trong thực tiễn trong Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15) đã bổ sung quy định về trách nhiệm của tổ chức xử lý dữ liệu tại khoản 1 Điều 8, và Nghị định 356/2025/NĐ-CP cho phép chủ thể dữ liệu rút lại sự đồng ý theo Điều 12, nhưng các quy định này vẫn chưa làm rõ tiêu chí xác định tính tự nguyện của sự đồng ý, cũng như chưa xử lý triệt để các trường hợp "*chấp nhận hoặc không được sử dụng dịch vụ*". Ngoài ra, pháp luật Việt Nam hiện nay vẫn chủ yếu áp dụng cơ chế hậu kiểm, thể hiện qua các quy định về xử lý vi phạm tại Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP, mà chưa thiết lập đầy đủ các cơ chế kiểm soát mang tính phòng ngừa. Điều này dẫn đến việc các hành vi vi phạm thường chỉ được phát hiện sau khi hậu quả đã xảy ra, làm giảm hiệu quả bảo vệ dữ liệu cá nhân trong thực tiễn. Đồng thời, cần xem xét về hạn chế trong việc thiết lập các nguyên tắc quản trị dữ liệu hiện đại như trách nhiệm giải trình (accountability) và kiểm soát toàn bộ vòng đời dữ liệu, đặc biệt trong hoạt động chia sẻ dữ liệu cho bên thứ ba. Đây là những yếu tố quan trọng nhằm bảo đảm trách nhiệm của doanh nghiệp không chấm dứt sau khi dữ liệu được chuyển giao.

2.3. Đánh giá thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

2.3.1. Kết quả đạt được trong thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Trong những năm gần đây, cùng với sự phát triển mạnh mẽ của nền kinh tế số và quá trình chuyển đổi số quốc gia, vấn đề bảo vệ dữ liệu cá nhân ngày càng nhận được sự quan tâm của Nhà nước, doanh nghiệp và toàn xã hội. Thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng tại Việt Nam đã đạt được một số kết quả tích cực nhất định, thể hiện ở các khía cạnh sau:

Thứ nhất, hoạt động thanh tra, kiểm tra và xử lý vi phạm liên quan đến dữ liệu cá nhân ngày càng được tăng cường. Theo báo cáo của Bộ Công an, tình trạng mua bán và lộ lọt dữ liệu cá nhân tại Việt Nam diễn ra phổ biến, với hàng chục nghìn vụ việc được phát hiện mỗi năm, trong đó nhiều vụ liên quan đến rò rỉ dữ liệu quy mô

lớn trong các lĩnh vực tài chính, viễn thông và thương mại điện tử[36]. Trên cơ sở đó, các cơ quan chức năng đã tiến hành điều tra, xử lý nhiều đường dây mua bán dữ liệu cá nhân, góp phần răn đe và nâng cao hiệu quả thực thi pháp luật.

Thứ hai, cơ chế tiếp nhận và xử lý sự cố dữ liệu cá nhân đã từng bước được triển khai thông qua các cơ quan chuyên trách. Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) thường xuyên tiếp nhận và xử lý các sự cố an toàn thông tin, trong đó có nhiều vụ việc liên quan đến rò rỉ dữ liệu cá nhân. Khi xảy ra sự cố, các cơ quan chức năng tiến hành xác minh, cảnh báo và phối hợp với các đơn vị liên quan để xử lý, cho thấy pháp luật đã được áp dụng thông qua các quy trình nghiệp vụ cụ thể trong thực tiễn.

Thứ ba, khung pháp lý về bảo vệ dữ liệu cá nhân tại Việt Nam từng bước được hình thành và hoàn thiện. Trước đây, các quy định liên quan đến bảo vệ dữ liệu cá nhân được quy định rải rác trong nhiều văn bản pháp luật khác nhau như Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018, Bộ luật Dân sự năm 2015 và một số văn bản pháp luật chuyên ngành khác. Hiện nay, việc ban hành các văn bản pháp luật chuyên biệt như Luật Dữ liệu 2024 (Luật số 60/2024/QH15) và Luật Bảo vệ dữ liệu cá nhân 2025 (Luật số 91/2025/QH15), Nghị định 356/2025/NĐ-CP đã tạo ra khuôn khổ pháp lý rõ ràng hơn, buộc doanh nghiệp phải quan tâm đến nghĩa vụ bảo vệ dữ liệu cá nhân trong quá trình hoạt động. Trên thực tế, nhiều doanh nghiệp, đặc biệt trong các lĩnh vực tài chính, ngân hàng, viễn thông và thương mại điện tử, đã chủ động xây dựng chính sách nội bộ về bảo vệ dữ liệu cá nhân của khách hàng. Chẳng hạn, trong lĩnh vực ngân hàng, các tổ chức như Vietcombank, BIDV, Techcombank đều đã công bố công khai chính sách bảo mật thông tin khách hàng trên website chính thức, trong đó quy định rõ phạm vi thu thập dữ liệu, mục đích sử dụng, thời gian lưu trữ và trách nhiệm của các bộ phận liên quan trong việc bảo vệ dữ liệu. Trong lĩnh vực viễn thông, các doanh nghiệp như Viettel, VNPT, MobiFone cũng đã xây dựng các quy định nội bộ về quản lý và bảo vệ thông tin thuê bao, bao

[36] Hội thảo "Tuân thủ Luật Bảo vệ dữ liệu cá nhân: Thách thức, rủi ro và giải pháp công nghệ" cung cấp thông tin: Trong 6 tháng đầu năm 2025 đã có hơn 110 triệu bản ghi dữ liệu bị rao bán trái phép trên các diễn đàn không chính thống. Tình hình càng trở nên nghiêm trọng hơn trong quý 3 năm 2025, hơn 502 triệu bản ghi dữ liệu của các tổ chức, doanh nghiệp bị rò rỉ, trong khi số tài khoản cá nhân bị đánh cắp tăng 64% so với quý trước. Báo Công an Nhân dân. (2024). *Báo động thực trạng dữ liệu cá nhân bị lộ lọt, thiệt hại hàng nghìn tỷ đồng*. https://cand.com.vn/Cong-nghe/bao-dong-thuc-trang-du-lieu-ca-nhan-bi-lo-lot-thiet-hai-hang-ngan-ty-dong-i800138/

gồm cơ chế kiểm soát truy cập dữ liệu và quy trình xử lý khi có sự cố rò rỉ thông tin. Tương tự, trong lĩnh vực thương mại điện tử, các nền tảng lớn như Shopee, Lazada, Tiki đều ban hành chính sách bảo mật dữ liệu cá nhân, trong đó quy định rõ trách nhiệm của doanh nghiệp trong việc thu thập, xử lý và chia sẻ dữ liệu khách hàng, cũng như quyền của người dùng đối với dữ liệu của mình.

Thứ tư, hoạt động đào tạo, bồi dưỡng cán bộ, công chức liên quan đến bảo vệ dữ liệu cá nhân đã được triển khai thông qua một số chương trình cụ thể. Chẳng hạn, Bộ Thông tin và Truyền thông thông qua Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) thường xuyên tổ chức các chương trình diễn tập và tập huấn về ứng cứu sự cố an toàn thông tin mạng cho cán bộ các bộ, ngành và địa phương. Bộ Công an cũng triển khai các chương trình đào tạo liên quan đến phòng, chống tội phạm công nghệ cao và bảo vệ thông tin trong không gian mạng. Ngoài ra, trong khuôn khổ Chương trình chuyển đổi số quốc gia, nhiều hoạt động bồi dưỡng về quản trị dữ liệu và an toàn thông tin đã được tổ chức cho đội ngũ cán bộ quản lý nằm nâng cao kỹ năng quản lý trong lĩnh vực quản lý dữ liệu và bảo vệ dữ liệu.

Thứ năm, nhận thức của xã hội về quyền bảo vệ dữ liệu cá nhân từng bước được nâng cao. Cùng với sự phát triển của truyền thông và mạng xã hội, các vụ việc liên quan đến rò rỉ hoặc lạm dụng dữ liệu cá nhân ngày càng nhận được sự quan tâm của dư luận. Người tiêu dùng ngày càng chú ý hơn đến việc bảo vệ thông tin cá nhân của mình khi sử dụng các dịch vụ trực tuyến hoặc khi cung cấp dữ liệu cho các tổ chức, doanh nghiệp. Sự gia tăng nhận thức của người dân về quyền dữ liệu cá nhân góp phần tạo ra áp lực xã hội buộc các doanh nghiệp phải tuân thủ nghiêm túc hơn các quy định pháp luật về bảo vệ dữ liệu cá nhân.

Nhìn chung, những kết quả nêu trên cho thấy Việt Nam đã có những bước tiến quan trọng trong việc xây dựng và thực thi pháp luật về bảo vệ dữ liệu cá nhân. Mặc dù hệ thống pháp luật và cơ chế thực thi vẫn còn nhiều vấn đề cần tiếp tục hoàn thiện, song các kết quả đạt được trong thời gian qua đã tạo nền tảng quan trọng cho việc nâng cao trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng và thúc đẩy sự phát triển bền vững của nền kinh tế số tại Việt Nam.

