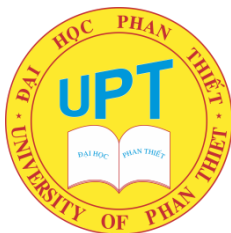


**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC PHAN THIẾT**



NGUYỄN VŨ VƯƠNG

**PHÁP LUẬT VỀ BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG
TỪ THỰC TIỄN TRÊN ĐỊA BÀN TỈNH BÌNH THUẬN**

**ĐỀ ÁN TỐT NGHIỆP THẠC SĨ
LUẬT KINH TẾ**

Bình Thuận - 2025

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC PHAN THIẾT**



NGUYỄN VŨ VƯƠNG

**PHÁP LUẬT VỀ BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG
TỪ THỰC TIỄN TRÊN ĐỊA BÀN TỈNH BÌNH THUẬN**

CHUYÊN NGÀNH LUẬT KINH TẾ

MÃ SỐ: 8380107

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

NGƯỜI HƯỚNG DẪN KHOA HỌC:

TS. PHAN HOÀI NAM

Bình Thuận - 2025

NHẬN XÉT CỦA HỘI ĐỒNG XÉT DUYỆT

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Phan Thiết, ngày tháng năm 20...

Hội đồng xét duyệt

LỜI CAM ĐOAN

Tôi xin cam đoan Đề án này là công trình nghiên cứu của riêng tôi. Các kết quả nêu trong Đề án chưa được công bố trong bất kỳ công trình nào khác. Các số liệu ví dụ và trích dẫn trong Đề án đảm bảo tính chính xác, tin cậy và trung thực. Tôi đã hoàn thành tất cả các môn học và đã thanh toán tất cả các nghĩa vụ tài chính theo quy định của Phòng Quản lý sau đại học - Trường Đại học Phan Thiết.

Vậy tôi viết Lời cam đoan này để nghị Phòng Quản lý sau đại học Trường Đại học Phan Thiết xem xét để tôi có thể bảo vệ Đề án.

Tôi xin chân thành cảm ơn!

Người cam đoan

Nguyễn Vũ Vương

MỤC LỤC

PHẦN MỞ ĐẦU	1
1. Tính cấp thiết của đề tài.....	1
2. Tình hình nghiên cứu.....	2
3. Mục đích và nhiệm vụ nghiên cứu	5
4. Đối tượng và phạm vi nghiên cứu	6
5. Phương pháp luận và phương pháp nghiên cứu	7
6. Ý nghĩa khoa học và giá trị ứng dụng của đề án	7
7. Kết cấu của đề án.....	8
CHƯƠNG 1. MỘT SỐ VẤN ĐỀ LÝ LUẬN VỀ THÔNG TIN NGƯỜI TIÊU DÙNG, BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG	9
1.1. Khái quát chung về thông tin người tiêu dùng	9
1.1.1. Khái niệm về thông tin người tiêu dùng.....	9
1.1.2. Đặc điểm của thông tin người tiêu dùng	10
1.1.3. Phân loại thông tin người tiêu dùng	10
1.2. Khái quát về bảo vệ thông tin người tiêu dùng	12
1.2.1. Khái niệm về bảo vệ thông tin người tiêu dùng	12
1.2.2. Đặc điểm của bảo vệ thông tin người tiêu dùng.....	13
1.2.3. Phân loại bảo vệ thông tin người tiêu dùng.....	13
1.2.4. Sự cần thiết bảo vệ thông tin người tiêu dùng.....	14
1.3. Pháp luật của một số khu vực và quốc gia trên thế giới về bảo vệ thông tin người tiêu dùng	15
1.3.1. Pháp luật về bảo vệ thông tin người tiêu dùng của Liên minh châu Âu	15
1.3.2. Pháp luật về bảo vệ thông tin người tiêu dùng của Nhật Bản	16
1.3.3. Pháp luật về bảo vệ thông tin người tiêu dùng của Singapore	16
KẾT LUẬN CHƯƠNG 1	18
CHƯƠNG 2: QUY ĐỊNH CỦA PHÁP LUẬT VIỆT NAM VỀ BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG.....	19
2.1. Quy định của pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng.....	19
2.1.1. Quy định về nhận diện thông tin người tiêu dùng.....	19
2.1.2. Quy định về xử lý, chuyển giao thông tin người tiêu dùng.....	21

2.1.3. Quy định về các hành vi xâm phạm thông tin người tiêu dùng	23
2.1.4. Quy định về các biện pháp bảo vệ thông tin người tiêu dùng.....	26
2.2. Đánh giá quy định của pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng	29
KẾT LUẬN CHƯƠNG 2	32
CHƯƠNG 3. THỰC TIỄN BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG Ở VIỆT NAM VÀ TỈNH BÌNH THUẬN. MỘT SỐ KIẾN NGHỊ HOÀN THIỆN PHÁP LUẬT VIỆT NAM VỀ BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG	34
3.1. Thực trạng các quy định của pháp luật về bảo vệ thông tin người tiêu dùng	34
3.1.1. Một số kết quả đạt được	34
3.1.2. Những hạn chế còn tồn tại trong thực tiễn thực hiện pháp luật về bảo vệ thông tin người tiêu dùng ở Việt Nam.....	41
3.1.3. Nguyên nhân của những hạn chế còn tồn tại.....	50
3.2. Một số kiến nghị hoàn thiện pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng	52
3.2.1. Định hướng chung về hoàn thiện pháp luật về bảo vệ thông tin người tiêu dùng	52
3.2.2. Một số kiến nghị cụ thể hoàn thiện pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng.....	54
3.2.2.1. Giải pháp hoàn thiện pháp luật.....	54
3.2.2.2. Giải pháp nhằm nâng cao hiệu quả hoạt động thực hiện pháp luật trên thực tế	56
3.2.2.3. Giải pháp nhằm nâng cao hiệu quả hoạt động thực hiện pháp luật trên thực tế tại tỉnh Bình Thuận	58
KẾT LUẬN CHƯƠNG 3	62
KẾT LUẬN	63
DANH MỤC TÀI LIỆU THAM KHẢO	65

DANH MỤC CHỮ VIẾT TẮT

Thứ tự	Chữ viết tắt	Nghĩa đầy đủ
1.	APPI	Đạo luật bảo vệ Dữ liệu cá nhân Nhật Bản (Act on the Protection of Personal Information)
2.	BLDS	Bộ Luật Dân sự
3.	BLHS	Bộ Luật Hình sự
4.	DLCN	Dữ liệu cá nhân
5.	EU	Liên minh Châu Âu (European Union)
6.	GDPR	Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation)
7.	Nghị định số 15/2020/NĐ-CP	Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính Phủ quy định về 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
8.	Nghị định số 13/2023/NĐ-CP	Nghị định số 13/2023/NĐ-CP ngày 17/04/2023 của Chính Phủ quy định về Bảo vệ dữ liệu cá nhân
9.	NTD	Người tiêu dùng
10.	OECD	Tổ chức Hợp tác và Phát triển Kinh tế
11.	PDPA	Luật Bảo vệ Dữ liệu cá nhân Singapore (Personal Data Protection)
12.	TTCN	Thông tin cá nhân

MỞ ĐẦU

1. Tính cấp thiết của Đề tài

Thông tin của người dùng là cá nhân hay tổ chức trong thời đại số hiện nay là dữ liệu quan trọng. Và các dữ liệu này đang trở thành “**tài sản**” có tầm quan trọng hàng đầu của nền kinh tế số. Như vậy, xem thông tin cá nhân (TTCN) là một loại tài sản sẽ giúp mỗi người thận trọng hơn khi cung cấp thông tin trên môi trường mạng. Ở góc độ vĩ mô hơn, tận dụng tối đa nguồn tài nguyên mới mẻ này chúng ta cần khung pháp lý chặt chẽ với những chế tài nghiêm minh hơn đối với các hành vi vi phạm thông tin cá nhân.

Hiến pháp năm 2013 đã kế thừa các quy định của các bản Hiến pháp trước đây, khẳng định quyền riêng tư của cá nhân là bất khả xâm phạm, đồng thời phát triển mở rộng phạm vi quyền riêng tư không chỉ là quyền bất khả xâm phạm về thân thể, nhà ở, thư tín mà còn bao gồm quyền bảo vệ bí mật cá nhân, trong đó có thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình (Điều 21).

Thời gian gần đây, Đảng và Nhà nước đã ban hành nhiều văn bản chỉ đạo vấn đề này. Bảo vệ dữ liệu cá nhân (DLCN) được tiến hành song song, đồng thời với sự phát triển kinh tế, xã hội, đi liền với tất cả các khâu, quá trình nhưng phải đảm bảo không hạn chế sự phát triển, đổi mới và sáng tạo.

Trên thực tế, TTCN của hơn 2/3 dân số nước ta đang được lưu trữ, đăng tải, chia sẻ và thu thập trên không gian mạng với nhiều hình thức và mức độ chi tiết khác nhau. Việc thu thập TTCN được tích hợp sâu trong từng sản phẩm, dịch vụ và khó có thể nhận biết, xác thực đúng sai và bảo đảm mục đích sử dụng như thông báo.

Tình trạng lộ dữ liệu cá nhân diễn ra phổ biến trên không gian mạng. Người tiêu dùng (NTD) chưa có ý thức bảo vệ TTCN, đăng tải công khai hoặc lộ trong quá trình chuyển giao, lưu trữ, trao đổi phục vụ hoạt động kinh doanh hoặc do biện pháp bảo vệ không tương xứng dẫn tới bị chiếm đoạt và đăng tải công khai.

Tình trạng mua bán TTCN hiện đang diễn ra phổ biến, công khai, với các thông tin thô và TTCN đã qua xử lý nhiều hành vi chưa được xử lý vì thiếu quy định của pháp luật.

Đề xảy ra tình trạng trên, có nhiều nguyên nhân, nhưng trước hết phải kể đến những hạn chế từ chính những quy định pháp luật đang điều chỉnh về vấn đề này.

Nhận thức được tính cấp thiết và ý nghĩa thực tiễn của vấn đề bảo vệ thông tin cá nhân người tiêu dùng, học viên lựa chọn đề tài ***“Pháp luật về bảo vệ thông tin người tiêu dùng từ thực tiễn trên địa bàn tỉnh Bình Thuận”*** làm đề tài Đề án thạc sỹ chuyên ngành Luật Kinh tế của mình.

2. Tình hình nghiên cứu

Liên quan đến pháp luật về bảo vệ thông tin người tiêu dùng là vấn đề quan trọng, được nhiều quốc gia trên thế giới trong đó có Việt Nam quan tâm và chú trọng. Thông qua việc xây dựng chính sách tích cực, Chính phủ của các nước nói chung và của Việt Nam nói riêng luôn đề cao tính sáng tạo, thúc đẩy các nhà khoa học, nghiên cứu sinh thực hiện các công trình nghiên cứu chuyên sâu, trong đó có những công trình khoa học pháp lý đã được thực hiện.

2.1. Một số công trình nghiên cứu trong nước

Về góc độ công trình nghiên cứu, có thể kể đến công trình như Trần Thị Hồng Hạnh, *“Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay”*, Luận án tiến sĩ, Học viện Chính trị Quốc gia Hồ Chí Minh, 2018. Công trình này nghiên cứu về hoàn thiện pháp luật bảo vệ thông tin cá nhân ở Việt Nam hiện nay. Công trình đã chỉ ra được các khái niệm, đặc điểm, nội dung, vai trò cơ bản trong pháp luật về bảo vệ TTCN và đề ra các tiêu chí, các yếu tố ảnh hưởng rõ ràng đánh giá mức độ hoàn thiện của pháp luật về bảo vệ TTCN. Công trình cũng đưa ra được các dẫn chứng pháp luật quốc tế để soi chiếu với quá trình hình thành và phát triển và thực trạng pháp luật bảo vệ TTCN ở Việt Nam, từ đó đưa ra những quan điểm và giải pháp để hoàn thiện pháp luật ở Việt Nam để kết lại đề tài. Tuy nhiên, mục đích của công trình là hoàn thiện pháp luật Việt Nam nên công trình này không đi sâu vào những phương hướng giải quyết khác, chưa có kiến nghị cụ thể mà chỉ là định hướng.

Bên cạnh đó các công trình như Lê Thị Thảo, *“Pháp luật bảo vệ quyền riêng tư của cá nhân trong hoạt động thương mại điện tử ở Việt Nam hiện nay”*, Luận án Tiến sĩ Luật học, Học viện Khoa học xã hội, Viện Hàn lâm Khoa học xã hội Việt Nam, 2021; công trình của Trần Quốc Bình, *“Pháp luật bảo vệ dữ liệu cá nhân ở Việt Nam trong*

bối cảnh hội nhập quốc tế”, Luận án Tiến sĩ Luật học, Đại học Quốc gia Hà Nội, 2020; công trình của Nguyễn Thanh Tùng, “*Pháp luật về bảo vệ thông tin cá nhân trong lĩnh vực thương mại điện tử: Kinh nghiệm quốc tế và vận dụng vào Việt Nam*”, Luận án Tiến sĩ Luật học, Học viện Chính trị Quốc gia Hồ Chí Minh, 2022... Các công trình trên có ưu điểm là Phân tích hệ thống pháp luật và thực tiễn thực thi quyền riêng tư ở Việt Nam một cách toàn diện, có chiều sâu lý luận và kinh nghiệm đối sánh (EU – GDPR, Mỹ, Nhật Bản). Tuy nhiên vẫn còn hạn chế là các giải pháp còn mang tính định hướng, thiếu đề xuất kỹ thuật pháp lý cụ thể cho hệ thống luật Việt Nam.

Về góc độ bài viết, tạp chí, có nhiều bài viết tạp chí của các học giả uy tín cũng đề cập đến vấn đề BVTNTD ở Việt nam như bài viết của **Lê Văn Hưng**, “Vai trò của pháp luật trong bảo vệ thông tin cá nhân của người tiêu dùng trên môi trường mạng”, **Tạp chí**: Nhà nước và Pháp luật, Số 12/2020; bài viết của **Phan Thị Thu Hằng**, “Bảo vệ thông tin cá nhân – quyền cơ bản trong nền kinh tế số”, **Tạp chí**: Thông tin Khoa học Pháp lý, Bộ Tư pháp, Số 4/2022; bài viết của **TS. Nguyễn Thị Tuyết Nhung**, “Bảo vệ dữ liệu cá nhân trong thương mại điện tử ở Việt Nam – Thực trạng và giải pháp”, **Tạp chí**: Luật học, Số 5/2022, Trường Đại học Luật Hà Nội; bài viết của **Trần Thị Hòa**, “Một số vấn đề pháp lý về bảo vệ thông tin người tiêu dùng trong hoạt động thương mại điện tử”, **Tạp chí**: Khoa học Kiểm sát, Số 3/2021. Các bài viết tạp chí trên có ưu điểm là Nêu bật vai trò chủ đạo của Nhà nước trong việc xây dựng hành lang pháp lý bảo vệ thông tin cá nhân, hằng định quyền bảo vệ thông tin cá nhân là một quyền cơ bản trong thời đại số, gắn với quyền con người. Tuy nhiên vẫn còn hạn chế là các bài viết còn mang tính tổng quan, thiên về lý luận chưa đi sâu vào phân tích quy phạm pháp luật cụ thể.

Ở cấp độ nghiên cứu khoa học có những công trình nghiên cứu khoa học của sinh viên đến từ các cơ sở đào tạo luật uy tín trong cả nước như Trường Đại học Luật Hà Nội, Trường Đại học Luật TP. Hồ Chí Minh. Một số công trình nghiên cứu có thể kể đến như: Nguyễn Ngọc Phúc Đăng (2018), Nghiên cứu luật bảo vệ thông tin cá nhân của Singapore và kinh nghiệm cho Việt Nam, Đề tài Nghiên cứu khoa học Eureka, Trường Đại học Luật Thành phố Hồ Chí Minh, 2018; Bùi Duy Khánh, Trần Minh Phú, Dương Yên Nhi (2021), Pháp luật Việt Nam về bảo vệ DLCN trong giai đoạn cách mạng công nghiệp 4.0 - Bài học kinh nghiệm của các quốc gia trên thế giới, đạt giải Nhất giải

thường Sinh viên nghiên cứu khoa học của Trường Đại học Luật Hà Nội năm 2021. Nhìn chung các đề tài này đều đi theo hướng nghiên cứu, so sánh các quy định của pháp luật Việt Nam và quy định của các quốc gia, khu vực trên thế giới về bảo vệ DLCN, từ đó đưa ra những kiến nghị hoàn thiện pháp luật cũng như nâng cao hiệu quả thực hiện bảo vệ DLCN trên thực tế. Tuy nhiên, với hạn chế là những đề tài nghiên cứu khoa học của sinh viên, với trình độ nhận thức còn có hạn, những đề tài này vẫn tồn tại những hạn chế nhất định

2.2. Công trình nghiên cứu nước ngoài

Một số công trình nghiên cứu nước ngoài về đề tài này nổi bật có thể kể đến như: Cuốn sách “Information Privacy Law” (Luật về Quyền riêng tư thông tin) của tác giả Daniel J. Solove & Paul M. Schwartz, nhà xuất bản Aspen Publishers, năm 2003 (cập nhật và tái bản nhiều năm liên tiếp), được xem là giáo trình tiêu chuẩn tại nhiều trường luật ở Mỹ; Cuốn sách “Privacy and Data Protection Law” (Luật bảo vệ quyền riêng tư và dữ liệu cá nhân), Tác giả: Lee A. Bygrave, Nhà xuất bản: Oxford University Press, năm 2014, Phân tích pháp lý rõ ràng về các khung luật quốc tế và khu vực (đặc biệt là EU – GDPR).

Về góc độ bài viết, tạp chí, có thể kể đến Daniel J. Solove (Hoa Kỳ), "The Digital Person: Technology and Privacy in the Information Age" (Con người số: Công nghệ và quyền riêng tư trong thời đại thông tin), Tạp chí: New York University Press, 2004, à tác phẩm nền tảng phân tích sâu sắc mối quan hệ giữa công nghệ, quyền riêng tư và sự kiểm soát dữ liệu cá nhân. Là tài liệu tham khảo có giá trị cho nhiều quốc gia trong xây dựng pháp luật bảo vệ thông tin cá nhân; Paul M. Schwartz & Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (Vấn đề PII: Quyền riêng tư và khái niệm mới về thông tin nhận dạng cá nhân), Tạp chí: *New York University Law Review*, Vol. 86, No. 6 (2011), Đề xuất khái niệm mở rộng về “thông tin nhận dạng cá nhân” (PII), từ đó làm nền tảng cho xây dựng luật bảo vệ dữ liệu. Có ảnh hưởng lớn đến sự hình thành GDPR ở châu Âu.

Ở cấp độ công trình nghiên cứu, có công trình của Viktor Mayer-Schönberger, “Delete: The Virtue of Forgetting in the Digital Age” (Xóa bỏ: Đức hạnh của việc lãng quên trong kỷ nguyên số) , Nhà xuất bản **Princeton University Press**, 2009, đề xuất

khái niệm “quyền được lãng quên”, rất cần thiết trong bảo vệ thông tin người tiêu dùng; công trình của Alan Westin, “Privacy and Freedom” (Quyền riêng tư và Tự do), nhà xuất bản **Atheneum**, 1967, là tác phẩm nền tảng, xác lập định nghĩa và tầm quan trọng của quyền riêng tư.

Trong quá trình nghiên cứu, tác giả đánh giá đây là những nguồn tài liệu tốt, có giá trị tham khảo lớn với hoạt động áp dụng pháp luật dân sự nói chung cũng như áp dụng pháp luật nhằm đảm bảo chất lượng bảo vệ thông tin NTD. Tuy nhiên, phạm vi nghiên cứu các công trình này chưa thực sự chuyên sâu và bao quát về bảo vệ thông tin NTD từ góc độ lý luận đến quy định pháp luật hay vấn đề áp dụng pháp luật trong thực tiễn. Do đó, tác giả khẳng định đối tượng nghiên cứu và phạm vi nghiên cứu của các đề tài của tác giả không trùng lặp. Đề tài “Pháp luật về bảo vệ thông tin người tiêu dùng từ thực tiễn trên địa bàn Tỉnh Bình Thuận” là một đề tài có tính mới, tính thời sự. Trong đề án của mình, tác giả sẽ kế thừa, trích dẫn những kết luận khoa học quý báu của các công trình trên, đồng thời mở rộng và nghiên cứu chuyên sâu hơn các vấn đề lý luận cũng như quy định của pháp luật Việt Nam hiện hành về TTCN và bảo vệ thông tin NTD, đồng thời so sánh, đối chiếu với quy định của một số quốc gia, khu vực trên thế giới để đưa ra những giải pháp hoàn thiện quy định của pháp luật và nâng cao hiệu quả công tác thực hiện trên thực tế

3. Mục đích và nhiệm vụ nghiên cứu

Mục tiêu của luận văn là nghiên cứu các vấn đề lý luận về thông tin NTD và bảo vệ thông tin NTD, trên cơ sở phân tích những điểm tích cực và hạn chế của pháp luật hiện hành về bảo vệ thông tin NTD cũng như những tính cực và hạn chế của việc thực hiện các quy định của pháp luật về bảo vệ thông tin NTD trên thực tế, từ đó đề xuất những giải pháp, kiến nghị nhằm hoàn thiện quy định của pháp luật về bảo vệ thông tin NTD và nâng cao hiệu quả công tác thực hiện quy định của pháp luật trên thực tế. Để thực hiện được mục đích này, Đề án đặt ra những nhiệm vụ cụ thể sau:

- Nghiên cứu những vấn đề lý luận cơ bản về NTD, thông tin NTD, bảo vệ thông tin NTD và cơ chế pháp lý bảo vệ thông tin NTD.
- Nghiên cứu quy định về bảo vệ thông tin NTD của một số quốc gia, khu vực trên thế giới đã đạt được những thành tựu nhất định về bảo vệ thông tin NTD, từ đó có sự so sánh đối chiếu với các quy định của pháp luật Việt Nam về bảo vệ thông tin NTD.

- Đánh giá thực trạng những quy định của pháp luật về bảo vệ thông tin NTD cũng như thực tiễn thi hành pháp luật để xác định những thành tựu gì đã đạt được và còn tồn tại những mặt hạn chế nào.

- Nghiên cứu đề xuất giải pháp nhằm nâng cao hiệu quả của công tác bảo vệ thông tin NTD ở Việt Nam.

4. Đối tượng và phạm vi nghiên cứu

4.1. Đối tượng nghiên cứu

Trong khuôn khổ Luận văn này, tác giả tập trung nghiên cứu về:

- Hệ thống pháp luật Việt Nam về bảo vệ thông tin NTD được quy định tại nhiều văn bản pháp luật khác nhau như BLDS năm 2015, BLHS năm 2015 sửa đổi bổ sung năm 2017, Luật bảo vệ quyền lợi người tiêu dùng 2023, Luật an ninh mạng năm 2018, Luật an toàn thông tin mạng 2015 và các văn bản có liên quan khác.

