

HỌC VIỆN CHÍNH TRỊ QUỐC GIA HỒ CHÍ MINH

BÙI THỊ THÙY DUNG

HOÀN THIỆN PHÁP LUẬT  
VỀ AN NINH MẠNG Ở VIỆT NAM

LUẬN ÁN TIẾN SĨ  
NGÀNH: LÝ LUẬN VÀ LỊCH SỬ NHÀ NƯỚC VÀ PHÁP LUẬT

HÀ NỘI - 2026

**HỌC VIỆN CHÍNH TRỊ QUỐC GIA HỒ CHÍ MINH**

**BÙI THỊ THÙY DUNG**

**HOÀN THIỆN PHÁP LUẬT  
VỀ AN NINH MẠNG Ở VIỆT NAM**

**LUẬN ÁN TIẾN SĨ**

**NGÀNH: LÝ LUẬN VÀ LỊCH SỬ NHÀ NƯỚC VÀ PHÁP LUẬT**

**Mã số: 9380106**

**Người hướng dẫn khoa học: 1. PGS.TS. Bùi Thị Hạnh**

**2. PGS.TS. Nguyễn Thị Tuyết Mai**

**HÀ NỘI - 2026**

## LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các số liệu, kết quả nêu trong luận án là trung thực, có nguồn gốc rõ ràng và được trích dẫn đầy đủ theo quy định.

**Tác giả**



**Bùi Thị Thùy Dung**

## MỤC LỤC

|                                                                                                                |     |
|----------------------------------------------------------------------------------------------------------------|-----|
| MỞ ĐẦU .....                                                                                                   | 1   |
| Chương 1. TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN .....                                    | 11  |
| 1.1. Những công trình nghiên cứu liên quan đến đề tài luận án .....                                            | 11  |
| 1.2. Khái quát kết quả nghiên cứu liên quan đến đề tài luận án và những vấn đề đặt ra .....                    | 33  |
| 1.3. Giả thuyết và câu hỏi nghiên cứu.....                                                                     | 37  |
| Chương 2. CƠ SỞ LÝ LUẬN CỦA HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG.....                                          | 40  |
| 2.1. Khung lý thuyết nghiên cứu pháp luật về an ninh mạng .....                                                | 40  |
| 2.2. Khái niệm, đặc điểm, vai trò, cấu trúc lý luận của pháp luật về an ninh mạng ở Việt Nam .....             | 46  |
| 2.3. Khái niệm và các tiêu chí hoàn thiện pháp luật về an ninh mạng ở Việt Nam .....                           | 61  |
| 2.4. Điều kiện bảo đảm hoàn thiện pháp luật về an ninh mạng .....                                              | 78  |
| 2.5. Pháp luật quốc tế và một số quốc gia trên thế giới về an ninh mạng và giá trị tham khảo với Việt Nam..... | 85  |
| Chương 3. THỰC TRẠNG PHÁP LUẬT VÀ THỰC TIỄN THỰC HIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM HIỆN NAY.....       | 98  |
| 3.1. Quá trình hình thành, phát triển của pháp luật về an ninh mạng ở Việt Nam .....                           | 98  |
| 3.2. Đánh giá thực trạng pháp luật về an ninh mạng ở Việt Nam hiện nay.....                                    | 108 |
| 3.3. Đánh giá thực tiễn thực hiện pháp luật về an ninh mạng ở Việt Nam hiện nay .....                          | 142 |
| Chương 4. YÊU CẦU, QUAN ĐIỂM VÀ GIẢI PHÁP HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM .....                | 160 |
| 4.1. Yêu cầu hoàn thiện pháp luật về an ninh mạng ở Việt Nam .....                                             | 160 |
| 4.2. Quan điểm hoàn thiện pháp luật về an ninh mạng ở Việt Nam.....                                            | 164 |
| 4.3. Giải pháp hoàn thiện pháp luật về an ninh mạng ở Việt Nam.....                                            | 169 |
| KẾT LUẬN .....                                                                                                 | 197 |
| DANH MỤC CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ.....                                                               | 200 |
| DANH MỤC TÀI LIỆU THAM KHẢO .....                                                                              | 201 |
| PHỤ LỤC .....                                                                                                  | 224 |

## **DANH MỤC CÁC CHỮ VIẾT TẮT**

|        |   |                                  |
|--------|---|----------------------------------|
| ANQG   | : | An ninh quốc gia                 |
| QPPL   | : | Quy phạm pháp luật               |
| SOC    | : | Trung tâm Điều hành An ninh mạng |
| TTATXH | : | Trật tự, an toàn xã hội          |

## MỞ ĐẦU

### 1. Lý do lựa chọn đề tài

Trong bối cảnh hiện nay, cùng với sự phát triển mạnh mẽ của công nghệ số, Internet và các nền tảng kết nối, không gian mạng đã trở thành môi trường thiết yếu đối với hoạt động của Nhà nước, nền kinh tế và đời sống xã hội. Các công nghệ mới như trí tuệ nhân tạo, dữ liệu lớn, điện toán đám mây, Internet vạn vật, blockchain đang làm thay đổi sâu sắc phương thức quản trị quốc gia, mô hình sản xuất, kinh doanh, cung ứng dịch vụ và sinh hoạt xã hội. Tuy nhiên, sự phát triển nhanh chóng đó cũng làm gia tăng các nguy cơ đe dọa an ninh mạng cả về quy mô, tính chất và mức độ nguy hiểm.

Tấn công mạng, gián điệp mạng, lộ, mất dữ liệu, lừa đảo công nghệ cao, phát tán thông tin sai sự thật, xâm phạm bí mật nhà nước, bí mật cá nhân và thao túng không gian mạng đã trở thành những thách thức hiện hữu đối với mọi quốc gia. Bởi vậy, hiện nay, an ninh mạng không còn là vấn đề kỹ thuật đơn lẻ, mà đã trở thành vấn đề chiến lược, trực tiếp liên quan tới an ninh quốc gia (ANQG), trật tự, an toàn xã hội (TTATXH), quyền con người, quyền công dân và năng lực phát triển bền vững của đất nước.

Tại Việt Nam, quá trình xây dựng Chính phủ điện tử, Chính phủ số, kinh tế số và xã hội số đã tạo ra những tiền đề quan trọng cho phát triển đất nước. Kéo theo đó, không gian mạng đã trở thành địa bàn trọng yếu, nhạy cảm, nơi tập trung nhiều nguy cơ xâm phạm ANQG và quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Thực tế, chỉ một điểm yếu pháp lý hoặc khoảng trống về thể chế trong lĩnh vực này cũng có thể dẫn đến hậu quả nghiêm trọng tới chính trị, quốc phòng, an ninh, kinh tế và xã hội.

Nhận thức rõ yêu cầu đó, Đảng và Nhà nước Việt Nam đã ban hành nhiều chủ trương, quan điểm chỉ đạo có ý nghĩa chiến lược đối với bảo vệ Tổ quốc trên không gian mạng, bảo đảm an ninh mạng và thúc đẩy chuyển đổi số. Đặc biệt như: Nghị quyết số 29-NQ/TW ngày 25/7/2018 của Bộ Chính trị

về Chiến lược bảo vệ Tổ quốc trên không gian mạng; Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược an ninh mạng quốc gia; Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia. Có thể nói, những văn bản chỉ đạo trên đã xác định bảo vệ Tổ quốc trên không gian mạng, bảo đảm an ninh mạng là nhiệm vụ trọng yếu, thường xuyên, lâu dài của cả hệ thống chính trị; đồng thời nhấn mạnh vai trò của thể chế như điều kiện tiên quyết, cần hoàn thiện và đi trước một bước.

Hiện nay, hoàn thiện pháp luật về an ninh mạng ở Việt Nam không chỉ là yêu cầu kỹ thuật lập pháp, mà còn là nhiệm vụ chính trị - pháp lý quan trọng nhằm thể chế hóa chủ trương của Đảng về bảo vệ ANQG, bảo đảm TTATXH và thúc đẩy chuyển đổi số. Mục tiêu hướng tới là pháp luật về an ninh mạng phải đủ mạnh để phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng; đồng thời, bảo đảm tính minh bạch, khả thi, nhân văn, tạo lập môi trường pháp lý ổn định cho đổi mới sáng tạo, phát triển kinh tế số và xã hội số.

Hướng tới mục tiêu đó, thời gian qua, Nhà nước ta đã ban hành nhiều văn bản pháp luật quan trọng như Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018 và các văn bản hướng dẫn thi hành. Các văn bản trên đã tạo lập cơ sở pháp lý quan trọng cho việc bảo vệ hệ thống thông tin, bảo vệ ANQG, bảo đảm TTATXH, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng. Bên cạnh đó, ngày 10/12/2025, việc Quốc hội thông qua Luật An ninh mạng số 116/2025/QH15 đã một lần nữa cho thấy xu hướng hoàn thiện pháp luật về an ninh mạng ở Việt Nam theo hướng thống nhất, đồng bộ và phù hợp hơn với yêu cầu quản trị không gian mạng trong bối cảnh chuyển đổi số.

Tuy nhiên, thực tiễn phát triển nhanh chóng của công nghệ và không gian mạng đặt ra yêu cầu phải tiếp tục nghiên cứu toàn diện, hệ thống và chuyên sâu hơn pháp luật về an ninh mạng. Trong đó, tiêu biểu là việc cần

đánh giá mức độ đầy đủ, đồng bộ, khả thi của pháp luật; làm rõ mối quan hệ giữa pháp luật về an ninh mạng với pháp luật về an toàn thông tin mạng, dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, hình sự, tố tụng hình sự và hợp tác quốc tế; đồng thời xác định các giải pháp bảo đảm thi hành pháp luật trong thực tiễn.

Từ những phân tích trên, việc nghiên cứu đề tài “***Hoàn thiện pháp luật về an ninh mạng ở Việt Nam***” là yêu cầu khách quan, cấp bách và có ý nghĩa chiến lược. Đây không chỉ là đòi hỏi xuất phát từ nhiệm vụ bảo vệ ANQG, bảo đảm TTATXH trên không gian mạng, mà còn là điều kiện quan trọng để thể chế hóa quan điểm chỉ đạo của Đảng, đặc biệt là bảo vệ quyền con người, quyền công dân, nâng cao hiệu lực quản lý nhà nước, thúc đẩy đổi mới sáng tạo, phát triển kinh tế số và xây dựng Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam trong kỷ nguyên số.

## **2. Mục tiêu, nhiệm vụ nghiên cứu**

### ***2.1. Mục tiêu nghiên cứu***

Mục tiêu nghiên cứu của luận án là xây dựng cơ sở lý luận vững chắc và xác lập bộ tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng ở Việt Nam và đề xuất các định hướng và giải pháp hoàn thiện pháp luật nhằm nâng cao hiệu quả bảo vệ an ninh mạng trong bối cảnh chuyển đổi số và hội nhập quốc tế, trên cơ sở phân tích thực trạng pháp luật và thực tiễn thi hành.

Luận án hướng tới các mục tiêu cụ thể bao gồm: làm rõ khái niệm, đặc điểm, vai trò, nội dung và yêu cầu của pháp luật về an ninh mạng trong bối cảnh chuyển đổi số và hội nhập quốc tế; xác lập các tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng; đánh giá thực trạng pháp luật theo các tiêu chí đã xác lập; đề xuất định hướng và giải pháp hoàn thiện pháp luật nhằm bảo đảm sự cân bằng giữa yêu cầu bảo vệ ANQG, TTATXH với yêu cầu xây dựng môi trường số an toàn, minh bạch, tôn trọng quyền con người, quyền công dân.

### ***2.2. Nhiệm vụ nghiên cứu***

Để đạt được mục tiêu trên, luận án thực hiện các nhiệm vụ chủ yếu sau:

*Một là*, tổng quan, đánh giá các công trình nghiên cứu trong và ngoài nước có liên quan đến đề tài, qua đó xác định khoảng trống nghiên cứu, câu hỏi nghiên cứu và giả thuyết nghiên cứu.

*Hai là*, xây dựng cơ sở lý luận của của hoàn thiện pháp luật về an ninh mạng; bao gồm khung lý thuyết của hoàn thiện pháp luật về an ninh mạng, vai trò, cấu trúc lý luận của pháp luật về an ninh mạng, khái niệm và các tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng, kinh nghiệm xây dựng pháp luật về an ninh mạng của một số quốc gia, khu vực, tổ chức quốc tế để rút ra giá trị tham khảo phù hợp với Việt Nam.

*Ba là*, phân tích, đánh giá thực trạng pháp luật và thực tiễn thực thi pháp luật về an ninh mạng ở Việt Nam theo các tiêu chí đã xác lập và theo các nhóm chế định cơ bản; chỉ ra ưu điểm, hạn chế, bất cập và nguyên nhân.

*Bốn là*, đề xuất định hướng và giải pháp hoàn thiện pháp luật về an ninh mạng ở Việt Nam nhằm khắc phục khoảng trống, mâu thuẫn, chồng chéo và nâng cao hiệu quả bảo vệ an ninh mạng trong điều kiện chuyển đổi số, đồng thời đảm bảo khả thi, minh bạch và cân bằng lợi ích giữa các chủ thể.

### **3. Đối tượng và phạm vi nghiên cứu**

#### **3.1. Đối tượng nghiên cứu**

Đối tượng nghiên cứu của luận án là pháp luật về an ninh mạng ở Việt Nam dưới góc độ ngành Lý luận và lịch sử nhà nước và pháp luật. Luận án tiếp cận pháp luật về an ninh mạng như một lĩnh vực pháp luật có tính liên ngành, gắn với bảo vệ ANQG, TTATXH, an ninh dữ liệu, quyền con người, quyền công dân và trách nhiệm của các chủ thể trên không gian mạng.

Cụ thể, luận án nghiên cứu sáu nhóm chế định cơ bản của pháp luật về an ninh mạng, gồm: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý hành vi vi phạm; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế trong lĩnh vực an ninh mạng. Bên cạnh đó, luận án cũng nghiên cứu thực tiễn thực hiện pháp luật, quan điểm, chủ trương của Đảng, chính sách của Nhà nước và kinh nghiệm pháp luật của một số quốc gia, khu vực, tổ chức quốc tế có giá trị tham khảo đối với Việt Nam.

### ***3.2. Phạm vi nghiên cứu***

Về nội dung, luận án nghiên cứu pháp luật về an ninh mạng ở Việt Nam theo sáu nhóm chế định cơ bản và đánh giá theo các tiêu chí về nội dung pháp luật, kỹ thuật pháp lý và thực thi pháp luật.

Về không gian, luận án nghiên cứu pháp luật về an ninh mạng tại Việt Nam; đồng thời khảo cứu có chọn lọc pháp luật và kinh nghiệm của một số quốc gia, khu vực, tổ chức quốc tế có giá trị tham khảo đối với Việt Nam như Hoa Kỳ, Liên minh châu Âu, Liên bang Nga, Trung Quốc, Singapore và một số cơ chế hợp tác quốc tế liên quan đến an ninh mạng.

Về thời gian, luận án nghiên cứu hệ thống pháp luật và thực tiễn áp dụng pháp luật về an ninh mạng ở Việt Nam giai đoạn từ khi Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 được ban hành đến hết năm 2025. Việc đánh giá thực trạng pháp luật và thực tiễn áp dụng pháp luật được thực hiện trên cơ sở các quy định pháp luật có hiệu lực và đã được triển khai trong thực tiễn thuộc giai đoạn nghiên cứu. Đối với Luật An ninh mạng số 116/2025/QH15, mặc dù được Quốc hội thông qua trong năm 2025, nhưng do có hiệu lực sau thời điểm kết thúc phạm vi nghiên cứu thực trạng của luận án nên chỉ được sử dụng để tham chiếu xu hướng lập pháp và định hướng tiếp tục hoàn thiện pháp luật trong các phần nghiên cứu có liên quan.

## **4. Cơ sở lý luận và phương pháp nghiên cứu**

### ***4.1. Cơ sở lý luận***

Luận án được nghiên cứu trên nền tảng lý luận của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh về Nhà nước và pháp luật; Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam năm 2013, sửa đổi, bổ sung năm 2025; các điều ước, hiệp định mà Việt Nam tham gia hoặc ký kết; quan điểm chỉ đạo của Đảng, chính sách của Nhà nước về bảo vệ ANQG, bảo đảm TTATXH, bảo vệ quyền con người, quyền công dân, xây dựng Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam và phát triển không gian mạng an toàn, lành mạnh.

#### ***4.2. Phương pháp luận và phương pháp nghiên cứu***

Luận án được thực hiện trên cơ sở phương pháp luận duy vật biện chứng và duy vật lịch sử, pháp luật về an ninh mạng được đặt trong mối quan hệ vận động giữa yêu cầu bảo vệ ANQG, bảo đảm TTATXH, bảo vệ quyền con người, quyền công dân và yêu cầu phát triển không gian mạng an toàn, lành mạnh trong bối cảnh chuyển đổi số. Trên nền tảng phương pháp luận đó, luận án sử dụng kết hợp các phương pháp nghiên cứu pháp lý truyền thống với phương pháp nghiên cứu thực tiễn, nhằm bảo đảm việc phân tích không chỉ ở bình diện quy phạm mà còn kiểm chứng khả năng vận hành của pháp luật trong thực tế.

Phương pháp phân tích quy phạm pháp luật (QPPL) được sử dụng xuyên suốt luận án để làm rõ nội dung, phạm vi điều chỉnh, chủ thể áp dụng, điều kiện áp dụng và hậu quả pháp lý của các quy định về an ninh mạng. Phương pháp này được triển khai thông qua việc phân tích các quy định của Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018, các văn bản hướng dẫn thi hành và những văn bản pháp luật có liên quan về dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, hình sự, tổ tụng hình sự, xử lý vi phạm hành chính và hợp tác quốc tế. Kết quả phân tích được sử dụng để xác định nội dung, cấu trúc, ưu điểm, hạn chế và mức độ hoàn thiện của pháp luật về an ninh mạng theo các nhóm chế định của luận án.

Phương pháp hệ thống hóa và tổng hợp được sử dụng để tập hợp, phân loại các văn bản pháp luật, quan điểm khoa học, báo cáo thực tiễn và tài liệu nghiên cứu có liên quan đến an ninh mạng. Việc hệ thống hóa được thực hiện theo sáu nhóm chế định gồm: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý hành vi vi phạm; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế trong lĩnh vực an ninh mạng. Trên cơ sở đó, luận án tổng hợp các kết quả nghiên cứu để xây dựng khung lý luận, tiêu chí đánh giá và các nhóm giải pháp hoàn thiện pháp luật.

Phương pháp lịch sử pháp lý được sử dụng để phân tích quá trình hình thành và phát triển của pháp luật về an ninh mạng ở Việt Nam qua các giai đoạn. Việc vận dụng phương pháp này nhằm làm rõ sự chuyển biến trong tư duy lập pháp từ quản lý Internet, bảo đảm an toàn thông tin mạng đến bảo vệ an ninh mạng với tư cách là lĩnh vực gắn trực tiếp với ANQG, TTATXH, chủ quyền quốc gia trên không gian mạng và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức.

Phương pháp so sánh pháp luật được sử dụng để khảo cứu có chọn lọc pháp luật và kinh nghiệm của một số quốc gia, khu vực, tổ chức quốc tế về an ninh mạng. Việc so sánh không nhằm sao chép mô hình pháp luật nước ngoài, mà tập trung nhận diện các giá trị tham khảo phù hợp với điều kiện chính trị, pháp lý, kinh tế, xã hội và năng lực thực thi của Việt Nam, nhất là các kinh nghiệm về quản trị rủi ro, bảo vệ hạ tầng thông tin trọng yếu, nghĩa vụ báo cáo sự cố, trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng, bảo vệ dữ liệu và hợp tác quốc tế trong phòng, chống tội phạm mạng.

Phương pháp phân tích tình huống, vụ việc được sử dụng để kiểm tra tính khả thi của các quy định pháp luật trong thực tiễn. Các tình huống, vụ việc được lựa chọn trên cơ sở tính điển hình, mức độ liên quan đến các nhóm chế định của pháp luật về an ninh mạng và khả năng phản ánh những khó khăn trong áp dụng pháp luật, như tấn công mạng, lộ, mất dữ liệu, lừa đảo trực tuyến, phát tán thông tin sai sự thật, mua bán dữ liệu cá nhân, xử lý chứng cứ điện tử và phối hợp với doanh nghiệp cung cấp dịch vụ trên không gian mạng. Kết quả phân tích tình huống được sử dụng để kiểm chứng các nhận định về tính đầy đủ, đồng bộ, khả thi và hiệu quả thực thi của pháp luật.

Phương pháp thống kê mô tả và xử lý dữ liệu thứ cấp được sử dụng thông qua việc khai thác số liệu, báo cáo, bản án, quyết định xử phạt, tài liệu của cơ quan nhà nước, tổ chức quốc tế và các công trình nghiên cứu đã công bố. Các dữ liệu này được phân loại theo nhóm vấn đề nghiên cứu, đối chiếu

với các tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng, từ đó nhận diện xu hướng vi phạm, mức độ tác động, những khó khăn trong tổ chức thực hiện pháp luật và yêu cầu đặt ra đối với hoàn thiện pháp luật.

Phương pháp phỏng vấn, trao đổi chuyên gia được sử dụng như một phương pháp nghiên cứu định tính nhằm kiểm chứng, bổ sung và làm sâu sắc hơn các nhận định của luận án về thực trạng pháp luật, thực tiễn thực hiện pháp luật và giải pháp hoàn thiện pháp luật về an ninh mạng. Luận án thực hiện phỏng vấn, trao đổi với 30 chuyên gia đang công tác, nghiên cứu hoặc tham gia thực tiễn trong lĩnh vực an ninh mạng và các lĩnh vực pháp luật có liên quan. Việc lựa chọn chuyên gia được thực hiện theo các tiêu chí: có kinh nghiệm chuyên môn trực tiếp trong lĩnh vực an ninh mạng; có khả năng cung cấp nhận định độc lập, có căn cứ thực tiễn; bảo đảm sự đa dạng về vị trí công tác và góc nhìn chuyên môn. Việc phỏng vấn, trao đổi được thực hiện trong quá trình hoàn thiện nội dung đánh giá thực trạng và xây dựng giải pháp của luận án. Nội dung phỏng vấn được thiết kế gồm các nhóm câu hỏi về: nhận diện phạm vi pháp luật về an ninh mạng; mức độ đầy đủ, đồng bộ, khả thi và minh bạch của các quy định hiện hành; khó khăn trong phát hiện, xử lý hành vi vi phạm... Ý kiến chuyên gia được ghi nhận bằng phiếu trao đổi, ghi chép nghiên cứu hoặc tổng hợp nội dung trả lời theo chủ đề. Các ý kiến được mã hóa theo nhóm chủ thể và chủ đề nội dung, sau đó được đối chiếu, phân loại và sử dụng như nguồn dữ liệu định tính để kiểm chứng, bổ sung cho các nhận định trong luận án. Kết quả phỏng vấn có vai trò hỗ trợ nhận diện vấn đề thực tiễn, làm rõ nguyên nhân hạn chế và kiểm tra tính khả thi của các kiến nghị hoàn thiện pháp luật.

Về việc sử dụng phương pháp theo từng chương, Chương 1 sử dụng phương pháp tổng quan tài liệu, phân tích, tổng hợp và phê bình học thuật để xác định khoảng trống nghiên cứu, câu hỏi nghiên cứu và giả thuyết nghiên cứu. Chương 2 sử dụng phương pháp phân tích khái niệm, phân tích QPPL,

hệ thống hóa, tổng hợp và so sánh pháp luật để xây dựng cơ sở lý luận, tiêu chí hoàn thiện pháp luật và giá trị tham khảo từ kinh nghiệm nước ngoài. Chương 3 sử dụng phương pháp phân tích QPPL, thống kê mô tả, phân tích tình huống, tổng hợp thực tiễn và phỏng vấn chuyên gia để đánh giá thực trạng pháp luật và thực tiễn thực hiện pháp luật về an ninh mạng ở Việt Nam. Chương 4 sử dụng phương pháp tổng hợp, suy luận pháp lý, đánh giá tính khả thi và kết quả tham vấn chuyên gia để đề xuất quan điểm, yêu cầu và giải pháp hoàn thiện pháp luật về an ninh mạng ở Việt Nam.

### **5. Những đóng góp mới về khoa học của luận án**

Luận án có một số đóng góp mới về khoa học như sau:

*Thứ nhất*, luận án góp phần bổ sung, phát triển cơ sở lý luận và thực tiễn của pháp luật về an ninh mạng ở Việt Nam. Trên cơ sở làm rõ khái niệm, đặc điểm, vai trò, nội dung của pháp luật về an ninh mạng, luận án xây dựng cơ sở khoa học để đánh giá mức độ hoàn thiện của lĩnh vực pháp luật này; đồng thời, phân tích quy định pháp luật hiện hành theo các nhóm chế định cơ bản, nhằm nhận diện những khoảng trống pháp lý, sự chồng chéo, thiếu thống nhất và hạn chế trong cơ chế thực thi. Từ đó, luận án đề xuất định hướng và giải pháp hoàn thiện pháp luật về an ninh mạng ở Việt Nam trên các phương diện thể chế, tổ chức thực thi, phối hợp giữa các chủ thể, phát triển nguồn lực và hợp tác quốc tế, góp phần nâng cao hiệu quả bảo vệ ANQG, bảo đảm TTATXH trên không gian mạng.

*Thứ hai*, luận án làm rõ những yêu cầu mới đặt ra đối với việc hoàn thiện pháp luật về an ninh mạng trong bối cảnh chuyển đổi số, phát triển kinh tế số, dữ liệu số, trí tuệ nhân tạo và hội nhập quốc tế. Luận án luận giải sự cần thiết phải bảo đảm hài hòa giữa yêu cầu bảo vệ ANQG, bảo đảm TTATXH với bảo vệ quyền con người, quyền công dân trên không gian mạng; qua đó góp phần định hướng hoàn thiện pháp luật về an ninh mạng theo hướng hiện đại, đồng bộ, khả thi và phù hợp với yêu cầu quản trị không gian mạng trong tình hình mới.

## **6. Ý nghĩa lý luận và thực tiễn của luận án**

### **6.1. Về lý luận**

Luận án góp phần hệ thống hóa và làm rõ cơ sở lý luận về pháp luật an ninh mạng, tiêu chí đánh giá mức độ hoàn thiện pháp luật và điều kiện bảo đảm hoàn thiện pháp luật về an ninh mạng. Luận án cũng nghiên cứu kinh nghiệm pháp luật về an ninh mạng của một số quốc gia, khu vực, tổ chức quốc tế, từ đó chỉ ra những vấn đề có giá trị tham khảo đối với Việt Nam.

Bên cạnh đó, luận án hệ thống hóa, phân tích những bất cập, thiếu sót trong sáu nhóm chế định lớn của pháp luật về an ninh mạng; đồng thời xác định, luận giải các giải pháp hoàn thiện và bảo đảm thực thi hiệu quả pháp luật về an ninh mạng trong bối cảnh Việt Nam hiện nay.

### **6.2. Về thực tiễn**

Luận án là tài liệu tham khảo có giá trị đối với các chủ thể thực hiện nhiệm vụ lập pháp, lập quy, quản lý nhà nước, xây dựng và tổ chức thi hành pháp luật về an ninh mạng ở Việt Nam, đặc biệt trong quá trình sửa đổi, bổ sung, ban hành các văn bản QPPL có liên quan.

Đồng thời, luận án có thể được sử dụng làm tài liệu học thuật, tài liệu tham khảo trong đào tạo, bồi dưỡng, nghiên cứu về pháp luật an ninh mạng, quản lý nhà nước trên không gian mạng và công tác bảo đảm an ninh mạng tại các cơ quan, tổ chức có liên quan.

## **7. Kết cấu của luận án**

Ngoài phần mở đầu, kết luận, phụ lục và danh mục tài liệu tham khảo, nội dung luận án được kết cấu gồm 04 chương, 14 tiết.

## Chương 1

### TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN

#### 1.1. NHỮNG CÔNG TRÌNH NGHIÊN CỨU LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN

##### 1.1.1. Những công trình nghiên cứu lý luận hoàn thiện pháp luật về an ninh mạng

###### 1.1.1.1. Nhóm công trình nghiên cứu trong nước

(1) Các công trình nghiên cứu là sách:

- Cuốn sách *Hoàn thiện hệ thống pháp luật đáp ứng yêu cầu xây dựng Nhà nước pháp quyền xã hội chủ nghĩa ở Việt Nam hiện nay* của Đào Trí Úc và Trương Thị Hồng Hà [86] là công trình có giá trị lý luận quan trọng trong nghiên cứu về hoàn thiện pháp luật. Công trình đã luận giải các tiêu chí cơ bản đánh giá chất lượng hệ thống pháp luật như tính toàn diện, tính đồng bộ, tính minh bạch, tính ổn định tương đối, tính phù hợp với thực tiễn và yêu cầu về kỹ thuật lập pháp. Luận án kế thừa các luận điểm này trong Chương 2 để xây dựng khung tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng ở Việt Nam. Tuy nhiên, công trình chủ yếu tiếp cận ở bình diện lý luận chung, chưa đi sâu nghiên cứu các lĩnh vực pháp luật chuyên ngành và thực tiễn thi hành pháp luật. Vì vậy, luận án cần tiếp tục vận dụng các tiêu chí nêu trên để đánh giá thực trạng pháp luật về an ninh mạng, đồng thời đề xuất các giải pháp hoàn thiện phù hợp với yêu cầu chuyển đổi số và hội nhập quốc tế.

- Cuốn sách *Xây dựng và hoàn thiện hệ thống pháp luật Việt Nam trong bối cảnh xây dựng Nhà nước pháp quyền xã hội chủ nghĩa* của Nguyễn Minh Đoan và Nguyễn Minh Đức [82] là công trình có giá trị lý luận quan trọng trong nghiên cứu về xây dựng và hoàn thiện hệ thống pháp luật. Công trình đã làm rõ những vấn đề cơ bản về bản chất, cấu trúc và tính hệ thống của pháp luật trong điều kiện xây dựng Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam, đồng thời tiếp cận pháp luật như một chỉnh thể thống nhất, có tính liên

kết và vận động cùng sự phát triển của xã hội. Luận án kế thừa các luận điểm này trong Chương 2 để xây dựng hệ tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tuy nhiên, công trình chủ yếu nghiên cứu ở bình diện lý luận chung của hệ thống pháp luật, chưa đi sâu vào các lĩnh vực pháp luật chuyên ngành như pháp luật về an ninh mạng. Vì vậy, luận án tiếp tục vận dụng và phát triển các luận điểm của công trình nhằm xây dựng khung tiêu chí đánh giá phù hợp với đặc thù của pháp luật về an ninh mạng ở Việt Nam.

- Cuốn sách *Chiến lược phát triển pháp luật Việt Nam đến năm 2030, tầm nhìn đến năm 2045: Những vấn đề lý luận và thực tiễn* của Võ Khánh Vinh [201] là công trình có giá trị tham khảo quan trọng trong nghiên cứu về phát triển và hoàn thiện pháp luật. Công trình đã làm rõ các vấn đề lý luận về mục tiêu, định hướng và yêu cầu của quá trình xây dựng, phát triển pháp luật trong điều kiện xây dựng Nhà nước pháp quyền xã hội chủ nghĩa. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 4, đặc biệt về vai trò của chiến lược phát triển pháp luật và yêu cầu hoàn thiện pháp luật đáp ứng yêu cầu phát triển đất nước trong giai đoạn mới. Tuy nhiên, công trình chủ yếu tiếp cận ở tầm chiến lược và lý luận chung, chưa nghiên cứu chuyên sâu đối với các lĩnh vực pháp luật chuyên ngành như pháp luật về an ninh mạng. Vì vậy, luận án tiếp tục vận dụng các luận điểm của công trình để làm rõ yêu cầu hoàn thiện pháp luật về an ninh mạng trong bối cảnh chuyên đổi số và hội nhập quốc tế.

- Cuốn sách *Hoàn thiện pháp luật kinh doanh tại Việt Nam nhằm đáp ứng các yêu cầu của Hiệp định Thương mại tự do FTA thế hệ mới* của Lê Thị Hoài Thu [177] là công trình có giá trị tham khảo trong nghiên cứu về tác động của các FTA thế hệ mới đối với hệ thống pháp luật quốc gia và yêu cầu nội luật hóa các cam kết quốc tế. Luận án kế thừa cách tiếp cận so sánh pháp luật của công trình này trong Chương 2 và Chương 4 nhằm nhận diện các yêu cầu hoàn thiện pháp luật trong bối cảnh hội nhập quốc tế. Tuy nhiên, công trình chưa tập trung phân tích thực tiễn thi hành pháp luật và những vấn đề

phát sinh trong quá trình thực hiện các cam kết quốc tế. Vì vậy, luận án tiếp tục nghiên cứu yêu cầu hoàn thiện pháp luật về an ninh mạng trong bối cảnh hội nhập quốc tế và chuyển đổi số, đồng thời đánh giá khả năng tiếp thu và thực thi các chuẩn mực pháp lý quốc tế tại Việt Nam.

- Cuốn sách *Hoàn thiện pháp luật về xử lý vi phạm hành chính* của Đặng Thanh Sơn [172] là công trình có giá trị tham khảo quan trọng trong nghiên cứu về lý luận và thực tiễn xử lý vi phạm hành chính ở Việt Nam. Công trình đã hệ thống hóa các vấn đề lý luận cơ bản, đồng thời phân tích những kết quả đạt được và những hạn chế trong thi hành pháp luật về xử lý vi phạm hành chính. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 3, đặc biệt là các nội dung liên quan đến vai trò, ý nghĩa và định hướng hoàn thiện pháp luật về xử lý vi phạm hành chính. Tuy nhiên, công trình chưa đi sâu đánh giá hiệu quả thực thi trong các lĩnh vực quản lý nhà nước cụ thể. Vì vậy, luận án tiếp tục nghiên cứu việc áp dụng pháp luật về xử lý vi phạm hành chính trong lĩnh vực an ninh mạng, qua đó nhận diện những hạn chế và đề xuất giải pháp hoàn thiện phù hợp với yêu cầu thực tiễn hiện nay.

- Cuốn sách “*Pháp luật về an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao ở Việt Nam*” do GS.TS Nguyễn Ngọc Anh làm chủ biên [2] đã hệ thống hóa các vấn đề lý luận cơ bản về không gian mạng, ANQG trên môi trường số và tội phạm công nghệ cao. Dưới lăng kính khoa học pháp lý, cuốn sách đã đi sâu phân tích, bình luận các quy phạm của Luật An ninh mạng năm 2018, kết hợp với các chế định pháp luật hình sự và tố tụng hình sự. Qua đó đánh giá được thực tiễn áp dụng pháp luật của các lực lượng chức năng, chỉ ra những vướng mắc trong việc xử lý hành vi vi phạm, từ đó đề xuất giải pháp nâng cao hiệu quả phòng ngừa, đấu tranh. Tuy nhiên, định hướng tiếp cận của công trình chủ yếu nghiêng về khoa học luật hình sự và biện pháp nghiệp vụ an ninh truyền thống; chưa đi sâu vào khía cạnh kiến tạo thể chế đồng bộ mang tính quản lý nhà nước như: cơ chế pháp lý bảo vệ chủ quyền dữ liệu, kiểm soát an ninh chuỗi cung ứng công nghệ hay trách nhiệm minh bạch thuật toán của

nền tảng xuyên biên giới. Đây chính là những khoảng trống pháp lý mang tính dân sự, kinh tế - kỹ thuật mà Luận án sẽ tập trung giải quyết.

(2) Các công trình nghiên cứu là đề tài:

- Đề tài *Phương hướng hoàn thiện hệ thống văn bản pháp luật về bảo vệ ANQG trong tình hình hiện nay* của Trung tướng Trần Vi Dân [69] là công trình có giá trị tham khảo quan trọng về lý luận và thực tiễn xây dựng, hoàn thiện pháp luật trong lĩnh vực bảo vệ ANQG. Công trình đã đề xuất cách tiếp cận hệ thống trong đánh giá thực trạng và định hướng hoàn thiện pháp luật. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 3, đặc biệt là phương pháp đánh giá mức độ hoàn thiện pháp luật và nhận diện các giải pháp hoàn thiện. Tuy nhiên, công trình chủ yếu tiếp cận ở phạm vi pháp luật về bảo vệ ANQG nói chung, chưa đi sâu vào lĩnh vực an ninh mạng. Vì vậy, luận án tiếp tục vận dụng và phát triển các luận điểm của công trình để nghiên cứu, đề xuất giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với yêu cầu thực tiễn hiện nay.

- Đề tài *Hoàn thiện pháp luật hình sự Việt Nam đáp ứng yêu cầu phòng, chống tội phạm trong bối cảnh Cách mạng công nghiệp lần thứ tư* của Bộ Tư pháp [30] là tài liệu có giá trị tham khảo trong nghiên cứu tác động của Cách mạng công nghiệp 4.0 đối với tội phạm và pháp luật hình sự. Luận án kế thừa các luận điểm của công trình trong Chương 2 và Chương 3, đặc biệt về tác động của chuyên đổi số, công nghệ mới và yêu cầu nâng cao khả năng thích ứng của pháp luật trước các nguy cơ an ninh phi truyền thống. Tuy nhiên, công trình chủ yếu tiếp cận từ góc độ pháp luật hình sự, chưa làm rõ đầy đủ mối liên hệ với pháp luật về an ninh mạng và các lĩnh vực pháp luật có liên quan. Vì vậy, luận án tiếp tục nghiên cứu tác động của công nghệ số đối với pháp luật về an ninh mạng, qua đó đề xuất giải pháp hoàn thiện pháp luật nhằm đáp ứng yêu cầu bảo vệ ANQG trong bối cảnh chuyển đổi số.

- Đề tài *Nghiên cứu xây dựng những định hướng chính sách lớn hoàn thiện pháp luật về xử lý vi phạm hành chính* của Bộ Tư pháp [28] là công trình

có giá trị tham khảo quan trọng trong nghiên cứu hoàn thiện pháp luật về xử lý vi phạm hành chính. Công trình đã đề xuất các định hướng hoàn thiện pháp luật gắn với yêu cầu bảo đảm quyền con người, quyền công dân, nâng cao hiệu lực, hiệu quả quản lý nhà nước và đáp ứng yêu cầu hội nhập quốc tế. Luận án kế thừa các quan điểm này trong Chương 2 và Chương 3, đặc biệt là yêu cầu bảo đảm sự hài hòa giữa quản lý nhà nước và bảo vệ quyền, lợi ích hợp pháp của các chủ thể. Tuy nhiên, công trình chủ yếu tiếp cận ở bình diện chính sách và định hướng lập pháp, chưa đi sâu đánh giá hiệu quả thực thi trong các lĩnh vực cụ thể. Vì vậy, luận án tiếp tục nghiên cứu việc áp dụng các chế tài và cơ chế xử lý vi phạm pháp luật về an ninh mạng, từ đó đề xuất các giải pháp hoàn thiện phù hợp với yêu cầu quản lý nhà nước trong bối cảnh chuyển đổi số.

(3) Các công trình nghiên cứu là bài viết:

- Bài viết *Pháp luật về điện toán đám mây trong thương mại điện tử ở một số quốc gia và Việt Nam* của Nguyễn Mai Linh, Ngô Thị Hương Giang, Nguyễn Quý Cảnh và Nguyễn Phương Anh [4] đã phân tích các vấn đề pháp lý liên quan đến điện toán đám mây, đặc biệt là bảo vệ dữ liệu cá nhân, an toàn thông tin và quản lý nhà nước trong môi trường số. Luận án kế thừa cách tiếp cận so sánh pháp luật của công trình khi nghiên cứu các vấn đề pháp lý về dữ liệu và an ninh mạng trong bối cảnh chuyển đổi số tại Chương 2. Tuy nhiên, bài viết chủ yếu mang tính khái quát, chưa đánh giá sâu thực tiễn thi hành pháp luật và những rủi ro phát sinh trong hoạt động điện toán đám mây. Vì vậy, luận án tiếp tục nghiên cứu thực tiễn áp dụng pháp luật và đề xuất giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với điều kiện Việt Nam.

- Bài viết *Xây dựng khung pháp lý hoàn chỉnh cho thị trường dữ liệu và các dịch vụ số* của Hồng Quân và Hà Trung [138] có giá trị tham khảo trong nghiên cứu về vai trò của dữ liệu và yêu cầu hoàn thiện khung pháp lý phục vụ phát triển kinh tế số, Chính phủ số. Luận án kế thừa các quan điểm của công trình trong Chương 2 và Chương 3, đặc biệt là cách tiếp cận coi dữ liệu là nguồn lực quan trọng của chuyển đổi số và yêu cầu xây dựng khung

pháp lý đồng bộ. Tuy nhiên, nghiên cứu chủ yếu tiếp cận ở góc độ chính sách, chưa phân tích sâu các cơ chế pháp lý về quản trị, chia sẻ và bảo vệ dữ liệu. Vì vậy, luận án tiếp tục làm rõ mối quan hệ giữa dữ liệu, an ninh mạng và bảo đảm ANQG, TTATXH, từ đó đề xuất các giải pháp hoàn thiện pháp luật phù hợp với yêu cầu chuyển đổi số ở Việt Nam.

- Bài viết *Pháp luật về bảo vệ quyền lợi người tiêu dùng sử dụng dịch vụ vay trực tuyến tại các công ty tài chính* của Trần Thế Hệ [94] đã phân tích các quy định pháp luật hiện hành, chỉ ra những hạn chế và đề xuất giải pháp hoàn thiện cơ chế bảo vệ người tiêu dùng trong môi trường tài chính số. Luận án kế thừa cách tiếp cận này trong Chương 3 khi đánh giá thực trạng pháp luật và nhận diện các khoảng trống pháp lý cần hoàn thiện. Tuy nhiên, nghiên cứu chủ yếu tập trung vào phân tích QPPL, chưa đánh giá sâu hiệu quả thực thi và trách nhiệm của các chủ thể cung cấp dịch vụ. Vì vậy, luận án tiếp tục nghiên cứu thực tiễn áp dụng pháp luật, qua đó đề xuất các giải pháp hoàn thiện cơ chế bảo vệ quyền và lợi ích hợp pháp của các chủ thể trong môi trường số.

- Bài viết “*Hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu chuyển đổi số quốc gia*” của Nguyễn Thị Thuận [183] đã đặt vấn đề hoàn thiện thể chế an ninh mạng trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư và định hướng phát triển nền kinh tế số. Tác giả đã phân tích sự dịch chuyển rủi ro từ an ninh truyền thống sang an ninh phi truyền thống, nhấn mạnh các thách thức về rò rỉ dữ liệu cá nhân và tấn công có chủ đích vào hạ tầng thông tin trọng yếu. Trên cơ sở đó, bài báo đưa ra các kiến nghị vĩ mô nhằm sửa đổi quy định về trách nhiệm bảo mật của doanh nghiệp cung cấp dịch vụ số và yêu cầu nội luật hóa tiêu chuẩn quốc tế. Tuy nhiên, công trình này mới chỉ dừng lại ở việc nhận diện các bất cập mang tính hiện tượng và đưa ra định hướng chính sách chung mà chưa xây dựng được một hệ thống giải pháp lập pháp cụ thể, toàn diện, đặc biệt thiếu vắng các cơ chế pháp lý ứng phó với rủi ro công nghệ mới như: kiểm định an ninh đối với trí tuệ nhân tạo (AI), quản trị không gian tầm thấp hay cơ chế pháp lý thử nghiệm có kiểm

soát (Sandbox). Luận án sẽ kế thừa các định hướng này để kiến nghị cụ thể hóa thành các QPPL hoàn chỉnh.

(4) Các công trình nghiên cứu là luận án:

- Luận án *Hoàn thiện pháp luật về trung cầu ý dân ở Việt Nam hiện nay* của Phạm Hồng Diên [70] đã làm rõ khái niệm, nội hàm, vai trò của pháp luật về trung cầu ý dân và các điều kiện bảo đảm thực hiện quyền hiến định của công dân. Luận án kế thừa các luận điểm này trong Chương 2, đặc biệt là cách tiếp cận về quyền hiến định và các yêu cầu hoàn thiện pháp luật. Tuy nhiên, công trình chủ yếu nghiên cứu ở bình diện lý luận và phân tích văn bản pháp luật, chưa đánh giá sâu thực tiễn thi hành và các vướng mắc phát sinh trong quá trình áp dụng pháp luật. Vì vậy, luận án tiếp tục nghiên cứu thực tiễn thi hành pháp luật, nhận diện những bất cập và đề xuất giải pháp hoàn thiện trên cơ sở thực tiễn và kinh nghiệm quốc tế.

- Luận án *Hoàn thiện pháp luật về đầu tư công ở Việt Nam hiện nay* của Nguyễn Hương Ly [109] đã phân tích các vấn đề lý luận cơ bản và đánh giá thực trạng pháp luật về đầu tư công ở Việt Nam. Luận án kế thừa cách tiếp cận kết hợp giữa nghiên cứu lý luận và đánh giá thực tiễn của công trình này trong Chương 2, đặc biệt là các luận điểm về yêu cầu hoàn thiện pháp luật nhằm nâng cao hiệu quả quản lý nhà nước. Tuy nhiên, công trình chủ yếu tập trung vào lĩnh vực đầu tư công, chưa xem xét đầy đủ các tác động của chuyển đổi số và hội nhập quốc tế đối với quá trình hoàn thiện pháp luật. Vì vậy, luận án tiếp tục nghiên cứu các yêu cầu mới đặt ra đối với pháp luật về an ninh mạng trong bối cảnh chuyển đổi số, qua đó đề xuất các giải pháp hoàn thiện phù hợp với thực tiễn phát triển hiện nay.

#### ***1.1.1.2. Nhóm công trình nghiên cứu ở nước ngoài***

(1) Các công trình nghiên cứu là sách:

- Cuốn sách *Reforming Legal Systems: Global Perspectives (Cải cách hệ thống pháp luật: Quan điểm toàn cầu)* của tập thể tác giả Asif H. Qureshi, Li Zhuangxu, Cecilia J. Flores Elizondo [205] là công trình có giá trị tham

khảo quan trọng về cải cách hệ thống pháp luật từ góc độ so sánh quốc tế. Luận án kế thừa cách tiếp cận so sánh và phương pháp phân tích các yếu tố tác động đến quá trình hoàn thiện pháp luật trong Chương 2. Tuy nhiên, công trình chủ yếu nghiên cứu trên phương diện lý luận và kinh nghiệm chung, chưa tập trung vào các lĩnh vực pháp luật chuyên ngành như an ninh mạng. Vì vậy, luận án cần tiếp tục vận dụng các kinh nghiệm quốc tế để xây dựng tiêu chí đánh giá và đề xuất giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với điều kiện Việt Nam.

- Cuốn sách *Global Perspectives on Reforming the Criminal Justice System (Góc nhìn Toàn cầu về Cải cách Hệ thống Tư pháp Hình sự)* của tác giả Michael Pittaro [243] cung cấp những kinh nghiệm quốc tế về cải cách pháp luật và hệ thống tư pháp theo các chuẩn mực quốc tế. Luận án kế thừa cách tiếp cận so sánh và các luận điểm về vai trò của chuẩn mực quốc tế trong quá trình hoàn thiện pháp luật tại Chương 2 và Chương 4. Tuy nhiên, công trình chủ yếu tập trung vào lĩnh vực tư pháp hình sự và chưa làm rõ khả năng vận dụng các mô hình cải cách trong những bối cảnh pháp lý cụ thể. Vì vậy, luận án cần tiếp tục nghiên cứu việc tiếp thu kinh nghiệm quốc tế nhằm đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với điều kiện Việt Nam và yêu cầu hội nhập quốc tế.

- Cuốn sách *Law Reforms Around the World: Perspectives from National and International Law (Cải cách pháp luật trên toàn thế giới: Góc nhìn từ luật pháp quốc gia và quốc tế)* của tác giả Asif H. Qureshi [206] là công trình có giá trị tham khảo quan trọng về cải cách pháp luật trong bối cảnh toàn cầu hóa và hội nhập quốc tế. Luận án kế thừa cách tiếp cận so sánh pháp luật và các luận điểm về tác động của cơ chế pháp lý quốc tế đối với quá trình hoàn thiện pháp luật quốc gia trong Chương 2 và Chương 4. Tuy nhiên, công trình chủ yếu mang tính khái quát, chưa phân tích sâu khả năng vận dụng các kinh nghiệm cải cách vào từng lĩnh vực pháp luật cụ thể. Vì vậy,

luận án tiếp tục nghiên cứu việc tiếp thu kinh nghiệm quốc tế nhằm đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với điều kiện Việt Nam và yêu cầu hội nhập quốc tế.

(2) Các công trình nghiên cứu là luận án:

- Luận án *Vulnerabilities, Cybersecurity, and the Role of Law and Regulation (Lỗ hổng bảo mật, an ninh mạng và vai trò của pháp luật, quy định)* của Jian Jiang [227] đã phân tích vai trò của pháp luật và các cơ chế quản lý trong phòng ngừa, phát hiện và khắc phục các lỗ hổng bảo mật - một trong những nguyên nhân chủ yếu dẫn đến các nguy cơ mất an ninh mạng. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 3, đặc biệt là cách tiếp cận kết hợp giữa pháp luật, quy định kỹ thuật và quản trị rủi ro nhằm bảo đảm an ninh mạng. Tuy nhiên, công trình chủ yếu dựa trên kinh nghiệm quốc tế và chưa đánh giá thực tiễn áp dụng pháp luật trong điều kiện Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu thực trạng thi hành pháp luật về an ninh mạng, phân tích các rủi ro phát sinh trong môi trường số và đề xuất các giải pháp hoàn thiện pháp luật phù hợp với yêu cầu bảo đảm an ninh mạng hiện nay.

- Luận án *European (Visegrád countries) Cyber-security in Applying for Asian Countries: The Case of Vietnam (An ninh mạng châu Âu, nhóm nước Visegrád, áp dụng cho các quốc gia châu Á: trường hợp Việt Nam)* của Nguyễn Hữu Phước Đại [217] đã nghiên cứu kinh nghiệm bảo đảm an ninh mạng của các nước Visegrád và khả năng vận dụng đối với Việt Nam. Luận án kế thừa cách tiếp cận so sánh quốc tế của công trình trong Chương 2 và Chương 4, đặc biệt là các nội dung về chính sách, pháp luật và tổ chức bảo đảm an ninh mạng. Tuy nhiên, công trình chủ yếu tập trung vào việc giới thiệu và đối chiếu kinh nghiệm quốc tế, chưa phân tích sâu tính phù hợp của các mô hình này với điều kiện pháp lý và thực tiễn Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu khả năng tiếp thu kinh nghiệm quốc tế và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với điều kiện Việt Nam và yêu cầu hội nhập quốc tế.

Nhìn chung, các công trình nghiên cứu trên đã cung cấp nền tảng lý luận chung về hoàn thiện pháp luật, đặc biệt là các tiêu chí như tính đầy đủ, tính đồng bộ, tính thống nhất, tính khả thi, tính minh bạch, tính phù hợp và kỹ thuật lập pháp. Tuy nhiên, phần lớn các nghiên cứu mới dừng ở cấp độ lý luận chung hoặc nghiên cứu một lĩnh vực pháp luật khác, chưa vận dụng trực tiếp vào pháp luật về an ninh mạng. Vì vậy, luận án kế thừa hệ tiêu chí chung về hoàn thiện pháp luật, đồng thời phát triển các tiêu chí này cho phù hợp với đặc thù của pháp luật về an ninh mạng, nhất là tính liên ngành, tính xuyên biên giới, tính thích ứng với công nghệ và yêu cầu cân bằng giữa bảo vệ ANQG với bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức.

### **1.1.2. Những công trình nghiên cứu thực tiễn hoàn thiện pháp luật về an ninh mạng**

#### **1.1.2.1. Nhóm công trình nghiên cứu trong nước**

(1) Các công trình nghiên cứu là sách:

- Cuốn sách *Tăng cường công tác thông tin tuyên truyền phòng, ngừa, chống vi phạm trên mạng Internet* của Hoàng Thành Nam [115] cung cấp cái nhìn tổng quan về tình hình an ninh mạng và các nguy cơ vi phạm trên không gian mạng, đồng thời nhấn mạnh vai trò của công tác tuyên truyền, nâng cao nhận thức trong phòng ngừa vi phạm. Luận án kế thừa các nhận định này trong Chương 2 và Chương 3, đặc biệt là xu hướng gia tăng các hành vi vi phạm trên không gian mạng và yêu cầu tăng cường các biện pháp phòng ngừa. Tuy nhiên, công trình chủ yếu tiếp cận từ góc độ tuyên truyền và chính sách, chưa phân tích sâu các khía cạnh pháp lý và cơ chế thực thi. Vì vậy, luận án cần tiếp tục nghiên cứu vai trò của pháp luật trong phòng ngừa, phát hiện và xử lý vi phạm trên không gian mạng, từ đó đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu chuyển đổi số hiện nay.

- Cuốn sách *Pháp luật hình sự Việt Nam trước thách thức an ninh phi truyền thống* của Trịnh Tiến Việt [200] đã phân tích những thách thức của an ninh phi truyền thống đối với pháp luật hình sự Việt Nam và đề xuất định

hướng hoàn thiện pháp luật nhằm nâng cao hiệu quả phòng, chống tội phạm. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 3, đặc biệt là các phân tích về nguy cơ an ninh phi truyền thống trong môi trường số. Tuy nhiên, công trình chủ yếu tiếp cận từ góc độ pháp luật hình sự, chưa đi sâu đánh giá hiệu quả thực thi và tác động của công nghệ đối với các nguy cơ an ninh mới. Vì vậy, luận án cần tiếp tục nghiên cứu thực trạng pháp luật về an ninh mạng, đánh giá các thách thức phát sinh từ quá trình chuyển đổi số và đề xuất giải pháp hoàn thiện pháp luật nhằm tăng cường bảo vệ ANQG trên không gian mạng.

- Cuốn sách *Hoàn thiện pháp luật điều chỉnh mô hình kinh tế chia sẻ ở Việt Nam hiện nay* của Chu Thị Hoa [90] đã làm rõ cơ sở lý luận, đặc điểm và những vấn đề pháp lý đặt ra từ sự phát triển của mô hình kinh tế chia sẻ trong bối cảnh chuyển đổi số. Luận án kế thừa các luận điểm của công trình trong Chương 2 và Chương 3, đặc biệt là các phân tích về các quan hệ pháp lý mới phát sinh và yêu cầu hoàn thiện pháp luật trước sự phát triển của công nghệ số. Tuy nhiên, công trình chủ yếu tập trung vào khung pháp lý chung, chưa đánh giá sâu hiệu quả thực thi và các rủi ro pháp lý phát sinh trong thực tiễn. Vì vậy, luận án tiếp tục nghiên cứu các thách thức pháp lý trong môi trường số, qua đó đề xuất giải pháp hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu phát triển kinh tế số ở Việt Nam hiện nay.

(2) Các công trình nghiên cứu là bài viết:

- Bài viết *Bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số* của Hoàng Thị Quyên [170] đã làm rõ khái niệm chủ quyền quốc gia trên không gian mạng và những thách thức đặt ra đối với hoạt động bảo vệ chủ quyền trong bối cảnh chuyển đổi số. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 3, đặc biệt là các nội dung về mối quan hệ giữa chủ quyền quốc gia và không gian mạng, cũng như yêu cầu hoàn thiện cơ chế bảo vệ chủ quyền quốc gia trên môi trường số. Tuy nhiên, nghiên cứu chủ yếu tiếp cận ở góc độ lý luận, chưa phân tích sâu các cơ chế pháp lý

và thực tiễn thi hành pháp luật. Vì vậy, luận án tiếp tục nghiên cứu nội hàm pháp lý của chủ quyền quốc gia trên không gian mạng, đánh giá thực trạng pháp luật và đề xuất giải pháp hoàn thiện nhằm nâng cao hiệu quả bảo vệ chủ quyền quốc gia trong bối cảnh chuyển đổi số và hội nhập quốc tế.

- Bài viết *Những khía cạnh pháp lý về cấm sử dụng vũ lực, đe dọa sử dụng vũ lực và quyền tự vệ của quốc gia trên không gian mạng trong luật quốc tế* của Đỗ Thị Hà [84] đã làm rõ các nguyên tắc cơ bản của luật quốc tế liên quan đến việc sử dụng vũ lực và quyền tự vệ của quốc gia trên không gian mạng. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 4, đặc biệt là cách tiếp cận gắn bảo vệ chủ quyền quốc gia trên không gian mạng với các giới hạn pháp lý của quyền tự vệ. Tuy nhiên, nghiên cứu chủ yếu tiếp cận từ góc độ luật quốc tế, chưa làm rõ khả năng nội luật hóa và cơ chế thực thi trong pháp luật Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu cơ sở pháp lý bảo vệ chủ quyền quốc gia trên không gian mạng, đồng thời đề xuất các giải pháp hoàn thiện pháp luật Việt Nam đáp ứng yêu cầu bảo vệ ANQG trong bối cảnh chuyển đổi số và hội nhập quốc tế.

- Bài viết *Trung Quốc với vấn đề chủ quyền không gian mạng* của Nguyễn Việt Lâm [103] đã phân tích quan điểm, cách tiếp cận và kinh nghiệm của Trung Quốc trong việc thúc đẩy và bảo vệ chủ quyền không gian mạng ở cả cấp độ quốc gia và quốc tế. Luận án kế thừa các luận điểm này trong Chương 2 và Chương 4, đặc biệt là cách tiếp cận nghiên cứu chủ quyền không gian mạng gắn với công nghệ, an ninh và lợi ích quốc gia. Tuy nhiên, nghiên cứu chủ yếu tập trung vào trường hợp Trung Quốc, chưa phân tích sâu khả năng vận dụng đối với điều kiện pháp lý và thể chế của Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu cơ sở pháp lý của chủ quyền quốc gia trên không gian mạng, đồng thời tham chiếu kinh nghiệm quốc tế để đề xuất các giải pháp bảo vệ chủ quyền và lợi ích quốc gia phù hợp với điều kiện Việt Nam.

- Bài viết *Giải pháp tăng cường bảo vệ không gian mạng theo quan điểm của Đảng và pháp luật của Nhà nước* của Trần Tuấn Duy và Phan Trần

Mai Phương [73] đã khái quát quan điểm của Đảng, chính sách pháp luật của Nhà nước về bảo vệ không gian mạng và làm rõ vai trò của an ninh mạng trong bảo vệ ANQG. Luận án kế thừa các luận điểm này trong Chương 2, đặc biệt là các nội dung về hoàn thiện cơ sở pháp lý, nâng cao nhận thức xã hội và tăng cường hợp tác quốc tế trong bảo vệ không gian mạng. Tuy nhiên, bài viết chủ yếu mang tính định hướng chính sách, chưa phân tích sâu cơ chế pháp lý và hiệu quả thực thi trong thực tiễn. Vì vậy, luận án tiếp tục nghiên cứu thực trạng thi hành pháp luật, làm rõ trách nhiệm của các chủ thể liên quan và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu bảo vệ ANQG trong bối cảnh chuyển đổi số.

- Bài viết *Hướng tiếp cận và hoàn thiện pháp luật bảo vệ dữ liệu cá nhân tại Việt Nam trước tác động lập pháp của thế giới và khu vực* của Bạch Thị Nhã Nam [114] đã khái quát các mô hình pháp luật về bảo vệ dữ liệu cá nhân và những xu hướng lập pháp tiêu biểu trên thế giới. Luận án kế thừa cách tiếp cận so sánh pháp luật của công trình trong Chương 2, đặc biệt là các nội dung về giá trị pháp lý của dữ liệu cá nhân, cơ chế bảo vệ dữ liệu và kinh nghiệm quốc tế. Tuy nhiên, bài viết chủ yếu tập trung vào phân tích mô hình lập pháp, chưa đánh giá sâu thực tiễn thi hành pháp luật và cơ chế bảo vệ dữ liệu cá nhân tại Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu thực trạng pháp luật, đánh giá những bất cập trong cơ chế bảo vệ dữ liệu cá nhân và đề xuất các giải pháp hoàn thiện pháp luật đáp ứng yêu cầu chuyển đổi số và bảo đảm an ninh mạng.

(3) Các công trình nghiên cứu là luận án:

- Luận án *Pháp luật về bảo vệ quyền lợi người tiêu dùng trong thương mại điện tử ở Việt Nam* của Nguyễn Ngọc Quyền [173] đã làm rõ những bất cập của pháp luật hiện hành và khẳng định sự cần thiết phải hoàn thiện cơ chế bảo vệ quyền lợi người tiêu dùng trong môi trường thương mại điện tử. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2, đặc biệt là các phân tích về rủi ro pháp lý và yêu cầu nâng cao hiệu quả bảo vệ các chủ thể trong môi trường số. Tuy nhiên, công trình chủ yếu tập trung vào lĩnh vực thương

mại điện tử, chưa phân tích sâu các vấn đề pháp lý mới liên quan đến dữ liệu cá nhân, nền tảng số và an ninh mạng. Vì vậy, luận án tiếp tục nghiên cứu các rủi ro pháp lý phát sinh trong môi trường số, đánh giá thực tiễn thi hành pháp luật và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu chuyển đổi số hiện nay.

- Luận án *Pháp luật về thương mại điện tử ở Việt Nam* của Phí Mạnh Cường [56] đã phân tích những bất cập của pháp luật hiện hành và tham khảo kinh nghiệm quốc tế trong điều chỉnh các quan hệ thương mại điện tử. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2, đặc biệt là các quan điểm về bảo vệ quyền lợi người tiêu dùng, bảo đảm an toàn giao dịch và minh bạch thông tin trong môi trường số. Tuy nhiên, công trình chủ yếu tập trung vào khía cạnh thương mại điện tử, chưa đánh giá đầy đủ thực tiễn thi hành pháp luật và những thách thức mới phát sinh từ nền tảng số và chuyển đổi số. Vì vậy, luận án tiếp tục nghiên cứu các rủi ro pháp lý trên không gian mạng, đánh giá hiệu quả thực thi pháp luật và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với yêu cầu hội nhập quốc tế và phát triển kinh tế số.

#### ***1.1.2.2. Nhóm công trình nghiên cứu ở nước ngoài***

(1) Các công trình nghiên cứu là sách:

- Sách *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (Tình thế lưỡng nan về an ninh mạng: xâm nhập trái phép, niềm tin và nỗi lo của các quốc gia) của Ben Buchanan [211] đã làm rõ mối quan hệ giữa an ninh mạng, ANQG và quan hệ quốc tế trong bối cảnh không gian mạng ngày càng trở thành môi trường cạnh tranh chiến lược giữa các quốc gia. Luận án kế thừa các luận điểm này trong Chương 2, đặc biệt là cách tiếp cận an ninh mạng từ góc độ bảo vệ ANQG và chủ quyền trên không gian mạng. Tuy nhiên, công trình chủ yếu tiếp cận từ góc độ chiến lược và chính trị quốc tế, chưa phân tích sâu các cơ chế pháp lý bảo đảm an ninh mạng trong pháp luật quốc gia. Vì vậy, luận án tiếp tục nghiên cứu các cơ chế pháp

lý về phòng ngừa, phát hiện, xử lý hành vi xâm phạm an ninh mạng và hợp tác quốc tế, qua đó đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với yêu cầu bảo vệ ANQG ở Việt Nam.