2.3.2. Hạn chế, bất cập trong thực tiễn thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Mặc dù trong thời gian qua Việt Nam đã có nhiều nỗ lực trong việc xây dựng và thực thi các quy định pháp luật liên quan đến bảo vệ dữ liệu cá nhân, song thực tiễn áp dụng pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng vẫn còn tồn tại nhiều hạn chế và bất cập. Những hạn chế này không chỉ xuất phát từ sự chưa hoàn thiện của hệ thống pháp luật mà còn từ những khó khăn trong quá trình tổ chức thực thi và từ nhận thức cũng như năng lực quản trị dữ liệu của các doanh nghiệp.

Thứ nhất, quy định pháp luật còn mang tính nguyên tắc, thiếu cụ thể nên khó triển khai trong thực tiễn**.** Hiện nay, nhiều quy định về trách nhiệm bảo vệ dữ liệu cá nhân mới dừng ở mức nguyên tắc chung. Chẳng hạn, Điều 5 Luật Dữ liệu 2024 quy định về nguyên tắc bảo vệ, quản trị và sử dụng dữ liệu như bảo đảm an toàn, bảo mật, toàn vẹn dữ liệu; tuy nhiên, chưa cụ thể hóa thành các tiêu chuẩn kỹ thuật hoặc quy trình bắt buộc mà doanh nghiệp phải tuân thủ. Tương tự, khoản 1 Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025 quy định tổ chức, cá nhân vi phạm phải chịu trách nhiệm pháp lý, nhưng không quy định rõ tiêu chí xác định mức độ vi phạm tương ứng với từng loại nghĩa vụ cụ thể. Điều này dẫn đến thực tế là doanh nghiệp gặp khó khăn trong việc xác định mức độ tuân thủ, còn cơ quan nhà nước cũng thiếu căn cứ cụ thể để đánh giá hành vi vi phạm, làm giảm hiệu quả thực hiện pháp luật.

Thứ hai, cơ chế phòng ngừa rủi ro chưa được thiết lập đầy đủ, pháp luật vẫn thiên về hậu kiểm. Pháp luật hiện hành đã bước đầu quy định nghĩa vụ thông báo và xử lý sự cố dữ liệu tại Điều 28 và Điều 29 Nghị định 356/2025/NĐ-CP, theo đó doanh nghiệp phải thông báo vi phạm và thực hiện các biện pháp khắc phục. Tuy nhiên, các quy định này chủ yếu được áp dụng sau khi sự cố đã xảy ra, mà chưa đặt ra cơ chế phòng ngừa rủi ro mang tính bắt buộc trước đó, như đánh giá tác động xử lý dữ liệu hay kiểm toán hệ thống định kỳ. So với chuẩn quốc tế (GDPR), nơi yêu cầu đánh giá tác động dữ liệu (DPIA) đối với các hoạt động có rủi ro cao, pháp luật Việt Nam vẫn chưa thiết lập đầy đủ cơ chế kiểm soát rủi ro từ giai đoạn đầu. Điều này làm cho việc

thực hiện pháp luật trong thực tiễn còn mang tính phản ứng, chưa chủ động phòng ngừa vi phạm.

Thứ ba, chế tài xử lý vi phạm chưa đủ mạnh, chưa tương xứng với lợi ích kinh tế từ hành vi vi phạm. Hiện nay, chế tài xử phạt đối với hành vi vi phạm dữ liệu cá nhân chủ yếu là xử phạt hành chính với mức tối đa vài trăm triệu đồng theo các quy định xử phạt trong lĩnh vực công nghệ thông tin và an ninh mạng. Trong khi đó, theo Điều 83 GDPR, mức phạt có thể lên tới 20 triệu EUR hoặc 4% doanh thu toàn cầu của doanh nghiệp. Sự chênh lệch này dẫn đến thực tế là trong một số trường hợp, doanh nghiệp có thể coi việc vi phạm pháp luật về dữ liệu cá nhân như một "chi phí kinh doanh", làm giảm hiệu quả răn đe của pháp luật trong thực tiễn. Điều này cho thấy chế tài của Việt Nam chưa gắn với quy mô và năng lực tài chính của doanh nghiệp.

Thứ tư, cơ chế giám sát và kiểm tra việc tuân thủ còn hạn chế**.** Mặc dù pháp luật đã giao trách nhiệm cho các cơ quan quản lý trong việc giám sát và xử lý vi phạm, nhưng hiện chưa có quy định cụ thể về cơ chế kiểm tra định kỳ, kiểm toán dữ liệu hoặc giám sát độc lập đối với các hệ thống xử lý dữ liệu của doanh nghiệp. Các quy định tại Nghị định 356/2025/NĐ-CP chủ yếu tập trung vào nghĩa vụ báo cáo và xử lý khi có vi phạm, mà chưa thiết lập cơ chế giám sát thường xuyên. Điều này dẫn đến việc phát hiện vi phạm trong thực tế thường phụ thuộc vào sự cố xảy ra hoặc phản ánh từ bên ngoài, thay vì được kiểm soát một cách chủ động.

Thứ năm, thiếu hệ thống thống kê và công bố dữ liệu vi phạm, làm hạn chế hiệu quả thực hiện pháp luật**.** Hiện nay, pháp luật chưa quy định rõ trách nhiệm xây dựng và công bố cơ sở dữ liệu quốc gia về vi phạm dữ liệu cá nhân, dẫn đến tình trạng thiếu thông tin chính thức về số lượng, quy mô và mức độ các vụ vi phạm.
Điều này không chỉ gây khó khăn cho việc đánh giá hiệu quả thực thi pháp luật, mà còn hạn chế khả năng xây dựng chính sách phù hợp trong lĩnh vực bảo vệ dữ liệu cá nhân. Trong khi đó, tại nhiều quốc gia, cơ quan quản lý có nghĩa vụ công bố các vụ vi phạm dữ liệu lớn, góp phần nâng cao tính minh bạch và trách nhiệm giải trình.

Từ những phân tích trên, có thể thấy rằng hạn chế cốt lõi của pháp luật Việt Nam trong thực tiễn hiện nay nằm ở việc chưa chuyển hóa đầy đủ các quy định mang

tính nguyên tắc thành cơ chế thực thi cụ thể, có khả năng kiểm soát rủi ro và ràng buộc trách nhiệm của doanh nghiệp trong toàn bộ quá trình xử lý dữ liệu cá nhân.

2.3.3. Nguyên nhân và vấn đề đặt ra

Những hạn chế trong thực tiễn thực hiện pháp luật về bảo vệ dữ liệu cá nhân tại Việt Nam không chỉ là vấn đề của quá trình triển khai mà còn phản ánh những nguyên nhân sâu xa từ cách tiếp cận lập pháp, điều kiện phát triển kinh tế – xã hội và năng lực quản lý nhà nước trong lĩnh vực này.

Trước hết, nguyên nhân xuất phát từ việc pháp luật về bảo vệ dữ liệu cá nhân tại Việt Nam còn ở giai đoạn phát triển ban đầu, chưa có sự tích lũy đầy đủ về lý luận và thực tiễn. Việc ban hành Luật Dữ liệu 2024 và Luật Bảo vệ dữ liệu cá nhân 2025 diễn ra trong bối cảnh nhu cầu điều chỉnh phát sinh nhanh chóng từ thực tiễn chuyển đổi số, dẫn đến việc nhiều quy định mang tính định hướng, chưa có điều kiện kiểm nghiệm và hoàn thiện qua thực tiễn áp dụng.

Thứ hai, đặc điểm của nền kinh tế số tại Việt Nam đang phát triển nhanh nhưng chưa đồng bộ về quản trị dữ liệu. Doanh nghiệp, đặc biệt là doanh nghiệp vừa và nhỏ, thường ưu tiên mục tiêu khai thác dữ liệu phục vụ kinh doanh hơn là đầu tư vào hệ thống bảo vệ dữ liệu. Điều này tạo ra khoảng cách giữa yêu cầu pháp lý và khả năng thực hiện trên thực tế, khiến việc tuân thủ pháp luật mang tính hình thức hoặc chưa đầy đủ.

Thứ ba, từ sự phức tạp và tính liên ngành của vấn đề dữ liệu cá nhân. Việc bảo vệ dữ liệu không chỉ liên quan đến pháp luật mà còn gắn chặt với yếu tố kỹ thuật, công nghệ và quản trị hệ thống. Trong khi đó, hệ thống pháp luật hiện hành và cơ chế tổ chức thực thi chưa thực sự tích hợp hiệu quả giữa các yếu tố này, dẫn đến khó khăn trong việc chuyển hóa quy định pháp luật thành các biện pháp cụ thể trong thực tiễn.