- Quy định của pháp luật một số quốc gia, khu vực trên thế giới về bảo vệ thông tin NTD để đưa ra những đánh giá, nhận xét, rút ra những kinh nghiệm để Việt Nam có thể áp dụng trong quá trình hoàn thiện pháp luật về bảo vệ thông tin NTD.

- Hoạt động thực hiện pháp luật về bảo vệ thông tin NTD tại Việt Nam.

4.2. Phạm vi nghiên cứu

Đề án này được tác giả tiến hành thực hiện trong giới hạn văn bản pháp luật chuyên ngành có liên quan, giới hạn không gian và thời gian, cụ thể:

Về phạm vi văn bản pháp luật: Tác giả nghiên cứu các quy định liên quan đến vấn đề bảo vệ thông tin NTD quy định của BLDS năm 2015, BLHS năm 2015 sửa đổi bổ sung năm 2017, Luật bảo vệ quyền lợi người tiêu dùng 2023, Luật An Ninh Mạng 2018, Luật An toàn thông tin mạng 2015, Luật khám chữa bệnh năm 2006,... và một số Nghị định về xử lý vi phạm hành chính như Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 quy định về Bảo vệ Dữ liệu cá nhân, Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 quy định về 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, Nghị định số 88/2019/NĐ-CP ngày 14/11/2019 quy định về xử phạt vi phạm hành chính trong lĩnh vực

vực tiền tệ và ngân hàng.

Về không gian: Tác giả thực hiện nghiên cứu hoạt động thực hiện pháp luật về bảo vệ thông tin NTD trên phạm vi toàn quốc và thực tế ở tỉnh Bình Thuận.

Về thời gian: Tác giả chủ yếu nghiên cứu các quy định pháp luật và hoạt động thực hiện pháp luật đang có hiệu lực pháp luật và tác động đến Việt Nam trong vòng 10 năm trở lại đây cùng với sự phát triển vượt bậc của internet.

5. Phương pháp nghiên cứu

- *Phương pháp phân tích, tổng hợp, so sánh*: được sử dụng ở tất cả các nội dung của Đề án.

- *Phương pháp kết hợp lý luận với phân tích quy định của pháp luật*: được áp dụng khi nghiên cứu các quan điểm khoa học về đổi mới nội dung trách nhiệm của tổ chức, cá nhân kinh doanh đối với việc BVTTNTD trước những tác động của hội nhập và toàn cầu hóa. Phương pháp này được sử dụng tại Chương 1 của Đề án.

- *Phương pháp hệ thống hoá*: được sử dụng ở tất cả nội dung của Đề án

6. Ý nghĩa khoa học và giá trị ứng dụng của Đề án

6.1. Ý nghĩa khoa học

- Đề tài có ý nghĩa khoa học quan trọng trong việc bổ sung và hoàn thiện cơ sở lý luận liên quan đến bảo vệ quyền lợi người tiêu dùng, đặc biệt là quyền được bảo mật thông tin cá nhân – một nội dung ngày càng được chú trọng trong bối cảnh chuyển đổi số và phát triển kinh tế số hiện nay.

- Đề tài góp phần hệ thống hóa và làm rõ các khái niệm pháp lý, các nguyên tắc điều chỉnh trong hoạt động thu thập, xử lý và sử dụng thông tin cá nhân; đồng thời cung cấp cái nhìn thực tiễn sinh động từ Bình Thuận để kiểm nghiệm và hoàn thiện các quy định pháp luật hiện hành.

- Kết quả nghiên cứu của đề tài có thể được ứng dụng thiết thực trong thực tiễn pháp lý và quản lý nhà nước ở địa phương, cụ thể như sau:

6.2. Giá trị ứng dụng

- Là cơ sở để đề xuất, kiến nghị các giải pháp hoàn thiện pháp luật và nâng cao

hiệu quả tổ chức thực thi pháp luật về bảo vệ thông tin người tiêu dùng tại tỉnh Bình Thuận.

- Góp phần nâng cao nhận thức và trách nhiệm của các chủ thể có liên quan như cơ quan quản lý nhà nước, doanh nghiệp và người dân trong việc bảo vệ thông tin cá nhân của người tiêu dùng.

- Có thể được sử dụng làm tài liệu tham khảo trong nghiên cứu, giảng dạy và học tập các lĩnh vực liên quan.

- Là tiền đề cho việc mở rộng nghiên cứu tại các địa phương khác nhằm thúc đẩy quá trình hoàn thiện pháp luật trên phạm vi toàn quốc.

7. Kết cấu của Đề án

Ngoài lời mở đầu, kết luận, danh mục tài liệu tham khảo, đề án được chia làm 3 chương:

Chương 1: Một số vấn đề lý luận về thông tin người tiêu dùng, bảo vệ thông tin người tiêu dùng.

Chương 2: Quy định của pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng.

Chương 3: Thực tiễn bảo vệ thông tin người tiêu dùng ở Việt Nam và tỉnh Bình Thuận. Một số kiến nghị hoàn thiện pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng.

CHƯƠNG 1

MỘT SỐ VẤN ĐỀ LÝ LUẬN VỀ THÔNG TIN NGƯỜI TIÊU DÙNG, BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG

1.1. Khái quát chung về thông tin người tiêu dùng

1.1.1. Khái niệm thông tin người tiêu dùng

Trong nền kinh tế thị trường hiện đại, đặc biệt là dưới tác động của quá trình chuyển đổi số và sự phát triển mạnh mẽ của thương mại điện tử, thông tin người tiêu dùng ngày càng đóng vai trò quan trọng trong các hoạt động sản xuất, phân phối, kinh doanh và marketing. Tuy nhiên, cho đến nay, hệ thống pháp luật Việt Nam vẫn chưa có một định nghĩa thống nhất và trực tiếp về “thông tin người tiêu dùng”. Do đó, để tiếp cận khái niệm này, cần vận dụng các quy định pháp luật hiện hành liên quan, đồng thời kế thừa cách hiểu phổ biến trong lý luận và thực tiễn.

Theo Luật Bảo vệ quyền lợi người tiêu dùng năm 2010, tuy không trực tiếp định nghĩa "thông tin người tiêu dùng", nhưng nội dung của luật cho thấy đây là đối tượng cần được bảo vệ trong các mối quan hệ giữa người tiêu dùng và tổ chức, cá nhân kinh doanh. Bên cạnh đó, Nghị định số 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân quy định: “Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử liên quan đến một cá nhân hoặc giúp xác định một cá nhân cụ thể.” Từ đó có thể suy luận, **thông tin người tiêu dùng là một bộ phận của dữ liệu cá nhân**, gắn liền với quá trình tiêu dùng hàng hóa, dịch vụ của một cá nhân hoặc tổ chức không vì mục đích kinh doanh.

Từ góc độ lý luận, có thể hiểu:

Thông tin người tiêu dùng là toàn bộ dữ liệu liên quan đến danh tính, hành vi, nhu cầu và quá trình sử dụng hàng hóa, dịch vụ của một cá nhân hoặc tổ chức trong vai trò người tiêu dùng, được tạo ra, thu thập, lưu trữ hoặc xử lý trong quá trình tiêu dùng.

Khái niệm này không chỉ bao gồm những thông tin định danh cơ bản mà còn mở rộng sang thông tin hành vi, thông tin tài chính, thông tin vị trí... và là đối tượng ngày càng được khai thác mạnh mẽ bởi các doanh nghiệp trong thời đại số.

1.1.2. Đặc điểm của thông tin người tiêu dùng

Thông tin người tiêu dùng mang những đặc điểm cơ bản sau:

Thứ nhất, thông tin người tiêu dùng có tính cá nhân và gắn liền với danh tính cụ thể. Đây là loại thông tin giúp xác định một người tiêu dùng duy nhất, từ đó cho phép tổ chức kinh doanh thực hiện các hoạt động cá nhân hóa sản phẩm, dịch vụ, quảng cáo.

Thứ hai, thông tin người tiêu dùng có giá trị kinh tế và thương mại cao. Trong thời đại số, thông tin được xem là một loại “tài sản mềm” có thể định giá. Việc thu thập và phân tích thông tin người tiêu dùng cho phép doanh nghiệp xây dựng chiến lược tiếp thị, dự báo nhu cầu thị trường và tối ưu hóa lợi nhuận. Chính vì vậy, **thông tin người tiêu dùng đã trở thành một đối tượng bị khai thác triệt để bởi các nền tảng kỹ thuật số.**

Thứ ba, thông tin người tiêu dùng dễ bị xâm phạm, rò rỉ và khó kiểm soát. Khác với hàng hóa hữu hình, một khi thông tin đã bị tiết lộ, người tiêu dùng khó có thể thu hồi hoặc khôi phục quyền kiểm soát. Thực tế đã có nhiều vụ việc cho thấy hàng triệu dữ liệu người tiêu dùng bị rò rỉ trên môi trường mạng, dẫn đến hậu quả nghiêm trọng về tài sản, uy tín và an toàn cá nhân.

Thứ tư, thông tin người tiêu dùng là đối tượng cần được bảo vệ đặc biệt trong pháp luật hiện đại. Trên thế giới, nhiều quốc gia đã ban hành luật riêng về bảo vệ dữ liệu cá nhân (như GDPR của Liên minh châu Âu, CCPA của bang California – Hoa Kỳ), trong đó coi thông tin người tiêu dùng là trung tâm của quyền riêng tư số. Tại Việt Nam, bên cạnh các quy định phân tán trong nhiều văn bản pháp luật, việc ban hành Nghị định số 13/2023/NĐ-CP là bước tiến quan trọng nhằm cụ thể hóa nghĩa vụ bảo vệ dữ liệu của các tổ chức, cá nhân kinh doanh.

1.1.3. Phân loại thông tin người tiêu dùng

Tùy theo mục tiêu nghiên cứu và cách tiếp cận khác nhau, thông tin người tiêu dùng có thể được phân loại theo nhiều tiêu chí khác nhau. Dưới đây là hai cách phân loại cơ bản, phổ biến trong nghiên cứu và thực tiễn pháp lý:

a) Theo mức độ nhạy cảm của thông tin:

Thông tin cá nhân cơ bản: Là những dữ liệu định danh thông thường như họ tên, ngày tháng năm sinh, giới tính, địa chỉ liên hệ, số điện thoại, email... Các thông tin này giúp xác định sơ bộ danh tính người tiêu dùng nhưng chưa thể hiện đặc điểm nhạy cảm.

Thông tin cá nhân nhạy cảm (sensitive personal data): Bao gồm thông tin tài chính, thẻ ngân hàng, mã số thuế, tình trạng sức khỏe, định vị vị trí, lịch sử tiêu dùng, thói quen mua sắm, sinh trắc học... Đây là nhóm thông tin dễ bị lợi dụng để thực hiện các hành vi xâm phạm quyền riêng tư, gian lận tài chính hoặc gây tổn hại đến đời sống cá nhân của người tiêu dùng.

b) Theo mục đích sử dụng trong thực tiễn thương mại:

Thông tin định danh người tiêu dùng: Dùng để xác thực danh tính người tiêu dùng, phục vụ quản lý tài khoản hoặc giao hàng (ví dụ: họ tên, địa chỉ, mã khách hàng, CMND/CCCD...).

Thông tin hành vi tiêu dùng: Thu thập trong quá trình sử dụng dịch vụ, lướt web, mua hàng trực tuyến... nhằm phân tích sở thích, thói quen, hành vi tiêu dùng (ví dụ: thời điểm mua hàng, danh mục ưa thích, sản phẩm thường tìm kiếm...).

Thông tin tài chính: Bao gồm số tài khoản ngân hàng, thẻ tín dụng, lịch sử giao dịch, điểm tín dụng... thường được sử dụng trong hoạt động thanh toán, vay tiêu dùng hoặc xác định mức độ tin cậy tín dụng.

Sự phân loại nêu trên cho thấy, **mỗi nhóm thông tin có giá trị và độ nhạy cảm khác nhau**, từ đó đòi hỏi **mức độ bảo vệ pháp lý tương ứng** trong từng trường hợp cụ thể.

Như vậy có thể thấy, thông tin người tiêu dùng là một loại dữ liệu đặc thù, phản ánh các khía cạnh cá nhân, hành vi và nhu cầu tiêu dùng trong xã hội hiện đại. Thông tin này không chỉ có giá trị về mặt nhận diện mà còn mang tính chiến lược đối với các hoạt động kinh doanh. Chính vì vậy, việc nhận diện rõ khái niệm, phân loại và đặc điểm của thông tin người tiêu dùng là tiền đề quan trọng để xây dựng khung pháp lý bảo vệ phù hợp, cân bằng giữa quyền riêng tư của người tiêu dùng và quyền thu thập, xử lý dữ liệu của doanh nghiệp trong nền kinh tế số.

1.2. Khái quát về bảo vệ thông tin người tiêu dùng

1.2.1. Khái niệm bảo vệ thông tin người tiêu dùng

Trong nền kinh tế số hiện đại, thông tin cá nhân – đặc biệt là thông tin tiêu dùng – đã trở thành một loại tài sản giá trị, có thể bị thu thập, phân tích, thương mại hóa một cách dễ dàng. Chính vì vậy, nhu cầu đặt ra một cơ chế pháp lý hữu hiệu để bảo vệ thông tin người tiêu dùng đang trở nên ngày càng cấp bách, cả trên phạm vi quốc gia lẫn toàn cầu.

Theo Khoản 15 Điều 3 Luật Bảo vệ quyền lợi người tiêu dùng sửa đổi năm 2023 (có hiệu lực từ ngày 1/7/2024), thông tin người tiêu dùng được định nghĩa là: *“Thông tin do người tiêu dùng cung cấp hoặc hình thành trong quá trình tham gia giao dịch, sử dụng hàng hóa, dịch vụ, bao gồm thông tin cá nhân và thông tin khác có liên quan đến người tiêu dùng.”* Từ khái niệm này, có thể hiểu rằng bảo vệ thông tin người tiêu dùng là việc thiết lập và áp dụng hệ thống các quy tắc pháp lý và kỹ thuật nhằm đảm bảo an toàn, bảo mật và quyền kiểm soát của người tiêu dùng đối với dữ liệu cá nhân và dữ liệu hành vi tiêu dùng.

Trên bình diện quốc tế, Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR) – văn bản tiêu chuẩn cao nhất hiện nay về bảo vệ dữ liệu cá nhân – xác định tại Điều 5 rằng dữ liệu cá nhân phải được xử lý hợp pháp, công bằng và minh bạch; được thu thập cho các mục đích cụ thể, rõ ràng, và hợp pháp; và không được lưu giữ lâu hơn mức cần thiết¹. Như vậy, yêu cầu bảo vệ thông tin cá nhân – trong đó có người tiêu dùng – là nguyên tắc cốt lõi trong các hệ thống pháp lý hiện đại.

Từ những phân tích trên, có thể hiểu **bảo vệ thông tin người tiêu dùng** là:

Tổng thể các quy phạm pháp luật, biện pháp kỹ thuật, tổ chức và đạo đức nghề nghiệp được áp dụng bởi các chủ thể có liên quan trong mối quan hệ tiêu dùng, nhằm bảo đảm rằng thông tin của người tiêu dùng – bao gồm cả dữ liệu cá nhân và dữ liệu hành vi tiêu dùng – được thu thập, xử lý, lưu trữ và chia sẻ một cách hợp pháp, chính đáng, minh bạch và an toàn, không xâm phạm đến quyền riêng tư, danh dự và lợi ích hợp pháp của người tiêu dùng.

¹ Nguồn: Điều 5 GDPR: <https://gdpr-info.eu/art-5-gdpr/>

1.2.2. Đặc điểm của bảo vệ thông tin người tiêu dùng

Tính pháp lý: Đây là lĩnh vực được điều chỉnh bởi hệ thống pháp luật cả công lẫn tư, trong đó nổi bật là Luật Bảo vệ quyền lợi người tiêu dùng (2010, sửa đổi 2023), Luật An ninh mạng (2018), Luật An toàn thông tin mạng (2015), Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, cùng với các quy định xử phạt trong Nghị định 98/2020/NĐ-CP về xử phạt vi phạm thương mại.

Tính chất phòng ngừa và bảo đảm quyền kiểm soát: Bảo vệ thông tin không chỉ nhằm ngăn ngừa việc lạm dụng thông tin, mà còn đảm bảo người tiêu dùng có quyền tra cứu, yêu cầu sửa đổi, cập nhật, hoặc xóa bỏ thông tin của mình. Quyền này được công nhận tại Điều 12 Nghị định 13/2023/NĐ-CP.

Tính phụ thuộc vào công nghệ: Việc bảo vệ dữ liệu cá nhân, nhất là trong môi trường thương mại điện tử và dịch vụ số, phụ thuộc rất lớn vào hạ tầng công nghệ và năng lực kỹ thuật số của doanh nghiệp.

Tính tương tác đa chủ thể: Ngoài Nhà nước, còn có sự tham gia của doanh nghiệp, tổ chức xã hội và bản thân người tiêu dùng trong quá trình bảo vệ và quản lý thông tin cá nhân.

Tính quốc tế hóa: Bảo vệ thông tin người tiêu dùng ngày càng chịu ảnh hưởng từ các chuẩn mực quốc tế như GDPR² (EU), Đạo luật Bảo vệ quyền riêng tư của người tiêu dùng bang California (CCPA³ – Mỹ), hay Hướng dẫn về bảo vệ người tiêu dùng trong thương mại điện tử của UNCTAD⁴ và OECD⁵.

1.2.3. Phân loại bảo vệ thông tin người tiêu dùng

Tùy theo cách tiếp cận và mục tiêu điều chỉnh, có thể phân loại bảo vệ thông tin người tiêu dùng theo các tiêu chí sau:

Theo chủ thể bảo vệ:

Bảo vệ bởi Nhà nước: Thể hiện qua việc ban hành pháp luật, xây dựng chính sách, thanh tra, kiểm tra và xử phạt. Ví dụ, theo Điều 34 Luật Bảo vệ quyền lợi người

² Nguồn: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

³ Nguồn: <https://oag.ca.gov/privacy/ccpa>

⁴ Nguồn: <https://unctad.org/topic/competition-and-consumer-protection/un-guidelines-on-consumer-protection>

⁵ Nguồn: <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>

tiêu dùng sửa đổi 2023, Bộ Công Thương có trách nhiệm quản lý nhà nước về bảo vệ quyền lợi người tiêu dùng, bao gồm cả thông tin cá nhân.

Bảo vệ bởi tổ chức, doanh nghiệp: Các doanh nghiệp, đặc biệt là doanh nghiệp thương mại điện tử, có trách nhiệm thiết lập chính sách bảo mật rõ ràng, thu thập dữ liệu đúng mục đích, bảo đảm an toàn dữ liệu theo Điều 14 và Điều 16 của Nghị định 13/2023/NĐ-CP.

Bảo vệ bởi người tiêu dùng: Thể hiện ở ý thức cảnh giác, sử dụng công cụ kiểm soát dữ liệu cá nhân, và khi cần thiết, khởi kiện hoặc yêu cầu cơ quan có thẩm quyền can thiệp khi quyền lợi bị xâm hại (Điều 8 Luật BVQLNTD 2023).

Theo phương thức bảo vệ:

Pháp lý: Thông qua hệ thống luật, quy định, điều khoản hợp đồng và các công cụ pháp lý khác.

Kỹ thuật: Áp dụng các công nghệ bảo mật như mã hóa, tường lửa, công nghệ xác thực đa yếu tố (MFA), công nghệ blockchain, v.v.

Tổ chức – quản trị: Thiết lập quy trình kiểm soát nội bộ, chính sách an ninh thông tin, kiểm toán dữ liệu, đào tạo nhân sự về bảo vệ dữ liệu cá nhân.

Theo giai đoạn xử lý thông tin:

Giai đoạn thu thập: Phải có sự đồng ý rõ ràng, cụ thể từ người tiêu dùng (Điều 11 Nghị định 13/2023/NĐ-CP).

Giai đoạn lưu trữ và xử lý: Chỉ sử dụng đúng mục đích, không chia sẻ cho bên thứ ba nếu chưa có sự đồng ý.

Giai đoạn xóa bỏ hoặc chuyển giao: Người tiêu dùng có quyền yêu cầu xóa hoặc chuyển dữ liệu, trừ trường hợp bị giới hạn theo luật định (Điều 19 Nghị định 13/2023/NĐ-CP).

1.2.4. Sự cần thiết bảo vệ thông tin người tiêu dùng

Việc bảo vệ thông tin người tiêu dùng là yêu cầu tất yếu trong sự phát triển của xã hội số, thể hiện qua các khía cạnh sau:

Thứ nhất, thông tin cá nhân là một phần của quyền con người. Quyền được bảo vệ đời sống riêng tư, bao gồm dữ liệu cá nhân, được ghi nhận tại Công ước quốc tế về các quyền dân sự và chính trị (ICCPR, Điều 17)⁶, Hiến pháp Việt Nam 2013 (Điều 21), và được cụ thể hóa tại nhiều văn bản pháp luật hiện hành.

Thứ hai, tình trạng lạm dụng, rò rỉ, mua bán trái phép dữ liệu cá nhân đang gia tăng nghiêm trọng. Báo cáo của Kaspersky năm 2023 cho thấy Việt Nam là một trong những quốc gia đứng đầu Đông Nam Á về số lượng vụ rò rỉ dữ liệu người dùng. Nhiều trường hợp bị gọi điện lừa đảo, tin nhắn quảng cáo rác, giả mạo danh tính để vay nợ... đều bắt nguồn từ việc thông tin tiêu dùng bị thu thập và sử dụng trái phép.

Thứ ba, bảo vệ thông tin là điều kiện để thúc đẩy thương mại điện tử và chuyển đổi số. Nếu người tiêu dùng cảm thấy không an toàn, họ sẽ từ chối giao dịch trực tuyến. Do đó, việc xây dựng hệ thống bảo vệ dữ liệu mạnh mẽ là nền tảng để phát triển kinh tế số bền vững.

Thứ tư, bảo vệ dữ liệu cá nhân là yêu cầu của các FTA thế hệ mới. Các hiệp định như CPTPP (Điều 14.8) và EVFTA đều yêu cầu các quốc gia thành viên có cơ chế bảo vệ dữ liệu cá nhân, bao gồm quyền được thông báo, quyền truy cập và sửa đổi dữ liệu, cũng như quyền yêu cầu xóa dữ liệu.