- Sách *Information risk and security: preventing and investigating workplace computer crime (Rủi ro thông tin và an ninh: phòng ngừa và điều tra tội phạm máy tính tại công sở)* của Edward Wilding [219] đã làm rõ các vấn đề về rủi ro thông tin, an ninh thông tin và phòng ngừa tội phạm máy tính trong môi trường tổ chức. Luận án kế thừa cách tiếp cận quản trị rủi ro và các biện pháp phòng ngừa, phát hiện, xử lý các mối đe dọa đối với hệ thống thông tin trong Chương 2. Tuy nhiên, công trình chủ yếu tiếp cận từ góc độ quản lý và kỹ thuật, chưa phân tích sâu các cơ chế pháp lý và trách nhiệm của các chủ thể trong bảo đảm an ninh mạng. Vì vậy, luận án tiếp tục nghiên cứu cơ sở pháp lý về quản trị rủi ro, trách nhiệm của các chủ thể và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với yêu cầu chuyển đổi số ở Việt Nam.

(2) Các công trình nghiên cứu là bài viết:

- Bài viết *The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes (Sự hình thành pháp luật an ninh mạng của EU)* của Lee A. Bygrave [235] đã phân tích quá trình hình thành và phát triển pháp luật về an ninh mạng của EU trong mối liên hệ với quản trị rủi ro, bảo vệ dữ liệu cá nhân và quản trị kinh tế số. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2, đặc biệt là cách tiếp cận hệ thống, liên ngành và kinh nghiệm bảo đảm tính thống nhất giữa các lĩnh vực pháp luật có liên quan. Tuy nhiên, công trình chủ yếu nghiên cứu trong bối cảnh pháp lý của EU, chưa làm rõ khả năng vận dụng đối với điều kiện pháp lý và thể chế của Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu khả năng tiếp thu kinh nghiệm quốc tế, làm rõ mối quan hệ giữa pháp luật về an ninh mạng với các lĩnh vực pháp luật liên quan và đề xuất các giải pháp hoàn thiện pháp luật phù hợp với yêu cầu chuyển đổi số ở Việt Nam.

- Bài viết *Cybersecurity Law and Regulation (Luật và quy định về an ninh mạng)* của Uchenna Jerome Orji [255] có giá trị tham khảo quan trọng trong nghiên cứu các khía cạnh pháp lý của an ninh mạng và kinh nghiệm xây dựng pháp luật tại nhiều quốc gia. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2, đặc biệt là cách tiếp cận so sánh pháp luật, vai trò của điều ước quốc tế và trách nhiệm của Nhà nước trong bảo đảm an ninh mạng. Tuy nhiên, công trình được thực hiện trong bối cảnh pháp lý trước những phát triển mạnh mẽ của dữ liệu lớn, trí tuệ nhân tạo và nền tảng số xuyên biên giới. Vì vậy, luận án tiếp tục nghiên cứu các vấn đề pháp lý mới về an ninh mạng, đồng thời đánh giá khả năng tiếp thu kinh nghiệm quốc tế để đề xuất các giải pháp hoàn thiện pháp luật phù hợp với yêu cầu bảo vệ ANQG trong bối cảnh chuyển đổi số.

- Bài viết *Legal Aspects of Cybersecurity (Các khía cạnh pháp lý của an ninh mạng)* của A. Appazov [204] đã phân tích những vấn đề pháp lý cơ bản liên quan đến an ninh mạng và tội phạm mạng, bao gồm bảo vệ quyền con người, quyền riêng tư, thẩm quyền tài phán, chứng cứ điện tử và hợp tác quốc tế. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2, đặc biệt là các luận điểm về trách nhiệm pháp lý và cơ chế hợp tác trong bảo đảm an ninh mạng. Tuy nhiên, công trình được thực hiện trong bối cảnh năm 2014 nên chưa phản ánh đầy đủ những thách thức mới từ trí tuệ nhân tạo, dữ liệu lớn và các nền tảng số xuyên biên giới. Vì vậy, luận án tiếp tục nghiên cứu các vấn đề pháp lý mới về an ninh mạng, đánh giá thực tiễn thi hành pháp luật tại Việt Nam và đề xuất các giải pháp hoàn thiện pháp luật nhằm bảo vệ quyền con người, ANQG và tăng cường hợp tác quốc tế trong môi trường số.

Nhìn chung, các công trình nghiên cứu trên có điểm mạnh là đã chỉ rõ vai trò của an ninh mạng trong bảo vệ ANQG, chủ quyền số, TTATXH và lợi ích quốc gia trên không gian mạng. Tuy nhiên, một số nghiên cứu có xu hướng nhấn mạnh logic bảo vệ an ninh mà chưa phân tích đầy đủ giới hạn quyền lực nhà nước, cơ chế kiểm soát biện pháp can thiệp, quyền riêng tư,

quyền tiếp cận thông tin, quyền tự do kinh doanh hợp pháp và bảo vệ dữ liệu cá nhân. Đây là vấn đề luận án cần tiếp tục phát triển theo hướng cân bằng giữa yêu cầu bảo vệ ANQG với yêu cầu bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức trong Nhà nước pháp quyền.

### **1.1.3. Những công trình khoa học nghiên cứu giải pháp hoàn thiện pháp luật về an ninh mạng**

#### **1.1.3.1. Nhóm công trình nghiên cứu trong nước**

(1) Các công trình nghiên cứu là đề tài:

- Đề tài *Nghiên cứu đề xuất các biện pháp xử lý vi phạm hành chính trong lĩnh vực an toàn thông tin trên mạng* của Bộ Thông tin và Truyền thông [23] đã phân tích thực trạng vi phạm an toàn thông tin trên mạng và các quy định pháp luật liên quan đến xử lý vi phạm hành chính trong lĩnh vực này. Luận án kế thừa các kết quả nghiên cứu của công trình trong Chương 4, đặc biệt là các nội dung về cơ sở pháp lý, cơ chế quản lý nhà nước và yêu cầu hoàn thiện các biện pháp xử lý vi phạm. Tuy nhiên, nghiên cứu chủ yếu tiếp cận ở góc độ tổng quan, chưa đánh giá sâu hiệu quả thực thi pháp luật và những thách thức phát sinh từ công nghệ mới. Vì vậy, luận án tiếp tục nghiên cứu thực tiễn áp dụng pháp luật, nhận diện các vướng mắc trong xử lý vi phạm và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với bối cảnh chuyển đổi số hiện nay.

- Đề tài *Nghiên cứu kinh nghiệm xây dựng chiến lược quốc gia về an toàn không gian mạng và đề xuất cho Việt Nam* của Bộ Thông tin và Truyền thông [24] đã nghiên cứu quan điểm, kinh nghiệm quốc tế và các nội dung cơ bản trong xây dựng chiến lược quốc gia về an toàn không gian mạng. Luận án kế thừa các kết quả nghiên cứu này trong Chương 4, đặc biệt là cách tiếp cận so sánh quốc tế và các luận điểm về tầm nhìn, mục tiêu, nguyên tắc và kế hoạch hành động trong bảo đảm an toàn không gian mạng. Tuy nhiên, công trình chủ yếu mang tính tổng quan, chưa đánh giá sâu hiệu quả triển khai chiến lược trong thực tiễn Việt Nam và cơ chế phối hợp giữa các chủ thể liên

quan. Vì vậy, luận án tiếp tục nghiên cứu thực tiễn thực hiện chiến lược, nhận diện các vướng mắc và đề xuất giải pháp hoàn thiện pháp luật, cơ chế quản trị an ninh mạng phù hợp với bối cảnh chuyển đổi số hiện nay.

(2) Các công trình nghiên cứu là bài viết:

- Bài viết *Tội phạm sử dụng công nghệ cao và phòng chống tội phạm sử dụng công nghệ cao tại Việt Nam* của Hạ Thị Thiều Dao và Lại Văn Tài [68] đã phân tích thực trạng, đặc điểm và xu hướng gia tăng của tội phạm sử dụng công nghệ cao tại Việt Nam, đồng thời đề xuất một số giải pháp phòng ngừa và đấu tranh với loại tội phạm này. Luận án kế thừa các kết quả nghiên cứu của công trình trong Chương 3, đặc biệt là các nhận định về mức độ nguy hiểm và những thách thức đối với an ninh, an toàn trên không gian mạng. Tuy nhiên, nghiên cứu chủ yếu tiếp cận từ góc độ thực tiễn và chính sách, chưa phân tích sâu cơ sở pháp lý và hiệu quả thực thi các quy định hiện hành. Vì vậy, luận án tiếp tục nghiên cứu thực trạng áp dụng pháp luật, nhận diện những bất cập trong cơ chế phòng ngừa, xử lý vi phạm và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu bảo vệ ANQG trong bối cảnh chuyển đổi số.

- Bài viết *Kinh nghiệm quốc tế về xử lý tội phạm công nghệ cao và một số khuyến nghị cho Việt Nam* của Nguyễn Hoàng Chỉ Mai [124] đã phân tích kinh nghiệm pháp luật của một số quốc gia trong phòng ngừa và xử lý tội phạm công nghệ cao, đồng thời đưa ra các khuyến nghị đối với Việt Nam. Luận án kế thừa các kết quả nghiên cứu này trong Chương 3 và Chương 4, đặc biệt là các kinh nghiệm quốc tế về khung pháp lý, cơ chế xử lý và biện pháp phòng ngừa tội phạm công nghệ cao. Tuy nhiên, nghiên cứu chủ yếu mang tính tổng hợp, chưa đánh giá sâu khả năng áp dụng các kinh nghiệm này trong điều kiện thực tiễn Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu thực trạng áp dụng pháp luật, đánh giá tính khả thi của các kinh nghiệm quốc tế và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với yêu cầu chuyển đổi số hiện nay.

(3) Các công trình nghiên cứu là luận án:

- Luận án *Trách nhiệm hình sự của pháp nhân thương mại trong Luật Hình sự Việt Nam* của Vũ Văn Tư [188] đã phân tích các quy định pháp luật hiện hành về trách nhiệm hình sự của pháp nhân thương mại và những yêu cầu đặt ra trong quá trình áp dụng. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2 và Chương 3, đặc biệt là cách tiếp cận kết hợp giữa phân tích quy định pháp luật và thực tiễn áp dụng nhằm nhận diện những bất cập cần hoàn thiện. Tuy nhiên, công trình chủ yếu tập trung vào khía cạnh lý luận và pháp luật hiện hành, chưa đánh giá sâu hiệu quả thực thi và những khó khăn phát sinh trong thực tiễn. Vì vậy, luận án tiếp tục nghiên cứu thực trạng áp dụng pháp luật, nhận diện các vướng mắc trong xử lý vi phạm của tổ chức trên không gian mạng và đề xuất các giải pháp hoàn thiện pháp luật phù hợp với yêu cầu bảo đảm an ninh mạng hiện nay.

- Luận án *Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo Luật hình sự Việt Nam* của Nguyễn Quý Khuyển [100] đã xây dựng cơ sở lý luận và phân tích thực trạng áp dụng pháp luật hình sự đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2 và Chương 3, đặc biệt là các phân tích về thực trạng pháp luật và những khó khăn trong xử lý tội phạm công nghệ cao. Tuy nhiên, công trình chủ yếu tiếp cận từ góc độ luật hình sự, chưa làm rõ mối quan hệ với pháp luật về an ninh mạng và quản trị không gian mạng. Vì vậy, luận án tiếp tục nghiên cứu sự phối hợp giữa các cơ chế pháp lý liên quan, đánh giá thực tiễn áp dụng pháp luật và đề xuất các giải pháp hoàn thiện pháp luật nhằm nâng cao hiệu quả phòng ngừa, phát hiện và xử lý các hành vi vi phạm trên không gian mạng.

- Luận án *Thực hiện pháp luật về an ninh mạng ở Việt Nam* của Bùi Thị Long [107] là công trình có giá trị tham khảo trực tiếp và quan trọng đối với đề tài nghiên cứu về hoàn thiện pháp luật an ninh mạng. Công trình đã xây dựng

tương đối đầy đủ cơ sở lý luận về thực hiện pháp luật an ninh mạng, làm rõ khái niệm, đặc điểm, nội dung, hình thức, vai trò và các điều kiện bảo đảm thực hiện pháp luật trong lĩnh vực này. Đồng thời, luận án đã phân tích thực trạng thực hiện pháp luật về an ninh mạng ở Việt Nam, chỉ ra những kết quả đạt được, hạn chế và nguyên nhân của các bất cập trong quá trình tổ chức thi hành pháp luật.

Luận án kế thừa công trình này trong Chương 2, Chương 3 và Chương 4, đặc biệt là các luận điểm về cơ sở lý luận của pháp luật an ninh mạng, vai trò của thực hiện pháp luật trong bảo vệ ANQG trên không gian mạng, cũng như các điều kiện bảo đảm hiệu quả thi hành pháp luật. Các phân tích về hạn chế, nguyên nhân và giải pháp nâng cao hiệu quả thực hiện pháp luật là nguồn tham khảo quan trọng để luận án tiếp tục nhận diện những vấn đề đặt ra đối với quá trình hoàn thiện pháp luật về an ninh mạng ở Việt Nam.

Tuy nhiên, công trình chủ yếu tiếp cận từ góc độ thực hiện pháp luật, trong khi chưa nghiên cứu toàn diện vấn đề hoàn thiện pháp luật về an ninh mạng với tư cách một hệ thống quy phạm có cấu trúc, tiêu chí đánh giá và cơ chế điều chỉnh riêng. Bên cạnh đó, nghiên cứu chưa phân tích sâu các yêu cầu mới phát sinh từ chuyển đổi số, dữ liệu lớn, trí tuệ nhân tạo, nền tảng số xuyên biên giới và hội nhập quốc tế. Vì vậy, luận án tiếp tục phát triển hướng nghiên cứu này bằng việc đánh giá thực trạng pháp luật hiện hành, nhận diện các khoảng trống, sự chồng chéo, thiếu thống nhất trong quy định pháp luật và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với yêu cầu bảo vệ ANQG, quyền con người, quyền công dân và quản trị không gian mạng trong bối cảnh hiện nay.

#### ***1.1.3.2. Nhóm công trình nghiên cứu ở nước ngoài***

(1) Các công trình nghiên cứu là sách:

- Cuốn sách *Computer forensics: cybercriminal, laws and evidence* (*Giám định máy tính: tội phạm mạng, pháp luật và chứng cứ*) của Marie-elen

Maras [242] là công trình có giá trị tham khảo quan trọng trong nghiên cứu về tội phạm mạng, chứng cứ điện tử và điều tra số. Luận án kế thừa các luận điểm của công trình trong Chương 2 và Chương 3, đặc biệt là cách tiếp cận kết hợp giữa pháp luật và kỹ thuật trong thu thập, sử dụng chứng cứ điện tử và xử lý tội phạm mạng. Tuy nhiên, công trình chủ yếu dựa trên kinh nghiệm quốc tế, chưa phân tích sâu khả năng áp dụng trong điều kiện pháp luật Việt Nam và những thách thức mới từ chuyển đổi số. Vì vậy, luận án tiếp tục nghiên cứu thực tiễn áp dụng pháp luật, cơ chế thu thập chứng cứ điện tử và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với bối cảnh hiện nay.

- Cuốn sách *Cybercrime and Digital Forensics: An Introduction (Tội phạm mạng và pháp y kỹ thuật số: Giới thiệu)* của Thomas I. Holt, Adam M. Bossler, Kathryn C. Seigfried Speller [259] là công trình có giá trị tham khảo trong nghiên cứu về tội phạm mạng và điều tra số. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2 và Chương 3, đặc biệt là cách tiếp cận kết hợp giữa pháp luật và công nghệ trong phòng ngừa, phát hiện và xử lý tội phạm mạng. Tuy nhiên, công trình chủ yếu dựa trên kinh nghiệm quốc tế, chưa phân tích sâu khả năng áp dụng trong điều kiện pháp luật và thực tiễn Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu thực trạng áp dụng pháp luật, cơ chế điều tra tội phạm mạng và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu chuyển đổi số và hội nhập quốc tế.

## (2) Các công trình nghiên cứu là luận án

- Luận án *Cybersecurity Policy Development at the State Level: A Case Study of Middle Tennessee (Xây dựng chính sách an ninh mạng ở cấp tiểu bang: nghiên cứu trường hợp Middle Tennessee)* của Daniel Leslie S. Cherr [216] là công trình có giá trị tham khảo trong nghiên cứu về xây dựng và thực thi chính sách an ninh mạng ở cấp địa phương. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2 và Chương 4, đặc biệt là các luận điểm về quản trị chính sách công, cơ chế phối hợp liên cơ quan và vai trò của các chủ thể trong bảo đảm an ninh mạng. Tuy nhiên, công trình được xây

dụng trong bối cảnh quản trị của Hoa Kỳ nên chưa làm rõ khả năng vận dụng đối với điều kiện thể chế và tổ chức bộ máy nhà nước ở Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu cơ chế phối hợp giữa các cơ quan, tổ chức trong bảo đảm an ninh mạng và đề xuất các giải pháp hoàn thiện pháp luật, nâng cao hiệu quả quản trị an ninh mạng phù hợp với bối cảnh Việt Nam hiện nay.

- Luận án *Research on Information Security in Business Processes Related to Global Risks (Nghiên cứu về an toàn thông tin trong quy trình kinh doanh gắn với rủi ro toàn cầu)* của Georg Sven Lampe [223] là công trình có giá trị tham khảo trong nghiên cứu về quản trị rủi ro, an toàn thông tin và trách nhiệm tuân thủ của tổ chức, doanh nghiệp trong môi trường số. Luận án kế thừa các kết quả nghiên cứu này trong Chương 2 và Chương 3, đặc biệt là các luận điểm về quản lý rủi ro, trách nhiệm tuân thủ pháp luật và việc tích hợp các yêu cầu về an ninh, an toàn thông tin vào hoạt động quản trị tổ chức. Tuy nhiên, công trình chủ yếu được xây dựng trên cơ sở lý luận và thực tiễn quốc tế, chưa phân tích sâu khả năng áp dụng trong điều kiện pháp lý và môi trường kinh doanh tại Việt Nam. Vì vậy, luận án tiếp tục nghiên cứu thực trạng quản trị rủi ro, an ninh thông tin của các chủ thể trên không gian mạng và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng phù hợp với yêu cầu chuyển đổi số và hội nhập quốc tế hiện nay.

Nhìn chung, các nghiên cứu trên đã giúp nhận diện các loại hành vi vi phạm, đặc điểm của tội phạm mạng, khó khăn trong điều tra, thu thập chứng cứ, xác định thẩm quyền và xử lý hành vi có yếu tố xuyên biên giới. Tuy nhiên, các nghiên cứu thường đi theo từng nhóm hành vi hoặc từng lĩnh vực pháp luật như hình sự, hành chính, an toàn thông tin, viễn thông, dữ liệu, thương mại điện tử. Chưa có nhiều nghiên cứu đánh giá một cách hệ thống mối quan hệ giữa hành vi vi phạm, chế tài xử lý, biện pháp bảo vệ an ninh mạng, địa vị pháp lý của chủ thể và cơ chế thực thi trong một chỉnh thể pháp luật về an ninh mạng. Vì vậy, luận án cần phân tích các vấn đề này theo sáu nhóm chế định đã xác định.

## **1.2. KHÁI QUÁT KẾT QUẢ NGHIÊN CỨU LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN VÀ NHỮNG VẤN ĐỀ ĐẶT RA**

### **1.2.1. Khái quát kết quả nghiên cứu liên quan đến đề tài luận án**

Qua nghiên cứu, khảo sát các công trình khoa học trong và ngoài nước có liên quan đến đề tài, nghiên cứu sinh rút ra được một số đánh giá như sau:

#### ***1.2.1.1. Những vấn đề đã được các nghiên cứu giải quyết tương đối rõ ràng, cụ thể***

Các công trình nghiên cứu đã luận giải tương đối rõ ràng nhiều vấn đề quan trọng trên cả ba phương diện về lý luận, thực trạng và giải pháp. Về lý luận, các nghiên cứu đã xác lập nền tảng vững chắc để đánh giá chất lượng pháp luật thông qua các tiêu chí cốt lõi về tính đầy đủ, đồng bộ, thống nhất, khả thi, minh bạch và kỹ thuật lập pháp. Về thực trạng, các công trình không chỉ khẳng định tầm quan trọng của pháp luật về an ninh mạng đối với ANQG, chủ quyền và phát triển kinh tế số, mà còn nhận diện rõ các dạng tội phạm mạng, những điểm nghẽn trong thực thi pháp luật và sự giao thoa phức tạp giữa pháp luật về an ninh mạng với các lĩnh vực chuyên ngành khác (dữ liệu cá nhân, thương mại điện tử...). Những kết quả nghiên cứu toàn diện về lý luận và thực trạng này chính là tiền đề khoa học quan trọng để luận án kế thừa, qua đó xây dựng cơ sở lý luận, xác lập tiêu chí đánh giá và định hướng đề xuất giải pháp mang tính hệ thống nhằm hoàn thiện pháp luật về an ninh mạng tại Việt Nam.

#### ***1.2.1.2. Những vấn đề chưa được các nghiên cứu giải quyết đầy đủ***

Mặc dù có nhiều công trình nghiên cứu liên quan, song các nghiên cứu hiện có vẫn chưa giải quyết đầy đủ một số vấn đề. Cụ thể là:

*Thứ nhất*, các công trình nghiên cứu chưa phân định thật sự rành mạch phạm vi điều chỉnh của pháp luật về an ninh mạng với các lĩnh vực pháp luật giáp ranh có tính giao thoa (như an toàn thông tin mạng, bảo vệ dữ liệu cá nhân, viễn thông, thương mại điện tử,...). Bên cạnh đó, chưa có nhiều công trình đi sâu đánh giá một cách toàn diện về “khả năng thích ứng” của các quy phạm pháp luật nội dung trước sự phát triển của các công nghệ mới. Việc giải quyết triệt để bài toán cân bằng lợi ích, giữa yêu cầu bảo vệ ANQG, bảo đảm

TTATXH với yêu cầu bảo vệ quyền, lợi ích hợp pháp, quyền riêng tư của cá nhân, tổ chức trên không gian mạng vẫn chưa được luận giải thật sự sâu sắc và đầy đủ.

*Thứ hai*, các công trình nghiên cứu chưa tập trung phân tích và đánh giá một cách có hệ thống về tính minh bạch và kỹ thuật lập pháp của hệ thống văn bản quy phạm pháp luật về an ninh mạng. Cụ thể, những bất cập về sự thiếu thống nhất trong khái niệm, thuật ngữ chuyên ngành; sự chồng chéo hoặc thiếu logic trong cấu trúc văn bản giữa luật chung và các đạo luật chuyên ngành rải rác chưa được nhận diện triệt để. Đặc biệt, các giải pháp hoàn thiện được đề xuất trong nhiều nghiên cứu trước đây phần lớn còn mang tính định hướng chung chung, chưa được thiết kế dựa trên một logic kỹ thuật pháp lý chặt chẽ.

*Thứ ba*, các công trình nghiên cứu phần lớn còn nặng về phân tích quy phạm (trên văn bản) mà thiếu đi sự kết nối sâu sắc với phân tích thực tiễn tổ chức thực hiện pháp luật. Nhiều công trình mới chỉ dừng lại ở việc mô tả pháp luật hiện hành, nhưng chưa đánh giá thấu đáo “tính khả thi” của các quy định khi áp dụng vào môi trường thực tiễn mang tính phi biên giới của không gian mạng. Những vấn đề cốt lõi về hiệu quả của cơ chế thực thi, sự vận hành của cơ chế phối hợp giữa các cơ quan nhà nước, trách nhiệm giải trình của doanh nghiệp (đặc biệt là các nền tảng xuyên biên giới) và năng lực tự bảo vệ quyền của cá nhân, tổ chức chưa được làm rõ. Đây là khoảng trống lớn mà luận án cần tập trung giải quyết để bảo đảm các quy định pháp luật không chỉ nằm trên giấy mà có thể thực sự đi vào đời sống.

### ***1.2.1.3. Những vấn đề các nghiên cứu còn tồn tại tranh luận, chưa thống nhất***

Từ các tài liệu đã khảo cứu, có thể nhận diện một số vấn đề còn tranh luận trong nghiên cứu pháp luật về an ninh mạng.

*Một là*, tranh luận về phạm vi của an ninh mạng. Một số nghiên cứu tiếp cận an ninh mạng chủ yếu như vấn đề kỹ thuật, bảo vệ hệ thống thông tin và dữ liệu; trong khi một số nghiên cứu khác coi an ninh mạng là bộ phận của

ANQG, gắn với chủ quyền quốc gia, TTATXH và quyền, lợi ích hợp pháp của các chủ thể trên không gian mạng.

*Hai là*, tranh luận về mối quan hệ giữa bảo vệ an ninh và bảo vệ quyền con người, quyền công dân. Một hướng tiếp cận nhấn mạnh tăng cường công cụ quản lý nhà nước để kiểm soát rủi ro trên không gian mạng; hướng khác nhấn mạnh quyền riêng tư, dữ liệu cá nhân, tự do thông tin, quyền tiếp cận thông tin và cơ chế kiểm soát quyền lực nhà nước.

*Ba là*, tranh luận về mô hình điều chỉnh pháp luật. Một số mô hình thiên về quy định cứng, chế tài mạnh và nghĩa vụ bắt buộc; trong khi mô hình khác nhấn mạnh quản trị rủi ro, tiêu chuẩn kỹ thuật, hợp tác công - tư, trách nhiệm giải trình và cơ chế tuân thủ linh hoạt. Luận án lựa chọn cách tiếp cận tích hợp: pháp luật về an ninh mạng cần đủ mạnh để bảo vệ ANQG, nhưng cũng phải minh bạch, khả thi, kiểm soát được quyền lực nhà nước và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức.

### **1.2.2. Những vấn đề luận án cần tiếp tục nghiên cứu**

Từ việc đánh giá các hướng nghiên cứu hiện có, luận án xác định các vấn đề cần tiếp tục nghiên cứu bao gồm:

*Thứ nhất*, các công trình nghiên cứu hiện nay chủ yếu tiếp cận vấn đề an ninh mạng dưới lăng kính của khoa học Luật hình sự, Tội phạm học (tập trung vào chế tài, hình phạt, đấu tranh phòng chống tội phạm) hoặc chuyên ngành Quản lý hành chính nhà nước (tập trung vào hoạt động quản lý, thanh tra, kiểm tra). Hiện nay, vẫn thiếu vắng một công trình nghiên cứu tổng thể, chuyên sâu tiếp cận dưới góc độ chuyên ngành Lý luận và lịch sử nhà nước và pháp luật. Cụ thể, chưa có công trình nào luận giải một cách hệ thống các vấn đề lý luận cốt lõi như: bản chất pháp lý của không gian mạng; khái niệm, đặc điểm, nội dung của pháp luật an ninh mạng; các nguyên tắc, tiêu chí đánh giá mức độ hoàn thiện của hệ thống pháp luật an ninh mạng trong điều kiện xây dựng Nhà nước pháp quyền xã hội chủ nghĩa.

*Thứ hai*, khoảng trống về cấu trúc pháp luật về an ninh mạng. Các nghiên cứu hiện có chưa hệ thống hóa đầy đủ pháp luật về an ninh mạng theo sáu nhóm chế định: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm; chế tài xử lý; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế về an ninh mạng. Thực tiễn cho thấy pháp luật an ninh mạng nói chung có sự giao thoa mật thiết với pháp luật dân sự, kinh tế, quốc tế. Tuy nhiên, các nghiên cứu hiện hành thường đề xuất giải pháp mang tính cục bộ cho từng chế định đơn lẻ. Vẫn còn thiếu một hệ thống quan điểm chỉ đạo toàn diện về các nhóm chế định mang tính đồng bộ, chiến lược lâu dài nhằm vừa bảo vệ vững chắc ANQG, vừa không cản trở quyền tự do kinh doanh, quyền con người và tiến trình hội nhập quốc tế của Việt Nam.

*Thứ ba*, khoảng trống về phân tích thực thi pháp luật. Một số nghiên cứu đã đề cập đến thực trạng pháp luật hoặc thực hiện pháp luật, nhưng chưa phân tích đầy đủ tính khả thi, hiệu quả thực thi, cơ chế phối hợp, năng lực của cơ quan thực thi và khả năng bảo vệ quyền của cá nhân, tổ chức. Đặc biệt trong bối cảnh bùng nổ của chuyển đổi số, kinh tế số và các công nghệ chiến lược mới (trí tuệ nhân tạo, điện toán đám mây, Internet vạn vật) đã làm nảy sinh những yêu cầu pháp lý hoàn toàn mới (như bảo vệ chủ quyền dữ liệu, an ninh chuỗi cung ứng, luồng dữ liệu xuyên biên giới). Các vấn đề này, hiện chưa được hệ thống hóa và đánh giá một cách toàn diện dưới góc độ kiến tạo thể chế.

*Thứ tư*, khoảng trống về giải pháp hoàn thiện. Nhiều giải pháp còn chung chung, chưa chỉ rõ cần sửa đổi quy định nào, bổ sung cơ chế nào, thiết kế lại chế định nào và giải pháp đó khắc phục hạn chế cụ thể nào.

Trên cơ sở các vấn đề cần tiếp tục nghiên cứu, luận án lựa chọn cách tiếp cận tích hợp để nghiên cứu hoàn thiện pháp luật về an ninh mạng ở Việt Nam. Đồng thời, luận án không tiếp cận pháp luật về an ninh mạng chỉ như công cụ tăng cường quyền lực quản lý nhà nước trên không gian mạng. Ngược lại, luận án cho rằng hoàn thiện pháp luật về an ninh mạng phải đồng thời giải quyết hai yêu cầu. Một mặt, pháp luật phải cung cấp cơ sở pháp lý

đầy đủ, đồng bộ và hiệu quả để phòng ngừa, phát hiện, ngăn chặn, xử lý các nguy cơ, hành vi xâm phạm an ninh mạng. Mặt khác, pháp luật phải thiết lập giới hạn, điều kiện, trình tự, trách nhiệm giải trình và cơ chế kiểm soát việc áp dụng các biện pháp bảo vệ an ninh mạng, bảo đảm quyền và lợi ích hợp pháp của cá nhân, tổ chức.

Từ lập trường đó, luận án sử dụng sáu nhóm chế định của pháp luật về an ninh mạng làm trục phân tích, gồm: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý hành vi vi phạm; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế. Đồng thời, luận án đánh giá các nhóm chế định này theo các tiêu chí: tính đầy đủ, tính đồng bộ, tính khả thi, tính minh bạch, khả năng thích ứng với công nghệ, hiệu quả thực thi và mức độ bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng.

### **1.3. GIẢI THUYẾT VÀ CÂU HỎI NGHIÊN CỨU**

#### **1.3.1. Giả thuyết nghiên cứu**

Thời gian qua, pháp luật về an ninh mạng ở Việt Nam tuy đã hình thành khung điều chỉnh cơ bản, nhưng vẫn còn những hạn chế về tính đầy đủ, tính đồng bộ, tính khả thi, tính minh bạch và khả năng thích ứng trước sự biến đổi nhanh của công nghệ số. Những hạn chế này làm giảm hiệu quả phòng ngừa, phát hiện và xử lý các nguy cơ, hành vi xâm phạm an ninh mạng. Vì vậy, nếu hệ thống pháp luật về an ninh mạng được hoàn thiện theo hướng đồng bộ, khả thi, minh bạch, thích ứng với công nghệ và bảo đảm cân bằng giữa yêu cầu bảo vệ ANQG với bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức, thì hiệu quả quản lý nhà nước và bảo vệ an ninh mạng ở Việt Nam sẽ được nâng cao.

Giả thuyết này được kiểm chứng thông qua ba cấp độ phân tích: một là, xây dựng cơ sở lý luận và tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng; hai là, đánh giá thực trạng pháp luật và thực tiễn thực hiện pháp luật về an ninh mạng ở Việt Nam theo các tiêu chí đã xác lập; ba là,

đề xuất các giải pháp hoàn thiện pháp luật tương ứng với những hạn chế và nguyên nhân đã nhận diện.

### **1.3.2. Câu hỏi nghiên cứu**

Với vấn đề nghiên cứu trên, luận án xác lập và tìm lời giải đáp cho một câu hỏi nghiên cứu chung (khái quát toàn diện nội dung luận án) và ba câu hỏi nghiên cứu cụ thể (tương ứng với ba phần chính của luận án).

Câu hỏi nghiên cứu chung là: Pháp luật về an ninh mạng ở Việt Nam cần được hoàn thiện theo những tiêu chí, nội dung và cơ chế thực thi nào để bảo đảm tính đầy đủ, đồng bộ, khả thi, minh bạch và thích ứng với sự phát triển nhanh của công nghệ số, đồng thời cân bằng giữa yêu cầu bảo vệ ANQG với bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng?

Các câu hỏi nghiên cứu cụ thể là:

(1) Cơ sở lý luận và tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng cần được xác lập như thế nào, đặc biệt trong bối cảnh chuyển đổi số, dữ liệu lớn, trí tuệ nhân tạo và sự gia tăng của các nguy cơ an ninh phi truyền thống trên không gian mạng?

(2) Pháp luật về an ninh mạng ở Việt Nam hiện nay đang bộc lộ những hạn chế nào về tính đầy đủ, tính đồng bộ, tính khả thi, tính minh bạch, phân định thẩm quyền, cơ chế thực thi và bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức?

(3) Cần hoàn thiện pháp luật về an ninh mạng ở Việt Nam theo những định hướng, nhóm giải pháp và thiết kế pháp lý cụ thể nào để khắc phục các hạn chế nêu trên và nâng cao hiệu quả bảo vệ an ninh mạng trong điều kiện chuyển đổi số? Đặc biệt, sau khi Luật An ninh mạng năm 2025 có hiệu lực, pháp luật về an ninh mạng ở nước ta cần được hoàn thiện như thế nào để đồng thời vừa bảo vệ ANQG gia, vừa bảo đảm quyền con người, quyền công dân, bảo vệ an ninh dữ liệu và cung cấp các điều kiện để phát triển kinh tế số?

## **Tiểu kết Chương 1**

Chương 1, nghiên cứu sinh trình bày tổng quan quá trình nghiên cứu, bao gồm nghiên cứu công trình khoa học từ các sách, đề tài khoa học, bài viết tạp chí, luận án, luận văn của các tác giả trong và ngoài nước có liên quan đến đề tài Luận án “Hoàn thiện pháp luật về an ninh mạng ở Việt Nam hiện nay”. Các công trình nghiên cứu liên quan đến đề tài luận án được phân loại thành các nhóm như sau: Những công trình nghiên cứu lý luận hoàn thiện pháp luật về an ninh mạng; những công trình nghiên cứu thực tiễn hoàn thiện pháp luật về an ninh mạng; những công trình khoa học nghiên cứu giải pháp hoàn thiện pháp luật về an ninh mạng.

Kết quả tổng quan cho thấy các nghiên cứu hiện có đã cung cấp nhiều cơ sở quan trọng cho việc nhận thức về an ninh mạng và pháp luật về an ninh mạng. Tuy nhiên, các nghiên cứu vẫn còn một số khoảng trống, cụ thể như: chưa phân định rõ phạm vi của pháp luật về an ninh mạng; chưa xây dựng bộ tiêu chí chuyên biệt để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng; chưa phân tích đầy đủ pháp luật về an ninh mạng theo các nhóm chế định cơ bản; chưa làm rõ thực trạng thực thi pháp luật và cơ chế vận hành của các quy phạm trong thực tiễn; đồng thời các giải pháp hoàn thiện còn thiếu sự liên kết chặt chẽ với hạn chế, nguyên nhân và tiêu chí đánh giá.

Trên cơ sở đó, luận án xác định vấn đề nghiên cứu trung tâm là: pháp luật về an ninh mạng ở Việt Nam cần được hoàn thiện theo những tiêu chí, nội dung và cơ chế thực thi nào để bảo đảm tính đầy đủ, đồng bộ, khả thi, minh bạch, thích ứng với công nghệ và cân bằng giữa bảo vệ ANQG với bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng. Và đây là căn cứ để luận án xây dựng cơ sở lý luận ở Chương 2, đánh giá thực trạng ở Chương 3 và đề xuất giải pháp hoàn thiện ở Chương 4.

## **Chương 2**

### **CƠ SỞ LÝ LUẬN CỦA HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG**

#### **2.1. KHUNG LÝ THUYẾT NGHIÊN CỨU PHÁP LUẬT VỀ AN NINH MẠNG**

##### **2.1.1. Cơ sở xác lập khung lý thuyết nghiên cứu pháp luật về an ninh mạng**

Pháp luật về an ninh mạng là một lĩnh vực pháp lý đặc thù, chịu tác động mạnh mẽ của sự phát triển khoa học, công nghệ và tính chất phức tạp của môi trường mạng. Để xây dựng và hoàn thiện lĩnh vực pháp luật này, việc xác lập một nền tảng lý thuyết vững chắc, đa chiều và có tính hệ thống là yêu cầu tiên quyết. Dưới góc độ lý luận nhà nước và pháp luật, nghiên cứu pháp luật về an ninh mạng không thể chỉ tiếp cận từ góc độ kỹ thuật bảo mật hoặc quản lý hành chính đơn thuần, mà cần phải đặt trong một khung lý thuyết tích hợp, kết hợp nhiều học thuyết pháp lý, chính trị và xã hội học hiện đại. Điều này giúp giải quyết hài hòa mối quan hệ giữa một bên là quyền lực quản lý của Nhà nước nhằm bảo đảm ANQG, TTATXH với một bên là yêu cầu bảo vệ các quyền cơ bản của con người, thúc đẩy phát triển kinh tế số, xã hội số và đổi mới sáng tạo. Theo đó, cơ sở xác lập khung lý thuyết nghiên cứu pháp luật về an ninh mạng bao gồm:

- Lý thuyết an ninh mở rộng và an ninh hóa của trường phái Copenhagen (tiêu biểu là Barry Buzan, Ole Wæver và Jaap de Wilde) khởi xướng đóng vai trò nền tảng trong việc nhận diện bản chất phi truyền thống của an ninh mạng [209]. Lý thuyết này chỉ ra rằng, trong bối cảnh toàn cầu hóa và bùng nổ công nghệ, khái niệm ANQG không còn giới hạn bó hẹp trong phạm vi quân sự truyền thống (bảo vệ lãnh thổ vật lý trước sự xâm lược vũ trang từ bên ngoài). Trái lại, ANQG hiện đại đã được mở rộng và đan cài chặt chẽ với năm lĩnh vực cốt lõi: quân sự, chính trị, kinh tế, xã hội và môi trường. Sự chuyển biến này phản ánh thực tế rằng các quốc gia phải đối mặt với những nguy cơ phi truyền thống có thể làm suy yếu thể chế từ bên trong

mà không cần tiếng súng chiến tranh. Áp dụng vào không gian mạng, lý thuyết an ninh mở rộng giúp chúng ta nhận diện an ninh mạng như một vấn đề an ninh phi truyền thống có sức tác động toàn diện và đa chiều. Một cuộc tấn công mạng quy mô lớn, một chiến dịch gián điệp thông tin hay hành vi phá hoại dữ liệu số nhắm vào hệ thống thông tin trọng yếu quốc gia không chỉ đơn thuần gây ra sự cố kỹ thuật; mà nó có thể làm tê liệt hệ thống tài chính, giao thông, viễn thông (ảnh hưởng an ninh kinh tế); làm lộ lọt bí mật nhà nước, can thiệp vào hoạt động quản trị công (ảnh hưởng an ninh chính trị); hoặc gieo rắc sự hoang mang, kích động bạo lực, lan truyền thông tin sai sự thật quy mô lớn (ảnh hưởng an ninh xã hội). Do đó, pháp luật về an ninh mạng đóng vai trò là công cụ thể chế hóa tư duy an ninh toàn diện, thiết lập cơ chế kiểm soát, phòng ngừa rủi ro đa chiều và bảo vệ các giá trị cốt lõi của quốc gia trên không gian mạng.

- Lý thuyết về chủ quyền số và quyền kiểm soát Internet (được phát triển bởi các học giả tiêu biểu như Jack Goldsmith và Tim Wu trong tác phẩm “Who Controls the Internet?”) khẳng định rằng không gian mạng không phải là một vùng lãnh thổ ảo hoàn toàn độc lập, nằm ngoài sự kiểm soát của Nhà nước và pháp luật [226]. Mặc dù ở phương diện hình thức biểu hiện, không gian mạng mang tính phi vật lý và xuyên biên giới, nhưng xét về thực chất, mọi hoạt động trên mạng đều được xây dựng trên nền tảng hạ tầng vật lý (máy chủ, đường truyền cáp quang, trung tâm dữ liệu) nằm dưới quyền quản lý hành chính của các quốc gia cụ thể và do các chủ thể (con người, tổ chức) chịu sự ràng buộc bởi quốc tịch và trật tự pháp lý quốc gia thực hiện. Từ luận điểm này, lý thuyết chủ quyền số xác lập quyền tài phán quốc gia trên không gian mạng dựa trên các nguyên tắc chủ quyền truyền thống (theo lãnh thổ và cá nhân). Nhà nước có quyền hạn và trách nhiệm pháp lý trong việc đặt ra các quy định điều chỉnh hành vi trên mạng, yêu cầu các nhà cung cấp dịch vụ viễn thông, Internet và các nền tảng xuyên biên giới phải tuân thủ luật pháp quốc gia khi cung cấp dịch vụ vào lãnh thổ nước mình. Tuy nhiên, chủ quyền số trong một Nhà nước pháp quyền hiện đại không thể hiểu là quyền kiểm soát

tuyệt đối, tùy tiện của Nhà nước. Việc áp dụng quyền lực công trên không gian mạng phải chịu sự giới hạn chặt chẽ bởi Hiến pháp, pháp luật, các nguyên tắc bảo vệ quyền con người, nguyên tắc tương xứng, trách nhiệm giải trình và cơ chế kiểm soát quyền lực hiệu quả. Do đó, việc hoàn thiện pháp luật về an ninh mạng vừa phải củng cố năng lực bảo vệ chủ quyền số quốc gia, vừa phải thiết lập ranh giới pháp lý minh bạch để ngăn ngừa nguy cơ tùy tiện, lạm quyền từ phía các cơ quan thực thi.

- Lý thuyết “Code is Law” (Mã nguồn là Luật) với việc điều chỉnh bằng kiến trúc kỹ thuật được giáo sư Lawrence Lessig trình bày trong tác phẩm kinh điển “Code and Other Laws of Cyberspace” là một bước đột phá trong tư duy quản trị môi trường mạng [233]. Lessig lập luận rằng hành vi của con người trên không gian mạng bị điều chỉnh và chi phối bởi bốn yếu tố cấu thành chính: pháp luật, chuẩn mực xã hội, thị trường và kiến trúc kỹ thuật; mà trong thế giới số, mã nguồn và cấu trúc phần mềm chính là kiến trúc kỹ thuật đó. “Code” thiết lập các giao thức kết nối, phân quyền truy cập, định dạng dữ liệu và giới hạn hành vi của người dùng một cách tự động, trực tiếp và triệt để, thực hiện chức năng điều chỉnh tương tự như các QPPL. Tính chất đặc thù này yêu cầu pháp luật về an ninh mạng không thể chỉ dựa vào các mệnh lệnh “cấm” và “phạt” mang tính hành chính truyền thống. Hiệu quả thực thi pháp luật trên không gian mạng phụ thuộc trực tiếp vào khả năng chuyển hóa các nghĩa vụ pháp lý thành các tiêu chuẩn kỹ thuật, quy chuẩn công nghệ và giao thức bảo mật bắt buộc đối với các chủ thể thiết kế, vận hành hệ thống thông tin. Pháp luật điều chỉnh công nghệ bằng cách buộc các nhà sản xuất phần cứng, nhà phát triển phần mềm và nhà cung cấp dịch vụ số phải tích hợp các biện pháp bảo vệ an ninh mạng (như mã hóa dữ liệu, xác thực hai yếu tố, lưu vết điện tử, tường lửa) ngay từ khâu thiết kế hệ thống. Song, việc điều chỉnh bằng công nghệ này cũng cần được kiểm soát chặt chẽ bởi pháp luật để bảo đảm tính minh bạch và trách nhiệm giải trình. Khi các hệ thống kỹ thuật tự động hóa việc lọc, chặn thông tin hoặc hạn chế quyền truy cập của người dùng, pháp luật phải thiết lập cơ chế khiếu nại, giải trình rõ ràng để bảo vệ

quyền con người, tránh tình trạng công nghệ vận hành như một công cụ tước đoạt quyền lợi hợp pháp của cá nhân, tổ chức mà không có cơ chế kiểm tra, kiểm soát.

- Lý thuyết xã hội rủi ro (Risk Society) Lý thuyết xã hội rủi ro được nhà xã hội học Ulrich Beck phát triển trong tác phẩm “Risk Society: Towards a New Modernity” đã chỉ ra rằng, xã hội hiện đại đang chuyển dịch từ việc phân phối của cải sang việc phân phối các rủi ro do chính quá trình hiện đại hóa và phát triển công nghệ sinh ra [256]. Những rủi ro này mang tính hệ thống, cấu trúc, lan truyền nhanh và vượt qua các giới hạn hành chính, lãnh thổ quốc gia truyền thống. Trong môi trường số, các mối đe dọa như tấn công mạng bằng mã độc tống tiền (ransomware), lộ lọt dữ liệu người dùng quy mô lớn, lừa đảo công nghệ cao, thao túng thông tin bằng trí tuệ nhân tạo (AI) và deepfake là biểu hiện điển hình của rủi ro cấu trúc xã hội hiện đại.

Hệ quả pháp lý của lý thuyết xã hội rủi ro đối với hoàn thiện pháp luật về an ninh mạng là sự thay đổi tư duy lập pháp: chuyển mạnh từ logic “xử lý sau vi phạm” sang logic “quản trị rủi ro chủ động từ sớm, từ xa”. Pháp luật an ninh mạng hiện đại không thể chỉ thiết kế theo hướng chờ vi phạm xảy ra rồi mới điều tra, áp dụng chế tài trừng phạt. Bởi trong môi trường mạng, khi sự cố đã xảy ra, thiệt hại về tài sản, dữ liệu, bí mật nhà nước, uy tín quốc gia hay niềm tin công chúng là vô cùng lớn và không thể khôi phục nguyên trạng. Vì vậy, pháp luật phải thiết lập một hệ thống các quy phạm định hướng hành vi phòng ngừa: bắt buộc đánh giá tác động rủi ro an ninh mạng, phân loại hệ thống thông tin và dữ liệu theo mức độ rủi ro để áp dụng biện pháp bảo vệ tương xứng, quy định nghĩa vụ báo cáo sự cố khẩn cấp, chia sẻ chỉ dấu tấn công và thiết lập cơ chế khôi phục thảm họa sau sự cố.

- Lý thuyết quyền riêng tư và giám sát (được phát triển bởi Daniel J. Solove trong “Understanding Privacy” và học giả Mireille Hildebrandt) đặt ra yêu cầu cốt lõi về bảo vệ quyền con người trong môi trường công nghệ [215], [244]. Solove cho rằng quyền riêng tư không đơn thuần là quyền “được để

yên ổn” (the right to be left alone), mà là một tập hợp phức tạp các lợi ích liên quan đến việc thu thập, xử lý, lưu trữ, sử dụng, truyền đưa và bảo vệ thông tin cá nhân. Trong thế giới số, mỗi hành vi của công dân đều để lại vết chân số và có nguy cơ bị giám sát, khai thác trái phép bởi cả các tập đoàn công nghệ thương mại và các cơ quan quyền lực nhà nước.

Nói tóm lại, dưới góc độ Nhà nước pháp quyền xã hội chủ nghĩa, hoàn thiện pháp luật về an ninh mạng phải giải quyết triệt để mối quan hệ biện chứng giữa bảo vệ ANQG và bảo vệ quyền con người, quyền công dân. Do đó, Nhà nước cần có các công cụ pháp lý mạnh mẽ để giám sát không gian mạng, ngăn chặn tội phạm, thu thập chứng cứ điện tử; tuy nhiên, các công cụ này (như chặn lọc thông tin, thu thập dữ liệu truy cập, giám sát hệ thống) phải được giới hạn rõ ràng bởi các quy định pháp luật. Pháp luật phải quy định cụ thể căn cứ, thẩm quyền, trình tự, thủ tục áp dụng các biện pháp can thiệp kỹ thuật này, đồng thời thiết lập cơ chế kiểm soát tư pháp độc lập, trách nhiệm giải trình và quyền khiếu nại, yêu cầu bồi thường thiệt hại của công dân khi quyền lợi bị xâm phạm trái pháp luật. Điều này bảo đảm rằng công tác bảo vệ an ninh mạng luôn tuân thủ nguyên tắc hiến định, bảo vệ phẩm giá và quyền tự do của con người trong kỷ nguyên số.

### **2.1.2. Khung lý thuyết tích hợp nghiên cứu pháp luật về an ninh mạng**

Trên cơ sở phân tích và kế thừa có chọn lọc các học thuyết nền tảng nêu trên, luận án xác lập một khung lý thuyết tích hợp làm kim chỉ nam xuyên suốt quá trình nghiên cứu, đánh giá thực trạng và đề xuất giải pháp hoàn thiện pháp luật về an ninh mạng ở Việt Nam hiện nay. Khung lý thuyết tích hợp này không tiếp cận pháp luật về an ninh mạng như một công cụ quyền lực đơn thuần của Nhà nước, mà xem xét nó như một hệ thống quản trị rủi ro đa chiều, hoạt động trong khuôn khổ Nhà nước pháp quyền xã hội chủ nghĩa, hướng tới sự cân bằng và phát triển bền vững. Khung lý thuyết tích hợp này bao gồm năm đặc tính cốt lõi sau:

*Một là*, pháp luật về an ninh mạng là công cụ bảo đảm quốc phòng, an ninh và bảo vệ chủ quyền quốc gia trên không gian mạng. Đặc tính này kế thừa lý thuyết an ninh mở rộng và chủ quyền số, xác định nhiệm vụ trọng yếu hàng đầu của pháp luật là thiết lập hành lang pháp lý đầy đủ, đồng bộ để nhận diện, phòng ngừa, đấu tranh và xử lý hiệu quả các hành vi tấn công mạng, gián điệp mạng, khủng bố mạng, chiến tranh thông tin và bảo vệ hệ thống hạ tầng thông tin quan trọng về ANQG.

*Hai là*, pháp luật về an ninh mạng là cơ chế quản trị rủi ro công nghệ chủ động. Kế thừa lý thuyết xã hội rủi ro, đặc tính này đòi hỏi pháp luật phải dịch chuyển trọng tâm từ xử lý hậu quả sang phòng ngừa từ sớm, từ xa. Quan điểm này được thể hiện thông qua việc quy định nghĩa vụ đánh giá rủi ro định kỳ, phân loại hệ thống thông tin theo cấp độ để áp dụng tiêu chuẩn bảo mật tương xứng, xây dựng cơ chế cảnh báo sớm, báo cáo sự cố khẩn cấp và khôi phục hệ thống sau tấn công mạng.

*Ba là*, pháp luật về an ninh mạng là khung khổ phân bổ trách nhiệm đa chủ thể. Đặc tính này nhận diện bảo vệ an ninh mạng không phải là trách nhiệm độc quyền của cơ quan nhà nước, mà là trách nhiệm chung của toàn xã hội. Pháp luật có vai trò phân định rõ ràng quyền hạn, nghĩa vụ, trách nhiệm giải trình và mối quan hệ phối hợp giữa cơ quan quản lý nhà nước, lực lượng chuyên trách, chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ số và người sử dụng mạng.

*Bốn là*, pháp luật về an ninh mạng đặt trong khuôn khổ Nhà nước pháp quyền và bảo vệ quyền con người. Kế thừa lý thuyết quyền riêng tư và pháp quyền công nghệ, đặc tính này đặt ra giới hạn pháp lý nghiêm ngặt đối với việc áp dụng các biện pháp can thiệp kỹ thuật của cơ quan nhà nước. Bảo đảm các biện pháp này tuân thủ nguyên tắc hợp pháp, cần thiết, tương xứng, minh bạch; đồng thời thiết lập cơ chế giám sát, trách nhiệm giải trình và quyền khiếu nại, bồi thường của chủ thể bị tác động.

Năm là, pháp luật về an ninh mạng phải thích ứng linh hoạt với sự phát triển của công nghệ nhưng bảo đảm tính ổn định tương đối của hệ thống. Kế thừa lý thuyết “Code is Law”, đặc tính này đòi hỏi kỹ thuật lập pháp phải kết hợp hài hòa giữa các quy phạm nguyên tắc mang tính định hướng lâu dài với các quy chuẩn kỹ thuật, tiêu chuẩn công nghệ cập nhật linh hoạt thông qua văn bản dưới luật. Đảm bảo pháp luật luôn bao quát được các công nghệ mới nổi (AI, Big Data, Cloud Computing, Blockchain) mà không tạo ra gánh nặng tuân thủ quá mức cản trở sự đổi mới sáng tạo, chuyển đổi số và phát triển kinh tế số, xã hội số.

Khung tiếp cận này là cơ sở để luận án xây dựng khái niệm, xác định đặc điểm, cấu trúc, tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng, đồng thời sử dụng làm công cụ phân tích ở Chương 3 và xây dựng giải pháp ở Chương 4.

## **2.2. KHÁI NIỆM, ĐẶC ĐIỂM, VAI TRÒ, CẤU TRÚC LÝ LUẬN CỦA PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM**

### **2.2.1. Khái niệm pháp luật về an ninh mạng**

Để làm rõ khái niệm pháp luật về an ninh mạng, trước hết cần thống nhất nhận thức về không gian mạng và an ninh mạng. Đây là hai khái niệm có quan hệ chặt chẽ với nhau, bởi an ninh mạng chỉ có thể được nhận diện đầy đủ khi đặt trong môi trường tồn tại, vận hành và phát sinh các quan hệ xã hội đặc thù là không gian mạng.

Trong bối cảnh Cách mạng công nghiệp lần thứ tư, không gian mạng không còn là môi trường kỹ thuật thuần túy, mà đã trở thành không gian tồn tại, giao tiếp, trao đổi thông tin, sản xuất, kinh doanh, quản trị nhà nước, cung ứng dịch vụ công và thực hiện quyền, lợi ích hợp pháp của cá nhân, tổ chức. Không gian mạng được hình thành trên cơ sở sự kết nối của hạ tầng công nghệ thông tin, mạng viễn thông, mạng Internet, hệ thống thông tin, cơ sở dữ liệu, thiết bị số, nền tảng số và các hoạt động tương tác xã hội diễn ra thông qua các kết nối đó. Mặc dù không gian mạng có tính phi vật lý ở hình thức biểu hiện, nhưng các hành vi diễn ra trên không gian mạng có thể tạo ra hậu

quả trực tiếp trong đời sống thực, tác động đến ANQG, TTATXH, hoạt động kinh tế, quyền cá nhân, tài sản, dữ liệu và niềm tin xã hội.

Từ cách tiếp cận đó, có thể hiểu: *Không gian mạng là môi trường được hình thành từ sự kết nối của hạ tầng công nghệ thông tin, mạng viễn thông, mạng Internet, hệ thống thông tin, cơ sở dữ liệu, thiết bị số, nền tảng số và các tương tác xã hội diễn ra thông qua các kết nối đó; là môi trường có tính phi vật lý ở hình thức biểu hiện nhưng có khả năng tạo ra hậu quả thực tế đối với ANQG, TTATXH, hoạt động kinh tế, quyền và lợi ích hợp pháp của cá nhân, tổ chức.*

Trên cơ sở nhận thức về không gian mạng, an ninh mạng cần được tiếp cận không chỉ từ góc độ kỹ thuật bảo vệ hệ thống thông tin, mà còn từ góc độ bảo vệ ANQG, TTATXH, dữ liệu, quyền và lợi ích hợp pháp của các chủ thể trên không gian mạng. Theo khoản 1 Điều 3 Luật An ninh mạng năm 2018, an ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến ANQG, TTATXH, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Quy định này cho thấy pháp luật Việt Nam tiếp cận an ninh mạng với phạm vi rộng, không chỉ giới hạn ở bảo vệ kỹ thuật hệ thống, mà còn gắn trực tiếp với bảo vệ các lợi ích pháp lý quan trọng của Nhà nước, xã hội, tổ chức và cá nhân.

Về bản chất, an ninh mạng có thể được nhìn nhận ở hai phương diện cơ bản. *Thứ nhất*, đó là an ninh của thông tin, dữ liệu, hệ thống thông tin và hạ tầng kỹ thuật trên không gian mạng, bao gồm việc bảo đảm tính bí mật, tính toàn vẹn, tính sẵn sàng, tính xác thực và khả năng phục hồi của hệ thống, dữ liệu. *Thứ hai*, đó là an ninh của các quan hệ xã hội phát sinh trên không gian mạng, bao gồm việc phòng ngừa, phát hiện, ngăn chặn, xử lý các hành vi sử dụng không gian mạng để xâm phạm ANQG, TTATXH, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Vì vậy, trong phạm vi luận án, có thể hiểu: *An ninh mạng là trạng thái an toàn, ổn định, tin cậy và được bảo vệ của hoạt động trên không gian mạng,*

*trong đó hệ thống thông tin, dữ liệu, hạ tầng mạng, chủ thể và các quan hệ xã hội trên không gian mạng không bị xâm hại hoặc đe dọa xâm hại đến ANQG, TTATXH, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.*

Từ khái niệm an ninh mạng, có thể xác định pháp luật về an ninh mạng là tổng thể các QPPL điều chỉnh các quan hệ xã hội phát sinh trong hoạt động bảo vệ an ninh mạng. Pháp luật về an ninh mạng không đồng nhất với toàn bộ pháp luật điều chỉnh hoạt động trên không gian mạng, bởi không gian mạng còn là môi trường của nhiều lĩnh vực pháp luật khác như thương mại điện tử, giao dịch điện tử, viễn thông, sở hữu trí tuệ, tài chính số, bảo vệ người tiêu dùng, báo chí, truyền thông và quản trị dữ liệu. Pháp luật về an ninh mạng chỉ tập trung vào những quan hệ xã hội gắn trực tiếp với mục tiêu bảo vệ ANQG, TTATXH, hệ thống thông tin, dữ liệu, quyền và lợi ích hợp pháp của các chủ thể trước các nguy cơ, hành vi xâm phạm trên không gian mạng.

Theo đó, pháp luật về an ninh mạng có phạm vi điều chỉnh bao gồm các nhóm quan hệ cơ bản sau: quan hệ phát sinh trong việc xác lập nguyên tắc bảo vệ an ninh mạng; quan hệ về nhận diện và xử lý hành vi vi phạm pháp luật về an ninh mạng; quan hệ về chế tài xử lý hành vi vi phạm; quan hệ về địa vị pháp lý của cơ quan nhà nước, lực lượng chuyên trách, doanh nghiệp, chủ quản hệ thống thông tin, cá nhân, tổ chức sử dụng không gian mạng; quan hệ về áp dụng biện pháp bảo vệ an ninh mạng; quan hệ về phối hợp trong nước và hợp tác quốc tế trong lĩnh vực an ninh mạng.

Nghiên cứu kinh nghiệm xây dựng pháp luật và chiến lược an ninh mạng của các quốc gia cho thấy chưa tồn tại một cách tiếp cận thống nhất về an ninh mạng. Một số quốc gia và tổ chức khu vực, tiêu biểu như Hà Lan, Luxembourg và Liên minh châu Âu, tiếp cận an ninh mạng chủ yếu dưới góc độ bảo đảm an toàn thông tin và quản trị rủi ro. Trong khi đó, các quốc gia như Hoa Kỳ, Liên hiệp Anh, Canada, Australia, Liên bang Nga, Singapore, Nhật Bản và Việt Nam coi an ninh mạng là một bộ phận cấu thành của ANQG. Mặc dù có sự khác biệt về trọng tâm điều chỉnh, xu hướng chung

hiện nay là xây dựng pháp luật về an ninh mạng trên cơ sở kết hợp các cách tiếp cận về bảo vệ chủ quyền quốc gia trên không gian mạng, quản trị rủi ro, bảo vệ hạ tầng thông tin trọng yếu, bảo vệ dữ liệu và quyền con người, nhằm bảo đảm hài hòa giữa yêu cầu bảo vệ ANQG với phát triển kinh tế số, đổi mới sáng tạo và hội nhập quốc tế [19].

Từ đó, có thể đưa ra khái niệm: *Pháp luật về an ninh mạng là tổng thể các QPPL do Nhà nước ban hành hoặc thừa nhận, điều chỉnh các quan hệ xã hội phát sinh trong hoạt động bảo vệ ANQG, TTATXH, hệ thống thông tin, dữ liệu, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.*

Khái niệm này cho thấy pháp luật về an ninh mạng có một số nội hàm cơ bản.

*Thứ nhất*, pháp luật về an ninh mạng là bộ phận của hệ thống pháp luật, do Nhà nước ban hành và được bảo đảm thực hiện bằng quyền lực nhà nước. Do đó, các quy định về an ninh mạng phải phù hợp với Hiến pháp, bảo đảm tính hợp pháp, tính thống nhất và tính khả thi trong hệ thống pháp luật.

*Thứ hai*, pháp luật về an ninh mạng hướng tới mục tiêu bảo vệ đồng thời nhiều lợi ích pháp lý quan trọng, bao gồm ANQG, TTATXH, hệ thống thông tin, dữ liệu, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Đây là điểm khác biệt so với cách tiếp cận thuần túy kỹ thuật về an toàn thông tin mạng.

*Thứ ba*, pháp luật về an ninh mạng không chỉ bao gồm các quy định về hành vi bị cấm và chế tài xử lý, mà còn bao gồm các quy định về nguyên tắc, chủ thể, biện pháp phòng ngừa, quản trị rủi ro, cơ chế phối hợp, cơ chế thực thi và hợp tác quốc tế. Nói cách khác, pháp luật về an ninh mạng là một chỉnh thể gồm cả quy phạm nội dung, quy phạm thủ tục và các cơ chế bảo đảm thực hiện.

*Thứ tư*, pháp luật về an ninh mạng phải được đặt trong khuôn khổ Nhà nước pháp quyền. Điều này có nghĩa là quyền lực nhà nước trong lĩnh vực an

ninh mạng phải có giới hạn, có điều kiện áp dụng, có thẩm quyền rõ ràng, có trình tự, thủ tục, có cơ chế giám sát và trách nhiệm giải trình. Các biện pháp bảo vệ an ninh mạng, nhất là những biện pháp có khả năng tác động đến quyền riêng tư, dữ liệu cá nhân, quyền tiếp cận thông tin, quyền tự do kinh doanh hợp pháp, phải được áp dụng trên cơ sở cần thiết, hợp lý và tương xứng.

Để làm rõ khái niệm pháp luật về an ninh mạng đòi hỏi phải phân định ranh giới với các lĩnh vực pháp luật giáp ranh để tránh sự chồng chéo hoặc dàn trải trong nghiên cứu và thực thi:

- Với pháp luật về an toàn thông tin mạng, tiêu biểu là quy định tại Luật An toàn thông tin mạng năm 2015 chủ yếu điều chỉnh các quan hệ xã hội mang tính kỹ thuật - công nghệ thuần túy, tập trung vào việc bảo vệ thông tin và hệ thống thông tin tránh khỏi sự can thiệp, phá hoại kỹ thuật trái phép nhằm duy trì ba thuộc tính cơ bản của thông tin (tính bí mật, tính toàn vẹn, tính sẵn sàng). Trong khi đó, pháp luật về an ninh mạng có phạm vi điều chỉnh rộng và sâu sắc hơn, gắn chặt với khía cạnh chính trị, quốc phòng, bảo vệ chế độ, bảo vệ ANQG, bảo bảo TTATXH và khẳng định chủ quyền quốc gia trên môi trường số. Hai lĩnh vực này có mối quan hệ giao thoa bổ sung cho nhau, trong đó an toàn thông tin mạng là nền tảng kỹ thuật, còn an ninh mạng là mục tiêu chính trị - pháp lý ở cấp độ vĩ mô.