Thứ tư, hạn chế về nguồn nhân lực chuyên môn trong lĩnh vực bảo vệ dữ liệu cá nhân. Đội ngũ cán bộ, công chức thực thi pháp luật hiện nay chủ yếu được đào tạo theo hướng an ninh mạng hoặc công nghệ thông tin, trong khi các kiến thức chuyên sâu về pháp lý dữ liệu và trách nhiệm pháp lý của doanh nghiệp chưa được trang bị đầy đủ. Điều này ảnh hưởng trực tiếp đến hiệu quả áp dụng và thực hiện pháp luật trong các vụ việc cụ thể.

Thứ năm, nguyên nhân từ việc thiếu cơ chế thúc đẩy tuân thủ và trách nhiệm giải trình của doanh nghiệp. Trong bối cảnh chế tài chưa đủ mạnh và cơ chế giám sát chưa chặt chẽ, doanh nghiệp có xu hướng đánh giá thấp rủi ro pháp lý trong lĩnh vực dữ liệu cá nhân. Điều này làm giảm động lực tuân thủ và khiến pháp luật chưa phát huy đầy đủ vai trò điều chỉnh hành vi trong thực tiễn.

TIỂU KẾT CHƯƠNG 2

Chương 2 đã phân tích thực trạng pháp luật và thực tiễn thực hiện trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng tại Việt Nam và phân tích một số vụ việc điển hình phản ánh các dạng vi phạm phổ biến hiện nay, gồm: vi phạm nghĩa vụ bảo mật, thu thập và sử dụng trái phép dữ liệu cá nhân, cũng như chia sẻ, chuyển giao dữ liệu trái quy định. Việc lựa chọn và phân tích các tình huống này cho thấy trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân không phải là vấn đề lý thuyết thuần túy, mà đã và đang đặt ra những hệ quả pháp lý, kinh tế và xã hội rất cụ thể trong thực tiễn. Đồng thời, thông qua từng vụ việc, Chương 2 cũng chỉ ra rằng khoảng cách giữa quy định pháp luật và khả năng kiểm soát hành vi vi phạm trên thực tế vẫn còn đáng kể.

Qua phân tích cho thấy, pháp luật hiện hành đã từng bước hình thành khung điều chỉnh tương đối đầy đủ, đồng thời thực tiễn cũng ghi nhận những chuyển biến tích cực trong việc tuân thủ của doanh nghiệp và hoạt động áp dụng pháp luật của cơ quan nhà nước. Tuy nhiên, vẫn còn tồn tại nhiều hạn chế như quy định chưa cụ thể, cơ chế thực thi còn thiên về hậu kiểm và hiệu quả răn đe chưa cao. Những bất cập này xuất phát từ nhiều nguyên nhân khác nhau, đặt ra yêu cầu tiếp tục hoàn thiện pháp luật và nâng cao hiệu quả thực hiện trong thời gian tới. Đây cũng chính là cơ sở để Chương 3 đề xuất các giải pháp hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng.

CHƯƠNG 3. ĐỊNH HƯỚNG, KIẾN NGHỊ HOÀN THIỆN PHÁP LUẬT VÀ NÂNG CAO HIỆU QUẢ THỰC HIỆN TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA KHÁCH HÀNG

3.1. Định hướng hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Trong bối cảnh dữ liệu cá nhân trở thành nguồn lực quan trọng trong hoạt động kinh doanh và chuyển đổi số diễn ra mạnh mẽ, việc hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng cần được thực hiện theo những định hướng cơ bản sau:

Thứ nhất, trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng cần đặt trong tổng thể đường lối, chủ trương của Đảng và chính sách, pháp luật của Nhà nước về chuyển đổi số và bảo vệ quyền con người. Cụ thể, theo Văn kiện Đại hội đại biểu toàn quốc lần thứ XIV của Đảng, phát triển kinh tế số và kinh tế tư nhân được xác định là động lực quan trọng của nền kinh tế, đồng thời phải gắn với bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân. Đặc biệt, Nghị quyết số 68-NQ/TW ngày 04/5/2025 của Bộ Chính trị về phát triển kinh tế tư nhân đã nhấn mạnh yêu cầu xây dựng môi trường kinh doanh minh bạch, nâng cao trách nhiệm tuân thủ pháp luật của doanh nghiệp.

Về phía Nhà nước, hệ thống pháp luật về bảo vệ dữ liệu cá nhân ngày càng được hoàn thiện theo hướng chuyên biệt và thống nhất hơn. Bên cạnh các quy định nền tảng như Bộ luật Dân sự năm 2015, Luật An ninh mạng năm 2018 và Luật Bảo vệ quyền lợi người tiêu dùng năm 2023, khung pháp lý chuyên ngành đã được xác lập rõ nét với việc ban hành Luật Dữ liệu năm 2024 (Luật số 60/2024/QH15) và Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15). Đặc biệt, Nghị định số 356/2025/NĐ-CP, có hiệu lực từ ngày 01/01/2026, đã quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân, góp phần cụ thể hóa trách nhiệm của tổ chức, doanh nghiệp trong toàn bộ quá trình xử lý dữ liệu. Các quy định này thể hiện rõ định hướng của Nhà nước trong việc cân bằng giữa phát triển kinh tế số và bảo vệ quyền riêng tư của cá nhân, đồng thời đặt ra yêu cầu ngày càng cao đối với trách nhiệm của doanh nghiệp trong hoạt động xử lý dữ liệu.

Thứ hai, hoàn thiện pháp luật cần bảo đảm lấy quyền và lợi ích hợp pháp của chủ thể dữ liệu làm trung tâm, đồng thời xác lập rõ trách nhiệm pháp lý của doanh nghiệp trong toàn bộ vòng đời xử lý dữ liệu. Theo đó, pháp luật cần cụ thể hóa các quyền cơ bản của chủ thể dữ liệu như quyền được biết, quyền đồng ý, quyền truy cập, chỉnh sửa và xóa dữ liệu, bảo đảm các quyền này được thực thi thực chất trong thực tiễn. Tương ứng, trách nhiệm của doanh nghiệp phải được quy định rõ trong từng giai đoạn xử lý dữ liệu, từ thu thập, lưu trữ, sử dụng đến chia sẻ và chuyển giao, gắn với yêu cầu bảo đảm tính hợp pháp, minh bạch và an toàn dữ liệu. Đồng thời, cần tăng cường cơ chế trách nhiệm giải trình, buộc doanh nghiệp không chỉ tuân thủ mà còn phải chứng minh việc tuân thủ thông qua hệ thống quản trị nội bộ và kiểm soát rủi ro. Định hướng này góp phần nâng cao tính minh bạch, phòng ngừa vi phạm và bảo đảm hiệu quả bảo vệ quyền riêng tư trong môi trường số.

Thứ ba, pháp luật cần được hoàn thiện theo hướng tăng cường trách nhiệm giải trình của doanh nghiệp trong hoạt động xử lý dữ liệu cá nhân. Theo đó, doanh nghiệp không chỉ dừng lại ở nghĩa vụ tuân thủ các quy định về bảo vệ dữ liệu cá nhân, mà còn phải có nghĩa vụ chứng minh việc tuân thủ trong suốt quá trình xử lý dữ liệu. Điều này đòi hỏi pháp luật cần quy định rõ trách nhiệm của doanh nghiệp trong việc thiết lập và vận hành hệ thống quản trị dữ liệu nội bộ, bao gồm xây dựng chính sách bảo vệ dữ liệu, phân định rõ trách nhiệm giữa các bộ phận, cũng như thiết lập quy trình kiểm soát truy cập và sử dụng dữ liệu. Bên cạnh đó, doanh nghiệp cần thực hiện các biện pháp kiểm soát rủi ro như đánh giá định kỳ các hoạt động xử lý dữ liệu, phát hiện và xử lý kịp thời các nguy cơ vi phạm. Đồng thời, việc thiết lập hệ thống lưu vết (log) và ghi nhận toàn bộ hoạt động xử lý dữ liệu là yêu cầu quan trọng nhằm bảo đảm khả năng truy xuất, kiểm tra và phục vụ hoạt động thanh tra, kiểm tra của cơ quan nhà nước. Việc tăng cường trách nhiệm giải trình theo hướng này không chỉ nâng cao tính minh bạch và kỷ luật trong hoạt động của doanh nghiệp, mà còn tạo cơ sở pháp lý vững chắc cho việc xác định trách nhiệm khi xảy ra vi phạm, qua đó góp phần nâng cao hiệu quả thực thi pháp luật về bảo vệ dữ liệu cá nhân trong thực tiễn.