Thứ năm, xu thế toàn cầu hóa đòi hỏi Việt Nam phải hội nhập với các chuẩn mực quốc tế về dữ liệu. Nếu không có khung pháp lý phù hợp, Việt Nam sẽ bị xem là “quốc gia không an toàn về dữ liệu”, ảnh hưởng đến khả năng thu hút đầu tư, đặc biệt là trong lĩnh vực công nghệ, tài chính và thương mại điện tử.

1.3. Pháp luật của một số khu vực và quốc gia trên thế giới về bảo vệ thông tin người tiêu dùng

1.3.1. Pháp luật về bảo vệ thông tin người tiêu dùng của Liên minh châu Âu

Liên minh châu Âu là một trong những khu vực đi đầu trong việc xây dựng và thực thi các quy định pháp lý toàn diện về bảo vệ dữ liệu cá nhân. Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation – GDPR⁷), có hiệu lực từ ngày

⁶ Nguồn: Điều 17 trong Công ước Quốc tế về các Quyền Dân sự và Chính trị (ICCPR):

<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

⁷ Nguồn: <https://gdpr-info.eu/art-5-gdpr/>

25/5/2018, là văn bản pháp luật có tính ràng buộc cao, áp dụng cho toàn bộ 27 quốc gia thành viên EU và cả các tổ chức ngoài EU nếu xử lý dữ liệu cá nhân của công dân EU.

GDPR đặt ra các nguyên tắc nền tảng trong việc xử lý dữ liệu cá nhân, bao gồm: hợp pháp, công bằng và minh bạch; giới hạn mục đích sử dụng; tối thiểu hóa dữ liệu; tính chính xác; giới hạn thời gian lưu trữ; và bảo mật dữ liệu. Đặc biệt, Điều 5 GDPR nêu rõ dữ liệu cá nhân phải được thu thập cho các mục đích cụ thể, hợp pháp và minh bạch, đồng thời phải được bảo vệ khỏi truy cập trái phép hoặc rò rỉ.

Một điểm nổi bật của GDPR là quy định quyền của chủ thể dữ liệu, bao gồm quyền được thông báo, quyền truy cập, quyền yêu cầu chỉnh sửa, xóa bỏ dữ liệu (“right to be forgotten”), quyền phản đối và quyền di chuyển dữ liệu (data portability). Các doanh nghiệp vi phạm có thể bị phạt đến 20 triệu euro hoặc 4% doanh thu toàn cầu hàng năm, tùy theo mức nào cao hơn.

1.3.2. Pháp luật về bảo vệ thông tin người tiêu dùng của Nhật Bản

Nhật Bản là quốc gia châu Á đầu tiên xây dựng luật bảo vệ dữ liệu cá nhân sớm và hệ thống hóa bài bản. Luật Bảo vệ Thông tin Cá nhân (Act on the Protection of Personal Information – APPI⁸) được ban hành từ năm 2003 và được sửa đổi đáng kể vào các năm 2015, 2017 và 2020. APPI áp dụng cho cả doanh nghiệp trong và ngoài Nhật Bản, nếu xử lý dữ liệu của cá nhân tại Nhật.

Luật APPI quy định rằng các tổ chức phải nêu rõ mục đích sử dụng dữ liệu cá nhân trước khi thu thập và không được thay đổi mục đích này nếu không có sự đồng ý của chủ thể dữ liệu. Ngoài ra, luật còn đưa ra giới hạn nghiêm ngặt với việc chia sẻ dữ liệu cho bên thứ ba, trừ khi có sự chấp thuận hoặc các điều kiện pháp lý rõ ràng.

Một điểm đáng chú ý là Nhật Bản đã đạt được sự công nhận “mức độ bảo vệ dữ liệu tương đương” với GDPR của EU, tạo điều kiện cho việc luân chuyển dữ liệu xuyên biên giới. Điều này khẳng định sự tương thích cao của pháp luật Nhật Bản với các chuẩn mực quốc tế.

1.3.3. Pháp luật về bảo vệ thông tin người tiêu dùng của Singapore

Singapore ban hành Luật Bảo vệ Dữ liệu Cá nhân (Personal Data Protection Act

⁸ Nguồn: <https://www.ppc.go.jp/en/legal/>

– PDPA⁹) vào năm 2012 và đã sửa đổi quan trọng vào năm 2020. PDPA điều chỉnh cách các tổ chức thu thập, sử dụng, tiết lộ và bảo vệ dữ liệu cá nhân của cá nhân tại Singapore. Luật này do Cơ quan Bảo vệ Dữ liệu Cá nhân Singapore (Personal Data Protection Commission – PDPC) giám sát và thực thi.

PDPA quy định 11 nghĩa vụ chính đối với các tổ chức, bao gồm: nghĩa vụ đồng ý (Consent Obligation), thông báo (Notification), mục đích (Purpose Limitation), truy cập và chỉnh sửa (Access and Correction), bảo mật (Protection), giữ lại (Retention), và trách nhiệm giải trình (Accountability). Các doanh nghiệp phải triển khai các biện pháp kỹ thuật và tổ chức phù hợp nhằm bảo vệ thông tin cá nhân khỏi bị truy cập trái phép, mất mát hoặc hư hại.

Một điểm mới trong sửa đổi PDPA 2020 là việc cho phép xử lý dữ liệu cá nhân mà không cần sự đồng ý trong một số tình huống nhất định như lợi ích hợp pháp, đồng thời tăng mức phạt tối đa lên đến 1 triệu SGD cho các vi phạm nghiêm trọng.

⁹ Nguồn: <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>

KẾT LUẬN CHƯƠNG 1

Tại chương 1 với nội dung nghiên cứu về một số vấn đề lý luận về bảo vệ thông tin NTD, tác giả đề án đã phân tích và đưa ra những kết luận sau:

Thứ nhất, thông tin người tiêu dùng được hiểu là những dữ liệu định danh hoặc có thể định danh liên quan đến cá nhân trong quá trình tham gia giao dịch, tiêu dùng sản phẩm, dịch vụ. Thông tin này có thể được phân loại thành thông tin cơ bản, thông tin nhạy cảm và thông tin hành vi tiêu dùng. Đặc điểm của thông tin người tiêu dùng là tính cá nhân, dễ bị khai thác trái phép, khó kiểm soát và có giá trị kinh tế lớn.

Thứ hai, việc bảo vệ thông tin người tiêu dùng là một yêu cầu tất yếu trong nền kinh tế số và xã hội hiện đại. Khái niệm này phản ánh tổng thể các biện pháp pháp lý, kỹ thuật và hành chính nhằm đảm bảo thông tin cá nhân không bị thu thập, sử dụng, tiết lộ hoặc khai thác trái phép. Bảo vệ thông tin có thể được phân loại theo phạm vi pháp lý (bảo vệ bằng pháp luật dân sự, hình sự, hành chính...) hoặc theo đối tượng thực hiện (nhà nước, doanh nghiệp, cá nhân). Sự cần thiết của việc bảo vệ thông tin đến từ nguy cơ rủi ro, mất kiểm soát dữ liệu, ảnh hưởng quyền riêng tư và uy tín xã hội của cá nhân.

Thứ ba, pháp luật của các nước như Liên minh châu Âu, Nhật Bản và Singapore đều cho thấy xu hướng đề cao quyền kiểm soát dữ liệu của người tiêu dùng và nâng cao trách nhiệm pháp lý của tổ chức thu thập – xử lý thông tin. GDPR của EU nổi bật với cơ chế đồng ý minh bạch, trách nhiệm giải trình và xử phạt nghiêm khắc. Nhật Bản chú trọng cân bằng giữa bảo vệ dữ liệu và thương mại quốc tế, trong khi Singapore áp dụng mô hình linh hoạt, thực tiễn, phù hợp với môi trường doanh nghiệp năng động. Các mô hình pháp lý này là cơ sở tham khảo quan trọng cho Việt Nam trong quá trình hoàn thiện pháp luật về bảo vệ thông tin người tiêu dùng.

CHƯƠNG 2

QUY ĐỊNH CỦA PHÁP LUẬT VIỆT NAM VỀ BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG

2.1. Quy định của pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng

2.1.1. Quy định về nhận diện thông tin người tiêu dùng

Trong bối cảnh chuyển đổi số và sự bùng nổ của các hoạt động thương mại điện tử, thông tin của người tiêu dùng ngày càng trở thành đối tượng của nhiều hành vi thu thập, xử lý, khai thác, chia sẻ trái phép. Do đó, việc nhận diện đúng và đầy đủ thông tin người tiêu dùng là nền tảng để xây dựng khung pháp lý bảo vệ phù hợp và hiệu quả.

Theo khoản 1 Điều 3 **Luật Bảo vệ quyền lợi người tiêu dùng năm 2023**, *“Thông tin của người tiêu dùng là thông tin cá nhân hoặc thông tin phát sinh trong quá trình tiêu dùng, có thể xác định được danh tính của người tiêu dùng, bao gồm thông tin về nhân thân, thông tin tài chính, thông tin giao dịch, hành vi tiêu dùng và các loại thông tin khác theo quy định của pháp luật.”* Định nghĩa này mở rộng phạm vi không chỉ bao gồm các dữ liệu nhân thân như tên, địa chỉ, số điện thoại, mà còn bao gồm cả dữ liệu phát sinh trong quá trình mua sắm, phản ánh thói quen, xu hướng tiêu dùng, hành vi trực tuyến... Những dạng thông tin này đều có giá trị cao trong hoạt động phân tích thị trường, quảng cáo, cá nhân hóa dịch vụ và cũng tiềm ẩn nguy cơ xâm phạm nghiêm trọng đến quyền riêng tư nếu bị khai thác trái phép.

Để làm rõ nội hàm khái niệm thông tin người tiêu dùng, có thể đối chiếu với định nghĩa thông tin cá nhân tại khoản 4 Điều 2 **Luật An ninh mạng năm 2018**: *“Thông tin cá nhân là thông tin gắn liền với việc xác định danh tính của một người cụ thể, bao gồm tên, ngày tháng năm sinh, nghề nghiệp, địa chỉ thường trú, số điện thoại, địa chỉ thư điện tử, số CMND, số tài khoản ngân hàng...”*.

Đặc biệt, với sự ra đời của **Nghị định số 13/2023/NĐ-CP** về bảo vệ dữ liệu cá nhân, khái niệm và phân loại thông tin cá nhân – trong đó có thông tin người tiêu dùng – đã được quy định rõ ràng và chi tiết hơn. Khoản 4 Điều 2 của Nghị định phân chia thông tin cá nhân thành hai nhóm:

Thông tin cá nhân cơ bản: bao gồm họ tên, giới tính, ngày tháng năm sinh, dân tộc, quốc tịch, số CMND/CCCD, địa chỉ thường trú, email, số điện thoại...

Thông tin cá nhân nhạy cảm: bao gồm dữ liệu về sức khỏe, tài chính, đời sống riêng tư, quan điểm chính trị, định vị địa lý, dữ liệu sinh trắc học...

Việc phân loại như vậy giúp Nhà nước và các chủ thể có liên quan xác định được mức độ rủi ro và áp dụng các biện pháp bảo vệ thông tin tương ứng. Trong thương mại điện tử, thông tin nhạy cảm của người tiêu dùng như lịch sử mua hàng, vị trí GPS, tài khoản ngân hàng, thói quen truy cập... thường bị thu thập thông qua cookies, phần mềm hoặc hành vi trực tuyến. Do đó, cần được nhận diện đúng để có cơ chế bảo vệ thích đáng.

Ngoài ra, theo Điều 15 **Luật Bảo vệ quyền lợi người tiêu dùng năm 2023**, tổ chức, cá nhân kinh doanh hàng hóa, dịch vụ chỉ được phép thu thập thông tin người tiêu dùng khi đã có **sự đồng ý rõ ràng, cụ thể và minh bạch** từ phía người tiêu dùng. Thông tin thu thập phải phục vụ đúng mục đích ban đầu đã công bố và không được sử dụng cho mục đích khác nếu không được sự chấp thuận lại từ người tiêu dùng.

Trong lĩnh vực viễn thông và công nghệ thông tin, Thông tư số 38/2016/TT-BTTTT của Bộ Thông tin và Truyền thông cũng yêu cầu các doanh nghiệp cung cấp dịch vụ mạng phải có chính sách bảo mật, đồng thời thông báo rõ ràng về mục đích, phạm vi và thời gian lưu trữ thông tin cá nhân.

Ngoài các quy định mang tính chung, một số ngành nghề cụ thể như tài chính, ngân hàng, y tế cũng có quy định riêng để nhận diện và bảo vệ thông tin khách hàng. Chẳng hạn, **Thông tư số 20/2019/TT-NHNN** quy định rõ các loại thông tin mà tổ chức tín dụng được phép thu thập khi khách hàng mở tài khoản hoặc vay vốn, bao gồm dữ liệu nhân thân, dữ liệu tài chính và mục đích sử dụng vốn.

Tóm lại, hệ thống pháp luật Việt Nam đã có những bước tiến quan trọng trong việc xây dựng khung pháp lý để nhận diện thông tin người tiêu dùng. Việc phân định rõ loại thông tin, phạm vi và hình thức sử dụng là cơ sở thiết yếu để điều chỉnh hành vi của các bên trong môi trường giao dịch hiện đại, đồng thời giúp tăng cường hiệu quả thực thi pháp luật trong bảo vệ quyền lợi người tiêu dùng

2.1.2. Quy định về xử lý, chuyển giao thông tin người tiêu dùng

Xử lý và chuyển giao thông tin cá nhân của người tiêu dùng là những hoạt động nhạy cảm, có ảnh hưởng trực tiếp đến quyền riêng tư, an toàn dữ liệu và lòng tin của người tiêu dùng đối với các tổ chức kinh doanh. Do vậy, pháp luật Việt Nam đã từng bước xây dựng khuôn khổ pháp lý để kiểm soát chặt chẽ các hoạt động này, phù hợp với nguyên tắc bảo vệ dữ liệu cá nhân trong bối cảnh kinh tế số.

Quy định chung về xử lý thông tin cá nhân

Khoản 6 Điều 2 **Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân** định nghĩa: *“Xử lý dữ liệu cá nhân là một hoặc nhiều hoạt động tác động đến dữ liệu cá nhân như thu thập, ghi chép, phân tích, xác minh, lưu trữ, thay đổi, cung cấp, chia sẻ, truy xuất, thu hồi, mã hóa, giải mã, hủy hoặc tiêu hủy dữ liệu cá nhân...”*

Đây là quy định pháp lý đầu tiên tại Việt Nam xác định rõ ràng khái niệm "xử lý dữ liệu cá nhân" với phạm vi toàn diện, giúp phân biệt giữa các giai đoạn khác nhau như thu thập – phân tích – lưu trữ – chuyển giao. Đặc biệt, tại **Điều 3 Nghị định này**, các nguyên tắc xử lý dữ liệu cá nhân được đề cập rõ ràng, gồm: tính hợp pháp, minh bạch, mục đích cụ thể, hạn chế xử lý, chính xác, bảo mật, lưu trữ có giới hạn và trách nhiệm giải trình.

Xử lý và chuyển giao thông tin người tiêu dùng theo Luật Bảo vệ quyền lợi người tiêu dùng

Điều 15 **Luật Bảo vệ quyền lợi người tiêu dùng năm 2023** quy định rất cụ thể về **việc thu thập, lưu trữ và sử dụng thông tin người tiêu dùng**, nhấn mạnh nguyên tắc:

Phải có **sự đồng ý rõ ràng và trước** của người tiêu dùng.

Tổ chức, cá nhân kinh doanh **phải thông báo công khai** về mục đích, phạm vi và hình thức xử lý thông tin.

Không được thu thập quá mức cần thiết hoặc ngoài phạm vi đã thông báo.

Phải bảo đảm an toàn thông tin và có biện pháp xử lý sự cố rò rỉ dữ liệu.

Tại **khoản 4 Điều 15**, luật còn yêu cầu doanh nghiệp khi muốn chia sẻ, cung cấp thông tin người tiêu dùng cho bên thứ ba **phải được sự đồng ý riêng biệt** từ người tiêu dùng, trừ các trường hợp luật định như phục vụ hoạt động điều tra, xét xử, thi hành án...

Đây là điểm tiến bộ so với Luật năm 2010, thể hiện sự tiệm cận với tiêu chuẩn quốc tế như GDPR của EU, trong đó yêu cầu **consent¹⁰ phải được xác lập rõ ràng, có thể rút lại, không gắn với điều kiện ép buộc**.

Quy định về chuyển giao thông tin ra nước ngoài

Một nội dung đặc biệt quan trọng được đề cập tại **Điều 11 Nghị định số 13/2023/NĐ-CP** là **việc chuyển dữ liệu cá nhân ra nước ngoài**. Theo đó, tổ chức, cá nhân muốn chuyển dữ liệu người tiêu dùng ra nước ngoài phải: Đăng ký với Bộ Công an; Có văn bản cam kết đảm bảo bảo vệ dữ liệu tương đương với tiêu chuẩn Việt Nam; Bảo đảm người tiêu dùng đã biết và đồng ý.

Đây là quy định mang tính bảo hộ cao, tương tự như nguyên tắc “adequacy” trong **GDPR**, khi dữ liệu người dân châu Âu chỉ được chuyển sang các quốc gia có mức bảo vệ tương đương.

Các hành vi bị cấm trong xử lý, chuyển giao thông tin người tiêu dùng

Điều 17 **Luật Bảo vệ quyền lợi người tiêu dùng năm 2023** nghiêm cấm các hành vi: Mua bán, trao đổi, tặng cho thông tin người tiêu dùng không có sự đồng ý; Sử dụng thông tin sai mục đích; Lợi dụng việc thu thập thông tin để quấy rối, đe dọa hoặc xâm hại quyền riêng tư; Không thực hiện nghĩa vụ bảo mật, không thông báo sự cố rò rỉ thông tin.

Ngoài ra, Điều 288 **Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung 2017)** quy định tội "Đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông", với mức phạt có thể lên đến **1 tỷ đồng hoặc 7 năm tù giam** trong trường hợp nghiêm trọng, có hành vi chiếm đoạt, buôn bán dữ liệu cá nhân.

Tóm lại, quy định pháp luật Việt Nam đã có bước phát triển rõ rệt về nội dung xử lý và chuyển giao thông tin người tiêu dùng, hướng đến nguyên tắc minh bạch, đồng

¹⁰ "Consent" (trong lĩnh vực bảo vệ dữ liệu cá nhân) được hiểu là **sự đồng ý rõ ràng, cụ thể, có ý thức và tự nguyện của chủ thể dữ liệu** cho phép tổ chức/cá nhân thu thập, xử lý hoặc chia sẻ thông tin cá nhân của họ.

thuận, hạn chế mục đích và bảo mật dữ liệu. Tuy nhiên, trong thực tế, việc triển khai và kiểm soát vẫn còn gặp nhiều thách thức như thiếu hướng dẫn kỹ thuật, năng lực thực thi hạn chế, sự phức tạp trong thương mại điện tử xuyên biên giới... Những vấn đề này sẽ được phân tích kỹ hơn ở phần **Đánh giá tại mục 2.2.**

2.1.3. Quy định về các hành vi xâm phạm thông tin người tiêu dùng

Trong nền kinh tế thị trường hiện đại, thông tin cá nhân của người tiêu dùng không chỉ đơn thuần là dữ liệu mà còn là tài sản có giá trị cao, có thể bị khai thác để phục vụ cho các mục đích kinh doanh, chính trị hoặc lừa đảo. Việc xâm phạm thông tin người tiêu dùng đang diễn ra ngày càng phổ biến, tinh vi và khó kiểm soát, đặc biệt trong môi trường thương mại điện tử và không gian mạng. Do đó, hệ thống pháp luật Việt Nam đã ghi nhận và từng bước hoàn thiện cơ chế pháp lý nhằm nhận diện, ngăn chặn và xử lý các hành vi xâm phạm thông tin người tiêu dùng, thông qua nhiều đạo luật chuyên ngành và quy định liên quan.

Xác định các hành vi xâm phạm thông tin người tiêu dùng

Theo khoản 3 Điều 6 của **Luật Bảo vệ quyền lợi người tiêu dùng năm 2010**, một nguyên tắc quan trọng là "Tổ chức, cá nhân kinh doanh hàng hóa, dịch vụ chỉ được thu thập, sử dụng, chuyển giao thông tin của người tiêu dùng khi được người tiêu dùng đồng ý." Quy định này tạo thành cơ sở pháp lý để xác định các hành vi vi phạm nguyên tắc thu thập và sử dụng thông tin, bao gồm:

Thu thập thông tin cá nhân mà không thông báo, không có sự đồng ý rõ ràng từ người tiêu dùng;

Sử dụng thông tin của người tiêu dùng vào mục đích ngoài phạm vi được người tiêu dùng cho phép;

Chuyển giao, tiết lộ thông tin của người tiêu dùng cho bên thứ ba khi chưa được đồng ý;

Không áp dụng các biện pháp bảo mật cần thiết, để lộ dữ liệu do lỗi hệ thống hoặc quản trị lỏng lẻo.

Cần nhấn mạnh rằng những hành vi này không chỉ vi phạm đạo đức kinh doanh mà còn vi phạm nghiêm trọng quyền riêng tư, quyền nhân thân của người tiêu dùng –

một quyền được pháp luật ghi nhận là bất khả xâm phạm (Điều 38 Bộ luật Dân sự 2015).

Quy định chi tiết tại Nghị định 117/2023/NĐ-CP

Nghị định số 117/2023/NĐ-CP có hiệu lực từ ngày 01/07/2024 được ban hành để hướng dẫn thi hành Luật Bảo vệ quyền lợi người tiêu dùng (sửa đổi), đã cụ thể hóa các hành vi xâm phạm thông tin người tiêu dùng. Theo đó, Điều 12 Nghị định quy định rõ:

“Tổ chức, cá nhân kinh doanh không được thực hiện việc thu thập, lưu trữ, xử lý, sử dụng, chuyển giao thông tin của người tiêu dùng khi chưa có sự đồng ý, trừ trường hợp được pháp luật cho phép”.

Đặc biệt, các hành vi bị cấm bao gồm:

Gửi tin nhắn, cuộc gọi, thư điện tử quảng cáo không mong muốn dựa trên thông tin cá nhân thu thập trái phép;

Sử dụng thông tin tiêu dùng để phân loại khách hàng, cá biệt hóa giá cả hoặc tạo rào cản cạnh tranh không lành mạnh;

Chuyển nhượng, bán lại dữ liệu cá nhân người tiêu dùng mà không được sự đồng ý hoặc không có cơ sở pháp lý rõ ràng.

Quy định này tiếp cận khá gần với tiêu chuẩn quốc tế như GDPR của EU, trong đó nguyên tắc “minimization” và “consent” được đặc biệt đề cao.

Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân

Dưới góc độ rộng hơn, Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân xác lập khung pháp lý toàn diện để điều chỉnh việc xử lý dữ liệu cá nhân, trong đó có dữ liệu của người tiêu dùng. Theo Điều 9 Nghị định:

“Mọi hoạt động xử lý dữ liệu cá nhân phải dựa trên một trong các căn cứ pháp lý hợp pháp, trong đó sự đồng ý của chủ thể dữ liệu là bắt buộc đối với mọi hành vi thu thập, lưu trữ, sử dụng và chuyển giao.”

Điều 10 và 11 quy định rõ các **hành vi bị nghiêm cấm**, bao gồm:

Tiết lộ dữ liệu cá nhân của người khác mà không có sự đồng ý;

Mua bán dữ liệu cá nhân dưới mọi hình thức;

Không thông báo rõ ràng về mục đích và phạm vi sử dụng thông tin cá nhân cho người tiêu dùng;

Cản trở hoặc không tạo điều kiện để người tiêu dùng thực hiện quyền truy cập, chỉnh sửa hoặc yêu cầu xóa dữ liệu.

Như vậy, với sự có mặt của Nghị định 13, các hành vi xâm phạm thông tin người tiêu dùng đã được xác định rõ và có cơ chế ngăn chặn cụ thể.

Các quy định trong Luật An ninh mạng 2018 và văn bản hướng dẫn

Luật An ninh mạng 2018 tiếp tục khẳng định tính nghiêm trọng của hành vi xâm phạm thông tin cá nhân, trong đó Điều 17 nêu rõ:

"Nghiêm cấm hành vi thu thập, khai thác, sử dụng, mua bán trái phép thông tin cá nhân của người khác trên không gian mạng."

Hành vi sử dụng công nghệ để chiếm đoạt dữ liệu người tiêu dùng (ví dụ: bằng phần mềm gián điệp, giả mạo ứng dụng, phishing...) bị xem là hành vi xâm phạm nghiêm trọng và có thể bị xử lý hình sự.

Đặc biệt, theo **Nghị định 53/2022/NĐ-CP**, doanh nghiệp nước ngoài cung cấp dịch vụ trên không gian mạng tại Việt Nam (như Facebook, Google, Shopee...) bắt buộc phải lưu trữ dữ liệu người dùng tại Việt Nam, có văn phòng đại diện và phối hợp với cơ quan chức năng khi có yêu cầu. Điều này nhằm hạn chế tình trạng rò rỉ thông tin ra nước ngoài và tăng cường khả năng xử lý vi phạm.

Chế tài xử lý hành vi xâm phạm

Hành vi xâm phạm thông tin người tiêu dùng có thể bị xử phạt **hành chính hoặc hình sự**, tùy theo mức độ:

Xử phạt hành chính: Theo **Điều 84 và 85 của Nghị định 98/2020/NĐ-CP**, hành vi tiết lộ, sử dụng trái phép thông tin khách hàng có thể bị phạt từ 10 triệu đến 70 triệu đồng, kèm biện pháp khắc phục như buộc tiêu hủy thông tin đã thu thập trái phép.

Xử lý hình sự: Bộ luật Hình sự 2015 (sửa đổi 2017) quy định tại: **Điều 288:** tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông; **Điều 159:**

tội xâm phạm bí mật thư tín, điện thoại, điện tín; **Điều 291**: tội phát tán chương trình tin học gây thiệt hại dữ liệu.

Người vi phạm có thể bị **phạt tiền đến 1 tỷ đồng hoặc phạt tù đến 7 năm** tùy theo hậu quả gây ra.

Tóm lại, các hành vi xâm phạm thông tin người tiêu dùng đã và đang trở thành mối đe dọa nghiêm trọng đối với quyền riêng tư và an toàn cá nhân của người dân. Trước thực trạng đó, hệ thống pháp luật Việt Nam đã không ngừng hoàn thiện, đưa ra các quy định ngày càng chi tiết, rõ ràng và có tính răn đe cao. Tuy nhiên, để các quy định này thực sự phát huy hiệu quả, cần có sự vào cuộc đồng bộ của các cơ quan chức năng, doanh nghiệp và chính người tiêu dùng thông qua việc nâng cao nhận thức, kỹ năng bảo vệ dữ liệu và phản ứng với hành vi vi phạm.

2.1.4. Quy định về các biện pháp bảo vệ thông tin người tiêu dùng

Việc bảo vệ thông tin người tiêu dùng không chỉ dừng lại ở việc xác định phạm vi thông tin được thu thập, hay xử lý thông tin một cách hợp pháp, mà còn đòi hỏi sự triển khai đồng bộ các biện pháp bảo vệ toàn diện, nhằm phòng ngừa, ngăn chặn và xử lý các nguy cơ xâm phạm thông tin cá nhân. Ở Việt Nam, hệ thống pháp luật hiện hành đã đưa ra nhiều quy định chi tiết về các biện pháp bảo vệ thông tin người tiêu dùng, vừa mang tính phòng ngừa, vừa có tính xử lý khi xảy ra vi phạm.

Biện pháp kỹ thuật bảo vệ thông tin

Các quy định pháp luật Việt Nam nhấn mạnh vai trò của các biện pháp kỹ thuật trong việc bảo đảm an toàn dữ liệu cá nhân, trong đó có thông tin người tiêu dùng. Cụ thể, theo quy định tại Điều 7, Luật An toàn thông tin mạng 2015, các tổ chức, doanh nghiệp phải thực hiện các biện pháp kỹ thuật bảo vệ dữ liệu, bao gồm: mã hóa dữ liệu, phân quyền truy cập, sử dụng phần mềm bảo mật, hệ thống phòng chống xâm nhập, sao lưu dữ liệu định kỳ và kiểm tra, giám sát chặt chẽ các hoạt động liên quan đến xử lý dữ liệu cá nhân. Việc áp dụng các biện pháp kỹ thuật này giúp ngăn chặn các hành vi xâm nhập, đánh cắp, thay đổi hoặc làm mất dữ liệu người tiêu dùng.

Ngoài ra, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân cũng quy định rõ ràng về yêu cầu áp dụng các biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ dữ liệu cá

nhân khỏi các nguy cơ mất mát, hư hỏng, truy cập trái phép, sử dụng sai mục đích hoặc tiết lộ trái phép. Cơ quan, tổ chức kinh doanh khi thu thập và xử lý thông tin người tiêu dùng phải thiết lập các hệ thống bảo mật thông tin, đào tạo nhân viên và định kỳ đánh giá rủi ro về bảo mật để kịp thời phát hiện và khắc phục lỗ hổng an ninh.

Biện pháp tổ chức và quản lý

Không chỉ dừng lại ở các biện pháp kỹ thuật, pháp luật Việt Nam còn yêu cầu các tổ chức, doanh nghiệp xây dựng và duy trì các biện pháp tổ chức để bảo vệ thông tin người tiêu dùng. Theo Thông tư 24/2022/TT-BTTTT của Bộ Thông tin và Truyền thông về quản lý và sử dụng dịch vụ Internet và thông tin trên mạng, các nền tảng kỹ thuật số phải xây dựng quy trình quản lý thông tin người dùng rõ ràng, đảm bảo lưu trữ, xử lý dữ liệu theo đúng quy định, đồng thời phải có đội ngũ chuyên trách hoặc phối hợp với các cơ quan chức năng để xử lý các vụ việc liên quan đến an ninh, bảo mật thông tin.

Các doanh nghiệp cũng cần có quy định nội bộ nghiêm ngặt về bảo mật thông tin, bao gồm việc phân công trách nhiệm rõ ràng cho cán bộ quản lý dữ liệu, đào tạo nhận thức về bảo vệ dữ liệu cá nhân cho toàn bộ nhân viên, đồng thời xây dựng quy trình xử lý khi xảy ra vi phạm để giảm thiểu thiệt hại và thông báo kịp thời cho người tiêu dùng và cơ quan quản lý nhà nước.

Quyền của người tiêu dùng và trách nhiệm của doanh nghiệp trong bảo vệ thông tin

Pháp luật Việt Nam bảo đảm quyền của người tiêu dùng trong việc kiểm soát thông tin cá nhân của mình thông qua các quy định cho phép người tiêu dùng được quyền truy cập, yêu cầu chỉnh sửa, cập nhật hoặc xóa bỏ thông tin sai lệch hoặc không còn phù hợp. Luật Bảo vệ quyền lợi người tiêu dùng năm 2010 (sửa đổi 2023) quy định doanh nghiệp có trách nhiệm thông báo rõ ràng cho người tiêu dùng về mục đích, phạm vi thu thập và sử dụng thông tin, đồng thời phải xin phép sự đồng ý một cách minh bạch trước khi thực hiện các hoạt động liên quan đến dữ liệu cá nhân.

Bên cạnh đó, doanh nghiệp còn có trách nhiệm bảo mật thông tin người tiêu dùng và không được tiết lộ, chuyển giao cho bên thứ ba nếu không được phép của người tiêu dùng hoặc không có quy định pháp luật cho phép. Khi có dấu hiệu rò rỉ, mất mát thông

tin, doanh nghiệp phải thông báo ngay cho người tiêu dùng và các cơ quan chức năng để phối hợp xử lý.

Yêu cầu lưu trữ và kiểm soát dữ liệu

Một điểm nổi bật trong quy định về biện pháp bảo vệ thông tin người tiêu dùng tại Việt Nam là yêu cầu về lưu trữ dữ liệu tại máy chủ trong nước, được quy định tại Nghị định 53/2022/NĐ-CP hướng dẫn Luật An ninh mạng. Theo đó, các doanh nghiệp trong và ngoài nước cung cấp dịch vụ tại Việt Nam bắt buộc phải lưu trữ dữ liệu người dùng Việt Nam trên lãnh thổ Việt Nam, nhằm tạo điều kiện thuận lợi cho việc kiểm tra, giám sát và xử lý vi phạm. Đây là một biện pháp quản lý quan trọng góp phần tăng cường chủ quyền số và giảm thiểu nguy cơ rò rỉ dữ liệu ra bên ngoài, đồng thời giúp tăng cường sự an toàn, tin cậy trong việc bảo vệ thông tin người tiêu dùng.

Các biện pháp pháp lý và chế tài xử lý

Bên cạnh các biện pháp kỹ thuật và tổ chức, hệ thống pháp luật Việt Nam còn quy định các chế tài xử phạt nghiêm minh nhằm răn đe, ngăn ngừa các hành vi vi phạm quyền riêng tư và bảo vệ thông tin người tiêu dùng. Các hành vi vi phạm về bảo vệ thông tin cá nhân sẽ bị xử phạt hành chính theo Nghị định 98/2020/NĐ-CP với mức phạt có thể lên đến hàng trăm triệu đồng, tùy theo tính chất và mức độ vi phạm. Trong trường hợp nghiêm trọng, vi phạm còn có thể bị truy cứu trách nhiệm hình sự theo Bộ luật Hình sự 2015 sửa đổi, bổ sung 2017.

Việc áp dụng đồng bộ các biện pháp phòng ngừa và xử lý này tạo thành một hệ thống liên hoàn, giúp nâng cao hiệu quả bảo vệ thông tin người tiêu dùng trước các nguy cơ xâm phạm ngày càng tinh vi, phức tạp trong kỷ nguyên số.

Tổng hợp lại, hệ thống quy định pháp luật Việt Nam về các biện pháp bảo vệ thông tin người tiêu dùng tập trung vào ba nhóm chính: (i) các biện pháp kỹ thuật bảo vệ an toàn thông tin như mã hóa, phân quyền truy cập và giám sát hệ thống; (ii) các biện pháp tổ chức, quản lý như quy trình lưu trữ, đào tạo nhân sự và xử lý vi phạm; (iii) quyền của người tiêu dùng được bảo đảm với các cơ chế kiểm soát và doanh nghiệp phải tuân thủ nghiêm các nghĩa vụ pháp lý. Đặc biệt, các quy định về lưu trữ dữ liệu tại máy chủ trong nước và chế tài xử lý vi phạm góp phần tạo dựng một môi trường pháp lý vững chắc, tăng cường sự tin cậy và bảo vệ quyền lợi người tiêu dùng trong bối cảnh phát

triển nhanh chóng của công nghệ số.

2.2. Đánh giá quy định của pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng

Việc bảo vệ thông tin người tiêu dùng là một trong những yêu cầu cấp thiết và mang tính toàn cầu trong bối cảnh cách mạng công nghiệp 4.0 và nền kinh tế số phát triển mạnh mẽ. Pháp luật Việt Nam trong những năm gần đây đã có nhiều bước tiến quan trọng nhằm hoàn thiện khuôn khổ pháp lý bảo vệ thông tin cá nhân nói chung và thông tin người tiêu dùng nói riêng. Tuy nhiên, khi nhìn nhận toàn diện về các quy định hiện hành, cần có một cái nhìn đánh giá khách quan, vừa khẳng định những thành tựu đã đạt được, vừa chỉ ra những hạn chế và thách thức cần khắc phục để nâng cao hiệu quả bảo vệ thông tin người tiêu dùng trong tương lai.

Những điểm mạnh của pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng

Trước hết, có thể thấy sự đồng bộ và tiến bộ trong hệ thống pháp luật liên quan đến bảo vệ thông tin cá nhân và thông tin người tiêu dùng. Các văn bản như Luật An toàn thông tin mạng 2015, Luật Bảo vệ quyền lợi người tiêu dùng 2010 (sửa đổi, bổ sung năm 2023), Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, Nghị định 53/2022/NĐ-CP về an ninh mạng, và các Thông tư hướng dẫn đã tạo thành một khung pháp lý tương đối hoàn chỉnh. Các quy định này đã thể hiện rõ nguyên tắc xử lý dữ liệu cá nhân một cách hợp pháp, minh bạch, tôn trọng quyền của người tiêu dùng, đồng thời yêu cầu các doanh nghiệp phải chịu trách nhiệm cao trong việc bảo vệ thông tin.

Ngoài ra, các quy định về biện pháp kỹ thuật và tổ chức bảo vệ thông tin đã được chú trọng, đảm bảo rằng doanh nghiệp, tổ chức phải xây dựng hệ thống bảo mật đồng bộ, áp dụng các công nghệ tiên tiến để ngăn ngừa rủi ro. Việc yêu cầu lưu trữ dữ liệu người dùng trong nước (Nghị định 53/2022/NĐ-CP) là một bước đi quan trọng giúp tăng cường kiểm soát, nâng cao năng lực giám sát và xử lý vi phạm. Đây cũng là giải pháp góp phần đảm bảo chủ quyền số quốc gia, tạo dựng lòng tin cho người tiêu dùng khi tham gia vào nền kinh tế số.

Bên cạnh đó, việc quy định rõ ràng quyền của người tiêu dùng trong việc kiểm soát thông tin cá nhân của mình (quyền truy cập, chỉnh sửa, hủy bỏ thông tin) đã tạo nên

sự cân bằng quyền lực giữa người tiêu dùng và tổ chức, doanh nghiệp. Điều này không chỉ bảo vệ người tiêu dùng khỏi các hành vi xâm phạm mà còn thúc đẩy văn hóa minh bạch và trách nhiệm trong xử lý dữ liệu.

Những hạn chế và những thách thức đặt ra

Mặc dù đạt được nhiều tiến bộ, hệ thống pháp luật về bảo vệ thông tin người tiêu dùng của Việt Nam vẫn còn một số hạn chế cần được nhìn nhận và giải quyết.

Thứ nhất, tính đồng bộ và khả năng áp dụng thực tiễn của các quy định chưa thực sự hiệu quả. Một số văn bản pháp luật, như Luật Bảo vệ quyền lợi người tiêu dùng và Luật An toàn thông tin mạng, còn có các quy định chung chung, chưa cụ thể hóa rõ ràng các hành vi vi phạm và biện pháp xử lý tương ứng. Điều này dẫn đến khó khăn trong việc áp dụng thống nhất, tạo khoảng trống pháp lý cho một số hành vi vi phạm tinh vi, đặc biệt trong môi trường thương mại điện tử và các nền tảng số phức tạp.

Thứ hai, quy định về quyền của người tiêu dùng còn hạn chế ở khía cạnh thực thi. Trên thực tế, người tiêu dùng thường gặp khó khăn trong việc phát hiện, chứng minh và yêu cầu xử lý các hành vi xâm phạm thông tin cá nhân của mình. Thiếu các kênh hỗ trợ pháp lý và cơ chế khiếu nại, tố cáo hiệu quả khiến cho quyền lợi người tiêu dùng chưa được bảo vệ đầy đủ. Ngoài ra, nhận thức của người tiêu dùng về quyền riêng tư và bảo vệ dữ liệu cá nhân vẫn còn hạn chế, gây ra nguy cơ tự nguyện cung cấp thông tin cá nhân không cần thiết và dễ bị lợi dụng.

Thứ ba, năng lực của các cơ quan quản lý nhà nước còn nhiều thách thức trong việc kiểm soát, giám sát và xử lý vi phạm liên quan đến bảo vệ thông tin người tiêu dùng. Việc phối hợp giữa các cơ quan trong quản lý và xử lý sự cố bảo mật chưa thực sự chặt chẽ, chưa có các hệ thống cảnh báo sớm hiệu quả để phòng ngừa các nguy cơ rò rỉ, tấn công mạng. Đồng thời, các cơ chế hợp tác quốc tế trong bảo vệ dữ liệu cá nhân vẫn còn hạn chế, trong khi thông tin người tiêu dùng có thể bị lưu chuyển xuyên biên giới, đòi hỏi sự phối hợp sâu rộng hơn.

Thứ tư, quy định về lưu trữ dữ liệu tại máy chủ trong nước, mặc dù có nhiều lợi ích nhưng cũng đặt ra thách thức lớn về mặt kỹ thuật, chi phí và quyền tự do kinh doanh của doanh nghiệp. Việc áp đặt này có thể làm gia tăng gánh nặng về chi phí đầu tư cơ sở hạ tầng cho doanh nghiệp, đặc biệt là các doanh nghiệp vừa và nhỏ, đồng thời làm

giảm tính linh hoạt trong việc quản lý và khai thác dữ liệu toàn cầu.

Các khuyến nghị nhằm hoàn thiện hệ thống pháp luật và nâng cao hiệu quả bảo vệ thông tin người tiêu dùng

Để khắc phục các hạn chế trên, pháp luật Việt Nam cần tiếp tục hoàn thiện theo hướng rõ ràng, cụ thể và đồng bộ hơn, đồng thời tăng cường các biện pháp thực thi. Cụ thể, cần sửa đổi, bổ sung các văn bản pháp luật liên quan để làm rõ hơn các khái niệm, quy trình xử lý dữ liệu, cũng như các hình thức vi phạm và chế tài tương ứng, nhằm giảm thiểu khoảng trống pháp lý.

Đồng thời, cần xây dựng và hoàn thiện hệ thống cơ chế hỗ trợ người tiêu dùng trong việc bảo vệ quyền lợi cá nhân như các trung tâm tư vấn, giải quyết tranh chấp về dữ liệu, cơ chế khiếu nại tố cáo minh bạch và thuận tiện. Cần đẩy mạnh công tác truyền thông, giáo dục nâng cao nhận thức cộng đồng về quyền riêng tư và bảo vệ thông tin cá nhân để người tiêu dùng chủ động hơn trong việc bảo vệ thông tin của mình.

Bên cạnh đó, tăng cường năng lực quản lý nhà nước về bảo vệ dữ liệu cá nhân bằng việc đầu tư trang thiết bị, đào tạo nhân lực chuyên môn, thiết lập các hệ thống cảnh báo, giám sát an ninh mạng hiện đại và phối hợp hiệu quả với các cơ quan liên quan trong nước cũng như quốc tế.

Cuối cùng, cần có các chính sách hỗ trợ doanh nghiệp trong việc xây dựng hạ tầng lưu trữ, bảo mật thông tin phù hợp, giảm bớt gánh nặng tài chính và kỹ thuật, đồng thời tạo môi trường cạnh tranh công bằng, khuyến khích đổi mới sáng tạo trong lĩnh vực bảo vệ dữ liệu.

Tổng quát lại, Pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng đã và đang có những bước tiến đáng ghi nhận, tạo nền tảng pháp lý quan trọng trong bảo vệ quyền riêng tư của người dân trong bối cảnh công nghệ số bùng nổ. Tuy nhiên, trước sự phát triển nhanh chóng và phức tạp của các hình thức thu thập, xử lý thông tin, việc nâng cao tính cụ thể, khả thi trong quy định pháp luật, tăng cường thực thi và nhận thức xã hội là điều kiện tiên quyết để nâng cao hiệu quả bảo vệ thông tin người tiêu dùng trong thực tiễn.

Việc hoàn thiện pháp luật không chỉ góp phần bảo vệ quyền lợi người tiêu dùng

mà còn là yếu tố thúc đẩy phát triển kinh tế số bền vững, xây dựng niềm tin của người tiêu dùng vào các nền tảng số và doanh nghiệp, đồng thời bảo đảm an ninh quốc gia trên không gian mạng.

KẾT LUẬN CHƯƠNG 2

Chương 2 của luận văn đã tập trung phân tích một cách hệ thống và toàn diện các quy định pháp luật hiện hành của Việt Nam liên quan đến bảo vệ thông tin người tiêu dùng. Thông qua việc phân tích từng nhóm quy phạm, có thể thấy rằng hệ thống pháp luật Việt Nam đã ghi nhận một cách khá rõ nét các quyền cơ bản của người tiêu dùng liên quan đến thông tin cá nhân, đồng thời đặt ra nghĩa vụ tương ứng đối với các tổ chức, cá nhân trong việc thu thập, xử lý, lưu trữ, chuyển giao và bảo mật thông tin này.

Trước hết, pháp luật đã bước đầu nhận diện rõ nội hàm của “thông tin người tiêu dùng” thông qua các định nghĩa pháp lý, từ đó làm cơ sở cho việc điều chỉnh hành vi và áp dụng các biện pháp bảo vệ phù hợp. Các quy định về xử lý, chuyển giao thông tin người tiêu dùng được thể hiện trong nhiều văn bản pháp luật như Luật Bảo vệ quyền lợi người tiêu dùng (sửa đổi năm 2023), Luật An ninh mạng, Nghị định 13/2023/NĐ-CP, Nghị định 53/2022/NĐ-CP, Thông tư 24/2022/TT-BTTTT,... phản ánh sự cập nhật, thích nghi của pháp luật Việt Nam với xu thế chuyển đổi số, kinh tế số và hội nhập quốc tế.

Ngoài ra, các hành vi xâm phạm thông tin người tiêu dùng cũng đã được pháp luật quy định cụ thể và có chế tài xử lý rõ ràng, từ xử phạt hành chính đến truy cứu trách nhiệm hình sự. Cùng với đó, các biện pháp bảo vệ thông tin người tiêu dùng cũng dần được hoàn thiện, trong đó nổi bật là việc thiết lập cơ chế xin "**consent**" (sự đồng ý của người tiêu dùng), tăng cường minh bạch trong xử lý dữ liệu, quy định về lưu trữ dữ liệu nội địa đối với doanh nghiệp nước ngoài hoạt động tại Việt Nam,...