- Với pháp luật bảo vệ dữ liệu cá nhân, đây là lĩnh vực tập trung điều chỉnh mối quan hệ giữa chủ thể dữ liệu và các bên kiểm soát, xử lý dữ liệu, thiết lập các quy trình, điều kiện thu thập, sử dụng, lưu trữ và chuyển giao thông tin cá nhân dựa trên sự đồng ý của người dùng. Vấn đề bảo vệ dữ liệu cá nhân chỉ thuộc phạm vi điều chỉnh của pháp luật về an ninh mạng khi các hành vi xâm phạm dữ liệu cá nhân xảy ra trên quy mô lớn, có tổ chức, hoặc nhắm vào hệ thống thông tin quan trọng quốc gia, gây ra nguy cơ đe dọa trực tiếp đến ANQG, TTATXH hoặc an ninh hệ thống mạng quốc gia.

- Với các lĩnh vực pháp luật chuyên ngành khác trên không gian mạng như giao dịch điện tử, viễn thông, thương mại điện tử, sở hữu trí tuệ, báo chí,

xuất bản, cần xác định rằng quy phạm của các lĩnh vực này không mặc nhiên thuộc phạm vi của pháp luật về an ninh mạng, trừ khi chúng trực tiếp điều chỉnh việc phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi xâm phạm an ninh mạng hoặc bảo vệ hạ tầng, dữ liệu trước các cuộc tấn công mạng.

Như vậy, trong phạm vi luận án, một quy phạm được xác định là thuộc pháp luật về an ninh mạng khi nó trực tiếp điều chỉnh hoạt động, trách nhiệm hoặc biện pháp bảo vệ an ninh mạng, hướng đến phòng ngừa, phát hiện, xử lý hoặc khắc phục các hành vi xâm nhập, tấn công, phá hoại hệ thống thông tin, dữ liệu hoặc hạ tầng số, đồng thời có cơ chế bảo đảm thực thi và áp dụng rõ ràng đối với các chủ thể trên không gian mạng. Ngược lại, quy phạm chỉ liên quan đến pháp luật về an ninh mạng là khi nó điều chỉnh các vấn đề gián tiếp hỗ trợ cho hoạt động bảo đảm an ninh mạng, chẳng hạn quản lý dữ liệu, bảo vệ quyền người dùng, tiêu chuẩn kỹ thuật hay cơ chế phối hợp giữa các cơ quan, không trực tiếp xử lý các hành vi xâm phạm an ninh mạng. Việc xác định rõ ranh giới này giúp Luận án tập trung phân tích, đánh giá các quy phạm trực tiếp, tránh dàn trải, đồng thời cung cấp cơ sở khoa học cho việc nhận diện khoảng trống, mâu thuẫn, chồng chéo trong pháp luật và đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng ở Việt Nam.

Pháp luật về an ninh mạng được tiếp cận theo hướng tập trung vào các quy phạm có chức năng bảo vệ an ninh mạng, không mở rộng sang toàn bộ pháp luật điều chỉnh kinh tế số, xã hội số hoặc quản trị dữ liệu nói chung. Cách tiếp cận này giúp xác định rõ phạm vi nghiên cứu, tránh đồng nhất pháp luật về an ninh mạng với toàn bộ pháp luật điều chỉnh hoạt động trên không gian mạng, đồng thời bảo đảm việc nghiên cứu có trọng tâm, phù hợp với mục tiêu của luận án.

### **2.2.2. Đặc điểm của pháp luật về an ninh mạng**

#### **2.2.2.1. Tính liên ngành**

Pháp luật về an ninh mạng có tính liên ngành sâu sắc. Đặc điểm này xuất phát từ bản chất phức hợp của không gian mạng - một môi trường kỹ

thuật số nhưng chi phối trực tiếp đến các quan hệ kinh tế, chính trị và xã hội. Các hành vi diễn ra trên không gian mạng không phụ thuộc hoàn toàn vào phạm vi điều chỉnh của một ngành luật độc lập. Cụ thể, một hành vi tấn công mạng có thể đồng thời xâm phạm ANQG (đối tượng điều chỉnh của luật hiến pháp, hành chính), gây thiệt hại về tài sản, dữ liệu (luật dân sự), xâm phạm hạ tầng thông tin (luật viễn thông) và cấu thành tội phạm (luật hình sự, tổ tụng hình sự).

Đặc điểm này đặt ra yêu cầu nội tại đối với hoạt động lập pháp: việc hoàn thiện pháp luật về an ninh mạng không thể tiến hành đơn lẻ, cục bộ mà đòi hỏi tính đồng bộ hóa cao độ trong tổng thể hệ thống pháp luật. Sự tương thích, giao thoa giữa đạo luật chuyên ngành về an ninh mạng với pháp luật dân sự, hình sự, giao dịch điện tử và bảo vệ dữ liệu cá nhân là điều kiện tiên quyết để ngăn ngừa xung đột pháp luật, khắc phục các khoảng trống về thẩm quyền và bảo đảm hiệu lực thi hành trong thực tiễn.

#### ***2.2.2.2. Tính thích ứng cao với công nghệ***

Đối tượng điều chỉnh của pháp luật về an ninh mạng là các quan hệ xã hội phát sinh trong môi trường số - nơi chịu sự tác động trực tiếp và biến đổi không ngừng của khoa học công nghệ. Sự gia tăng của các công nghệ chiến lược như trí tuệ nhân tạo (AI), điện toán đám mây, hay Internet vạn vật (IoT) làm xuất hiện các phương thức tấn công mạng mới với tốc độ vượt xa chu kỳ xây dựng và ban hành văn bản QPPL truyền thống. Do đó, đặc tính nổi bật của pháp luật về an ninh mạng là tính thích ứng cao, phản bác lại phương pháp lập pháp liệt kê tĩnh.

Tính thích ứng này được cụ thể hóa thông qua việc xây dựng các QPPL mang tính nguyên tắc, kết hợp với các tiêu chí nhận diện mở và cơ chế ủy quyền lập pháp linh hoạt. Điều này cho phép các cơ quan quản lý nhà nước kịp thời cập nhật các quy chuẩn kỹ thuật về an toàn thông tin và định danh điện tử mà không phá vỡ cấu trúc của đạo luật gốc. Mặc dù vậy, dưới lăng kính của nhà nước pháp quyền, tính linh hoạt phải chịu sự giới hạn bởi các nguyên tắc

hiến định, bảo đảm không dẫn đến sự mở rộng thẩm quyền tùy tiện, gây tổn hại đến quyền và lợi ích hợp pháp của các chủ thể tham gia không gian mạng.

### ***2.2.2.3. Tính phòng ngừa và quản trị rủi ro***

Đặc thù của các mối đe dọa trên không gian mạng là khả năng ẩn danh, tốc độ lan truyền theo cấp số nhân và hệ quả phá hủy trên diện rộng đối với các hệ thống hạ tầng thông tin trọng yếu. Tính chất này định hình đặc điểm phòng ngừa và quản trị rủi ro chủ động của pháp luật về an ninh mạng, đánh dấu sự chuyển dịch phương pháp điều chỉnh từ mô hình “trừng phạt hậu kiểm” sang mô hình “kiểm soát từ sớm, từ xa”.

Về mặt pháp lý, tính phòng ngừa được thể chế hóa thông qua các chế định bắt buộc về đánh giá rủi ro, phân loại cấp độ an toàn hệ thống thông tin, cơ chế giám sát, cảnh báo sớm và tổ chức diễn tập ứng phó sự cố. Hơn thế nữa, hoạt động quản trị rủi ro đòi hỏi pháp luật phải tuân thủ nguyên tắc tương xứng; theo đó, các biện pháp kiểm soát và nghĩa vụ pháp lý phải được thiết lập dựa trên mức độ rủi ro tương ứng của từng hệ thống cụ thể. Phương thức tiếp cận này vừa bảo đảm sự tập trung nguồn lực quốc gia vào việc bảo vệ các mục tiêu trọng yếu, vừa ngăn ngừa việc thiết lập các rào cản hành chính và chi phí tuân thủ bất hợp lý đối với doanh nghiệp, duy trì động lực cho tiến trình đổi mới sáng tạo.

### ***2.2.2.4. Tính xuyên biên giới***

Môi trường mạng mang đặc tính phi biên giới lãnh thổ, dẫn đến việc các quan hệ pháp luật phát sinh thường mang yếu tố nước ngoài. Một hành vi xâm phạm an ninh mạng có thể được thực hiện bởi chủ thể cư trú tại một quốc gia, thông qua máy chủ tại quốc gia thứ hai, nhằm tấn công mục tiêu tại Việt Nam. Đặc tính xuyên biên giới này làm phát sinh các thách thức pháp lý phức tạp liên quan đến xung đột thẩm quyền tài phán, thu thập chứng cứ điện tử và thực thi chế tài.

Thực tiễn cũng cho thấy, phần lớn dữ liệu và nền tảng hạ tầng số tại Việt Nam đang chịu sự chi phối của các tập đoàn công nghệ xuyên quốc gia. Hệ quả

tất yếu là pháp luật về an ninh mạng phải thiết lập các quy phạm đặc thù nhằm ràng buộc trách nhiệm pháp lý của các tổ chức cung cấp dịch vụ xuyên biên giới đối với nghĩa vụ lưu trữ dữ liệu, kiểm duyệt nội dung và phối hợp điều tra. Song song đó, hệ thống pháp luật quốc gia cần bảo đảm mức độ tương thích với các chuẩn mực và điều ước quốc tế, tạo tiền đề cho các hoạt động tương trợ tư pháp và dẫn độ tội phạm, nhưng vẫn phải duy trì nguyên tắc tối cao là bảo vệ độc lập, chủ quyền và quyền tài phán quốc gia.

#### ***2.2.2.5. Tính đa chủ thể trong thực thi***

Khác với các lĩnh vực pháp luật thuần túy dựa vào cơ chế quản lý nhà nước, việc bảo đảm an ninh mạng là kết quả của cơ chế đồng quản trị, đòi hỏi sự tham gia của toàn xã hội. Tính đa chủ thể của pháp luật về an ninh mạng được biểu hiện qua việc phân định rõ thẩm quyền, quyền và nghĩa vụ của ba nhóm chủ thể cơ bản.

*Thứ nhất*, Nhà nước và lực lượng chuyên trách đóng vai trò kiến tạo thể chế, điều phối vĩ mô, thanh tra, kiểm tra và trực tiếp tiến hành các biện pháp đấu tranh chống lại các hành vi xâm phạm ANQG.

*Thứ hai*, các doanh nghiệp cung cấp dịch vụ viễn thông, Internet và chủ quản hệ thống thông tin đóng vai trò là tuyến phòng thủ kỹ thuật đầu tiên; chịu trách nhiệm thiết lập các biện pháp bảo mật, lưu vết hoạt động và phối hợp ứng cứu sự cố.

*Thứ ba*, tổ chức và cá nhân sử dụng không gian mạng vừa là chủ thể thụ hưởng sự bảo hộ của pháp luật, vừa mang nghĩa vụ tuân thủ các quy tắc ứng xử và không lạm dụng môi trường số để thực hiện hành vi trái pháp luật. Sự minh định trách nhiệm pháp lý giữa các nhóm chủ thể này là nhân tố bảo đảm tính khả thi và hiệu lực thi hành của pháp luật về an ninh mạng.

#### ***2.2.2.6. Tính cân bằng giữa bảo vệ an ninh quốc gia và bảo vệ quyền con người, quyền công dân***

Một trong những đặc điểm pháp lý mang tính cốt lõi và phức tạp nhất của pháp luật về an ninh mạng là việc giải quyết mối quan hệ biện chứng giữa

yêu cầu bảo vệ ANQG, TTATXH và yêu cầu bảo vệ các quyền cơ bản của con người, quyền công dân. Để thực hiện chức năng phòng, chống tội phạm mạng, Nhà nước tất yếu phải được trao các công cụ pháp lý mang tính quyền lực như quyền giám sát hệ thống, thu thập dữ liệu điện tử, hoặc áp dụng các biện pháp ngăn chặn, đình chỉ dịch vụ mạng. Tuy nhiên, nếu thiếu vắng cơ chế kiểm soát quyền lực, các biện pháp này hoàn toàn có thể xâm phạm đến quyền riêng tư, bí mật đời tư, tự do biểu đạt và tự do kinh doanh của cá nhân, tổ chức.

Theo đó, dưới góc độ của khoa học pháp lý, tính cân bằng đòi hỏi mọi giới hạn quyền con người trên không gian mạng phải được quy định rõ trong văn bản luật, có căn cứ pháp lý vững chắc và tuân thủ nghiêm ngặt nguyên tắc cần thiết, tương xứng. Đồng thời, các QPPL phải thiết lập được trình tự, thủ tục áp dụng chặt chẽ, đi kèm với cơ chế giám sát độc lập, quyền khiếu nại và trách nhiệm giải trình nhằm phòng ngừa rủi ro, lạm quyền từ các cơ quan thực thi pháp luật.

### **2.2.3. Vai trò của pháp luật về an ninh mạng**

Dưới góc độ lý luận nhà nước và pháp luật, pháp luật về an ninh mạng không chỉ đơn thuần là tập hợp các quy tắc quản lý hành chính hay kỹ thuật đơn thuần, mà là một công cụ kiểm soát xã hội đặc thù mang tính quyền lực nhà nước. Vai trò của hệ thống pháp luật này được thể hiện một cách toàn diện trên bốn phương diện cốt lõi, từ việc bảo vệ sự tồn vong của chế độ, kiến tạo môi trường số an toàn đến việc bảo đảm các quyền cơ bản của con người trong kỷ nguyên công nghệ.

*Thứ nhất*, pháp luật về an ninh mạng đóng vai trò là công cụ pháp lý tối cao để bảo vệ ANQG, bảo đảm TTATXH, bảo vệ chủ quyền quốc gia trên không gian mạng và hệ thống thông tin quan trọng. Trong bối cảnh không gian mạng đã trở thành miền lãnh thổ thứ năm, các mối đe dọa từ gián điệp mạng, khủng bố mạng hay chiến tranh thông tin có khả năng làm suy yếu trực tiếp thể chế chính trị và làm tê liệt hạ tầng trọng yếu của quốc gia. Nhận thức được tính chất phi truyền thống của các nguy cơ này, pháp luật an ninh mạng kiến tạo một

khuôn khổ pháp lý vững chắc để Nhà nước thực thi quyền tài phán trên không gian số. Thông qua việc luật hóa các hành vi xâm phạm ANQG, pháp luật trao cho các lực lượng chuyên trách những công cụ pháp lý sắc bén nhằm chủ động nhận diện, phòng ngừa và đập tan mọi âm mưu phá hoại. Đồng thời, hệ thống pháp luật này thiết lập các tiêu chuẩn an toàn bắt buộc đối với các hệ thống thông tin quan trọng về ANQG, biến các yêu cầu kỹ thuật thành các nghĩa vụ pháp lý phải tuân thủ nghiêm ngặt, qua đó duy trì trật tự pháp lý và sự ổn định của xã hội trên không gian mạng.

*Thứ hai*, pháp luật về an ninh mạng là công cụ hữu hiệu để bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân trong môi trường số. Cùng với quá trình số hóa toàn diện, các quyền nhân thân và quyền tài sản của công dân ngày càng dễ bị tổn thương trước các hành vi đánh cắp dữ liệu, lừa đảo trực tuyến hay xâm phạm quyền riêng tư. Pháp luật an ninh mạng giải quyết vấn đề này bằng cách thiết lập một hành lang bảo vệ đa lớp. Một mặt, pháp luật quy định các chế tài nghiêm khắc đối với tội phạm mạng, tạo ra tính răn đe cần thiết để ngăn ngừa các hành vi xâm hại. Mặt khác, hệ thống pháp luật này ràng buộc chặt chẽ trách nhiệm pháp lý của các doanh nghiệp cung cấp dịch vụ số, buộc họ phải áp dụng các biện pháp bảo mật từ khâu thiết kế để bảo vệ dữ liệu người dùng. Đặc biệt, dưới góc nhìn của nhà nước pháp quyền, pháp luật an ninh mạng còn đóng vai trò như một cơ chế “tự giới hạn quyền lực” của Nhà nước. Bằng cách minh định rõ căn cứ, thẩm quyền và trình tự áp dụng các biện pháp kỹ thuật, nghiệp vụ, pháp luật ngăn chặn nguy cơ các cơ quan thực thi pháp luật lạm quyền, xâm phạm trái phép đến bí mật đời tư, tự do biểu đạt và quyền tự do kinh doanh của cá nhân, tổ chức.

*Thứ ba*, pháp luật về an ninh mạng tạo lập nền tảng pháp lý vững chắc cho hoạt động quản trị rủi ro công nghệ. Rủi ro công nghệ trong kỷ nguyên số không còn là rủi ro mang tính kỹ thuật đơn thuần mà đã chuyển hóa thành rủi ro an ninh và rủi ro pháp lý. Thay vì tiếp cận theo mô hình trừng phạt thụ động truyền thống, pháp luật an ninh mạng thể chế hóa tư duy quản trị rủi ro

chủ động từ sớm, từ xa. Vai trò này được hiện thực hóa thông qua việc pháp luật quy định các cơ chế đánh giá, phân loại hệ thống thông tin, thiết lập cảnh báo sớm và quy trình ứng phó, phục hồi sau sự cố. Hơn thế nữa, pháp luật thực hiện chức năng phân bổ trách nhiệm quản trị rủi ro một cách tương xứng giữa các chủ thể, bảo đảm sự cân bằng giữa yêu cầu kiểm soát an ninh nghiêm ngặt và mục tiêu không tạo ra rào cản hành chính cản trở sự đổi mới sáng tạo và năng lực cạnh tranh của doanh nghiệp.

*Thứ tư*, pháp luật về an ninh mạng cung cấp bộ công cụ pháp lý cho một tiến trình chuyển đổi số an toàn, minh bạch và bền vững. Mục tiêu cốt lõi của chiến lược phát triển Chính phủ số, kinh tế số và xã hội số chỉ có thể đạt được khi toàn xã hội có đủ “niềm tin số” vào môi trường mạng. Niềm tin này không thể tự nảy sinh mà phải được kiến tạo và bảo đảm bằng sức mạnh cưỡng chế của pháp luật. Bằng cách thiết lập các quy tắc ứng xử minh bạch, bảo vệ sự toàn vẹn của dữ liệu và định hình rõ giới hạn quyền - nghĩa vụ của các bên tham gia, pháp luật an ninh mạng loại trừ các lực cản phát sinh từ tội phạm mạng, rò rỉ thông tin và sự phụ thuộc công nghệ. Thông qua đó, pháp luật an ninh mạng không chỉ thực hiện chức năng bảo vệ (tiêu cực) mà còn thực hiện chức năng kiến tạo (tích cực), đóng góp trực tiếp vào việc nâng cao hiệu lực, hiệu quả quản lý nhà nước và phát triển kinh tế - xã hội.

#### **2.2.4. Cấu trúc lý luận của pháp luật về an ninh mạng**

Dưới góc độ khoa học lý luận về nhà nước và pháp luật, pháp luật về an ninh mạng không phải là sự lắp ghép cơ học của các quy định rời rạc, mà là một hệ thống được cấu trúc bởi sáu nhóm chế định cơ bản. Các chế định này có mối quan hệ biện chứng, tác động qua lại và bổ trợ lẫn nhau, tạo thành một chỉnh thể điều chỉnh thống nhất nhằm bảo đảm trật tự pháp lý trên không gian mạng.

Sáu nhóm chế định này bao gồm: nhóm quy định về nguyên tắc bảo vệ an ninh mạng; nhóm quy định về hành vi vi phạm pháp luật về an ninh mạng; nhóm quy định về chế tài xử lý hành vi vi phạm; nhóm quy định về địa

vị pháp lý của các chủ thể; nhóm quy định về biện pháp bảo vệ an ninh mạng; nhóm quy định về hợp tác quốc tế trong lĩnh vực an ninh mạng. Đây là cấu trúc lý luận để nhận diện nội dung của pháp luật về an ninh mạng, đồng thời là cơ sở để đánh giá thực trạng và đề xuất giải pháp hoàn thiện pháp luật trong các phần tiếp theo của luận án.

### ***- Nhóm quy định về nguyên tắc bảo vệ an ninh mạng***

Trong cấu trúc lý luận của hệ thống pháp luật, nguyên tắc đóng vai trò là những tư tưởng chỉ đạo, mang tính xuất phát điểm và chi phối toàn bộ quá trình lập pháp cũng như thực thi pháp luật. Cơ sở khoa học của chế định này được định hình từ sự giao thoa biện chứng giữa lý thuyết nhà nước pháp quyền và lý thuyết an ninh mở rộng. Theo đó, khi an ninh mạng được nhận diện là một bộ phận cấu thành của ANQG phi truyền thống, Nhà nước tất yếu phải thiết lập các nguyên tắc mang tính chiến lược để quản trị không gian số. Tuy nhiên, để ngăn chặn xu hướng lạm dụng quyền lực công dưới danh nghĩa “an ninh hóa”, nhóm chế định này xác lập những giới hạn pháp lý rõ ràng thông qua việc hiến định các nguyên tắc về tôn trọng quyền con người, nguyên tắc bảo vệ tương xứng và trách nhiệm giải trình. Sự tồn tại mang tính hệ thống của chế định nguyên tắc bảo đảm cho toàn bộ cấu trúc pháp luật an ninh mạng vận hành đúng quỹ đạo, duy trì sự cân bằng động giữa yêu cầu bảo vệ chủ quyền số và việc bảo đảm các quyền tự do cơ bản của công dân.

### ***- Nhóm quy định về hành vi vi phạm pháp luật về an ninh mạng***

Theo lý luận chung, việc xác định hành vi vi phạm là hoạt động định hình ranh giới giữa vùng hành vi hợp pháp và hành vi bị cấm, phản ánh tính nguy hiểm cho xã hội của các hành vi xâm hại quan hệ xã hội được pháp luật bảo vệ. Do sự biến đổi liên tục của các rủi ro công nghệ trong xã hội số, chế định này đòi hỏi một kỹ thuật lập pháp đặc thù: kết hợp giữa mô hình liệt kê hành vi điển hình với hệ thống tiêu chí nhận diện mở. Kỹ thuật này giúp pháp luật bao quát trọn vẹn cả hai nhóm hành vi cơ bản: nhóm tấn công trực tiếp vào cấu trúc kỹ thuật của hệ thống thông tin (như phát tán mã độc) và nhóm lợi dụng

không gian mạng làm công cụ để xâm hại các lợi ích truyền thống (như lừa đảo tài chính, thao túng dư luận). Thước đo tính khoa học của chế định này nằm ở khả năng thích ứng cao, bảo đảm pháp luật không bị vô hiệu hóa trước sự trỗi dậy của các công nghệ đột phá như trí tuệ nhân tạo (AI) hay công nghệ giả mạo sâu (deepfake).

***- Nhóm quy định về chế tài xử lý hành vi vi phạm***

Chế tài là thuộc tính bản chất bảo đảm tính nghiêm minh và hiệu lực bắt buộc chung của QPPL thông qua sức mạnh cưỡng chế nhà nước. Cơ sở khoa học của chế định này dựa trên nguyên tắc tương xứng và tính phân tầng trách nhiệm pháp lý. Do tồn tại trên không gian mạng mang tính phi vật lý và có quy mô thiệt hại khó định lượng (như suy giảm niềm tin số hay mất mát dữ liệu), chế tài an ninh mạng được thiết kế thành một hệ thống đồng bộ. Hệ thống này tích hợp linh hoạt giữa chế tài hình sự đối với các hành vi nguy hiểm cao độ, chế tài hành chính để xử lý nhanh các vi phạm nghĩa vụ quản trị và trách nhiệm dân sự nhằm khôi phục lợi ích cho chủ thể bị xâm hại. Đặc biệt, tính khoa học của chế định này còn thể hiện ở việc ứng dụng các chế tài kỹ thuật đặc thù như phong tỏa dòng tiền ảo, cưỡng chế xóa dữ liệu thu thập bất hợp pháp hay đình chỉ quyền vận hành hệ thống, qua đó ngăn chặn sự lan truyền rủi ro dây chuyền trong cấu trúc kinh tế - xã hội.

***- Nhóm quy định về địa vị pháp lý của các chủ thể***

Mọi quá trình điều chỉnh pháp luật chỉ thực sự phát huy hiệu quả khi quyền, nghĩa vụ và trách nhiệm của các bên tham gia được phân định tường minh. Không gian mạng là một thực thể vận hành chủ yếu dựa trên hạ tầng kỹ thuật do các tập đoàn công nghệ tư nhân quản lý, do đó, cơ sở khoa học của chế định này dựa trên lý thuyết đa chủ thể trong quản trị rủi ro. Pháp luật an ninh mạng bác bỏ mô hình quản lý đơn chủ thể từ trên xuống, thay vào đó thiết lập một bản đồ phân bổ trách nhiệm xã hội tương xứng với rủi ro hệ thống. Chế định này phân định rõ giới hạn quyền lực của lực lượng chuyên trách (vai trò nòng cốt), xác lập nghĩa vụ đồng quản lý rủi ro của doanh

nghiệp cung cấp dịch vụ số (chủ quản hạ tầng) và bảo vệ quyền tự quyết dữ liệu của người sử dụng. Việc pháp điển hóa địa vị pháp lý theo hướng này giúp tối ưu hóa nguồn lực, chuyển hóa trách nhiệm bảo vệ an ninh mạng thành nghĩa vụ phối hợp liên kết mang tính toàn dân.

***- Nhóm quy định về biện pháp bảo vệ an ninh mạng***

Dưới góc độ lý luận, biện pháp pháp lý là công cụ thực tế để hiện thực hóa quyền lực nhà nước nhằm phòng ngừa rủi ro và khôi phục trật tự bị xâm hại. Chế định này được xây dựng trên nền tảng lý luận về kiến trúc kỹ thuật (“Code is Law”) kết hợp với lý thuyết quản trị rủi ro chủ động. Theo đó, pháp luật an ninh mạng không chỉ dựa vào các mệnh lệnh cấm đoán hành chính mà còn chuyển hóa các nghĩa vụ pháp lý thành các tiêu chuẩn kỹ thuật bắt buộc (như mã hóa, kiểm soát truy cập, định danh điện tử). Đồng thời, do việc áp dụng các biện pháp can thiệp kỹ thuật (chặn lọc thông tin, thu thập dữ liệu) luôn tiềm ẩn nguy cơ xâm phạm quyền riêng tư và tự do kinh doanh, tính khoa học của chế định này đòi hỏi một quy trình kiểm soát quyền lực nghiêm ngặt. Pháp luật phải xác định minh bạch căn cứ, điều kiện áp dụng, giới hạn thẩm quyền, thời hạn thực hiện và trách nhiệm giải trình của cơ quan áp dụng biện pháp can thiệp.

***- Nhóm quy định về hợp tác quốc tế trong lĩnh vực an ninh mạng***

Trong khoa học pháp lý, hợp tác quốc tế là công cụ then chốt để giải quyết xung đột tài phán và mở rộng không gian thực thi pháp luật trong bối cảnh toàn cầu hóa. không gian mạng mang bản chất phi lãnh thổ, nơi một hành vi vi phạm có thể liên quan đồng thời đến nhiều quốc gia thông qua các chuỗi trung chuyển dữ liệu phức tạp. Cơ sở khoa học của chế định này được xây dựng trên lý thuyết chủ quyền số kết hợp và sự tương thích lập pháp quốc tế. Chế định này tạo hành lang pháp lý để nội luật hóa các chuẩn mực chung của luật quốc tế, thiết lập cơ sở vững chắc cho hoạt động tương trợ tư pháp, thu thập chứng cứ điện tử xuyên biên giới, dẫn độ tội phạm và điều phối ứng cứu sự cố khẩn cấp. Đây là cầu nối pháp lý giúp Nhà nước vừa bảo vệ vững chắc chủ

quyền số quốc gia, vừa nâng cao năng lực chủ động hội nhập vào cơ chế quản trị an ninh toàn cầu.

Tóm lại, sáu nhóm chế định nêu trên tạo thành cấu trúc lý luận cơ bản của pháp luật về an ninh mạng. Các nhóm chế định này có mối quan hệ chặt chẽ, bổ sung cho nhau và cùng hướng tới mục tiêu bảo vệ ANQG, TTATXH, hệ thống thông tin, dữ liệu, quyền và lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng. Đây cũng là cơ sở để Chương 3 của luận án đánh giá thực trạng pháp luật về an ninh mạng ở Việt Nam và Chương 4 đề xuất các giải pháp hoàn thiện pháp luật tương ứng với từng nhóm chế định.

## **2.3. KHÁI NIỆM VÀ CÁC TIÊU CHÍ HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM**

### **2.3.1. Khái niệm hoàn thiện pháp luật về an ninh mạng**

Trong bối cảnh chuyển đổi số quốc gia diễn ra mạnh mẽ, không gian mạng đã trở thành môi trường quan trọng đối với hoạt động quản lý nhà nước, phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh và thực hiện các quyền, lợi ích hợp pháp của cá nhân, tổ chức. Các hoạt động của Nhà nước, doanh nghiệp và người dân ngày càng phụ thuộc vào hệ thống thông tin, cơ sở dữ liệu, nền tảng số, dịch vụ trực tuyến và hạ tầng kết nối. Sự phụ thuộc đó làm cho an ninh mạng không còn là vấn đề kỹ thuật thuần túy, mà trở thành vấn đề pháp lý, quản trị và ANQG. Vì vậy, pháp luật về an ninh mạng giữ vai trò là công cụ quan trọng để Nhà nước điều chỉnh các quan hệ xã hội phát sinh trên không gian mạng, phòng ngừa, phát hiện, ngăn chặn, xử lý các nguy cơ, hành vi xâm phạm an ninh mạng, đồng thời bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Tuy nhiên, thực tiễn cũng cho thấy các nguy cơ, thách thức trên không gian mạng luôn biến đổi nhanh chóng, phức tạp và khó dự báo. Các hành vi như tấn công mạng, gián điệp mạng, lộ, mất dữ liệu, xâm phạm bí mật nhà nước, lừa đảo trực tuyến, sử dụng công nghệ cao để phạm tội, phát tán thông tin sai sự thật, giả mạo danh tính, xâm phạm dữ liệu cá nhân, lợi dụng tài sản

số hoặc nền tảng xuyên biên giới để thực hiện hành vi vi phạm pháp luật đang đặt ra nhiều vấn đề mới cho hoạt động lập pháp và thực thi pháp luật. Trong khi đó, pháp luật luôn có độ trễ nhất định so với sự phát triển của công nghệ và thực tiễn xã hội. Chính vì vậy, hoàn thiện pháp luật về an ninh mạng là yêu cầu khách quan, thường xuyên và lâu dài, không chỉ nhằm khắc phục những bất cập hiện có, mà còn nhằm tạo lập khả năng thích ứng của pháp luật trước các rủi ro mới trong tương lai.

Hoàn thiện pháp luật nói chung là quá trình Nhà nước xây dựng mới, sửa đổi, bổ sung, thay thế hoặc bãi bỏ các quy định pháp luật, đồng thời hoàn thiện cơ chế tổ chức thực hiện pháp luật, qua đó bảo đảm hệ thống pháp luật ngày càng đầy đủ, đồng bộ, thống nhất, minh bạch, khả thi và phù hợp với yêu cầu điều chỉnh các quan hệ xã hội trong từng giai đoạn phát triển của đất nước. Do đó, hoàn thiện pháp luật về an ninh mạng trước hết cần được hiểu là quá trình rà soát, đánh giá, sửa đổi, bổ sung, bãi bỏ hoặc ban hành mới các QPPL nhằm bảo đảm cho hệ thống pháp luật về an ninh mạng ngày càng đầy đủ, đồng bộ, thống nhất, minh bạch, khả thi và phù hợp với thực tiễn phát triển của không gian mạng. Quá trình này không chỉ hướng tới việc “có thêm” quy định pháp luật, mà quan trọng hơn là làm cho các quy định pháp luật hiện hành vận hành hiệu quả hơn, khắc phục được khoảng trống, mâu thuẫn, chồng chéo, bất cập trong nội dung điều chỉnh và cơ chế thực thi.

Cần nhấn mạnh rằng, hoàn thiện pháp luật về an ninh mạng không đồng nhất với việc ban hành một đạo luật mới hoặc sửa đổi một văn bản pháp luật riêng lẻ. Pháp luật về an ninh mạng là một lĩnh vực có tính liên ngành, liên quan đến nhiều nhóm quy phạm thuộc pháp luật về ANQG, công nghệ thông tin, viễn thông, giao dịch điện tử, dữ liệu, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước, xử lý vi phạm hành chính, hình sự, tổ tụng hình sự và hợp tác quốc tế. Do đó, hoàn thiện pháp luật về an ninh mạng phải được tiếp cận như quá trình hoàn thiện tổng thể một hệ thống pháp luật, trong đó các quy phạm phải được liên kết với nhau một cách thống nhất, tránh tình trạng mỗi lĩnh vực điều chỉnh một phần nhưng thiếu cơ chế phối hợp chung.

Từ góc độ nội dung, hoàn thiện pháp luật về an ninh mạng bao gồm việc hoàn thiện các nhóm quy định cơ bản về nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý hành vi vi phạm; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế trong lĩnh vực an ninh mạng. Các nhóm quy định này có mối quan hệ chặt chẽ với nhau. Nguyên tắc bảo vệ an ninh mạng định hướng cho toàn bộ hệ thống pháp luật; quy định về hành vi vi phạm xác định ranh giới giữa hành vi hợp pháp và hành vi bị cấm; chế tài xử lý bảo đảm tính răn đe và khắc phục hậu quả; địa vị pháp lý của các chủ thể xác định quyền, nghĩa vụ, thẩm quyền và trách nhiệm; biện pháp bảo vệ an ninh mạng tạo công cụ phòng ngừa, phát hiện, ngăn chặn, xử lý nguy cơ; còn hợp tác quốc tế là điều kiện bảo đảm hiệu quả thực thi trong bối cảnh không gian mạng có tính xuyên biên giới.

Từ góc độ bảo đảm thực thi, hoàn thiện pháp luật về an ninh mạng không chỉ là hoàn thiện hệ thống văn bản QPPL, mà còn bao gồm hoàn thiện thiết chế, cơ chế phối hợp, nguồn nhân lực, cơ sở vật chất, hạ tầng kỹ thuật, tiêu chuẩn, quy chuẩn kỹ thuật và cơ chế kiểm soát việc áp dụng pháp luật. Một quy định pháp luật dù được xây dựng chặt chẽ về mặt câu chữ vẫn khó phát huy hiệu quả nếu thiếu cơ quan thực thi đủ năng lực, thiếu quy trình phối hợp rõ ràng, thiếu công cụ kỹ thuật, thiếu cơ chế giám sát và thiếu trách nhiệm giải trình. Vì vậy, hoàn thiện pháp luật trong lĩnh vực này phải gắn kết chặt chẽ giữa xây dựng pháp luật và tổ chức thi hành pháp luật.

Từ góc độ phương thức, hoàn thiện pháp luật về an ninh mạng phải được đặt trong toàn bộ quy trình chính sách pháp luật, bao gồm nhận diện vấn đề, đánh giá nguyên nhân, phân tích tác động chính sách, lựa chọn phương án điều chỉnh, thể chế hóa thành QPPL, tổ chức thi hành, kiểm tra, giám sát và tổng kết thực tiễn. Điều đó có nghĩa là việc hoàn thiện pháp luật không kết thúc tại thời điểm văn bản được ban hành. Ngược lại, sau khi văn bản có hiệu lực, pháp luật cần tiếp tục được theo dõi, đánh giá, kiểm nghiệm trong thực tiễn để kịp thời phát hiện những điểm chưa phù hợp, từ đó tiếp tục sửa đổi, bổ sung hoặc hướng dẫn thi hành.

Một yêu cầu quan trọng của hoàn thiện pháp luật về an ninh mạng là bảo đảm sự cân bằng giữa bảo vệ ANQG, TTATXH với bảo vệ quyền con người, quyền công dân, quyền và lợi ích hợp pháp của cá nhân, tổ chức. Các biện pháp bảo vệ an ninh mạng như kiểm tra, giám sát, thu thập dữ liệu điện tử, yêu cầu cung cấp thông tin, gỡ bỏ hoặc ngăn chặn thông tin, đình chỉ dịch vụ, hạn chế hoạt động của hệ thống thông tin có thể cần thiết để bảo vệ ANQG và TTATXH, nhưng đồng thời cũng có thể tác động đến quyền riêng tư, dữ liệu cá nhân, quyền tiếp cận thông tin và quyền tự do kinh doanh hợp pháp. Vì vậy, hoàn thiện pháp luật về an ninh mạng phải làm rõ căn cứ áp dụng, thẩm quyền, điều kiện, trình tự, thủ tục, giới hạn, thời hạn và cơ chế kiểm soát đối với các biện pháp này.

Bên cạnh đó, hoàn thiện pháp luật về an ninh mạng phải bảo đảm khả năng thích ứng với sự phát triển của công nghệ. Đây là yêu cầu đặc thù của lĩnh vực này. Nếu pháp luật chỉ liệt kê cứng các hành vi, công nghệ hoặc phương thức tấn công cụ thể, pháp luật sẽ nhanh chóng lạc hậu. Ngược lại, nếu pháp luật quy định quá chung, thiếu tiêu chí nhận diện, sẽ gây khó khăn cho áp dụng và có thể làm phát sinh nguy cơ tùy tiện. Do đó, pháp luật về an ninh mạng cần kết hợp giữa quy định nguyên tắc, tiêu chí nhận diện mở, danh mục hành vi điển hình, tiêu chuẩn kỹ thuật cập nhật và cơ chế hướng dẫn thi hành linh hoạt. Cách thiết kế này giúp pháp luật vừa ổn định, vừa đủ linh hoạt để điều chỉnh các vấn đề mới như trí tuệ nhân tạo, dữ liệu lớn, deepfake, tài sản số, điện toán đám mây, Internet vạn vật và nền tảng số xuyên biên giới.

Trong điều kiện hội nhập quốc tế, hoàn thiện pháp luật về an ninh mạng cũng phải bảo đảm sự tương thích cần thiết với điều ước quốc tế mà Việt Nam là thành viên, đồng thời tiếp thu có chọn lọc kinh nghiệm của các quốc gia, khu vực và tổ chức quốc tế. Tuy nhiên, việc tiếp thu kinh nghiệm nước ngoài không có nghĩa là sao chép mô hình pháp luật của quốc gia khác, mà phải đặt trong điều kiện chính trị, pháp lý, kinh tế, xã hội, năng lực công nghệ và yêu cầu bảo vệ ANQG của Việt Nam. Đây là yêu cầu quan trọng để

bảo đảm pháp luật về an ninh mạng vừa phù hợp với thông lệ quốc tế, vừa giữ vững chủ quyền, lợi ích quốc gia và bản sắc pháp lý của Việt Nam.

Từ những phân tích trên, có thể hiểu: *Hoàn thiện pháp luật về an ninh mạng là quá trình rà soát, đánh giá, sửa đổi, bổ sung, bãi bỏ hoặc ban hành mới các QPPL về an ninh mạng, đồng thời củng cố cơ chế thực thi, thiết chế bảo đảm, nguồn lực, tiêu chuẩn kỹ thuật, cơ chế phối hợp và cơ chế kiểm soát việc áp dụng pháp luật, nhằm xây dựng hệ thống pháp luật đầy đủ, đồng bộ, minh bạch, khả thi, thích ứng với sự phát triển của công nghệ, bảo đảm hiệu quả bảo vệ ANQG, TTATXH, đồng thời bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng.*

Như vậy, hoàn thiện pháp luật về an ninh mạng là quá trình hoàn thiện tổng thể cả nội dung quy phạm, phương thức tổ chức thực hiện và các điều kiện bảo đảm thi hành pháp luật. Quá trình này vừa mang tính lập pháp, vừa mang tính tổ chức thực thi; vừa hướng tới bảo vệ ANQG, TTATXH, vừa hướng tới bảo vệ quyền con người, quyền công dân; vừa đòi hỏi sự ổn định của pháp luật, vừa đòi hỏi khả năng thích ứng với công nghệ mới. Đây là cơ sở lý luận quan trọng để xác lập các tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng ở Việt Nam trong các nội dung tiếp theo của luận án.

### **2.3.2. Các tiêu chí đánh giá sự hoàn thiện pháp luật về an ninh mạng**

Từ nghiên cứu lý luận và thực tiễn, có thể khẳng định rằng việc đánh giá mức độ hoàn thiện của pháp luật nói chung và pháp luật về an ninh mạng nói riêng phải dựa trên hệ tiêu chí nhất định. Kế thừa các quan điểm khoa học về tiêu chí hoàn thiện pháp luật, đặc biệt là các tiêu chí về tính toàn diện, tính đồng bộ, tính phù hợp và trình độ kỹ thuật pháp lý của hệ thống pháp luật, luận án cho rằng việc đánh giá pháp luật về an ninh mạng cần vừa bảo đảm yêu cầu chung của hệ thống pháp luật, vừa phù hợp với tinh thần Nghị quyết số 27-NQ/TW, Nghị quyết số 66-NQ/TW và đặc thù của lĩnh vực an ninh mạng. Đây là lĩnh vực có tính liên ngành, kỹ thuật cao, xuyên biên giới, gắn với quản trị rủi ro và luôn đặt ra yêu cầu hài hòa giữa bảo vệ ANQG,

TTATXH với bảo vệ quyền con người, quyền công dân trên không gian mạng. Vì vậy, tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng cần được cụ thể hóa thành hệ tiêu chí chuyên biệt, trên cơ sở kế thừa lý luận chung về hoàn thiện pháp luật và phản ánh đúng yêu cầu bảo vệ an ninh mạng trong bối cảnh chuyển đổi số.

### ***2.3.2.1. Nhóm tiêu chí về nội dung pháp luật***

#### ***- Tiêu chí về tính đầy đủ***

Tính đầy đủ là tiêu chí nội dung cơ bản để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh mức độ pháp luật bao quát các quan hệ xã hội cơ bản, phổ biến và cần thiết phát sinh trong quá trình bảo vệ an ninh mạng. Theo đó, pháp luật về an ninh mạng được coi là đầy đủ khi đã thiết lập được hệ thống quy phạm điều chỉnh tương đối toàn diện các nhóm vấn đề cốt lõi, bao gồm: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý vi phạm; địa vị pháp lý, quyền và nghĩa vụ của các chủ thể; biện pháp bảo vệ an ninh mạng; cơ chế tổ chức thực thi và hợp tác quốc tế trong lĩnh vực an ninh mạng.

Việc xem xét tiêu chí này được thực hiện thông qua các biểu hiện chủ yếu như: sự hiện diện của các quy định điều chỉnh trực tiếp từng nhóm vấn đề cơ bản của pháp luật về an ninh mạng; mức độ bao quát đối với các nguy cơ, rủi ro và hành vi xâm phạm phổ biến trên không gian mạng; sự xác định rõ ràng về chủ thể, thẩm quyền, trách nhiệm, biện pháp áp dụng và hậu quả pháp lý tương ứng. Đồng thời, cần xem xét khả năng của pháp luật trong việc điều chỉnh các vấn đề mới phát sinh từ chuyển đổi số, dữ liệu lớn, trí tuệ nhân tạo và các nền tảng số xuyên biên giới. Như vậy, tính đầy đủ không chỉ được phản ánh ở số lượng quy định hiện có mà còn ở khả năng bao quát và điều chỉnh các vấn đề trọng yếu thuộc phạm vi bảo vệ an ninh mạng.

Cơ sở để đánh giá tiêu chí này bao gồm hệ thống văn bản QPPL hiện hành, các văn bản hướng dẫn thi hành, báo cáo tổng kết thực tiễn thi hành pháp luật, số liệu về xử lý vi phạm, các vụ việc điển hình, cùng với ý kiến của

chuyên gia, nhà quản lý và các chủ thể có liên quan trong quá trình khảo sát, nghiên cứu.

Trên cơ sở đó, mức độ đáp ứng tiêu chí tính đầy đủ có thể được xem xét theo ba mức độ. Pháp luật được đánh giá là đầy đủ khi các nhóm chế định cơ bản đều đã được điều chỉnh tương đối toàn diện và có khả năng bao quát các nguy cơ, hành vi xâm phạm chủ yếu trên không gian mạng. Pháp luật được đánh giá là tương đối đầy đủ khi phần lớn các nội dung cốt lõi đã được điều chỉnh nhưng vẫn còn một số khoảng trống hoặc những quy định chưa theo kịp yêu cầu thực tiễn. Pháp luật được đánh giá là chưa đầy đủ khi còn thiếu các quy định điều chỉnh những vấn đề trọng yếu hoặc chưa xác lập được cơ chế pháp lý cần thiết để phòng ngừa, phát hiện và xử lý các hành vi xâm phạm an ninh mạng.

Tuy nhiên, tính đầy đủ không đồng nghĩa với việc pháp luật phải điều chỉnh toàn bộ các vấn đề phát sinh trên không gian mạng. Việc đánh giá cần tập trung vào những quan hệ xã hội có liên quan trực tiếp đến bảo vệ ANQG, TTATXH, hệ thống thông tin, dữ liệu và quyền, lợi ích hợp pháp của cá nhân, tổ chức trước các nguy cơ, hành vi xâm phạm trên không gian mạng. Cách tiếp cận này vừa bảo đảm tính khoa học của tiêu chí đánh giá, vừa phù hợp với phạm vi điều chỉnh và mục tiêu của pháp luật về an ninh mạng.

#### *- Tiêu chí về tính đồng bộ*

Tính đồng bộ là tiêu chí quan trọng để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh mức độ thống nhất, hài hòa và liên kết giữa các quy định trong hệ thống pháp luật về an ninh mạng, cũng như sự tương thích giữa pháp luật về an ninh mạng với các lĩnh vực pháp luật có liên quan. Một hệ thống pháp luật về an ninh mạng được coi là đồng bộ khi các quy định được thiết kế theo một chỉnh thể thống nhất, không mâu thuẫn, không chồng chéo, không trùng lặp không cần thiết và không tạo ra khoảng trống pháp lý trong điều chỉnh các quan hệ xã hội phát sinh trên không gian mạng.

Việc đánh giá tiêu chí này được thực hiện thông qua một số biểu hiện chủ yếu. Trước hết là sự thống nhất nội tại giữa các nhóm chế định cơ bản của

pháp luật về an ninh mạng, bao gồm nguyên tắc bảo vệ an ninh mạng, hành vi vi phạm, chế tài xử lý, quyền và nghĩa vụ của các chủ thể, biện pháp bảo vệ an ninh mạng và cơ chế tổ chức thực hiện. Các quy định này phải có sự liên kết logic, trong đó hành vi vi phạm phải gắn với chế tài xử lý tương ứng; quyền, nghĩa vụ của chủ thể phải gắn với trách nhiệm pháp lý; biện pháp bảo vệ an ninh mạng phải phù hợp với thẩm quyền, trình tự, thủ tục và cơ chế kiểm soát việc thực hiện.

Bên cạnh đó, tính đồng bộ còn được thể hiện ở sự thống nhất giữa pháp luật về an ninh mạng với các lĩnh vực pháp luật có liên quan như an toàn thông tin mạng, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, công nghệ thông tin, bảo vệ bí mật nhà nước, xử lý vi phạm hành chính, pháp luật hình sự, tổ tụng hình sự và hợp tác quốc tế. Việc đánh giá cần xem xét mức độ tương thích của các quy định, sự phân định rõ phạm vi điều chỉnh, thẩm quyền quản lý và cơ chế phối hợp giữa các cơ quan, tổ chức có liên quan, qua đó hạn chế tình trạng xung đột, chồng chéo hoặc áp dụng pháp luật không thống nhất.

Cơ sở để đánh giá tiêu chí này bao gồm hệ thống văn bản QPPL hiện hành về an ninh mạng và các lĩnh vực pháp luật có liên quan; các văn bản hướng dẫn thi hành; báo cáo tổng kết, rà soát, hệ thống hóa văn bản QPPL; kết quả thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo; các vụ việc thực tiễn phát sinh trong quá trình áp dụng pháp luật; cùng với ý kiến của chuyên gia, nhà quản lý và các chủ thể có liên quan.

Trên cơ sở đó, tính đồng bộ của pháp luật về an ninh mạng có thể được xem xét theo ba mức độ. Pháp luật được đánh giá là đồng bộ khi các quy định có sự thống nhất cả về nội dung, thẩm quyền, trách nhiệm và cơ chế thực hiện, đồng thời bảo đảm sự tương thích với các lĩnh vực pháp luật liên quan. Pháp luật được đánh giá là tương đối đồng bộ khi nhìn chung đã bảo đảm sự thống nhất nhưng vẫn còn một số quy định chồng chéo, giao thoa hoặc thiếu sự liên thông trong tổ chức thực hiện. Pháp luật được đánh giá là chưa đồng bộ khi tồn tại nhiều quy định mâu thuẫn, chồng chéo hoặc thiếu cơ chế phối hợp, gây khó khăn cho việc áp dụng và thực thi pháp luật trong thực tiễn.

Trong bối cảnh an ninh mạng là lĩnh vực có tính liên ngành, liên lĩnh vực và chịu tác động mạnh mẽ của sự phát triển công nghệ, tính đồng bộ không chỉ là yêu cầu đối với từng quy phạm riêng lẻ mà còn là yêu cầu đối với toàn bộ hệ thống pháp luật. Đây là cơ sở quan trọng để bảo đảm tính thống nhất của hệ thống pháp luật, nâng cao hiệu lực, hiệu quả quản lý nhà nước và khả năng bảo vệ ANQG trên không gian mạng.

*- Tiêu chí về khả năng thích ứng với công nghệ*

Khả năng thích ứng với công nghệ là tiêu chí đặc thù để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh khả năng của pháp luật trong việc nhận diện, tiếp nhận và điều chỉnh kịp thời những vấn đề mới phát sinh từ sự phát triển nhanh chóng của khoa học, công nghệ, như trí tuệ nhân tạo, dữ liệu lớn, điện toán đám mây, Internet vạn vật, blockchain, tài sản số, định danh điện tử, nền tảng số xuyên biên giới và các phương thức tấn công mạng mới. Pháp luật về an ninh mạng chỉ có thể vận hành hiệu quả khi vừa bảo đảm tính ổn định cần thiết của QPPL, vừa có khả năng thích ứng trước các rủi ro công nghệ phát sinh trên không gian mạng.

Việc xem xét tiêu chí này có thể dựa trên một số biểu hiện chủ yếu. Trước hết là mức độ cập nhật của các quy định pháp luật đối với công nghệ, mô hình hoạt động và nguy cơ an ninh mạng mới. Tiếp đó là khả năng vận dụng các quy định hiện hành để xử lý các tình huống phát sinh trong thực tiễn mà không phải thường xuyên sửa đổi, bổ sung văn bản pháp luật. Bên cạnh đó, pháp luật cần có các quy định mang tính nguyên tắc, tiêu chí nhận diện mở, nhóm hành vi điển hình và cơ chế cập nhật tiêu chuẩn kỹ thuật thông qua văn bản dưới luật hoặc hướng dẫn chuyên ngành. Những biểu hiện này cho thấy pháp luật không chỉ phản ứng với hành vi vi phạm đã xảy ra mà còn có khả năng dự liệu, phòng ngừa và kiểm soát các rủi ro công nghệ trong tương lai.

Khả năng thích ứng với công nghệ còn được phản ánh ở việc pháp luật thiết lập được cơ chế quản trị rủi ro phù hợp với đặc điểm của môi trường số. Trong lĩnh vực an ninh mạng, nhiều nguy cơ, lỗ hổng và sự cố kỹ thuật có thể

xuất hiện trước khi hành vi vi phạm được nhận diện đầy đủ hoặc trước khi hậu quả xảy ra. Vì vậy, pháp luật cần quy định các cơ chế như đánh giá rủi ro, phân loại hệ thống thông tin, phân loại dữ liệu, cảnh báo sớm, báo cáo sự cố, kiểm tra, giám sát và khắc phục hậu quả sự cố an ninh mạng. Đồng thời, nghĩa vụ pháp lý của các chủ thể cần được thiết kế theo mức độ rủi ro của từng loại hệ thống thông tin, dữ liệu, dịch vụ số hoặc hoạt động trên không gian mạng, qua đó vừa bảo đảm hiệu quả quản lý nhà nước, vừa không tạo ra gánh nặng tuân thủ không cần thiết đối với đổi mới sáng tạo.

Cơ sở để đánh giá tiêu chí này bao gồm hệ thống văn bản QPPL hiện hành về an ninh mạng và các lĩnh vực liên quan; chiến lược, chính sách quốc gia về chuyển đổi số, an ninh mạng, an toàn thông tin mạng; báo cáo chuyên ngành của cơ quan quản lý nhà nước; số liệu, vụ việc điển hình trong thực tiễn hành pháp luật; cùng với ý kiến của chuyên gia pháp lý, chuyên gia công nghệ và các chủ thể có liên quan. Trên cơ sở đó, pháp luật có thể được đánh giá là có khả năng thích ứng tốt khi các quy định hiện hành bao quát được phần lớn rủi ro công nghệ mới, có cơ chế cập nhật linh hoạt và có khả năng áp dụng ổn định trong thực tiễn. Pháp luật được đánh giá là thích ứng ở mức tương đối khi đã điều chỉnh một số vấn đề công nghệ mới nhưng vẫn còn khoảng trống hoặc thiếu hướng dẫn cụ thể. Pháp luật được đánh giá là chưa thích ứng khi chưa có quy định phù hợp đối với các nguy cơ, mô hình công nghệ mới hoặc việc áp dụng pháp luật còn lúng túng, thiếu thống nhất.

Tuy nhiên, khả năng thích ứng với công nghệ phải được đặt trong khuôn khổ Nhà nước pháp quyền. Việc sử dụng các quy định mang tính nguyên tắc, tiêu chí nhận diện mở hoặc cơ chế cập nhật kỹ thuật linh hoạt không được dẫn đến việc mở rộng tùy tiện phạm vi điều chỉnh của pháp luật, áp dụng pháp luật thiếu thống nhất hoặc hạn chế không cần thiết quyền, lợi ích hợp pháp của cá nhân, tổ chức. Do đó, yêu cầu thích ứng với công nghệ cần được thực hiện đồng thời với yêu cầu bảo đảm tính minh bạch, tính dự báo và tính ổn định của pháp luật, qua đó tạo lập sự cân bằng giữa bảo vệ an

ninh mạng, bảo vệ quyền con người, quyền công dân và thúc đẩy phát triển kinh tế số, xã hội số trong bối cảnh chuyển đổi số hiện nay.

*- Tiêu chí về bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức*

Bảo đảm quyền và lợi ích hợp pháp của cá nhân, tổ chức là tiêu chí quan trọng để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh khả năng của pháp luật trong việc bảo đảm sự cân bằng giữa yêu cầu bảo vệ ANQG, TTATXH với việc tôn trọng, bảo vệ và bảo đảm các quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng. Trong bối cảnh chuyển đổi số, các chủ thể có thể phải đối mặt với nhiều nguy cơ như xâm phạm quyền riêng tư, dữ liệu cá nhân, danh dự, uy tín, tài sản, bí mật kinh doanh hoặc các hành vi lừa đảo, giả mạo và xâm phạm quyền, lợi ích hợp pháp khác trên không gian mạng. Vì vậy, pháp luật về an ninh mạng chỉ được coi là hoàn thiện khi thiết lập được cơ chế pháp lý phù hợp để phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi xâm phạm này.

Việc xem xét tiêu chí này có thể dựa trên một số biểu hiện chủ yếu. Trước hết là mức độ ghi nhận và bảo đảm các quyền cơ bản của cá nhân, tổ chức trên không gian mạng, như quyền về đời sống riêng tư, quyền được bảo vệ dữ liệu cá nhân, quyền bảo vệ danh dự, nhân phẩm, uy tín, tài sản, bí mật kinh doanh và các quyền, lợi ích hợp pháp khác theo quy định của pháp luật. Bên cạnh đó, pháp luật cần thiết lập các cơ chế bảo vệ quyền hiệu quả, bao gồm quyền yêu cầu chấm dứt hành vi vi phạm, yêu cầu cải chính hoặc gỡ bỏ thông tin sai sự thật, yêu cầu bảo vệ dữ liệu cá nhân, khiếu nại, tố cáo, yêu cầu bồi thường thiệt hại và yêu cầu cơ quan có thẩm quyền áp dụng các biện pháp bảo vệ cần thiết.

Tiêu chí này còn được thể hiện ở việc pháp luật xác định rõ trách nhiệm của các chủ thể có liên quan, bao gồm cơ quan nhà nước, doanh nghiệp cung cấp dịch vụ số, tổ chức quản lý dữ liệu và người sử dụng không gian mạng. Đồng thời, các biện pháp bảo vệ an ninh mạng phải được quy định trên cơ sở bảo đảm nguyên tắc cần thiết, hợp lý và tương xứng, theo đó việc hạn chế quyền chỉ được thực hiện trong những trường hợp thật sự cần thiết vì lý

do quốc phòng, ANQG, TTATXH hoặc để bảo vệ quyền, lợi ích hợp pháp của chủ thể khác theo quy định của pháp luật.

Cơ sở để đánh giá tiêu chí này bao gồm các quy định của Hiến pháp, pháp luật về an ninh mạng và các lĩnh vực có liên quan; các báo cáo tổng kết thi hành pháp luật; số liệu về khiếu nại, tố cáo, xử lý vi phạm; các vụ việc điển hình; cùng với ý kiến của chuyên gia, cơ quan quản lý nhà nước, doanh nghiệp và người sử dụng trong quá trình khảo sát, nghiên cứu.

Trên cơ sở đó, mức độ bảo đảm quyền và lợi ích hợp pháp của cá nhân, tổ chức có thể được xem xét theo ba mức độ. Pháp luật được đánh giá là bảo đảm tốt khi các quyền và cơ chế bảo vệ được quy định rõ ràng, đầy đủ, khả thi và được thực hiện hiệu quả trong thực tiễn. Pháp luật được đánh giá là bảo đảm ở mức tương đối khi các quyền và cơ chế bảo vệ cơ bản đã được ghi nhận nhưng vẫn còn những hạn chế về tính cụ thể, tính thống nhất hoặc hiệu quả thực thi. Pháp luật được đánh giá là chưa bảo đảm khi còn thiếu các quy định cần thiết hoặc thiếu cơ chế bảo vệ hữu hiệu, dẫn đến khó khăn trong việc thực hiện và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng.

Tiêu chí này cho thấy mục tiêu của việc hoàn thiện pháp luật về an ninh mạng không chỉ nhằm tăng cường hiệu quả bảo vệ ANQG mà còn hướng tới bảo đảm quyền con người, quyền công dân và quyền, lợi ích hợp pháp của các chủ thể trong môi trường số, qua đó tạo lập sự cân bằng giữa yêu cầu bảo đảm an ninh và yêu cầu phát triển.

#### ***2.3.2.2. Nhóm tiêu chí về tiêu chí về kỹ thuật pháp lý***

##### ***- Tiêu chí về tính minh bạch***

Tính minh bạch là tiêu chí quan trọng để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh mức độ rõ ràng, chính xác, dễ tiếp cận và khả năng dự báo của các quy định pháp luật, qua đó giúp các chủ thể hiểu và thực hiện đúng quyền, nghĩa vụ của mình, đồng thời bảo đảm việc áp dụng pháp luật được thống nhất, khách quan và hạn chế sự tùy

nghi trong thực thi. Trong lĩnh vực an ninh mạng, tính minh bạch có ý nghĩa đặc biệt quan trọng bởi nhiều biện pháp quản lý nhà nước có thể tác động trực tiếp đến quyền con người, quyền công dân, quyền và lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng.

Việc xem xét tiêu chí này có thể dựa trên một số biểu hiện chủ yếu. Trước hết là mức độ rõ ràng, chính xác và thống nhất của ngôn ngữ pháp lý, đặc biệt đối với các khái niệm, thuật ngữ chuyên ngành, hành vi vi phạm, điều kiện áp dụng biện pháp bảo vệ an ninh mạng và chế tài xử lý vi phạm. Bên cạnh đó, tính minh bạch còn được thể hiện ở việc pháp luật xác định cụ thể quyền, nghĩa vụ, trách nhiệm của các chủ thể; thẩm quyền của cơ quan nhà nước; trình tự, thủ tục thực hiện; cũng như điều kiện, phạm vi và giới hạn áp dụng các biện pháp can thiệp. Một hệ thống pháp luật minh bạch phải cho phép các chủ thể nhận biết được hành vi nào được thực hiện, hành vi nào bị cấm, hậu quả pháp lý có thể phát sinh và cơ chế bảo vệ quyền khi bị xâm phạm.

Ngoài ra, tính minh bạch còn được phản ánh thông qua khả năng tiếp cận và áp dụng pháp luật trong thực tiễn, bao gồm tính dễ tra cứu của văn bản QPPL, tính thống nhất giữa các văn bản có liên quan, mức độ đầy đủ của các văn bản hướng dẫn thi hành và khả năng hiểu, vận dụng thống nhất của các cơ quan, tổ chức, cá nhân.

Cơ sở để đánh giá tiêu chí này bao gồm hệ thống văn bản QPPL về an ninh mạng và các lĩnh vực liên quan; các văn bản hướng dẫn thi hành; báo cáo tổng kết thi hành pháp luật; kết quả rà soát, hệ thống hóa văn bản; các vụ việc thực tiễn phát sinh trong quá trình áp dụng pháp luật; cùng với ý kiến của chuyên gia, cơ quan quản lý nhà nước, doanh nghiệp và người sử dụng không gian mạng.

Trên cơ sở đó, mức độ minh bạch của pháp luật về an ninh mạng có thể được xem xét theo ba mức độ. Pháp luật được đánh giá là minh bạch cao khi các quy định được diễn đạt rõ ràng, thống nhất, dễ hiểu, dễ áp dụng; quyền, nghĩa vụ, trách nhiệm, thẩm quyền và trình tự thực hiện được xác định

cụ thể. Pháp luật được đánh giá là minh bạch ở mức tương đối khi phần lớn các quy định đã rõ ràng nhưng vẫn còn một số nội dung chưa thống nhất hoặc cần được hướng dẫn chi tiết hơn. Pháp luật được đánh giá là thiếu minh bạch khi tồn tại các quy định mơ hồ, khó hiểu, chồng chéo hoặc thiếu căn cứ xác định trách nhiệm, thẩm quyền và cách thức áp dụng trong thực tiễn.

Tiêu chí này góp phần bảo đảm tính công khai, khả năng dự báo và tính khả thi của pháp luật về an ninh mạng, qua đó nâng cao hiệu quả thực thi pháp luật, đồng thời bảo vệ tốt hơn quyền và lợi ích hợp pháp của các chủ thể trong môi trường số.