Thứ tư, việc hoàn thiện pháp luật cần bảo đảm tính đồng bộ, thống nhất và khả thi của hệ thống quy định về bảo vệ dữ liệu cá nhân. Hiện nay, các quy định còn phân

tán và thiếu thống nhất, gây khó khăn trong áp dụng. Do đó, cần rà soát, hệ thống hóa các văn bản liên quan, bảo đảm sự thống nhất giữa pháp luật về dữ liệu với các lĩnh vực như dân sự, an ninh mạng và thương mại điện tử, đồng thời cụ thể hóa các quy định để nâng cao tính khả thi. Bên cạnh đó, việc hoàn thiện pháp luật cần hướng tới xây dựng một hành lang pháp lý minh bạch, ổn định, cho phép doanh nghiệp khai thác và sử dụng dữ liệu cá nhân một cách hợp pháp phục vụ hoạt động kinh doanh. Theo đó, cần xác định rõ phạm vi, điều kiện và giới hạn của việc xử lý dữ liệu, bảo đảm doanh nghiệp có cơ sở pháp lý để triển khai các mô hình kinh doanh dựa trên dữ liệu, nhưng không làm suy giảm mức độ bảo vệ quyền riêng tư của cá nhân.

Thứ năm, hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân trong hoạt động kinh doanh cần gắn với xu thế hội nhập quốc tế và sự phát triển của kinh tế số. Trong bối cảnh các hoạt động xử lý dữ liệu ngày càng mang tính xuyên biên giới, pháp luật Việt Nam cần được xây dựng theo hướng tiệm cận các chuẩn mực quốc tế về bảo vệ dữ liệu cá nhân, nhằm tạo điều kiện cho doanh nghiệp tham gia vào thị trường toàn cầu. Đồng thời, pháp luật cần quy định rõ cơ chế đối với việc chuyển dữ liệu ra nước ngoài, bảo đảm vừa thuận lợi cho hoạt động kinh doanh, vừa kiểm soát được rủi ro đối với quyền riêng tư của cá nhân. Bên cạnh đó, sự phát triển nhanh của các mô hình kinh doanh dựa trên dữ liệu như thương mại điện tử, nền tảng số hay trí tuệ nhân tạo đặt ra yêu cầu pháp luật phải có tính linh hoạt nhất định. Theo đó, các quy định cần được thiết kế theo hướng vừa bảo đảm tính ổn định, vừa có khả năng thích ứng với sự thay đổi của công nghệ và mô hình kinh doanh, tránh tình trạng lạc hậu hoặc không theo kịp thực tiễn. Như vậy, việc hoàn thiện pháp luật theo định hướng này không chỉ góp phần nâng cao năng lực cạnh tranh của doanh nghiệp Việt Nam trong hội nhập quốc tế, mà còn bảo đảm hiệu quả bảo vệ dữ liệu cá nhân trong bối cảnh kinh tế số phát triển mạnh mẽ.

3.2. Kiến nghị hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Để làm rõ và nâng cao hiệu lực điều chỉnh của pháp luật đối với trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, cần tập trung vào các giải pháp hoàn thiện pháp luật theo các nhóm nội dung sau:

3.2.1. Hoàn thiện, pháp luật cần bổ sung các quy định cụ thể về trách nhiệm giải trình của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Trên cơ sở những hạn chế đã được phân tích tại Chương 2, một trong những yêu cầu quan trọng đặt ra là cần hoàn thiện pháp luật theo hướng tăng cường và cụ thể hóa trách nhiệm giải trình của doanh nghiệp trong hoạt động xử lý dữ liệu cá nhân. Việc hoàn thiện cần được thực hiện theo trình tự từ luật đến văn bản dưới luật nhằm bảo đảm tính thống nhất và hiệu lực thi hành.

Thứ nhất, cần bổ sung và làm rõ nội hàm của trách nhiệm giải trình trong các văn bản như Luật Dữ liệu năm 2024 và Luật Bảo vệ dữ liệu cá nhân năm 2025. Theo đó, pháp luật cần quy định rõ doanh nghiệp không chỉ có nghĩa vụ tuân thủ các quy định về bảo vệ dữ liệu cá nhân mà còn phải chủ động chứng minh việc tuân thủ. Nội dung này cần được cụ thể hóa thành các nghĩa vụ pháp lý cơ bản như: xây dựng và duy trì hệ thống quản trị dữ liệu nội bộ; ban hành chính sách bảo vệ dữ liệu cá nhân; phân công rõ trách nhiệm của từng bộ phận và cá nhân trong doanh nghiệp đối với hoạt động xử lý dữ liệu. Đồng thời, luật cần ghi nhận nghĩa vụ của doanh nghiệp trong việc thiết lập cơ chế kiểm soát nội bộ và quản trị rủi ro đối với các hoạt động xử lý dữ liệu, coi đây là một tiêu chí bắt buộc để đánh giá mức độ tuân thủ pháp luật.

Thứ hai, cần sửa đổi, bổ sung Điều 8 Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15) theo hướng bổ sung nghĩa vụ của doanh nghiệp trong việc lưu trữ và cung cấp chứng cứ tuân thủ. Theo đó, doanh nghiệp phải có trách nhiệm ghi nhận và lưu vết toàn bộ quá trình xử lý dữ liệu cá nhân, bao gồm thông tin về mục đích xử lý, phạm vi sử dụng, chủ thể truy cập và thời gian xử lý, nhằm bảo đảm khả năng kiểm tra, giám sát của cơ quan nhà nước và nghiên cứu bổ sung một điều mới (Điều 8a) về trách nhiệm giải trình của bên kiểm soát và xử lý dữ liệu, quy định rõ nghĩa vụ lưu trữ hồ sơ xử lý dữ liệu, cung cấp tài liệu chứng minh việc tuân thủ khi có yêu cầu, cũng như nghĩa vụ báo cáo, giải trình trong trường hợp xảy ra sự cố dữ liệu cá nhân.

Thứ ba, Nghị định 356/2025/NĐ-CP cần được hoàn thiện theo hướng bổ sung các quy định chi tiết về trách nhiệm giải trình của doanh nghiệp. Cụ thể, có thể bổ sung một điều khoản riêng về quy định về nội dung và tiêu chí thực hiện trách nhiệm

giải trình, bao gồm: yêu cầu doanh nghiệp thiết lập hệ thống quản trị dữ liệu nội bộ; quy trình kiểm soát truy cập và sử dụng dữ liệu; nghĩa vụ thực hiện đánh giá rủi ro và kiểm toán dữ liệu định kỳ. Nghị định cũng cần quy định rõ nghĩa vụ lưu trữ hồ sơ xử lý dữ liệu (records of processing), bao gồm thông tin về mục đích xử lý, loại dữ liệu, chủ thể truy cập và thời gian xử lý; đồng thời hướng dẫn cụ thể về hình thức, thời hạn lưu trữ và trách nhiệm cung cấp các tài liệu này cho cơ quan có thẩm quyền khi có yêu cầu. Ngoài ra, cần bổ sung quy định về nghĩa vụ báo cáo và giải **trình** trong trường hợp xảy ra sự cố dữ liệu, coi đây là căn cứ để đánh giá mức độ tuân thủ và xác định trách nhiệm pháp lý của doanh nghiệp. Việc cụ thể hóa các nội dung này tại cấp nghị định sẽ góp phần bảo đảm tính khả thi của các quy định tại luật, đồng thời tạo cơ sở pháp lý rõ ràng cho hoạt động kiểm tra, giám sát và xử lý vi phạm trong thực tiễn.

3.2.2. Hoàn thiện cơ chế giám sát và thực thi pháp luật về bảo vệ dữ liệu cá nhân của khách hàng

Trước hết, ở cấp độ luật, cần tiếp tục hoàn thiện Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15) theo hướng bổ sung các quy định cụ thể về cơ chế giám sát. Theo đó, cần quy định rõ hơn thẩm quyền, trách nhiệm và cơ chế phối hợp giữa các cơ quan quản lý nhà nước trong lĩnh vực này, đặc biệt giữa Bộ Công an, Bộ Thông tin và Truyền thông và các cơ quan quản lý chuyên ngành. Đồng thời, cần bổ sung quy định về cơ chế giám sát thường xuyên đối với các doanh nghiệp có hoạt động xử lý dữ liệu quy mô lớn, coi đây là đối tượng trọng điểm cần kiểm soát. Bên cạnh đó, cần bổ sung vào luật quy định về nghĩa vụ đăng ký hoặc thông báo hoạt động xử lý dữ liệu cá nhân đối với một số loại hình doanh nghiệp hoặc hoạt động có rủi ro cao. Cơ chế này sẽ giúp cơ quan nhà nước chủ động nắm bắt, theo dõi và giám sát các hoạt động xử lý dữ liệu ngay từ đầu, thay vì chỉ can thiệp khi đã xảy ra vi phạm.