Tuy nhiên, qua đánh giá, chương này cũng chỉ ra rằng pháp luật Việt Nam vẫn còn nhiều bất cập như thiếu tính đồng bộ, chồng chéo giữa các văn bản pháp luật; cơ chế thực thi còn yếu; mức xử phạt chưa đủ sức răn đe; người tiêu dùng thiếu thông tin và kỹ năng để tự bảo vệ quyền của mình; và hệ thống pháp lý vẫn chưa bắt kịp với tốc độ phát triển của công nghệ và mô hình kinh doanh mới.

Bên cạnh đó, thông qua các ví dụ thực tiễn, số liệu điều tra và một số bản án điển hình, chương 2 đã minh chứng rõ ràng cho những lỗ hổng trong thực thi pháp luật, sự thiếu nhất quán trong việc áp dụng pháp luật cũng như khoảng cách giữa quy định pháp lý và thực tế triển khai. Điều này đặt ra yêu cầu cấp thiết phải tiếp tục hoàn thiện pháp luật cả về nội dung lẫn hình thức tổ chức thực thi.

Tóm lại, pháp luật Việt Nam đã tạo dựng được nền tảng tương đối rõ ràng cho việc bảo vệ thông tin người tiêu dùng. Tuy nhiên, để thực sự phát huy hiệu quả và tạo dựng lòng tin trong xã hội số, cần có sự điều chỉnh toàn diện cả về chính sách, kỹ thuật, và tổ chức thực hiện, từ trung ương đến địa phương – đặc biệt trong bối cảnh tỉnh Bình Thuận đang đẩy mạnh ứng dụng công nghệ thông tin trong hoạt động thương mại, hành chính công và du lịch thông minh.

CHƯƠNG 3

THỰC TIỄN BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG Ở VIỆT NAM VÀ TỈNH BÌNH THUẬN. MỘT SỐ KIẾN NGHỊ HOÀN THIỆN PHÁP LUẬT VIỆT NAM VỀ BẢO VỆ THÔNG TIN NGƯỜI TIÊU DÙNG

3.1. Thực trạng các quy định của pháp luật về bảo vệ thông tin người tiêu dùng

3.1.1. Một số kết quả đạt được

Trong những năm gần đây, hệ thống pháp luật Việt Nam ngày càng thể hiện rõ vai trò trong việc định hướng và điều chỉnh hoạt động xử lý, bảo mật thông tin người tiêu dùng. Cụ thể:

Thứ nhất là hoàn thiện hệ thống pháp luật liên quan.

Một trong những thành tựu quan trọng trong thực tiễn bảo vệ thông tin người tiêu dùng ở Việt Nam trong thời gian gần đây là việc **hoàn thiện hệ thống pháp luật** liên quan, đặc biệt là thông qua hai văn bản quan trọng: **Luật Bảo vệ quyền lợi người tiêu dùng năm 2023** và **Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân**. Hai văn bản này đánh dấu bước tiến lớn trong việc tiếp cận với các chuẩn mực quốc tế về quyền riêng tư và bảo vệ dữ liệu cá nhân trong kỷ nguyên số.

Luật Bảo vệ quyền lợi người tiêu dùng năm 2023

Luật này được Quốc hội thông qua ngày 20/6/2023 và sẽ có hiệu lực từ ngày 01/7/2024. So với Luật năm 2010, luật sửa đổi năm 2023 đã có bước tiến vượt bậc khi quy định rõ ràng, đầy đủ hơn về trách nhiệm bảo vệ thông tin người tiêu dùng, phù hợp với bối cảnh phát triển của thương mại điện tử và kinh tế số.

Một số nội dung nổi bật:

Điều 6 quy định rõ quyền của người tiêu dùng trong việc được bảo vệ bí mật và an toàn thông tin cá nhân; được cung cấp thông tin về mục đích, phạm vi thu thập, sử dụng và lưu giữ thông tin của mình.

Điều 7 quy định nghĩa vụ của tổ chức, cá nhân kinh doanh trong việc bảo mật thông tin, chỉ được thu thập, sử dụng thông tin khi có sự đồng ý rõ ràng của người tiêu dùng và không được chuyển giao cho bên thứ ba nếu không được phép.

Đặc biệt, luật quy định chi tiết về các hành vi bị nghiêm cấm, như: tiết lộ, cung cấp, sử dụng trái phép thông tin cá nhân người tiêu dùng; lừa dối để chiếm đoạt thông tin cá nhân; thu thập thông tin mà không có sự đồng ý...

Luật cũng lần đầu tiên đặt ra cơ chế bảo vệ người tiêu dùng trong môi trường số, cụ thể là trong các giao dịch trực tuyến, hợp đồng điện tử, ứng dụng công nghệ.

Nghị định 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân

Được ban hành ngày 17/4/2023, Nghị định này là văn bản pháp lý đầu tiên tại Việt Nam đặt nền móng chính thức cho chế độ bảo vệ dữ liệu cá nhân một cách toàn diện, bao gồm cả dữ liệu chung và dữ liệu nhạy cảm. Nghị định có hiệu lực từ ngày 01/7/2023.

Một số điểm nổi bật:

Điều 3 định nghĩa dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản (họ tên, ngày sinh, địa chỉ,...) và dữ liệu cá nhân nhạy cảm (sức khỏe, tài chính, định vị, tín ngưỡng,...).

Điều 11 đến 16 quy định về quyền của chủ thể dữ liệu, bao gồm quyền được biết, quyền được đồng ý, quyền truy cập, quyền rút lại sự đồng ý, quyền xóa dữ liệu...

Điều 17 quy định cụ thể về nghĩa vụ của bên xử lý dữ liệu cá nhân, như phải có biện pháp kỹ thuật bảo mật, lưu giữ hồ sơ xử lý dữ liệu, đánh giá tác động khi xử lý dữ liệu nhạy cảm.

Điều 20 yêu cầu các bên thu thập, xử lý dữ liệu phải có sự đồng ý rõ ràng của chủ thể, và đồng ý này phải được thể hiện dưới hình thức có thể in, sao lưu, hoặc truy xuất dưới dạng dữ liệu.

Đặc biệt, Nghị định quy định xử phạt lên đến 100 triệu đồng đối với hành vi vi phạm, và có thể xử lý hình sự nếu gây hậu quả nghiêm trọng (dẫn chiếu theo Bộ luật Hình sự 2015, sửa đổi năm 2017 – Điều 288, 289, 290...).

Tác động thực tiễn

Việc ban hành hai văn bản nêu trên cho thấy Việt Nam đã bước đầu tiệm cận với tiêu chuẩn quốc tế, như Quy định chung về bảo vệ dữ liệu (GDPR) của Liên minh Châu Âu. Đây cũng là công cụ pháp lý quan trọng trong đấu tranh với các hành vi xâm phạm

thông tin cá nhân, nhất là trong bối cảnh tình trạng rò rỉ dữ liệu, giả mạo, lừa đảo qua mạng ngày càng phức tạp.

Ví dụ: Trong vụ việc triệt phá đường dây mua bán 56 triệu dữ liệu cá nhân tại Thừa Thiên Huế tháng 2/2024, công an đã dựa trên các căn cứ từ Nghị định 13/2023/NĐ-CP để lập hồ sơ khởi tố các đối tượng về hành vi thu thập, buôn bán trái phép thông tin cá nhân.

Thứ hai, tăng cường hoạt động thanh tra, kiểm tra, giám sát và xử lý vi phạm của các cơ quan quản lý nhà nước. Trong năm 2023, công tác này đã có nhiều chuyển biến tích cực và mang lại hiệu quả thiết thực.

Theo báo cáo của Cục Cảnh tranh và Bảo vệ người tiêu dùng (Bộ Công Thương), trong năm 2023, các cơ quan chức năng đã tổ chức khoảng 1.500 cuộc thanh tra, kiểm tra, giám sát đối với các tổ chức, doanh nghiệp cung cấp hàng hóa, dịch vụ, đặc biệt là trong lĩnh vực thương mại điện tử và tài chính tiêu dùng – nơi có nguy cơ cao xảy ra xâm phạm thông tin cá nhân.

Thông qua các hoạt động kiểm tra, cơ quan chức năng đã phát hiện nhiều trường hợp vi phạm liên quan đến: Thu thập thông tin cá nhân không có sự đồng ý rõ ràng, minh bạch từ người tiêu dùng; Chia sẻ thông tin cá nhân cho bên thứ ba mà không được phép; Rò rỉ, đánh cắp hoặc sử dụng trái phép dữ liệu người tiêu dùng phục vụ cho mục đích quảng cáo, tín dụng đen, lừa đảo qua mạng...

Một số vụ việc tiêu biểu được xử lý

Tháng 3/2023, Công ty TNHH Thương mại điện tử X (Hà Nội) bị Cục Quản lý thị trường kiểm tra và phát hiện thu thập dữ liệu cá nhân người tiêu dùng thông qua ứng dụng di động mà không công bố chính sách quyền riêng tư, vi phạm quy định tại Điều 6 và Điều 7 của Luật Bảo vệ quyền lợi người tiêu dùng 2023. Công ty này bị xử phạt 65 triệu đồng và buộc gỡ bỏ các dữ liệu đã thu thập trái phép.

Tháng 10/2023, cơ quan công an TP.HCM triệt phá một đường dây sử dụng thông tin cá nhân của người tiêu dùng để đăng ký sim rác, tài khoản ngân hàng giả, gây thiệt hại hàng tỷ đồng. Vụ việc được khởi tố theo Điều 288 Bộ luật Hình sự 2015 (sửa đổi 2017) về hành vi “đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn

thông”.

Tháng 6/2023, Sở Thông tin và Truyền thông TP. Đà Nẵng xử phạt một doanh nghiệp cung cấp nền tảng dịch vụ chăm sóc khách hàng trực tuyến vì vi phạm quy định tại Điều 20 Nghị định 13/2023/NĐ-CP, không có biện pháp bảo mật phù hợp dẫn đến làm rò rỉ dữ liệu cá nhân của hơn 10.000 người tiêu dùng.

Việc đẩy mạnh hoạt động thanh tra, kiểm tra không chỉ **răn đe và xử lý vi phạm kịp thời**, mà còn góp phần **nâng cao ý thức tuân thủ pháp luật** của doanh nghiệp, đặc biệt trong việc bảo vệ thông tin khách hàng – một tài sản vô hình có giá trị lớn trong kỷ nguyên số.

Thứ ba, nâng cao nhận thức của người tiêu dùng và cộng đồng xã hội về tầm quan trọng của thông tin cá nhân cũng đóng vai trò đặc biệt quan trọng trong việc phòng ngừa vi phạm, giảm thiểu rủi ro và tăng cường hiệu quả thực thi pháp luật.

Trong thời gian gần đây, nhiều chiến dịch truyền thông về an toàn thông tin, bảo vệ dữ liệu cá nhân, bảo vệ người tiêu dùng trong môi trường số đã được các cơ quan nhà nước, tổ chức chính trị - xã hội triển khai đồng bộ:

Chiến dịch “Bảo vệ dữ liệu cá nhân – Trách nhiệm của mỗi chúng ta” được Bộ Công an phối hợp Bộ Thông tin và Truyền thông phát động từ tháng 5/2023 trên toàn quốc. Chiến dịch này hướng đến việc truyền tải thông tin đơn giản, dễ hiểu về các quyền của người dân theo Nghị định 13/2023/NĐ-CP, như quyền được biết, quyền đồng ý, quyền rút lại thông tin, quyền yêu cầu xóa dữ liệu...

Cục Cảnh tranh và Bảo vệ người tiêu dùng **tổ chức các** “Ngày hội người tiêu dùng”, “Diễn đàn bảo vệ người tiêu dùng trong thương mại điện tử” tại Hà Nội, TP.HCM, Đà Nẵng... với sự tham gia của hàng nghìn lượt người, nhằm nâng cao hiểu biết của công chúng về quyền bảo vệ thông tin, cách phản ánh hành vi vi phạm, và các dấu hiệu nhận biết lừa đảo công nghệ cao.

Chiến dịch “Kỹ năng số cho người tiêu dùng”, do Tổng cục Quản lý thị trường phối hợp với Google Việt Nam triển khai từ năm 2022, đã tiếp cận trên 2 triệu người dùng qua nền tảng trực tuyến và các hoạt động trực tiếp tại địa phương. Nội dung bao

gồm hướng dẫn cách cài đặt bảo mật hai lớp, cách kiểm soát thông tin cá nhân, cách phản ánh hành vi xâm phạm thông tin đến cơ quan chức năng.

Qua khảo sát năm 2023 của Viện Nghiên cứu Quản lý Kinh tế Trung ương (CIEM), **hơn 65% người tiêu dùng đô thị đã có ý thức cài đặt các công cụ bảo mật** như OTP, xác thực hai yếu tố (2FA), không chia sẻ mã xác thực cho bên thứ ba. **Khoảng 70% số người được khảo sát biết rằng họ có quyền yêu cầu doanh nghiệp xóa dữ liệu cá nhân** khi không còn sử dụng dịch vụ¹¹.

Đặc biệt, nhận thức về hành vi lừa đảo qua mạng như “giả danh cơ quan nhà nước yêu cầu cung cấp mã OTP”, “gửi link giả mạo ngân hàng” hay “gọi điện giả cảnh sát điều tra”... đã được nâng cao rõ rệt nhờ các clip tuyên truyền phát trên truyền hình và mạng xã hội như YouTube, TikTok, Zalo.

Thứ tư, áp dụng công nghệ trong bảo vệ thông tin: Một số doanh nghiệp lớn như Viettel, VNPT, Shopee, Tiki,... đã chủ động đầu tư hệ thống bảo mật, mã hóa thông tin, đồng thời công bố minh bạch các chính sách quyền riêng tư và cơ chế thu thập, xử lý dữ liệu.

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, các hành vi xâm phạm dữ liệu cá nhân, đánh cắp thông tin người tiêu dùng cũng ngày càng tinh vi, có tổ chức. Vì vậy, việc áp dụng công nghệ hiện đại vào việc bảo vệ thông tin người tiêu dùng không chỉ là yêu cầu pháp lý, mà còn trở thành tiêu chuẩn đạo đức và chiến lược phát triển bền vững của doanh nghiệp.

Một số doanh nghiệp lớn trong các lĩnh vực viễn thông, thương mại điện tử, tài chính... đã tiên phong đầu tư vào các hệ thống công nghệ bảo mật đa tầng, kết hợp mã hóa dữ liệu, kiểm soát truy cập và cảnh báo sớm vi phạm.

Tập đoàn Viettel: Năm 2023, Viettel đã triển khai hệ thống giám sát an toàn thông tin SIEM (Security Information and Event Management) giúp phân tích hành vi bất thường trong truy cập dữ liệu. Tập đoàn này cũng đang vận hành Trung tâm Giám sát an ninh mạng (SOC) quy mô quốc gia, có khả năng xử lý hàng triệu log dữ liệu mỗi

¹¹ Nguồn: <https://ciem.org.vn/tin-tuc/9304/vien-nghien-cuu-quan-ly-kinh-te-trung-uong-khao-sat-kinh-nghiem-xay-dung-va-hoan-thien-the-che-lien-ket-vung-tai-trung-quoc-tu-ngay-25-den-29-thang-11-nam-2024?newsgroup=Tin%20%E1%BB%A9c%20-%20s%E1%BB%B1%20ki%E1%BB%87n%09>

ngày, chủ động ngăn chặn tấn công vào cơ sở dữ liệu khách hàng¹².

VNPT (Tập đoàn Bưu chính Viễn thông Việt Nam): Với vai trò đơn vị cung cấp hạ tầng công nghệ số, VNPT đầu tư mạnh vào các giải pháp mã hóa end-to-end, xác thực đa yếu tố (MFA) trong dịch vụ MyVNPT, VNPT Pay và các nền tảng giáo dục, y tế mà doanh nghiệp này vận hành¹³. VNPT cũng là đơn vị tiên phong trong việc công bố minh bạch chính sách quyền riêng tư theo yêu cầu của Nghị định 13/2023/NĐ-CP.

Shopee, Tiki và Lazada: Là các sàn thương mại điện tử lớn tại Việt Nam, các đơn vị này đã tích hợp các giải pháp bảo vệ thông tin như: Xác thực người dùng bằng OTP khi đăng nhập hoặc thay đổi thông tin cá nhân; Tùy chọn cho người tiêu dùng quản lý quyền truy cập thông tin cá nhân; Chính sách bảo mật rõ ràng, minh bạch về thời gian lưu trữ, mục đích sử dụng dữ liệu theo đúng yêu cầu của Luật Bảo vệ quyền lợi người tiêu dùng 2023 và Luật An ninh mạng 2018.

TPBank và Techcombank: Trong lĩnh vực tài chính, ngân hàng, các ngân hàng số tại Việt Nam đã đầu tư mạnh vào AI phát hiện gian lận (fraud detection), xác thực sinh trắc học và hệ thống mã hóa AES 256-bit đạt chuẩn quốc tế.

Tại tỉnh Bình Thuận, các cơ quan chức năng như Sở Công Thương, Cục Quản lý thị trường, Trung tâm Xúc tiến thương mại và Sở Thông tin – Truyền thông cũng đã bước đầu có hoạt động tuyên truyền, kiểm tra liên quan đến bảo vệ thông tin người tiêu dùng, nhất là trong lĩnh vực thương mại điện tử và du lịch trực tuyến.

Tỉnh Bình Thuận là một trong những địa phương có tốc độ phát triển nhanh trong các lĩnh vực du lịch, thương mại dịch vụ và thương mại điện tử, đặc biệt tại các khu vực trọng điểm như thành phố Phan Thiết, thị xã La Gi, huyện Hàm Thuận Nam... Sự gia tăng của các giao dịch điện tử đồng thời đặt ra những thách thức lớn trong việc bảo vệ thông tin cá nhân và dữ liệu người tiêu dùng.

¹² Nguồn: <https://viettelfamily.com/viettel-mang-nen-tang-giam-sat-dieu-hanh-attt-the-he-moi-toi-mwc-2025>

¹³ Nguồn: <https://vnpt.com.vn/tu-van/vnpt-cung-cap-ha-tang-vien-thong-va-dich-vu-so-phuc-vu-dai-hoi-xiii-cong-doan-viet-nam.html>

Về công tác tuyên truyền, phổ biến pháp luật về bảo vệ thông tin cá nhân và quyền người tiêu dùng

Các cơ quan chức năng tại Bình Thuận như Sở Công Thương, Sở Thông tin và Truyền thông, Cục Quản lý thị trường tỉnh, Trung tâm Xúc tiến thương mại... đã bước đầu triển khai một số hoạt động nhằm nâng cao nhận thức cho người tiêu dùng, doanh nghiệp và cán bộ quản lý.

Trong năm 2023, Sở Công Thương tỉnh Bình Thuận đã phối hợp với Hội Bảo vệ quyền lợi người tiêu dùng tổ chức 03 hội nghị tuyên truyền tại các huyện Hàm Thuận Bắc, Bắc Bình và thành phố Phan Thiết, thu hút hơn 500 lượt người tham gia, với nội dung trọng tâm về quyền bảo vệ thông tin cá nhân, nghĩa vụ thông báo thu thập dữ liệu trong thương mại điện tử¹⁴.

Cùng năm, Sở Thông tin và Truyền thông đã ban hành Công văn số 1724/STTTT-BCVT yêu cầu các đơn vị viễn thông, cung cấp nền tảng số trên địa bàn tỉnh tăng cường rà soát bảo mật thông tin người dùng, kiểm tra điều kiện cung cấp dịch vụ số, đặc biệt là với các sản phẩm dịch vụ trực tuyến, ứng dụng đặt phòng, đặt tour.

Trung tâm Xúc tiến thương mại Bình Thuận đã tích hợp nội dung “bảo vệ quyền lợi người tiêu dùng” trong các khóa tập huấn chuyển đổi số cho doanh nghiệp địa phương, hướng dẫn cách công bố chính sách thu thập thông tin, chính sách quyền riêng tư theo đúng quy định tại Luật Bảo vệ quyền lợi người tiêu dùng 2023¹⁵.

Hoạt động kiểm tra, thanh tra việc bảo vệ dữ liệu người tiêu dùng trong thực tiễn

Song song với công tác tuyên truyền, Cục Quản lý thị trường tỉnh Bình Thuận đã phối hợp với các ngành liên quan triển khai kiểm tra định kỳ và đột xuất đối với các cơ sở kinh doanh dịch vụ có yếu tố thương mại điện tử, đặc biệt trong các lĩnh vực nhạy cảm như: bán hàng online, đặt phòng lưu trú, dịch vụ lữ hành trực tuyến...

Theo báo cáo nội bộ năm 2023 của Đội QLTT số 1 (thuộc Cục QLTT tỉnh), đơn vị này đã tiến hành 12 cuộc kiểm tra tại các cơ sở kinh doanh online và 03 sản phẩm

¹⁴ Nguồn: <https://sct.binhthuan.gov.vn/thuong-mai-dich-vu/hoi-nghi-tuyen-truyen-pho-bien-cac-quy-dinh-phap-luat-ve-bao-ve-quyen-loi-nguoi-tieu-dung-nam-20-892124>

¹⁵ Nguồn: <https://tapchicongthuong.vn/binh-thuan--tiếp-tục-day-manh-tuyen-truyen-cuoc-van-dong--nguoi-viet-nam-uu-tien-dung-hang-viet-nam-119057.htm>

mại điện tử địa phương, trong đó phát hiện 02 cơ sở vi phạm trong việc thu thập thông tin khách hàng mà không thông báo rõ ràng mục đích, cách xử lý dữ liệu, vi phạm Điều 9 Nghị định 13/2023/NĐ-CP.

Trong quý IV/2023, Thanh tra Sở Công Thương đã lập biên bản xử phạt **01** doanh nghiệp du lịch tại Phan Thiết vì hành vi tự ý chia sẻ thông tin khách hàng cho bên thứ ba mà không có sự đồng ý bằng văn bản hoặc hình thức tương đương, mức phạt hành chính là 17.500.000 đồng, căn cứ theo Nghị định 98/2020/NĐ-CP và Nghị định 13/2023/NĐ-CP¹⁶.

Ngoài ra, đầu năm 2024, UBND tỉnh Bình Thuận cũng đã có văn bản chỉ đạo các sở ngành đẩy mạnh ứng dụng công nghệ trong giám sát hoạt động thương mại điện tử, đặc biệt là trong dịp cao điểm lễ hội, tết và mùa du lịch hè – thời điểm phát sinh nhiều đơn thư phản ánh về lừa đảo, đánh cắp thông tin khách hàng qua website đặt phòng, đặt tour ảo.