*- Tiêu chí về kỹ thuật lập pháp*

Kỹ thuật lập pháp là tiêu chí quan trọng để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh chất lượng cấu trúc, logic nội dung, cách diễn đạt và mức độ chính xác của các QPPL, qua đó bảo đảm pháp luật được xây dựng chặt chẽ, thống nhất, dễ hiểu, dễ áp dụng và phù hợp với đặc thù của môi trường số. Trong lĩnh vực an ninh mạng, kỹ thuật lập pháp có ý nghĩa đặc biệt quan trọng vì nhiều quy định vừa mang tính pháp lý, vừa gắn với yếu tố kỹ thuật, công nghệ và các phương thức vi phạm luôn biến đổi.

Việc xem xét tiêu chí này có thể dựa trên một số biểu hiện chủ yếu. Trước hết là sự rõ ràng và hợp lý trong cấu trúc của văn bản, điều khoản và QPPL. Mỗi quy định cần xác định tương đối đầy đủ chủ thể áp dụng, chủ thể chịu sự điều chỉnh, quyền và nghĩa vụ của các bên, điều kiện áp dụng, trình tự, thủ tục thực hiện, chế tài xử lý và cơ chế bảo vệ quyền của chủ thể bị tác động. Bên cạnh đó, kỹ thuật lập pháp còn được thể hiện ở sự thống nhất về thuật ngữ, cách diễn đạt, sự liên kết giữa các quy định và khả năng áp dụng ổn định trong thực tiễn.

Đối với pháp luật về an ninh mạng, kỹ thuật lập pháp cần bảo đảm sự kết hợp hợp lý giữa quy định mang tính nguyên tắc với quy định cụ thể; giữa tiêu chí nhận diện mở với danh mục hành vi điển hình; giữa tính ổn định của

văn bản luật với khả năng cập nhật thông qua văn bản hướng dẫn, tiêu chuẩn, quy chuẩn kỹ thuật hoặc cơ chế chuyên ngành. Cách thiết kế này giúp pháp luật có thể điều chỉnh các hành vi vi phạm trên không gian mạng một cách linh hoạt nhưng vẫn bảo đảm tính xác định, tính dự báo và giới hạn pháp lý cần thiết.

Cơ sở để đánh giá tiêu chí này bao gồm hệ thống văn bản QPPL về an ninh mạng và các lĩnh vực liên quan; kết quả rà soát, hệ thống hóa văn bản; báo cáo tổng kết thi hành pháp luật; các vướng mắc phát sinh trong thực tiễn áp dụng; ý kiến của chuyên gia, cơ quan quản lý nhà nước, cơ quan thực thi pháp luật, doanh nghiệp và các chủ thể có liên quan.

Trên cơ sở đó, kỹ thuật lập pháp của pháp luật về an ninh mạng có thể được xem xét theo ba mức độ. Pháp luật được đánh giá là có kỹ thuật lập pháp tốt khi các quy định được xây dựng rõ ràng, logic, thống nhất về thuật ngữ, xác định đầy đủ chủ thể, quyền, nghĩa vụ, điều kiện áp dụng, thẩm quyền, trình tự, thủ tục và chế tài xử lý. Pháp luật được đánh giá là đáp ứng ở mức tương đối khi phần lớn quy định đã rõ ràng, có thể áp dụng được nhưng vẫn còn một số điều khoản chưa chặt chẽ, thiếu hướng dẫn hoặc chưa thật sự thống nhất. Pháp luật được đánh giá là còn hạn chế về kỹ thuật lập pháp khi nhiều quy định còn mơ hồ, thiếu thống nhất về thuật ngữ, cấu trúc lỏng lẻo hoặc gây khó khăn cho việc hiểu, áp dụng và tổ chức thực hiện trong thực tiễn.

Tiêu chí kỹ thuật lập pháp góp phần bảo đảm pháp luật về an ninh mạng không chỉ đúng về định hướng chính sách mà còn có khả năng vận hành hiệu quả trong thực tiễn. Một hệ thống quy phạm được xây dựng với kỹ thuật lập pháp tốt sẽ nâng cao khả năng tiếp cận pháp luật, tăng cường tính thống nhất trong áp dụng và góp phần bảo vệ hiệu quả an ninh mạng, quyền và lợi ích hợp pháp của các chủ thể trong môi trường số.

### ***2.3.2.3. Nhóm tiêu chí về thực thi pháp luật***

#### ***- Tiêu chí về tính khả thi***

Tính khả thi là tiêu chí quan trọng để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh khả năng các quy định

pháp luật được triển khai và thực hiện hiệu quả trong thực tiễn, phù hợp với điều kiện kinh tế, xã hội, kỹ thuật, tổ chức và năng lực quản lý của Nhà nước cũng như khả năng tuân thủ của các chủ thể có liên quan. Một quy định pháp luật chỉ thực sự phát huy giá trị khi không chỉ đúng về nội dung mà còn có thể được thực hiện trên thực tế.

Việc xem xét tiêu chí này có thể dựa trên một số biểu hiện chủ yếu. Trước hết là mức độ rõ ràng, cụ thể của các quy định về thẩm quyền, trách nhiệm, trình tự, thủ tục và điều kiện áp dụng. Bên cạnh đó, tính khả thi còn được thể hiện ở sự phù hợp giữa các nghĩa vụ pháp lý được đặt ra với năng lực thực hiện của cơ quan nhà nước, doanh nghiệp, tổ chức và cá nhân; khả năng triển khai các biện pháp bảo vệ an ninh mạng trong thực tiễn; cũng như sự tồn tại của cơ chế phối hợp, cơ chế giám sát và các điều kiện bảo đảm thi hành. Đối với những biện pháp có khả năng tác động đến quyền và lợi ích hợp pháp của cá nhân, tổ chức, pháp luật cần quy định rõ căn cứ áp dụng, thẩm quyền quyết định, phạm vi, thời hạn thực hiện và cơ chế kiểm soát nhằm bảo đảm vừa hiệu quả vừa khả thi trong thực tế.

Cơ sở để đánh giá tiêu chí này bao gồm hệ thống văn bản QPPL hiện hành; các báo cáo tổng kết thi hành pháp luật; số liệu về mức độ tuân thủ, xử lý vi phạm và thực hiện các biện pháp bảo vệ an ninh mạng; kết quả thanh tra, kiểm tra; các vụ việc thực tiễn phát sinh; cùng với ý kiến của cơ quan quản lý nhà nước, cơ quan thực thi pháp luật, doanh nghiệp, chuyên gia và các chủ thể có liên quan.

Trên cơ sở đó, tính khả thi của pháp luật về an ninh mạng có thể được xem xét theo ba mức độ. Pháp luật được đánh giá là có tính khả thi cao khi các quy định rõ ràng, phù hợp với điều kiện thực tiễn, có thể áp dụng trực tiếp và được thực hiện hiệu quả trong thực tế. Pháp luật được đánh giá là có tính khả thi ở mức tương đối khi phần lớn các quy định có thể triển khai nhưng vẫn còn một số khó khăn về nguồn lực, cơ chế phối hợp hoặc hướng dẫn thi hành. Pháp luật được đánh giá là có tính khả thi thấp khi nhiều quy định khó

thực hiện, thiếu điều kiện bảo đảm hoặc vượt quá khả năng đáp ứng của các chủ thể thực hiện, dẫn đến hiệu quả thi hành thấp hoặc không được thực hiện trên thực tế.

Tiêu chí tính khả thi cho phép đánh giá không chỉ chất lượng của các quy định pháp luật mà còn mức độ tương thích giữa pháp luật với điều kiện thực tiễn. Đây là cơ sở quan trọng để nhận diện những quy định khó thực hiện, từ đó đề xuất các giải pháp hoàn thiện pháp luật về an ninh mạng theo hướng hiệu quả, khả thi và phù hợp với yêu cầu bảo vệ ANQG trong bối cảnh chuyển đổi số.

*- Tiêu chí về hiệu quả của cơ chế thực thi*

Hiệu quả của cơ chế thực thi là tiêu chí quan trọng để đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng. Tiêu chí này phản ánh mức độ các quy định pháp luật được thực hiện trên thực tế và khả năng đạt được các mục tiêu đặt ra trong bảo vệ ANQG, TTATXH, quyền và lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng. Một hệ thống pháp luật về an ninh mạng chỉ thực sự hoàn thiện khi các quy định không chỉ tồn tại trên phương diện pháp lý mà còn được triển khai hiệu quả trong thực tiễn. Việc xem xét tiêu chí này có thể dựa trên một số biểu hiện chủ yếu. Trước hết là năng lực của các cơ quan, tổ chức có thẩm quyền trong việc phòng ngừa, phát hiện, ngăn chặn, xử lý và khắc phục hậu quả của các hành vi xâm phạm an ninh mạng. Bên cạnh đó, hiệu quả thực thi còn được thể hiện thông qua khả năng phối hợp giữa các cơ quan nhà nước, doanh nghiệp và các chủ thể có liên quan; mức độ tuân thủ pháp luật của tổ chức, cá nhân; khả năng phát hiện và xử lý kịp thời các hành vi vi phạm; hiệu quả của các biện pháp bảo vệ hệ thống thông tin, dữ liệu và ứng phó sự cố an ninh mạng. Trong bối cảnh không gian mạng có tính xuyên biên giới, hiệu quả thực thi còn được phản ánh qua khả năng hợp tác quốc tế trong trao đổi thông tin, hỗ trợ điều tra, thu thập chứng cứ điện tử và xử lý các vụ việc có yếu tố nước ngoài.

Cơ sở để đánh giá tiêu chí này bao gồm các báo cáo tổng kết thi hành pháp luật; số liệu về thanh tra, kiểm tra, xử lý vi phạm; thống kê về sự cố an

ninh mạng, tội phạm mạng và kết quả khắc phục hậu quả; kết quả khảo sát, phỏng vấn các cơ quan thực thi, doanh nghiệp và chuyên gia; cùng với các vụ việc điển hình phát sinh trong thực tiễn áp dụng pháp luật.

Trên cơ sở đó, hiệu quả của cơ chế thực thi pháp luật về an ninh mạng có thể được xem xét theo ba mức độ. Pháp luật được đánh giá là có hiệu quả thực thi cao khi các quy định được triển khai tương đối đầy đủ, các chủ thể tuân thủ tốt, cơ chế phối hợp vận hành hiệu quả và các mục tiêu bảo vệ an ninh mạng cơ bản đạt được trong thực tiễn. Pháp luật được đánh giá là có hiệu quả thực thi ở mức tương đối khi phần lớn quy định được thực hiện nhưng vẫn còn những hạn chế về nguồn lực, năng lực thực thi hoặc cơ chế phối hợp. Pháp luật được đánh giá là có hiệu quả thực thi thấp khi nhiều quy định khó áp dụng, tỷ lệ tuân thủ thấp, việc phát hiện và xử lý vi phạm còn hạn chế hoặc chưa đạt được các mục tiêu quản lý đã đặt ra.

Tiêu chí này cho thấy mức độ hoàn thiện của pháp luật về an ninh mạng không chỉ phụ thuộc vào chất lượng của các QPPL mà còn phụ thuộc vào thiết chế thực thi, nguồn lực bảo đảm và khả năng tổ chức thực hiện trong thực tiễn. Vì vậy, hoàn thiện pháp luật về an ninh mạng phải gắn liền với việc nâng cao năng lực thực thi, tăng cường cơ chế phối hợp và bảo đảm các điều kiện cần thiết cho việc áp dụng pháp luật một cách hiệu quả.

## **2.4. ĐIỀU KIỆN BẢO ĐẢM HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG**

### **2.4.1. Điều kiện chính trị - pháp lý**

Điều kiện chính trị - pháp lý là điều kiện nền tảng bảo đảm cho quá trình hoàn thiện pháp luật về an ninh mạng ở Việt Nam được thực hiện đúng định hướng, đúng thẩm quyền, phù hợp với yêu cầu bảo vệ ANQG, TTATXH và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng. Pháp luật về an ninh mạng là lĩnh vực có liên quan trực tiếp đến chủ quyền quốc gia, ANQG, quyền con người, quyền công dân, hoạt động quản lý nhà nước, chuyển đổi số và phát triển kinh tế số. Vì vậy, việc hoàn thiện pháp luật

trong lĩnh vực này không thể tách rời nền tảng chính trị - pháp lý của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

Trước hết, hoàn thiện pháp luật về an ninh mạng phải bảo đảm phù hợp với Hiến pháp. Các quy định pháp luật về an ninh mạng phải bảo đảm thống nhất với các nguyên tắc hiến định về bảo vệ Tổ quốc, bảo vệ ANQG, bảo đảm TTATXH, tôn trọng, bảo vệ và bảo đảm quyền con người, quyền công dân.

Bên cạnh đó, hoàn thiện pháp luật về an ninh mạng phải phù hợp với quan điểm, đường lối của Đảng về bảo vệ ANQG, xây dựng Nhà nước pháp quyền xã hội chủ nghĩa, phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia. Đây là cơ sở định hướng chính trị quan trọng để xác định mục tiêu, yêu cầu và phạm vi hoàn thiện pháp luật về an ninh mạng. Trong điều kiện không gian mạng ngày càng trở thành môi trường chiến lược gắn với chủ quyền quốc gia, ANQG và sự phát triển đất nước, pháp luật về an ninh mạng phải thể chế hóa kịp thời các định hướng chính trị thành các QPPL cụ thể, khả thi và có hiệu lực thực thi hành trong thực tế.

Điều kiện chính trị - pháp lý còn đòi hỏi việc hoàn thiện pháp luật về an ninh mạng phải gắn với yêu cầu xây dựng và hoàn thiện Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam. Theo đó, pháp luật về an ninh mạng phải bảo đảm tính hợp hiến, hợp pháp, thống nhất, minh bạch, khả thi; quyền lực nhà nước trong lĩnh vực an ninh mạng phải được phân công, phối hợp và kiểm soát hiệu quả. Đây là yêu cầu quan trọng nhằm bảo đảm hoạt động bảo vệ an ninh mạng không bị tùy tiện, lạm quyền hoặc xâm phạm không cần thiết đến quyền, lợi ích hợp pháp của cá nhân, tổ chức.

Ngoài ra, hoàn thiện pháp luật về an ninh mạng phải phù hợp với chính sách của Nhà nước về chuyển đổi số, phát triển kinh tế số, xã hội số và bảo vệ dữ liệu. An ninh mạng không chỉ là công cụ bảo vệ, mà còn là điều kiện bảo đảm cho chuyển đổi số an toàn, minh bạch và bền vững. Pháp luật về an ninh mạng cần được hoàn thiện theo hướng vừa bảo vệ ANQG, vừa tạo lập

môi trường pháp lý thuận lợi cho đổi mới sáng tạo, phát triển công nghệ và hoạt động hợp pháp của doanh nghiệp, người dân trên không gian mạng.

Đồng thời, điều kiện chính trị - pháp lý cũng đặt ra yêu cầu bảo đảm sự thống nhất giữa pháp luật về an ninh mạng với các lĩnh vực pháp luật có liên quan như pháp luật về an toàn thông tin mạng, dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, công nghệ thông tin, bảo vệ bí mật nhà nước, xử lý vi phạm hành chính, hình sự, tố tụng hình sự và hợp tác quốc tế. Do tính liên ngành của an ninh mạng, nếu thiếu sự thống nhất về chính sách và kỹ thuật lập pháp, hệ thống pháp luật dễ phát sinh chồng chéo, mâu thuẫn hoặc khoảng trống pháp lý. Vì vậy, việc hoàn thiện pháp luật về an ninh mạng phải được đặt trong tổng thể hoàn thiện hệ thống pháp luật quốc gia.

#### **2.4.2. Điều kiện về nhận thức lý luận và tư duy lập pháp**

Điều kiện về nhận thức lý luận và tư duy lập pháp có ý nghĩa đặc biệt quan trọng đối với quá trình hoàn thiện pháp luật về an ninh mạng. Đây là lĩnh vực mới, phức tạp, có tốc độ biến đổi nhanh và chịu sự tác động trực tiếp của khoa học, công nghệ. Vì vậy, nếu thiếu nhận thức lý luận đúng đắn, đầy đủ và cập nhật, việc xây dựng pháp luật về an ninh mạng dễ rơi vào tình trạng phiến diện, chấp vá, hoặc chỉ phản ứng trước các vấn đề đã phát sinh mà chưa có khả năng dự báo, phòng ngừa và quản trị rủi ro.

Trước hết, pháp luật về an ninh mạng cần được xây dựng trên cơ sở nhận thức đúng về tính liên ngành của lĩnh vực này. An ninh mạng không chỉ là vấn đề thuộc phạm vi công nghệ thông tin, mà còn liên quan trực tiếp đến ANQG, TTATXH, dữ liệu, viễn thông, giao dịch điện tử, bảo vệ bí mật nhà nước, bảo vệ quyền con người, quyền công dân, xử lý vi phạm hành chính, hình sự, tố tụng hình sự và hợp tác quốc tế. Do đó, tư duy lập pháp trong lĩnh vực này phải là tư duy liên ngành, bảo đảm sự kết nối giữa các lĩnh vực pháp luật có liên quan, tránh tình trạng mỗi ngành, mỗi lĩnh vực điều chỉnh một phần nhưng thiếu sự thống nhất trong tổng thể.

Đặc biệt, tư duy lập pháp về an ninh mạng phải bảo đảm sự cân bằng giữa yêu cầu bảo vệ an ninh và bảo vệ quyền. Do đó, tư duy lập pháp phù hợp trong lĩnh vực an ninh mạng phải là tư duy cân bằng, dựa trên nguyên tắc pháp quyền. Pháp luật cần đủ mạnh để bảo vệ ANQG, chủ quyền quốc gia trên không gian mạng, hệ thống thông tin quan trọng, dữ liệu và TTATXH; đồng thời phải đủ minh bạch, cần thiết, tương xứng và có cơ chế kiểm soát để bảo vệ quyền con người, quyền công dân.

Ngoài ra, nhận thức lý luận và tư duy lập pháp về an ninh mạng cần chuyển từ tư duy xử lý sau vi phạm sang tư duy quản trị rủi ro. Trong môi trường mạng, khi sự cố đã xảy ra, thiệt hại về dữ liệu, bí mật nhà nước, tài sản, danh dự, uy tín, niềm tin xã hội và hoạt động của hệ thống thông tin có thể rất khó khắc phục hoàn toàn. Vì vậy, pháp luật cần được thiết kế theo hướng phòng ngừa từ sớm, từ xa; nhận diện nguy cơ; đánh giá rủi ro; phân loại hệ thống thông tin, dữ liệu và chủ thể theo mức độ rủi ro; thiết lập cơ chế cảnh báo, báo cáo sự cố, ứng cứu, phục hồi và khắc phục hậu quả.

#### **2.4.3. Điều kiện về thiết chế và cơ chế phối hợp**

Điều kiện về thiết chế và cơ chế phối hợp là một trong những điều kiện quan trọng bảo đảm cho việc hoàn thiện pháp luật về an ninh mạng được thực hiện hiệu quả. An ninh mạng là lĩnh vực có tính liên ngành, liên quan đến nhiều cơ quan, nhiều lĩnh vực quản lý và nhiều nhóm chủ thể khác nhau. Vì vậy, nếu thiếu thiết chế phù hợp và cơ chế phối hợp rõ ràng, pháp luật về an ninh mạng dù được quy định đầy đủ vẫn khó phát huy hiệu quả trong thực tiễn.

Trước hết, cần có thiết chế thực thi đủ mạnh, có chức năng, nhiệm vụ và thẩm quyền được xác định rõ ràng. Trong lĩnh vực an ninh mạng, nhiều cơ quan cùng tham gia vào quá trình quản lý, bảo vệ, xử lý sự cố và đấu tranh phòng, chống hành vi vi phạm. Việc phân định này có ý nghĩa quan trọng nhằm tránh chồng chéo, trùng lặp, đùn đẩy trách nhiệm hoặc bỏ trống nhiệm vụ trong quá trình thực thi pháp luật.

Bên cạnh việc xác định thiết chế, cần thiết lập cơ chế phối hợp liên ngành thống nhất, thường xuyên và có tính bắt buộc. An ninh mạng không thể

được bảo đảm hiệu quả nếu mỗi cơ quan chỉ xử lý vấn đề trong phạm vi chức năng riêng của mình mà thiếu kết nối với các cơ quan khác. Cơ chế phối hợp cần quy định rõ trình tự tiếp nhận, xử lý thông tin; cơ chế chia sẻ dữ liệu, cảnh báo nguy cơ; quy trình phối hợp ứng phó sự cố; thời hạn phản hồi; trách nhiệm bảo mật thông tin; trách nhiệm báo cáo và trách nhiệm pháp lý trong trường hợp chậm trễ, không phối hợp hoặc phối hợp không đầy đủ.

Ngoài ra, thiết chế và cơ chế phối hợp trong lĩnh vực an ninh mạng phải gắn với cơ chế kiểm soát trách nhiệm. Mỗi chủ thể tham gia bảo vệ an ninh mạng cần được xác định rõ quyền hạn, nghĩa vụ và trách nhiệm pháp lý. Cơ chế kiểm soát trách nhiệm là điều kiện cần thiết để hạn chế lạm quyền, nâng cao trách nhiệm giải trình và bảo đảm tính minh bạch trong thực thi pháp luật.

Như vậy, điều kiện về thiết chế và cơ chế phối hợp là điều kiện bảo đảm trực tiếp cho hiệu quả hoàn thiện và thực thi pháp luật về an ninh mạng. Một hệ thống pháp luật về an ninh mạng chỉ có thể vận hành hiệu quả khi có thiết chế thực thi rõ ràng, cơ chế phối hợp liên ngành chặt chẽ, cơ chế chia sẻ thông tin an toàn, quy trình xử lý sự cố thống nhất và trách nhiệm của các chủ thể được kiểm soát bằng pháp luật. Đây là cơ sở quan trọng để nâng cao hiệu lực quản lý nhà nước, bảo vệ ANQG, TTATXH và quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng.

#### **2.4.4. Điều kiện về nguồn lực con người và kỹ thuật**

Điều kiện về nguồn lực con người và kỹ thuật là điều kiện có ý nghĩa trực tiếp đối với tính khả thi của pháp luật về an ninh mạng. Đây là lĩnh vực có tính chuyên môn sâu, đòi hỏi sự kết hợp giữa tri thức pháp lý, kiến thức công nghệ thông tin, năng lực điều tra số, khả năng phân tích dữ liệu, kỹ năng giám sát hệ thống và năng lực ứng phó sự cố. Vì vậy, pháp luật về an ninh mạng chỉ có thể được tổ chức thực hiện hiệu quả khi có đội ngũ nhân lực phù hợp và hạ tầng kỹ thuật tương ứng.

Trước hết, cần có đội ngũ chuyên gia pháp lý am hiểu về an ninh mạng. Việc xây dựng, hoàn thiện và áp dụng pháp luật trong lĩnh vực này không thể

chỉ dựa trên kiến thức pháp luật truyền thống, mà phải gắn với hiểu biết về hệ thống thông tin, dữ liệu, nền tảng số, chứng cứ điện tử, tội phạm mạng, bảo vệ dữ liệu cá nhân và các công nghệ mới. Bên cạnh đội ngũ chuyên gia pháp lý, cần có lực lượng chuyên gia kỹ thuật đủ năng lực để hỗ trợ thực thi pháp luật về an ninh mạng.

Ngoài yếu tố con người, pháp luật về an ninh mạng còn đòi hỏi hạ tầng kỹ thuật phù hợp. Cần có hệ thống giám sát, cảnh báo sớm, công cụ phân tích dữ liệu, cơ sở dữ liệu phục vụ điều tra, hệ thống bảo quản chứng cứ điện tử, nền tảng chia sẻ thông tin và công cụ hỗ trợ ứng phó sự cố. Nếu thiếu các phương tiện kỹ thuật này, các quy định về kiểm tra, giám sát, thu thập dữ liệu điện tử, ứng cứu sự cố và xử lý hành vi vi phạm sẽ khó được thực hiện hiệu quả.

Đồng thời, nguồn lực kỹ thuật phải được tổ chức theo hướng hiện đại, an toàn, bảo mật và có khả năng kết nối giữa các cơ quan, tổ chức có liên quan. Việc sử dụng công cụ kỹ thuật trong thực thi pháp luật về an ninh mạng phải được đặt trong khuôn khổ pháp luật, bảo đảm bí mật nhà nước, dữ liệu cá nhân, bí mật kinh doanh và quyền, lợi ích hợp pháp của cá nhân, tổ chức.

#### **2.4.5. Điều kiện về hợp tác quốc tế**

Điều kiện về hợp tác quốc tế là điều kiện bảo đảm quan trọng đối với quá trình hoàn thiện pháp luật về an ninh mạng. Đặc điểm nổi bật của không gian mạng là tính xuyên biên giới, phi vật lý và phụ thuộc vào hạ tầng kỹ thuật, dữ liệu, nền tảng số, dịch vụ số được phân bố tại nhiều quốc gia, vùng lãnh thổ khác nhau. Do đó, nhiều nguy cơ, hành vi xâm phạm an ninh mạng ở Việt Nam có thể được thực hiện từ bên ngoài lãnh thổ Việt Nam; dữ liệu, chứng cứ điện tử, tài khoản, máy chủ, công cụ tấn công hoặc dòng tiền có thể được lưu giữ, trung chuyển, che giấu ở nhiều quốc gia khác nhau. Trong điều kiện đó, pháp luật quốc gia nếu không gắn với cơ chế hợp tác quốc tế sẽ khó phát huy hiệu quả đầy đủ trong phòng ngừa, phát hiện, điều tra, xử lý và khắc phục hậu quả của hành vi vi phạm.

Trước hết, hoàn thiện pháp luật về an ninh mạng cần gắn với hợp tác quốc tế về chia sẻ thông tin và cảnh báo nguy cơ. Việc chia sẻ thông tin về

phương thức, thủ đoạn, dấu hiệu tấn công, lỗ hổng bảo mật, mã độc, tài khoản nghi vấn, địa chỉ IP, tên miền độc hại và các nguy cơ mới có ý nghĩa quan trọng trong phòng ngừa, cảnh báo sớm và ứng phó sự cố an ninh mạng.

Ngoài ra, hợp tác quốc tế giúp Việt Nam tiếp thu có chọn lọc kinh nghiệm pháp luật, tiêu chuẩn kỹ thuật và mô hình quản trị an ninh mạng của các quốc gia, khu vực và tổ chức quốc tế. Tuy nhiên, việc tiếp thu này phải phù hợp với điều kiện chính trị, pháp lý, kinh tế, xã hội, năng lực công nghệ và yêu cầu bảo vệ ANQG của Việt Nam. Hợp tác quốc tế không nhằm sao chép máy móc mô hình pháp luật nước ngoài, mà nhằm bổ sung luận cứ khoa học và thực tiễn cho việc xây dựng hệ thống pháp luật về an ninh mạng đồng bộ, hiện đại, khả thi và tương thích ở mức cần thiết với các chuẩn mực quốc tế.

Đồng thời, hợp tác quốc tế trong lĩnh vực an ninh mạng phải được đặt trong khuôn khổ bảo vệ chủ quyền quốc gia, lợi ích quốc gia, quyền con người, quyền công dân và quyền, lợi ích hợp pháp của cá nhân, tổ chức.

#### **2.4.6. Điều kiện về giám sát, trách nhiệm giải trình và bảo vệ quyền con người, quyền công dân trên không gian mạng**

Điều kiện về giám sát, trách nhiệm giải trình và bảo vệ quyền là điều kiện quan trọng bảo đảm cho quá trình hoàn thiện pháp luật về an ninh mạng được thực hiện phù hợp với yêu cầu của Nhà nước pháp quyền. An ninh mạng là lĩnh vực có liên quan trực tiếp đến ANQG, TTATXH, nhưng đồng thời cũng có khả năng tác động sâu sắc đến quyền con người, quyền công dân, quyền và lợi ích hợp pháp của cá nhân, tổ chức. Vì vậy, việc áp dụng các biện pháp bảo vệ an ninh mạng phải được đặt trong khuôn khổ pháp luật, chịu sự giám sát, có trách nhiệm giải trình và có cơ chế bảo vệ quyền của chủ thể bị tác động.

Bên cạnh đó, pháp luật cần thiết lập cơ chế giám sát đối với hoạt động áp dụng các biện pháp bảo vệ an ninh mạng. Cơ chế giám sát hiệu quả sẽ góp phần hạn chế lạm quyền, nâng cao tính minh bạch và bảo đảm tính hợp pháp của hoạt động thực thi pháp luật về an ninh mạng.

Trách nhiệm giải trình cũng là yêu cầu không thể thiếu trong lĩnh vực an ninh mạng. Cơ quan, tổ chức, cá nhân có thẩm quyền khi áp dụng biện

pháp bảo vệ an ninh mạng phải có trách nhiệm giải thích, làm rõ căn cứ pháp lý, mục đích, phạm vi, thời hạn và hậu quả pháp lý của biện pháp được áp dụng trong trường hợp pháp luật quy định.

Một nội dung quan trọng khác là pháp luật phải bảo đảm quyền khiếu nại, tố cáo, yêu cầu khắc phục hậu quả và yêu cầu bồi thường thiệt hại của cá nhân, tổ chức khi quyền, lợi ích hợp pháp của họ bị xâm phạm do việc áp dụng biện pháp bảo vệ an ninh mạng trái pháp luật hoặc không đúng thẩm quyền, trình tự, thủ tục. Đây là cơ chế bảo vệ quyền cần thiết nhằm bảo đảm sự cân bằng giữa yêu cầu bảo vệ ANQG và yêu cầu bảo vệ quyền con người, quyền công dân.

## **2.5. PHÁP LUẬT QUỐC TẾ VÀ MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI VỀ AN NINH MẠNG VÀ GIÁ TRỊ THAM KHẢO VỚI VIỆT NAM**

### **2.5.1. Pháp luật quốc tế và một số quốc gia trên thế giới về an ninh mạng**

Việc lựa chọn Hoa Kỳ, Liên minh châu Âu, Liên bang Nga, Trung Quốc và Singapore làm đối tượng nghiên cứu so sánh xuất phát từ tính đại diện của các mô hình tiếp cận pháp luật về an ninh mạng khác nhau trên thế giới. Hoa Kỳ đại diện cho mô hình đề cao bảo vệ hạ tầng thông tin trọng yếu, quản trị rủi ro và hợp tác công - tư; EU đại diện cho mô hình cân bằng giữa bảo đảm an ninh mạng với bảo vệ quyền con người, quyền riêng tư và dữ liệu cá nhân; Liên bang Nga và Trung Quốc đại diện cho mô hình chú trọng bảo vệ chủ quyền quốc gia trên không gian mạng, kiểm soát dữ liệu và bảo đảm ANQG; trong khi Singapore là quốc gia có điều kiện phát triển tương đồng hơn với Việt Nam ở khu vực châu Á, được đánh giá có hệ thống pháp luật về an ninh mạng hiện đại, linh hoạt và hiệu quả. Việc nghiên cứu các quốc gia và khu vực này giúp luận án tiếp cận được những kinh nghiệm lập pháp tiêu biểu, phản ánh các xu hướng phát triển khác nhau của pháp luật về an ninh mạng trên thế giới, từ đó rút ra những giá trị tham khảo phù hợp cho việc hoàn thiện pháp luật về an ninh mạng ở Việt Nam, bảo đảm hài hòa giữa yêu cầu bảo vệ ANQG, thúc đẩy chuyển đổi số và bảo vệ quyền, lợi ích hợp pháp của các chủ thể trên không gian mạng.

### ***2.5.1.1. Pháp luật về an ninh mạng của Liên hợp quốc***

Ở cấp độ quốc tế, Công ước của Liên bang hợp quốc về chống tội phạm mạng được Đại hội đồng Liên hợp quốc thông qua ngày 24/12/2024 và mở ký tại Hà Nội ngày 25/10/2025, đánh dấu bước phát triển quan trọng trong quá trình hình thành pháp lý toàn cầu về phòng chống tội phạm mạng. Công ước không chỉ thiết lập các mức chuẩn chung về hình hóa hành vi phạm tội trên không gian mạng mà còn thiết lập cơ chế tổ tụng quốc tế trong thu thập, bảo quản, chia sẻ chứng cứ điện tử và hỗ trợ điều tra, truy tố tội phạm xuyên biên giới. Điều này cho thấy luật pháp về an ninh mạng không thể chỉ được xây dựng trên cơ sở quy định trong phạm vi quốc gia mà cần được hoàn thiện theo hướng dẫn tương thích với các chuẩn mực và cơ chế hợp tác quốc tế, đặc biệt trong các lĩnh vực liên quan đến chứng cứ điện tử, dữ liệu biên giới, trách nhiệm của nhà cung cấp dịch vụ số và tương thích tư vấn

### ***2.5.1.2. Pháp luật về an ninh mạng của Liên minh châu Âu***

Tại cộng đồng Liên minh châu Âu (EU), pháp luật về an ninh mạng được xây dựng theo hướng hài hòa hóa giữa các thành viên quốc gia, đồng thời gắn kết an ninh mạng với bảo vệ dữ liệu, thị trường số và quyền của người dùng. Tại Chương trình nghị sự về An ninh của châu Âu nói chung, các quốc gia EU đã (i) nhấn mạnh vào việc thực hiện các chính sách hiện có về an ninh mạng, các cuộc tấn công chống lại thông tin hệ thống; (ii) mở rộng luật chống gian lận và làm giả các phương tiện thanh toán không dùng tiền mặt để ứng phó với hình thức tội phạm mới hơn trong lĩnh vực tài chính; (iii) xem xét các trở ngại đối với việc điều tra tội phạm mạng, đặc biệt là các vấn đề thuộc thẩm quyền và quy tắc có thẩm quyền về tiếp cận bằng chứng và thông tin; (iv) tăng cường hành động xây dựng năng lực không gian mạng thông qua các công cụ hỗ trợ bên ngoài. Nội dung Phụ lục 3, nghiên cứu đã liệt kê một số văn bản pháp lý về an ninh mạng đang có hiệu lực tại EU.

Trong đó, có một số văn bản pháp lý tiêu biểu như: Chỉ thị NIS2 đã quy định về việc phân loại chủ thể thành các thực thể thiết yếu và quan trọng,

yêu cầu áp dụng quản lý rủi ro, bảo đảm cung cấp chuỗi ninh, xử lý lỗi và báo cáo sự cố. Chỉ thị này cũng thiết lập quy trình báo cáo nhiều giai đoạn: cảnh báo sớm trong 24 giờ, thông báo sự cố trong 72 giờ và báo cáo cuối cùng trong thời hạn một tháng. Ngoài NIS2, EU còn có Đạo luật An ninh mạng năm 2019, trao nhiệm vụ và vị trí mạnh hơn cho ENISA, đồng thời thiết lập mật mã chứng minh an ninh mạng cho sản phẩm, dịch vụ và quy trình ICT. Gần đây, Đạo luật Phục hồi Mạng đã đưa ra yêu cầu an ninh mạng bắt buộc đối với sản phẩm có yếu tố số, bao gồm phần cứng và phần mềm, đặt trách nhiệm lớn hơn lên nhà sản xuất trong toàn bộ vòng đời sản phẩm.

Nghiên cứu hệ thống pháp luật của EU cho thấy pháp luật về an ninh mạng cần được thiết kế theo hướng đồng bộ giữa an ninh mạng, quản trị rủi ro, nghĩa vụ báo cáo sự cố và bảo vệ quyền. Thực tế hiện nay, pháp luật nước ta cần được quy định theo hướng phân loại chủ thể căn cứ vào mức độ rủi ro, quy định nghĩa vụ bảo mật và báo cáo sự cố tương ứng, đồng thời bảo đảm sự liên thông giữa an ninh mạng, bảo vệ dữ liệu và trách nhiệm của doanh nghiệp.

### ***2.5.1.3. Pháp luật về an ninh mạng của Hoa Kỳ***

Xuất phát từ đặc trưng quản trị theo hướng đa nguyên, số các quy định, văn bản pháp lý của Hoa Kỳ về lĩnh vực an ninh mạng rất đa dạng. Pháp luật về an ninh mạng của Hoa Kỳ được xây dựng theo mô hình nhiều tầng, kết hợp giữa luật liên bang, quy định lớn, sắc lệnh hành pháp, tiêu chuẩn kỹ thuật và luật của tiểu bang. Thực tế, căn cứ cụ thể vào tiêu chí ngành, dữ liệu lưu trữ, quy định ở các tiểu bang mà mỗi chủ thể trong xã hội phải tự xác định những văn bản pháp lý cần chấp hành. Nội dung Phụ lục 3, nghiên cứu đã liệt kê một số văn bản pháp lý về an ninh mạng đang có hiệu lực tại Hoa Kỳ.

Những năm gần đây, Chính phủ Hoa Kỳ đã chú trọng hoàn thiện hành lang pháp lý trong lĩnh vực an ninh mạng. Ở cấp độ pháp lý liên bang, Sắc lệnh hành pháp số 14028 năm 2021 về cải thiện an ninh mạng quốc gia đã tăng cường yêu cầu bảo đảm an ninh chuỗi cung ứng phần mềm, đặc biệt đối với các phần mềm quan trọng phục vụ hoạt động của Chính phủ liên bang.

Cùng với đó, NIST Cybersecurity Framework 2.0 được công bố vào năm 2024 là hướng dẫn quản trị rủi ro an ninh mạng cho các cơ quan nhà nước, doanh nghiệp và tổ chức thuộc nhiều quy mô, lĩnh vực khác nhau. Một điểm đáng chú ý trong luật pháp Hoa Kỳ là cơ chế báo cáo và chia sẻ thông tin về sự cố mạng. Đạo luật CIRCIA năm 2022 yêu cầu CISA xây dựng quy định buộc các thực thể thuộc hạ tầng trọng yếu phải báo cáo sự cố mạng.

Ở cấp độ tiểu bang, chính quyền từng bang đều có bộ phận phụ trách riêng về vấn đề an ninh mạng. Tuy nhiên, cách tiếp cận, cơ cấu tổ chức và cách thức hoạt động của từng bang lại có sự khác nhau và bộ phận này không phải báo cáo lên chính quyền liên bang. Hiện nay, toàn bộ 50 tiểu bang của Hoa Kỳ, Quận Columbia, Guam, Puerto Rico và Quần đảo Virgin đều có luật yêu cầu thông báo khi thông tin cá nhân bị xâm phạm. Các luật này bao gồm từ luật thông báo vi phạm đến các quy định về quyền riêng tư dữ liệu. Trong các bang, California được đánh giá là nơi có luật an ninh mạng toàn diện nhất Hoa Kỳ. Ngày 28/6/2018, đạo luật về quyền riêng tư của người tiêu dùng ở California (sau đây viết tắt là CCPA) đã được ban hành. Đây là văn bản quy định về việc bảo vệ thông tin cá nhân của cư dân California, yêu cầu các công ty cung cấp cho khách hàng quyền truy cập và kiểm soát dữ liệu của họ. Tại tiểu bang Washington, tội phạm mạng được quy định tại Đạo luật Tội phạm mạng của hiện hành thì tội phạm mạng được quy định tại Chương 9A.90 RCW. Tại tiểu bang Texas, một số tội danh đã được nêu cụ thể tại Bộ luật Hình sự.

Như vậy, kinh nghiệm của Hoa Kỳ cho thấy pháp luật về an ninh mạng không nên chỉ dừng ở quy định cấm hoặc xử phạt. Quy định pháp luật cần gắn liền với cơ chế quản lý rủi ro, tiêu chuẩn kỹ thuật, an ninh chuỗi cung ứng phần mềm, cơ chế báo cáo sự cố, chia sẻ thông tin và hợp tác công - tư. Kinh nghiệm của Hoa Kỳ cho thấy các tiêu chuẩn kỹ thuật như NIST CSF có thể đóng vai trò “cầu nối” giữa QPPL và thực tiễn vận hành của doanh nghiệp.

#### ***2.5.1.4. Pháp luật về an ninh mạng của Liên bang Nga***

Liên bang Nga luôn xác định an ninh mạng là lĩnh vực trọng điểm, đặc biệt quan trọng và xem đây là thành tố cấu thành của ANQG cùng với các lĩnh

vực như quốc phòng, đối ngoại, kinh tế, truyền thông. Quan điểm này đã được khẳng định và đề cập tới trong Chiến lược An ninh quốc gia 2009 - 2020, Thuyết Quốc phòng Liên bang Nga năm 2010, Chính sách Đối ngoại Liên bang Nga năm 2013, Chính sách Quốc phòng Liên bang Nga năm 2014, Chính sách An ninh quốc gia Liên bang Nga năm 2014. Đánh giá tổng thể, ta thấy rằng, khác với nhiều quốc gia trên thế giới, quan điểm của nhà nước Liên bang Nga không coi an ninh mạng là một mặt trận riêng lẻ mà nó được lồng ghép, cộng hưởng trong các chính sách, chiến lược phát triển về an ninh thông tin.

Nghiên cứu pháp luật của Liên bang Nga về an ninh mạng ta thấy rằng: Ngay từ cuối thế kỷ XX, cùng với việc quy chuẩn hóa hệ thống an ninh mạng và công nghệ thông tin thì pháp luật về an ninh mạng tại quốc gia này đã thực sự được quan tâm, chú trọng. Do đó, ngay tại phiên bản gốc của Bộ luật Hình sự số 13/06/1996 N 63-FZ, Liên bang Nga đã quy định về các yếu tố của tội phạm xâm phạm an ninh mạng. Sau này, việc phát triển khuôn khổ pháp lý để chống tội phạm mạng diễn ra theo từng giai đoạn và bối cảnh thực tế của đất nước. Năm 2014, để tăng cường công tác bảo vệ dữ liệu cá nhân nhằm đáp ứng trước tình hình chính trị trong và ngoài nước, đặc biệt trong bối cảnh các trang mạng xã hội bị lợi dụng để chống đối chính phủ, Liên bang Nga đã ban hành Luật số 242-FZ về nội địa hóa dữ liệu. Nội dung đạo luật này tập trung vào chính sách quản lý mạng xã hội ở Liên bang Nga. Theo đó, tất cả các pháp nhân có hoạt động về Internet, quản lý hộp thư điện tử, công cụ tìm kiếm, các mạng xã hội nội địa hoặc nước ngoài nhằm đến người dùng Liên bang Nga đều phải ghi chép, hệ thống hóa, lưu trữ và xác định dữ liệu người dùng. Tất cả các thông tin của người sử dụng phải được lưu trữ tại máy chủ đặt tại lãnh thổ Liên bang Nga. Văn bản này cũng yêu cầu các công ty viễn thông và nhà cung cấp dịch vụ Internet phải cắt giảm dịch vụ đối với người sử dụng trong một số trường hợp. Nội dung Phụ lục 3, nghiên cứu đã liệt kê một số văn bản pháp lý về an ninh mạng đang có hiệu lực tại Liên bang Nga.

Như vậy, Liên bang Nga có quan điểm cơ bản khác với các quốc gia phương Tây về đối tượng và hành vi cấu thành các nguy cơ đến từ không gian

mạng, về sự cân bằng giữa bảo đảm quyền tự do cá nhân và lợi ích quốc gia trên không gian mạng. Với quan điểm của mình, nhà nước Liên bang Nga đã thiết lập cơ chế, công cụ để thu thập chứng cứ trên mạng, nắm quyền vận hành, đóng cửa các tài nguyên mạng mà không cần phải có quyết định của tòa án.

#### ***2.5.1.5. Pháp luật về an ninh mạng của Trung Quốc***

Trong thời đại mới, Trung Quốc xác định an ninh mạng là một thành phần quan trọng trong bối cảnh an ninh mới. Báo cáo của Đại hội toàn quốc lần thứ 20 của Đảng Cộng sản Trung Quốc đề xuất “bảo đảm mô hình phát triển mới với mô hình an ninh mới” và “tăng cường xây dựng hệ thống an ninh cho nền kinh tế, cơ sở hạ tầng lớn, tài chính, mạng, dữ liệu, sinh học, tài nguyên, hạt nhân, không gian và đại dương”. Với tiền đề là bảo đảm an ninh mạng, Trung Quốc đã tận dụng tối đa tài nguyên dữ liệu và tối đa hóa giá trị của dữ liệu, xem đây là chìa khóa để chuyển đổi kỹ thuật số của chính phủ và doanh nghiệp, thúc đẩy sự phát triển chất lượng cao của nền kinh tế kỹ thuật số. Do đó, tại Trung Quốc việc hiện đại hóa hệ thống pháp luật về an ninh mạng không chỉ cần thiết để bảo vệ quyền, lợi ích hợp pháp của cư dân mạng và sự phát triển của kinh tế mạng mà còn là điều kiện cần thiết để bảo vệ chủ quyền mạng quốc gia và an ninh quốc phòng. Thời gian qua, hệ thống pháp luật về an ninh mạng đã dần được hình thành và hoàn thiện với những văn bản được liệt kê cụ thể tại Phụ lục 3.

Kinh nghiệm của Trung Quốc cho thấy cách tiếp cận nhấn mạnh chủ quyền không gian mạng, ANQG, bảo vệ hạ tầng thông tin quan trọng và nghĩa vụ của nhà vận hành mạng. Bản dịch Luật An ninh mạng Trung Quốc cho thấy Điều 1 của luật này đặt mục tiêu bảo vệ an ninh mạng, chủ quyền không gian mạng, ANQG, lợi ích công cộng và quyền, lợi ích hợp pháp của công dân, pháp nhân, tổ chức khác. Giá trị tham khảo đối với Việt Nam là có thể nghiên cứu cơ chế bảo vệ chủ quyền số và hạ tầng thông tin quan trọng, nhưng cần tránh sao chép máy móc và phải đặt trong khuôn khổ Hiến pháp, nhà nước pháp quyền, bảo vệ quyền con người, quyền công dân.

#### ***2.5.1.6. Pháp luật về an ninh mạng của Singapore***

Trong Hiệp hội các quốc gia Đông Nam Á (gọi tắt là ASEAN), Singapore là quốc gia có mô hình luật pháp về an ninh mạng được thiết kế tương đối toàn diện về cơ quan đầu mối, chủ quản vận hành và phạm vi bảo vệ hạ tầng thông tin trọng yếu. Nghiên cứu pháp luật về an ninh mạng của Singapore, một số văn bản pháp lý quan trọng đã được liệt kê cụ thể tại Phụ lục 3.

Trong đó, Luật An ninh mạng năm 2018 được xem là văn bản quan trọng khi đã thiết lập được khuôn khổ pháp lý để giám sát và duy trì an ninh mạng quốc gia; bảo vệ cơ sở hạ tầng thông tin quan trọng; trao quyền cho Cơ quan An ninh mạng Singapore trong phòng ngừa, ứng phó sự cố; thiết lập cơ chế chia sẻ thông tin; và cấp phép đối với một số nhà cung cấp dịch vụ an ninh mạng như đánh giá lỗ hổng bảo mật (kiểm thử xâm nhập), giám sát Trung tâm Điều hành An ninh mạng (SOC). Luật An ninh mạng sửa đổi năm 2024 đã mở rộng phạm vi điều chỉnh để phù hợp với bối cảnh công nghệ mới, bao gồm trách nhiệm của chủ sở hữu hạ tầng thông tin trọng yếu khi sử dụng điện toán đám mây, nghĩa là phải báo cáo sự cố trong chuỗi cung ứng và khả năng điều chỉnh các hệ thống có tính chất nền tảng hoặc trung gian như nhà cung cấp dịch vụ đám mây, trung tâm dữ liệu. Cách tiếp cận của Singapore cũng lưu ý rằng việc quản lý dịch vụ an ninh mạng nên theo hướng “đúng trọng tâm, đúng nguy cơ”, tránh việc mở rộng quá mức gây cản trở thị trường dịch vụ an ninh mạng.

#### **2.5.2. Một số bài học kinh nghiệm đối với Việt Nam**

Do xuất phát điểm về công nghệ, môi trường ICT và định hướng phát triển, hoạch định chính sách khác nhau. Do đó, khi nghiên cứu học tập kinh nghiệm hoàn thiện pháp luật về an ninh mạng của các quốc gia khác trên thế giới thì Việt Nam cần (i) nắm được nguyên nhân tại sao các quốc gia ấy xây dựng và hoàn thiện pháp luật của mình theo hướng như vậy, họ xây dựng những quy định đó trong bối cảnh đất nước như thế nào, hiện trạng vấn đề an toàn, an ninh mạng mà quốc gia đang phải đối mặt là gì; (ii) xác định rõ quan

điểm xây dựng, hoàn thiện pháp luật về an ninh mạng cùng với những mục tiêu, tầm nhìn, nguyên tắc hoạt động và kế hoạch hành động mà họ hướng đến; (iii) xác định rõ khung tiêu chí và những vấn đề cụ thể có thể áp dụng với Việt Nam.

Từ kinh nghiệm của Hoa Kỳ, EU, Nga, Trung Quốc, Singapore và Liên hợp quốc, nghiên cứu sinh đưa ra một số bài học kinh nghiệm sau:

***2.5.2.1. Xác định an ninh mạng là nội dung trọng yếu của bảo vệ an ninh quốc gia, trật tự, an toàn xã hội và phát triển kinh tế số***

Nghiên cứu pháp luật về an ninh mạng của một số quốc gia trên thế giới cho thấy an ninh mạng không còn là vấn đề kỹ thuật đơn thuần, mà đã trở thành nội dung trọng yếu của ANQG, an ninh kinh tế, an ninh xã hội và bảo vệ quyền con người, quyền công dân.. Nhận thức này đã được thể chế hóa trong các chiến lược ANQG, đạo luật chuyên ngành và nhiều văn bản pháp luật của các quốc gia, tạo cơ sở pháp lý quan trọng cho việc phòng ngừa, phát hiện và ứng phó với các nguy cơ đe dọa từ không gian mạng.

Bên cạnh việc xác định rõ vị trí, vai trò của an ninh mạng trong bảo vệ ANQG, nhiều quốc gia còn chú trọng xây dựng cơ chế chia sẻ thông tin mạng nhằm nâng cao hiệu quả phòng ngừa và ứng phó với các mối đe dọa trên không gian mạng. Điển hình, Hoa Kỳ đã ban hành Đạo luật Chia sẻ thông tin an ninh mạng, trong đó quy định cơ chế chia sẻ, trao đổi thông tin giữa các cơ quan nhà nước và khu vực tư nhân, đồng thời xác định rõ các biện pháp phòng thủ mạng như sử dụng công cụ, kỹ thuật, quy trình và giải pháp công nghệ để phát hiện, ngăn chặn và giảm thiểu các nguy cơ đe dọa an ninh mạng cũng như các lỗ hổng bảo mật của hệ thống thông tin. Tương tự, pháp luật Trung Quốc cũng đặc biệt coi trọng nhiệm vụ bảo vệ an ninh mạng quốc gia.

Từ những kinh nghiệm trên có thể khẳng định rằng việc xác định an ninh mạng là một bộ phận cấu thành quan trọng của ANQG, đồng thời xây dựng cơ chế chia sẻ thông tin mạng hiệu quả giữa các cơ quan, tổ chức và doanh nghiệp là yêu cầu cần thiết trong bối cảnh chuyển đổi số hiện nay. Đây

là cơ sở quan trọng giúp nâng cao năng lực phòng ngừa, phát hiện sớm và ứng phó kịp thời với các nguy cơ trên không gian mạng, góp phần bảo vệ chủ quyền quốc gia, bảo đảm TTATXH và thúc đẩy phát triển bền vững.

#### ***2.5.2.2. Bắt buộc sử dụng thông tin thật khi sử dụng dịch vụ trên không gian mạng, nghiêm cấm lan truyền tin tức giả trên mạng xã hội***

Thực tế, việc bắt buộc sử dụng thông tin định danh thật khi tham gia các dịch vụ trên không gian mạng, đồng thời kiểm soát và xử lý nghiêm hành vi phát tán tin giả trên mạng xã hội, là một trong những giải pháp quan trọng nhằm bảo đảm an ninh mạng và duy trì trật tự xã hội. Quy định này góp phần hạn chế những tác động tiêu cực xuất phát từ tính ẩn danh của Internet, nâng cao trách nhiệm của người dùng đối với các hành vi được thực hiện trên môi trường trực tuyến, đồng thời tạo điều kiện thuận lợi cho cơ quan nhà nước trong công tác quản lý, giám sát và xử lý vi phạm. Thực tiễn tại Trung Quốc cho thấy việc áp dụng cơ chế đăng ký và sử dụng danh tính thật đối với người dùng Internet đã trở thành một công cụ pháp lý quan trọng trong quản lý không gian mạng.

Từ những kinh nghiệm nêu trên có thể rút ra bài học cho Việt Nam là cần tiếp tục hoàn thiện các quy định pháp luật theo hướng tăng cường trách nhiệm xác thực danh tính người dùng khi tham gia các hoạt động trên không gian mạng, đồng thời xây dựng cơ chế kiểm soát và xử lý hiệu quả đối với hành vi lan truyền thông tin giả, thông tin sai sự thật. Đây là cơ sở quan trọng để xây dựng môi trường mạng an toàn, minh bạch, góp phần bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân, đồng thời phục vụ mục tiêu phát triển kinh tế số và bảo đảm ổn định xã hội.

#### ***2.5.2.3. Công khai giám sát, chặn lọc thông tin xuyên tạc, sai sự thật trên không gian mạng***

Nghiên cứu pháp luật về an ninh mạng của một số quốc gia trên thế giới cho thấy việc xây dựng cơ chế công khai giám sát, chặn lọc và xử lý thông tin xuyên tạc, sai sự thật trên không gian mạng là một nội dung quan

trọng trong bảo đảm an ninh mạng quốc gia. Thực tiễn quản lý của Trung Quốc cho thấy hiệu quả của việc thiết lập hệ thống pháp luật tương đối toàn diện, kết hợp giữa hoạt động giám sát của cơ quan nhà nước với trách nhiệm của các doanh nghiệp cung cấp dịch vụ Internet trong việc kiểm soát thông tin trên môi trường mạng.

Do đó, trong bối cảnh hiện nay cần xây dựng và hoàn thiện cơ sở pháp lý quy định rõ thẩm quyền, trách nhiệm của các cơ quan chức năng trong công tác giám sát, phát hiện và xử lý các thông tin sai sự thật, xuyên tạc hoặc có nội dung gây ảnh hưởng đến ANQG, TTATXH. Đồng thời, cần thiết lập cơ chế phối hợp hiệu quả giữa cơ quan quản lý nhà nước và các doanh nghiệp cung cấp dịch vụ trên không gian mạng nhằm bảo đảm việc ngăn chặn, gỡ bỏ thông tin vi phạm được thực hiện kịp thời và hiệu quả.

Như vậy, kinh nghiệm quốc tế cho thấy, cần tăng cường trách nhiệm pháp lý của các doanh nghiệp cung cấp dịch vụ Internet, mạng xã hội, nền tảng số và các nhà cung cấp nội dung trực tuyến. Xác lập cơ chế kết hợp giữa công nghệ kiểm duyệt tự động với hoạt động kiểm duyệt của con người nhằm nâng cao hiệu quả quản lý nội dung trên không gian mạng. Chú trọng xây dựng cơ chế quản lý dữ liệu và yêu cầu các nhà cung cấp dịch vụ bảo đảm khả năng lưu trữ, cung cấp thông tin phục vụ công tác thanh tra, kiểm tra, điều tra và xử lý vi phạm theo quy định của pháp luật. Song song với đó, pháp luật cần quy định rõ quy trình ứng phó đối với các vụ việc phát tán thông tin độc hại hoặc thông tin bị cấm, trong đó yêu cầu doanh nghiệp nhanh chóng gỡ bỏ nội dung vi phạm, hạn chế khả năng lan truyền, tạm dừng hoặc chấm dứt cung cấp dịch vụ đối với tài khoản vi phạm và lưu giữ dữ liệu cần thiết để phục vụ công tác quản lý nhà nước.

#### ***2.5.2.4. Xây dựng bộ quy tắc, tiêu chuẩn, quy chuẩn trong lĩnh vực an ninh mạng***

Việc xây dựng hệ thống quy tắc, tiêu chuẩn và quy chuẩn kỹ thuật trong lĩnh vực an ninh mạng là yêu cầu quan trọng nhằm bảo đảm tính thống nhất giữa các giải pháp công nghệ với khung khổ pháp lý. Đây cũng là xu

hướng chung được nhiều quốc gia áp dụng để tạo lập cơ sở pháp lý và kỹ thuật cho việc triển khai các biện pháp bảo đảm an ninh mạng.

Thực tiễn, Hoa Kỳ là quốc gia đặc biệt chú trọng xây dựng các bộ tiêu chuẩn và hướng dẫn chuyên ngành về an ninh mạng áp dụng cho từng lĩnh vực cụ thể. Các tiêu chuẩn được thiết kế theo hướng linh hoạt, có khả năng cập nhật thường xuyên để đáp ứng sự phát triển nhanh chóng của công nghệ và các phương thức tấn công mạng mới. Trong khi đó, Trung Quốc lựa chọn cách tiếp cận mang tính tập trung và bắt buộc hơn khi xây dựng hệ thống tiêu chuẩn, quy chuẩn quốc gia về an ninh mạng. Pháp luật nước này quy định việc nghiên cứu, xây dựng và hoàn thiện các tiêu chuẩn kỹ thuật quốc gia là nhiệm vụ quan trọng trong bảo đảm an ninh mạng quốc gia.

Với Việt Nam trong bối cảnh hiện nay, việc xây dựng và hoàn thiện hệ thống quy tắc, tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng là điều kiện cần thiết để nâng cao hiệu quả quản lý nhà nước, bảo đảm an toàn cho các hệ thống thông tin và hạ tầng số quan trọng. Đây là cơ sở quan trọng để nâng cao năng lực phòng ngừa, phát hiện và ứng phó với các nguy cơ trên không gian mạng, góp phần bảo vệ ANQG và thúc đẩy quá trình chuyển đổi số bền vững.

#### ***2.5.2.5. Thiết kế chế tài xử phạt theo hướng phân tầng, tương xứng với tính chất, mức độ, hậu quả và quy mô vi phạm***

Thực tiễn từ Hoa Kỳ, Liên minh châu Âu (EU), Singapore và nhiều quốc gia phát triển cho thấy các chế tài xử phạt không chỉ hướng đến mục tiêu trừng phạt mà còn bảo đảm tính răn đe, phòng ngừa và nâng cao trách nhiệm tuân thủ của các tổ chức, cá nhân tham gia hoạt động trên không gian mạng. Theo đó, mức xử phạt thường được xác định dựa trên nhiều tiêu chí như tính chất hành vi vi phạm, mức độ lỗi, hậu quả gây ra, số lượng chủ thể bị ảnh hưởng, giá trị lợi ích thu được từ hành vi vi phạm cũng như vai trò và trách nhiệm của chủ thể thực hiện hành vi.

Đối với các hành vi có nguy cơ đe dọa trực tiếp đến ANQG, an toàn thông tin hoặc quyền riêng tư của cá nhân, nhiều quốc gia áp dụng chế tài nghiêm khắc hơn, kết hợp giữa xử phạt hành chính, trách nhiệm dân sự và trách

nhiệm hình sự. Các hành vi như mua bán trái phép dữ liệu cá nhân, xử lý dữ liệu không đúng quy định, che giấu hoặc không báo cáo sự cố an ninh mạng nghiêm trọng, tấn công mạng, phát tán mã độc, xâm nhập trái phép hoặc xâm phạm hệ thống thông tin quan trọng đều được xem là những vi phạm nghiêm trọng và bị xử lý ở mức cao. Bên cạnh hình thức xử phạt chính, pháp luật các nước còn quy định nhiều biện pháp khắc phục hậu quả nhằm khôi phục trạng thái an toàn của hệ thống và bảo vệ quyền, lợi ích hợp pháp của các chủ thể bị ảnh hưởng.

Một bài học quan trọng khác được rút ra từ kinh nghiệm của Hoa Kỳ, EU và Singapore là việc gắn chế tài xử phạt với hệ thống tiêu chuẩn, quy chuẩn kỹ thuật, cơ chế quản trị rủi ro và trách nhiệm giải trình của tổ chức, doanh nghiệp. Theo đó, pháp luật chỉ có thể được thực thi hiệu quả khi các nghĩa vụ pháp lý được cụ thể hóa bằng các tiêu chuẩn kỹ thuật, quy trình quản lý nội bộ, cơ chế kiểm tra, đánh giá, kiểm toán và báo cáo định kỳ. Đây là cơ sở để cơ quan quản lý xác định hành vi vi phạm, đồng thời giúp doanh nghiệp có căn cứ rõ ràng để tổ chức thực hiện và chứng minh việc tuân thủ pháp luật.

Từ những kinh nghiệm trên có thể rút ra rằng Việt Nam cần tiếp tục hoàn thiện hệ thống chế tài xử phạt theo hướng bảo đảm tính phân hóa, tương xứng với tính chất và mức độ vi phạm, đồng thời tăng cường áp dụng các biện pháp khắc phục hậu quả nhằm bảo vệ hiệu quả quyền, lợi ích hợp pháp của tổ chức, cá nhân. Bên cạnh đó, cần xây dựng và hoàn thiện hệ thống tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an ninh mạng, an toàn thông tin, bảo vệ dữ liệu cá nhân, định danh và xác thực điện tử; bảo đảm sự liên thông giữa các quy định xử phạt với các tiêu chuẩn kỹ thuật và cơ chế quản trị rủi ro.

## **Tiểu kết Chương 2**

Chương 2 đã xác lập cơ sở lý luận và khung phân tích cho việc nghiên cứu hoàn thiện pháp luật về an ninh mạng ở Việt Nam. Trên cơ sở khung lý thuyết tích hợp, luận án tiếp cận pháp luật về an ninh mạng như một lĩnh vực pháp luật liên ngành, vừa gắn với bảo vệ ANQG, chủ quyền số, TTATXH, vừa gắn với quản trị rủi ro công nghệ, bảo vệ quyền con người, quyền công dân,

quyền riêng tư, dữ liệu cá nhân và quyền, lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng.

Luận án xác định pháp luật về an ninh mạng không phải là toàn bộ pháp luật điều chỉnh mọi hoạt động trên không gian mạng, mà là tổng thể các quy phạm có chức năng bảo vệ an ninh mạng thông qua sáu nhóm chế định: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm; chế tài xử lý; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế.

Trên cơ sở đó, luận án xác lập các tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng, gồm: tính đầy đủ, tính đồng bộ, tính khả thi, tính minh bạch và kỹ thuật lập pháp, khả năng thích ứng với công nghệ, hiệu quả của cơ chế thực thi và mức độ bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức. Các tiêu chí này sẽ được sử dụng như công cụ phân tích ở Chương 3 khi đánh giá thực trạng pháp luật và thực tiễn thực hiện pháp luật về an ninh mạng ở Việt Nam; đồng thời là cơ sở để xây dựng định hướng và giải pháp hoàn thiện ở Chương 4.

Phần kinh nghiệm quốc tế cho thấy pháp luật về an ninh mạng cần được thiết kế theo hướng kết hợp giữa bảo vệ ANQG, quản trị rủi ro, tiêu chuẩn kỹ thuật, trách nhiệm đa chủ thể, hợp tác quốc tế và bảo vệ quyền. Các kinh nghiệm này không được sử dụng để sao chép mô hình nước ngoài, mà để rút ra các giá trị tham khảo phù hợp với điều kiện chính trị, pháp lý, kinh tế, xã hội và năng lực thực thi của Việt Nam.