Trên cơ sở các quy định mang tính nguyên tắc tại luật, tiếp tục hoàn thiện Nghị định 356/2025/NĐ-CP theo hướng cụ thể hóa cơ chế giám sát và thực thi. Cụ thể, cần bổ sung một điều khoản riêng quy định về hoạt động thanh tra, kiểm tra trong lĩnh vực bảo vệ dữ liệu cá nhân, trong đó xác định rõ:

- Tiêu chí lựa chọn đối tượng kiểm tra (doanh nghiệp xử lý dữ liệu lớn, dữ liệu nhạy cảm);
- Tần suất kiểm tra định kỳ và kiểm tra đột xuất;
- Quy trình kiểm tra, bao gồm việc yêu cầu cung cấp hồ sơ xử lý dữ liệu và tài liệu chứng minh tuân thủ.

Đồng thời, cần quy định cụ thể cơ chế tiếp nhận và xử lý phản ánh, khiếu nại của cá nhân liên quan đến vi phạm dữ liệu cá nhân, bảo đảm quyền của chủ thể dữ liệu được bảo vệ một cách hiệu quả. Việc thiết lập kênh tiếp nhận thông tin từ người dân không chỉ góp phần phát hiện vi phạm kịp thời mà còn tăng cường giám sát xã hội đối với hoạt động của doanh nghiệp. Ngoài ra, cần hoàn thiện quy định về công bố thông tin và minh bạch hóa vi phạm, theo đó cơ quan có thẩm quyền có thể công khai các vụ việc vi phạm nghiêm trọng về dữ liệu cá nhân. Đây là biện pháp có tác dụng răn đe mạnh mẽ, đồng thời nâng cao trách nhiệm tuân thủ của doanh nghiệp.

3.2.3. Hoàn thiện quy định về tổ chức thực hiện và kỹ thuật của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Cần bổ sung và cụ thể hóa trong Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15) các quy định về tổ chức thực hiện trong nội bộ doanh nghiệp. Theo đó, cần quy định rõ nghĩa vụ của doanh nghiệp trong việc thiết lập bộ máy quản lý dữ liệu, bao gồm việc chỉ định bộ phận hoặc cá nhân phụ trách bảo vệ dữ liệu cá nhân, chịu trách nhiệm tổ chức thực hiện, kiểm tra và giám sát việc tuân thủ pháp luật trong doanh nghiệp. Đồng thời, cần quy định trách nhiệm của người đứng đầu doanh nghiệp trong việc bảo đảm thực hiện các nghĩa vụ bảo vệ dữ liệu, qua đó nâng cao tính chịu trách nhiệm trong quản trị.

Quy định cụ thể nghĩa vụ của doanh nghiệp trong việc xây dựng và vận hành quy trình nội bộ về xử lý dữ liệu cá nhân, bao gồm quy trình thu thập, lưu trữ, sử dụng, chia sẻ và xử lý khi có sự cố. Các quy trình này phải được chuẩn hóa, công khai trong nội bộ và thường xuyên rà soát, cập nhật nhằm phù hợp với sự thay đổi của công nghệ và hoạt động kinh doanh.

Về mặt kỹ thuật, cần bổ sung các quy định yêu cầu doanh nghiệp áp dụng các biện pháp bảo mật tối thiểu đối với dữ liệu cá nhân. Cụ thể, có thể quy định tại cấp luật nguyên tắc bắt buộc về:

- Mã hóa dữ liệu cá nhân quan trọng hoặc dữ liệu nhạy cảm;
- Phân quyền truy cập theo chức năng, nhiệm vụ;
- Kiểm soát và ghi nhận hoạt động truy cập dữ liệu;
- Phát hiện và cảnh báo truy cập trái phép.

Trên cơ sở đó, ở cấp độ nghị định, cần cụ thể hóa các yêu cầu kỹ thuật này trong Nghị định 356/2025/NĐ-CP bằng việc bổ sung một điều khoản riêng quy định về tiêu chuẩn kỹ thuật trong bảo vệ dữ liệu cá nhân. Theo đó, nghị định cần hướng dẫn chi tiết về các biện pháp bảo mật phù hợp với từng loại dữ liệu và quy mô xử lý dữ liệu của doanh nghiệp, tránh áp dụng một cách cứng nhắc cho mọi đối tượng.

3.2.4. Hoàn thiện quy định về quản trị dữ liệu và hệ thống bảo mật thông tin của nhiều doanh nghiệp

Cần bổ sung và cụ thể hóa trong Luật Dữ liệu năm 2024 (Luật số 60/2024/QH15) các quy định về quản trị dữ liệu trong doanh nghiệp. Theo đó, cần xác lập nguyên tắc doanh nghiệp phải xây dựng hệ thống quản trị dữ liệu theo hướng có kiểm soát, bao gồm phân loại dữ liệu, xác định rõ mục đích xử lý và kiểm soát vòng đời dữ liệu. Đồng thời, pháp luật cần quy định rõ trách nhiệm của doanh nghiệp trong việc thiết lập cơ chế quản lý tập trung, tránh tình trạng dữ liệu bị phân tán, khó kiểm soát trong nội bộ.

Quy định về phân loại dữ liệu cá nhân theo mức độ rủi ro, đặc biệt đối với dữ liệu nhạy cảm, từ đó làm cơ sở áp dụng các biện pháp bảo vệ tương ứng. Việc phân loại dữ liệu không chỉ giúp doanh nghiệp ưu tiên nguồn lực bảo vệ mà còn tạo điều kiện cho cơ quan nhà nước trong việc giám sát và đánh giá mức độ tuân thủ.

Về hệ thống bảo mật thông tin, pháp luật cần quy định rõ yêu cầu doanh nghiệp phải thiết lập hệ thống bảo mật theo nhiều lớp (multi-layer security), bao gồm bảo mật hạ tầng, ứng dụng và dữ liệu. Đồng thời, cần xác định rõ các nguyên tắc cơ bản như bảo mật ngay từ thiết kế (security by design), bảo mật theo mặc định (security by default) và kiểm soát truy cập dựa trên vai trò (role-based access control).

Đối với Nghị định 356/2025/NĐ-CP cần bổ sung một điều khoản riêng quy định về quản trị dữ liệu và bảo mật thông tin. Theo đó, nghị định cần hướng dẫn cụ thể:

- Tiêu chí xây dựng hệ thống quản trị dữ liệu;
- Yêu cầu phân loại dữ liệu và xác định mức độ bảo vệ tương ứng;
- Tiêu chuẩn tối thiểu về bảo mật hệ thống thông tin;
- Quy trình kiểm tra, đánh giá và nâng cấp hệ thống bảo mật.

Ngoài ra, cần quy định nghĩa vụ của doanh nghiệp trong việc đánh giá định kỳ hệ thống bảo mật, kiểm tra lỗ hổng và thực hiện các biện pháp khắc phục kịp thời. Đồng thời, cần khuyến khích hoặc tiến tới bắt buộc áp dụng các tiêu chuẩn quốc tế về quản trị dữ liệu và an toàn thông tin nhằm nâng cao năng lực bảo vệ dữ liệu cá nhân trong bối cảnh hội nhập.

3.2.5. Hoàn thiện quy định về nghĩa vụ của doanh nghiệp và quyền bảo vệ dữ liệu cá nhân của người tiêu dùng

Cần sửa đổi, bổ sung Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15) theo hướng hoàn thiện Điều 4 về quyền của chủ thể dữ liệu, trong đó cụ thể hóa các quyền của người tiêu dùng như quyền được biết về mục đích xử lý dữ liệu, quyền từ chối hoặc rút lại sự đồng ý, quyền yêu cầu chỉnh sửa, xóa dữ liệu và quyền yêu cầu bồi thường khi dữ liệu bị xâm phạm. Đồng thời, cần sửa đổi, bổ sung Điều 8 về nghĩa vụ của bên xử lý dữ liệu, theo hướng quy định rõ nghĩa vụ của doanh nghiệp trong việc cung cấp thông tin minh bạch, dễ hiểu về hoạt động xử lý dữ liệu, không được gộp sự đồng ý xử lý dữ liệu với các điều khoản giao dịch, cũng như bảo đảm cơ chế để người tiêu dùng thực hiện quyền một cách thuận tiện và hiệu quả.

Bên cạnh đó, cần hoàn thiện Luật Bảo vệ quyền lợi người tiêu dùng năm 2023 theo hướng bổ sung một điều mới về bảo vệ dữ liệu cá nhân của người tiêu dùng, trong đó xác định rõ dữ liệu cá nhân là một nội dung thuộc quyền lợi người tiêu dùng cần được bảo vệ, đồng thời quy định trách nhiệm của tổ chức, cá nhân kinh doanh trong việc thu thập, sử dụng và bảo mật dữ liệu. Trên cơ sở các quy định tại cấp luật, cần tiếp tục cụ thể hóa tại Nghị định 356/2025/NĐ-CP bằng việc bổ sung các điều

khoản hướng dẫn quy định về nghĩa vụ cung cấp thông tin, cơ chế thực hiện quyền của người tiêu dùng và xử lý vi phạm liên quan đến dữ liệu cá nhân.