3.1.2. Những hạn chế còn tồn tại trong thực tiễn thực hiện pháp luật về bảo vệ thông tin người tiêu dùng ở Việt Nam

Bên cạnh các kết quả đạt được, vẫn còn tồn tại nhiều bất cập trong thực tiễn thi hành pháp luật về bảo vệ thông tin người tiêu dùng:

Thứ nhất, thiếu đồng bộ và chồng chéo trong hệ thống pháp luật: Nhiều quy định về bảo vệ dữ liệu cá nhân, thông tin người tiêu dùng được ban hành rải rác ở các luật khác nhau (Luật Bảo vệ quyền lợi người tiêu dùng, Luật An ninh mạng, Luật Giao dịch điện tử, Luật Viễn thông...), gây khó khăn trong việc thực thi và xác định trách nhiệm pháp lý.

Một trong những hạn chế đáng chú ý nhất hiện nay trong thực tiễn bảo vệ thông tin người tiêu dùng ở Việt Nam là sự **thiếu nhất quán, đồng bộ và chồng chéo giữa các quy định pháp luật hiện hành**, gây ra không ít khó khăn trong quá trình thực thi, áp dụng pháp luật và bảo vệ quyền lợi người tiêu dùng một cách hiệu quả.

¹⁶ Nguồn: <https://sct.binhthuan.gov.vn/1319/32424/67380/634705/hoat-dong-thanh-tra/so-cong-thuong-tham-gia-doan-thanh-tra-lien-nganh-trong-thang-hanh-dong-vi-an-toan-thuc-pham-cua.aspx>

Một là, thông tin cá nhân và thông tin người tiêu dùng hiện được điều chỉnh bởi nhiều văn bản pháp luật, tiêu biểu như:

Luật Bảo vệ quyền lợi người tiêu dùng 2023 (sửa đổi): quy định quyền của người tiêu dùng được bảo vệ thông tin cá nhân (Điều 6, Điều 7), nghĩa vụ của tổ chức, cá nhân kinh doanh trong thu thập, lưu trữ, sử dụng thông tin (Chương III).

Luật An ninh mạng 2018: yêu cầu doanh nghiệp trong và ngoài nước cung cấp dịch vụ tại Việt Nam phải lưu trữ dữ liệu cá nhân người dùng tại Việt Nam (Điều 26) và có trách nhiệm bảo đảm an toàn dữ liệu (Điều 17).

Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân: quy định chi tiết các quyền của chủ thể dữ liệu, nguyên tắc xử lý dữ liệu cá nhân và xử lý vi phạm hành chính liên quan.

Luật Viễn thông 2009 (đang được sửa đổi): có quy định về trách nhiệm bảo mật thông tin thuê bao, người dùng dịch vụ viễn thông (Điều 6, Điều 88).

Luật Giao dịch điện tử 2023: điều chỉnh các vấn đề liên quan đến định danh điện tử, chữ ký số và các giao dịch cần mã hóa.

Tuy nhiên, các văn bản này chưa có sự thống nhất cao, mỗi luật lại dùng khái niệm, thuật ngữ khác nhau như “dữ liệu cá nhân”, “thông tin cá nhân”, “thông tin người tiêu dùng”, “dữ liệu định danh điện tử”, gây lúng túng cho cả cơ quan quản lý, doanh nghiệp và người tiêu dùng trong việc hiểu đúng và áp dụng đúng.

Hai là, thiếu cơ chế phối hợp liên ngành và hướng dẫn cụ thể

Trong thực tiễn, nhiều cơ quan cùng có trách nhiệm quản lý dữ liệu người tiêu dùng, gồm: Bộ Công Thương (Cục Cạnh tranh và Bảo vệ người tiêu dùng), Bộ Thông tin và Truyền thông (Cục An toàn thông tin), Bộ Công an (Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao), Bộ Tư pháp (Vụ Pháp luật dân sự - kinh tế).

Tuy nhiên, thiếu một cơ quan đầu mối rõ ràng, dẫn đến tình trạng thiếu thống nhất trong xử lý vi phạm. Nhiều vụ việc rò rỉ dữ liệu xảy ra nhưng không xác định được cơ quan có thẩm quyền chính xử lý, hoặc việc xử lý chậm, không đủ sức răn đe.

Ví dụ: vụ rò rỉ hơn 17 GB dữ liệu khách hàng của một chuỗi bán lẻ điện thoại tại TP.HCM vào tháng 8/2023 được lan truyền trên diễn đàn hacker, nhưng đến tháng 11/2023 vẫn chưa có thông báo chính thức về kết quả điều tra và biện pháp xử lý. Trong khi đó, người tiêu dùng bị ảnh hưởng không có nơi phản ánh cụ thể và không được bồi thường thiệt hại¹⁷.

Ba là, xung đột giữa các quy định pháp lý và khoảng trống pháp luật

Có những trường hợp mà quy định giữa các luật lại mâu thuẫn hoặc không làm rõ phạm vi áp dụng, ví dụ:

Luật An ninh mạng 2018 quy định doanh nghiệp nước ngoài phải lưu trữ dữ liệu tại Việt Nam, nhưng đến nay chưa có quy định cụ thể về việc kiểm tra, giám sát và xử lý vi phạm nếu doanh nghiệp không tuân thủ.

Trong khi đó, Luật Bảo vệ quyền lợi người tiêu dùng 2023 quy định người tiêu dùng có quyền yêu cầu xóa dữ liệu cá nhân, nhưng không có hướng dẫn chi tiết cách thực hiện quyền này với các nền tảng xuyên biên giới như Facebook, TikTok, Google.

Ngoài ra, một số khái niệm pháp lý chưa được định nghĩa rõ ràng trong luật như “thông tin nhạy cảm của người tiêu dùng”, “xử lý dữ liệu đặc biệt”, “thu thập thông tin trái phép”, khiến việc định tội và xử phạt trong các vụ việc cụ thể gặp khó khăn.

Thứ hai, thực thi pháp luật chưa nghiêm: Một số doanh nghiệp vẫn thu thập, sử dụng và chia sẻ thông tin cá nhân của người tiêu dùng trái pháp luật, nhưng việc phát hiện và xử lý còn ít. Theo báo cáo của Bộ Công Thương (2023), chỉ khoảng 15% vụ việc vi phạm về bảo vệ dữ liệu cá nhân bị xử lý đến cùng.

Mặc dù hệ thống pháp luật Việt Nam về bảo vệ thông tin cá nhân, đặc biệt là thông tin người tiêu dùng, đã từng bước được hoàn thiện, song thực tiễn cho thấy việc tổ chức thực thi pháp luật còn lỏng lẻo, thiếu hiệu lực, dẫn đến việc các hành vi vi phạm vẫn tái diễn, gây ảnh hưởng nghiêm trọng đến quyền lợi chính đáng của người tiêu dùng.

Một là, nhiều doanh nghiệp vẫn vi phạm mà không bị xử lý nghiêm minh

¹⁷ Nguồn: <https://laodong.vn/kinh-doanh/vu-ro-ri-17gb-du-lieu-pi-network-phu-nhan-hacker-gap-lua-bo-tay-nguoi-912638.laod>

Hiện nay, không ít doanh nghiệp trong các lĩnh vực như thương mại điện tử, tài chính – ngân hàng, viễn thông... vẫn thu thập, phân tích, lưu trữ và chia sẻ dữ liệu cá nhân của khách hàng mà không có sự đồng ý rõ ràng, hoặc sử dụng thông tin đó vào mục đích quảng cáo, bán hàng, phân phối cho bên thứ ba.

Ví dụ: Vụ rò rỉ dữ liệu người dùng của app vay tiền online, trong đó thông tin về CMND/CCCD, danh bạ điện thoại, hình ảnh cá nhân của hàng nghìn người dân bị phát tán và sử dụng để khủng bố tinh thần, đe dọa, ép trả nợ. Dù được phản ánh rộng rãi, đến nay chỉ một số ít đơn vị bị xử phạt hành chính hoặc đình chỉ tạm thời hoạt động¹⁸.

Hai là, tỷ lệ phát hiện và xử lý vi phạm còn rất thấp

Theo báo cáo của Bộ Công Thương năm 2023, cơ quan quản lý đã tiếp nhận gần 2.300 phản ánh, khiếu nại từ người tiêu dùng liên quan đến rò rỉ, lạm dụng thông tin cá nhân¹⁹. Tuy nhiên, chỉ khoảng 15% số vụ được xử lý đến cùng, bao gồm xác minh, kết luận và ra quyết định xử phạt hoặc có biện pháp khắc phục. Con số này cho thấy:

Công tác thanh tra, giám sát vẫn mang tính chất hình thức hoặc bị phân tán, không có cơ chế theo dõi, đánh giá xuyên suốt.

Thiếu hệ thống tiếp nhận, xử lý khiếu nại về vi phạm thông tin cá nhân một cách chuyên biệt và hiệu quả, khiến nhiều người tiêu dùng ngần ngại khi phản ánh hoặc không biết gửi đến cơ quan nào.

Một số doanh nghiệp cố tình trì hoãn, né tránh cung cấp thông tin trong quá trình điều tra, nhưng vẫn không bị chế tài mạnh, do chưa có quy định xử lý nghiêm việc cản trở thanh tra về dữ liệu cá nhân.

Ba là, thiếu cơ chế giám sát cộng đồng và xử lý hình sự

Dù nhiều hành vi xâm phạm thông tin người tiêu dùng có dấu hiệu cấu thành tội phạm (ví dụ như Tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín của người khác – Điều 159 Bộ luật Hình sự; hay Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính – Điều 288), nhưng rất ít vụ việc được chuyển sang điều tra hình sự.

¹⁸ Nguồn: <https://lsvn.vn/canh-bao-rui-ro-tu-viec-de-ro-ri-thong-tin-can-cuoc-cong-dan-1683617735-a130197.html>

¹⁹ Nguồn: <https://lsvn.vn/tiep-nhan-hang-tram-khieu-nai-cua-nguoi-tieu-dung-lien-quan-bat-dong-san-bao-hiem-1724296762-a146439.html>

Nguyên nhân là do: Khó khăn trong thu thập chứng cứ kỹ thuật số; Thiếu đội ngũ điều tra viên có chuyên môn sâu về dữ liệu và công nghệ thông tin; Tâm lý e ngại, sợ bị trả thù hoặc mất thời gian khi khởi kiện của người tiêu dùng.

Ví dụ điển hình: Vụ rò rỉ dữ liệu khách hàng của chuỗi siêu thị điện máy Điện Xanh vào tháng 9/2023 khiến hàng chục nghìn tài khoản bị rao bán trên các diễn đàn dark web. Mặc dù gây bức xúc dư luận, song đến nay chưa có doanh nghiệp hoặc cá nhân nào bị xử lý hình sự, mà mới chỉ dừng ở việc “điều tra, làm rõ” theo thông cáo báo chí²⁰.

Thứ ba, thiếu cơ chế giám sát độc lập: Việt Nam chưa có một cơ quan chuyên trách độc lập về bảo vệ dữ liệu cá nhân như các mô hình ở châu Âu, Nhật Bản hay Singapore. Việc thanh tra, xử phạt hiện nay chủ yếu giao cho các cơ quan chuyên ngành, khiến hiệu lực thực thi chưa cao.

Việc bảo vệ thông tin người tiêu dùng không chỉ đòi hỏi một hệ thống pháp luật đầy đủ mà còn cần có một cơ quan giám sát độc lập, chuyên trách và minh bạch để đảm bảo quyền lợi của người dân được bảo vệ một cách khách quan, hiệu quả. Tuy nhiên, tại Việt Nam, hiện chưa có một cơ quan giám sát dữ liệu cá nhân độc lập và chuyên biệt như các mô hình phổ biến tại nhiều quốc gia phát triển, dẫn đến nhiều bất cập trong công tác thực thi và bảo vệ quyền lợi người tiêu dùng.

Một là, thiếu mô hình cơ quan giám sát chuyên trách độc lập

Ở các khu vực như Liên minh châu Âu (EU), việc bảo vệ dữ liệu cá nhân do các cơ quan độc lập, ví dụ như Ủy ban Bảo vệ Dữ liệu (Data Protection Authority - DPA) thực hiện, được thiết lập theo các tiêu chuẩn quốc tế, như quy định tại Điều 51 – GDPR²¹. Các cơ quan này có quyền lực rộng lớn trong việc điều tra, xử phạt, và ra quyết định liên quan đến vi phạm dữ liệu cá nhân, đồng thời vận hành hoàn toàn độc lập với các bộ, ngành khác để tránh xung đột lợi ích.

Tương tự, tại **Nhật Bản**, Ủy ban Bảo vệ Thông tin cá nhân (PPC) được thành lập với chức năng giám sát và điều phối thực thi luật bảo vệ dữ liệu cá nhân. Ở **Singapore**,

²⁰ Nguồn: <https://laodong.vn/kinh-doanh/nong-thuc-hu-viec-ro-ri-thong-tin-31000-giao-dich-the-ngan-hang-cua-khach-hang-the-gioi-di-dong-640262.laod>

²¹ Nguồn: <https://gdpr-info.eu/art-51-gdpr/>

Cơ quan Bảo vệ Dữ liệu cá nhân (PDPC) cũng đóng vai trò giám sát độc lập và xử lý vi phạm.

Ngược lại, tại Việt Nam, các hoạt động thanh tra, giám sát và xử lý vi phạm liên quan đến bảo vệ thông tin người tiêu dùng thường do nhiều cơ quan khác nhau đảm nhiệm như: Bộ Công Thương (thực thi Luật Bảo vệ quyền lợi người tiêu dùng); Bộ Thông tin và Truyền thông (quản lý hoạt động viễn thông, internet); Bộ Công An (điều tra tội phạm liên quan đến dữ liệu); Sở Công Thương, Sở Thông tin và Truyền thông địa phương.

Việc phân tán này gây ra nhiều khó khăn trong phối hợp, cũng như thiếu đi sự độc lập cần thiết để xử lý các vi phạm một cách khách quan.

Hai là, hiệu lực thực thi chưa cao do thiếu cơ chế phối hợp đồng bộ

Bởi không có cơ quan giám sát độc lập chuyên trách, các cuộc thanh tra, kiểm tra thường mang tính chất rời rạc, chồng chéo hoặc thiếu chiều sâu. Mỗi bộ, ngành có một phạm vi quản lý riêng, nhưng trong thực tế, các vi phạm về bảo vệ thông tin người tiêu dùng thường xuyên liên quan chéo nhiều lĩnh vực như công nghệ, thương mại điện tử, dịch vụ tài chính...

Điều này khiến cho: Việc phát hiện vi phạm bị chậm trễ, không kịp thời; Các biện pháp xử lý không đồng bộ, thậm chí có thể mâu thuẫn; Thiếu sự kiểm soát chặt chẽ và báo cáo minh bạch về kết quả thực thi.

Ba là, hạn chế trong việc tiếp nhận và xử lý khiếu nại từ người tiêu dùng

Do không có một đầu mối chuyên trách độc lập, người tiêu dùng khi phát hiện vi phạm hoặc bị xâm phạm thông tin cá nhân thường gặp khó khăn trong việc tìm đúng cơ quan để phản ánh. Điều này làm giảm hiệu quả tiếp nhận phản ánh, khiếu nại và tăng nguy cơ vi phạm kéo dài.

Một số tổ chức xã hội và chuyên gia luật đã kiến nghị cần sớm thành lập một cơ quan bảo vệ dữ liệu cá nhân độc lập theo mô hình các nước phát triển, nhằm tăng cường sự minh bạch, trách nhiệm và hiệu quả xử lý vi phạm.

Thứ tư, người tiêu dùng thiếu kỹ năng bảo vệ dữ liệu: Đa số người dân còn chưa hiểu rõ quyền lợi và nghĩa vụ liên quan đến thông tin cá nhân, dễ dàng cung cấp dữ liệu cho bên thứ ba mà không có sự cảnh giác hoặc đọc kỹ điều khoản.

Bên cạnh những hạn chế về mặt pháp lý và cơ chế giám sát, một trong những nguyên nhân quan trọng dẫn đến việc bảo vệ thông tin người tiêu dùng ở Việt Nam chưa hiệu quả là do người tiêu dùng còn thiếu kỹ năng và nhận thức về bảo vệ dữ liệu cá nhân. Đây là thách thức chung không chỉ của Việt Nam mà còn của nhiều quốc gia đang phát triển khi chuyển đổi số ngày càng sâu rộng.

Một là, thiếu hiểu biết về quyền lợi và nghĩa vụ bảo vệ dữ liệu cá nhân

Nhiều nghiên cứu và khảo sát xã hội học gần đây cho thấy phần lớn người tiêu dùng Việt Nam chưa nắm rõ hoặc chưa được trang bị đầy đủ kiến thức về các quyền cơ bản liên quan đến bảo vệ thông tin cá nhân. Ví dụ, họ chưa hiểu rõ quyền được biết, quyền được sửa đổi, quyền từ chối hoặc yêu cầu xóa thông tin cá nhân theo quy định tại Luật Bảo vệ dữ liệu cá nhân 2023 hay các văn bản hướng dẫn liên quan.

Việc này khiến người tiêu dùng dễ bị tổn thương trong các giao dịch thương mại điện tử hoặc khi tham gia các dịch vụ số, bởi họ thường chấp nhận điều khoản sử dụng một cách máy móc, không đọc kỹ nội dung, hoặc không biết cách từ chối cung cấp các thông tin không cần thiết.

Hai là, tâm lý chủ quan, thiếu cảnh giác khi chia sẻ thông tin.

Nhiều người tiêu dùng có tâm lý chủ quan, cho rằng việc cung cấp thông tin cá nhân là bình thường, không ảnh hưởng lớn, hoặc không biết được hậu quả từ việc thông tin bị lộ, bị lạm dụng. Điều này làm gia tăng nguy cơ các hành vi thu thập dữ liệu trái phép, rò rỉ thông tin cá nhân trên mạng xã hội, thương mại điện tử và các nền tảng số khác.

Báo chí trong nước thời gian qua liên tục phản ánh các vụ việc như: Người tiêu dùng bị lừa đảo qua tin nhắn SMS giả mạo ngân hàng hoặc các tổ chức tài chính; Rò rỉ thông tin khách hàng từ các sàn thương mại điện tử lớn; Các trường hợp mất tiền trong tài khoản ngân hàng do lộ thông tin cá nhân khi tham gia các ứng dụng không an toàn.

Các vụ việc này không chỉ gây thiệt hại kinh tế mà còn làm tổn hại đến uy tín các doanh nghiệp và niềm tin của người tiêu dùng.

Ba là, thiếu các chương trình đào tạo và tuyên truyền bài bản.

Mặc dù các cơ quan nhà nước và tổ chức xã hội đã triển khai một số chiến dịch nâng cao nhận thức, tuy nhiên việc phổ biến kiến thức bảo vệ dữ liệu cá nhân vẫn còn chưa rộng khắp, đặc biệt ở các vùng nông thôn, miền núi hoặc các nhóm dân cư có trình độ văn hóa thấp.

Bốn là, hậu quả của việc thiếu kỹ năng bảo vệ dữ liệu.

Việc người tiêu dùng thiếu kỹ năng và nhận thức dẫn đến: Tăng nguy cơ bị xâm phạm quyền riêng tư, gây khó khăn cho việc phát hiện và tố cáo các hành vi vi phạm, làm giảm hiệu quả thực thi pháp luật khi các vi phạm không được phát hiện kịp thời, làm suy giảm niềm tin của người tiêu dùng vào thị trường số và dịch vụ trực tuyến.

Thứ năm, Tại tỉnh Bình Thuận, công tác tuyên truyền còn hạn chế, nhiều doanh nghiệp nhỏ và vừa hoạt động thương mại điện tử chưa ý thức rõ trách nhiệm trong bảo mật thông tin người tiêu dùng, đặc biệt trong ngành du lịch, bán lẻ, vận tải điện tử.

Tỉnh Bình Thuận, với nền kinh tế phát triển nhanh trong các lĩnh vực như du lịch, thương mại điện tử, bán lẻ và vận tải điện tử, đang đứng trước nhiều thách thức trong việc bảo vệ thông tin người tiêu dùng. Một trong những hạn chế nổi bật là công tác tuyên truyền về bảo vệ thông tin cá nhân còn chưa đủ mạnh và bao phủ rộng rãi, đặc biệt đối với các doanh nghiệp nhỏ và vừa.

Một là, công tác tuyên truyền còn hạn chế.

Mặc dù các cơ quan chức năng như Sở Công Thương, Cục Quản lý thị trường, Trung tâm Xúc tiến thương mại và Sở Thông tin – Truyền thông tỉnh Bình Thuận đã có những hoạt động tuyên truyền, nâng cao nhận thức về bảo vệ thông tin người tiêu dùng, song phạm vi và hiệu quả các chiến dịch này vẫn còn nhiều hạn chế: Nội dung tuyên truyền chủ yếu tập trung vào các doanh nghiệp lớn hoặc các đơn vị nhà nước, thiếu các chương trình đào tạo chuyên sâu, thiết thực dành cho các doanh nghiệp nhỏ và vừa, việc tiếp cận thông tin đến các doanh nghiệp hoạt động tại khu vực nông thôn, vùng sâu vùng xa còn rất hạn chế, đặc biệt, các ngành nghề có đặc thù như du lịch, bán lẻ, vận tải điện

tử – vốn là các lĩnh vực thu hút lượng lớn thông tin cá nhân của khách hàng – chưa được quan tâm đúng mức về mặt tuyên truyền pháp luật và kỹ năng bảo mật.

Hai là, ý thức trách nhiệm bảo mật thông tin của doanh nghiệp nhỏ và vừa còn thấp.

Nhiều doanh nghiệp nhỏ và vừa trên địa bàn tỉnh Bình Thuận hoạt động trong lĩnh vực thương mại điện tử và các dịch vụ liên quan chưa có nhận thức đầy đủ về trách nhiệm bảo vệ thông tin người tiêu dùng. Nguyên nhân bao gồm: Thiếu nguồn lực, nhân lực chuyên môn để xây dựng và vận hành hệ thống bảo mật thông tin, không cập nhật đầy đủ các quy định pháp luật mới về bảo vệ dữ liệu cá nhân như Nghị định 13/2023/NĐ-CP, Chưa có chính sách và quy trình nội bộ rõ ràng về xử lý, lưu trữ, chuyển giao thông tin cá nhân khách hàng, Một số doanh nghiệp thậm chí chưa hiểu rõ các rủi ro pháp lý, tổn thất kinh tế có thể phát sinh từ việc để lộ hay sử dụng sai thông tin khách hàng.

Ba là, các ngành nghề trọng điểm dễ tổn thương.