### **Chương 3**

## **THỰC TRẠNG PHÁP LUẬT VÀ THỰC TIỄN THỰC HIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM HIỆN NAY**

### **3.1. QUÁ TRÌNH HÌNH THÀNH, PHÁT TRIỂN CỦA PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM**

#### **3.1.1. Giai đoạn trước năm 2013**

Giai đoạn trước năm 2013 có thể được xem là giai đoạn hình thành tiền đề của pháp luật về an ninh mạng ở Việt Nam. Trong giai đoạn này, pháp luật về an ninh mạng chưa được xác lập với tư cách là một lĩnh vực pháp luật độc lập, thống nhất và chuyên biệt; các quy định có liên quan còn phân tán trong nhiều lĩnh vực như công nghệ thông tin, giao dịch điện tử, Internet, viễn thông, bảo vệ thông tin cá nhân, bảo vệ bí mật thông tin, xử lý vi phạm hành chính và xử lý hình sự đối với một số hành vi xâm phạm hệ thống thông tin, mạng máy tính, mạng viễn thông. Xét theo sáu nhóm chế định cơ bản của pháp luật về an ninh mạng, giai đoạn này mới hình thành những yếu tố ban đầu.

*Thứ nhất*, về nguyên tắc bảo vệ an ninh mạng, pháp luật chủ yếu tiếp cận từ yêu cầu quản lý Internet, bảo đảm an toàn thông tin, bảo mật giao dịch điện tử và bảo vệ hạ tầng viễn thông, chưa đặt an ninh mạng trong chính thể gắn với chủ quyền quốc gia trên không gian mạng, quản trị rủi ro, bảo vệ dữ liệu và bảo vệ quyền trong môi trường số.

*Thứ hai*, về hành vi vi phạm, các văn bản như Luật Giao dịch điện tử năm 2005, Luật Công nghệ thông tin năm 2006, Nghị định số 90/2008/NĐ-CP, Nghị định số 97/2008/NĐ-CP và các quy định có liên quan đã bước đầu nhận diện một số hành vi nguy hiểm như xâm nhập trái phép, phát tán virus, phần mềm độc hại, phá hoại hạ tầng thông tin, đánh cắp mật khẩu, thông tin riêng và gây rối hoạt động của hệ thống thông tin.

*Thứ ba*, về chế tài xử lý, việc sửa đổi, bổ sung Bộ luật Hình sự năm 1999 vào năm 2009 và ban hành Thông tư liên tịch số 10/2012 đã tạo cơ sở

pháp lý quan trọng để xử lý một số tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, cho thấy nhận thức lập pháp đã chuyển từ quản lý hành chính, kỹ thuật sang yêu cầu đấu tranh phòng, chống tội phạm trên môi trường mạng.

*Thứ tư*, về địa vị pháp lý của các chủ thể, pháp luật bước đầu ghi nhận vai trò quản lý của cơ quan nhà nước, trách nhiệm của doanh nghiệp cung cấp dịch vụ Internet, viễn thông và nghĩa vụ của tổ chức, cá nhân sử dụng dịch vụ, nhưng chưa hình thành đầy đủ cơ chế phân công, phối hợp, trách nhiệm giải trình và bảo vệ quyền của chủ thể trên không gian mạng.

*Thứ năm*, về biện pháp bảo vệ an ninh mạng, các quy định chủ yếu dừng ở bảo đảm an toàn giao dịch điện tử, bảo vệ thông tin, chống thư rác, bảo vệ hạ tầng viễn thông, ngăn chặn một số hành vi xâm nhập, phá hoại hệ thống, chưa hình thành chuỗi biện pháp phòng ngừa, phát hiện, cảnh báo, ứng cứu, khắc phục và phục hồi theo tiếp cận quản trị rủi ro.

*Thứ sáu*, về hợp tác quốc tế, các quy định còn mờ nhạt, chưa thiết lập đầy đủ cơ chế hợp tác trong thu thập chứng cứ điện tử, xử lý hành vi vi phạm xuyên biên giới, phối hợp với nhà cung cấp dịch vụ nước ngoài và bảo vệ dữ liệu xuyên biên giới.

Nhìn chung, pháp luật về an ninh mạng ở Việt Nam trước năm 2013 mang tính tiền đề, phân tán và phản ứng nhiều hơn là dự báo. Tuy chưa hình thành một lĩnh vực pháp luật độc lập, nhưng các quy định trong Luật Giao dịch điện tử năm 2005, Luật Công nghệ thông tin năm 2006, Luật Viễn thông năm 2009, Luật Bảo vệ quyền lợi người tiêu dùng năm 2010 và các văn bản dưới luật có liên quan đã tạo nền tảng pháp lý ban đầu về thông tin số, giao dịch số, hạ tầng số, dữ liệu cá nhân, hành vi vi phạm và trách nhiệm pháp lý trên môi trường mạng. Đây là cơ sở quan trọng cho quá trình chuyên biệt hóa pháp luật về an toàn thông tin mạng và an ninh mạng trong các giai đoạn tiếp theo, đặc biệt là sự ra đời của Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018.

### **3.1.2. Giai đoạn từ năm 2013 đến trước thời điểm ban hành Luật An ninh mạng 2018**

Trên cơ sở các quy định pháp luật được hình thành ở giai đoạn trước năm 2013, từ năm 2013 đến trước thời điểm ban hành Luật An ninh mạng năm 2018, pháp luật Việt Nam về an ninh mạng tiếp tục có bước phát triển quan trọng. Nếu như giai đoạn trước đó các quy định chủ yếu tập trung vào quản lý Internet, công nghệ thông tin, giao dịch điện tử và viễn thông, thì trong giai đoạn này, pháp luật đã từng bước chuyển sang hướng chú trọng hơn đến bảo đảm an toàn thông tin mạng, nhận diện các hành vi vi phạm trên không gian mạng, xác định trách nhiệm của các chủ thể, thiết lập biện pháp bảo vệ hệ thống thông tin và hoàn thiện chế tài xử lý đối với các hành vi vi phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

Có thể đánh giá sự phát triển của pháp luật về an ninh mạng trong giai đoạn này theo sáu nhóm chế định cơ bản như sau:

*Thứ nhất*, về nguyên tắc bảo vệ an ninh mạng. Trong giai đoạn này, pháp luật đã bước đầu xác lập rõ hơn yêu cầu bảo đảm an toàn, an ninh thông tin mạng trong hoạt động quản lý, cung cấp, sử dụng dịch vụ Internet, hệ thống thông tin và dữ liệu điện tử. Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng là văn bản có ý nghĩa quan trọng, thay thế và tích hợp nhiều quy định trước đó về quản lý dịch vụ Internet, thông tin điện tử, trò chơi điện tử trên mạng. Đặc biệt, Luật An toàn thông tin mạng năm 2015 đã đánh dấu bước phát triển rõ nét trong việc xác lập các nguyên tắc bảo đảm an toàn thông tin mạng. Luật này quy định các nguyên tắc về bảo vệ thông tin, hệ thống thông tin; bảo đảm tính bí mật, tính toàn vẹn, tính sẵn sàng của thông tin; bảo vệ thông tin cá nhân; bảo vệ hệ thống thông tin theo cấp độ; phát triển nguồn nhân lực và quản lý nhà nước về an toàn thông tin mạng. Mặc dù Luật An toàn thông tin mạng năm 2015 chưa điều chỉnh trực tiếp an ninh mạng theo nghĩa bảo vệ ANQG trên không gian mạng, nhưng đã tạo nền tảng pháp lý

quan trọng cho việc bảo vệ thông tin, hệ thống thông tin và dữ liệu trong môi trường mạng.

*Thứ hai*, về hành vi vi phạm pháp luật trong lĩnh vực an ninh mạng. Giai đoạn này ghi nhận sự mở rộng đáng kể các quy định về hành vi vi phạm pháp luật liên quan đến an ninh mạng, an toàn thông tin mạng, công nghệ thông tin và mạng viễn thông. Nghị định số 72/2013/NĐ-CP đã quy định nhiều hành vi bị nghiêm cấm trong quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng. Luật An toàn thông tin mạng năm 2015 tiếp tục bổ sung nhiều nhóm hành vi bị nghiêm cấm, trong đó có các hành vi: ngăn chặn trái pháp luật việc truyền tải thông tin trên mạng; can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép, làm sai lệch thông tin trên mạng trái pháp luật; gây ảnh hưởng hoặc cản trở trái pháp luật hoạt động bình thường của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin; phát tán thư rác, phần mềm độc hại; thiết lập hệ thống thông tin giả mạo, lừa đảo; thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác.

Bên cạnh đó, Bộ luật Hình sự năm 2015, được sửa đổi, bổ sung năm 2017, đã quy định cụ thể hơn nhóm tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông tại Mục 2 Chương XXI. So với các quy định trước đây, Bộ luật này đã mở rộng phạm vi xử lý, bổ sung một số tội danh mới như tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật; tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng; tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh; tội cố ý gây nhiễu có hại. Đây là bước phát triển quan trọng trong việc hình sự hóa các hành vi nguy hiểm phát sinh trong môi trường công nghệ thông tin, mạng viễn thông.

*Thứ ba*, về địa vị pháp lý của các chủ thể có liên quan. Trong giai đoạn từ năm 2013 đến trước khi ban hành Luật An ninh mạng năm 2018, địa vị pháp

lý của các chủ thể trong lĩnh vực an toàn, an ninh thông tin mạng từng bước được xác định rõ hơn. Luật An toàn thông tin mạng năm 2015 quy định quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an toàn thông tin mạng; trách nhiệm của doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng; trách nhiệm của chủ quản hệ thống thông tin; trách nhiệm của cơ quan quản lý nhà nước trong lĩnh vực an toàn thông tin mạng. Ngoài ra, một số văn bản pháp luật khác cũng có liên quan đến việc xác định địa vị pháp lý của các chủ thể trên không gian mạng. Bộ luật Dân sự năm 2015 quy định về quyền dân sự, bảo vệ quyền nhân thân, quyền tài sản, giao dịch dân sự và trách nhiệm dân sự; Bộ luật Tố tụng hình sự năm 2015 ghi nhận dữ liệu điện tử là nguồn chứng cứ; Luật Báo chí năm 2016 và Luật Tiếp cận thông tin năm 2016 có các quy định liên quan đến quyền tiếp cận, cung cấp, sử dụng thông tin và trách nhiệm của các chủ thể trong hoạt động thông tin, truyền thông.

*Thứ tư*, về biện pháp bảo vệ an ninh mạng, an toàn thông tin mạng. Luật An toàn thông tin mạng năm 2015 đã đặt nền tảng pháp lý quan trọng cho việc thiết lập các biện pháp bảo vệ an toàn thông tin mạng. Cụ thể bao gồm: biện pháp kỹ thuật, biện pháp tổ chức - quản lý, biện pháp pháp lý và biện pháp phối hợp trong bảo vệ hệ thống thông tin, dữ liệu và dịch vụ trên mạng. Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ là văn bản có ý nghĩa quan trọng trong giai đoạn này. Nghị định đã xác lập cơ chế phân loại hệ thống thông tin theo cấp độ, từ đó đặt ra yêu cầu bảo vệ tương ứng với từng cấp độ. Cách tiếp cận này thể hiện bước chuyển từ bảo vệ thông tin theo phương thức chung sang bảo vệ theo mức độ rủi ro, mức độ quan trọng của hệ thống thông tin.

*Thứ năm*, về chế tài xử lý hành vi vi phạm. Chế tài xử lý các hành vi vi phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông và an toàn thông tin mạng được hoàn thiện đáng kể trong giai đoạn này. Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017 và năm 2025), đã quy định hệ thống tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông với cấu thành cụ thể hơn, chế tài nghiêm khắc hơn và phù hợp hơn với tính chất nguy hiểm của

các hành vi vi phạm trong môi trường số. Bộ luật Hình sự đã cụ thể hóa nhiều dấu hiệu hậu quả và tình tiết định khung tăng nặng như thu lợi bất chính, gây thiệt hại, làm lây nhiễm phương tiện điện tử hoặc hệ thống thông tin, làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc làm đình trệ hoạt động của cơ quan, tổ chức. Việc mở rộng hình phạt tiền, tăng mức phạt tiền và bổ sung hình phạt bổ sung trong một số trường hợp đã góp phần nâng cao khả năng răn đe và xử lý đối với các hành vi vi phạm trong lĩnh vực này. Bên cạnh chế tài hình sự, hệ thống chế tài hành chính trong lĩnh vực công nghệ thông tin, viễn thông, Internet, giao dịch điện tử và an toàn thông tin mạng cũng tiếp tục được hoàn thiện thông qua các nghị định xử phạt chuyên ngành. Điều này tạo cơ sở để xử lý linh hoạt các hành vi vi phạm tùy theo tính chất, mức độ nguy hiểm của hành vi.

*Thứ sáu*, về hợp tác quốc tế trong lĩnh vực an ninh mạng. Hợp tác quốc tế trong lĩnh vực an ninh mạng, giai đoạn này bước đầu được ghi nhận trong Luật An toàn thông tin mạng năm 2015. Nội dung hợp tác bao gồm trao đổi thông tin, chia sẻ kinh nghiệm, hỗ trợ đào tạo, hợp tác kỹ thuật, phối hợp xử lý sự cố an toàn thông tin mạng và phòng, chống các hành vi vi phạm trên môi trường mạng có yếu tố nước ngoài.

Có thể khẳng định rằng, giai đoạn từ năm 2013 đến trước thời điểm ban hành Luật An ninh mạng năm 2018 là giai đoạn pháp luật Việt Nam từng bước hình thành khung điều chỉnh tương đối rõ nét đối với các vấn đề liên quan đến an toàn thông tin mạng, công nghệ thông tin, mạng viễn thông và các hành vi vi phạm trên không gian mạng. Sáu nhóm nội dung cơ bản của pháp luật về an ninh mạng gồm nguyên tắc bảo vệ, hành vi vi phạm, địa vị pháp lý của chủ thể, biện pháp bảo vệ, chế tài xử lý và hợp tác quốc tế đều đã được đề cập ở những mức độ khác nhau. Tuy nhiên, pháp luật trong giai đoạn này vẫn chưa hình thành một hệ thống chuyên biệt, thống nhất về an ninh mạng. Các quy định còn phân tán trong nhiều văn bản, chủ yếu tiếp cận từ

góc độ an toàn thông tin mạng, công nghệ thông tin, viễn thông, giao dịch điện tử và xử lý tội phạm công nghệ cao.

### **3.1.3. Giai đoạn sau khi ban hành Luật An ninh mạng 2018 đến hiện nay**

Giai đoạn từ khi Luật An ninh mạng năm 2018 được ban hành đến nay là giai đoạn pháp luật về an ninh mạng ở Việt Nam có bước phát triển rõ nét theo hướng chuyên biệt, đầy đủ và có tính hệ thống hơn. Nếu ở giai đoạn trước, các quy định liên quan đến an ninh mạng chủ yếu phân tán trong pháp luật về công nghệ thông tin, viễn thông, giao dịch điện tử, an toàn thông tin mạng và pháp luật hình sự, thì từ năm 2018, Luật An ninh mạng đã trở thành văn bản trung tâm điều chỉnh trực tiếp hoạt động bảo vệ ANQG, TTATXH trên không gian mạng; đồng thời quy định trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

Sự ra đời của Luật An ninh mạng năm 2018 đã đánh dấu bước chuyển quan trọng trong tư duy pháp lý về an ninh mạng ở Việt Nam. An ninh mạng không còn chỉ được tiếp cận như vấn đề kỹ thuật hoặc an toàn thông tin, mà được xác định là lĩnh vực pháp luật gắn trực tiếp với bảo vệ ANQG, TTATXH, bảo vệ hệ thống thông tin quan trọng, dữ liệu, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng. Trên cơ sở Luật An ninh mạng năm 2018, nhiều văn bản pháp luật có liên quan tiếp tục được ban hành, sửa đổi, bổ sung, tạo thành khung pháp lý ngày càng đầy đủ hơn cho lĩnh vực an ninh mạng.

Có thể đánh giá sự phát triển của pháp luật về an ninh mạng trong giai đoạn này theo sáu nhóm chế định cơ bản như sau:

*Thứ nhất*, về nguyên tắc bảo vệ an ninh mạng. Luật An ninh mạng năm 2018 đã xác lập các nguyên tắc cơ bản trong hoạt động bảo vệ an ninh mạng, trong đó nhấn mạnh yêu cầu bảo vệ ANQG, TTATXH trên không gian mạng; kết hợp giữa phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng; bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. So với giai đoạn trước, các nguyên tắc bảo vệ an ninh mạng đã được

thể hiện rõ hơn, có tính định hướng trực tiếp hơn đối với hoạt động xây dựng, áp dụng và thực thi pháp luật trong lĩnh vực này.

*Thứ hai*, về hành vi vi phạm pháp luật về an ninh mạng. Luật An ninh mạng năm 2018 đã quy định tương đối toàn diện các nhóm hành vi bị nghiêm cấm trên không gian mạng. Các hành vi này bao gồm việc sử dụng không gian mạng để xâm phạm ANQG, TTATXH; phát tán thông tin sai sự thật; xâm phạm bí mật nhà nước, bí mật cá nhân, bí mật gia đình, bí mật kinh doanh; tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; phá hoại hệ thống thông tin quan trọng về ANQG; cản trở hoạt động của lực lượng bảo vệ an ninh mạng hoặc lợi dụng hoạt động bảo vệ an ninh mạng để vi phạm pháp luật.

Bên cạnh Luật An ninh mạng năm 2018, các luật chuyên ngành khác cũng tiếp tục bổ sung nhiều quy định có liên quan đến hành vi vi phạm trên không gian mạng. Luật Bảo vệ bí mật nhà nước năm 2018 quy định các hành vi bị nghiêm cấm liên quan đến làm lộ, chiếm đoạt, mua bán, truyền đưa, đăng tải bí mật nhà nước trên mạng Internet, mạng máy tính, mạng viễn thông. Luật Giao dịch điện tử năm 2023 quy định các hành vi như giả mạo, làm sai lệch, xóa, hủy, sao chép, di chuyển trái pháp luật thông điệp dữ liệu; gian lận, giả mạo, chiếm đoạt hoặc sử dụng trái pháp luật tài khoản giao dịch điện tử, chứng thư điện tử, chữ ký điện tử. Luật Viễn thông năm 2023 quy định các hành vi như thu trộm, nghe trộm, xem trộm thông tin trên mạng viễn thông; trộm cắp, sử dụng trái phép tài nguyên viễn thông, mật khẩu, khóa mật mã và thông tin riêng của tổ chức, cá nhân.

*Thứ ba*, về chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng. Giai đoạn sau năm 2018, chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng được hoàn thiện ở nhiều cấp độ. Tùy theo tính chất, mức độ vi phạm, chủ thể vi phạm có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, truy cứu trách nhiệm hình sự, buộc bồi thường thiệt hại hoặc áp dụng các biện pháp khắc phục hậu quả theo quy định của pháp luật. Luật Xử lý vi phạm hành

chính được sửa đổi, bổ sung năm 2020 và năm 2025 đã tiếp tục hoàn thiện cơ sở pháp lý cho việc xử phạt vi phạm hành chính trong các lĩnh vực có liên quan như công nghệ thông tin, viễn thông, tần số vô tuyến điện, an ninh mạng, an toàn thông tin mạng, giao dịch điện tử, thương mại điện tử. Nghị định số 15/2020/NĐ-CP của Chính phủ 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 đã quy định cụ thể nhiều hành vi vi phạm và mức xử phạt tương ứng. Ở phương diện hình sự Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017 và năm 2025) tiếp tục là cơ sở pháp lý quan trọng để xử lý các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông cùng với các hành vi sử dụng không gian mạng để thực hiện tội phạm. Bộ luật Tố tụng hình sự cũng đã ghi nhận dữ liệu điện tử là nguồn chứng cứ, tạo cơ sở pháp lý cho việc thu thập, kiểm tra, đánh giá và sử dụng chứng cứ điện tử trong quá trình giải quyết vụ án.

*Thứ tư*, về địa vị pháp lý của các chủ thể trong lĩnh vực an ninh mạng. Luật An ninh mạng năm 2018 đã quy định tương đối rõ trách nhiệm của các chủ thể tham gia hoạt động bảo vệ an ninh mạng. Các chủ thể này bao gồm cơ quan nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng, cơ quan, tổ chức, doanh nghiệp cung cấp dịch vụ trên không gian mạng, chủ quản hệ thống thông tin và cá nhân sử dụng không gian mạng. Tại Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng đã tiếp tục cụ thể hóa một số nội dung liên quan đến lực lượng chuyên trách bảo vệ an ninh mạng, trách nhiệm của cơ quan, tổ chức, doanh nghiệp trong việc phối hợp bảo vệ an ninh mạng. Qua đó, địa vị pháp lý của các chủ thể trong lĩnh vực an ninh mạng được xác định rõ hơn, tạo cơ sở cho hoạt động phối hợp, phân công trách nhiệm và tổ chức thực thi pháp luật về an ninh mạng.

*Thứ năm*, về biện pháp bảo vệ an ninh mạng. Luật An ninh mạng năm 2018 đã quy định hệ thống biện pháp bảo vệ an ninh mạng tương đối toàn diện, bao gồm thẩm định an ninh mạng, đánh giá điều kiện an ninh mạng,

kiểm tra an ninh mạng, giám sát an ninh mạng, ứng phó, khắc phục sự cố an ninh mạng, đấu tranh bảo vệ an ninh mạng, sử dụng mật mã để bảo vệ thông tin mạng và các biện pháp quản lý nhà nước khác theo quy định của pháp luật. Nghị định số 04/2019/NĐ-CP ngày 27/12/2019 của Chính phủ quy định chi tiết về trình tự, thủ tục áp dụng một số biện pháp bảo vệ an toàn, an ninh mạng và Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng đã cụ thể hóa thêm một số biện pháp như yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng; thu thập dữ liệu điện tử liên quan đến hành vi xâm phạm ANQG, TTATXH; trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng. Tuy nhiên, do các biện pháp này có thể tác động đến quyền, lợi ích hợp pháp của cá nhân, tổ chức, pháp luật cần tiếp tục hoàn thiện theo hướng quy định rõ hơn về căn cứ áp dụng, điều kiện áp dụng, thẩm quyền, trình tự, thủ tục, thời hạn, phạm vi áp dụng, trách nhiệm giải trình và cơ chế khiếu nại, giám sát.

*Thứ sáu*, về hợp tác quốc tế trong lĩnh vực an ninh mạng. Luật An ninh mạng năm 2018 đã quy định nguyên tắc và nội dung hợp tác quốc tế trong lĩnh vực an ninh mạng. Nội dung hợp tác bao gồm nghiên cứu, phân tích xu hướng an ninh mạng; xây dựng cơ chế, chính sách hợp tác; chia sẻ thông tin, kinh nghiệm; hỗ trợ đào tạo, trang thiết bị, công nghệ bảo vệ an ninh mạng; phòng, chống tội phạm mạng; ngăn ngừa nguy cơ đe dọa an ninh mạng; ký kết và thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng.

Có thể khẳng định rằng, giai đoạn sau khi ban hành Luật An ninh mạng năm 2018 đến nay là giai đoạn pháp luật về an ninh mạng ở Việt Nam phát triển mạnh mẽ cả về phạm vi điều chỉnh, cấu trúc chế định và cơ chế thực thi. Sáu nhóm chế định cơ bản của pháp luật về an ninh mạng gồm nguyên tắc bảo vệ, hành vi vi phạm, chế tài xử lý, địa vị pháp lý của chủ thể, biện pháp bảo vệ và hợp tác quốc tế đều đã được thể hiện tương đối rõ nét.

Năm 2025, việc Quốc hội thông qua Luật An ninh mạng số 116/2025/QH15 đã đánh dấu bước phát triển mới trong quá trình hoàn thiện

pháp luật về an ninh mạng, hướng tới một khuôn khổ pháp lý thống nhất, đồng bộ hơn giữa an ninh mạng, an toàn thông tin mạng, an ninh dữ liệu và bảo vệ quyền, lợi ích hợp pháp của các chủ thể trên không gian mạng. Sự ra đời của Luật An ninh mạng năm 2025 cho thấy pháp luật về an ninh mạng ở Việt Nam đã chuyển sang giai đoạn phát triển mới, theo hướng bao quát hơn, hệ thống hơn và gắn chặt hơn với yêu cầu quản trị không gian mạng trong bối cảnh chuyển đổi số. Nếu Luật An ninh mạng năm 2018 là đạo luật chuyên biệt đầu tiên đặt nền tảng pháp lý cho hoạt động bảo vệ ANQG, TTATXH trên không gian mạng, thì Luật An ninh mạng năm 2025 tiếp tục mở rộng, cập nhật và làm rõ hơn khuôn khổ pháp lý về an ninh mạng, bảo vệ an ninh mạng, quyền, nghĩa vụ và trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Xét theo sáu nhóm chế định nghiên cứu, Luật An ninh mạng năm 2025 có ý nghĩa bổ sung quan trọng. Từ đó có thể đánh giá rằng, Luật An ninh mạng năm 2025 không làm mất đi ý nghĩa của việc nghiên cứu hoàn thiện pháp luật về an ninh mạng, mà trái lại càng làm nổi bật yêu cầu nghiên cứu này ở cấp độ cao hơn. Bởi lẽ, khi một đạo luật mới được ban hành, nhiệm vụ khoa học không chỉ là ghi nhận sự ra đời của văn bản, mà còn phải tiếp tục đánh giá mức độ đầy đủ, đồng bộ, minh bạch, khả thi của các quy định mới; xác định mối quan hệ giữa Luật An ninh mạng năm 2025 với pháp luật về dữ liệu, an ninh dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, hình sự, tố tụng hình sự và hợp tác quốc tế; đồng thời làm rõ điều kiện bảo đảm thi hành luật trong thực tiễn.

### **3.2. ĐÁNH GIÁ THỰC TRẠNG PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM HIỆN NAY**

#### **3.2.1. Những ưu điểm và nguyên nhân ưu điểm của pháp luật về an ninh mạng ở Việt Nam**

##### ***3.2.1.1. Những ưu điểm của pháp luật về an ninh mạng ở Việt Nam***

##### ***- Những ưu điểm trong nhóm quy định nguyên tắc bảo vệ an ninh mạng***

Nhóm quy định về nguyên tắc bảo vệ an ninh mạng giữ vai trò nền tảng, định hướng cho toàn bộ hoạt động xây dựng, áp dụng và tổ chức thực

hiện pháp luật về an ninh mạng. Trên cơ sở các tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, những ưu điểm chủ yếu của nhóm quy định này nổi bật như sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, các quy định về nguyên tắc bảo vệ an ninh mạng đã bước đầu bảo đảm tính đầy đủ, tính đồng bộ, khả năng thích ứng với công nghệ và yêu cầu bảo vệ quyền, lợi ích hợp pháp của các chủ thể trên không gian mạng. Luật An ninh mạng năm 2018 đã xác lập các nguyên tắc cơ bản cho hoạt động bảo vệ an ninh mạng, như bảo vệ ANQG, bảo đảm TTATXH; kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng với phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân; phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời các hành vi xâm phạm an ninh mạng. Các nguyên tắc này không chỉ tạo cơ sở cho việc xây dựng các quy định cụ thể về hành vi vi phạm, biện pháp bảo vệ và chế tài xử lý mà còn góp phần kết nối pháp luật về an ninh mạng với các lĩnh vực pháp luật có liên quan như an toàn thông tin mạng, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử và pháp luật hình sự. Đồng thời, việc đề cao yêu cầu phòng ngừa, quản trị rủi ro và bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân cho thấy pháp luật đã bước đầu thích ứng với đặc thù của môi trường số và yêu cầu chuyển đổi số quốc gia.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, các nguyên tắc bảo vệ an ninh mạng được quy định trực tiếp trong Luật An ninh mạng năm 2018 với nội dung tương đối khái quát, ổn định và có tính định hướng cao. Cách thức thiết kế này góp phần bảo đảm tính minh bạch và tính thống nhất trong áp dụng pháp luật, đồng thời tạo cơ sở để giải thích và vận dụng pháp luật đối với những vấn đề mới phát sinh trên không gian mạng mà các quy định cụ thể chưa dự liệu đầy đủ. Việc ghi nhận các nguyên tắc trong đạo luật chuyên ngành cũng góp phần nâng cao tính hệ thống của pháp luật về an ninh mạng, bảo đảm sự liên kết giữa các chế định và hạn chế nguy cơ áp dụng pháp luật tùy nghi trong thực tiễn.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, các nguyên tắc bảo vệ an ninh mạng đã tạo cơ sở pháp lý cho việc xác định trách nhiệm và cơ chế phối hợp giữa các chủ thể tham gia bảo vệ an ninh mạng. Trên cơ sở các nguyên tắc này, pháp luật đã từng bước xác định vai trò của lực lượng chuyên trách bảo vệ an ninh mạng, các cơ quan quản lý nhà nước, chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên không gian mạng và người sử dụng không gian mạng. Đây là tiền đề quan trọng để triển khai các hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm và ứng phó với các nguy cơ, sự cố an ninh mạng trong thực tiễn. Đồng thời, các nguyên tắc này cũng tạo cơ sở cho việc huy động nguồn lực xã hội, tăng cường phối hợp liên ngành và mở rộng hợp tác quốc tế trong bảo vệ an ninh mạng.

Nhìn chung, nhóm quy định về nguyên tắc bảo vệ an ninh mạng đã tạo nền tảng pháp lý quan trọng cho việc xây dựng và vận hành hệ thống pháp luật về an ninh mạng ở Việt Nam. Các quy định này không chỉ định hướng cho hoạt động bảo vệ ANQG trên không gian mạng mà còn góp phần bảo đảm tính thống nhất, minh bạch và hiệu quả trong quá trình tổ chức thực hiện pháp luật về an ninh mạng.

***- Những ưu điểm trong nhóm quy định hành vi vi phạm pháp luật về an ninh mạng***

Nhóm quy định về hành vi vi phạm pháp luật về an ninh mạng giữ vị trí trung tâm trong hệ thống pháp luật về an ninh mạng, bởi đây là cơ sở để xác định ranh giới giữa hành vi hợp pháp và hành vi bị cấm trên không gian mạng; đồng thời là tiền đề để áp dụng chế tài, biện pháp bảo vệ an ninh mạng và cơ chế bảo vệ quyền, lợi ích hợp pháp của các chủ thể bị xâm phạm. Trên cơ sở ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, có thể nhận diện những ưu điểm chủ yếu của nhóm quy định này như sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, pháp luật hiện hành đã từng bước nhận diện tương đối toàn diện các nhóm hành vi vi phạm cơ bản trên không gian mạng. Luật An ninh mạng năm 2018 đã quy định

nhiều hành vi bị nghiêm cấm như sử dụng không gian mạng để xâm phạm ANQG, TTATXH; thông tin sai sự thật; xâm phạm quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; xâm nhập, chiếm quyền điều khiển, làm gián đoạn hoặc phá hoại hệ thống thông tin quan trọng về ANQG. Bên cạnh đó, Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017 đã hình sự hóa nhiều hành vi nguy hiểm trong lĩnh vực công nghệ thông tin, mạng viễn thông và phương tiện điện tử; còn Nghị định số 15/2020/NĐ-CP, được sửa đổi, bổ sung bởi Nghị định số 14/2022/NĐ-CP, đã tạo cơ sở xử phạt hành chính đối với nhiều hành vi vi phạm chưa đến mức truy cứu trách nhiệm hình sự. Đặc biệt, Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân tiếp tục bổ sung cơ sở pháp lý để nhận diện, phòng ngừa và xử lý hành vi thu thập, chuyển giao, mua bán trái phép dữ liệu cá nhân trong môi trường số.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, các hành vi vi phạm pháp luật về an ninh mạng đã từng bước được mô tả cụ thể, rõ ràng hơn. Pháp luật không chỉ sử dụng các khái niệm khái quát như “xâm phạm an ninh mạng”, mà đã cụ thể hóa thành các hành vi như tấn công mạng, phát tán mã độc, xâm nhập trái phép hệ thống thông tin, chiếm đoạt dữ liệu, đưa thông tin sai sự thật, xâm phạm bí mật nhà nước, xâm phạm bí mật cá nhân, sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để chiếm đoạt tài sản. Việc quy định các hành vi vi phạm ở nhiều cấp độ văn bản khác nhau, từ luật đến nghị định xử phạt vi phạm hành chính, tạo điều kiện phân tầng trách nhiệm pháp lý tương ứng với tính chất, mức độ nguy hiểm của hành vi.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, việc pháp luật nhận diện tương đối rõ các nhóm hành vi vi phạm đã tạo cơ sở quan trọng cho hoạt động phòng ngừa, phát hiện, ngăn chặn và xử lý hành vi xâm phạm an ninh mạng. Cơ quan có thẩm quyền có căn cứ để lựa chọn biện pháp xử lý phù hợp như xử phạt vi phạm hành chính, truy cứu trách nhiệm hình sự, yêu cầu gỡ bỏ thông tin vi phạm, thu thập dữ liệu điện tử, áp dụng biện pháp bảo vệ hệ thống

thông tin hoặc phối hợp với doanh nghiệp cung cấp dịch vụ trên không gian mạng. Đồng thời, nhóm quy định này góp phần bảo vệ quyền và lợi ích hợp pháp của cá nhân, tổ chức trước các hành vi xâm phạm dữ liệu cá nhân, bí mật đời tư, danh dự, uy tín, tài sản, bí mật kinh doanh và các quyền, lợi ích hợp pháp khác trên không gian mạng.

Nhìn chung, nhóm quy định về hành vi vi phạm pháp luật về an ninh mạng đã tạo lập cơ sở pháp lý quan trọng để nhận diện, phân loại và xử lý các hành vi xâm phạm trên không gian mạng, qua đó góp phần bảo vệ ANQG, TTATXH, đồng thời bảo vệ quyền con người, quyền công dân và quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trong bối cảnh chuyển đổi số.

***- Những ưu điểm trong nhóm quy định chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng***

Chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng là công cụ pháp lý bảo đảm cho các quy định về an ninh mạng được thực hiện nghiêm minh trong thực tiễn. Nếu nhóm quy định về hành vi vi phạm xác định ranh giới giữa hành vi hợp pháp và hành vi bị cấm, thì nhóm quy định về chế tài xác định hậu quả pháp lý bất lợi mà chủ thể vi phạm phải gánh chịu. Trên cơ sở ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, có thể nhận diện những ưu điểm chủ yếu của nhóm quy định này như sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, pháp luật hiện hành đã bước đầu thiết lập được hệ thống chế tài tương đối đa dạng, phù hợp với tính chất, mức độ nguy hiểm của hành vi vi phạm. Chủ thể vi phạm có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, truy cứu trách nhiệm hình sự, buộc bồi thường thiệt hại hoặc áp dụng các biện pháp khắc phục hậu quả. Luật an ninh mạng năm 2018 đặt cơ sở cho việc xử lý nghiêm minh hành vi vi phạm, bao gồm các biện pháp như xóa bỏ thông tin vi phạm, ngăn chặn, tạm ngừng, đình chỉ hoạt động hoặc xử lý theo quy định pháp luật. Nghị định số 15/2020/NĐ-CP quy định chế tài hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin, an toàn thông tin mạng và giao dịch điện tử; Bộ

luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017 quy định các tội phạm liên quan đến công nghệ thông tin, mạng viễn thông, phương tiện điện tử. Qua đó, pháp luật đã hình thành cơ chế chế tài đa tầng, kết hợp giữa xử lý hành chính, hình sự, dân sự và khắc phục hậu quả.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, các quy định về chế tài đã bước đầu được thiết kế rõ hơn về hình thức xử lý, mức xử lý, thẩm quyền áp dụng và hậu quả pháp lý. Trong xử phạt vi phạm hành chính, pháp luật phân biệt giữa hình thức xử phạt chính, hình thức xử phạt bổ sung và biện pháp khắc phục hậu quả; đồng thời quy định mức phạt khác nhau đối với cá nhân và tổ chức. Nghị định số 15/2020/NĐ-CP quy định các hình thức xử phạt như cảnh cáo, phạt tiền, tịch thu tang vật, phương tiện vi phạm, đình chỉ hoạt động có thời hạn, buộc gỡ bỏ thông tin sai sự thật hoặc thông tin vi phạm pháp luật. Đối với trách nhiệm hình sự, Bộ luật Hình sự quy định cấu thành tội phạm và khung hình phạt tương ứng, tạo cơ sở phân hóa trách nhiệm pháp lý theo tính chất, mức độ nguy hiểm của hành vi. Cách thiết kế này góp phần nâng cao tính minh bạch, tính dự báo và khả năng áp dụng thống nhất của pháp luật.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, nhóm quy định về chế tài đã tạo cơ sở pháp lý quan trọng cho hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý và khắc phục hậu quả của hành vi xâm phạm an ninh mạng. Đối với hành vi chưa đến mức truy cứu trách nhiệm hình sự, cơ quan có thẩm quyền có thể áp dụng chế tài hành chính theo Nghị định số 15/2020/NĐ-CP; đối với hành vi có tính chất nguy hiểm cao như xâm nhập trái phép hệ thống thông tin, phát tán mã độc, chiếm đoạt tài sản qua mạng hoặc mua bán trái phép thông tin tài khoản ngân hàng, có thể xem xét truy cứu trách nhiệm hình sự theo Bộ luật Hình sự. Các biện pháp như buộc gỡ bỏ thông tin vi phạm, buộc cải chính thông tin, buộc khôi phục tình trạng ban đầu hoặc bồi thường thiệt hại cũng góp phần bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức bị xâm phạm trên không gian mạng. Đặc biệt, Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân đã bổ sung cơ sở pháp lý quan

trọng cho việc xử lý hành vi vi phạm liên quan đến thu thập, xử lý, chuyển giao và bảo vệ dữ liệu cá nhân.

Nhìn chung, nhóm quy định về chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng đã tạo lập cơ sở pháp lý quan trọng để bảo đảm hiệu lực, hiệu quả của pháp luật về an ninh mạng. Các chế tài hiện hành không chỉ có ý nghĩa trừng phạt, răn đe mà còn góp phần phòng ngừa, khắc phục hậu quả và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức trong môi trường số.

***- Những ưu điểm trong nhóm quy định địa vị pháp lý của các chủ thể tham gia hoạt động trong lĩnh vực an ninh mạng***

Nhóm quy định về địa vị pháp lý của các chủ thể tham gia hoạt động trong lĩnh vực an ninh mạng có vai trò quan trọng trong việc xác định vị trí, quyền, nghĩa vụ, trách nhiệm, thẩm quyền và cơ chế phối hợp giữa các chủ thể trong bảo vệ an ninh mạng. Trên cơ sở ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, có thể nhận diện những ưu điểm chủ yếu của nhóm quy định này như sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, pháp luật về an ninh mạng đã từng bước xác lập tương đối đầy đủ các nhóm chủ thể tham gia bảo vệ an ninh mạng. Luật An ninh mạng năm 2018 và Luật An ninh mạng năm 2025 đã ghi nhận các chủ thể cơ bản như cơ quan quản lý nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng, chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên không gian mạng, tổ chức xử lý dữ liệu và cá nhân, tổ chức sử dụng không gian mạng. Các quy định này có sự liên kết với pháp luật về viễn thông, công nghệ thông tin, giao dịch điện tử, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước và xử lý vi phạm hành chính; đồng thời phản ánh xu hướng mở rộng trách nhiệm bảo vệ an ninh mạng từ khu vực nhà nước sang toàn xã hội.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, pháp luật đã từng bước phân định rõ hơn quyền, nghĩa vụ, trách nhiệm và thẩm quyền của từng nhóm chủ thể. Luật An ninh mạng năm 2018 quy định trách nhiệm của cơ

quan, tổ chức, cá nhân; doanh nghiệp cung cấp dịch vụ trên không gian mạng; chủ quản hệ thống thông tin và lực lượng chuyên trách bảo vệ an ninh mạng. Việc phân định trách nhiệm theo từng nhóm chủ thể giúp hạn chế cách quy định chung chung, khó áp dụng; đồng thời tạo cơ sở xác định trách nhiệm pháp lý khi xảy ra vi phạm hoặc sự cố an ninh mạng, góp phần nâng cao tính minh bạch và khả năng dự báo của pháp luật.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, nhóm quy định này đã tạo cơ sở cho cơ chế phối hợp đa chủ thể trong bảo vệ an ninh mạng. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và Bộ Quốc phòng giữ vai trò nòng cốt; các bộ, ngành, địa phương, chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên không gian mạng, tổ chức và cá nhân có trách nhiệm phối hợp trong phòng ngừa, phát hiện, ngăn chặn và xử lý hành vi vi phạm pháp luật về an ninh mạng. Đồng thời, pháp luật từng bước xác lập cơ chế huy động tổ chức, cá nhân tham gia bảo vệ an ninh mạng, qua đó phát huy nguồn lực xã hội trong bảo vệ ANQG trên không gian mạng.

Bên cạnh đó, pháp luật không chỉ xác định cá nhân, tổ chức là chủ thể có nghĩa vụ tuân thủ mà còn là chủ thể được bảo vệ trước các hành vi xâm phạm dữ liệu cá nhân, bí mật đời tư, danh dự, nhân phẩm, uy tín, tài sản, bí mật kinh doanh và các quyền, lợi ích hợp pháp khác. Điều này góp phần bảo đảm sự cân bằng giữa yêu cầu bảo vệ ANQG với bảo vệ quyền con người, quyền công dân trong môi trường số.

Nhìn chung, nhóm quy định về địa vị pháp lý của các chủ thể tham gia hoạt động trong lĩnh vực an ninh mạng đã tạo lập cơ sở pháp lý quan trọng cho việc xác định trách nhiệm, thẩm quyền và cơ chế phối hợp giữa các chủ thể có liên quan; qua đó góp phần nâng cao hiệu quả thực thi pháp luật về an ninh mạng trong bối cảnh chuyển đổi số hiện nay.

#### ***- Những ưu điểm trong nhóm quy định biện pháp bảo vệ an ninh mạng***

Nhóm quy định về biện pháp bảo vệ an ninh mạng có vai trò xác lập các công cụ pháp lý để phòng ngừa, phát hiện, ngăn chặn, xử lý và khắc phục

các nguy cơ, sự cố, hành vi xâm phạm an ninh mạng. Trên cơ sở ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, có thể nhận diện những ưu điểm chủ yếu của nhóm quy định này như sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, pháp luật về an ninh mạng đã bước đầu thiết lập được hệ thống biện pháp bảo vệ tương đối toàn diện, bao quát nhiều giai đoạn của quá trình bảo vệ an ninh mạng. Luật An ninh mạng năm 2018 đã quy định các biện pháp như thẩm định an ninh mạng, đánh giá điều kiện an ninh mạng, kiểm tra, giám sát, ứng phó, khắc phục sự cố, đấu tranh bảo vệ an ninh mạng và sử dụng mật mã để bảo vệ thông tin mạng. Các biện pháp này phản ánh chu trình bảo vệ an ninh mạng từ phòng ngừa, phát hiện, cảnh báo, ngăn chặn đến xử lý và khắc phục hậu quả. Đồng thời, nhóm quy định này có sự gắn kết với pháp luật về an toàn thông tin mạng, viễn thông, giao dịch điện tử, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước, xử lý vi phạm hành chính, hình sự và tố tụng hình sự, qua đó bước đầu bảo đảm tính đầy đủ, tính đồng bộ và khả năng thích ứng với đặc thù kỹ thuật của lĩnh vực an ninh mạng.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, các biện pháp bảo vệ an ninh mạng đã được quy định thành những nhóm tương đối rõ ràng, có tên gọi, mục đích và phạm vi áp dụng khác nhau. Việc phân định các biện pháp như thẩm định, đánh giá điều kiện, kiểm tra, giám sát, ứng phó sự cố, khắc phục sự cố và đấu tranh bảo vệ an ninh mạng giúp cơ quan có thẩm quyền xác định căn cứ, mục đích và phương thức áp dụng từng biện pháp; đồng thời giúp cơ quan, tổ chức, doanh nghiệp và cá nhân nhận diện trách nhiệm pháp lý của mình khi tham gia hoặc chịu tác động bởi hoạt động bảo vệ an ninh mạng. Cách thiết kế theo nhóm chức năng cũng làm rõ mối liên hệ giữa biện pháp phòng ngừa, kiểm soát rủi ro, xử lý sự cố và khắc phục hậu quả.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, các quy định về biện pháp bảo vệ an ninh mạng đã tạo cơ sở pháp lý cho việc tổ chức thực hiện nhiệm vụ bảo vệ an ninh mạng trong thực tiễn. Luật An ninh mạng năm 2018

gắn các biện pháp bảo vệ với vai trò của lực lượng chuyên trách bảo vệ an ninh mạng, chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên không gian mạng và các cơ quan, tổ chức, cá nhân có liên quan. Đây là cơ sở để triển khai hoạt động kiểm tra, giám sát, cảnh báo, ứng phó, khắc phục sự cố và phối hợp xử lý tình huống nguy hiểm về an ninh mạng. Các biện pháp này không chỉ nhằm bảo vệ ANQG, TTATXH mà còn góp phần bảo vệ hệ thống thông tin, dữ liệu, hoạt động bình thường của cơ quan, tổ chức, doanh nghiệp và quyền, lợi ích hợp pháp của cá nhân trên không gian mạng.

Nhìn chung, nhóm quy định về biện pháp bảo vệ an ninh mạng đã tạo lập cơ sở pháp lý quan trọng cho việc phòng ngừa, phát hiện, ngăn chặn, xử lý và khắc phục các nguy cơ, sự cố, hành vi xâm phạm an ninh mạng. Các quy định này thể hiện sự chuyển biến từ tư duy xử lý sau vi phạm sang tư duy phòng ngừa, cảnh báo sớm và quản trị rủi ro, góp phần nâng cao hiệu quả bảo vệ ANQG, hệ thống thông tin, dữ liệu và quyền, lợi ích hợp pháp của các chủ thể trong bối cảnh chuyển đổi số.

***- Những ưu điểm trong nhóm quy định hợp tác quốc tế về an ninh mạng***

Hợp tác quốc tế về an ninh mạng có ý nghĩa quan trọng trong bối cảnh các hành vi xâm phạm an ninh mạng thường có yếu tố xuyên biên giới, liên quan đến máy chủ, dữ liệu, tài khoản, chứng cứ điện tử, dòng tiền và chủ thể vi phạm ở nhiều quốc gia, vùng lãnh thổ khác nhau. Trên cơ sở ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, có thể nhận diện những ưu điểm chủ yếu của nhóm quy định này như sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, pháp luật về an ninh mạng đã bước đầu ghi nhận tương đối đầy đủ nội dung hợp tác quốc tế. Luật An ninh mạng năm 2018 xác định hợp tác quốc tế là một nội dung quan trọng trong bảo vệ an ninh mạng, bao gồm trao đổi thông tin, chia sẻ kinh nghiệm, đào tạo, nghiên cứu, ứng dụng khoa học công nghệ, phòng, chống tội phạm mạng, ngăn ngừa nguy cơ đe dọa an ninh mạng, tham gia điều ước quốc tế, thỏa thuận quốc tế và triển khai các chương trình, dự án hợp tác

quốc tế. Nhóm quy định này cũng có sự liên kết với pháp luật hình sự, tố tụng hình sự, tương trợ tư pháp, dẫn độ, viễn thông, giao dịch điện tử, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước và an toàn thông tin mạng, qua đó bước đầu đáp ứng yêu cầu xử lý các vụ việc an ninh mạng có yếu tố nước ngoài.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, pháp luật đã bước đầu xác lập nguyên tắc, nội dung và trách nhiệm hợp tác quốc tế trong lĩnh vực an ninh mạng theo hướng tương đối rõ ràng. Hợp tác quốc tế về an ninh mạng được đặt trên cơ sở tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng, cùng có lợi, phù hợp với pháp luật Việt Nam và điều ước quốc tế mà Việt Nam là thành viên. Việc quy định hợp tác quốc tế thành một nội dung riêng trong pháp luật về an ninh mạng giúp làm rõ phạm vi, định hướng điều chỉnh và tạo cơ sở để các cơ quan có thẩm quyền vận dụng trong từng tình huống cụ thể.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, các quy định về hợp tác quốc tế đã tạo cơ sở pháp lý cho việc nâng cao năng lực phòng ngừa, phát hiện, điều tra, xử lý và khắc phục hậu quả của các hành vi xâm phạm an ninh mạng có yếu tố nước ngoài. Pháp luật đã bước đầu phân định trách nhiệm của các cơ quan có liên quan như Bộ Công an, Bộ Quốc phòng, Bộ Ngoại giao và các bộ, ngành, địa phương trong hoạt động hợp tác quốc tế về an ninh mạng theo chức năng, nhiệm vụ, quyền hạn được giao. Đồng thời, việc đặt hoạt động hợp tác trong khuôn khổ tôn trọng chủ quyền quốc gia, phù hợp với pháp luật Việt Nam và điều ước quốc tế góp phần bảo đảm ANQG, bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức khi chia sẻ dữ liệu, thông tin người dùng, chứng cứ điện tử hoặc thông tin thuộc bí mật nhà nước.

Nhìn chung, nhóm quy định về hợp tác quốc tế trong lĩnh vực an ninh mạng đã tạo lập cơ sở pháp lý quan trọng để Việt Nam tham gia, phối hợp và xử lý các vấn đề an ninh mạng có yếu tố xuyên biên giới. Các quy định này góp phần tăng cường chia sẻ thông tin, kinh nghiệm, công nghệ, nguồn lực và

nâng cao hiệu quả bảo vệ ANQG, quyền và lợi ích hợp pháp của cá nhân, tổ chức trong bối cảnh chuyển đổi số và hội nhập quốc tế.

### ***3.2.1.2. Nguyên nhân của những ưu điểm trong pháp luật về an ninh mạng ở Việt Nam***

Những ưu điểm của pháp luật về an ninh mạng hiện hành không hình thành tự phát mà là kết quả tất yếu của quá trình nhận thức và hoàn thiện thể chế qua nhiều giai đoạn.

*Thứ nhất*, xuất phát từ sự đổi mới tư duy chiến lược của Đảng và Nhà nước, coi an ninh mạng không chỉ là vấn đề kỹ thuật đơn thuần mà là yếu tố cốt lõi của ANQG, chủ quyền số và quản trị quốc gia trong kỷ nguyên chuyển đổi số.

*Thứ hai*, sự gia tăng phức tạp của tội phạm công nghệ cao và các nguy cơ trên không gian mạng đã tạo áp lực thực tiễn, buộc công tác lập pháp phải liên tục cập nhật, chuyên biệt hóa các quy định từ quản lý kỹ thuật đơn thuần như tại Luật An toàn thông tin mạng 2015 sang bảo vệ an ninh toàn diện tại Luật An ninh mạng 2025.

*Thứ ba*, việc chủ động hội nhập quốc tế và đề cao quyền con người đã thúc đẩy pháp luật an ninh mạng Việt Nam tiệm cận các chuẩn mực chung, bảo đảm sự cân bằng giữa yêu cầu bảo vệ nghiêm ngặt ANQG với việc tôn trọng quyền riêng tư, bảo vệ dữ liệu cá nhân và kiến tạo môi trường thuận lợi cho đổi mới sáng tạo, kinh tế số.

Như vậy, những ưu điểm của pháp luật về an ninh mạng ở Việt Nam bắt nguồn từ sự kết hợp giữa yêu cầu chính trị - pháp lý, nhu cầu thực tiễn bảo vệ ANQG, quá trình chuyển đổi số, sự phát triển của khoa học - công nghệ, yêu cầu bảo vệ quyền con người, quyền công dân và xu hướng hội nhập quốc tế. Các nguyên nhân này đã góp phần làm cho pháp luật về an ninh mạng ở Việt Nam từng bước phát triển theo hướng đầy đủ hơn, đồng bộ hơn, khả thi hơn và phù hợp hơn với yêu cầu bảo vệ, quản lý, phát triển không gian mạng trong kỷ nguyên số.

### **3.2.2. Những tồn tại, bất cập và nguyên nhân tồn tại, bất cập của pháp luật về an ninh mạng ở Việt Nam**

#### ***3.2.2. 1. Những tồn tại, bất cập của pháp luật về an ninh mạng ở Việt Nam***

##### ***- Tồn tại, bất cập trong nhóm quy định về nguyên tắc bảo vệ an ninh mạng***

Xét theo ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật, nhóm quy định về nguyên tắc bảo vệ an ninh mạng vẫn còn một số tồn tại, bất cập chủ yếu sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, hệ thống nguyên tắc bảo vệ an ninh mạng hiện hành chưa bao quát đầy đủ các yêu cầu đặc thù của quản trị an ninh mạng trong bối cảnh chuyển đổi số. Luật An ninh mạng năm 2018 đã ghi nhận các nguyên tắc về bảo vệ ANQG, TTATXH; bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; kết hợp bảo vệ an ninh mạng với phát triển kinh tế - xã hội. Tuy nhiên, các nguyên tắc như quản trị rủi ro, phân tầng bảo vệ theo mức độ quan trọng của hệ thống thông tin, bảo vệ dữ liệu theo vòng đời, trách nhiệm giải trình, kiểm soát quyền lực khi áp dụng biện pháp bảo vệ an ninh mạng và bảo đảm quyền của chủ thể bị tác động vẫn chưa được thể hiện đầy đủ như những nguyên tắc độc lập.

Ví dụ điển hình như vụ việc năm 2024, cơ quan chuyên trách bảo vệ an ninh mạng phát hiện 83 chiến dịch tấn công mạng từ 45 nhóm tin tặc, gián điệp mạng quốc tế, với gần 5.700 chỉ dấu xâm nhập nhằm vào hệ thống thông tin trọng yếu. Các đối tượng đã kiểm soát, khống chế hệ thống máy chủ và máy tính tại một số cơ quan, đơn vị quan trọng như Văn phòng Quốc hội, Bộ Công Thương, một số cơ quan thuộc Đảng bộ Khối các cơ quan Trung ương, thành phố Đà Nẵng, tỉnh Thanh Hóa và một số đơn vị trong lực lượng vũ trang nhân dân; riêng tại Văn phòng Quốc hội, máy chủ và máy tính bị mã độc gián điệp kiểm soát, làm lộ, mất tài liệu bí mật nhà nước. Thực tiễn này cho thấy nguyên tắc bảo vệ trọng điểm đối với hệ thống thông tin quan trọng về ANQG chưa được cụ thể hóa đầy đủ thành cơ chế phân loại, đánh giá rủi ro, ưu tiên nguồn lực, giám sát liên tục và phòng vệ nhiều lớp [61].

Bên cạnh đó, nguyên tắc thích ứng với công nghệ mới còn chưa rõ. Trong khi không gian mạng chịu tác động mạnh của trí tuệ nhân tạo, dữ liệu lớn, điện toán đám mây, Internet vạn vật, thiết bị kết nối thông minh và nền tảng xuyên biên giới, pháp luật vẫn chủ yếu tiếp cận theo mô hình bảo vệ hệ thống thông tin truyền thống. Thực tiễn sử dụng thiết bị ghi âm, ghi hình, camera giám sát có nguồn gốc nước ngoài, tồn tại lỗ hổng bảo mật và có khả năng tự động truyền dữ liệu lên kho dữ liệu đám mây ở nước ngoài cho thấy cần bổ sung nguyên tắc kiểm soát rủi ro đối với thiết bị kết nối, hạ tầng số và chuỗi cung ứng công nghệ.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, một số nguyên tắc bảo vệ an ninh mạng còn thiếu tính minh bạch, chưa bảo đảm mức độ rõ ràng cần thiết để áp dụng thống nhất. Các khái niệm như an ninh mạng, an toàn thông tin mạng, an ninh dữ liệu, dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi, hệ thống thông tin quan trọng về ANQG vẫn còn có sự giao thoa về nội hàm và phạm vi áp dụng. Điều này có thể gây khó khăn trong xác định căn cứ áp dụng pháp luật, cơ quan có thẩm quyền, chủ thể chịu trách nhiệm và biện pháp bảo vệ tương ứng.

Đặc biệt, tiêu chí nhận diện, phân loại và cập nhật danh mục hệ thống thông tin quan trọng về ANQG còn chưa thật sự rõ. Trong bối cảnh chuyển đổi số, nhiều hệ thống thông tin không thuộc cơ quan nhà nước nhưng có ảnh hưởng trực tiếp đến tài chính, năng lượng, viễn thông, y tế, giao thông, dữ liệu dân cư và dịch vụ công thiết yếu. Nếu pháp luật chưa làm rõ tiêu chí đánh giá dựa trên quy mô người dùng, tính chất dữ liệu, mức độ phụ thuộc của xã hội và hậu quả khi hệ thống bị tấn công hoặc gián đoạn, việc áp dụng nguyên tắc bảo vệ trọng điểm sẽ thiếu thống nhất.

Ngoài ra, mối quan hệ giữa nguyên tắc bảo vệ an ninh mạng với nguyên tắc bảo vệ dữ liệu, bảo vệ bí mật nhà nước và bảo đảm quyền con người, quyền công dân trong môi trường số vẫn cần được làm rõ hơn. Trong các vụ lộ, mất thông tin, tài liệu nội bộ hoặc tài liệu có yếu tố bí mật nhà

nước, cơ quan có thẩm quyền thường phải đồng thời áp dụng pháp luật về an ninh mạng, bảo vệ bí mật nhà nước, dữ liệu cá nhân, an toàn thông tin mạng và xử lý vi phạm. Nếu các nguyên tắc nền tảng chưa được phân định rõ, việc xác định nguyên tắc ưu tiên áp dụng và trách nhiệm phối hợp giữa các cơ quan sẽ gặp khó khăn.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, việc chuyển hóa các nguyên tắc bảo vệ an ninh mạng thành cơ chế thực hiện cụ thể còn chưa đồng bộ và chưa thật sự khả thi. Pháp luật đã ghi nhận các nguyên tắc về phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng; bảo vệ hệ thống thông tin quan trọng về ANQG; phối hợp giữa cơ quan, tổ chức, cá nhân trong bảo vệ an ninh mạng. Tuy nhiên, các nguyên tắc này cần tiếp tục được cụ thể hóa thành quy trình nghiệp vụ thống nhất, tiêu chuẩn kỹ thuật bắt buộc, cơ chế cảnh báo sớm, cơ chế chia sẻ thông tin sự cố, tiêu chí phân loại rủi ro và trách nhiệm cụ thể của từng chủ thể.

Thực tiễn kiểm tra an ninh mạng trong quá trình triển khai Đề án 06 của Chính phủ thời gian qua cho thấy, còn khoảng cách giữa yêu cầu pháp luật và điều kiện tổ chức thực hiện. Cơ quan chức năng đã phát hiện nhiều điểm yếu, lỗ hổng bảo mật nghiêm trọng trong hệ điều hành, thiết bị và phần mềm ứng dụng tại hệ thống thông tin của một số bộ, ngành, địa phương; một số đơn vị còn sử dụng hạ tầng mạng lỗi thời, hệ thống máy chủ và phần mềm chưa đáp ứng đầy đủ yêu cầu bảo vệ an ninh, an toàn thông tin. Điều này cho thấy nguyên tắc phòng ngừa, bảo vệ trọng điểm và quản trị rủi ro chưa được bảo đảm bằng điều kiện nhân lực, tài chính, công cụ kỹ thuật và cơ chế kiểm tra, giám sát tương xứng.

Ngoài ra, cơ chế phối hợp trong thực thi các nguyên tắc bảo vệ an ninh mạng vẫn cần tiếp tục hoàn thiện. Nếu pháp luật chỉ dừng lại ở nguyên tắc phối hợp chung mà chưa quy định rõ đầu mối điều phối, thời hạn phản ứng, trách nhiệm chia sẻ dữ liệu, cơ chế bảo mật thông tin và trách nhiệm giải trình, thì khi xảy ra sự cố, việc xử lý có thể chậm trễ, thiếu thống nhất hoặc bỏ trống trách nhiệm.

Một vấn đề khác là các nguyên tắc kiểm soát việc áp dụng biện pháp bảo vệ an ninh mạng chưa được cụ thể hóa đầy đủ. Các biện pháp như giám sát, thu thập dữ liệu điện tử, yêu cầu cung cấp thông tin, yêu cầu gỡ bỏ thông tin, ngăn chặn truy cập hoặc hạn chế hoạt động của hệ thống thông tin có thể cần thiết để bảo vệ ANQG, TTATXH, nhưng cũng có khả năng tác động đến quyền riêng tư, dữ liệu cá nhân, bí mật kinh doanh, quyền tiếp cận thông tin và quyền tự do kinh doanh hợp pháp. Vì vậy, pháp luật cần tiếp tục làm rõ nguyên tắc hợp pháp, cần thiết, tương xứng, minh bạch, trách nhiệm giải trình, quyền khiếu nại và cơ chế kiểm soát quyền lực khi áp dụng biện pháp bảo vệ an ninh mạng.

***- Tồn tại, bất cập trong nhóm quy định hành vi vi phạm pháp luật về an ninh mạng***

Xét theo ba nhóm tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng, nhóm quy định hành vi vi phạm pháp luật về an ninh mạng còn một số tồn tại, bất cập chủ yếu sau đây:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, pháp luật hiện hành chưa bao quát đầy đủ các hành vi vi phạm mới phát sinh trên không gian mạng. Mặc dù Luật An toàn thông tin mạng năm 2015, Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017, Luật An ninh mạng năm 2018 và các văn bản chuyên ngành đã quy định nhiều nhóm hành vi vi phạm liên quan đến an ninh mạng, công nghệ thông tin, mạng viễn thông, dữ liệu, giao dịch điện tử và phương tiện điện tử, nhưng sự phát triển nhanh của công nghệ số đã làm xuất hiện nhiều dạng hành vi mới, có phương thức thực hiện tinh vi hơn, phạm vi tác động rộng hơn và hậu quả khó kiểm soát hơn.

Thực tiễn năm 2024 cho thấy, các đối tượng phạm tội đã sử dụng công nghệ Deepfake AI để làm giả căn cước công dân, vượt qua cơ chế xác thực sinh trắc học nhằm mở tài khoản ngân hàng phục vụ hoạt động phạm tội. Trong vụ việc này, cơ quan chức năng đã triệt phá chuyên án và khởi tố 06 đối tượng liên quan đến hành vi làm giả căn cước công dân bằng công nghệ

Deepfake AI để mở tài khoản ngân hàng. Vụ việc cho thấy hành vi vi phạm trên không gian mạng đã chuyển sang khai thác trí tuệ nhân tạo, dữ liệu sinh trắc học, định danh điện tử và cơ chế xác thực số; trong khi pháp luật hiện hành chưa nhận diện đầy đủ nhóm hành vi sử dụng trí tuệ nhân tạo để giả mạo danh tính số, thao túng dữ liệu xác thực, tự động hóa hành vi lừa đảo hoặc hỗ trợ thực hiện tội phạm mạng [61].

Bên cạnh đó, pháp luật còn chưa bao quát đầy đủ các hành vi vi phạm liên quan đến tài sản số, tiền mã hóa và giao dịch ẩn danh trên không gian mạng. Thực tiễn cho thấy hoạt động giao dịch tiền ảo, tiền mã hóa diễn biến phức tạp; một số đối tượng lợi dụng khoảng trống pháp lý để phát hành tiền ảo, huy động vốn, lôi kéo nhà đầu tư theo mô hình đa cấp, đồng thời sử dụng tiền mã hóa để ẩn danh giao dịch, che giấu dòng tiền hoặc thanh toán cho các hành vi vi phạm pháp luật. Khi pháp luật chưa xác định rõ địa vị pháp lý của tài sản số và chưa thiết lập đầy đủ cơ chế truy nguyên, phong tỏa, thu giữ, định giá, xử lý tài sản mã hóa, việc chứng minh hành vi vi phạm, xác định thiệt hại và bảo vệ người bị hại còn gặp nhiều khó khăn.