3.3. Kiến nghị nâng cao hiệu quả thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng

Bên cạnh việc hoàn thiện quy định pháp luật, để nâng cao hiệu quả thực hiện trách nhiệm bảo vệ dữ liệu cá nhân của khách hàng, cần triển khai các giải pháp thực thi từ phía doanh nghiệp, cơ quan quản lý nhà nước và người dân như sau:

3.3.1. Giải pháp từ phía doanh nghiệp

Bên cạnh việc hoàn thiện quy định pháp luật, nâng cao hiệu quả thực thi pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng cần đặt trọng tâm vào nhóm giải pháp tuân thủ (compliance) xuất phát từ chính doanh nghiệp. Bởi lẽ, trách nhiệm bảo vệ dữ liệu cá nhân trong hoạt động kinh doanh trước hết là nghĩa vụ pháp lý của doanh nghiệp với tư cách là chủ thể trực tiếp thu thập, xử lý và khai thác dữ liệu. Do đó, nếu chỉ dừng lại ở việc kiến nghị cơ quan nhà nước hoàn thiện pháp luật mà không đề xuất giải pháp cụ thể cho doanh nghiệp, thì hiệu quả thực tiễn của đề án sẽ chưa đáp ứng yêu cầu đặt ra từ mục tiêu nghiên cứu.

Trước hết, doanh nghiệp cần xây dựng và vận hành một chương trình tuân thủ bảo vệ dữ liệu cá nhân mang tính hệ thống, thể hiện ở việc ban hành chính sách nội bộ, thiết lập quy trình xử lý dữ liệu, phân quyền truy cập và kiểm soát trách nhiệm trong từng bộ phận. Việc tuân thủ không chỉ dừng lại ở yêu cầu "có quy định" mà phải bảo đảm "thực thi được" trong thực tế, thông qua cơ chế giám sát nội bộ, lưu trữ hồ sơ chứng minh tuân thủ và đánh giá định kỳ mức độ rủi ro trong hoạt động xử lý dữ liệu cá nhân. Đây là cơ sở để doanh nghiệp thể hiện trách nhiệm giải trình, hạn chế rủi ro pháp lý và giảm thiểu khả năng phát sinh tranh chấp với khách hàng.

Tiếp theo, doanh nghiệp cần triển khai quy trình đánh giá tác động bảo vệ dữ liệu cá nhân (Data Protection Impact Assessment – DPIA) đối với các hoạt động xử lý dữ liệu có nguy cơ cao. DPIA giúp doanh nghiệp nhận diện sớm các nguy cơ xâm phạm dữ liệu, đánh giá mức độ ảnh hưởng đối với quyền và lợi ích của khách hàng, từ đó đưa ra biện pháp giảm thiểu phù hợp. Việc áp dụng DPIA đặc biệt cần thiết trong các lĩnh vực kinh doanh có cường độ xử lý dữ liệu lớn như thương mại điện tử,

tài chính – ngân hàng, nền tảng số và các dịch vụ số hóa. Thông qua DPIA, doanh nghiệp chuyển từ mô hình tuân thủ thụ động sang tuân thủ chủ động, không chỉ xử lý hậu quả khi xảy ra sự cố mà còn phòng ngừa vi phạm ngay từ giai đoạn thiết kế và vận hành hệ thống.

Song song đó, doanh nghiệp cần thiết lập cơ chế Cán bộ bảo vệ dữ liệu cá nhân (Data Protection Officer – DPO) hoặc bộ phận chuyên trách về bảo vệ dữ liệu cá nhân. DPO đóng vai trò tham mưu, giám sát tuân thủ và làm đầu mối phối hợp giữa doanh nghiệp với cơ quan quản lý nhà nước cũng như với chủ thể dữ liệu. Cơ chế DPO giúp doanh nghiệp chuẩn hóa quy trình xử lý dữ liệu, nâng cao chất lượng quản trị rủi ro và hạn chế tình trạng vi phạm do thiếu chuyên môn hoặc thiếu bộ phận chịu trách nhiệm rõ ràng trong nội bộ. Việc thiết lập DPO cũng là biểu hiện của trách nhiệm giải trình và trách nhiệm tuân thủ trong hoạt động xử lý dữ liệu cá nhân.

Ngoài ra, để nâng cao hiệu quả thực hiện nghĩa vụ bảo mật dữ liệu, doanh nghiệp cần tăng cường ứng dụng các công nghệ bảo vệ dữ liệu cá nhân và quyền riêng tư (Privacy-Enhancing Technologies – PETs) như mã hóa dữ liệu, ẩn danh hóa hoặc giả danh hóa, kiểm soát truy cập, xác thực đa yếu tố, giám sát an toàn thông tin và lưu vết hoạt động xử lý dữ liệu. Việc ứng dụng PETs không chỉ góp phần bảo đảm an toàn dữ liệu cá nhân trong toàn bộ vòng đời xử lý mà còn giúp doanh nghiệp giảm thiểu hậu quả nếu xảy ra sự cố rò rỉ dữ liệu. Trong bối cảnh các hành vi xâm phạm dữ liệu ngày càng tinh vi, PETs là một trong những giải pháp mang tính thực chất, có thể đo lường hiệu quả và phù hợp với yêu cầu tuân thủ trong hoạt động kinh doanh hiện đại.

Cuối cùng, doanh nghiệp cần chú trọng giải pháp về con người và quản trị nội bộ thông qua đào tạo định kỳ, nâng cao nhận thức tuân thủ cho nhân sự, thiết lập cơ chế kiểm soát truy cập theo nguyên tắc tối thiểu và tăng cường kỷ luật bảo mật. Thực tiễn cho thấy, yếu tố con người thường là nguyên nhân phổ biến dẫn đến rò rỉ dữ liệu, do đó việc xây dựng văn hóa tuân thủ trong doanh nghiệp là giải pháp quan trọng nhằm bảo đảm trách nhiệm bảo vệ dữ liệu cá nhân của khách hàng được thực hiện một cách hiệu quả và bền vững.

Như vậy, việc nâng cao hiệu quả thực hiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng cần kết hợp đồng bộ giữa giải pháp hoàn thiện pháp luật và giải pháp tuân thủ trong nội bộ doanh nghiệp. Trong đó, nhóm giải pháp compliance với trọng tâm DPIA – DPO – PETs đóng vai trò then chốt, góp phần giúp doanh nghiệp thực hiện trách nhiệm pháp lý một cách chủ động, minh bạch và hiệu quả, đồng thời bảo đảm quyền và lợi ích hợp pháp của khách hàng trong hoạt động kinh doanh.

3.3.2. Giải pháp từ phía cơ quan quản lý nhà nước

Thứ nhất, cơ quan quản lý nhà nước cần tăng cường công tác hướng dẫn, thanh tra và kiểm tra chuyên đề về bảo vệ dữ liệu cá nhân đối với doanh nghiệp, kịp thời phát hiện và xử lý các hành vi vi phạm. Việc kiểm tra định kỳ sẽ tạo áp lực tuân thủ và nâng cao tính răn đe của pháp luật.

Thứ hai, cần đẩy mạnh công tác tuyên truyền, phổ biến pháp luật về bảo vệ dữ liệu cá nhân tới cộng đồng doanh nghiệp và người dân, giúp nâng cao nhận thức và ý thức tuân thủ pháp luật. Đồng thời, việc công khai minh bạch các vụ việc vi phạm và biện pháp xử lý cũng là cơ sở để phòng ngừa vi phạm tương tự trong thực tiễn.

Thứ ba, cơ quan nhà nước cần tăng cường cơ chế phối hợp liên ngành trong quản lý và bảo vệ dữ liệu cá nhân, đặc biệt trong các lĩnh vực có mức độ xử lý dữ liệu cao như thương mại điện tử, tài chính – ngân hàng, viễn thông và nền tảng số. Cơ chế phối hợp hiệu quả sẽ góp phần nâng cao năng lực giám sát và xử lý vi phạm trong thực tế.

Bên cạnh việc hoàn thiện các quy định pháp luật, cần đặc biệt chú trọng đến giải pháp nâng cao nhận thức của người dân thông qua hoạt động tuyên truyền, phổ biến pháp luật về bảo vệ dữ liệu cá nhân. Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, người dân ngày càng tham gia nhiều vào các hoạt động trực tuyến, việc hiểu biết về quyền và nghĩa vụ liên quan đến dữ liệu cá nhân trở nên hết sức cần thiết. Tuy nhiên, trên thực tế, nhiều người tiêu dùng vẫn chưa nhận thức đầy đủ về quyền của mình, cũng như chưa có kỹ năng cần thiết để bảo vệ thông tin cá nhân trước các rủi ro trên môi trường số.