Ngành du lịch: Bình Thuận là địa phương phát triển mạnh về du lịch biển, thu hút lượng lớn khách du lịch trong và ngoài nước. Các đơn vị lữ hành, khách sạn, homestay thường thu thập nhiều thông tin cá nhân nhạy cảm của khách hàng như giấy tờ tùy thân, thông tin thanh toán, lịch trình... Tuy nhiên, việc bảo mật các thông tin này chưa được chú trọng đúng mức, dễ dẫn đến rủi ro rò rỉ hoặc sử dụng sai mục đích.

Ngành bán lẻ: Nhiều cửa hàng bán lẻ trên nền tảng trực tuyến, chợ điện tử nhỏ chưa áp dụng các giải pháp bảo mật dữ liệu hiệu quả, thường xuyên có tình trạng thông tin khách hàng bị lưu trữ không an toàn hoặc bị truy cập trái phép.

Ngành vận tải điện tử: Các dịch vụ đặt xe công nghệ tại Bình Thuận như Grab, Be, hay các đơn vị vận tải nhỏ lẻ chưa đồng bộ trong việc bảo vệ dữ liệu khách hàng, tiềm ẩn nguy cơ lộ lọt thông tin cá nhân qua hệ thống đăng ký, thanh toán và theo dõi hành trình.

Bốn là, hậu quả và thách thức.

Việc thiếu nhận thức và biện pháp bảo mật khiến thông tin người tiêu dùng dễ bị xâm phạm, dẫn đến mất uy tín cho doanh nghiệp và làm giảm niềm tin của khách hàng.

Các vụ việc vi phạm bảo mật dữ liệu cá nhân tuy chưa nhiều nhưng có xu hướng gia tăng, đặc biệt trong bối cảnh chuyển đổi số và thương mại điện tử phát triển nhanh tại địa phương.

Công tác thanh tra, kiểm tra chưa đi vào chiều sâu, thiếu sự phối hợp chặt chẽ giữa các cơ quan quản lý với doanh nghiệp và cộng đồng dân cư.

3.1.3. Nguyên nhân của những hạn chế còn tồn tại

Thứ nhất, pháp luật mới ban hành, chưa có thời gian triển khai đồng bộ

Luật Bảo vệ quyền lợi người tiêu dùng sửa đổi năm 2023 và Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân là những văn bản pháp luật quan trọng, tạo nền tảng vững chắc cho việc bảo vệ thông tin người tiêu dùng. Tuy nhiên, do các quy định này mới chính thức có hiệu lực nên vẫn đang trong giai đoạn đầu triển khai thực tiễn. Điều này dẫn đến một số khó khăn nhất định như: Cơ quan quản lý và doanh nghiệp vẫn đang trong quá trình làm quen, điều chỉnh hoạt động theo các quy định mới, một số nội dung pháp luật chưa được hướng dẫn chi tiết hoặc có sự chồng chéo, gây khó khăn trong việc áp dụng đồng bộ trên toàn quốc, các thủ tục hành chính, cơ chế phối hợp và quy trình xử lý vi phạm chưa được hoàn thiện, gây ra sự trì trệ trong thực thi.

Đặc biệt, tại các địa phương như Bình Thuận, việc triển khai đồng bộ các quy định pháp luật này gặp khó khăn do hạn chế về nguồn lực và năng lực thực thi pháp luật.

Thứ hai, thiếu nguồn nhân lực và cơ chế kiểm tra hiệu quả

Một trong những nguyên nhân căn bản làm cho việc thực thi pháp luật về bảo vệ thông tin người tiêu dùng chưa đạt hiệu quả cao là sự thiếu hụt về nguồn nhân lực có chuyên môn sâu về công nghệ thông tin, bảo mật dữ liệu và pháp lý: Ở cấp huyện, thị xã, các cán bộ phụ trách lĩnh vực này thường thiếu kinh nghiệm hoặc chưa được đào tạo bài bản, trang thiết bị, công cụ hỗ trợ kiểm tra, giám sát cũng chưa đáp ứng được yêu cầu của công tác quản lý trong bối cảnh chuyển đổi số mạnh mẽ, việc phối hợp giữa các cơ quan chức năng, đơn vị thực thi còn chưa chặt chẽ, dẫn đến nhiều vụ việc vi phạm không được phát hiện hoặc xử lý kịp thời.

Điều này làm giảm hiệu lực của các quy định pháp luật và tạo ra kẽ hở để các hành vi xâm phạm thông tin người tiêu dùng xảy ra.

Thứ ba, doanh nghiệp ưu tiên lợi ích kinh tế hơn tuân thủ pháp luật

Trong bối cảnh cạnh tranh ngày càng gay gắt trên thị trường, nhiều doanh nghiệp, đặc biệt là các doanh nghiệp nhỏ và vừa, có xu hướng đặt lợi ích kinh tế lên hàng đầu. Điều này dẫn đến một số thực trạng đáng lo ngại như: Việc thu thập, khai thác thông tin người tiêu dùng phục vụ cho mục đích quảng cáo, tiếp thị mà không xin phép hoặc không minh bạch về cách thức sử dụng thông tin, chia sẻ dữ liệu khách hàng cho bên thứ ba nhằm tăng lợi nhuận mà không có sự đồng thuận rõ ràng, thiếu hoặc bỏ qua các biện pháp bảo mật thông tin phù hợp để giảm chi phí vận hành.

Hậu quả là quyền riêng tư và lợi ích của người tiêu dùng bị xâm phạm, dẫn đến mất niềm tin vào doanh nghiệp và thị trường.

Thứ tư, ý thức bảo mật của người dân chưa cao

Phần lớn người tiêu dùng hiện nay vẫn chưa có thói quen bảo vệ thông tin cá nhân một cách chủ động và có ý thức cảnh giác khi giao dịch trực tuyến hoặc cung cấp dữ liệu cho các tổ chức, doanh nghiệp: Người dân thường không đọc kỹ các điều khoản về quyền riêng tư khi đăng ký dịch vụ, sử dụng ứng dụng, thiếu thông tin và kỹ năng nhận diện các hành vi xâm phạm, lừa đảo qua mạng, hạn chế trong việc tiếp cận các tài liệu, chương trình tuyên truyền về quyền và nghĩa vụ bảo vệ dữ liệu cá nhân.

Điều này khiến người tiêu dùng trở thành mục tiêu dễ dàng cho các hành vi thu thập, sử dụng thông tin trái phép.

Thứ năm, thiếu cơ chế xử lý vi phạm có tính răn đe mạnh

Một thực tế đáng lo ngại là các mức xử phạt hiện hành đối với hành vi vi phạm quyền riêng tư và bảo vệ thông tin người tiêu dùng còn khá thấp so với mức độ thiệt hại mà các vi phạm này gây ra: Mức phạt chưa đủ sức răn đe đối với các tập đoàn công nghệ lớn hoặc doanh nghiệp có lượng dữ liệu người dùng khổng lồ, việc xử lý vi phạm chủ yếu dựa vào các biện pháp hành chính, thiếu các chế tài hình sự nghiêm khắc hoặc các biện pháp khắc phục hậu quả cụ thể, quá trình xử lý vi phạm kéo dài, thủ tục phức tạp, dẫn đến hiệu quả thi hành pháp luật không cao, thiếu sự minh bạch và công khai kết quả xử lý vi phạm, khiến người tiêu dùng khó giám sát và tin tưởng vào hệ thống pháp luật.

Chính những yếu tố trên làm giảm tính khả thi và hiệu quả trong việc bảo vệ thông tin cá nhân người tiêu dùng, gây ra những hệ lụy nghiêm trọng trong bối cảnh chuyển đổi số và thương mại điện tử phát triển mạnh mẽ như hiện nay.

3.2. Một số kiến nghị hoàn thiện pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng

3.2.1. Định hướng chung về hoàn thiện pháp luật về bảo vệ thông tin người tiêu dùng

Việc hoàn thiện khung pháp lý về bảo vệ thông tin người tiêu dùng là một nhiệm vụ cấp thiết nhằm đáp ứng sự phát triển nhanh chóng của công nghệ số, thương mại điện tử và bảo vệ quyền lợi người dân trong bối cảnh hiện đại. Các định hướng chung dưới đây được đề xuất dựa trên thực tiễn triển khai, so sánh kinh nghiệm quốc tế và những bất cập còn tồn tại trong hệ thống pháp luật Việt Nam hiện nay:

Thứ nhất, xây dựng hệ thống pháp luật đồng bộ, nhất quán, dễ tiếp cận

Một trong những điểm yếu của hệ thống pháp luật Việt Nam hiện nay là tính phân mảnh, chồng chéo giữa các luật như Luật Bảo vệ quyền lợi người tiêu dùng, Luật An ninh mạng, Luật Giao dịch điện tử, Luật Viễn thông... dẫn đến khó khăn trong áp dụng, kiểm soát và xử lý vi phạm. Do đó, định hướng quan trọng là: Tập trung xây dựng khung pháp luật đồng bộ, có tính liên kết chặt chẽ giữa các luật, nghị định, thông tư liên quan đến bảo vệ dữ liệu cá nhân và thông tin người tiêu dùng; Đơn giản hóa, minh bạch hóa các quy định, đảm bảo người tiêu dùng và doanh nghiệp dễ dàng tiếp cận, hiểu rõ quyền và nghĩa vụ; Thiết lập các tiêu chuẩn pháp lý rõ ràng về phạm vi thông tin được bảo vệ, các hành vi bị cấm và biện pháp xử lý vi phạm.

Thứ hai, định hướng phát triển cơ chế bảo vệ chủ động, có tính phòng ngừa

Bên cạnh các quy định về xử lý vi phạm, pháp luật cần được xây dựng để tập trung vào phòng ngừa rủi ro, bảo vệ thông tin ngay từ đầu chuỗi thu thập, xử lý. Cụ thể: Áp dụng các nguyên tắc bảo mật theo chuẩn mực quốc tế như “Privacy by Design” (bảo vệ quyền riêng tư ngay từ thiết kế sản phẩm/dịch vụ) và “Privacy by Default” (mặc định bảo vệ dữ liệu cá nhân); Quy định bắt buộc các tổ chức, doanh nghiệp xây dựng kế hoạch, chính sách bảo mật, đánh giá rủi ro định kỳ và có các biện pháp kỹ thuật bảo vệ

hiệu quả; Xây dựng các tiêu chuẩn kỹ thuật về mã hóa, lưu trữ, truy cập dữ liệu phù hợp với thực tiễn công nghệ số hiện đại.

Thứ, ba xây dựng cơ chế giám sát, kiểm tra và xử lý vi phạm hiệu quả, độc lập

Thực tiễn cho thấy việc bảo vệ thông tin cá nhân cần có một cơ quan chuyên trách độc lập, có thẩm quyền giám sát, thanh tra, xử lý vi phạm một cách khách quan, hiệu quả. Định hướng cần: Thành lập cơ quan bảo vệ dữ liệu cá nhân độc lập, giống mô hình Ủy ban Bảo vệ dữ liệu cá nhân của EU (EDPB) hay Singapore, chịu trách nhiệm trực tiếp trước Quốc hội hoặc Chính phủ; Trang bị đầy đủ nhân lực, công cụ, công nghệ để phát hiện sớm các vi phạm, bảo đảm xử lý nghiêm minh, kịp thời; Xây dựng hệ thống báo cáo, thống kê minh bạch về tình hình vi phạm và xử lý, làm cơ sở cho việc đánh giá chính sách và điều chỉnh pháp luật.

Thứ tư, tăng cường vai trò người tiêu dùng trong bảo vệ quyền lợi của chính mình

Luật pháp cần thiết kế các quy định để tăng cường quyền chủ động của người tiêu dùng trong việc kiểm soát thông tin cá nhân của mình: Quy định rõ quyền đồng ý (consent) một cách tự nguyện, minh bạch, có thể rút lại bất cứ lúc nào; Quyền truy cập, chỉnh sửa, yêu cầu xóa hoặc hạn chế xử lý dữ liệu cá nhân; Cơ chế khiếu nại, tố cáo nhanh chóng và dễ dàng tiếp cận.

Thứ năm, hòa nhập với chuẩn mực, xu hướng quốc tế

Trong bối cảnh hội nhập sâu rộng và kinh tế số phát triển mạnh mẽ, pháp luật Việt Nam cần được thiết kế phù hợp với các tiêu chuẩn, thông lệ quốc tế, từ đó tạo điều kiện thuận lợi cho giao thương, hợp tác quốc tế trong lĩnh vực bảo vệ dữ liệu cá nhân và người tiêu dùng. Cụ thể: Tham khảo các luật và quy định như Quy định chung về bảo vệ dữ liệu (GDPR) của Liên minh châu Âu, Luật Bảo vệ dữ liệu cá nhân của Nhật Bản, Singapore; Đưa ra các tiêu chuẩn chung để các doanh nghiệp Việt Nam có thể dễ dàng áp dụng khi mở rộng hoạt động ra thị trường nước ngoài; Tăng cường hợp tác quốc tế trong phòng chống các hành vi vi phạm quyền riêng tư xuyên biên giới.

Thứ sáu, đẩy mạnh ứng dụng công nghệ trong quản lý và bảo vệ thông tin

Pháp luật cần được thiết kế linh hoạt để ứng phó với sự phát triển nhanh chóng của công nghệ số, AI, big data, thương mại điện tử, đồng thời khuyến khích doanh nghiệp ứng dụng các giải pháp công nghệ tiên tiến trong bảo vệ dữ liệu: Thúc đẩy phát triển các tiêu chuẩn kỹ thuật, quy trình kiểm tra bảo mật và chứng nhận sản phẩm công nghệ; Hỗ trợ, khuyến khích doanh nghiệp áp dụng các hệ thống bảo mật, mã hóa dữ liệu tiên tiến; Xây dựng hệ thống cảnh báo sớm, giám sát liên tục các rủi ro bảo mật trên mạng.

3.2.2. Một số kiến nghị cụ thể hoàn thiện pháp luật Việt Nam về bảo vệ thông tin người tiêu dùng

Nhằm hiện thực hóa các định hướng chung nêu trên, dưới đây là các kiến nghị cụ thể tập trung vào hoàn thiện pháp luật và nâng cao hiệu quả thực thi nhằm bảo vệ tốt hơn thông tin người tiêu dùng, đảm bảo quyền riêng tư, an toàn dữ liệu trong bối cảnh kinh tế số ngày càng phát triển.

3.2.2.1. Giải pháp hoàn thiện pháp luật

Việc hoàn thiện khung pháp lý về bảo vệ thông tin người tiêu dùng không chỉ cần tập trung vào việc bổ sung các quy định mới mà còn phải làm rõ, chi tiết hóa những nguyên tắc, quyền và nghĩa vụ liên quan. Các giải pháp cụ thể như sau:

Thứ nhất, cụ thể hóa và làm rõ các quy định về việc thu thập, xử lý thông tin cá nhân

Hiện nay, nhiều quy định trong Luật Bảo vệ quyền lợi người tiêu dùng (sửa đổi 2023) và Nghị định 13/2023/NĐ-CP vẫn còn chung chung về nguyên tắc thu thập và xử lý thông tin cá nhân. Do đó, cần ban hành các văn bản hướng dẫn chi tiết, quy định rõ các tiêu chuẩn sau: *Minh bạch trong thu thập thông tin*, doanh nghiệp phải thông báo rõ mục đích, phạm vi và loại dữ liệu thu thập đến người tiêu dùng trước khi thực hiện. Người tiêu dùng phải được cung cấp thông tin đầy đủ, dễ hiểu về việc thu thập dữ liệu để họ có thể đưa ra quyết định sáng suốt; *Nguyên tắc tối thiểu hóa dữ liệu*, chỉ được thu thập những thông tin cần thiết phục vụ mục đích đã công bố, tránh thu thập dư thừa, gây xâm phạm quyền riêng tư; *Bắt buộc sự đồng ý rõ ràng*, cần quy định chặt chẽ hơn về việc doanh nghiệp phải xin phép người tiêu dùng trước khi thu thập, xử lý dữ liệu (theo cơ chế opt-in), tránh tình trạng đồng ý ngầm hoặc ép buộc; *Quy định về chuyển giao và*

chia sẻ dữ liệu, phải có sự đồng ý cụ thể của người tiêu dùng trước khi dữ liệu được chuyển giao cho bên thứ ba, đồng thời quy định rõ trách nhiệm và nghĩa vụ của các bên trong việc bảo vệ dữ liệu khi chuyển giao.

Thứ hai, tăng cường quyền của người tiêu dùng đối với dữ liệu cá nhân

Luật cần quy định mạnh mẽ hơn các quyền của người tiêu dùng, bao gồm: *Quyền truy cập và chỉnh sửa*, người tiêu dùng có quyền yêu cầu doanh nghiệp cung cấp bản sao dữ liệu cá nhân đang được lưu trữ, đồng thời có quyền chỉnh sửa hoặc cập nhật thông tin khi phát hiện sai sót; *Quyền xóa dữ liệu (quyền bị lãng quên)*, cho phép người tiêu dùng yêu cầu xóa dữ liệu cá nhân khi không còn cần thiết cho mục đích thu thập hoặc khi người tiêu dùng rút lại sự đồng ý; *Quyền rút lại sự đồng ý*, người tiêu dùng có thể bất cứ lúc nào rút lại sự đồng ý đối với việc sử dụng thông tin cá nhân mà không gặp khó khăn hay bị hạn chế; *Quyền phản đối và khiếu nại*, quy định rõ cơ chế, thủ tục để người tiêu dùng có thể phản đối việc sử dụng dữ liệu cá nhân sai mục đích, đồng thời có quyền khiếu nại hoặc khởi kiện doanh nghiệp vi phạm.

Thứ ba, xây dựng chế tài xử phạt nghiêm minh, có tính răn đe cao

Các biện pháp xử lý vi phạm về bảo vệ thông tin cá nhân hiện nay còn thiếu tính nghiêm minh và chưa đủ sức răn đe: *Tăng mức xử phạt*, đề xuất tăng mức phạt hành chính tối đa đối với các hành vi vi phạm về bảo vệ thông tin cá nhân, bao gồm phạt tiền lớn, đình chỉ hoạt động, thu hồi giấy phép; *Mở rộng hình thức xử phạt*, cân nhắc áp dụng xử lý hình sự đối với các hành vi thu thập, sử dụng, rò rỉ thông tin cá nhân với quy mô lớn, gây thiệt hại nghiêm trọng; *Bồi thường thiệt hại*, luật cần quy định rõ nghĩa vụ bồi thường thiệt hại vật chất, tinh thần cho người tiêu dùng khi thông tin cá nhân bị xâm phạm, làm rõ cơ chế giải quyết tranh chấp, bảo vệ quyền lợi của người tiêu dùng; *Bắt buộc công khai khắc phục hậu quả*, bác doanh nghiệp vi phạm phải công khai xin lỗi, khắc phục hậu quả như cải thiện hệ thống bảo mật, hỗ trợ người tiêu dùng.

Thứ tư, xây dựng cơ quan quản lý chuyên trách độc lập về bảo vệ dữ liệu cá nhân

Hiện nay, việc quản lý, giám sát và xử lý vi phạm về bảo vệ thông tin người tiêu dùng còn phân tán giữa nhiều cơ quan chuyên ngành. Để nâng cao hiệu quả thực thi pháp luật: *Thành lập cơ quan chuyên trách*, cần có một Ủy ban hoặc Cơ quan bảo vệ dữ liệu cá nhân độc lập, chịu trách nhiệm chính trong việc giám sát, thanh tra, xử lý vi phạm

và hướng dẫn thực hiện pháp luật; *Quy định rõ quyền hạn*, cơ quan này cần có quyền thu thập thông tin, tiến hành thanh tra đột xuất, áp dụng biện pháp xử lý vi phạm, phối hợp với các cơ quan chức năng khác; *Tăng cường nguồn lực*, đảm bảo cơ quan được trang bị đầy đủ nguồn lực về nhân lực, công nghệ, tài chính để thực hiện nhiệm vụ.

Thứ năm, hoàn thiện các quy định về an toàn kỹ thuật và bảo mật dữ liệu: Ban hành tiêu chuẩn kỹ thuật bắt buộc, thiết lập các tiêu chuẩn bảo mật tối thiểu mà doanh nghiệp phải tuân thủ, bao gồm việc mã hóa dữ liệu, bảo vệ chống truy cập trái phép, sao lưu, phục hồi dữ liệu; *Báo cáo rủi ro bảo mật*, doanh nghiệp phải định kỳ báo cáo đánh giá an ninh thông tin và các sự cố bảo mật cho cơ quan quản lý, đồng thời có trách nhiệm công bố minh bạch với người tiêu dùng; *Khuyến khích ứng dụng công nghệ mới*, áp dụng trí tuệ nhân tạo, blockchain, xác thực đa yếu tố để tăng cường bảo vệ dữ liệu, nâng cao khả năng phát hiện và phòng ngừa rủi ro.

3.2.2.2. Giải pháp nhằm nâng cao hiệu quả hoạt động thực hiện pháp luật trên thực tế

Để bảo vệ quyền lợi người tiêu dùng một cách thực chất, việc hoàn thiện khung pháp lý là cần thiết, song quan trọng hơn là phải đảm bảo hiệu quả thực thi pháp luật trên thực tế. Dưới đây là một số giải pháp trọng điểm nhằm nâng cao hiệu quả thực hiện các quy định bảo vệ thông tin người tiêu dùng:

Thứ nhất, tăng cường năng lực cho các cơ quan quản lý và thanh tra

Đào tạo, bồi dưỡng chuyên môn: Cần tổ chức các khóa đào tạo chuyên sâu về kỹ thuật bảo vệ dữ liệu, xử lý vi phạm và pháp luật liên quan cho cán bộ thanh tra, kiểm tra, điều tra. Việc này giúp nâng cao năng lực nhận diện, xử lý các vi phạm phức tạp trong lĩnh vực bảo vệ thông tin người tiêu dùng.

Trang bị công nghệ hiện đại: Các cơ quan chức năng cần được đầu tư các công cụ kỹ thuật số hiện đại như phần mềm phát hiện xâm nhập, hệ thống giám sát mạng, phân tích dữ liệu lớn... để chủ động phát hiện các vi phạm, rò rỉ thông tin, hành vi thu thập dữ liệu trái phép.

Tăng cường phối hợp liên ngành: Do tính chất đa ngành của việc bảo vệ thông tin cá nhân, các cơ quan như Bộ Công Thương, Bộ Thông tin và Truyền thông, Bộ Công

an, Ủy ban bảo vệ dữ liệu... cần xây dựng cơ chế phối hợp chặt chẽ, trao đổi thông tin kịp thời và xử lý nhanh các vụ việc vi phạm.