Mặt khác, các quy định về hành vi vi phạm pháp luật về an ninh mạng còn phân tán trong nhiều lĩnh vực pháp luật như công nghệ thông tin, viễn thông, giao dịch điện tử, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước, sở hữu trí tuệ, hình sự, tố tụng hình sự và xử lý vi phạm hành chính. Chẳng hạn, hành vi mua bán dữ liệu cá nhân có thể đồng thời liên quan đến pháp luật về bảo vệ dữ liệu cá nhân, an ninh mạng, thương mại điện tử, lừa đảo chiếm đoạt tài sản và tội phạm sử dụng công nghệ cao; hành vi sử dụng tiền mã hóa để che giấu dòng tiền có thể liên quan đến pháp luật về an ninh mạng, phòng, chống rửa tiền, tài chính - ngân hàng và xử lý hình sự. Nếu thiếu cơ chế liên thông giữa các lĩnh vực này, việc xác định văn bản áp dụng, thẩm quyền xử lý, chế tài tương ứng và ranh giới giữa xử lý hành chính với xử lý hình sự sẽ gặp nhiều trở ngại.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, một số quy định về hành vi vi phạm pháp luật về an ninh mạng còn thiếu tiêu chí nhận diện cụ

thể, dẫn đến khó khăn trong áp dụng thống nhất. Nhiều hành vi được mô tả bằng các khái niệm rộng như “gây hậu quả nghiêm trọng”, “gây rối loạn”, “gây thiệt hại”, “phát tán thông tin sai sự thật”, “xâm phạm quyền, lợi ích hợp pháp”, “thông tin có tác hại lớn” hoặc “ảnh hưởng đến ANQG”. Nếu thiếu tiêu chí hướng dẫn về phạm vi tác động, mức độ thiệt hại, hậu quả, lỗi và mối quan hệ nhân quả thì dễ dẫn đến cách hiểu và áp dụng khác nhau giữa các cơ quan thực thi.

Điển hình là vụ việc tung tin thất thiệt liên quan đến Ngân hàng SCB trong tháng 10 và tháng 11 năm 2022. Một số cá nhân đã đăng tải, chia sẻ thông tin sai sự thật trên mạng xã hội về hoạt động của ngân hàng, làm phát sinh tâm lý hoang mang trong dư luận và ảnh hưởng đến hoạt động bình thường của tổ chức tín dụng. Tại Hà Nội, cá nhân N.K.C. bị xử phạt hành chính 7,5 triệu đồng về hành vi cung cấp, chia sẻ thông tin sai sự thật liên quan đến Ngân hàng SCB; ở một số địa phương khác, cơ quan công an cũng triệu tập, làm việc với các cá nhân đăng tải thông tin thất thiệt về hoạt động ngân hàng [59].

Căn cứ pháp lý được áp dụng là Điều 101 Nghị định số 15/2020/NĐ-CP, được sửa đổi, bổ sung bởi Nghị định số 14/2022/NĐ-CP về xử phạt hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống hoặc xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân. Từ vụ việc này có thể thấy, khó khăn đặt ra không chỉ là xác định hành vi “cung cấp, chia sẻ thông tin sai sự thật”, mà còn là đánh giá mức độ nguy hiểm của hành vi để lựa chọn chế tài phù hợp. Cùng là thông tin sai sự thật về ngân hàng, hậu quả pháp lý có thể khác nhau tùy thuộc vào phạm vi lan truyền, số lượng người tiếp cận, mức độ gây hoang mang, ảnh hưởng đến hoạt động bình thường của ngân hàng, thiệt hại đối với người gửi tiền, doanh nghiệp, thị trường tài chính và TTATXH. Do đó, pháp luật cần tiếp tục hoàn thiện tiêu chí phân biệt giữa vi phạm hành chính và hành vi có dấu hiệu tội phạm, nhất là trong trường hợp thông tin sai sự thật

lan truyền rộng, gây thiệt hại lớn hoặc tác động tiêu cực đến an ninh tài chính, tiền tệ.

Bất cập về kỹ thuật pháp lý cũng thể hiện rõ trong việc xử lý hành vi đánh bạc trên không gian mạng. Năm 2020, lực lượng chức năng triệt phá chuyên án tổ chức đánh bạc qua hệ thống “Nổ Hũ”, trong đó có hàng triệu tài khoản đăng ký tham gia, với lượng tiền đánh bạc lên tới 64.000 tỷ đồng. Mặc dù hành vi tổ chức đánh bạc, đánh bạc trên không gian mạng đã có cơ sở xử lý theo Bộ luật Hình sự, nhưng thực tiễn điều tra cho thấy việc xác định số tiền dùng để đánh bạc, giá trị quy đổi của vật phẩm ảo, lịch sử giao dịch điện tử, số lần tham gia, vai trò của từng chủ thể trong hệ thống và mối quan hệ giữa nhà cái, đại lý, người chơi vẫn rất phức tạp. Điều này đặt ra yêu cầu cần có hướng dẫn pháp lý cụ thể hơn về cách xác định giá trị giao dịch, chứng cứ điện tử, dòng tiền và yếu tố cấu thành đối với hành vi đánh bạc trực tuyến [57].

Đối với hành vi xâm phạm quyền tác giả, quyền liên quan trên môi trường số, việc xác định thiệt hại và khoản thu lợi bất chính cũng còn vướng mắc. Trên thực tế, nhiều website phát lậu phim, bóng đá, chương trình truyền hình hoặc sách điện tử có bản quyền đồng thời thu tiền quảng cáo, phí thành viên hoặc tài trợ. Thiệt hại của chủ thể quyền không chỉ là doanh thu bị mất trực tiếp, mà còn bao gồm thiệt hại về uy tín, thị phần, khả năng khai thác thương mại và giá trị thương hiệu. Việc thiếu hướng dẫn cụ thể về cách xác định thiệt hại và khoản thu lợi bất chính trong môi trường số làm cho quá trình xử lý gặp khó khăn, nhất là khi cần xác định ngưỡng xử lý hành chính hoặc truy cứu trách nhiệm hình sự.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, việc nhận diện, phân loại và đánh giá mức độ nguy hiểm của hành vi vi phạm pháp luật về an ninh mạng còn gặp nhiều khó khăn trong thực tiễn. Đặc thù của hành vi vi phạm trên không gian mạng là có thể được thực hiện nhanh, ẩn danh, xuyên biên giới, thông qua nhiều lớp công cụ kỹ thuật và gây hậu quả lan rộng. Vì vậy, việc xác định hành vi, chủ thể vi phạm, lỗi, hậu quả, mối quan hệ nhân

quả, mức độ thiệt hại và dòng tiền phạm tội thường phức tạp hơn so với hành vi vi phạm trong môi trường vật lý.

Thực tiễn đấu tranh với tội phạm sử dụng công nghệ cao cho thấy việc chứng minh hành vi vi phạm trong các vụ án có yếu tố công nghệ, tài khoản ảo, dữ liệu điện tử và dòng tiền số vẫn gặp nhiều trở ngại. Đối với chuyên án “Nổ Hũ”, cơ quan chức năng không chỉ phải chứng minh hành vi tổ chức đánh bạc, đánh bạc, mà còn phải xác định hệ thống tài khoản, đại lý, công thanh toán, lịch sử giao dịch, vật phẩm ảo, giá trị quy đổi và dòng tiền giữa các chủ thể tham gia. Đối với các vụ việc liên quan đến tiền mã hóa, khó khăn còn lớn hơn do giao dịch có tính ẩn danh, phân tán, có thể dịch chuyển qua nhiều ví điện tử và sàn giao dịch khác nhau. Điều này cho thấy khoảng cách đáng kể giữa quy định pháp luật và khả năng chứng minh hành vi vi phạm trong thực tiễn.

Một bất cập khác là ranh giới giữa vi phạm hành chính và tội phạm hình sự trong lĩnh vực an ninh mạng chưa phải lúc nào cũng được phân định rõ. Nhiều hành vi trên không gian mạng có hậu quả lan rộng nhưng thiệt hại vật chất trực tiếp khó định lượng; trong khi hậu quả về uy tín, niềm tin xã hội, dữ liệu cá nhân, bí mật kinh doanh hoặc an toàn hệ thống thông tin lại rất lớn. Chẳng hạn, hành vi phát tán thông tin sai sự thật, lừa đảo trực tuyến, chiếm đoạt tài khoản mạng xã hội, đánh cắp dữ liệu cá nhân hoặc quảng bá mô hình đầu tư tiền ảo có thể ban đầu được xử lý hành chính; nhưng khi phạm vi lan truyền rộng, số lượng người bị hại lớn, thiệt hại tài sản đáng kể hoặc ảnh hưởng đến TTATXH thì cần xem xét trách nhiệm hình sự. Tuy nhiên, pháp luật hiện hành vẫn thiếu tiêu chí cụ thể để xác định ngưỡng chuyển hóa này, nhất là tiêu chí về số lượng người bị tác động, phạm vi lan truyền, giá trị thiệt hại, mức độ thu lợi bất chính, mục đích của chủ thể thực hiện và hậu quả kinh tế - xã hội.

Hiệu quả thực thi còn bị hạn chế bởi tình trạng mua bán, thu thập, khai thác và sử dụng trái phép dữ liệu cá nhân diễn ra phổ biến. Năm 2024, cơ quan chuyên trách bảo vệ an ninh mạng phát hiện trên một số diễn đàn, hội

nhóm trên không gian mạng hoạt động trao đổi, mua bán thông tin, dữ liệu cá nhân công khai, tổ chức thành đường dây quy mô lớn với hàng nghìn thành viên tham gia. Đáng chú ý, có vụ việc 50.000 hồ sơ hành khách hạng nhất của Vietnam Airlines bị rao bán; thông tin chuyến bay Vietnam Airlines trong chuyến thăm và làm việc của Thủ tướng Australia bị rao bán; đồng thời hơn 136.770 bản ghi thông tin của cán bộ, chiến sĩ trong lực lượng vũ trang bị lộ lọt. Những vụ việc này cho thấy pháp luật tuy đã có quy định về bảo vệ dữ liệu cá nhân, nhưng việc nhận diện, xử lý hành vi mua bán dữ liệu, xác định thiệt hại và mối liên hệ giữa hành vi mua bán dữ liệu với các hành vi lừa đảo, chiếm đoạt tài sản, xúc phạm danh dự, nhân phẩm hoặc xâm phạm đời sống riêng tư vẫn còn nhiều khó khăn [61].

***- Tồn tại, bất cập trong nhóm quy định về biện pháp bảo vệ an ninh mạng***

Xét theo ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, nhóm quy định về biện pháp bảo vệ an ninh mạng còn một số tồn tại, bất cập chủ yếu sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, các biện pháp bảo vệ an ninh mạng hiện hành chưa bao quát đầy đủ các nguy cơ, rủi ro mới phát sinh trên không gian mạng. Mặc dù pháp luật đã quy định nhiều biện pháp như kiểm tra, giám sát, thu thập dữ liệu điện tử, yêu cầu gỡ bỏ thông tin vi phạm, ứng phó, khắc phục sự cố và xử lý tình huống nguy hiểm về an ninh mạng, nhưng vẫn chưa thật sự đầy đủ để ứng phó với các rủi ro mới như tấn công chuỗi cung ứng, mã độc tổng tiền, tấn công thiết bị IoT, khai thác dữ liệu lớn trái phép, tấn công hạ tầng điện toán đám mây hoặc lợi dụng tài sản số để che giấu dòng tiền vi phạm pháp luật.

Thực tiễn năm 2024 cho thấy, các cuộc tấn công mã hóa dữ liệu, đòi tiền chuộc nhằm vào Tổng công ty Điện lực Thành phố Hồ Chí Minh, Công ty Cổ phần Chứng khoán VNDIRECT, Công ty Cổ phần Mobicast và Công ty Cổ phần Viễn thông Di động Đông Dương Telecom đã gây gián đoạn hoạt

động và ảnh hưởng đến quyền, lợi ích hợp pháp của số lượng lớn người sử dụng dịch vụ. Những vụ việc này cho thấy pháp luật đã có biện pháp ứng phó và khắc phục sự cố, nhưng còn thiếu các yêu cầu cụ thể về sao lưu dữ liệu, diễn tập phục hồi hệ thống, cảnh báo sớm, chia sẻ chỉ dấu tấn công và cơ chế phục hồi hoạt động sau sự cố [61].

Bên cạnh đó, các biện pháp bảo vệ an ninh mạng chưa theo kịp rủi ro phát sinh từ thiết bị kết nối mạng và hạ tầng số phân tán. Báo cáo của cơ quan chuyên trách bảo vệ an ninh mạng, thời gian qua ghi nhận nhiều thiết bị ghi âm, ghi hình, camera giám sát có nguồn gốc nước ngoài tồn tại lỗ hổng bảo mật, có nguy cơ thu thập và truyền dữ liệu ra nước ngoài. Điều này cho thấy pháp luật cần có các biện pháp chuyên biệt hơn để kiểm soát rủi ro đối với thiết bị IoT, camera giám sát và các hệ thống kết nối mạng trong đô thị thông minh, giao thông, y tế và năng lượng.

Ngoài ra, các biện pháp bảo vệ an ninh mạng còn phân tán trong nhiều lĩnh vực pháp luật như an ninh mạng, an toàn thông tin mạng, dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, bảo vệ bí mật nhà nước, xử lý vi phạm hành chính, hình sự và tố tụng hình sự. Khi xảy ra sự cố lộ, mất dữ liệu hoặc xâm nhập hệ thống, việc phối hợp giữa các cơ chế bảo vệ hiện hành vẫn chưa thật sự rõ ràng, đặc biệt về cơ quan chủ trì, trách nhiệm thông báo, bảo toàn chứng cứ điện tử và khắc phục hậu quả.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, một số biện pháp bảo vệ an ninh mạng chưa được quy định rõ về điều kiện, phạm vi, trình tự, thủ tục và giới hạn áp dụng. Các biện pháp như thu thập dữ liệu điện tử, giám sát an ninh mạng, yêu cầu cung cấp thông tin, gỡ bỏ hoặc ngăn chặn thông tin vi phạm, đình chỉ dịch vụ hoặc hạn chế hoạt động của hệ thống thông tin đều có khả năng tác động trực tiếp đến quyền và lợi ích hợp pháp của cá nhân, tổ chức.

Đối với biện pháp thu thập dữ liệu điện tử, pháp luật vẫn cần làm rõ loại dữ liệu được thu thập, chủ thể có thẩm quyền yêu cầu, thời hạn lưu giữ, mục đích sử dụng và trách nhiệm bảo mật. Đối với biện pháp yêu cầu gỡ bỏ

hoặc ngăn chặn thông tin vi phạm, cần tiếp tục cụ thể hóa tiêu chí nhận diện thông tin vi phạm, trình tự yêu cầu, thời hạn thực hiện, trách nhiệm của nền tảng số và quyền giải trình, khiếu nại của chủ thể bị tác động.

Thực tiễn cho thấy, cơ quan chức năng đã yêu cầu các nhà cung cấp dịch vụ xuyên biên giới gỡ bỏ hàng nghìn tài khoản, bài viết, video có nội dung vi phạm và ngăn chặn truy cập đối với nhiều trang mạng đặt máy chủ ở nước ngoài. Tuy nhiên, chính thực tiễn này cho thấy nhu cầu hoàn thiện hơn các quy định về căn cứ áp dụng, trách nhiệm giải trình và cơ chế kiểm tra nhằm bảo đảm cân bằng giữa bảo vệ ANQG với quyền tiếp cận thông tin, quyền tự do kinh doanh và các quyền, lợi ích hợp pháp khác.

Ngoài ra, kỹ thuật lập pháp hiện nay vẫn chủ yếu dựa trên mô hình bảo vệ hệ thống thông tin truyền thống, trong khi chưa phản ánh đầy đủ các yêu cầu mới như giám sát liên tục, phân tích hành vi bất thường, săn tìm mối đe dọa, chia sẻ chỉ dấu tấn công, kiểm soát rủi ro điện toán đám mây, truy vết tài sản số và phối hợp với nền tảng xuyên biên giới.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, việc áp dụng các biện pháp bảo vệ an ninh mạng còn gặp khó khăn do hạn chế về nguồn lực, nhân lực, công cụ kỹ thuật và cơ chế phối hợp. Nhiều cơ quan, tổ chức, đặc biệt ở địa phương, doanh nghiệp nhỏ và vừa, cơ sở giáo dục, bệnh viện hoặc đơn vị sự nghiệp chưa có đội ngũ chuyên trách an ninh mạng, chưa có hệ thống giám sát, phát hiện mã độc và quy trình phản ứng sự cố phù hợp.

Hiệu quả thực thi cũng bị hạn chế bởi cơ chế phối hợp và thời hạn phản ứng chưa thật sự rõ ràng. Trong các vụ lừa đảo trực tuyến, nếu việc phối hợp giữa cơ quan chức năng, ngân hàng, nhà mạng và nền tảng xuyên biên giới không kịp thời thì việc bảo toàn chứng cứ, ngăn chặn dòng tiền, gỡ bỏ nội dung vi phạm và cảnh báo người dân sẽ không đạt hiệu quả như mong muốn. Đồng thời, số lượng nội dung, tài khoản, tên miền và ứng dụng vi phạm phát sinh nhanh trên nhiều nền tảng khác nhau tạo áp lực lớn đối với cơ chế thực thi hiện hành.

Bên cạnh đó, một số biện pháp bảo vệ an ninh mạng chưa được kiểm soát đầy đủ để bảo đảm cân bằng giữa yêu cầu bảo vệ ANQG với quyền và lợi ích hợp pháp của cá nhân, tổ chức. Các biện pháp giám sát an ninh mạng, thu thập dữ liệu điện tử, yêu cầu cung cấp thông tin hoặc lưu trữ dữ liệu nếu thiếu giới hạn rõ ràng về mục đích, phạm vi, thời hạn và cơ chế kiểm tra có thể ảnh hưởng đến quyền riêng tư, dữ liệu cá nhân, bí mật kinh doanh và quyền tự do kinh doanh hợp pháp.

***- Tồn tại, bất cập trong nhóm quy định về địa vị pháp lý của các chủ thể tham gia hoạt động trong lĩnh vực an ninh mạng***

Xét theo ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật, nhóm quy định về địa vị pháp lý của các chủ thể tham gia hoạt động trong lĩnh vực an ninh mạng còn một số bất cập chủ yếu sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, pháp luật hiện hành chưa xác định đầy đủ và tương xứng địa vị pháp lý của các chủ thể mới trong hệ sinh thái số như nhà cung cấp dịch vụ điện toán đám mây, nền tảng xuyên biên giới, trung gian thanh toán, ví điện tử, đơn vị xử lý dữ liệu thuê ngoài, tổ chức cung cấp dịch vụ định danh, xác thực điện tử, doanh nghiệp vận hành nền tảng trí tuệ nhân tạo, sàn giao dịch tài sản số và tổ chức cung cấp dịch vụ an ninh mạng.

Thực tiễn các vụ lộ, mất dữ liệu quy mô lớn cho thấy chuỗi xử lý dữ liệu thường có sự tham gia của nhiều chủ thể như đơn vị thu thập dữ liệu, bên xử lý dữ liệu thuê ngoài, nhà cung cấp hạ tầng lưu trữ, nền tảng cung cấp dịch vụ và bên thứ ba khai thác dữ liệu. Tuy nhiên, pháp luật chưa xác định rõ trách nhiệm riêng biệt của từng chủ thể trong bảo đảm an ninh dữ liệu, thông báo sự cố, bảo toàn chứng cứ điện tử, phối hợp điều tra, khắc phục hậu quả và bồi thường thiệt hại, nhất là khi dữ liệu được lưu trữ trên hạ tầng điện toán đám mây hoặc máy chủ ở nước ngoài.

Địa vị pháp lý của doanh nghiệp cung cấp nền tảng xuyên biên giới cũng cần được làm rõ hơn, đặc biệt về nghĩa vụ phản hồi yêu cầu của cơ quan có thẩm quyền, bảo toàn dữ liệu tài khoản, cung cấp thông tin phục vụ điều

tra, ngăn chặn tái xuất hiện nội dung vi phạm và trách nhiệm khi không hợp tác hoặc hợp tác chậm. Tương tự, sự phát triển của trí tuệ nhân tạo đặt ra yêu cầu xác định trách nhiệm của nhà phát triển, nhà cung cấp và đơn vị vận hành nền tảng trí tuệ nhân tạo trong cảnh báo rủi ro, kiểm soát lạm dụng, lưu giữ nhật ký kỹ thuật, bảo đảm an toàn mô hình và phối hợp xử lý vi phạm.

Ngoài ra, địa vị pháp lý của các chủ thể còn bị phân tán giữa nhiều văn bản pháp luật chuyên ngành. Ví dụ, một sàn thương mại điện tử có thể đồng thời là doanh nghiệp cung cấp nền tảng số, bên xử lý dữ liệu cá nhân, chủ thể bảo vệ quyền lợi người tiêu dùng và chủ thể phối hợp xử lý lừa đảo, hàng giả, xâm phạm sở hữu trí tuệ hoặc phát tán mã độc. Nếu thiếu cơ chế liên thông, cả doanh nghiệp và cơ quan thực thi đều có thể gặp khó khăn trong xác định nghĩa vụ ưu tiên, cơ quan chủ trì và cơ chế xử lý phù hợp.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, một số quy định về quyền, nghĩa vụ và trách nhiệm của các chủ thể còn chung chung. Các quy định như “có trách nhiệm phối hợp”, “bảo đảm an ninh mạng”, “thực hiện yêu cầu của cơ quan có thẩm quyền” cần được cụ thể hóa về trường hợp phối hợp, loại thông tin phải cung cấp, thời hạn, phương thức thực hiện, trách nhiệm bảo mật, quyền yêu cầu giải thích, quyền từ chối yêu cầu không có căn cứ và hậu quả pháp lý khi không thực hiện.

Trong xử lý lừa đảo trực tuyến, cơ quan có thẩm quyền có thể yêu cầu doanh nghiệp viễn thông, ngân hàng, trung gian thanh toán, ví điện tử, nền tảng mạng xã hội hoặc nhà cung cấp dịch vụ lưu trữ cung cấp dữ liệu tài khoản, nhật ký truy cập, địa chỉ IP, thông tin định danh, lịch sử giao dịch hoặc dữ liệu thanh toán. Nếu pháp luật không quy định rõ phạm vi thông tin, điều kiện yêu cầu, trình tự, thời hạn phản hồi, tiêu chuẩn bảo mật và trách nhiệm khi cung cấp sai, thiếu hoặc chậm, việc thực thi sẽ thiếu thống nhất và có thể ảnh hưởng đến quyền riêng tư, dữ liệu cá nhân, bí mật kinh doanh của người sử dụng dịch vụ.

Bên cạnh đó, pháp luật chưa thể hiện rõ nguyên tắc phân tầng nghĩa vụ theo mức độ rủi ro của từng loại chủ thể. Một doanh nghiệp nhỏ không thể

có cùng năng lực kỹ thuật, tài chính và nhân sự như ngân hàng, doanh nghiệp viễn thông, nền tảng xuyên biên giới, doanh nghiệp điện toán đám mây hoặc chủ quản hệ thống thông tin quan trọng. Nếu áp dụng cùng một mức nghĩa vụ cho mọi chủ thể, pháp luật có thể làm giảm tính khả thi và tạo gánh nặng tuân thủ không hợp lý.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, cơ chế phối hợp giữa các chủ thể vẫn còn phân tán, chồng chéo hoặc thiếu đầu mối điều phối thống nhất. Thực tiễn xử lý các tài khoản giả mạo cơ quan nhà nước, ngân hàng, doanh nghiệp cung cấp dịch vụ công hoặc sàn thương mại điện tử để lừa đảo người dân cho thấy việc xử lý đòi hỏi sự phối hợp giữa cơ quan công an, doanh nghiệp viễn thông, ngân hàng, trung gian thanh toán, nền tảng mạng xã hội, cơ quan quản lý thông tin và truyền thông, cũng như chủ thể bị giả mạo. Nếu thiếu đầu mối điều phối, thời hạn phản hồi và nghĩa vụ hợp tác rõ ràng của nền tảng xuyên biên giới, việc gỡ bỏ tài khoản giả mạo, bảo toàn dữ liệu, truy vết dòng tiền và bảo vệ người bị hại sẽ thiếu hiệu quả.

Tính khả thi của các nghĩa vụ pháp lý còn phụ thuộc vào nguồn lực và năng lực kỹ thuật của từng chủ thể. Nhiều doanh nghiệp nhỏ và vừa, cơ sở giáo dục, bệnh viện, đơn vị sự nghiệp hoặc doanh nghiệp khởi nghiệp chưa có đội ngũ chuyên trách an ninh mạng, công cụ phát hiện mã độc hoặc quy trình ứng phó sự cố. Nếu pháp luật chỉ quy định nghĩa vụ chung mà không có cơ chế hỗ trợ, phân loại rủi ro và lộ trình tuân thủ phù hợp, các quy định này khó được thực hiện hiệu quả.

Một bất cập khác là địa vị pháp lý của chủ thể bị tác động bởi biện pháp bảo vệ an ninh mạng cần được làm rõ hơn, nhất là quyền được thông báo, quyền yêu cầu giải thích, quyền khiếu nại, quyền yêu cầu khắc phục hậu quả, quyền yêu cầu bồi thường và quyền được bảo vệ dữ liệu cá nhân. Chẳng hạn, khi doanh nghiệp bị yêu cầu tạm dừng dịch vụ trực tuyến hoặc cá nhân bị gỡ bỏ nội dung trên nền tảng số, pháp luật cần làm rõ căn cứ áp dụng, phạm vi, thời hạn, quyền giải trình, quyền khiếu nại và điều kiện khôi phục quyền, lợi ích hợp pháp.

***- Tồn tại, bất cập trong nhóm quy định về chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng***

Xét theo ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, nhóm quy định về chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng còn một số tồn tại, bất cập chủ yếu sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, hệ thống chế tài hiện hành chưa bao quát đầy đủ các dạng vi phạm mới và chủ thể vi phạm mới trong môi trường số. Mặc dù pháp luật đã quy định các chế tài hành chính, hình sự, dân sự và biện pháp khắc phục hậu quả đối với nhiều hành vi vi phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, giao dịch điện tử, an toàn thông tin mạng và an ninh mạng, nhưng trước sự phát triển của trí tuệ nhân tạo, dữ liệu lớn, tài sản số, tiền mã hóa, nền tảng xuyên biên giới và dịch vụ điện toán đám mây, nhiều hành vi vi phạm vẫn chưa có chế tài trực diện, tương xứng và dễ áp dụng.

Chẳng hạn, các hành vi sử dụng công nghệ số để giả mạo danh tính, tạo tài khoản ảo, tự động hóa hoạt động lừa đảo hoặc phát tán thông tin sai sự thật hiện vẫn chủ yếu được xử lý thông qua các cấu thành vi phạm truyền thống, chưa phản ánh đầy đủ yếu tố tự động hóa, quy mô lan truyền và mức độ nguy hiểm của công nghệ mới. Tương tự, các hành vi liên quan đến tài sản số, tiền mã hóa và giao dịch ẩn danh còn gặp khó khăn trong xử lý do địa vị pháp lý của tài sản số và cơ chế định giá, phong tỏa, thu giữ, xử lý tài sản mã hóa chưa hoàn thiện.

Tính đồng bộ của hệ thống chế tài cũng còn hạn chế. Cùng một hành vi vi phạm trên không gian mạng có thể bị điều chỉnh bởi nhiều văn bản khác nhau với mức xử phạt, thẩm quyền xử lý và biện pháp khắc phục hậu quả khác nhau. Kết quả kiểm tra toàn diện hoạt động của TikTok tại Việt Nam năm 2023 cho thấy đối với nền tảng xuyên biên giới có quy mô người dùng lớn, việc xử lý không chỉ dừng lại ở phạt tiền hoặc gỡ bỏ nội dung vi phạm mà còn đòi hỏi trách nhiệm về thuật toán đề xuất, cơ chế kiểm duyệt, bảo vệ người dùng và

ngăn ngừa tái phạm. Tuy nhiên, hệ thống chế tài hiện hành vẫn chưa phát triển đầy đủ theo hướng trách nhiệm nền tảng và trách nhiệm khắc phục mang tính cấu trúc [60].

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, một số quy định về chế tài còn thiếu rõ ràng trong việc phân biệt giữa hình thức xử phạt, biện pháp khắc phục hậu quả và biện pháp quản lý nhà nước. Trong nhiều trường hợp, pháp luật chưa xác định rõ điều kiện áp dụng, thứ tự ưu tiên và mối quan hệ giữa các hậu quả pháp lý như phạt tiền, đình chỉ hoạt động, tước quyền sử dụng giấy phép, thu hồi giấy phép, buộc gỡ bỏ thông tin vi phạm hoặc buộc nộp lại khoản thu lợi bất hợp pháp.

Bất cập này cũng thể hiện ở việc xác định ngưỡng chuyển hóa giữa xử lý hành chính và xử lý hình sự. Pháp luật đã đặt ra nguyên tắc xử lý căn cứ vào tính chất, mức độ vi phạm và hậu quả, nhưng vẫn thiếu tiêu chí cụ thể về số lượng người bị tác động, phạm vi lan truyền, giá trị thiệt hại, mức độ thu lợi bất chính và hậu quả kinh tế - xã hội.

Vụ án BestBuy IPTV là ví dụ điển hình. Đây là vụ án xử lý hình sự đối với hành vi cung cấp dịch vụ IPTV bất hợp pháp, phát sóng trái phép nội dung có bản quyền, trong đó Tòa án đã áp dụng hình phạt và buộc nộp lại khoản thu lợi bất chính. Tuy nhiên, thực tiễn vụ việc cho thấy, việc xác định thiệt hại, khoản thu lợi bất chính, doanh thu quảng cáo, doanh thu thuê bao và mức độ ảnh hưởng đến thị trường bản quyền số vẫn còn nhiều khó khăn. Tương tự, vụ việc liên quan đến Phimmoi.net cho thấy khó khăn trong xác định trách nhiệm pháp lý của các chủ thể tham gia vận hành hệ thống, khoản thu lợi bất chính, trách nhiệm liên đới và các biện pháp ngăn chặn tái phạm thông qua tên miền hoặc nền tảng khác [61].

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, việc áp dụng chế tài trong thực tiễn còn gặp nhiều khó khăn, đặc biệt đối với pháp nhân thương mại, nền tảng xuyên biên giới và các chủ thể thu lợi lớn từ hành vi vi phạm trên không gian mạng. Mặc dù pháp luật hình sự đã ghi nhận trách nhiệm hình

sự của pháp nhân thương mại đối với một số tội danh, nhưng trong thực tiễn việc xử lý vẫn chủ yếu tập trung vào cá nhân trực tiếp thực hiện hành vi hoặc dừng lại ở chế tài hành chính đối với tổ chức.

Đối với các nền tảng xuyên biên giới, việc thực thi chế tài còn gặp khó khăn do khác biệt về trụ sở pháp lý, máy chủ, cơ chế đại diện và quyền tài phán. Thực tiễn kiểm tra và xử lý vi phạm đối với các nền tảng số lớn cho thấy chế tài phạt tiền hoặc yêu cầu gỡ bỏ nội dung vi phạm có ý nghĩa nhất định, nhưng chưa đủ nếu thiếu cơ chế buộc nền tảng thay đổi quy trình kiểm duyệt, cải thiện cơ chế tiếp nhận yêu cầu hoặc minh bạch thuật toán đề xuất.

Bên cạnh đó, chế tài hiện hành chưa bảo đảm đầy đủ yêu cầu khắc phục hậu quả cho chủ thể bị xâm phạm. Trong lĩnh vực an ninh mạng, thiệt hại không chỉ là thiệt hại vật chất mà còn bao gồm thiệt hại về dữ liệu cá nhân, bí mật kinh doanh, uy tín, cơ hội kinh doanh và chi phí phục hồi hệ thống. Nếu chế tài chỉ dừng lại ở phạt tiền mà chưa gắn với nghĩa vụ khắc phục hậu quả, xóa dữ liệu đã chiếm đoạt, thông báo cho người bị ảnh hưởng, phục hồi hệ thống hoặc bồi thường thiệt hại thì quyền và lợi ích hợp pháp của chủ thể bị xâm phạm chưa được bảo vệ tương xứng.

Ngoài ra, mức xử phạt hành chính trong một số trường hợp chưa tương xứng với khoản lợi bất hợp pháp mà chủ thể vi phạm thu được, đặc biệt đối với các hành vi mua bán dữ liệu cá nhân, kinh doanh nội dung vi phạm bản quyền hoặc khai thác trái phép dữ liệu người dùng. Điều này làm giảm hiệu quả răn đe và phòng ngừa của chế tài.

***- Tồn tại, bất cập trong nhóm quy định hợp tác quốc tế về an ninh mạng***

Xét theo ba nhóm tiêu chí đánh giá mức độ hoàn thiện pháp luật về an ninh mạng, nhóm quy định hợp tác quốc tế về an ninh mạng còn một số bất cập chủ yếu sau:

*Thứ nhất*, xét theo nhóm tiêu chí về nội dung pháp luật, quy định về hợp tác quốc tế trong lĩnh vực an ninh mạng chưa bao quát đầy đủ các cơ chế hợp tác cần thiết. Pháp luật đã ghi nhận hợp tác trong chia sẻ thông tin, hỗ trợ

kỹ thuật, đào tạo, phòng, chống tội phạm mạng và phối hợp xử lý sự cố; tuy nhiên, các điều ước quốc tế, hiệp định song phương, thỏa thuận hợp tác chuyên biệt với quốc gia, vùng lãnh thổ, cơ quan chuyên trách nước ngoài và doanh nghiệp cung cấp dịch vụ xuyên biên giới vẫn còn hạn chế. Trong các vụ lừa đảo trực tuyến, chiếm đoạt tài sản, tấn công mạng hoặc sử dụng tiền mã hóa để che giấu dòng tiền, nếu không có cơ chế hợp tác nhanh với quốc gia nơi đặt máy chủ, nền tảng số, nhà cung cấp dịch vụ đám mây hoặc sàn giao dịch tài sản số, cơ quan có thẩm quyền sẽ gặp khó khăn trong bảo toàn dữ liệu, xác minh tài khoản, truy vết dòng tiền và thu thập chứng cứ điện tử.

Bên cạnh đó, hợp tác quốc tế về an ninh mạng còn thiếu sự liên thông đầy đủ với pháp luật tố tụng hình sự, tương trợ tư pháp, dẫn độ, phòng chống rửa tiền, quản lý tài sản số, bảo vệ dữ liệu cá nhân và chứng cứ điện tử. Điều này làm cho việc xử lý các vụ việc có yếu tố nước ngoài dễ bị chậm trễ, thiếu đồng bộ, nhất là khi cần đồng thời thực hiện nhiều yêu cầu như bảo toàn dữ liệu, xác minh định danh, thu thập nhật ký truy cập, phong tỏa tài sản và phối hợp điều tra.

*Thứ hai*, xét theo nhóm tiêu chí về kỹ thuật pháp lý, pháp luật hiện hành còn thiếu quy định chi tiết về thu thập, bảo quản, chuyển giao và sử dụng chứng cứ điện tử xuyên biên giới. Chứng cứ điện tử có đặc điểm dễ bị xóa, sửa đổi, mã hóa, phân tán hoặc lưu giữ ở nước ngoài, nên nếu thiếu cơ chế rõ ràng về bảo toàn dữ liệu, yêu cầu cung cấp dữ liệu, xác thực nguồn gốc, bảo đảm tính toàn vẹn và chuỗi lưu giữ chứng cứ thì giá trị chứng minh trong tố tụng có thể bị ảnh hưởng. Ví dụ, trong các vụ lừa đảo qua thư điện tử doanh nghiệp, dữ liệu quan trọng như nhật ký đăng nhập, địa chỉ IP, nội dung trao đổi, thông tin tài khoản nhận tiền và dữ liệu xác thực thường do nhà cung cấp dịch vụ nước ngoài lưu giữ; việc thu thập hợp pháp các dữ liệu này đòi hỏi cơ chế hợp tác nhanh, rõ ràng và đáp ứng tiêu chuẩn chứng cứ.

Ngoài ra, pháp luật cũng cần làm rõ phạm vi dữ liệu được chia sẻ, mục đích sử dụng, thời hạn lưu giữ, trách nhiệm bảo mật và cơ chế kiểm soát việc sử dụng dữ liệu trong hợp tác quốc tế. Nếu thiếu các giới hạn này, hoạt

động hợp tác có thể làm phát sinh nguy cơ xâm phạm quyền riêng tư, dữ liệu cá nhân, bí mật kinh doanh và quyền, lợi ích hợp pháp của cá nhân, tổ chức.

*Thứ ba*, xét theo nhóm tiêu chí về thực thi pháp luật, việc hợp tác quốc tế trong lĩnh vực an ninh mạng còn gặp khó khăn do khác biệt về quyền tài phán, tiêu chuẩn chứng cứ, trình tự tố tụng, năng lực thực thi và mức độ sẵn sàng hợp tác giữa các quốc gia. Trong môi trường mạng, hành vi vi phạm có thể được thực hiện tại một quốc gia, máy chủ đặt tại quốc gia khác, nạn nhân ở Việt Nam và dòng tiền đi qua nhiều vùng lãnh thổ. Vì vậy, việc xác định cơ quan có thẩm quyền, quốc gia cần yêu cầu hỗ trợ và phương thức thu thập chứng cứ không phải lúc nào cũng thuận lợi.

Hiệu quả thực thi còn bị hạn chế bởi sự thiếu thống nhất về tiêu chuẩn an ninh mạng, quy trình ứng cứu sự cố và cơ chế chia sẻ thông tin giữa các quốc gia. Đồng thời, pháp luật Việt Nam cần tiếp tục rà soát, cập nhật để tương thích với các chuẩn mực quốc tế mới, nhất là Công ước Liên hợp quốc về chống tội phạm mạng, thường được gọi là Công ước Hà Nội. Công ước này đặt ra các yêu cầu về hình sự hóa hành vi tội phạm mạng, xác lập thẩm quyền, hợp tác quốc tế, tương trợ tư pháp, dẫn độ, thu thập và chia sẻ chứng cứ điện tử xuyên biên giới, đồng thời gắn với yêu cầu bảo đảm quyền con người trong quá trình điều tra, xử lý tội phạm mạng.

Nhìn chung, nhóm quy định về hợp tác quốc tế trong lĩnh vực an ninh mạng đã tạo cơ sở bước đầu cho việc phối hợp xử lý các vụ việc có yếu tố nước ngoài. Tuy nhiên, trong bối cảnh tội phạm mạng ngày càng tinh vi, xuyên biên giới và gắn với công nghệ mới, nhóm quy định này cần tiếp tục được hoàn thiện theo hướng mở rộng nội dung hợp tác, cụ thể hóa quy trình chia sẻ dữ liệu và chứng cứ điện tử, thiết lập cơ chế hợp tác khẩn cấp với nền tảng số, nhà cung cấp dịch vụ đám mây, sàn giao dịch tài sản số, đồng thời bảo đảm hài hòa giữa yêu cầu bảo vệ ANQG với quyền, lợi ích hợp pháp của cá nhân, tổ chức.

### ***3.2.2.2. Nguyên nhân của những tồn tại, hạn chế trong pháp luật về an ninh mạng ở Việt Nam***

Những tồn tại, bất cập của pháp luật về an ninh mạng ở Việt Nam xuất phát từ nhiều nguyên nhân khác nhau, bao gồm cả nguyên nhân khách quan và nguyên nhân chủ quan. Các nguyên nhân này có mối quan hệ tác động qua lại với nhau, phản ánh đặc thù của an ninh mạng là lĩnh vực mới, có tính kỹ thuật cao, tính liên ngành, tính xuyên biên giới và luôn biến đổi nhanh theo sự phát triển của công nghệ. Các nguyên nhân gồm:

#### ***- Nguyên nhân khách quan***

*Thứ nhất*, nguyên nhân cơ bản xuất phát từ tính mới, tính phức tạp và tốc độ biến đổi rất nhanh của không gian mạng. Không gian mạng là môi trường có tốc độ phát triển nhanh hơn nhiều so với chu kỳ xây dựng và sửa đổi pháp luật. Các công nghệ như trí tuệ nhân tạo, dữ liệu lớn, điện toán đám mây, Internet vạn vật, blockchain, tài sản số, nền tảng xuyên biên giới và các công cụ ẩn danh liên tục tạo ra những dạng hành vi mới, phương thức vi phạm mới và hậu quả pháp lý mới. Trong khi đó, pháp luật luôn cần thời gian để nhận diện vấn đề, đánh giá tác động chính sách, xây dựng quy phạm và tổ chức thi hành. Chính độ trễ này làm cho một số quy định pháp luật về an ninh mạng chưa kịp bao quát các hành vi mới như deepfake, tấn công chuỗi cung ứng, xâm phạm cơ sở dữ liệu quốc gia, lạm dụng trí tuệ nhân tạo, tài sản số, tiền mã hóa hoặc các hình thức tội phạm sử dụng nền tảng xuyên biên giới.

*Thứ hai*, nguyên nhân xuất phát từ tính liên ngành của pháp luật về an ninh mạng. An ninh mạng không phải là lĩnh vực biệt lập, mà có sự giao thoa với pháp luật về ANQG, an toàn thông tin mạng, dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, trí tuệ nhân tạo, công nghệ thông tin, bảo vệ bí mật nhà nước, hình sự, tổ tụng hình sự, xử lý vi phạm hành chính, tài chính - ngân hàng, sở hữu trí tuệ và hợp tác quốc tế. Do đó, các quy định về an ninh mạng tất yếu nằm trong nhiều văn bản pháp luật khác nhau. Tuy nhiên, khi thiếu cơ chế liên thông và phân định rõ ràng giữa các lĩnh vực, sự

phân tán này dễ dẫn đến chồng chéo, trùng lặp, bỏ trống thẩm quyền hoặc khó xác định căn cứ pháp lý áp dụng trong từng vụ việc cụ thể.

*Thứ ba*, nguyên nhân xuất phát từ khó khăn khách quan trong xác định thiệt hại, chứng cứ và trách nhiệm pháp lý trong môi trường số. Nhiều thiệt hại do hành vi vi phạm pháp luật về an ninh mạng gây ra không dễ định lượng, chẳng hạn thiệt hại về uy tín, niềm tin của khách hàng, gián đoạn hoạt động, mất cơ hội kinh doanh, rò rỉ dữ liệu cá nhân, nguy cơ bị lợi dụng dữ liệu trong tương lai hoặc ảnh hưởng lâu dài đến an ninh xã hội. Trong khi đó, chứng cứ điện tử dễ bị xóa, sửa đổi, mã hóa, phân tán hoặc lưu trữ ở nước ngoài. Điều này làm cho việc phân định giữa xử lý hành chính và xử lý hình sự, xác định mức độ nguy hiểm của hành vi, cá thể hóa trách nhiệm và áp dụng chế tài tương xứng gặp nhiều khó khăn.

*Thứ tư*, nguyên nhân đến từ sự khác biệt giữa pháp luật Việt Nam và pháp luật, tiêu chuẩn, cơ chế hợp tác quốc tế trong lĩnh vực an ninh mạng. Không gian mạng có tính xuyên biên giới, nhưng mỗi quốc gia lại có quy định khác nhau về quyền tài phán, tiêu chuẩn chứng cứ, bảo vệ dữ liệu cá nhân, bảo mật, điều tra số, dẫn độ, tương trợ tư pháp và chia sẻ thông tin. Sự khác biệt này làm cho hợp tác quốc tế trong xử lý tội phạm mạng, thu thập chứng cứ điện tử, truy vết dòng tiền, yêu cầu nền tảng xuyên biên giới cung cấp dữ liệu hoặc gỡ bỏ nội dung vi phạm gặp nhiều trở ngại. Việc nội luật hóa các chuẩn mực quốc tế mới, trong đó có các cơ chế về chứng cứ điện tử xuyên biên giới và bảo vệ quyền con người trong điều tra tội phạm mạng, cũng cần có thời gian và lộ trình phù hợp.

*Thứ năm*, nguyên nhân xuất phát từ yêu cầu phải cân bằng giữa bảo vệ ANQG và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức. Nếu pháp luật trao công cụ quá rộng mà thiếu điều kiện, trình tự, thủ tục và cơ chế kiểm soát, có thể phát sinh nguy cơ xâm phạm quyền riêng tư, dữ liệu cá nhân, quyền tiếp cận thông tin hoặc quyền tự do kinh doanh hợp pháp. Ngược lại, nếu pháp luật quy định quá hạn chế, cơ quan nhà nước có thể thiếu công cụ

cần thiết để ngăn chặn, xử lý các hành vi xâm phạm an ninh mạng. Chính yêu cầu cân bằng này làm cho việc thiết kế các quy định về giám sát, thu thập dữ liệu điện tử, yêu cầu cung cấp thông tin, gỡ bỏ thông tin, đình chỉ dịch vụ, xử lý dữ liệu và hợp tác quốc tế trở nên phức tạp hơn.

**- Nguyên nhân chủ quan**

*Thứ nhất*, nguyên nhân đến từ tư duy lập pháp trong lĩnh vực an ninh mạng vẫn còn có lúc thiên về phản ứng sau vi phạm hơn là quản trị rủi ro từ sớm, từ xa. Một số quy định pháp luật được xây dựng để xử lý các hành vi đã phát sinh trong thực tiễn, trong khi chưa chú trọng đầy đủ đến dự báo rủi ro, phân tầng nghĩa vụ, kiểm soát nguy cơ và phục hồi sau sự cố. Điều này lý giải vì sao hệ thống nguyên tắc bảo vệ an ninh mạng chưa thể hiện đầy đủ các nguyên tắc như quản trị rủi ro, phân loại hệ thống theo mức độ quan trọng, trách nhiệm giải trình, kiểm soát quyền lực và bảo vệ quyền của chủ thể bị tác động. Khi tư duy lập pháp chưa chuyển mạnh sang quản trị rủi ro, pháp luật dễ rơi vào tình trạng xử lý sự vụ, thiếu cơ chế phòng ngừa bền vững.

*Thứ hai*, nguyên nhân xuất phát từ kỹ thuật lập pháp và chuẩn hóa thuật ngữ chưa theo kịp yêu cầu của lĩnh vực có tính kỹ thuật cao. Pháp luật về an ninh mạng sử dụng nhiều khái niệm vừa mang tính pháp lý, vừa mang tính kỹ thuật như an ninh mạng, an toàn thông tin mạng, dữ liệu điện tử, chứng cứ điện tử, hệ thống thông tin quan trọng về ANQG, dữ liệu cá nhân, dữ liệu quan trọng, tấn công mạng, giám sát an ninh mạng, thu thập dữ liệu điện tử. Nếu các khái niệm này không được giải thích thống nhất, không có tiêu chí nhận diện rõ ràng hoặc được sử dụng khác nhau trong các văn bản khác nhau, gây khó khăn cho việc áp dụng pháp luật.

*Thứ ba*, nguyên nhân nằm ở việc đánh giá tác động chính sách trong lĩnh vực an ninh mạng chưa toàn diện và căn cứ trên đầy đủ dữ liệu thực tiễn. An ninh mạng là lĩnh vực đòi hỏi đánh giá tác động không chỉ về pháp lý, mà còn về kỹ thuật, kinh tế, xã hội, quyền con người, quyền công dân, quyền riêng tư, dữ liệu cá nhân, chi phí tuân thủ của doanh nghiệp và năng lực thực

thi của cơ quan nhà nước. Nếu quá trình xây dựng chính sách chưa lượng hóa đầy đủ chi phí, lợi ích, nguồn lực, khả năng tuân thủ và rủi ro thực thi, các quy định được ban hành có thể đúng về mục tiêu nhưng khó khả thi trong thực tế.

*Thứ tư*, nguyên nhân xuất phát từ điều kiện bảo đảm thực thi pháp luật còn chưa tương xứng với yêu cầu bảo vệ an ninh mạng. Việc thực hiện pháp luật về an ninh mạng đòi hỏi nguồn nhân lực có kiến thức liên ngành, công cụ kỹ thuật hiện đại, năng lực giám định số, hệ thống giám sát, cảnh báo sớm, cơ sở dữ liệu, quy trình ứng phó sự cố và cơ chế bảo toàn chứng cứ điện tử. Tuy nhiên, trên thực tế, không phải mọi cơ quan, địa phương, doanh nghiệp, tổ chức đều có đủ nguồn lực này. Điều đó làm cho một số quy định tuy đã được ban hành nhưng khó triển khai thống nhất, nhất là trong các tình huống cần phản ứng nhanh như tấn công ransomware, lộ lọt dữ liệu, giả mạo cơ quan nhà nước, lừa đảo trực tuyến hoặc sự cố đối với hệ thống thông tin quan trọng.

*Thứ năm*, nguyên nhân đến từ cơ chế phối hợp giữa các chủ thể trong lĩnh vực an ninh mạng chưa rõ ràng, ổn định và thống nhất. Bảo vệ an ninh mạng liên quan đến nhiều cơ quan, nhiều ngành, nhiều cấp, nhiều doanh nghiệp và nhiều chủ thể ngoài nhà nước. Nếu thiếu đầu mối điều phối, thiếu thời hạn phản hồi, thiếu quy trình chia sẻ thông tin, thiếu cơ chế bảo mật và thiếu trách nhiệm pháp lý khi không phối hợp, việc xử lý sự cố hoặc hành vi vi phạm có thể bị chậm trễ. Điều này đặc biệt rõ trong các vụ việc liên quan đến nền tảng xuyên biên giới, ngân hàng, viễn thông, trung gian thanh toán, thương mại điện tử, mạng xã hội và cơ quan điều tra.

### **3.3. ĐÁNH GIÁ THỰC TIỄN THỰC HIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM HIỆN NAY**

#### **3.3.1. Thực tiễn tuân thủ pháp luật về an ninh mạng**

Thực tiễn thực hiện pháp luật về an ninh mạng giai đoạn 2019 - 2025 cho thấy ý thức tuân thủ pháp luật của cơ quan, tổ chức, doanh nghiệp và cá nhân đã có chuyển biến tích cực. Công tác quán triệt, phổ biến chủ trương,

chính sách, pháp luật về an ninh mạng được triển khai rộng rãi trong hệ thống chính trị, doanh nghiệp và xã hội. Đến nay, 100% cấp ủy, chỉ bộ cơ quan Trung ương và địa phương đã tổ chức quán triệt cho cán bộ, công chức, viên chức, người lao động; điển hình như Đảng ủy Công an Trung ương chỉ đạo 60/60 đơn vị trực thuộc Bộ và 34/34 Công an tỉnh, thành phố tuyên truyền, phổ biến pháp luật về an ninh mạng; Đảng bộ Bộ Tài chính tổ chức quán triệt cho hơn 2.058 cán bộ, công chức, viên chức và người lao động; Đảng ủy Tập đoàn Bru chính Viễn thông Việt Nam chỉ đạo 100% chi bộ trực thuộc học tập, quán triệt. Đây là cơ sở quan trọng góp phần nâng cao nhận thức và trách nhiệm tuân thủ pháp luật về an ninh mạng [62].

Việc tuân thủ pháp luật còn thể hiện qua sự phối hợp của doanh nghiệp viễn thông, Internet và nền tảng số với cơ quan nhà nước có thẩm quyền. Các báo cáo tổng kết giai đoạn 2019 - 2025 cho thấy cơ quan chức năng đã yêu cầu Facebook, Google, TikTok, Zalo và các nền tảng khác gỡ bỏ, ngăn chặn hàng chục nghìn tài khoản, bài viết, video vi phạm pháp luật. Riêng năm 2025, các doanh nghiệp xuyên biên giới đã ngăn chặn, gỡ bỏ khoảng 15.500 tài khoản, bài viết, video vi phạm. Đồng thời, các doanh nghiệp viễn thông, Internet đã phối hợp ngăn chặn nhiều trang mạng, tên miền, ứng dụng có nội dung vi phạm. Cụ thể, năm 2024 là 43.883 trang mạng đặt máy chủ ở nước ngoài, năm 2025 con số trên là 318.216 trang mạng. Điều này phản ánh sự chuyển biến trong ý thức chấp hành yêu cầu quản lý nhà nước của doanh nghiệp cung cấp dịch vụ trên không gian mạng [61], [62].

Bên cạnh kết quả đạt được, thực tiễn tuân thủ pháp luật về an ninh mạng vẫn còn nhiều hạn chế. Tình trạng tấn công mạng, gián điệp mạng, lộ, mất bí mật nhà nước, thu thập, mua bán trái phép dữ liệu, lừa đảo trực tuyến, phát tán thông tin sai sự thật và thông tin xấu độc vẫn diễn biến phức tạp. Giai đoạn 2019 - 2025, cơ quan chức năng đã phát hiện hơn 7000 trang thông tin điện tử bị tấn công. Trong đó, điển hình như năm 2024, đã phát hiện 83 chiến dịch tấn công mạng từ 45 nhóm tin tặc, gián điệp mạng quốc tế, với gần 5.700

chỉ dấu xâm nhập; năm 2025 tiếp tục ghi nhận các nhóm tin tặc nước ngoài tấn công vào hệ thống thông tin trọng yếu của 12 bộ, ngành, địa phương và tấn công chuỗi cung ứng vào 13 tập đoàn, doanh nghiệp trong các lĩnh vực truyền thông, tài chính, công nghệ, năng lượng, vận tải, bưu chính, y tế. Các số liệu này cho thấy mức độ tuân thủ quy trình bảo vệ hệ thống thông tin ở một số cơ quan, tổ chức, doanh nghiệp chưa đáp ứng yêu cầu phòng ngừa rủi ro trong bối cảnh chuyển đổi số [61], [62].

Tình trạng lộ, mất bí mật nhà nước và dữ liệu cá nhân trên không gian mạng vẫn đáng lo ngại. Từ năm 2019 đến hết năm 2025, cơ quan chức năng đã phát hiện, xử lý 213 vụ lộ, mất bí mật nhà nước với khoảng 1400 tài liệu mật, ngoài ra còn tài liệu nội bộ, dữ liệu nhạy cảm và tài khoản thư điện tử công vụ. Riêng năm 2024 xác minh, xử lý 70 vụ, với 222 đầu tài liệu; năm 2025 tiếp tục xử lý 23 vụ. Đối với dữ liệu cá nhân, năm 2025 phát hiện 300 vụ rao bán với hơn 1,7 triệu bản ghi dữ liệu trong các lĩnh vực y tế, giáo dục, dịch vụ công, ngân hàng, điện lực, bảo hiểm, chứng khoán, căn cước công dân, vận chuyển, viễn thông. Những vụ việc này cho thấy việc tuân thủ nghĩa vụ bảo vệ bí mật nhà nước, dữ liệu cá nhân và bảo mật thông tin khách hàng tại một số cơ quan, tổ chức, doanh nghiệp còn hạn chế [61], [62].

Tội phạm sử dụng công nghệ cao tiếp tục gia tăng, phản ánh sự thiếu tuân thủ pháp luật của một bộ phận cá nhân, tổ chức trên không gian mạng. Giai đoạn 2019 - 2025, cơ quan chức năng đã khởi tố gần 2400 vụ án với 1800 bị can. Riêng năm 2025, cơ quan chức năng đã phát hiện, tiếp nhận 4.814 vụ việc lừa đảo qua mạng, gây thiệt hại hơn 3.400 tỷ đồng, khởi tố điều tra 2.188 vụ án với 796 bị can. Hiện nay, các phương thức thực hiện hành vi phạm tội ngày càng tinh vi như “bắt cóc online”, giả danh cơ quan chức năng, giả mạo ngân hàng, sử dụng deepfake, camera ảo để vượt qua xác thực sinh trắc học, tổ chức đánh bạc qua mạng, sử dụng tiền mã hóa để che giấu dòng tiền, thiết lập nhóm Telegram để mua bán dữ liệu, tài khoản ngân hàng, ví điện tử [62].

Việc tuân thủ các quy định về bảo vệ hệ thống thông tin, bảo đảm an toàn hệ thống thông tin theo cấp độ cũng chưa đồng đều. Năm 2024, cơ quan chuyên trách bảo vệ an ninh mạng đã kiểm tra 65 bộ, ngành, địa phương kết nối Cơ sở dữ liệu quốc gia về dân cư và phát hiện 2.487 điểm yếu, lỗ hổng bảo mật nghiêm trọng. Năm 2025, khi kiểm tra tại 31/34 địa phương trong quá trình triển khai mô hình chính quyền địa phương hai cấp, cơ quan chức năng phát hiện nhiều hệ thống trung tâm hành chính chưa trang bị đầy đủ giải pháp bảo đảm an ninh mạng; việc quản lý tài khoản đăng nhập, quyền quản trị, giám sát an ninh mạng và an ninh dữ liệu còn hạn chế [61], [62].

Những hạn chế trên xuất phát từ nhiều nguyên nhân, trong đó có nhận thức, thói quen sử dụng công nghệ và kỷ luật an toàn thông tin của một bộ phận cán bộ, công chức, viên chức, người lao động và người sử dụng dịch vụ còn chưa cao. Một số đơn vị còn chủ quan trong quản lý hệ thống, giao phó hoàn toàn cho đơn vị thuê vận hành, chưa kiểm soát đầy đủ quyền quản trị, chưa thường xuyên rà soát, khắc phục lỗ hổng; còn tình trạng sử dụng phần mềm không rõ nguồn gốc, đặt mật khẩu yếu, cấm thiết bị lạ vào máy tính cơ quan, truyền gửi tài liệu qua dịch vụ không bảo đảm an toàn. Cơ chế báo cáo, chia sẻ thông tin về sự cố an ninh mạng ở một số cơ quan, tổ chức, doanh nghiệp cũng chưa chủ động, kịp thời do tâm lý e ngại ảnh hưởng đến uy tín hoặc trách nhiệm.

### **3.3.2. Thực tiễn thi hành pháp luật về an ninh mạng**

Thời gian qua, công tác thi hành pháp luật về an ninh mạng đã có nhiều chuyển biến tích cực. Trước hết, việc thể chế hóa, ban hành và tổ chức thực hiện các cơ chế, chính sách, đề án, dự án liên quan đến lĩnh vực an ninh mạng được triển khai tương đối đồng bộ. Hệ thống văn bản QPPL về an ninh mạng, bảo vệ dữ liệu cá nhân, viễn thông, quản lý Internet và an toàn thông tin mạng từng bước được xây dựng, hoàn thiện, tạo hành lang pháp lý cho các cơ quan, tổ chức, doanh nghiệp và cá nhân triển khai hoạt động bảo đảm an toàn thông tin và an ninh mạng.

Từ năm 2019 đến nay, Bộ Công an đã chủ trì, tham mưu ban hành nhiều văn bản quan trọng như Luật An ninh mạng năm 2018; Nghị định số 53/2022/NĐ-CP quy định chi tiết một số điều của Luật An ninh mạng; Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân; Nghị định số 04/2019/NĐ-CP quy định chi tiết trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng; Thông tư số 29/2022/TT-BCA về quản lý, kết nối và chia sẻ dữ liệu số trong lực lượng Công an nhân dân; Thông tư số 86/2021/TT-BCA về bảo đảm an toàn thông tin số trong Công an nhân dân... Đồng thời, Bộ Công an đã phối hợp với các bộ, ngành rà soát, hoàn thiện hệ thống văn bản pháp luật để điều chỉnh các vấn đề mới phát sinh; xây dựng 15 quy chế phối hợp với Bộ Quốc phòng, Bộ Khoa học và Công nghệ, Bộ Y tế, Bộ Giáo dục và Đào tạo cùng các cơ quan liên quan; tổ chức nhiều hội nghị tuyên truyền, phổ biến pháp luật về an ninh mạng trên các phương tiện thông tin đại chúng.

Qua các báo cáo tổng kết giai đoạn 2019 - 2025, có thể thấy công tác thi hành pháp luật về an ninh mạng không chỉ dừng lại ở việc ban hành văn bản mà đã được cụ thể hóa thành các hoạt động quản lý, kiểm tra, giám sát, thẩm định, hướng dẫn và ứng cứu sự cố. Năm 2023, lực lượng chức năng triển khai 43 kế hoạch, tổ chức hơn 120 lượt kiểm tra, đánh giá an ninh mạng; phối hợp, hỗ trợ các cơ quan, đơn vị xác minh, xử lý gần 150 sự cố mạng nghiêm trọng; bảo đảm an ninh hệ thống mạng cho gần 20 hội nghị, sự kiện chính trị quan trọng. Năm 2024 và 2025, tiếp tục tổ chức nhiều cuộc diễn tập an ninh mạng trên phạm vi toàn quốc; bảo đảm an ninh mạng, an toàn thông tin cho 28 hội nghị, sự kiện chính trị quan trọng [59], [60], [61].

Công tác thi hành pháp luật trong bảo đảm an ninh hệ thống thông tin được triển khai theo hướng giám sát thường xuyên, liên tục, kết nối, cảnh báo và ứng phó sự cố. Hệ thống Trung tâm điều hành an ninh mạng thuộc Trung tâm An ninh mạng quốc gia đã kết nối, giám sát hệ thống của 23 cơ quan Đảng, Nhà nước, tập đoàn kinh tế và tài chính trọng yếu. Tính đến tháng

10/2025, Trung tâm An ninh mạng quốc gia đã kết nối với 42 đơn vị để chia sẻ dữ liệu cảnh báo SOC, thu thập khoảng 4,9 triệu cảnh báo an ninh mạng; thông báo 12 lỗ hổng bảo mật nghiêm trọng trên các giải pháp, ứng dụng của nhiều hệ thống thông tin trọng yếu; phối hợp phát hiện, xử lý và khắc phục 09 sự cố mạng nghiêm trọng; truy vết, giám sát hoạt động của 09 nhóm tin tặc nước ngoài và 08 nhóm tin tặc Việt Nam đang thực hiện các cuộc tấn công mạng. Những kết quả này cho thấy nhiệm vụ bảo đảm an ninh mạng, cảnh báo, ứng phó sự cố và bảo vệ hệ thống thông tin đã từng bước được cụ thể hóa bằng hoạt động kỹ thuật, nghiệp vụ và quản trị thực tế [62].

Việc thi hành pháp luật về an ninh mạng cũng gắn với các nhiệm vụ chuyển đổi số, xây dựng Chính phủ điện tử, Chính phủ số và bảo vệ các hệ thống thông tin phục vụ quản lý nhà nước. Năm 2025, công tác bảo đảm an ninh, an toàn hệ thống mạng tiếp tục được triển khai phục vụ sáp nhập đơn vị hành chính theo mô hình chính quyền địa phương hai cấp; cơ quan chức năng đã kiểm tra, hướng dẫn, khắc phục sự cố mất an ninh mạng tại trung tâm hành chính của 31 địa phương, đồng thời phối hợp, trao đổi 140 văn bản thẩm định hệ thống và hơn 10 đề án, dự án đầu tư ứng dụng công nghệ thông tin trong Bộ Công an.