Do đó, cần thiết phải tăng cường công tác tuyên truyền pháp luật theo hướng đa dạng hóa hình thức và nội dung. Trước hết, các cơ quan nhà nước cần xây dựng các chương trình truyền thông đại chúng về bảo vệ dữ liệu cá nhân thông qua các phương tiện như truyền hình, mạng xã hội, báo điện tử và các nền tảng số. Nội dung tuyên truyền cần được thiết kế đơn giản, dễ hiểu, gắn với các tình huống thực tiễn nhằm giúp người dân dễ dàng tiếp cận và áp dụng.

Bên cạnh đó, cần lồng ghép nội dung giáo dục về bảo vệ dữ liệu cá nhân vào chương trình giáo dục phổ thông và đào tạo đại học, nhằm hình thành nhận thức và kỹ năng bảo vệ dữ liệu ngay từ sớm. Đồng thời, cần khuyến khích sự tham gia của doanh nghiệp trong việc phổ biến kiến thức cho khách hàng thông qua các hướng dẫn sử dụng dịch vụ an toàn, cảnh báo rủi ro và cung cấp thông tin minh bạch về việc xử lý dữ liệu cá nhân.

Ngoài ra, cần thiết lập các kênh hỗ trợ và tư vấn pháp lý để người dân có thể dễ dàng tiếp cận thông tin, phản ánh vi phạm và thực hiện các quyền của mình liên quan đến dữ liệu cá nhân. Việc đẩy mạnh công tác tuyên truyền và phổ biến pháp luật không chỉ góp phần nâng cao nhận thức xã hội mà còn là điều kiện quan trọng để bảo đảm hiệu quả thực thi pháp luật trong lĩnh vực bảo vệ dữ liệu cá nhân.

3.3.3. Giải pháp từ phía người dân

Bên cạnh trách nhiệm của doanh nghiệp và vai trò quản lý của Nhà nước, người dân với tư cách là chủ thể dữ liệu cũng giữ vai trò quan trọng trong việc nâng cao hiệu quả thực hiện pháp luật về bảo vệ dữ liệu cá nhân. Thực tiễn cho thấy, một trong những nguyên nhân dẫn đến vi phạm dữ liệu cá nhân là do người dùng còn hạn chế trong nhận thức và kỹ năng bảo vệ thông tin của chính mình.

Trước hết, cần nâng cao nhận thức của người dân về quyền và nghĩa vụ liên quan đến dữ liệu cá nhân. Người tiêu dùng cần chủ động tìm hiểu các quyền cơ bản như quyền được biết, quyền đồng ý, quyền truy cập, chỉnh sửa và xóa dữ liệu, từ đó có thể đưa ra quyết định phù hợp khi cung cấp thông tin cá nhân cho doanh nghiệp. Việc hiểu rõ quyền của mình sẽ giúp người dân tránh tình trạng chấp nhận các điều khoản xử lý dữ liệu một cách hình thức hoặc thiếu cân nhắc.

Người dân cần nâng cao kỹ năng bảo vệ dữ liệu cá nhân trong môi trường số, như hạn chế chia sẻ thông tin không cần thiết, sử dụng các biện pháp bảo mật cơ bản (mật khẩu mạnh, xác thực hai yếu tố), và thận trọng khi cung cấp dữ liệu trên các nền tảng trực tuyến. Đồng thời, cần có ý thức kiểm tra, rà soát các quyền truy cập ứng dụng và dịch vụ đối với dữ liệu cá nhân của mình.

Ngoài ra, người dân cần chủ động thực hiện quyền của mình thông qua việc yêu cầu doanh nghiệp cung cấp thông tin, chỉnh sửa hoặc xóa dữ liệu khi cần thiết, cũng như phản ánh, khiếu nại đến cơ quan có thẩm quyền khi phát hiện hành vi vi phạm. Sự tham gia tích cực của người dân không chỉ góp phần bảo vệ quyền lợi cá nhân mà còn tạo áp lực xã hội buộc doanh nghiệp phải tuân thủ nghiêm túc các quy định pháp luật. Như vậy, việc nâng cao nhận thức và vai trò chủ động của người dân là một yếu tố quan trọng trong việc bảo đảm hiệu quả thực thi pháp luật về bảo vệ dữ liệu cá nhân, góp phần xây dựng môi trường số an toàn và minh bạch.

TIỂU KẾT CHƯƠNG 3

Chương 3 đã đề xuất các định hướng và giải pháp nhằm hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng tại Việt Nam. Các giải pháp được xây dựng theo hướng tiếp cận toàn diện, bao gồm hoàn thiện quy định pháp luật, tăng cường cơ chế giám sát và thực thi, cũng như nâng cao yêu cầu về tổ chức thực hiện và bảo đảm kỹ thuật trong doanh nghiệp.

Cụ thể, Chương 3 đã tập trung đề xuất việc bổ sung các quy định về trách nhiệm giải trình của doanh nghiệp, hoàn thiện cơ chế giám sát và thực thi pháp luật, đồng thời tăng cường các yêu cầu về quản trị dữ liệu, hệ thống bảo mật thông tin và nghĩa vụ của doanh nghiệp trong mối quan hệ với quyền của người tiêu dùng. Các giải pháp này được thiết kế theo hướng cụ thể hóa nghĩa vụ pháp lý, bảo đảm tính khả thi và gắn với thực tiễn hoạt động xử lý dữ liệu trong nền kinh tế số. Việc hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân không chỉ dừng lại ở việc bổ sung quy định, mà cần hướng tới xây dựng một cơ chế quản trị dữ liệu hiện đại, minh bạch và hiệu quả, trong đó doanh nghiệp phải chịu trách nhiệm toàn diện đối với hoạt động xử lý dữ liệu của mình. Qua đó, không chỉ góp phần bảo vệ quyền và lợi ích hợp pháp của cá nhân mà còn tạo nền tảng pháp lý vững chắc cho sự phát triển bền vững của nền kinh tế số tại Việt Nam.

KẾT LUẬN

Trong bối cảnh chuyển đổi số và sự phát triển mạnh mẽ của nền kinh tế dữ liệu, vấn đề bảo vệ dữ liệu cá nhân của khách hàng ngày càng trở thành yêu cầu cấp thiết đối với hoạt động quản lý nhà nước cũng như hoạt động kinh doanh của doanh nghiệp. Xuất phát từ yêu cầu đó, đề án đã tập trung nghiên cứu trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, qua đó góp phần làm rõ cơ sở lý luận, đánh giá thực trạng pháp luật và đề xuất các giải pháp hoàn thiện phù hợp với bối cảnh Việt Nam hiện nay.

Đề án đã hệ thống hóa và làm rõ các khái niệm cơ bản liên quan đến dữ liệu cá nhân, bảo vệ dữ liệu cá nhân và trách nhiệm của doanh nghiệp trong quá trình xử lý dữ liệu. Đặc biệt, đề án đã xác định trách nhiệm của doanh nghiệp không chỉ dừng lại ở nghĩa vụ tuân thủ pháp luật mà còn bao gồm trách nhiệm bảo mật, trách nhiệm giải trình và trách nhiệm bảo đảm quyền của chủ thể dữ liệu trong toàn bộ vòng đời xử lý dữ liệu.

Thông qua việc phân tích các tình huống điển hình như vụ việc liên quan đến việc chia sẻ dữ liệu người dùng của nền tảng Zalo hay sự cố rò rỉ dữ liệu tại Trung tâm Thông tin tín dụng quốc gia (CIC), đề án đã làm rõ những dấu hiệu vi phạm nghĩa vụ của doanh nghiệp trong bảo vệ dữ liệu cá nhân. Các tình huống này cho thấy thực trạng đáng lo ngại về việc thu thập, sử dụng và chia sẻ dữ liệu cá nhân chưa tuân thủ đầy đủ các nguyên tắc pháp lý, đặc biệt là nguyên tắc đồng ý, minh bạch và bảo mật dữ liệu. Đồng thời, các vụ việc cũng phản ánh những hạn chế trong cơ chế giám sát, thực thi pháp luật cũng như nhận thức của doanh nghiệp và người dân. Trên cơ sở phân tích thực trạng pháp luật hiện hành, đặc biệt là các quy định trong Luật Dữ liệu năm 2024 (Luật số 60/2024/QH15), Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15) và Nghị định 356/2025/NĐ-CP, đề án đã chỉ ra những bất cập như quy định chưa cụ thể, thiếu cơ chế bảo đảm thực thi hiệu quả, trách nhiệm giải trình của doanh nghiệp chưa được quy định đầy đủ, cũng như việc bảo vệ quyền của người tiêu dùng trong lĩnh vực dữ liệu cá nhân còn chưa toàn diện.