Thứ hai, đẩy mạnh công tác thanh tra, kiểm tra và xử lý vi phạm

Tổ chức thanh tra định kỳ và đột xuất: Các cuộc thanh tra, kiểm tra nên được tổ chức thường xuyên, đặc biệt với các doanh nghiệp lớn, các nền tảng thương mại điện tử, dịch vụ tài chính số... Đây là biện pháp phòng ngừa, ngăn chặn vi phạm trước khi xảy ra thiệt hại lớn.

Xử phạt nghiêm minh, công khai: Việc xử lý các vi phạm cần đảm bảo tính nghiêm minh, minh bạch, công khai danh sách các doanh nghiệp vi phạm để tăng sức răn đe và nâng cao ý thức tuân thủ. Điều này cũng giúp người tiêu dùng nhận biết, tránh lựa chọn các dịch vụ kém an toàn.

Khuyến khích tố giác vi phạm: Cần xây dựng kênh tiếp nhận phản ánh, tố giác vi phạm từ người tiêu dùng và các tổ chức xã hội, đồng thời bảo vệ người tố giác khỏi các hành vi trả thù. Việc này tạo ra cơ chế giám sát xã hội, hỗ trợ cơ quan quản lý phát hiện vi phạm nhanh chóng.

Thứ ba, nâng cao nhận thức và kỹ năng bảo vệ thông tin cho người tiêu dùng

Triển khai các chiến dịch truyền thông quy mô lớn: Cần tổ chức các chiến dịch truyền thông rộng rãi, sử dụng đa dạng các kênh như truyền hình, mạng xã hội, báo chí, hội thảo cộng đồng để phổ biến kiến thức về quyền lợi và cách bảo vệ thông tin cá nhân.

Xây dựng tài liệu hướng dẫn cụ thể: Các tài liệu, cẩm nang hướng dẫn người tiêu dùng cách kiểm tra, bảo mật thông tin cá nhân khi giao dịch trực tuyến, nhận diện các dấu hiệu lừa đảo, thu thập dữ liệu trái phép... cần được soạn thảo dễ hiểu, dễ tiếp cận.

Tăng cường hợp tác với các tổ chức xã hội và doanh nghiệp: Các tổ chức bảo vệ người tiêu dùng, hiệp hội doanh nghiệp cùng phối hợp để thực hiện các chương trình đào tạo, nâng cao nhận thức cộng đồng, góp phần xây dựng môi trường thương mại điện tử an toàn.

Thứ tư, thúc đẩy ứng dụng công nghệ bảo vệ thông tin

Khuyến khích doanh nghiệp áp dụng công nghệ bảo mật tiên tiến: Nhà nước cần

có chính sách hỗ trợ, ưu đãi để doanh nghiệp đầu tư vào các giải pháp bảo mật như mã hóa dữ liệu, hệ thống xác thực đa yếu tố, công nghệ blockchain trong lưu trữ dữ liệu.

Phát triển hệ sinh thái an toàn thông tin: Tạo môi trường thuận lợi cho các doanh nghiệp công nghệ an ninh mạng phát triển, cung cấp dịch vụ giám sát, phát hiện xâm nhập và xử lý sự cố kịp thời, giảm thiểu rủi ro cho người tiêu dùng.

Xây dựng hệ thống cảnh báo sớm: Thiết lập các trung tâm giám sát, cảnh báo sớm các nguy cơ tấn công mạng, rò rỉ dữ liệu trên quy mô quốc gia, giúp các bên liên quan phản ứng nhanh, bảo vệ hiệu quả thông tin người tiêu dùng.

Thứ năm, xây dựng cơ chế phản hồi và hỗ trợ người tiêu dùng

Thiết lập đường dây nóng, kênh hỗ trợ: Các cơ quan quản lý cần thiết lập kênh phản ánh, tư vấn về các vấn đề liên quan đến bảo vệ thông tin người tiêu dùng, giúp người dân giải quyết khiếu nại, khiếu kiện kịp thời.

Hỗ trợ pháp lý và bồi thường: Cần có cơ chế hỗ trợ pháp lý cho người tiêu dùng khi bị xâm phạm dữ liệu cá nhân, đồng thời quy định rõ trách nhiệm bồi thường thiệt hại của doanh nghiệp vi phạm.

Việc hoàn thiện và nâng cao hiệu quả thực thi pháp luật về bảo vệ thông tin người tiêu dùng không thể tách rời giữa khung pháp lý chặt chẽ và năng lực thực thi mạnh mẽ. Cần sự phối hợp toàn diện giữa Nhà nước, doanh nghiệp và người tiêu dùng nhằm xây dựng một môi trường bảo mật thông tin tin cậy, góp phần thúc đẩy phát triển thương mại điện tử và kinh tế số tại Việt Nam.

3.2.2.3. Giải pháp nhằm nâng cao hiệu quả hoạt động thực hiện pháp luật trên thực tế tại tỉnh Bình Thuận

Tỉnh Bình Thuận, với vị trí địa lý và sự phát triển kinh tế – xã hội đặc thù, đang chứng kiến sự bùng nổ của thương mại điện tử và các dịch vụ số, đặc biệt trong các ngành du lịch, bán lẻ, vận tải và dịch vụ trực tuyến. Tuy nhiên, việc bảo vệ thông tin người tiêu dùng tại địa phương còn nhiều hạn chế do sự chưa đồng bộ trong nhận thức, năng lực quản lý và mức độ áp dụng pháp luật. Do đó, để nâng cao hiệu quả thực thi pháp luật về bảo vệ thông tin người tiêu dùng trên địa bàn tỉnh, cần tập trung triển khai một số giải pháp trọng tâm sau:

Thứ nhất, tăng cường công tác tuyên truyền, phổ biến pháp luật sát với thực tiễn địa phương

Tỉnh Bình Thuận cần tổ chức thường xuyên các chương trình tuyên truyền, tập huấn, hội thảo về bảo vệ thông tin người tiêu dùng dành cho cán bộ quản lý nhà nước, doanh nghiệp và người dân, đặc biệt là các nhóm đối tượng dễ bị tổn thương như người tiêu dùng trẻ, người lớn tuổi hoặc ít tiếp xúc với công nghệ số. Các nội dung cần được lồng ghép các ví dụ thực tiễn về các vụ việc vi phạm quyền riêng tư tại địa phương, qua đó nâng cao nhận thức và ý thức cảnh giác cho cộng đồng.

Ví dụ, Sở Công Thương Bình Thuận có thể phối hợp với Trung tâm Xúc tiến thương mại và Sở Thông tin và Truyền thông xây dựng các chuyên đề đào tạo về bảo mật dữ liệu cá nhân cho các doanh nghiệp du lịch trực tuyến, đồng thời phát động các chiến dịch truyền thông trên các phương tiện đại chúng và mạng xã hội nhằm phổ biến quyền và trách nhiệm của người tiêu dùng.

Thứ hai, nâng cao năng lực và trang bị công cụ cho các lực lượng thực thi pháp luật

Việc kiểm tra, giám sát và xử lý các hành vi vi phạm về bảo vệ thông tin người tiêu dùng đòi hỏi sự chuyên nghiệp, chính xác và kịp thời. Do đó, tỉnh Bình Thuận cần đầu tư nguồn lực cho các cơ quan chuyên trách như Cục Quản lý thị trường, Công an tỉnh, Sở Thông tin và Truyền thông... trong việc đào tạo chuyên môn, trang bị phần mềm, công cụ kỹ thuật giám sát các giao dịch điện tử, phát hiện hành vi thu thập, sử dụng trái phép thông tin cá nhân.

Công tác phối hợp liên ngành giữa các đơn vị cũng cần được củng cố nhằm tạo ra “mặt trận chung” trong đấu tranh xử lý vi phạm, tránh tình trạng đơn vị này làm tròn trách nhiệm nhưng thiếu thông tin phối hợp với đơn vị khác.

Thứ ba, xây dựng cơ chế hỗ trợ, tư vấn pháp lý cho doanh nghiệp và người tiêu dùng

Tỉnh Bình Thuận có thể thành lập các điểm tư vấn pháp luật chuyên sâu về bảo vệ dữ liệu cá nhân và quyền người tiêu dùng tại các trung tâm thương mại, các khu công nghiệp, khu du lịch lớn và các địa bàn trọng điểm. Tại đây, doanh nghiệp và người dân

được tư vấn về quy định pháp luật, cách thức xây dựng chính sách bảo mật, cũng như giải đáp thắc mắc về quyền lợi khi bị xâm phạm thông tin.

Ví dụ, Trung tâm Xúc tiến Thương mại tỉnh có thể phối hợp với Hiệp hội doanh nghiệp để tổ chức các buổi tư vấn pháp luật định kỳ cho các doanh nghiệp nhỏ và vừa, đặc biệt trong lĩnh vực thương mại điện tử.

Thứ tư, khuyến khích áp dụng công nghệ hiện đại trong bảo vệ dữ liệu

Các doanh nghiệp trên địa bàn, nhất là trong các lĩnh vực dịch vụ trực tuyến, du lịch, bán lẻ, nên được khuyến khích và hỗ trợ kỹ thuật trong việc ứng dụng các giải pháp công nghệ bảo mật như mã hóa dữ liệu, xác thực đa yếu tố, giám sát truy cập và phòng chống tấn công mạng. Tỉnh có thể phối hợp với các nhà cung cấp dịch vụ công nghệ thông tin uy tín để xây dựng các chương trình hỗ trợ kỹ thuật, đào tạo cho doanh nghiệp về các công cụ bảo vệ thông tin.

Chẳng hạn, một số doanh nghiệp du lịch trực tuyến ở Bình Thuận đã bắt đầu áp dụng phần mềm quản lý dữ liệu khách hàng có tính năng bảo mật nâng cao, giảm thiểu rủi ro rò rỉ thông tin.

Thứ năm, xây dựng hệ thống giám sát, phản hồi hiệu quả và xử lý kịp thời các khiếu nại

Tỉnh cần thiết lập hệ thống tiếp nhận, xử lý các phản ánh, khiếu nại của người tiêu dùng liên quan đến việc xâm phạm thông tin cá nhân một cách nhanh chóng và minh bạch. Việc này không chỉ giúp bảo vệ quyền lợi người tiêu dùng mà còn góp phần phát hiện các hành vi vi phạm để xử lý nghiêm minh, tạo tính răn đe.

Ví dụ, Cục Quản lý thị trường Bình Thuận có thể phối hợp với các đơn vị truyền thông để quảng bá rộng rãi đường dây nóng, địa chỉ tiếp nhận khiếu nại, đảm bảo người dân và doanh nghiệp dễ dàng tiếp cận khi cần hỗ trợ.

Thứ sáu, đẩy mạnh phối hợp liên ngành và tăng cường kết nối với cơ quan trung ương

Thực tiễn thực thi pháp luật tại tỉnh Bình Thuận sẽ hiệu quả hơn khi có sự hỗ trợ chặt chẽ từ các cơ quan quản lý nhà nước cấp trung ương như Bộ Công Thương, Bộ Thông tin và Truyền thông. Việc trao đổi thông tin, chia sẻ dữ liệu và phối hợp trong

các chiến dịch thanh tra, kiểm tra sẽ giúp phát hiện và xử lý kịp thời các hành vi vi phạm về bảo vệ thông tin người tiêu dùng.

Việc tham gia các chương trình hợp tác quốc tế về bảo vệ dữ liệu cá nhân cũng góp phần nâng cao năng lực và áp dụng các mô hình quản lý tiên tiến, phù hợp với thực tiễn địa phương.

Tóm lại, việc nâng cao hiệu quả hoạt động thực thi pháp luật về bảo vệ thông tin người tiêu dùng tại tỉnh Bình Thuận không chỉ là trách nhiệm của các cơ quan nhà nước mà còn cần sự đồng thuận và hợp tác từ phía doanh nghiệp và cộng đồng. Một hệ thống pháp luật đồng bộ, năng lực thực thi mạnh mẽ cùng nhận thức cao của người dân sẽ tạo nền tảng vững chắc cho việc bảo vệ quyền lợi của người tiêu dùng trong thời đại số hiện nay.

KẾT LUẬN CHƯƠNG 3

Chương 3 đã làm rõ thực trạng thực tiễn về việc thực thi pháp luật bảo vệ thông tin người tiêu dùng tại Việt Nam nói chung và tỉnh Bình Thuận nói riêng. Qua đánh giá, có thể nhận thấy mặc dù pháp luật về bảo vệ thông tin người tiêu dùng đã đạt được một số kết quả tích cực, đặc biệt là sự hoàn thiện khung pháp lý với các văn bản quan trọng như Luật Bảo vệ quyền lợi người tiêu dùng (sửa đổi 2023) và Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, cùng với các hoạt động thanh tra, tuyên truyền và ứng dụng công nghệ của các doanh nghiệp lớn, thì vẫn còn tồn tại nhiều hạn chế và bất cập nghiêm trọng trong quá trình thực hiện.

Những hạn chế này gồm việc thiếu đồng bộ và chồng chéo trong hệ thống pháp luật, công tác thực thi còn yếu kém với tỷ lệ xử lý vi phạm thấp, chưa có cơ chế giám sát độc lập đủ mạnh, nhận thức và kỹ năng bảo vệ dữ liệu của người tiêu dùng còn hạn chế, đặc biệt là tại các địa phương như Bình Thuận, nơi công tác tuyên truyền và kiểm tra vẫn chưa đạt yêu cầu. Nguyên nhân chủ yếu xuất phát từ việc pháp luật mới được ban hành chưa có thời gian triển khai đồng bộ, thiếu nguồn nhân lực chuyên môn, doanh nghiệp ưu tiên lợi ích kinh tế hơn tuân thủ pháp luật, ý thức người tiêu dùng còn yếu, và mức xử phạt chưa đủ răn đe.

Từ thực trạng đó, chương đã đề xuất các kiến nghị hoàn thiện pháp luật và giải pháp nâng cao hiệu quả thực thi trên thực tế, trong đó tập trung vào việc hoàn thiện khung pháp lý, tăng cường công tác thanh tra, kiểm tra, nâng cao nhận thức cộng đồng, ứng dụng công nghệ bảo vệ dữ liệu, xây dựng cơ chế tư vấn pháp lý, cải thiện phối hợp liên ngành và đặc biệt là các giải pháp mang tính địa phương phù hợp với tình hình của tỉnh Bình Thuận.

Những kiến nghị và giải pháp này không chỉ nhằm nâng cao hiệu lực pháp luật mà còn góp phần xây dựng môi trường kinh doanh minh bạch, bảo vệ quyền lợi hợp pháp của người tiêu dùng trong bối cảnh kinh tế số ngày càng phát triển mạnh mẽ. Việc triển khai đồng bộ các biện pháp trên sẽ giúp tăng cường sự tin tưởng của người tiêu dùng và thúc đẩy sự phát triển bền vững của thị trường tại Bình Thuận cũng như trên toàn quốc.

KẾT LUẬN

Đề án đã hệ thống, phân tích một cách toàn diện các khía cạnh liên quan đến pháp luật về bảo vệ thông tin người tiêu dùng từ lý luận đến thực tiễn tại Việt Nam, đặc biệt là trên địa bàn tỉnh Bình Thuận. Qua ba chương nghiên cứu, một bức tranh tổng thể về vị trí, vai trò, cơ sở pháp lý cũng như những vấn đề đặt ra trong công tác bảo vệ thông tin người tiêu dùng đã được làm sáng tỏ.

Đề án đã tập trung làm rõ các khái niệm cơ bản, phạm vi, vai trò và tầm quan trọng của việc bảo vệ thông tin người tiêu dùng trong bối cảnh phát triển kinh tế số và thương mại điện tử. Bên cạnh đó, sự so sánh, đối chiếu với các mô hình pháp luật quốc tế tiêu biểu đã góp phần mở rộng hiểu biết, đồng thời tạo cơ sở để tham khảo, áp dụng phù hợp vào thực tiễn Việt Nam.

Đề án đi sâu vào nghiên cứu hệ thống pháp luật Việt Nam hiện hành về bảo vệ thông tin người tiêu dùng, đánh giá các quy định pháp lý, các biện pháp và trách nhiệm thực thi. Qua đó cho thấy mặc dù đã có nhiều văn bản pháp luật được ban hành nhằm bảo vệ quyền lợi người tiêu dùng, song vẫn còn tồn tại nhiều hạn chế, đặc biệt là về sự đồng bộ, tính khả thi và hiệu quả thực thi pháp luật. Những bất cập này không chỉ gây khó khăn trong quản lý mà còn ảnh hưởng trực tiếp đến quyền và lợi ích hợp pháp của người tiêu dùng.

Đề án tập trung phân tích thực trạng thực tiễn bảo vệ thông tin người tiêu dùng tại Việt Nam và tỉnh Bình Thuận, chỉ ra những thành tựu đạt được, đồng thời phản ánh rõ các hạn chế, nguyên nhân và khó khăn trong quá trình thực thi pháp luật. Trên cơ sở đó, luận văn đề xuất các kiến nghị cụ thể nhằm hoàn thiện khung pháp luật và nâng cao hiệu quả thực thi, góp phần xây dựng môi trường bảo vệ thông tin cá nhân ngày càng an toàn, minh bạch và bền vững.

Từ tổng thể nghiên cứu, có thể khẳng định rằng việc hoàn thiện và thực thi pháp luật bảo vệ thông tin người tiêu dùng không chỉ là yêu cầu cấp thiết trong bối cảnh chuyển đổi số và thương mại điện tử phát triển nhanh chóng, mà còn là tiền đề quan trọng để tạo dựng niềm tin và thúc đẩy sự phát triển kinh tế – xã hội lành mạnh, bền vững.

Đồng thời, nghiên cứu cũng mở ra nhiều hướng đi cho các nghiên cứu sâu hơn

về các biện pháp kỹ thuật, công nghệ mới, cũng như chính sách phù hợp với điều kiện đặc thù của từng địa phương. Việc tiếp tục hoàn thiện và áp dụng hiệu quả pháp luật bảo vệ thông tin người tiêu dùng sẽ là yếu tố quyết định giúp Việt Nam thích ứng với xu hướng phát triển toàn cầu và bảo vệ quyền lợi của người dân trong kỷ nguyên số.

DANH MỤC TÀI LIỆU THAM KHẢO

A. Tài liệu tiếng Việt

1. Văn bản pháp luật

Luật Bảo vệ quyền lợi người tiêu dùng (sửa đổi năm 2023).

Nghị định số 13/2023/NĐ-CP về chi tiết thi hành Luật Bảo vệ quyền lợi người tiêu dùng.

Luật An ninh mạng năm 2018.

Luật Giao dịch điện tử năm 2005 (sửa đổi, bổ sung năm 2015).

Luật Viễn thông năm 2009 (sửa đổi bổ sung năm 2017).

Các quy định của Bộ Công Thương và các văn bản pháp luật liên quan đến bảo vệ dữ liệu cá nhân người tiêu dùng.

Văn bản hướng dẫn, chỉ thị của UBND tỉnh Bình Thuận về quản lý và bảo vệ thông tin người tiêu dùng

2. Luận văn, luận án, đề tài nghiên cứu

Trần Thị Hồng Hạnh (2018), *Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay*, Luận án Tiến sĩ, Học viện Chính trị Quốc gia Hồ Chí Minh.

Lê Thị Thảo (2021), *Pháp luật bảo vệ quyền riêng tư của cá nhân trong hoạt động thương mại điện tử ở Việt Nam hiện nay*, Luận án Tiến sĩ Luật học, Học viện Khoa học xã hội, Viện Hàn lâm Khoa học Xã hội Việt Nam.

Trần Quốc Bình (2020), *Pháp luật bảo vệ dữ liệu cá nhân ở Việt Nam trong bối cảnh hội nhập quốc tế*, Luận án Tiến sĩ Luật học, Đại học Quốc gia Hà Nội.

Nguyễn Thanh Tùng (2022), *Pháp luật về bảo vệ thông tin cá nhân trong lĩnh vực thương mại điện tử: Kinh nghiệm quốc tế và vận dụng vào Việt Nam*, Luận án Tiến sĩ Luật học, Học viện Chính trị Quốc gia Hồ Chí Minh.

Nguyễn Ngọc Phúc Đăng (2018), *Nghiên cứu luật bảo vệ thông tin cá nhân của Singapore và kinh nghiệm cho Việt Nam*, Đề tài Nghiên cứu khoa học Euréka, Trường Đại học Luật TP. Hồ Chí Minh.

Bùi Duy Khánh, Trần Minh Phú, Dương Yên Nhi (2021), *Pháp luật Việt Nam về bảo vệ dữ liệu cá nhân trong giai đoạn cách mạng công nghiệp 4.0 - Bài học kinh nghiệm của các quốc gia trên thế giới*, Giải Nhất giải thưởng Sinh viên nghiên cứu khoa học, Trường Đại học Luật Hà Nội.

3. Báo, tạp chí, tin bài

Lê Văn Hưng (2020), "Vai trò của pháp luật trong bảo vệ thông tin cá nhân của người tiêu dùng trên môi trường mạng", *Nhà nước và Pháp luật*, số 12.

Phan Thị Thu Hằng (2022), "Bảo vệ thông tin cá nhân – quyền cơ bản trong nền kinh tế số", *Thông tin Khoa học Pháp lý*, Bộ Tư pháp, số 4.

Nguyễn Thị Tuyết Nhung (2022), "Bảo vệ dữ liệu cá nhân trong thương mại điện tử ở Việt Nam – Thực trạng và giải pháp", *Luật học*, Trường Đại học Luật Hà Nội, số 5.

Trần Thị Hòa (2021), "Một số vấn đề pháp lý về bảo vệ thông tin người tiêu dùng trong hoạt động thương mại điện tử", *Khoa học Kiểm sát*, số 3.

B. Tài liệu nước ngoài

1. Văn bản pháp luật

Quy định chung về bảo vệ dữ liệu cá nhân (GDPR) của Liên minh châu Âu (EU), 2016.

Luật Bảo vệ thông tin cá nhân (Act on the Protection of Personal Information - APPI), Nhật Bản, 2003 (sửa đổi năm 2017 và các lần sau đó).

Luật Bảo vệ dữ liệu cá nhân (Personal Data Protection Act - PDPA), Singapore, 2012 (cập nhật các sửa đổi mới nhất).

2. Tài liệu tham khảo

Daniel J. Solove & Paul M. Schwartz (2003), *Information Privacy Law*, Aspen Publishers.

Lee A. Bygrave (2014), *Privacy and Data Protection Law*, Oxford University Press.

Daniel J. Solove (2004), *The Digital Person: Technology and Privacy in the Information Age*, New York University Press.

Paul M. Schwartz & Daniel J. Solove (2011), "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *New York University Law Review*, Vol. 86, No. 6.

Viktor Mayer-Schönberger (2009), *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press.

Alan Westin (1967), *Privacy and Freedom*, Atheneum Publishers.