Bên cạnh đó, công tác xây dựng tiêu chuẩn, quy chuẩn và hướng dẫn kỹ thuật về an ninh mạng đã được quan tâm hơn. Năm 2025, cơ quan chức năng tham mưu xây dựng, ban hành tiêu chuẩn “An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng” TCVN 14423:2025; tiếp tục nghiên cứu, hoàn thiện các tiêu chuẩn, quy chuẩn, bộ tiêu chí về an ninh, an toàn hệ thống mạng; ban hành nhiều điện mật, thông báo hướng dẫn Công an các đơn vị, địa phương triển khai công tác bảo vệ an ninh hệ thống mạng, chống tấn công mạng, gián điệp mạng và khắc phục tình trạng lộ, mất bí mật nhà nước. Đây là cơ sở quan trọng để chuyển hóa quy định pháp luật thành yêu cầu kỹ thuật, nghiệp vụ cụ thể trong thực tiễn [62].

Công tác quản lý nhà nước đối với doanh nghiệp cung cấp dịch vụ xuyên biên giới cũng có chuyển biến. Các cơ quan chức năng đã tăng cường

yêu cầu các nền tảng như Meta, Google, Apple, TikTok phối hợp ngăn chặn, vô hiệu hóa thông tin xấu độc, vi phạm pháp luật, truy vết mục tiêu; đồng thời thiết lập cơ chế trao đổi trực tiếp với TikTok thông qua công cụ thực thi an toàn để xử lý yêu cầu nghiệp vụ. Điều này cho thấy pháp luật về an ninh mạng đã từng bước được thi hành thông qua cơ chế phối hợp với doanh nghiệp nền tảng số, nhất là trong xử lý thông tin vi phạm pháp luật trên không gian mạng.

Tuy nhiên, công tác thi hành pháp luật về an ninh mạng vẫn còn một số hạn chế. Trước hết, việc triển khai chưa thật sự đồng bộ giữa các bộ, ngành, địa phương; cơ chế phối hợp trong chia sẻ thông tin, cảnh báo và xử lý sự cố an ninh mạng chưa tối ưu. Một số quy định còn giao thoa giữa lĩnh vực an toàn thông tin mạng và an ninh mạng, dẫn đến khó xác định đầu mối chịu trách nhiệm khi xảy ra sự cố hoặc hành vi vi phạm. Cơ chế bắt buộc chia sẻ dữ liệu, báo cáo sự cố, cung cấp thông tin về lỗ hổng bảo mật, mã độc và chỉ dấu tấn công còn hạn chế, làm cho việc xử lý sự cố trong một số trường hợp chưa kịp thời, thiếu tính liên thông và chưa chủ động.

Bên cạnh đó, việc thi hành pháp luật trong phối hợp với doanh nghiệp viễn thông, ngân hàng, trung gian thanh toán, sàn thương mại điện tử và nền tảng số vẫn chưa đáp ứng đầy đủ yêu cầu thực tiễn. Cơ chế chia sẻ dữ liệu liên quan đến tài khoản ngân hàng, ví điện tử, thuê bao di động, địa chỉ IP, giao dịch bất thường và dấu vết kỹ thuật còn gặp khó khăn; một số doanh nghiệp chưa phối hợp kịp thời trong việc cung cấp dữ liệu phục vụ xác minh, điều tra, ngăn chặn vi phạm. Điều này ảnh hưởng đến hiệu quả thu hồi tài sản trong các vụ án lừa đảo trên không gian mạng, cũng như làm giảm khả năng phát hiện, xử lý sớm các hành vi vi phạm pháp luật về an ninh mạng.

Thực tiễn các báo cáo tổng kết cũng cho thấy năng lực tổ chức thi hành pháp luật giữa các cơ quan, đơn vị chưa đồng đều. Một số địa phương, cơ quan, tổ chức chưa có đội ngũ chuyên trách đủ mạnh, chưa đầu tư đầy đủ cho hạ tầng kỹ thuật, hệ thống giám sát, cảnh báo và ứng cứu sự cố. Việc

kiểm tra, đánh giá an ninh mạng trong quá trình triển khai mô hình chính quyền địa phương hai cấp cho thấy vẫn còn nhiều hệ thống thông tin tồn tại điểm yếu, lỗ hổng bảo mật; một số đơn vị chưa quản lý chặt chẽ tài khoản, quyền quản trị và chưa thực hiện đầy đủ yêu cầu bảo đảm an ninh dữ liệu. Đây là hạn chế có ảnh hưởng trực tiếp đến hiệu quả thi hành pháp luật về an ninh mạng.

Ngoài ra, công tác thi hành pháp luật về an ninh mạng còn chịu sức ép lớn từ sự phát triển nhanh của công nghệ và phương thức vi phạm mới. Các hình thức tấn công mạng, gián điệp mạng, sử dụng mã độc, tấn công từ chối dịch vụ, tấn công ransomware, giả mạo ứng dụng cơ quan nhà nước để chiếm đoạt tài khoản ngân hàng, khai thác lỗ hổng hệ thống và sử dụng nền tảng xuyên biên giới để thực hiện hành vi vi phạm ngày càng phức tạp. Trong khi đó, cơ chế phối hợp liên ngành, chia sẻ dữ liệu kỹ thuật, bảo toàn chứng cứ điện tử và huy động nguồn lực kỹ thuật vẫn cần tiếp tục được hoàn thiện để đáp ứng yêu cầu xử lý nhanh, chính xác và hiệu quả.

### **3.3.3. Thực tiễn sử dụng pháp luật về an ninh mạng**

Thực tiễn thời gian qua cho thấy, các cơ quan nhà nước, tổ chức, doanh nghiệp và cá nhân đã từng bước sử dụng các quy định, công cụ và cơ chế pháp lý về an ninh mạng để bảo vệ hệ thống thông tin, dữ liệu, quyền và lợi ích hợp pháp của mình trên không gian mạng. Các bộ, ngành, địa phương đã lồng ghép nhiệm vụ bảo đảm an toàn thông tin, an ninh mạng vào chương trình chuyển đổi số, xây dựng Chính phủ điện tử, Chính phủ số, chính quyền số và công dân số; đồng thời áp dụng cơ chế kết nối, trao đổi, chia sẻ dữ liệu an toàn nhằm đơn giản hóa thủ tục hành chính, phục vụ người dân, doanh nghiệp và nâng cao hiệu quả quản lý nhà nước.

Việc phát triển, ứng dụng Cơ sở dữ liệu quốc gia về dân cư, định danh và xác thực điện tử đã tạo điều kiện để cơ quan, tổ chức khai thác, thực hiện quyền, thẩm quyền và lợi ích hợp pháp của mình trong môi trường số, đồng thời đặt ra yêu cầu bảo đảm an ninh, an toàn dữ liệu. Trong quá trình triển

khai Đề án 06 của Chính phủ, nhiều cơ quan, địa phương đã sử dụng các cơ chế pháp lý về kết nối, chia sẻ dữ liệu, bảo vệ hệ thống thông tin và kiểm tra an ninh mạng để phục vụ cải cách thủ tục hành chính, cung cấp dịch vụ công trực tuyến và bảo vệ dữ liệu dân cư.

Các doanh nghiệp viễn thông, Internet, ngân hàng, trung gian thanh toán và doanh nghiệp cung cấp nền tảng số cũng đã từng bước sử dụng pháp luật về an ninh mạng để phối hợp với cơ quan chức năng trong bảo vệ người dùng, ngăn chặn thông tin vi phạm, xác minh tài khoản, thuê bao di động, địa chỉ IP, giao dịch bất thường và dữ liệu liên quan đến hành vi vi phạm pháp luật. Cơ quan chức năng đã phối hợp xác minh thông tin 620 tài khoản trên các ứng dụng Zalo, Grab nhằm phục vụ truy tìm dấu vết đối tượng vi phạm pháp luật; đồng thời vận động 1.121 người có sức ảnh hưởng và 05 công ty truyền thông, với tổng cộng hơn 200 triệu lượt theo dõi, tham gia các chiến dịch truyền thông phòng, chống vi phạm pháp luật trên không gian mạng. Hoạt động này góp phần nâng cao hiệu quả định hướng thông tin, cảnh báo rủi ro và phòng ngừa hành vi vi phạm pháp luật [62].

Người dân, doanh nghiệp và các tổ chức xã hội cũng từng bước sử dụng pháp luật và các kênh thông tin chính thống để tham gia bảo vệ an ninh mạng. Phong trào toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng được đẩy mạnh; nhiều đơn vị, địa phương đã xây dựng, phổ biến “Bộ cẩm nang tuyên truyền, phòng, chống tội phạm trên không gian mạng”; đồng thời tăng cường tuyên truyền qua tin nhắn SMS, ứng dụng của nhà mạng, Zalo, Signal và các phương tiện thông tin đại chúng. Đây là biểu hiện cho thấy công dân và tổ chức đã được hướng dẫn thực hiện quyền tiếp cận thông tin, quyền phản ánh, tố giác tội phạm, quyền tự bảo vệ và quyền tham gia bảo vệ TTATXH trên không gian mạng.

Tuy nhiên, thực tiễn sử dụng pháp luật về an ninh mạng vẫn còn một số hạn chế. Một bộ phận người dân, tổ chức và doanh nghiệp chưa nắm rõ hoặc chưa chủ động sử dụng các cơ chế pháp lý để bảo vệ dữ liệu cá nhân, tài khoản

số, tài sản số, quyền riêng tư, danh dự, uy tín và lợi ích hợp pháp của mình trên không gian mạng. Nhiều trường hợp bị lừa đảo trực tuyến, chiếm đoạt tài sản, giả mạo danh tính hoặc bị xâm phạm dữ liệu cá nhân nhưng chậm phản ánh, tố giác với cơ quan chức năng; không lưu giữ đầy đủ chứng cứ điện tử như tin nhắn, lịch sử giao dịch, thông tin tài khoản, đường dẫn, địa chỉ ví điện tử, số điện thoại hoặc địa chỉ IP liên quan. Điều này gây khó khăn cho việc xác minh, truy vết dòng tiền, thu thập chứng cứ và xử lý đối tượng vi phạm.

Bên cạnh đó, một số cơ quan, tổ chức chưa sử dụng hiệu quả các cơ chế pháp lý để yêu cầu hỗ trợ kỹ thuật, chia sẻ cảnh báo, kết nối giám sát, kiểm tra, đánh giá an ninh mạng và ứng cứu sự cố. Khi xảy ra sự cố, vẫn còn tình trạng xử lý nội bộ, chậm báo cáo hoặc chưa chủ động phối hợp với cơ quan chuyên trách. Tâm lý e ngại ảnh hưởng đến uy tín, trách nhiệm hoặc hoạt động sản xuất, kinh doanh làm giảm hiệu quả cảnh báo sớm, khắc phục sự cố và ngăn chặn nguy cơ lan rộng.

Ngoài ra, kỹ năng pháp lý và kỹ năng số của người sử dụng không gian mạng còn hạn chế. Nhiều người chưa biết cách nhận diện hành vi lừa đảo, giả mạo, thu thập dữ liệu trái phép; chưa biết sử dụng quyền yêu cầu bảo vệ dữ liệu cá nhân, quyền khiếu nại, tố cáo, quyền yêu cầu gỡ bỏ thông tin sai sự thật hoặc yêu cầu bồi thường thiệt hại. Đối với doanh nghiệp nhỏ và vừa, việc sử dụng pháp luật để xây dựng quy trình bảo vệ dữ liệu, quy chế an ninh mạng nội bộ, phương án ứng phó sự cố và cơ chế phối hợp với cơ quan nhà nước còn chưa thường xuyên.

### **3.3.4. Thực tiễn áp dụng pháp luật về an ninh mạng**

Thực tiễn áp dụng pháp luật về an ninh mạng thời gian qua đã đạt được nhiều kết quả rõ rệt, nổi bật nhất là trong đấu tranh, xử lý tội phạm và các hành vi vi phạm pháp luật trên không gian mạng. Từ năm 2019 đến nay, Bộ Công an đã xác lập hàng trăm chuyên án đấu tranh với các loại tội phạm xâm phạm ANQG TTATXH trên không gian mạng. Cơ quan chức năng đã tiếp nhận, xác minh và xử lý 1.539/1.577 nguồn tin về tội phạm, đạt tỷ lệ 96,47%; xử phạt vi

phạm hành chính 466 đối tượng; xác minh, truy tìm 1.093 đối tượng; đấu tranh, triệt phá 304 hội, nhóm phản động, chống đối hoạt động phức tạp với hơn 02 triệu thành viên; vô hiệu hóa 3.393 mục tiêu vi phạm, gồm 354 tài khoản Facebook và 3.039 video YouTube. Qua đó, đã ngăn chặn, vô hiệu hóa khoảng 22 triệu lượt phát tán bài viết sai phạm tiếp cận gần 300 triệu người theo dõi. Những kết quả này cho thấy pháp luật về an ninh mạng đã được áp dụng tương đối hiệu quả trong xử lý các vi phạm cụ thể, góp phần bảo đảm tính nghiêm minh của pháp luật trên không gian mạng [56], [57], [58], [59], [60], [61], [62].

Hoạt động áp dụng pháp luật cũng được thực hiện quyết liệt thông qua thẩm quyền yêu cầu gỡ bỏ, ngăn chặn thông tin vi phạm pháp luật. Từ năm 2019 đến nay, Bộ Công an đã phối hợp giám sát, ngăn chặn khoảng 42.345 tên miền có nội dung xấu, độc, chống phá Đảng và Nhà nước. Riêng trong giai đoạn dịch bệnh COVID-19, trên không gian mạng xuất hiện hơn 221.000 tin, bài trên các trang thông tin điện tử, blog, diễn đàn; hơn 565.000 lượt tương tác trên Facebook; khoảng 500 video clip trên YouTube phản ánh về tình hình dịch bệnh và công tác phòng, chống dịch. Các nội dung này thu hút hơn 600.000 lượt bình luận, 4,5 triệu lượt thích và chia sẻ, trong đó có hàng nghìn tin, bài xuyên tạc, sai sự thật, chưa được kiểm chứng. Việc phát hiện, phân loại, xử lý, gỡ bỏ và ngăn chặn các nguồn thông tin vi phạm đã góp phần bảo vệ trật tự quản lý nhà nước, bảo đảm quyền tiếp cận thông tin chính xác của người dân và giữ vững ổn định xã hội [56], [57], [58], [59], [60], [61], [62].

Các số liệu tổng kết giai đoạn 2019 - 2025 cho thấy hoạt động áp dụng pháp luật trong xử lý thông tin vi phạm trên không gian mạng ngày càng được tăng cường. Riêng năm 2023, các doanh nghiệp xuyên biên giới đã phối hợp ngăn chặn, gỡ bỏ 7.838/8.566 tài khoản, bài viết vi phạm, đạt khoảng 91%; năm 2024, cơ quan chức năng yêu cầu gỡ bỏ hơn 5.300 tài khoản, bài viết, video vi phạm pháp luật; năm 2025, con số này tăng lên khoảng 15.500 tài khoản, bài viết, video. Đồng thời, việc áp dụng biện pháp ngăn chặn truy cập đối với trang mạng vi phạm cũng được triển khai trên diện rộng; riêng năm 2024 đã ngăn chặn 43.883 trang mạng đặt máy chủ ở nước ngoài, năm 2025

ngăn chặn 318.216 trang mạng có nội dung vi phạm pháp luật Việt Nam. Các kết quả này phản ánh hiệu quả bước đầu của việc áp dụng pháp luật đối với doanh nghiệp nền tảng số, doanh nghiệp viễn thông và Internet trong xử lý thông tin vi phạm [60], [61], [62].

Công tác thanh tra, kiểm tra, đánh giá việc chấp hành pháp luật về an ninh mạng cũng là một nội dung quan trọng của hoạt động áp dụng pháp luật. Bộ Công an và Bộ Thông tin và Truyền thông đã xây dựng, tổ chức triển khai 43 kế hoạch với 124 lượt kiểm tra tại các bộ, ngành, địa phương; tiếp nhận, xử lý, xác minh 127/137 vụ việc, đạt tỷ lệ 93%, liên quan đến bảo đảm an ninh hệ thống thông tin quốc gia, hoạt động tấn công mạng, khai thác lỗ hổng bảo mật và rao bán dữ liệu cá nhân trên Internet. Thực hiện Kế hoạch số 441/KH-BCA-A05, các cơ quan chức năng đã kiểm tra hơn 130 hệ thống thông tin và 30 cơ sở dữ liệu chuyên ngành tại các bộ, ngành, địa phương; kiểm tra an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước trên môi trường mạng tại 02 cơ quan Trung ương; đồng thời kiểm tra, đánh giá hệ thống thông tin giải quyết thủ tục hành chính và cổng dịch vụ công một cửa của 41 bộ, ngành, địa phương trước khi kết nối với Cơ sở dữ liệu quốc gia [61].

Hoạt động kiểm tra, đánh giá an ninh mạng tiếp tục được mở rộng trong các năm gần đây. Năm 2024, cơ quan chuyên trách đã kiểm tra, đánh giá an ninh mạng đối với 65 bộ, ngành, địa phương kết nối Cơ sở dữ liệu quốc gia về dân cư, phát hiện 2.487 điểm yếu, lỗ hổng bảo mật nghiêm trọng trong hệ điều hành, thiết bị, phần mềm ứng dụng. Năm 2025, trong quá trình triển khai mô hình chính quyền địa phương hai cấp, cơ quan chức năng tiếp tục kiểm tra an ninh mạng tại 31/34 địa phương; phát hiện, xử lý 55 vụ việc mất an ninh mạng, lộ lọt tài khoản quản trị, hệ thống thông tin tồn tại điểm yếu, lỗ hổng bảo mật, lây nhiễm mã độc. Cũng trong năm 2025, cơ quan chức năng phát hiện 705 trang web tên miền “.vn”, trong đó có 30 trang web “.gov.vn”, bị tấn công thay đổi giao diện hoặc chèn nội dung tin tặc; hơn 10.000 tài khoản đăng nhập, quản trị hệ thống của các cơ quan, tổ chức trên toàn quốc bị

chia sẻ, rao bán công khai trên mạng. Những số liệu này cho thấy hoạt động áp dụng pháp luật về kiểm tra, phát hiện, yêu cầu khắc phục vi phạm và bảo vệ hệ thống thông tin đã được triển khai ngày càng cụ thể, trực tiếp [61], [62].

Việc áp dụng pháp luật đối với các doanh nghiệp viễn thông, Internet và doanh nghiệp cung cấp nền tảng số cũng được tăng cường. Cơ quan chức năng đã làm việc với các doanh nghiệp cung cấp nền tảng mạng xã hội xuyên biên giới, doanh nghiệp cung cấp dịch vụ gọi xe công nghệ, doanh nghiệp cung cấp dịch vụ viễn thông, Internet, quản trị viên hội nhóm và người có sức ảnh hưởng để đánh giá việc tuân thủ pháp luật Việt Nam; yêu cầu 11 doanh nghiệp cung cấp dịch vụ viễn thông, Internet áp dụng các biện pháp ngăn chặn người dùng trong nước truy cập vào các trang mạng có nội dung xấu, độc, vi phạm pháp luật Việt Nam; đồng thời thành lập các đoàn kiểm tra liên ngành để thanh tra, kiểm tra hoạt động quản lý, cung cấp dịch vụ viễn thông di động tại 07 doanh nghiệp, bao gồm Viettel, VNPT, MobiFone, Vietnamobile, Đông Dương Telecom, Mobicast và Gtel. Kết quả kiểm tra đã phát hiện nhiều tồn tại, sai phạm trong hoạt động cung cấp dịch vụ, quản lý tài khoản và định danh người dùng; qua đó đặt ra yêu cầu áp dụng các biện pháp chấn chỉnh, xử lý vi phạm và hoàn thiện cơ chế quản lý.

Hoạt động áp dụng pháp luật trong đấu tranh với tội phạm sử dụng công nghệ cao cũng đạt nhiều kết quả cụ thể. Năm 2024, lực lượng chức năng đã khởi tố 44 vụ án với 187 bị can trong các đường dây, ổ nhóm tội phạm mạng quy mô lớn, hoạt động phức tạp, xuyên quốc gia. Năm 2025, riêng tội phạm lừa đảo qua mạng, hệ lực lượng đã phát hiện, tiếp nhận 4.814 vụ việc, gây thiệt hại hơn 3.400 tỷ đồng; khởi tố điều tra 2.188 vụ án với 796 bị can. Cùng với đó, cơ quan chức năng tiếp tục đấu tranh với các hành vi như giả danh cơ quan chức năng, giả mạo nhân viên ngân hàng, sử dụng deepfake, camera ảo để vượt qua xác thực sinh trắc học, tổ chức đánh bạc qua mạng, sử dụng tiền mã hóa để che giấu dòng tiền, mua bán dữ liệu cá nhân và tài khoản ngân hàng trên các hội nhóm kín. Những kết quả này cho thấy pháp luật về an

ninh mạng đã được áp dụng thực tế trong xử lý các hành vi vi phạm mới, phức tạp, gắn với công nghệ cao [61], [62].

Việc áp dụng các biện pháp pháp lý để bảo vệ hệ thống thông tin trọng yếu cũng đạt nhiều kết quả đáng ghi nhận. Tính đến tháng 10/2025, Trung tâm An ninh mạng quốc gia đã kết nối với 42 đơn vị để chia sẻ dữ liệu cảnh báo SOC, thu thập khoảng 4,9 triệu cảnh báo an ninh mạng; thông báo 12 lỗ hổng bảo mật nghiêm trọng; phối hợp xử lý 09 sự cố mạng nghiêm trọng; truy vết, giám sát hoạt động của 09 nhóm tin tặc nước ngoài và 08 nhóm tin tặc Việt Nam. Đây là minh chứng cho việc các quy định pháp luật về giám sát, cảnh báo, kiểm tra, ứng phó sự cố và bảo vệ hệ thống thông tin đã được áp dụng trên thực tế thông qua các biện pháp nghiệp vụ, kỹ thuật cụ thể [62].

Bên cạnh những kết quả đạt được, công tác áp dụng pháp luật về an ninh mạng vẫn còn một số hạn chế. Một số quy định còn chồng chéo giữa các lĩnh vực an ninh mạng, an toàn thông tin mạng, bảo vệ dữ liệu cá nhân, viễn thông, mật mã và quản lý nền tảng xuyên biên giới, dẫn đến khó khăn trong xác định thẩm quyền, trình tự, thủ tục và trách nhiệm chủ trì khi xử lý vụ việc cụ thể. Nhiều vụ việc liên quan đồng thời đến dữ liệu cá nhân, tài khoản ngân hàng, ví điện tử, thuê bao viễn thông, địa chỉ IP, nền tảng xuyên biên giới, thương mại điện tử và tội phạm công nghệ cao, đòi hỏi sự phối hợp liên ngành chặt chẽ; tuy nhiên, cơ chế pháp lý và quy trình phối hợp hiện nay chưa thật sự đồng bộ.

Việc áp dụng pháp luật trong thu hồi tài sản bị chiếm đoạt trên không gian mạng còn gặp nhiều khó khăn. Cơ chế chia sẻ dữ liệu liên quan đến tài khoản ngân hàng, ví điện tử, thuê bao điện thoại, địa chỉ IP còn nhiều vướng mắc; một số doanh nghiệp viễn thông, ngân hàng, tổ chức trung gian thanh toán và sàn thương mại điện tử chưa chủ động phối hợp, chia sẻ dữ liệu với cơ quan Công an khi phát hiện giao dịch bất thường. Nhiều ngân hàng chưa trang bị phần mềm phân tích, truy tìm dòng tiền để phục vụ công tác thu hồi tài sản. Đây là rào cản lớn trong áp dụng pháp luật nhằm đấu tranh, phòng, chống tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng.

Một hạn chế khác là việc áp dụng pháp luật đối với các nền tảng xuyên biên giới, tài sản số, tiền mã hóa và chứng cứ điện tử vẫn còn nhiều khó khăn. Đối tượng vi phạm thường sử dụng máy chủ đặt ở nước ngoài, tài khoản ảo, ví điện tử, tiền mã hóa, dịch vụ mã hóa và nền tảng xuyên biên giới để che giấu danh tính, phân tán dữ liệu và tẩu tán tài sản. Trong khi đó, cơ chế hợp tác, thu thập, bảo toàn chứng cứ điện tử và yêu cầu doanh nghiệp nước ngoài phối hợp còn mất nhiều thời gian, ảnh hưởng đến hiệu quả xử lý vi phạm.

### **3.3.5. Nhận xét chung thực tiễn thực hiện pháp luật về an ninh mạng ở Việt Nam**

Nhìn chung, việc tổ chức thực hiện pháp luật về an ninh mạng thời gian qua đã đạt được những kết quả quan trọng trên cả bốn phương diện: Tuân thủ, thi hành, sử dụng và áp dụng pháp luật. Công tác quán triệt, phổ biến pháp luật được triển khai rộng rãi; cơ chế phối hợp liên ngành trong giám sát, cảnh báo, xử lý vi phạm từng bước được vận hành; ý thức và trách nhiệm của các cơ quan nhà nước, doanh nghiệp cung cấp dịch vụ viễn thông, nền tảng số và người dân dần được nâng cao.

Tuy nhiên, soi chiếu vào thực tiễn, khâu tổ chức thực hiện pháp luật về an ninh mạng vẫn bộc lộ những điểm nghẽn nhất định:

(1) Về tuân thủ pháp luật: Tình trạng cố tình vi phạm trên không gian mạng vẫn diễn biến phức tạp. Đáng chú ý là việc lộ lọt dữ liệu cá nhân, tấn công mạng, lừa đảo trực tuyến và phát tán thông tin xấu độc chưa được ngăn chặn triệt để.

(2) Về thi hành pháp luật: Hoạt động phối hợp liên ngành, chia sẻ thông tin cảnh báo và ứng phó sự cố giữa các cơ quan chức năng với doanh nghiệp trong một số tình huống thực tế còn thiếu sự đồng bộ, nhịp nhàng.

(3) Về sử dụng pháp luật: Người dân, cơ quan, tổ chức và doanh nghiệp chưa chủ động, linh hoạt trong việc sử dụng các công cụ, cơ chế pháp lý để tự bảo vệ mình, cũng như chưa kịp thời phản ánh, tố giác tội phạm khi đối mặt với rủi ro.

(4) Về áp dụng pháp luật: Các cơ quan có thẩm quyền đôi lúc còn lúng túng trong quy trình thụ lý, xác minh và xử lý các vụ việc phức tạp, có yếu tố xuyên biên giới; đặc biệt khâu truy vết và thu hồi tài sản trong các vụ án lừa đảo công nghệ cao thực tế triển khai gặp vô vàn trở ngại.

Nguyên nhân của những hạn chế, điểm nghẽn trong khâu tổ chức thực hiện nêu trên xuất phát từ các yếu tố khách quan và chủ quan sau đây:

Về nguyên nhân khách quan: Tính chất ẩn danh, phi biên giới và tốc độ lan truyền chóng mặt của không gian mạng tạo ra rào cản cực lớn cho công tác thực thi pháp luật. Tội phạm mạng và các chủ thể vi phạm triệt để lợi dụng công nghệ cao (Deepfake, AI, tiền mã hóa, tài khoản ảo...) cùng các phương thức che giấu dấu vết tinh vi. Điều này trực tiếp gây khó khăn cho các cơ quan thực thi trong quá trình phát hiện vi phạm, thu thập, phục hồi chứng cứ điện tử, định danh chủ thể và áp dụng các biện pháp ngăn chặn kịp thời.

Về nguyên nhân chủ quan, đây là nhóm nguyên nhân nòng cốt dẫn tới hạn chế trong thực tiễn thi hành, cụ thể là.

*Thứ nhất*, về nhận thức và ý thức: Nhận thức, kỹ năng an toàn thông tin và ý thức tuân thủ pháp luật, tự bảo vệ dữ liệu của một bộ phận người dân, tổ chức, cơ quan còn hạn chế. Tâm lý chủ quan, mất cảnh giác vẫn phổ biến, tạo lỗ hổng cho tội phạm triệt để khai thác, lợi dụng.

*Thứ hai*, về năng lực và nguồn lực thực thi: Năng lực của một bộ phận cán bộ chuyên trách, lực lượng điều tra số chưa thực sự theo kịp tốc độ biến hóa của công nghệ vi phạm. Hạ tầng kỹ thuật, hệ thống giám sát, cảnh báo sớm và công cụ hỗ trợ thu thập chứng cứ số chưa được đầu tư đồng bộ, thiếu hụt nguồn lực tài chính ở nhiều địa phương, ban ngành.

*Thứ ba*, về khâu tổ chức phối hợp thực tế: Việc vận hành cơ chế phối hợp thực tế giữa cơ quan quản lý nhà nước, lực lượng chuyên trách với các doanh nghiệp, đặc biệt là các nhà cung cấp nền tảng xuyên biên giới (trong việc gỡ bỏ nội dung, cung cấp dữ liệu phục vụ điều tra) đôi lúc còn chậm trễ, thủ tục hành chính kéo dài, làm lỡ “thời điểm vàng” trong xử lý vi phạm.

*Thứ tư*, về công tác tuyên truyền: Hoạt động phổ biến, giáo dục pháp luật về an ninh mạng ở một số nơi vẫn nặng tính hình thức, chưa đa dạng hóa phương thức tiếp cận và chưa đủ độ “sâu, sát” để biến thành kỹ năng phản xạ tự nhiên cho từng nhóm đối tượng cụ thể (người già, học sinh, sinh viên, công nhân...).

Tóm lại, từ thực tiễn trên cho thấy, để pháp luật về an ninh mạng thực sự đi vào đời sống, phát huy hiệu quả điều chỉnh, rào cản lớn nhất hiện nay không chỉ nằm ở bản thân các quy định của pháp luật mà nằm ở khâu tổ chức thực hiện. Những vướng mắc về năng lực áp dụng pháp luật, hạn chế trong ý thức tuân thủ, sự thiếu đồng bộ trong phối hợp thực tiễn và sự thiếu hụt về các điều kiện bảo đảm thi hành chính là cơ sở thực tiễn cấp thiết. Đây là tiền đề quan trọng để luận án tiếp tục đi sâu nghiên cứu, đề xuất các nhóm giải pháp nhằm đổi mới và nâng cao hiệu quả tổ chức thực hiện pháp luật về an ninh mạng tại Việt Nam.

### **Tiểu kết Chương 3**

Trên cơ sở khung lý luận đã khái quát tại chương 2 Luận án, nghiên cứu sinh đã khái lược quá trình hình thành, phát triển của pháp luật về an ninh mạng ở nước ta. Đánh giá chung, hiện nay, pháp luật về an ninh mạng ở nước ta đã được xác lập rõ nét và tương đối toàn diện với đầy đủ 06 nhóm chế định về: nguyên tắc về bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng; địa vị pháp lý của các chủ thể tham gia hoạt động trong lĩnh vực an ninh mạng; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế trong lĩnh vực an ninh mạng. Theo đó, 06 nhóm chế định trên của pháp luật về an ninh mạng được ban hành đã không chỉ đáp ứng trước yêu cầu thực tiễn mà còn thể hiện sự thích ứng mạnh mẽ của Đảng, Nhà nước ta với cuộc Cách mạng công nghiệp lần thứ tư, với bối cảnh hội nhập toàn diện, sâu rộng. Pháp luật về an ninh mạng ở Việt Nam đã có những bước phát triển đáng kể trong việc bảo vệ không gian mạng

quốc gia, bảo vệ quyền lợi của người dân và tạo ra cơ sở pháp lý cho việc xử lý các vi phạm trong không gian mạng.

Tuy nhiên, hiện vẫn tồn tại một số vấn đề bất cập trong việc đồng bộ hóa các quy định pháp lý, xử lý tội phạm mạng xuyên quốc gia, bảo vệ quyền riêng tư và dữ liệu cá nhân, cũng như thiếu một lực lượng chuyên trách mạnh mẽ để bảo vệ an ninh mạng. Nguyên nhân dẫn đến thực trạng này bao gồm các yếu tố liên quan đến sự phát triển nhanh chóng của công nghệ, sự thay đổi của các mối đe dọa mạng, thiếu hụt nguồn lực và nhân sự, cũng như sự thiếu đồng bộ trong các quy định pháp lý và thiếu sự phối hợp hiệu quả giữa các cơ quan chức năng.

Để khắc phục những vấn đề còn tồn tại trong pháp luật về an ninh mạng, cần có thực hiện đồng bộ nhiều giải pháp khác nhau như hoàn thiện pháp lý, tăng cường nguồn lực, hợp tác quốc tế, ứng dụng công nghệ và nâng cao nhận thức cộng đồng. Những giải pháp này không chỉ giúp bảo vệ an ninh mạng quốc gia mà còn góp phần xây dựng một môi trường mạng an toàn và bền vững cho người dân và tổ chức. Như vậy, các tồn tại, bất cập của pháp luật về an ninh mạng ở Việt Nam không chỉ xuất phát từ hạn chế nội tại của hệ thống pháp luật mà còn do tác động của bối cảnh công nghệ, toàn cầu hóa và đặc thù của không gian mạng. Việc nhận diện đầy đủ các nhóm hạn chế và nguyên nhân nêu trên là cơ sở quan trọng để đề xuất các nhóm giải pháp hoàn thiện pháp luật tại mục 4.3.1 theo hướng đồng bộ, hiện đại, khả thi và phù hợp với các chuẩn mực quốc tế, góp phần nâng cao hiệu quả bảo vệ an ninh mạng trong giai đoạn hiện nay.

## **Chương 4**

# **YÊU CẦU, QUAN ĐIỂM VÀ GIẢI PHÁP HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM**

## **4.1. YÊU CẦU HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM**

### **4.1.1. Bảo đảm sự lãnh đạo toàn diện, trực tiếp của Đảng, phát huy cao độ tính Đảng trong hoàn thiện pháp luật về an ninh mạng**

Bảo đảm sự lãnh đạo toàn diện, trực tiếp của Đảng trong việc xây dựng, chỉ đạo các chính sách về an ninh mạng là yêu cầu đầu tiên, quan trọng nhất và thể hiện rõ bản chất của Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam. Trong thực tiễn hiện nay, cần không ngừng nâng cao nhận thức của cán bộ, đảng viên và toàn thể xã hội về tầm quan trọng của không gian mạng cũng như nhiệm vụ bảo vệ an ninh mạng. Đảng ta cần phát huy mạnh mẽ vai trò tuyên truyền, giáo dục ý thức, trách nhiệm bảo vệ an ninh mạng cho các tầng lớp nhân dân, từ đó hình thành Thế trận An ninh nhân dân trên không gian mạng. Từ đó, để không ngừng phát huy vai trò, sức mạnh của quần chúng nhân dân trong nhiệm vụ bảo đảm an toàn, an ninh mạng, từ đó nắm bắt kịp thời, tận dụng hiệu quả các cơ hội do không gian mạng mang lại để phát triển kinh tế, xã hội và đồng thời luôn chủ động phòng ngừa, sẵn sàng ứng phó trước các tác động tiêu cực nhằm bảo vệ ANQG, bảo đảm TTATXH.

Theo đó, pháp luật về an ninh mạng cần được xây dựng và hoàn thiện theo hướng bảo vệ tối đa quyền lợi của quốc gia, đồng thời phù hợp với các điều kiện thực tế. Có nghĩa là mỗi quy định pháp lý về an ninh mạng được ban hành phải bảo đảm các yêu cầu về mặt pháp lý để bảo vệ an ninh mạng và đồng thời phải phản ánh đúng quan điểm, đường lối của Đảng trong việc bảo vệ ANQG.

Quá trình xây dựng và thực thi những quy định của pháp luật về an ninh mạng, Đảng ta cần lãnh đạo, chỉ đạo việc phối hợp giữa các cơ quan nhà nước, lực lượng vũ trang, các tổ chức, doanh nghiệp và người dân trong việc

bảo vệ an ninh mạng. Trong bối cảnh xã hội hiện nay, Đảng ta cần quan tâm, chú trọng việc lãnh đạo các cơ quan chức năng tăng cường kiểm tra, giám sát và xử lý nghiêm minh các hành vi vi phạm an ninh mạng, bảo đảm tính nghiêm minh của pháp luật. Đồng thời, cần chỉ đạo nghiên cứu các cơ chế mới để phát hiện, xử lý kịp thời các mối đe dọa an ninh mạng trong bối cảnh công nghệ ngày càng phát triển. Đặc biệt, để hoàn thiện pháp luật về an ninh mạng, Đảng ta cần nghiên cứu, xác lập cơ chế, tạo điều kiện để các tổ chức chính trị, xã hội, đặc biệt là các tổ chức thanh niên, phụ nữ và các tổ chức khác có thể tham gia vào công tác bảo vệ an ninh mạng.

#### **4.1.2. Đổi mới tư duy, định hướng hoàn thiện pháp luật về an ninh mạng theo hướng vừa bảo đảm yêu cầu quản lý nhà nước, vừa khuyến khích đổi mới, sáng tạo**

Đổi mới tư duy và định hướng hoàn thiện pháp luật về an ninh mạng là yêu cầu cấp thiết của nước ta trong bối cảnh phát triển của cuộc Cách mạng công nghiệp lần thứ Tư cùng với sự trỗi dậy của của trào lưu hội nhập toàn cầu. Để đạt được mục tiêu vừa bảo đảm yêu cầu quản lý nhà nước, vừa khuyến khích sáng tạo và giải phóng toàn bộ sức sản xuất, khơi thông mọi nguồn lực phát triển đất nước, pháp luật về an ninh mạng cần được xây dựng theo hướng vừa bảo đảm quyền, lợi ích hợp pháp của các tổ chức, cá nhân trong môi trường mạng vừa kiểm soát, xử lý hiệu quả và đủ tính răn đe với các hành vi vi phạm pháp luật về an ninh mạng. Tuy nhiên, trong quá trình thực thi pháp luật, cần bảo đảm rằng các quy định được ban hành không làm hạn chế sự sáng tạo, phát triển về công nghệ cùng với các hoạt động kinh tế số trong môi trường mạng. Do đó, đòi hỏi là Đảng, Nhà nước ta phải thiết lập các cơ chế giám sát và quản lý mềm dẻo, linh hoạt trong các lĩnh vực quản lý nhà nước có liên quan đến an ninh mạng.

Đặc biệt, bối cảnh hiện nay đòi hỏi chính sách và pháp luật về an ninh mạng cần khuyến khích, tạo động lực để các doanh nghiệp, tổ chức sáng tạo và đổi mới đặc biệt là trong các lĩnh vực công nghệ cao, trí tuệ nhân tạo, dữ

liệu lớn, blockchain... Chính sách pháp lý cũng cần tạo ra một môi trường pháp lý ổn định và dễ hiểu cho các tổ chức, doanh nghiệp và cá nhân trong việc thực hiện các sáng kiến đổi mới sáng tạo.

Pháp luật về an ninh mạng còn phải là công cụ thúc đẩy các nguồn lực xã hội, đặc biệt là trong việc huy động và sử dụng hiệu quả các nguồn lực phát triển kinh tế, giáo dục và văn hóa trong thời đại số. Việc bảo vệ dữ liệu và thông tin không chỉ để chống lại các nguy cơ mất mát tài nguyên, mà còn giúp khai thác, sử dụng hiệu quả tài nguyên và tối ưu hóa quá trình chuyển đổi số.

Trong một thế giới liên kết chặt chẽ như hiện nay, pháp luật về an ninh mạng không chỉ là vấn đề của một quốc gia mà còn là vấn đề toàn cầu. Do đó, pháp luật về an ninh mạng cần có những quy định nhằm bảo vệ lợi ích quốc gia nhưng cũng phải chú trọng đến sự hợp tác quốc tế, nhằm đối phó với các mối đe dọa từ không gian mạng xuyên biên giới.

Tóm lại, đổi mới tư duy và định hướng hoàn thiện pháp luật về an ninh mạng theo hướng vừa bảo đảm quản lý nhà nước vừa khuyến khích sáng tạo và phát triển nguồn lực đất nước là một quá trình phức tạp và cần sự phối hợp chặt chẽ giữa các cơ quan nhà nước, doanh nghiệp và các tổ chức quốc tế. Điều này tạo ra một môi trường pháp lý an toàn để thúc đẩy phát triển kinh tế số, công nghệ và sáng tạo.

#### **4.1.3. Tạo đột phá, gắn kết chặt chẽ giữa xây dựng, hoàn thiện pháp luật về an ninh mạng với công tác thi hành pháp luật trong thực tế**

Để tạo đột phá và gắn kết chặt chẽ giữa việc xây dựng, hoàn thiện pháp luật về an ninh mạng với công tác thi hành pháp luật trong thực tế cần tăng cường sự phối hợp giữa các cơ quan chức năng. Cụ thể là, cần xây dựng cơ chế liên kết hiệu quả giữa các cơ quan này, để tạo ra một hệ thống pháp lý và thi hành đồng bộ, giúp bảo đảm việc thực thi pháp luật về an ninh mạng nhanh chóng, chính xác và minh bạch. Pháp luật về an ninh mạng cần được hoàn thiện để có thể ứng phó linh hoạt với những thay đổi nhanh chóng trong

môi trường công nghệ. Điều này đòi hỏi các cơ quan chức năng phải thường xuyên rà soát, cập nhật và điều chỉnh các quy định pháp lý, nhằm bảo đảm rằng các quy định pháp lý đang có hiệu lực phù hợp với thực tế phát triển của công nghệ và ứng phó được trước các mối đe dọa về an ninh mạng. Đồng thời, cần nghiên cứu, thử nghiệm một số cơ chế pháp lý linh hoạt áp dụng trong thực tiễn và dễ thích ứng với sự thay đổi của môi trường mạng.

Pháp luật về an ninh mạng không thể chỉ do các cơ quan nhà nước thực thi mà còn cần sự tham gia tích cực của các doanh nghiệp, tổ chức và cộng đồng. Để làm được điều này, pháp luật cần tạo ra các cơ chế khuyến khích và hỗ trợ doanh nghiệp trong việc thực thi các quy định pháp luật về an ninh mạng. Bên cạnh đó, cần thường xuyên tuyên truyền và nâng cao nhận thức về an ninh mạng trong cộng đồng, coi đây là một phần quan trọng trong việc gắn kết pháp luật và thực tiễn thi hành. Đặc biệt, pháp luật về an ninh mạng cần phải có những quy định liên quan đến việc hợp tác quốc tế trong bảo vệ an ninh mạng, đặc biệt là trong các tình huống liên quan đến các mối đe dọa xuyên biên giới.

#### **4.1.4. Tăng cường chuyển đổi số, ứng dụng trí tuệ nhân tạo, dữ liệu lớn trong công tác hoàn thiện pháp luật về an ninh mạng**

Tăng cường chuyển đổi số và ứng dụng trí tuệ nhân tạo cùng dữ liệu lớn trong công tác hoàn thiện pháp luật về an ninh mạng là một xu hướng tất yếu trong bối cảnh bùng nổ của cuộc Cách mạng công nghiệp lần thứ tư. Việc áp dụng các công nghệ tiên tiến này không chỉ giúp nâng cao hiệu quả quản lý và thực thi pháp luật, mà còn góp phần bảo vệ ANQG và tạo ra môi trường mạng an toàn, minh bạch.

Pháp luật về an ninh mạng cần được hoàn thiện theo hướng “thông minh”, có khả năng tự động cập nhật và điều chỉnh theo tình hình thực tế. Các công nghệ AI có thể hỗ trợ phân tích các xu hướng pháp lý và những lỗ hổng trong hệ thống pháp luật hiện tại. AI có thể giúp tạo ra các cơ chế tự động điều chỉnh pháp luật, từ đó giúp hệ thống pháp lý luôn phản ánh được các thay đổi trong môi trường công nghệ và các mối đe dọa mới.

Blockchain, với tính năng bảo mật cao và khả năng duy trì tính toàn vẹn của dữ liệu, có thể được tích hợp vào hệ thống pháp lý về an ninh mạng để tăng cường độ tin cậy và bảo mật.

Thực tế, do AI có khả năng phân tích khối lượng dữ liệu lớn và phát hiện các mẫu vi phạm hoặc các hành vi đáng ngờ trong môi trường mạng do đó cần nghiên cứu ứng dụng AI trong giám sát và phát hiện vi phạm pháp luật về an ninh mạng. Điều này giúp giảm thiểu thiệt hại trước khi các cuộc tấn công xảy ra; AI có thể giúp tự động xử lý các báo cáo về sự cố an ninh mạng, phân tích các sự kiện và đưa ra các cảnh báo sớm, giúp các cơ quan chức năng can thiệp kịp thời.

Sử dụng dữ liệu lớn (Big Data) để phân tích và dự báo các mối đe dọa an ninh mạng. Dữ liệu lớn cung cấp góc nhìn sâu sắc về xu hướng và hành vi trên môi trường mạng, từ đó giúp dự báo và phòng ngừa các mối đe dọa. Điều này tạo ra cơ sở vững chắc để cải thiện pháp luật và chính sách liên quan.

## **4.2. QUAN ĐIỂM HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM**

### **4.2.1. Hoàn thiện pháp luật về an ninh mạng phải bảo đảm cân bằng giữa bảo vệ an ninh quốc gia và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức**

An ninh mạng gắn trực tiếp với ANQG, chủ quyền quốc gia trên không gian mạng, TTATXH và sự vận hành ổn định của Nhà nước, nền kinh tế, xã hội số. Trong bối cảnh hoạt động quản lý nhà nước, sản xuất, kinh doanh, giao dịch dân sự, cung ứng dịch vụ công và đời sống cá nhân ngày càng phụ thuộc vào hệ thống thông tin, dữ liệu số và hạ tầng kết nối, mọi nguy cơ xâm phạm an ninh mạng đều có thể gây tác động vượt ra ngoài phạm vi kỹ thuật đơn thuần. Vì vậy, pháp luật về an ninh mạng phải tạo lập cơ sở pháp lý cần thiết để Nhà nước và các cơ quan có thẩm quyền phòng ngừa, phát hiện, ngăn chặn, xử lý kịp thời, hiệu quả các nguy cơ, hành vi xâm phạm an ninh mạng.

Tuy nhiên, hoàn thiện pháp luật về an ninh mạng không thể chỉ được tiếp cận từ yêu cầu tăng cường công cụ quản lý nhà nước mà nó phải đặt trên cơ sở bảo đảm hài hòa giữa hai yêu cầu cơ bản: một mặt, pháp luật phải bảo đảm cho Nhà nước có đủ năng lực pháp lý để bảo vệ ANQG, TTATXH trên không gian mạng; mặt khác, pháp luật phải bảo đảm để quyền, lợi ích hợp pháp của cá nhân, tổ chức không bị hạn chế một cách tùy tiện, không cần thiết hoặc không tương xứng.

Từ quan điểm đó, pháp luật về an ninh mạng cần được hoàn thiện theo hướng quy định rõ các nguyên tắc áp dụng biện pháp bảo vệ an ninh mạng. Bên cạnh đó, cần tiếp tục hoàn thiện cơ chế kiểm soát quyền lực trong lĩnh vực an ninh mạng. Đây là yêu cầu quan trọng nhằm bảo đảm pháp luật về an ninh mạng không chỉ có hiệu lực trong bảo vệ ANQG, mà còn góp phần bảo vệ công lý, quyền và lợi ích hợp pháp của các chủ thể trong xã hội số.

Đối với cá nhân, tổ chức và doanh nghiệp, pháp luật về an ninh mạng cần xác định rõ quyền, nghĩa vụ và trách nhiệm pháp lý của từng nhóm chủ thể. Đặc biệt, trong bối cảnh Luật An ninh mạng năm 2025 đã được ban hành, quan điểm bảo đảm hài hòa giữa yêu cầu bảo vệ ANQG và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức càng cần được quán triệt trong quá trình xây dựng văn bản hướng dẫn thi hành và tổ chức thực hiện pháp luật.

#### **4.2.2. Hoàn thiện pháp luật về an ninh mạng phải dựa trên quản trị rủi ro, không chỉ dựa trên xử lý sau vi phạm**

Các nguy cơ trong lĩnh vực an ninh mạng có đặc điểm khác biệt so với những loại nguy cơ truyền thống. Bởi chúng thường phát sinh nhanh, lan truyền rộng, khó nhận diện kịp thời, khó xác định đầy đủ chủ thể thực hiện hành vi và có thể gây hậu quả nghiêm trọng trong thời gian rất ngắn. Đặc biệt, do tính chất xuyên biên giới của không gian mạng, hành vi vi phạm có thể được thực hiện từ bên ngoài lãnh thổ Việt Nam nhưng gây hậu quả trực tiếp trong lãnh thổ Việt Nam, làm cho việc phát hiện, ngăn chặn, điều tra và xử lý gặp nhiều khó khăn.

Trong bối cảnh đó, nếu pháp luật về an ninh mạng chỉ tập trung vào xử lý sau khi hành vi vi phạm đã xảy ra thì không đáp ứng được yêu cầu bảo vệ an ninh mạng trong điều kiện hiện nay. Đối với an ninh mạng, khi hậu quả đã xảy ra thì thiệt hại về dữ liệu, uy tín, tài sản, bí mật nhà nước, bí mật cá nhân, hoạt động của hệ thống thông tin hoặc niềm tin xã hội có thể rất khó khắc phục hoàn toàn. Vì vậy, pháp luật về an ninh mạng cần chuyển mạnh từ tư duy xử lý sau vi phạm sang tư duy quản trị rủi ro, lấy phòng ngừa, cảnh báo sớm, phát hiện sớm, ứng phó kịp thời và phục hồi nhanh làm trọng tâm.

Quản trị rủi ro trong lĩnh vực an ninh mạng đòi hỏi pháp luật phải được thiết kế theo hướng chủ động nhận diện, đánh giá, phân loại và kiểm soát nguy cơ trước khi nguy cơ chuyển hóa thành sự cố hoặc hành vi vi phạm gây hậu quả nghiêm trọng. Trên cơ sở nhận diện, đánh giá, phân loại nguy cơ, pháp luật cần xác lập yêu cầu bảo vệ tương ứng, tránh tình trạng áp dụng cào bằng nghĩa vụ bảo đảm an ninh mạng đối với mọi chủ thể, mọi hệ thống và mọi loại dữ liệu.

Cách tiếp cận dựa trên quản trị rủi ro cũng đòi hỏi phải hoàn thiện các quy định về cảnh báo sớm, kiểm tra định kỳ, giám sát an ninh mạng, diễn tập ứng phó sự cố, báo cáo sự cố, chia sẻ thông tin về nguy cơ và phục hồi sau sự cố. Đây là những công cụ pháp lý có ý nghĩa phòng ngừa đặc biệt quan trọng.

Đặc biệt, trong điều kiện chuyển đổi số quốc gia và sau khi Luật An ninh mạng năm 2025 được ban hành, yêu cầu quản trị rủi ro càng cần được quán triệt trong quá trình hoàn thiện pháp luật và tổ chức thi hành pháp luật về an ninh mạng. Các quy định pháp luật cần được cụ thể hóa theo hướng xác định rõ hệ thống thông tin nào cần được bảo vệ ở mức độ cao hơn, loại dữ liệu nào cần cơ chế bảo vệ nghiêm ngặt hơn, chủ thể nào có nghĩa vụ tuân thủ cao hơn và trường hợp nào phải áp dụng biện pháp ứng phó khẩn cấp.

#### **4.2.3. Hoàn thiện pháp luật về an ninh mạng phải bảo đảm tính đồng bộ giữa quy phạm pháp luật và cơ chế thực thi**

Một quy định pháp luật chỉ có giá trị thực tiễn khi có khả năng được tổ chức thi hành đầy đủ, thống nhất và hiệu quả. Đối với lĩnh vực an ninh mạng,

yêu cầu này càng có ý nghĩa đặc biệt quan trọng, bởi đây là lĩnh vực có tính kỹ thuật cao, tính liên ngành, tính xuyên biên giới và chịu sự tác động trực tiếp của sự phát triển nhanh chóng của công nghệ. Do đó, hoàn thiện pháp luật về an ninh mạng không thể chỉ dừng lại ở việc sửa đổi, bổ sung câu chữ trong văn bản QPPL, mà phải đồng thời hoàn thiện thiết chế thực thi, nguồn lực bảo đảm, quy trình phối hợp, năng lực kỹ thuật, cơ chế giám sát và trách nhiệm giải trình của các chủ thể có liên quan.

Trong thực tiễn, nếu pháp luật chỉ được hoàn thiện ở phương diện hình thức văn bản mà không có cơ chế tổ chức thực hiện tương ứng, thì các quy định dù đầy đủ về nội dung vẫn khó phát huy hiệu quả trong đời sống xã hội. Ngược lại, nếu chỉ chú trọng tăng cường hoạt động thực thi mà thiếu các quy định pháp luật rõ ràng, minh bạch và có giới hạn cụ thể, thì nguy cơ áp dụng tùy tiện, không thống nhất hoặc xâm phạm quyền, lợi ích hợp pháp của cá nhân, tổ chức có thể gia tăng.

Từ đó, hoàn thiện pháp luật về an ninh mạng cần được tiến hành đồng bộ trên cả hai phương diện: hoàn thiện nội dung QPPL và hoàn thiện cơ chế tổ chức thi hành pháp luật. Về nội dung quy phạm, pháp luật cần xác định rõ nguyên tắc bảo vệ an ninh mạng, hành vi vi phạm, chế tài xử lý, quyền và nghĩa vụ của các chủ thể, biện pháp bảo vệ an ninh mạng, cơ chế phối hợp và hợp tác quốc tế. Về cơ chế thực thi, cần hoàn thiện mô hình tổ chức lực lượng bảo vệ an ninh mạng, phân định rõ trách nhiệm giữa các cơ quan nhà nước, thiết lập quy trình phối hợp liên ngành, nâng cao năng lực kỹ thuật, tăng cường nguồn nhân lực chất lượng cao và bảo đảm điều kiện tài chính, công nghệ cho hoạt động thực thi pháp luật.

Bên cạnh đó, cần coi giám sát và trách nhiệm giải trình là bộ phận không thể tách rời của cơ chế thực thi pháp luật về an ninh mạng. Trong bối cảnh Luật An ninh mạng năm 2025 đã được ban hành, yêu cầu gắn kết giữa quy định pháp luật và cơ chế thực thi càng trở nên cấp thiết. Việc ban hành một đạo luật mới chỉ là bước khởi đầu của quá trình hoàn thiện pháp luật. Để đạo

luật đi vào đời sống, cần tiếp tục xây dựng các văn bản hướng dẫn thi hành, rà soát các văn bản pháp luật có liên quan, phân định rõ thẩm quyền của các cơ quan, bảo đảm nguồn lực tổ chức thực hiện và thiết lập cơ chế kiểm tra, giám sát việc thi hành. Nếu không có các điều kiện này, pháp luật về an ninh mạng có thể đầy đủ về mặt hình thức nhưng chưa bảo đảm hiệu quả thực tế.

#### **4.2.4. Hoàn thiện pháp luật về an ninh mạng phải thích ứng với công nghệ nhưng không chạy theo từng hiện tượng kỹ thuật đơn lẻ**

An ninh mạng là lĩnh vực chịu tác động trực tiếp, thường xuyên và sâu sắc của sự phát triển khoa học, công nghệ. Trong khi đó, pháp luật có tính ổn định tương đối và việc sửa đổi, bổ sung văn bản QPPL luôn phải tuân theo trình tự, thủ tục chặt chẽ. Do đó, pháp luật không thể và cũng không nên được thiết kế theo hướng sửa đổi liên tục để ứng phó với từng dạng tấn công mạng, từng công nghệ mới hoặc từng mô hình nền tảng mới phát sinh trong thực tiễn.

Nếu pháp luật được xây dựng theo cách quá chi tiết, liệt kê cứng từng hành vi, từng công nghệ hoặc từng phương thức kỹ thuật cụ thể, thì các quy định có thể nhanh chóng lạc hậu trước sự phát triển của công nghệ. Ngược lại, nếu pháp luật chỉ quy định quá chung, thiếu tiêu chí nhận diện và thiếu cơ chế hướng dẫn cụ thể, gây khó khăn cho quá trình áp dụng, làm giảm tính minh bạch, tính khả thi và có thể dẫn đến nguy cơ áp dụng tùy tiện. Vì vậy, hoàn thiện pháp luật về an ninh mạng cần được thực hiện theo hướng kết hợp hợp lý giữa tính ổn định của QPPL và tính linh hoạt của cơ chế tổ chức thực thi.

Theo đó, pháp luật về an ninh mạng cần được thiết kế trên cơ sở kết hợp giữa quy định nguyên tắc, tiêu chí nhận diện mở, danh mục hành vi điển hình, quy chuẩn kỹ thuật cập nhật và cơ chế hướng dẫn thi hành linh hoạt nhưng phải được đặt trong khuôn khổ của Nhà nước pháp quyền.

Trong bối cảnh Luật An ninh mạng năm 2025 đã được ban hành, yêu cầu bảo đảm khả năng thích ứng với công nghệ cần được quán triệt trong quá trình xây dựng văn bản hướng dẫn thi hành và rà soát các văn bản pháp luật có liên quan. Việc hoàn thiện này phải bảo đảm pháp luật không bị động trước sự

phát triển của công nghệ, nhưng cũng không cực đoan hóa việc kiểm soát đến mức cản trở đổi mới sáng tạo, phát triển kinh tế số và quyền tự do kinh doanh hợp pháp của doanh nghiệp.

### **4.3. GIẢI PHÁP HOÀN THIỆN PHÁP LUẬT VỀ AN NINH MẠNG Ở VIỆT NAM**

#### **4.3.1. Nhóm giải pháp hoàn thiện nội dung pháp luật về an ninh mạng theo các nhóm chế định**

##### ***4.3.1.1. Hoàn thiện nhóm quy định về nguyên tắc bảo vệ an ninh mạng***

Mặc dù pháp luật về an ninh mạng ở Việt Nam đã bước đầu xác lập được các nguyên tắc cơ bản trong hoạt động bảo vệ an ninh mạng, nhưng các quy định này vẫn còn phân tán, chưa thể hiện đầy đủ mối quan hệ giữa bảo vệ ANQG, quản trị rủi ro công nghệ và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức. Một số nguyên tắc có ý nghĩa nền tảng như nguyên tắc cần thiết, tương xứng, trách nhiệm giải trình, kiểm soát quyền lực nhà nước, phân tầng rủi ro và phối hợp đa chủ thể chưa được ghi nhận đầy đủ hoặc chưa được cụ thể hóa rõ ràng trong các quy định pháp luật hiện hành. Điều này làm cho việc áp dụng pháp luật trong thực tiễn có lúc còn thiếu thống nhất, thiếu cơ sở pháp lý rõ ràng, nhất là khi áp dụng các biện pháp bảo vệ an ninh mạng có khả năng tác động đến quyền, lợi ích hợp pháp của cá nhân, tổ chức.

Vì vậy, trong thời gian tới, cần tiếp tục nghiên cứu, bổ sung và cụ thể hóa hệ thống nguyên tắc bảo vệ an ninh mạng theo hướng đầy đủ, đồng bộ, minh bạch và phù hợp với yêu cầu xây dựng Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam trong kỷ nguyên số. Theo đó, pháp luật về an ninh mạng cần nghiên cứu điều chỉnh, bổ sung trực tiếp vào Điều 4 Luật An ninh mạng năm 2025 các nguyên tắc cơ bản sau:

*Thứ nhất*, bổ sung nguyên tắc quản trị rủi ro an ninh mạng. Cần xác định rõ bảo vệ an ninh mạng không chỉ là hoạt động xử lý hành vi vi phạm sau khi đã xảy ra, mà trước hết phải là quá trình nhận diện, đánh giá, dự báo,

phòng ngừa, cảnh báo, ứng phó và phục hồi trước các nguy cơ. Quản trị rủi ro cần chuyển dịch từ việc chỉ xử lý các vụ việc, sự cố đơn lẻ sang quản trị tổng thể; lấy năng lực chống chịu, chuyển trạng thái và phục hồi nhanh làm thước đo. Để cụ thể hóa, kiến nghị bổ sung Khoản 6 vào Điều 4 Luật An ninh mạng năm 2025 với nội dung: “6. Áp dụng nguyên tắc quản trị rủi ro; chủ động nhận diện, đánh giá, dự báo, phòng ngừa, cảnh báo từ sớm, từ xa; lấy năng lực chống chịu, chuyển trạng thái và phục hồi nhanh làm thước đo hiệu quả bảo vệ an ninh mạng.”

*Thứ hai*, cụ thể hóa, làm rõ nguyên tắc cân bằng giữa yêu cầu bảo vệ ANQG và bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức. Các biện pháp bảo vệ an ninh mạng phải được áp dụng đúng mục đích, đúng thẩm quyền, tương xứng với tính chất, mức độ nguy cơ. Yêu cầu này đòi hỏi pháp luật phải lấy con người làm trung tâm, coi an ninh con người trên không gian mạng là mục tiêu và thước đo cuối cùng; không được phép tạo gánh nặng hành chính hoặc cản trở hoạt động đổi mới sáng tạo hợp pháp. Do đó, kiến nghị sửa đổi, bổ sung Khoản 3 Điều 4 Luật An ninh mạng năm 2025 thành: “3. Kết hợp chặt chẽ giữa bảo vệ an ninh mạng với phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, bảo vệ dữ liệu cá nhân...; việc áp dụng các biện pháp bảo vệ phải tương xứng với mức độ rủi ro, lấy an ninh con người làm trung tâm và không tạo gánh nặng hành chính hoặc cản trở đổi mới sáng tạo hợp pháp của tổ chức, cá nhân.”

*Thứ ba*, bổ sung nguyên tắc về trách nhiệm giải trình trong hoạt động bảo vệ an ninh mạng. Cơ quan, tổ chức có thẩm quyền khi áp dụng biện pháp bảo vệ an ninh mạng phải có trách nhiệm giải thích, làm rõ căn cứ pháp lý, mục đích, phạm vi, thời hạn và hậu quả pháp lý của biện pháp được áp dụng. Đồng thời, cần pháp điển hóa trách nhiệm cá nhân đối với công tác này bằng việc gắn trách nhiệm bảo vệ với người đứng đầu. Về mặt lập pháp, kiến nghị bổ sung Khoản 7 vào Điều 4 Luật An ninh mạng năm 2025 với nội dung: “7.

Đề cao trách nhiệm giải trình. Người đứng đầu cơ quan, tổ chức chịu trách nhiệm trực tiếp, cao nhất về an ninh mạng, an ninh dữ liệu thuộc phạm vi quản lý; trách nhiệm này không được chuyển giao khi giao cho đơn vị chuyên trách hoặc thuê nhà cung cấp dịch vụ bên ngoài.”

*Thứ tư*, bổ sung nguyên tắc phối hợp đa chủ thể trong bảo vệ an ninh mạng. Bảo vệ an ninh mạng không chỉ là nhiệm vụ của cơ quan nhà nước, mà còn là trách nhiệm chung của doanh nghiệp, chủ quản hệ thống thông tin, tổ chức xã hội. Hệ thống pháp luật cần tạo cơ sở để tổ chức bảo vệ theo một kiến trúc thống nhất, liên thông; chuyển từ bảo vệ riêng lẻ sang bảo vệ hệ thống. Để hiện thực hóa điều này, kiến nghị sửa đổi, cụ thể hóa Khoản 2 Điều 4 Luật An ninh mạng năm 2025 thành: “2. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam; sự quản lý thống nhất của Nhà nước; tổ chức bảo vệ theo kiến trúc thống nhất, thiết lập cơ chế phối hợp và trách nhiệm liên thông giữa cơ quan nhà nước, chủ quản hệ thống thông tin và doanh nghiệp cung cấp nền tảng số; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc...”