Đề án đã đề xuất một hệ thống giải pháp tương đối toàn diện nhằm hoàn thiện pháp luật và nâng cao hiệu quả thực hiện trách nhiệm của doanh nghiệp trong bảo vệ

dữ liệu cá nhân của khách hàng. Các giải pháp được xây dựng theo hướng đồng bộ, bao gồm: bổ sung quy định về trách nhiệm giải trình của doanh nghiệp; hoàn thiện cơ chế giám sát và thực thi pháp luật; tăng cường yêu cầu về tổ chức thực hiện, quản trị dữ liệu và hệ thống bảo mật thông tin; đồng thời hoàn thiện các quy định về nghĩa vụ của doanh nghiệp gắn với quyền của người tiêu dùng. Bên cạnh đó, đề án cũng nhấn mạnh vai trò của doanh nghiệp, cơ quan quản lý nhà nước và người dân trong việc bảo đảm hiệu quả thực thi pháp luật trong thực tiễn.

Việc hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng cần được thực hiện theo hướng đặt chủ thể dữ liệu làm trung tâm, tăng cường trách nhiệm giải trình của doanh nghiệp và bảo đảm tính khả thi của cơ chế thực thi pháp luật. Đồng thời, cần xây dựng một hành lang pháp lý minh bạch, ổn định nhưng linh hoạt, phù hợp với sự phát triển nhanh chóng của công nghệ và các mô hình kinh doanh dựa trên dữ liệu. Tuy nhiên, do hạn chế về phạm vi nghiên cứu và điều kiện tiếp cận thông tin, đề án vẫn còn những điểm cần tiếp tục nghiên cứu, đặc biệt là các vấn đề liên quan đến quản lý dữ liệu xuyên biên giới, trách nhiệm pháp lý trong bối cảnh ứng dụng trí tuệ nhân tạo và việc xây dựng cơ chế giám sát độc lập về bảo vệ dữ liệu cá nhân tại Việt Nam.

Đề án đã đạt được mục tiêu nghiên cứu đề ra, góp phần cung cấp cơ sở lý luận và thực tiễn cho việc hoàn thiện pháp luật về trách nhiệm của doanh nghiệp trong bảo vệ dữ liệu cá nhân của khách hàng, đồng thời có thể là tài liệu tham khảo hữu ích cho hoạt động xây dựng chính sách và thực tiễn áp dụng pháp luật trong thời gian tới.

TÀI LIỆU THAM KHẢO

A. Văn bản quy phạm pháp luật

1. Quốc hội (2013), *Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam*, ban hành ngày 28/11/2013, Việt Nam.
2. Quốc hội (2015), *Bộ luật Dân sự*, số 91/2015/QH13, ban hành ngày 24/11/2015, Việt Nam.
3. Quốc hội (2015), *Bộ luật Hình sự*, số 100/2015/QH13, ban hành ngày 27/11/2015, Việt Nam.
4. Quốc hội (2017), *Luật sửa đổi, bổ sung một số điều của Bộ luật Hình sự*, số 12/2017/QH14, ban hành ngày 20/6/2017, Việt Nam.
5. Quốc hội (2018), *Luật An ninh mạng*, số 24/2018/QH14, ban hành ngày 12/6/2018, Việt Nam.
6. Quốc hội (2023), *Luật Bảo vệ quyền lợi người tiêu dùng*, số 19/2023/QH15, ban hành ngày 20/6/2023, Việt Nam.
7. Quốc hội (2023), *Luật Giao dịch điện tử*, số 20/2023/QH15, ban hành ngày 22/6/2023, Việt Nam.
8. Quốc hội (2024), *Luật Dữ liệu*, số 60/2024/QH15, ban hành ngày 30/11/2024, Việt Nam.
9. Quốc hội (2025), *Luật Bảo vệ dữ liệu cá nhân*, số 91/2025/QH15, ban hành năm 2025, Việt Nam.
10. Chính phủ (2013), *Nghị định số 52/2013/NĐ-CP về thương mại điện tử*, ban hành ngày 16/5/2013, Việt Nam.
11. Chính phủ (2020), *Nghị định số 15/2020/NĐ-CP 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*, ban hành ngày 03/02/2020, Việt Nam.
12. Chính phủ (2021), *Nghị định số 85/2021/NĐ-CP sửa đổi, bổ sung một số điều của Nghị định số 52/2013/NĐ-CP về thương mại điện tử*, ban hành ngày 25/9/2021, Việt Nam.
13. Chính phủ (2023), *Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân*, ban hành ngày 17/4/2023, Việt Nam.

14. Chính phủ (2025), *Nghị định số 356/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân*, ban hành năm 2025, Việt Nam.

B. Các tài liệu tham khảo khác

- Tài liệu tiếng Việt

1. Chu Thị Hoa. (2021). *Cần coi dữ liệu cá nhân là một loại tài sản phi truyền thống*. Báo Chính phủ. https://baochinhphu.vn/can-coi-du-lieu-ca-nhan-la-mot-loai-tai-san-phi-truyen-thong-102293775.htm (truy cập ngày 22/3/2026).
2. Dương, K. T. N., Huỳnh, T. T., Lê, T. K., & Mai, N. D. (2021). *Cải cách pháp luật đáp ứng nhu cầu bảo vệ dữ liệu cá nhân trong chuyển đổi số*. Nhà xuất bản Thông tin và Truyền thông.
3. Lê Thị Thuỳ Trang. (2017). *Nghiên cứu một số quy định về bảo vệ thông tin cá nhân trên thế giới và tại Việt Nam*. Trang Thông tin điện tử Cục Tin học hoá, Bộ Thông tin và Truyền thông.
4. Nguyễn Minh Thu và cộng sự. (2025). *Khung pháp lý về bảo vệ dữ liệu cá nhân trong bối cảnh xây dựng Chính phủ số tại Việt Nam*. Tạp chí Công Thương. https://tapchicongthuong.vn/khung-phap-ly-ve-bao-ve-du-lieu-ca-nhan-trong-boi-canh-xay-dung-chinh-phu-so-tai-viet-nam-139344.htm (truy cập ngày 22/3/2026).
5. Nguyễn Thị Long. (2022). Thực trạng pháp luật Việt Nam về bảo vệ dữ liệu cá nhân trong thời kỳ hội nhập. *Tạp chí Khoa học Kiểm sát*, 3(57).
6. Nguyễn Văn Cương. (2020). Thực trạng pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay và hướng hoàn thiện. *Tạp chí Thực tiễn pháp luật*, 15(415), tháng 8/2020.
7. Phạm Việt Tuấn. (2022). *Pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam* [Luận văn thạc sĩ, Trường Đại học Kinh tế TP. Hồ Chí Minh]. UEH Digital Repository. https://digital.lib.ueh.edu.vn/handle/UEH/64533
8. Trần Thị Thanh Bích, & Đào Thị Anh Thư. (2025). *Pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam - Những khoảng trống và hướng hoàn thiện*. Tạp chí Luật sư Việt Nam. https://lsvn.vn/phap-luat-ve-bao-ve-du-lieu-ca-nhan-o-viet-nam-

nhung-khoang-trong-va-huong-hoan-thien-a156811.html (truy cập ngày 22/3/2026).

9. Trần Thị Thu Phương. (2021). Quy định chung của Liên minh châu Âu về bảo vệ dữ liệu cá nhân và một số khuyến nghị đến Quốc hội, Chính phủ và doanh nghiệp Việt Nam. *Tạp chí Nghiên cứu Lập pháp*, 23(447), tháng 12/2021.
10. Vũ Công Giao, & Lê Trần Như Tuyên. (2020). *Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam*. Tạp chí Nghiên cứu Lập pháp. http://lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid=210546

- Tài liệu tiếng Anh

1. Amaral, A., et al. (2021). AI-enabled automation for privacy policy compliance. *IEEE Access*, 9.
2. Black, H. C., Garner, B. A., McDaniel, B. R., Schultz, D. W., & Company, W. P. (1999). *Black's law dictionary* (Vol. 196). West Group.
3. California Legislature. (2018). *California Consumer Privacy Act*. https://leginfo.legislature.ca.gov (Accessed: 20 March 2026).
4. Cisco. (2025). *The privacy advantage: Building trust in a digital world – Data privacy benchmark study 2025*. Cisco. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2025.pdf
5. European Data Protection Board. (2023). *Guidelines on personal data processing and compliance*. European Union.
6. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, 1–88. https://eur-lex.europa.eu
7. Kuner, C. (2017). *The GDPR: Understanding the EU General Data Protection Regulation*. Oxford University Press.
8. Miller, R. (2018). *Business law today*. Cengage Learning.

9. National Institute of Standards and Technology. (2010). *Guide to protecting personal information*. NIST.
10. OECD. (2013). *Guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing.
11. Singapore Statutes Online. (2012). *Personal Data Protection Act*. https://sso.agc.gov.sg (Accessed: 20 March 2026).
12. TrustArc. (2025). *Global privacy benchmarks report*. https://trustarc.com/wp-content/uploads/2025/06/2025-trustarc-global-privacy-benchmarks-report.pdf
13. Zhang, L., Moukafih, N., Alamri, H., Epiphaniou, G., & Maple, C. (2023). A BERT-based empirical study of privacy policies' compliance with GDPR. *2023 IEEE Conference on Communications and Network Security (CNS)*.