Việc bổ sung và cụ thể hóa các nguyên tắc tại Điều 4 nêu trên có ý nghĩa trực tiếp đối với việc nâng cao chất lượng của pháp luật về an ninh mạng. Trước hết, các nguyên tắc này góp phần tăng cường tính đồng bộ của hệ thống pháp luật, bởi chúng tạo ra định hướng chung cho việc xây dựng, sửa đổi các quy định cụ thể về hành vi vi phạm, chế tài xử lý, biện pháp bảo vệ. Đồng thời, khắc phục triệt để tính chung chung, tạo cơ sở pháp lý vững chắc, minh bạch để cơ quan có thẩm quyền áp dụng, còn cá nhân, tổ chức có thể nhận diện rõ quyền, nghĩa vụ và trách nhiệm pháp lý của mình.

#### ***4.3.1.2. Hoàn thiện nhóm quy định hành vi vi phạm pháp luật về an ninh mạng***

Các quy định về hành vi vi phạm pháp luật về an ninh mạng hiện nay vẫn còn một số hạn chế nhất định. Một số quy định chưa bao quát đầy đủ các hành vi mới phát sinh trong thực tiễn; một số dấu hiệu pháp lý của hành vi vi

phạm chưa được nhận diện rõ ràng; ranh giới giữa vi phạm hành chính và tội phạm hình sự trong lĩnh vực an ninh mạng còn có trường hợp khó xác định. Bên cạnh đó, pháp luật hiện hành chưa điều chỉnh đầy đủ hoặc chưa có cơ chế xử lý hiệu quả đối với các hành vi liên quan đến trí tuệ nhân tạo, deepfake, tài sản số, tiền mã hóa, dữ liệu cá nhân, cơ sở dữ liệu quốc gia, hệ thống định danh điện tử, xác thực điện tử và các nền tảng số xuyên biên giới. Điều này đòi hỏi phải có cơ chế pháp lý để nhận diện, xử lý các hành vi xâm phạm chuỗi cung ứng công nghệ, an ninh không gian tầm thấp và các chiến dịch thao túng nhận thức có tổ chức. Vì vậy, cần tiếp tục hoàn thiện nhóm quy định về hành vi vi phạm pháp luật về an ninh mạng theo các hướng sau:

*Thứ nhất*, thiết kế lại quy định về hành vi vi phạm pháp luật về an ninh mạng theo mô hình kết hợp giữa liệt kê hành vi điển hình và tiêu chí nhận diện mở. Trong điều kiện công nghệ số phát triển nhanh, nếu pháp luật chỉ liệt kê cứng các hành vi vi phạm cụ thể thì sẽ dễ lạc hậu trước sự xuất hiện của các phương thức, thủ đoạn mới. Ngược lại, nếu quy định quá khái quát, thiếu tiêu chí nhận diện cụ thể thì có thể gây khó khăn cho việc áp dụng pháp luật, thậm chí làm phát sinh nguy cơ áp dụng tùy tiện. Do đó, pháp luật về an ninh mạng, cụ thể là Điều 7 và Điều 13 Luật An ninh mạng năm 2025 cần được thiết kế theo hướng kết hợp giữa danh mục hành vi vi phạm điển hình với hệ thống tiêu chí nhận diện mở. Theo đó, pháp luật vẫn cần liệt kê các hành vi vi phạm cơ bản như quy định hiện hành nhưng cần nghiên cứu bổ sung một khoản mới, cụ thể như tại Khoản 9 Điều 7 để quy định các tiêu chí nhận diện hành vi xâm phạm an ninh mạng, bao gồm: mục tiêu xâm phạm; phương thức kỹ thuật được sử dụng; tính chất, mức độ hậu quả; phạm vi ảnh hưởng; tốc độ và khả năng lan truyền; loại dữ liệu, hệ thống hoặc chủ thể bị tác động; mức độ nguy cơ đối với ANQG, TTATXH; mức độ xâm phạm quyền và lợi ích hợp pháp của cá nhân, tổ chức. Tiêu chí nhận diện cũng cần bao quát đến mức độ ảnh hưởng đối với chủ quyền dữ liệu, an ninh nhận thức,

khả năng duy trì hoạt động thiết yếu của hạ tầng số quốc gia và niềm tin của xã hội.

*Thứ hai*, bổ sung hoặc cụ thể hóa các nhóm hành vi vi phạm mới phát sinh trên không gian mạng. Thực tiễn hiện nay cho thấy nhiều hành vi vi phạm pháp luật về an ninh mạng không còn được thực hiện theo phương thức truyền thống, mà gắn với công nghệ mới, nền tảng số, dữ liệu lớn và dịch vụ xuyên biên giới. Vì vậy, cần nghiên cứu bổ sung hoặc cụ thể hóa một số nhóm hành vi tại Luật An ninh mạng năm 2025, cụ thể như:

*Một là*, bổ sung quy định nghiêm cấm hành vi lợi dụng trí tuệ nhân tạo để lừa đảo, kích động, xuyên tạc hoặc giả mạo video, hình ảnh, giọng nói của người khác trái quy định pháp luật (kiến nghị sửa đổi, bổ sung điểm g Khoản 2 Điều 7 Luật An ninh mạng năm 2025). Pháp luật cần quy định rõ hành vi lợi dụng trí tuệ nhân tạo để tự động hóa các chiến dịch chiến tranh thông tin, phát tán thông tin xấu độc, tạo mã độc biến thể tự điều chỉnh để vượt qua các cơ chế xác thực. Yêu cầu bắt buộc dán nhãn nhận diện đối với nội dung do trí tuệ nhân tạo tạo ra và xử lý nghiêm hành vi cố tình xóa bỏ hoặc làm giả nhãn nhận diện này.

*Hai là*, bổ sung và làm rõ các hành vi gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin, cơ sở dữ liệu quốc gia (kiến nghị mở rộng Khoản 3 Điều 7). Ngoài ra, cần bổ sung hành vi tấn công chuỗi cung ứng công nghệ, can thiệp vào quá trình sản xuất, cài cắm mã độc, cửa hậu (backdoor) vào các bản cập nhật phần mềm, thiết bị nhằm đánh cắp dữ liệu hoặc gây gián đoạn trên diện rộng.

*Ba là*, cụ thể hóa hành vi thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân của người khác, cũng như các hành vi làm lộ bí mật nhà nước, bí mật kinh doanh, bí mật cá nhân (kiến nghị sửa đổi, bổ sung điểm h Khoản 2 Điều 7). Cần nhận diện

thêm hành vi làm sai lệch, đầu độc dữ liệu huấn luyện trí tuệ nhân tạo và hành vi chuyển giao, xử lý dữ liệu xuyên biên giới trái quy định, xâm phạm chủ quyền dữ liệu quốc gia.

*Bốn là*, bổ sung hành vi làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng, tài sản mã hóa, tài sản số; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; sử dụng danh tính giả, tài khoản số trái phép để lừa đảo, chiếm đoạt tài sản (kiến nghị sửa đổi, bổ sung điểm e Khoản 2 Điều 7 và điểm g Khoản 4 Điều 13). Đồng thời, cần bổ sung chế tài đối với hành vi thiết lập hạ tầng ẩn danh, tổng đài ảo xuyên biên giới để phục vụ mục đích lừa đảo.

*Năm là*, thiết lập, cung cấp dịch vụ hoặc hỗ trợ vận hành, kinh doanh, giao dịch, mua bán, tiếp thị trực tuyến cho sàn giao dịch, trang thông tin điện tử, ứng dụng trái phép trên không gian mạng, bao gồm: sàn thương mại điện tử, sàn giao dịch tài sản số, kinh doanh theo phương thức đa cấp (kiến nghị sửa đổi, bổ sung điểm e Khoản 4 Điều 13). Cần thiết lập chế tài xử lý đối với hành vi tổ chức chiến dịch thao túng thông tin, chiến tranh nhận thức nhằm can thiệp vào quá trình tiếp nhận thông tin, định hướng tư duy và làm suy giảm niềm tin xã hội.

*Sáu là*, bổ sung các hành vi quảng cáo, buôn bán hàng giả, hàng hóa nhập lậu, môi giới mại dâm, truyền bá văn hóa phẩm đồi trụy, lạm dụng tình dục trẻ em, quấy rối tình dục và các hành vi vi phạm pháp luật khác trên không gian mạng (kiến nghị sửa đổi, bổ sung điểm đ Khoản 4 Điều 13). Bổ sung hành vi vi phạm an ninh không gian tầm thấp như: chiếm quyền điều khiển, gây nhiễu, giả mạo tín hiệu định vị đối với phương tiện bay không người lái, xâm nhập vùng cấm, giám sát trái phép và rò rỉ dữ liệu cảm biến đe dọa ANQG (kiến nghị bổ sung vào Điều 7).

*Thứ ba*, làm rõ ranh giới giữa vi phạm pháp luật hành chính và tội phạm hình sự trong lĩnh vực an ninh mạng. Một trong những khó khăn lớn

hiện nay là việc xác định hành vi vi phạm pháp luật về an ninh mạng cần xử lý hành chính hay truy cứu trách nhiệm hình sự. Đặc thù của hành vi vi phạm trên không gian mạng là có thể gây hậu quả lan rộng, khó lường hóa thiệt hại, khó xác định đầy đủ chủ thể bị tác động và khó đánh giá ngay mức độ nguy hiểm của hành vi tại thời điểm phát hiện. Do đó, pháp luật cần bổ sung hướng dẫn cụ thể về các tiêu chí chuyển hóa từ xử lý hành chính sang xử lý hình sự nhằm thống nhất áp dụng các quy định tại Điều 7 và Điều 13 Luật An ninh mạng năm 2025. Các tiêu chí này cần bao gồm: mức độ thiệt hại về tài sản, dữ liệu, hệ thống thông tin; số lượng cá nhân, tổ chức bị ảnh hưởng; tính chất dữ liệu bị xâm phạm; mức độ gián đoạn hoạt động của hệ thống; phạm vi lan truyền của hành vi hoặc thông tin vi phạm; tính chất có tổ chức, chuyên nghiệp; yếu tố xuyên biên giới; mức độ thu lợi bất chính; mục đích xâm phạm ANQG, TTATXH; nguy cơ gây hậu quả nghiêm trọng dù hậu quả chưa xảy ra trên thực tế. Việc đánh giá mức độ nghiêm trọng còn phải dựa trên tiêu chí về khả năng duy trì hoạt động, năng lực phục hồi của các chức năng số thiết yếu sau khi bị tấn công và nguy cơ tạo ra “điểm lỗi chiến lược” đối với sự vận hành của quốc gia.

*Thứ tư*, bổ sung, hoàn thiện quy định về chứng cứ điện tử và định lượng thiệt hại trong xử lý hành vi vi phạm pháp luật về an ninh mạng. Đối với hành vi vi phạm pháp luật về an ninh mạng, chứng cứ điện tử có vai trò đặc biệt quan trọng. Tuy nhiên, chứng cứ điện tử có đặc điểm dễ bị thay đổi, sao chép, xóa bỏ, che giấu, làm sai lệch hoặc phân tán trên nhiều hệ thống, nhiều nền tảng, nhiều quốc gia. Vì vậy, pháp luật cần quy định rõ hơn về thu thập, bảo quản, phục hồi, giám định, đánh giá và sử dụng chứng cứ điện tử trong quá trình xử lý vi phạm. Cần xác định rõ giá trị chứng minh của nhật ký hệ thống, địa chỉ IP, dữ liệu truy cập, dữ liệu định danh thiết bị, bản sao dữ liệu bị thay đổi hoặc bị xóa, thông tin từ nhà cung cấp dịch vụ Internet, dữ liệu từ hệ thống giám sát an ninh mạng và kết quả giám định kỹ thuật số. Đồng thời, cần quy định chặt chẽ về tính toàn vẹn, tính xác thực và tính liên tục của chuỗi bảo quản

chứng cứ điện tử, bảo đảm chứng cứ được thu thập, lưu giữ và sử dụng hợp pháp. Bên cạnh đó, cần hoàn thiện phương pháp xác định thiệt hại do hành vi vi phạm pháp luật về an ninh mạng gây ra. Thiệt hại trong lĩnh vực này không chỉ là thiệt hại vật chất trực tiếp, mà còn bao gồm thiệt hại do mất dữ liệu, gián đoạn hệ thống, chi phí phục hồi, mất uy tín, xâm phạm danh dự, nhân phẩm, bí mật kinh doanh, quyền riêng tư, dữ liệu cá nhân và niềm tin của người sử dụng dịch vụ. Để giải quyết triệt để vấn đề này, cần luật hóa trách nhiệm của nhà cung cấp sản phẩm, dịch vụ công nghệ trong việc cung cấp thông tin, bảo toàn và chuyển giao chứng cứ điện tử, phối hợp ứng phó sự cố và hạn chế thiệt hại (kiến nghị sửa đổi, bổ sung điểm a Khoản 2 Điều 25 và bổ sung một khoản mới tại Điều 41 Luật An ninh mạng năm 2025). Đồng thời, hoàn thiện cơ sở pháp lý về thu giữ, phong tỏa tài sản số, truy vết dòng tiền mã hóa và các cơ chế tương trợ tư pháp, hợp tác quốc tế trong điều tra tội phạm mạng xuyên biên giới.

#### ***4.3.1.3. Hoàn thiện nhóm quy định chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng***

Chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng là một bộ phận quan trọng của pháp luật về an ninh mạng, có vai trò bảo đảm tính nghiêm minh của pháp luật, phòng ngừa vi phạm, răn đe chủ thể vi phạm, khắc phục hậu quả và khôi phục trật tự pháp lý bị xâm phạm trên không gian mạng. Trong thời gian qua, pháp luật Việt Nam đã bước đầu hình thành hệ thống chế tài tương đối đa dạng. Tuy nhiên, trước sự phát triển nhanh chóng của công nghệ số, sự gia tăng của các hành vi xâm phạm dữ liệu, quyền riêng tư, tài sản số, danh dự, uy tín, bí mật kinh doanh, hệ thống thông tin quan trọng và các hành vi vi phạm có yếu tố xuyên biên giới, hệ thống chế tài hiện hành vẫn còn bộc lộ một số hạn chế về tính phân tầng, tính tương xứng, tính răn đe và hiệu quả thực thi. Do đó, cần tiếp tục hoàn thiện nhóm quy định về chế tài xử lý hành vi vi phạm theo hướng đồng bộ, phân tầng, linh hoạt, cụ thể bằng việc sửa đổi, bổ sung Luật An ninh mạng năm 2025 như sau:

*Thứ nhất*, cần phân tầng chế tài xử lý theo mức độ rủi ro, hậu quả và tính chất nguy hiểm của hành vi vi phạm. Pháp luật về an ninh mạng không nên thiết kế chế tài theo hướng cào bằng. Trong lĩnh vực an ninh mạng, có những hành vi mới dừng lại ở mức vi phạm nghĩa vụ quản lý, nghĩa vụ bảo mật, nghĩa vụ báo cáo sự cố nhưng cũng có những hành vi gây thiệt hại nghiêm trọng đến ANQG, TTATXH. Vì vậy, chế tài cần được thiết kế theo hướng phân tầng, bảo đảm sự tương xứng. Để thể chế hóa điều này, kiến nghị sửa đổi Điều 5 Luật An ninh mạng năm 2025 quy định biện pháp bảo vệ an ninh mạng theo hướng phân nhóm các biện pháp chế tài. Cụ thể, bên cạnh các biện pháp xử phạt vi phạm hành chính, khởi tố hình sự (tại điểm n, o Khoản 1 Điều 5), cần bổ sung thêm nhóm chế tài cảnh cáo chuyên ngành như: “yêu cầu khắc phục lỗ hổng hoặc điểm yếu an ninh mạng”, “tạm đình chỉ, đình chỉ hoạt động, thu hồi giấy phép đối với doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng vi phạm điều kiện tại Điều 29”. Đồng thời, các Nghị định xử phạt vi phạm hành chính cần quy định khung tiền phạt lũy tiến dựa trên quy mô dữ liệu bị xâm phạm hoặc mức độ thiệt hại của hệ thống thông tin bị tấn công.

*Thứ hai*, cần tăng cường các chế tài mang tính khắc phục hậu quả và phục hồi quyền, lợi ích hợp pháp của chủ thể bị xâm phạm. Đặc thù của hành vi vi phạm pháp luật về an ninh mạng là hậu quả thường không chỉ thể hiện ở thiệt hại vật chất trực tiếp, mà còn bao gồm thiệt hại về dữ liệu, quyền riêng tư và niềm tin của người sử dụng. Do đó, kiến nghị bổ sung một Khoản mới vào Điều 5 Luật An ninh mạng năm 2025 về các biện pháp khắc phục hậu quả đặc thù trên không gian mạng. Cụ thể bao gồm: “Buộc thông báo vi phạm cho chủ thể dữ liệu hoặc chủ thể bị ảnh hưởng; buộc xóa dữ liệu thu thập, lưu trữ, mua bán, trao đổi trái phép quy định tại Điều 13; buộc thu hồi dữ liệu đã phát tán; buộc khôi phục tình trạng hệ thống thông tin ban đầu; buộc cải chính, xin lỗi công khai và thực hiện các biện pháp kỹ thuật, tổ chức để phòng ngừa tái phạm.”

*Thứ ba*, cần hoàn thiện chế tài đối với tổ chức, doanh nghiệp cung cấp dịch vụ trên không gian mạng. Trong môi trường số, doanh nghiệp cung cấp

dịch vụ viễn thông, Internet, nền tảng số và dịch vụ xuyên biên giới giữ vai trò đặc biệt quan trọng. Đối với nhóm chủ thể này, chế tài xử lý không chỉ dừng ở việc xử phạt tiền. Kiến nghị sửa đổi, bổ sung Điều 25 và Điều 41 Luật An ninh mạng năm 2025 quy định về trách nhiệm bảo đảm an ninh thông tin và trách nhiệm của doanh nghiệp cung cấp dịch vụ. Cần bổ sung chế tài: “Trường hợp doanh nghiệp trong và ngoài nước không tuân thủ nghĩa vụ cảnh báo sự cố, không cung cấp thông tin người dùng phục vụ điều tra theo điểm a Khoản 2 Điều 25; không ngăn chặn, gỡ bỏ thông tin vi phạm theo điểm b Khoản 2 Điều 25; cơ quan có thẩm quyền có quyền đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động cung cấp dịch vụ viễn thông, Internet, thu hồi tên miền theo điểm i và điểm m Khoản 1 Điều 5.”

Đối với doanh nghiệp cung cấp dịch vụ xuyên biên giới vào Việt Nam, cần có cơ chế bảo đảm tuân thủ phù hợp. Cần bổ sung vào Khoản 3 Điều 25 Luật An ninh mạng năm 2025 cơ chế xử lý khi doanh nghiệp không hợp tác hoặc cố tình kéo dài, né tránh trách nhiệm như không đặt chi nhánh/văn phòng đại diện, không phản hồi yêu cầu hợp pháp. Tuy nhiên, các nghĩa vụ này cần được thiết kế minh bạch, phù hợp với điều ước quốc tế mà Việt Nam là thành viên.

*Thứ tư*, cần bảo đảm chế tài xử lý không làm phát sinh gánh nặng tuân thủ bất hợp lý đối với cá nhân, tổ chức, doanh nghiệp. Hoàn thiện chế tài xử lý phải bảo đảm tính hợp lý, khả thi. Các nghĩa vụ tuân thủ và chế tài xử lý cần được thiết kế theo hướng phân tầng rủi ro. Kiến nghị áp dụng nguyên tắc này khi hướng dẫn thi hành Điều 8 và Điều 10 Luật An ninh mạng năm 2025. Theo đó, doanh nghiệp quản lý hệ thống thông tin cấp độ 3, 4, 5 xử lý dữ liệu lớn, nhạy cảm cần phải chịu chế tài nghiêm khắc hơn nếu không thực hiện nhiệm vụ bảo vệ an ninh mạng. Ngược lại, đối với doanh nghiệp nhỏ và vừa quản lý hệ thống cấp độ 1, 2, chế tài ưu tiên áp dụng biện pháp nhắc nhở, hướng dẫn khắc phục. Cách tiếp cận này vừa giúp bảo đảm hiệu quả quản lý

nhà nước, vừa khuyến khích đổi mới sáng tạo và không tạo gánh nặng tuân thủ quá mức.

*Thứ năm*, cần bảo đảm sự thống nhất giữa chế tài hành chính, chế tài hình sự, trách nhiệm dân sự và các biện pháp khắc phục hậu quả. Một hành vi vi phạm pháp luật về an ninh mạng có thể đồng thời làm phát sinh nhiều loại trách nhiệm pháp lý khác nhau. Do đó, cần tiếp tục hoàn thiện tiêu chí phân định giữa xử lý hành chính và xử lý hình sự trong lĩnh vực an ninh mạng để hướng dẫn áp dụng thống nhất Điều 13, Điều 15 và Điều 18 Luật An ninh mạng năm 2025. Các tiêu chí phân định cần dựa trên mức độ thiệt hại, quy mô tác động, số lượng người bị ảnh hưởng, tính chất dữ liệu bị xâm phạm, yếu tố có tổ chức, yếu tố xuyên biên giới, mục đích thu lợi bất chính và mức độ gây tổn hại tới ANQG, TTATXH.

#### ***4.3.1.4. Hoàn thiện nhóm quy định địa vị pháp lý của các chủ thể hoạt động trong lĩnh vực an ninh mạng***

Pháp luật hiện hành đã bước đầu xác định các chủ thể có liên quan đến hoạt động bảo vệ an ninh mạng như cơ quan quản lý nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng, chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên không gian mạng, tổ chức và cá nhân sử dụng không gian mạng. Tuy nhiên, thực tiễn cho thấy các quy định về địa vị pháp lý của các chủ thể này vẫn còn một số hạn chế như: thẩm quyền giữa một số cơ quan còn có điểm giao thoa; cơ chế phối hợp chưa rõ ràng; trách nhiệm của doanh nghiệp cung cấp dịch vụ xuyên biên giới chưa được quy định đầy đủ; quyền của cá nhân, tổ chức bị tác động bởi các biện pháp bảo vệ an ninh mạng chưa được cụ thể hóa tương xứng. Vì vậy, cần tiếp tục hoàn thiện nhóm quy định này bằng việc sửa đổi, bổ sung trực tiếp các điều khoản tại Luật An ninh mạng năm 2025 theo các hướng sau:

*Thứ nhất*, phân định rõ thẩm quyền giữa các cơ quan nhà nước trong lĩnh vực an ninh mạng. Pháp luật cần quy định rõ thẩm quyền của từng cơ

quan trọng các nhóm hoạt động cụ thể. Kiến nghị rà soát và bổ sung chi tiết tại Điều 39 Luật An ninh mạng năm 2025 quy định trách nhiệm quản lý nhà nước về an ninh mạng. Theo đó, tại các quy định về xử lý sự cố tại Điều 20, phòng chống tấn công mạng tại Điều 18 và bảo vệ hệ thống thông tin quan trọng về ANQG tại Điều 11 cần xác định rõ cơ quan chịu trách nhiệm chính, cơ quan phối hợp, trình tự phối hợp, chế độ chia sẻ thông tin, trách nhiệm báo cáo và trách nhiệm pháp lý khi không thực hiện hoặc thực hiện không đầy đủ nhiệm vụ được giao.

*Thứ hai*, hoàn thiện địa vị pháp lý của lực lượng chuyên trách bảo vệ an ninh mạng. Lực lượng chuyên trách giữ vai trò nòng cốt trong phòng ngừa, đấu tranh và xử lý các nguy cơ xâm phạm an ninh mạng. Tuy nhiên, để hoạt động hiệu quả và tránh lạm quyền, kiến nghị sửa đổi, bổ sung Điều 12 quy định kiểm tra an ninh mạng và Điều 21 quy định đấu tranh bảo vệ an ninh mạng của Luật An ninh mạng năm 2025. Cần quy định rõ giới hạn thẩm quyền, điều kiện áp dụng, trình tự, thủ tục thực hiện, thời hạn áp dụng, chế độ lưu trữ hồ sơ và cơ chế kiểm tra, giám sát đối với các biện pháp có khả năng tác động trực tiếp đến quyền riêng tư, tự do kinh doanh của cá nhân, tổ chức. Bên cạnh đó, cần thể chế hóa cơ chế bảo đảm nguồn nhân lực, kỹ thuật và tài chính đặc thù cho lực lượng này thông qua việc cụ thể hóa các chính sách tại Điều 31 và Điều 38 của Luật.

*Thứ ba*, bổ sung, làm rõ trách nhiệm pháp lý của doanh nghiệp cung cấp dịch vụ trên không gian mạng. Kiến nghị sửa đổi, bổ sung Khoản 2, Khoản 3 Điều 25 và Điều 41 Luật An ninh mạng năm 2025. Cần bổ sung nghĩa vụ bắt buộc cho các doanh nghiệp cung cấp dịch vụ viễn thông, mạng xã hội, điện toán đám mây và dịch vụ xuyên biên giới trong việc: áp dụng biện pháp kỹ thuật phòng ngừa nguy cơ mất an ninh mạng; cảnh báo rủi ro cho người sử dụng; báo cáo sự cố an ninh mạng theo quy định; lưu giữ và bảo toàn chứng cứ điện tử theo yêu cầu hợp pháp của cơ quan chức năng; thực hiện biện pháp bảo vệ quyền riêng tư và dữ liệu cá nhân của người dùng.

*Thứ tư*, bổ sung và cụ thể hóa quyền của cá nhân, tổ chức trên không gian mạng. Trong lĩnh vực an ninh mạng, cá nhân, tổ chức không chỉ là đối tượng có nghĩa vụ tuân thủ mà còn là chủ thể có quyền được bảo vệ. Hiện nay, Điều 42 Luật An ninh mạng năm 2025 chỉ quy định “Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng” mà thiếu đi các quy định về “Quyền”. Kiến nghị đổi tên Điều 42 thành “Quyền và trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng” và bổ sung một khoản mới về Quyền của người sử dụng. Cụ thể bao gồm: quyền được bảo vệ dữ liệu cá nhân, quyền được thông báo trong trường hợp dữ liệu bị xâm phạm, quyền yêu cầu gỡ bỏ hoặc cải chính thông tin xâm phạm quyền lợi ích hợp pháp, quyền khiếu nại, tố cáo và quyền yêu cầu bồi thường thiệt hại do vi phạm pháp luật về an ninh mạng gây ra.

*Thứ năm*, hoàn thiện cơ chế phối hợp giữa Nhà nước, doanh nghiệp và người sử dụng trong bảo vệ an ninh mạng. Kiến nghị thể chế hóa chính sách tại Khoản 4 Điều 3 Luật An ninh mạng năm 2025 về việc đẩy mạnh liên kết, đối tác công tư vào các điều luật cụ thể như Điều 14 quy định phòng ngừa, xử lý thông tin và Điều 22 về ngăn chặn xung đột thông tin. Pháp luật cần thiết lập cơ chế phối hợp đa chủ thể bao gồm quy định về chia sẻ thông tin cảnh báo nguy cơ; bảo vệ dữ liệu và chứng cứ điện tử; hỗ trợ người dùng bị xâm phạm; phối hợp trong điều tra, xác minh. Đồng thời, cần quy định nguyên tắc bảo mật thông tin, bảo vệ bí mật kinh doanh và trách nhiệm pháp lý của các chủ thể khi lạm dụng việc phối hợp để xâm phạm quyền, lợi ích hợp pháp của cá nhân, tổ chức.

#### ***4.3.1.5. Hoàn thiện nhóm quy định về biện pháp bảo vệ an ninh mạng***

Pháp luật hiện hành đã quy định khá rộng các biện pháp bảo vệ an ninh mạng, bao gồm kiểm tra, giám sát, thu thập dữ liệu điện tử, yêu cầu gỡ bỏ thông tin, ngăn chặn truy cập, đình chỉ dịch vụ, phong tỏa hoặc hạn chế hoạt động của hệ thống thông tin được liệt kê tại Khoản 1 Điều 5 Luật An ninh mạng năm 2025. Tuy nhiên, đây là nhóm biện pháp có khả năng tác động trực tiếp đến quyền, lợi ích hợp pháp của cá nhân, tổ chức, nhất là quyền

riêng tư, dữ liệu cá nhân, quyền tiếp cận thông tin và quyền tự do kinh doanh hợp pháp. Vì vậy, việc hoàn thiện nhóm quy định này cần được thực hiện theo hướng vừa bảo đảm hiệu quả bảo vệ an ninh mạng, vừa bảo đảm tính hợp hiến, hợp pháp, minh bạch, cần thiết và tương xứng trong quá trình áp dụng. Dựa trên cơ sở Luật An ninh mạng năm 2025, cần thiết kể lại các quy định theo các hướng sau:

*Thứ nhất*, thiết kế các biện pháp bảo vệ an ninh mạng theo chuỗi quản trị rủi ro. Pháp luật cần quy định đầy đủ chuỗi biện pháp bảo vệ an ninh mạng theo logic: phòng ngừa, phát hiện, cảnh báo sớm, ứng cứu, xử lý, khắc phục, phục hồi và đánh giá sau sự cố. Kiến nghị cấu trúc lại các biện pháp tại Khoản 1 Điều 5 Luật An ninh mạng năm 2025 thay vì liệt kê dàn trải từ điểm a đến điểm o. Việc nhóm các biện pháp theo vòng đời rủi ro sẽ phù hợp với định hướng chuyển mạnh từ ứng phó bị động sang chủ động nhận diện, dự báo, phòng ngừa, bảo vệ từ sớm, từ xa. Cách tiếp cận này phù hợp với đặc thù của an ninh mạng, bởi nhiều nguy cơ trên không gian mạng có tốc độ lan truyền nhanh, hậu quả lớn và khó khắc phục nếu chỉ xử lý sau khi vi phạm đã xảy ra.

*Thứ hai*, quy định rõ điều kiện áp dụng các biện pháp can thiệp vào hệ thống thông tin, dữ liệu và hoạt động trên không gian mạng. Pháp luật cần làm rõ điều kiện áp dụng từng biện pháp. Hiện tại, Khoản 2 Điều 5 Luật An ninh mạng năm 2025 giao Chính phủ quy định chi tiết nội dung, trình tự, thủ tục, thẩm quyền áp dụng các biện pháp bảo vệ. Tuy nhiên, đối với các biện pháp hạn chế quyền nghiêm trọng như đình chỉ, tạm đình chỉ cung cấp mạng viễn thông, Internet quy định tại điểm i Khoản 1 Điều 5 hay phong tỏa, thu hồi tên miền quy định tại điểm m Khoản 1 Điều 5 cần phải quy định trực tiếp các điều kiện, ngưỡng rủi ro bắt buộc phải thỏa mãn trước khi áp dụng. Việc quy định rõ điều kiện áp dụng ngay trong luật có ý nghĩa quan trọng nhằm bảo đảm tính minh bạch, hạn chế nguy cơ áp dụng tùy tiện và tạo cơ sở pháp lý thống nhất cho cơ quan có thẩm quyền trong quá trình thực thi pháp luật.

*Thứ ba*, bổ sung nguyên tắc tương xứng trong áp dụng biện pháp bảo vệ an ninh mạng. Theo đó, đối với nguy cơ ở mức thấp hoặc chưa gây hậu quả nghiêm trọng, có thể ưu tiên áp dụng các biện pháp cảnh báo, yêu cầu khắc phục, yêu cầu tăng cường bảo mật hoặc giám sát kỹ thuật. Chỉ trong trường hợp nguy cơ có khả năng gây thiệt hại nghiêm trọng, ảnh hưởng đến ANQG, hệ thống thông tin quan trọng, dữ liệu nhạy cảm hoặc quyền, lợi ích hợp pháp của nhiều chủ thể, mới áp dụng các biện pháp mạnh hơn. Kiến nghị bổ sung một khoản mới vào Điều 5 Luật An ninh mạng năm 2025 quy định rõ: “Việc lựa chọn và áp dụng các biện pháp bảo vệ an ninh mạng quy định tại Khoản 1 Điều này phải tương xứng với cấp độ hệ thống thông tin quy định tại Điều 8 và mức độ của tình huống nguy hiểm về an ninh mạng quy định tại Điều 20”.

*Thứ tư*, bổ sung, hoàn thiện cơ chế giám sát, khiếu nại và trách nhiệm giải trình trong áp dụng biện pháp bảo vệ an ninh mạng. Cần thiết lập cơ chế đề cá nhân, tổ chức bị ảnh hưởng bởi biện pháp bảo vệ an ninh mạng có thể khiếu nại, yêu cầu giải thích, yêu cầu xem xét lại quyết định áp dụng biện pháp, yêu cầu khắc phục thiệt hại hoặc bồi thường thiệt hại theo quy định của pháp luật, trừ trường hợp thuộc bí mật nhà nước hoặc trường hợp đặc biệt do pháp luật quy định. Kiến nghị cụ thể hóa vấn đề này bằng việc bổ sung quyền khiếu nại, quyền yêu cầu giải trình và bồi thường thiệt hại vào Điều 42 Luật An ninh mạng năm 2025 quy định quyền và trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng. Bên cạnh đó, cần tăng cường cơ chế giám sát nội bộ, giám sát của cơ quan có thẩm quyền và giám sát xã hội phù hợp đối với việc áp dụng các biện pháp có khả năng tác động đến quyền riêng tư, dữ liệu cá nhân, quyền tiếp cận thông tin và quyền tự do kinh doanh hợp pháp.

*Thứ năm*, hoàn thiện các tiêu chuẩn, quy chuẩn kỹ thuật và quy trình nghiệp vụ về bảo vệ an ninh mạng. Các biện pháp bảo vệ an ninh mạng chỉ có thể thực hiện hiệu quả khi được cụ thể hóa bằng tiêu chuẩn, quy chuẩn kỹ thuật và quy trình nghiệp vụ rõ ràng. Vì vậy, cần tiếp tục xây dựng, hoàn

thiện các tiêu chuẩn, quy chuẩn về bảo vệ hệ thống thông tin quan trọng, bảo vệ dữ liệu, đánh giá rủi ro, kiểm tra an ninh mạng, giám sát an ninh mạng, ứng cứu sự cố, lưu giữ nhật ký hệ thống, bảo quản chứng cứ điện tử và phục hồi sau sự cố. Kiến nghị cụ thể hóa Điều 27 Luật An ninh mạng năm 2025 quy định tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng theo hướng yêu cầu cơ quan quản lý nhà nước ban hành tiêu chuẩn phân tầng theo cấp độ rủi ro, quy mô hệ thống, tính chất dữ liệu và vai trò của chủ thể quản lý hệ thống thông tin; đồng thời thiết lập cơ chế kiểm định độc lập đối với các công nghệ, nền tảng, thiết bị quan trọng.

*Thứ sáu*, hoàn thiện cơ chế phối hợp giữa cơ quan nhà nước, doanh nghiệp và chủ quản hệ thống thông tin trong áp dụng biện pháp bảo vệ an ninh mạng. Pháp luật cần quy định rõ cơ chế chia sẻ thông tin cảnh báo nguy cơ, phối hợp ứng cứu sự cố, bảo vệ chứng cứ điện tử, bảo mật thông tin trong quá trình phối hợp, trách nhiệm báo cáo và trách nhiệm pháp lý khi không thực hiện hoặc thực hiện không đầy đủ nghĩa vụ phối hợp. Kiến nghị luật hóa yêu cầu này vào Điều 20 quy định phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng và Điều 41 quy định trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng của Luật An ninh mạng năm 2025. Đối với các sự cố nghiêm trọng, cần có cơ chế chỉ huy, điều phối thống nhất để bảo đảm phản ứng nhanh, tránh chông chéo hoặc chậm trễ trong xử lý, thể chế hóa nguyên tắc một đầu mối điều phối, một quy trình ứng phó liên thông từ Trung ương đến địa phương.

#### ***4.3.1.6. Hoàn thiện nhóm quy định hợp tác quốc tế về an ninh mạng***

Trên thực tế, nhiều hành vi xâm phạm an ninh mạng tại Việt Nam được thực hiện từ nước ngoài; máy chủ, dữ liệu, tài khoản, dòng tiền, công cụ tấn công hoặc chứng cứ điện tử có thể được lưu giữ, trung chuyển, che giấu thông qua các hệ thống, nền tảng, nhà cung cấp dịch vụ ở nhiều quốc gia. Tuy nhiên, hợp tác quốc tế trong lĩnh vực an ninh mạng hiện còn gặp không ít trở

ngại do sự khác biệt về thẩm quyền tài phán, tiêu chuẩn chứng cứ điện tử, quy trình tương trợ tư pháp, vị trí lưu trữ dữ liệu, mức độ hợp tác của nền tảng xuyên biên giới và yêu cầu bảo vệ dữ liệu cá nhân, quyền riêng tư. Do đó, cần tiếp tục hoàn thiện nhóm quy định về hợp tác quốc tế trong lĩnh vực an ninh mạng bằng việc sửa đổi, bổ sung trực tiếp Điều 6 quy định hợp tác quốc tế về an ninh mạng và các điều khoản khác liên quan tại Luật An ninh mạng năm 2025 theo hướng:

*Thứ nhất*, nghiên cứu, hoàn thiện quy định về thu thập, bảo toàn và chuyển giao chứng cứ điện tử xuyên biên giới. Chứng cứ điện tử có vai trò đặc biệt quan trọng trong phát hiện, điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng. Tuy nhiên, loại chứng cứ này dễ bị thay đổi, phân tán hoặc lưu giữ tại hệ thống đặt ngoài lãnh thổ Việt Nam. Kiến nghị cụ thể hóa điểm d Khoản 2 Điều 6 và điểm 1 Khoản 1 Điều 5 Luật An ninh mạng năm 2025 nhằm quy định rõ điều kiện, thẩm quyền, trình tự yêu cầu, thời hạn phản hồi, tiêu chuẩn bảo quản và giá trị pháp lý của chứng cứ điện tử được thu thập thông qua hợp tác quốc tế. Cần xác định rõ cơ quan có thẩm quyền gửi, tiếp nhận và xử lý yêu cầu hợp tác; cơ chế xác thực, bảo toàn tính toàn vẹn của dữ liệu và quy trình ghi nhận chuỗi lưu giữ chứng cứ. Đồng thời, cần bổ sung cơ sở pháp lý cho việc hợp tác quốc tế, tương trợ tư pháp trong truy tìm tài sản số, dòng tiền mã hóa và điều tra mạng lưới tội phạm mạng xuyên biên giới.

*Thứ hai*, bổ sung, hoàn thiện cơ chế hợp tác với nhà cung cấp dịch vụ xuyên biên giới. Trong nhiều vụ việc liên quan đến an ninh mạng, dữ liệu, tài khoản, nội dung vi phạm hoặc thông tin kỹ thuật cần thiết để xác minh hành vi thường do các nhà cung cấp dịch vụ xuyên biên giới nắm giữ. Kiến nghị sửa đổi, bổ sung Khoản 2, Khoản 3 Điều 25 và Điều 41 Luật An ninh mạng năm 2025 để xác định rõ nghĩa vụ phản hồi yêu cầu hợp pháp của cơ quan có thẩm quyền Việt Nam, nghĩa vụ bảo toàn dữ liệu, nghĩa vụ gỡ bỏ hoặc ngăn chặn nội dung vi phạm trong trường hợp có căn cứ rõ ràng. Cơ chế hợp tác này cần được thiết kế minh bạch, có giới hạn và phù hợp với nguyên tắc tôn trọng chủ quyền quốc gia.

Hơn nữa, cần thiết lập cơ chế cưỡng chế kỹ thuật trực tiếp, chặn lọc hoặc tạm dừng dịch vụ đối với các nền tảng cố tình vi phạm pháp luật Việt Nam, trốn tránh trách nhiệm cung cấp chứng cứ điện tử hoặc che giấu tội phạm.

*Thứ ba*, bổ sung, mở rộng hợp tác quốc tế về cảnh báo, chia sẻ thông tin và ứng phó sự cố an ninh mạng. Hợp tác quốc tế trong lĩnh vực an ninh mạng không chỉ nhằm phục vụ điều tra, xử lý sau khi hành vi vi phạm đã xảy ra, mà còn phải hướng đến phòng ngừa, cảnh báo sớm và ứng phó kịp thời. Kiến nghị luật hóa yêu cầu này vào điểm a, điểm e Khoản 2 Điều 6 và Điều 20 quy định phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng của Luật An ninh mạng năm 2025. Cần thúc đẩy cơ chế chia sẻ thông tin tình báo mạng về mã độc, lỗ hổng bảo mật, chiến dịch lừa đảo và các rủi ro xuyên biên giới. Pháp luật cần tạo cơ sở thiết lập các đầu mối hợp tác, đường dây nóng, cơ chế phối hợp tác chiến giữa cơ quan chức năng của Việt Nam với cơ quan có thẩm quyền nước ngoài, mạng lưới ứng cứu sự cố máy tính và doanh nghiệp công nghệ. Đặc biệt, cần xây dựng khung pháp lý để Việt Nam chủ động dẫn dắt, khởi xướng các sáng kiến quốc tế về an ninh mạng (như phát huy giá trị của Công ước Hà Nội), tham gia định hình các chuẩn mực, nguyên tắc quản trị an ninh công nghệ toàn cầu nhằm bảo vệ quyền tài phán và lợi ích quốc gia - dân tộc.

#### **4.3.2. Nhóm giải pháp bảo đảm tính đồng bộ, minh bạch và chất lượng lập pháp trong lĩnh vực an ninh mạng**

##### ***4.3.2.1. Rà soát, hệ thống hóa và xử lý chồng chéo giữa các văn bản pháp luật***

Rà soát, hệ thống hóa và xử lý chồng chéo giữa các văn bản pháp luật là giải pháp có ý nghĩa nền tảng trong quá trình hoàn thiện pháp luật về an ninh mạng ở Việt Nam. Pháp luật về an ninh mạng là lĩnh vực có tính liên ngành, không chỉ được điều chỉnh bởi Luật An ninh mạng, mà còn có mối quan hệ chặt chẽ với pháp luật về an toàn thông tin mạng, dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, trí tuệ nhân tạo, công nghệ thông

tin, bảo vệ bí mật nhà nước, xử lý vi phạm hành chính, hình sự, tố tụng hình sự và hợp tác quốc tế. Vì vậy, nếu không tiến hành rà soát, hệ thống hóa một cách tổng thể, việc hoàn thiện pháp luật dễ rơi vào tình trạng sửa đổi cục bộ, thiếu thống nhất, thậm chí làm phát sinh thêm mâu thuẫn, chồng chéo trong hệ thống pháp luật.

Trước hết, cần tổ chức rà soát toàn diện các quy định có liên quan đến an ninh mạng trong hệ thống pháp luật hiện hành. Việc rà soát này không chỉ giới hạn ở các văn bản trực tiếp điều chỉnh lĩnh vực an ninh mạng, mà còn phải bao quát các văn bản pháp luật có liên quan đến quản lý, sử dụng, bảo vệ hệ thống thông tin, dữ liệu, nền tảng số, dịch vụ số, chứng cứ điện tử, xử lý vi phạm trên không gian mạng và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức. Đặc biệt, trong bối cảnh Luật An ninh mạng năm 2025 đã được ban hành, việc rà soát càng cần được thực hiện khẩn trương nhằm đánh giá mức độ tương thích giữa đạo luật mới với các văn bản pháp luật hiện hành, từ đó kịp thời sửa đổi, bổ sung, thay thế hoặc bãi bỏ những quy định không còn phù hợp.

Việc rà soát không chỉ là thống kê số lượng văn bản pháp luật có liên quan, mà quan trọng là nhận diện chính xác những vấn đề đang cản trở tính đồng bộ, thống nhất, minh bạch và khả thi của pháp luật về an ninh mạng. Cụ thể, cần xác định rõ: quy định nào đang bị trùng lặp; quy định nào còn mâu thuẫn; quy định nào thiếu hướng dẫn thi hành; quy định nào khó thực hiện trong thực tiễn; quy định nào làm phát sinh gánh nặng tuân thủ không cần thiết cho cá nhân, tổ chức, doanh nghiệp; quy định nào chưa bảo đảm đầy đủ quyền, lợi ích hợp pháp của các chủ thể trên không gian mạng.

Việc rà soát, hệ thống hóa cần được thực hiện theo các nhóm chế định cơ bản của pháp luật về an ninh mạng, bao gồm: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý hành vi vi phạm; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế trong lĩnh vực an ninh mạng. Cách tiếp cận này giúp phát hiện rõ hơn những khoảng trống, điểm giao thoa, mâu thuẫn hoặc chồng chéo trong từng

nhóm quy định. Chẳng hạn, đối với nhóm quy định về hành vi vi phạm, cần rà soát sự thống nhất giữa Luật An ninh mạng, Bộ luật Hình sự, Luật Xử lý vi phạm hành chính và các nghị định xử phạt chuyên ngành. Đối với nhóm quy định về dữ liệu và bảo vệ dữ liệu cá nhân, cần rà soát mối quan hệ giữa pháp luật về an ninh mạng, pháp luật về dữ liệu, pháp luật về bảo vệ dữ liệu cá nhân và pháp luật về giao dịch điện tử.

Bên cạnh đó, cần xây dựng tiêu chí rà soát thống nhất để bảo đảm kết quả rà soát có giá trị thực tiễn. Các tiêu chí này bao gồm: tính hợp hiến, hợp pháp; tính thống nhất, đồng bộ trong hệ thống pháp luật; tính minh bạch, dễ tiếp cận; tính khả thi; khả năng thích ứng với sự phát triển của công nghệ; mức độ bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức; mức độ phù hợp với điều ước quốc tế mà Việt Nam là thành viên. Đối với lĩnh vực an ninh mạng, cần đặc biệt chú trọng tiêu chí về khả năng thực thi, bởi nhiều quy định tuy đầy đủ về mặt văn bản nhưng khó áp dụng trong thực tế do thiếu quy trình, thiếu hướng dẫn kỹ thuật, thiếu cơ chế phối hợp hoặc thiếu nguồn lực bảo đảm. Đồng thời, cần gắn hoạt động rà soát, hệ thống hóa với công tác pháp điển hóa, cập nhật cơ sở dữ liệu pháp luật và nâng cao khả năng tiếp cận pháp luật của cơ quan, tổ chức, cá nhân; được thực hiện thường xuyên, định kỳ và có sự tham gia của nhiều chủ thể.

Kết quả rà soát phải được sử dụng làm căn cứ trực tiếp cho hoạt động sửa đổi, bổ sung, thay thế hoặc bãi bỏ các quy định không còn phù hợp. Đối với những quy định trùng lặp, cần xác định văn bản giữ vai trò điều chỉnh chính để tránh lặp lại không cần thiết. Đối với những quy định mâu thuẫn, cần xác định rõ nguyên tắc ưu tiên áp dụng hoặc sửa đổi để bảo đảm thống nhất. Đối với những quy định thiếu hướng dẫn, cần kịp thời ban hành văn bản quy định chi tiết, nhất là các quy định liên quan đến điều kiện áp dụng biện pháp bảo vệ an ninh mạng, trình tự thu thập chứng cứ điện tử, trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng, cơ chế phối hợp giữa các cơ quan và quyền của cá nhân, tổ chức bị tác động. Đối với những quy

định gây gánh nặng tuân thủ không cần thiết, cần nghiên cứu điều chỉnh theo hướng phân tầng nghĩa vụ dựa trên mức độ rủi ro, quy mô chủ thể, loại dữ liệu xử lý và tính chất dịch vụ cung cấp.

#### ***4.3.2.2. Nâng cao chất lượng đánh giá tác động chính sách***

Nâng cao chất lượng đánh giá tác động chính sách là giải pháp quan trọng nhằm bảo đảm việc xây dựng, sửa đổi, bổ sung pháp luật về an ninh mạng được thực hiện trên cơ sở khoa học, khách quan và phù hợp với yêu cầu thực tiễn.

Trước hết, đánh giá tác động chính sách trong lĩnh vực an ninh mạng phải làm rõ tác động đối với ANQG, TTATXH. Tuy nhiên, việc đánh giá không chỉ dừng ở việc khẳng định sự cần thiết của chính sách, mà phải phân tích cụ thể chính sách đó góp phần xử lý nguy cơ nào, mức độ nguy cơ ra sao, phạm vi tác động thế nào, khả năng phòng ngừa và ứng phó sự cố đến đâu, có làm tăng năng lực bảo vệ hệ thống thông tin quan trọng hay không, có khắc phục được khoảng trống pháp lý hiện hành hay không. Bên cạnh đó, đánh giá tác động chính sách phải làm rõ mức độ cần thiết, tính hợp lý, tính tương xứng và giới hạn của từng biện pháp; đồng thời phải xác định cơ chế kiểm soát quyền lực, trách nhiệm giải trình, khiếu nại, tố cáo, bồi thường thiệt hại và khắc phục hậu quả trong trường hợp quyền, lợi ích hợp pháp của chủ thể bị tác động trái pháp luật. Đồng thời, khi thiết kế chính sách cần đánh giá khả năng tuân thủ của từng nhóm doanh nghiệp, tránh áp dụng cùng một mức nghĩa vụ cho mọi chủ thể mà không căn cứ vào quy mô, năng lực kỹ thuật, loại hình dịch vụ, mức độ rủi ro và phạm vi tác động của hoạt động kinh doanh. Một nội dung quan trọng khác là phải lượng hóa chi phí tuân thủ giúp cơ quan xây dựng chính sách lựa chọn phương án điều chỉnh hợp lý hơn, giảm gánh nặng không cần thiết cho xã hội. Trước khi ban hành quy định mới về an ninh mạng, đánh giá tác động chính sách phải trả lời được câu hỏi: cơ quan nào thực hiện, thực hiện bằng nguồn lực nào, cần bao nhiêu kinh phí, cần điều kiện kỹ thuật gì, có phát sinh nhiệm vụ mới cho cơ quan nhà nước hay không và nhiệm vụ đó có khả

thi trong điều kiện hiện nay hay không. Đặc biệt, đánh giá tác động chính sách phải xem xét khả năng cập nhật của pháp luật trước sự phát triển nhanh chóng của công nghệ. Vì vậy, khi đánh giá tác động chính sách cần phân tích khả năng thích ứng của phương án chính sách đối với pháp luật quốc tế, điều ước quốc tế mà Việt Nam là thành viên và các vấn đề mới như trí tuệ nhân tạo, dữ liệu lớn, deepfake, tài sản số, điện toán đám mây, Internet vạn vật, nền tảng số xuyên biên giới và các phương thức tấn công mạng mới.

Để nâng cao chất lượng đánh giá tác động chính sách, cần bảo đảm việc đánh giá dựa trên chứng cứ, dữ liệu và tham vấn thực chất. Các báo cáo đánh giá tác động không nên chỉ dừng ở nhận định định tính, mà cần sử dụng số liệu, vụ việc thực tiễn, kết quả khảo sát, ý kiến chuyên gia, kinh nghiệm quốc tế, phản ánh của doanh nghiệp và người dân. Cần mở rộng tham vấn đối với chuyên gia pháp lý, chuyên gia công nghệ, cơ quan thực thi, doanh nghiệp cung cấp dịch vụ số, tổ chức xã hội, hiệp hội nghề nghiệp và các nhóm chủ thể chịu sự điều chỉnh trực tiếp của chính sách. Việc tham vấn phải được thực hiện thực chất, có tiếp thu, giải trình rõ ràng, tránh hình thức hóa hoặc chỉ tham vấn ở giai đoạn cuối khi phương án chính sách đã cơ bản được định sẵn.

#### ***4.3.2.3. Chuẩn hóa thuật ngữ và kỹ thuật lập pháp***

Pháp luật về an ninh mạng là lĩnh vực pháp lý có tính kỹ thuật cao, thường xuyên sử dụng nhiều khái niệm chuyên môn như an ninh mạng, an toàn thông tin mạng, dữ liệu cá nhân, dữ liệu nhạy cảm, dữ liệu điện tử, chứng cứ điện tử, hệ thống thông tin quan trọng, tấn công mạng, giám sát an ninh mạng, thu thập dữ liệu điện tử, nền tảng số, định danh số, xác thực điện tử, tài sản số, deepfake, mã độc, ransomware... Nếu những thuật ngữ này không được sử dụng thống nhất, giải thích rõ ràng và đặt trong đúng ngữ cảnh pháp lý, thì có thể dẫn đến nhiều cách hiểu khác nhau, gây khó khăn cho quá trình áp dụng pháp luật và làm giảm hiệu quả thực thi.

Do đó, trước hết, cần xây dựng hệ thống thuật ngữ pháp lý thống nhất trong lĩnh vực an ninh mạng. Việc chuẩn hóa thuật ngữ không chỉ là việc dịch

hoặc sử dụng thống nhất các khái niệm kỹ thuật, mà còn là quá trình chuyển hóa các khái niệm kỹ thuật thành khái niệm pháp lý có nội hàm rõ ràng, phạm vi xác định và hậu quả pháp lý cụ thể. Chẳng hạn, thuật ngữ “tấn công mạng” cần được phân biệt với “xâm nhập trái phép”, “phát tán mã độc”, “cản trở hoạt động của hệ thống thông tin” hoặc “gây rối loạn hoạt động của mạng máy tính, mạng viễn thông”. Tương tự, cần phân biệt rõ “an ninh dữ liệu”, “bảo vệ dữ liệu cá nhân”, “dữ liệu điện tử” với “chứng cứ điện tử”. Việc phân định rõ các thuật ngữ này giúp xác định chính xác phạm vi điều chỉnh, thẩm quyền áp dụng, nghĩa vụ của chủ thể và chế tài xử lý tương ứng. Trong lĩnh vực an ninh mạng, các khái niệm như “nguy cơ nghiêm trọng”, “thông tin có tác hại lớn”, “ảnh hưởng đến ANQG”, “gây phương hại đến TTATXH”, “hệ thống quan trọng” cần được cụ thể hóa bằng các tiêu chí pháp lý hoặc kỹ thuật phù hợp. Các tiêu chí này có thể dựa trên mức độ thiệt hại, phạm vi ảnh hưởng, số lượng chủ thể bị tác động, loại dữ liệu bị xâm phạm, tính chất hệ thống bị tấn công, mức độ gián đoạn dịch vụ, yếu tố xuyên biên giới hoặc nguy cơ đối với ANQG.

Đồng thời, cần xây dựng cơ chế giải thích, hướng dẫn áp dụng thuật ngữ pháp lý - kỹ thuật trong lĩnh vực an ninh mạng. Do đây là lĩnh vực biến đổi nhanh, nhiều thuật ngữ mới có thể phát sinh từ thực tiễn công nghệ, nên việc giải thích thuật ngữ không nên chỉ dừng lại ở một danh mục cố định. Cần có cơ chế cập nhật định kỳ thông qua văn bản hướng dẫn, tiêu chuẩn kỹ thuật, án lệ hoặc thực tiễn áp dụng pháp luật phù hợp với thẩm quyền của từng cơ quan. Việc cập nhật này phải bảo đảm công khai, minh bạch, dễ tiếp cận và không làm thay đổi trái thẩm quyền nội dung cơ bản đã được quy định trong luật. Về kỹ thuật lập pháp, các quy định pháp luật về an ninh mạng cần được thiết kế theo cấu trúc chặt chẽ, logic và dễ áp dụng. Mỗi chế định cần xác định rõ: đối tượng điều chỉnh, chủ thể chịu trách nhiệm, hành vi bị cấm hoặc nghĩa vụ phải thực hiện, điều kiện áp dụng, thẩm quyền của cơ quan nhà nước, trình tự, thủ tục thực hiện, chế tài xử lý và cơ chế bảo vệ quyền, lợi ích hợp pháp của chủ thể bị tác động. Đối với các biện pháp có khả năng ảnh

hưởng đến quyền riêng tư, dữ liệu cá nhân, quyền tiếp cận thông tin hoặc quyền tự do kinh doanh hợp pháp, kỹ thuật lập pháp càng phải bảo đảm sự rõ ràng về căn cứ áp dụng, phạm vi áp dụng, thời hạn áp dụng, trách nhiệm giải trình, cơ chế khiếu nại và bồi thường thiệt hại nếu có vi phạm.

### **4.3.3. Nhóm giải pháp trong tổ chức thực hiện pháp luật về an ninh mạng**

#### ***4.3.3.1. Nâng cao năng lực của cơ quan thực thi pháp luật về an ninh mạng***

Nâng cao năng lực của cơ quan thực thi pháp luật về an ninh mạng là giải pháp có ý nghĩa trực tiếp đối với hiệu quả tổ chức thi hành pháp luật trong lĩnh vực này. Pháp luật về an ninh mạng dù được xây dựng đầy đủ, đồng bộ và hiện đại đến đâu cũng khó phát huy hiệu quả nếu cơ quan thực thi không có đủ năng lực chuyên môn, năng lực kỹ thuật, nguồn lực con người, phương tiện công nghệ và cơ chế phối hợp phù hợp. Đặc biệt, an ninh mạng là lĩnh vực có tính kỹ thuật cao, diễn biến nhanh, thủ đoạn vi phạm thường xuyên thay đổi, có yếu tố xuyên biên giới và gắn chặt với dữ liệu, hệ thống thông tin, nền tảng số, dịch vụ số. Vì vậy, năng lực của cơ quan thực thi pháp luật phải được nâng cao đồng bộ cả về nhận thức pháp lý, trình độ kỹ thuật, kỹ năng nghiệp vụ và khả năng phối hợp liên ngành.

Trước hết, cần tăng cường đào tạo chuyên sâu cho đội ngũ cán bộ thực thi pháp luật về an ninh mạng. Nội dung đào tạo không chỉ bao gồm kiến thức pháp luật về an ninh mạng, an toàn thông tin mạng, dữ liệu, bảo vệ dữ liệu cá nhân, viễn thông, giao dịch điện tử, hình sự, tố tụng hình sự và xử lý vi phạm hành chính, mà còn phải bao gồm các kỹ năng kỹ thuật cần thiết như thu thập, bảo quản và đánh giá chứng cứ điện tử; điều tra số; truy vết giao dịch; phân tích mã độc; phân tích nhật ký hệ thống; nhận diện phương thức tấn công mạng; xử lý dữ liệu lớn; xác định nguồn gốc, phương tiện, công cụ thực hiện hành vi vi phạm. Đây là những kỹ năng đặc thù, có vai trò quyết định trong việc phát hiện, chứng minh và xử lý các hành vi xâm phạm an ninh mạng.

Đồng thời, cần nâng cao năng lực thực thi pháp luật về an ninh mạng ở địa phương, không chỉ tập trung ở cấp trung ương. Trong bối cảnh chuyển đổi số diễn ra trên phạm vi cả nước, các nguy cơ, hành vi vi phạm pháp luật về an ninh mạng có thể phát sinh ở mọi địa bàn, từ đô thị lớn đến khu vực nông thôn, miền núi, vùng sâu, vùng xa.

Ngoài ra, cần hoàn thiện cơ chế phối hợp giữa các cơ quan thực thi pháp luật trong lĩnh vực an ninh mạng. Các vụ việc an ninh mạng thường liên quan đến nhiều lĩnh vực như an ninh, quốc phòng, tài chính, ngân hàng, thương mại điện tử, dữ liệu, viễn thông, tổ tụng hình sự và hợp tác quốc tế. Do đó, cần quy định rõ đầu mối phối hợp, trách nhiệm của từng cơ quan, phương thức chia sẻ thông tin, quy trình xử lý sự cố, cơ chế bảo mật thông tin và trách nhiệm trong trường hợp chậm trễ, đùn đẩy hoặc phối hợp không hiệu quả.

Bên cạnh yếu tố con người, cần đầu tư công cụ kỹ thuật phục vụ phát hiện, cảnh báo, giám sát, điều tra và ứng phó sự cố an ninh mạng. Các cơ quan thực thi cần được trang bị hệ thống phân tích mã độc, công cụ giám định dữ liệu điện tử, phần mềm truy vết giao dịch, hệ thống giám sát nguy cơ, công cụ phân tích dữ liệu lớn, nền tảng lưu trữ và bảo quản chứng cứ điện tử, cũng như các công cụ hỗ trợ điều tra đối với tài sản số, tiền mã hóa, nền tảng xuyên biên giới và các phương thức tấn công mới.

#### ***4.3.3.2. Thiết lập cơ chế phối hợp liên ngành rõ ràng***

Thiết lập cơ chế phối hợp liên ngành rõ ràng là yêu cầu cấp thiết nhằm nâng cao hiệu quả tổ chức thi hành pháp luật về an ninh mạng. An ninh mạng là lĩnh vực có tính liên ngành, liên vùng, liên thông và xuyên biên giới, liên quan đồng thời đến nhiều cơ quan, lĩnh vực quản lý. Vì vậy, việc bảo vệ an ninh mạng không thể được thực hiện hiệu quả nếu thiếu cơ chế phối hợp thống nhất, rõ trách nhiệm, rõ thẩm quyền và rõ quy trình xử lý giữa các cơ quan, tổ chức có liên quan.

Theo đó, cần xác định rõ cơ quan chủ trì và cơ quan phối hợp trong từng nhóm hoạt động cụ thể. Cơ chế phối hợp liên ngành cần quy định cụ thể

thời hạn xử lý đối với từng loại vụ việc. Trong lĩnh vực an ninh mạng, thời gian xử lý có ý nghĩa đặc biệt quan trọng, bởi nguy cơ có thể lan truyền rất nhanh, dữ liệu có thể bị xóa, sửa đổi, mã hóa hoặc chuyển dịch qua nhiều hệ thống, nhiều quốc gia. Cùng với đó, cần hoàn thiện cơ chế chia sẻ thông tin giữa các cơ quan, tổ chức trong bảo vệ an ninh mạng. Việc chia sẻ thông tin phải bao gồm thông tin cảnh báo nguy cơ, thông tin về phương thức, thủ đoạn tấn công mạng, thông tin về mã độc, lỗ hổng bảo mật, dấu hiệu vi phạm, dữ liệu phục vụ điều tra, chứng cứ điện tử và thông tin về kết quả xử lý sự cố. Một nội dung quan trọng khác là phải xác lập cơ chế trách nhiệm khi cơ quan, tổ chức chậm trễ, không phối hợp hoặc phối hợp không đầy đủ. Đồng thời, cần thiết lập cơ chế giải quyết xung đột thẩm quyền trong quá trình phối hợp liên ngành. Ngoài phối hợp giữa các cơ quan nhà nước, cần tăng cường cơ chế phối hợp giữa Nhà nước với doanh nghiệp cung cấp dịch vụ trên không gian mạng, chủ quản hệ thống thông tin, tổ chức xã hội, cơ sở nghiên cứu, đào tạo và chuyên gia kỹ thuật.

#### ***4.3.3.3. Bảo đảm nguồn lực thực hiện pháp luật***

Đặc thù của lĩnh vực an ninh mạng luôn đòi hỏi sự kết hợp giữa nguồn lực pháp lý, nguồn lực con người, nguồn lực tài chính, hạ tầng kỹ thuật, hệ thống dữ liệu, công cụ giám sát, phân tích và cơ chế phối hợp giữa nhiều chủ thể. Vì vậy, hoàn thiện pháp luật về an ninh mạng phải gắn liền với việc bảo đảm các điều kiện vật chất, kỹ thuật, nhân lực và tài chính đồng bộ cho quá trình thực hiện pháp luật.

Trước hết, cần bảo đảm nguồn lực ngân sách ổn định, phù hợp với yêu cầu bảo vệ an ninh mạng trong từng giai đoạn. Bên cạnh nguồn lực ngân sách, cần chú trọng phát triển nguồn nhân lực chất lượng cao trong lĩnh vực an ninh mạng. Ngoài ra, cần bảo đảm hạ tầng kỹ thuật và công cụ công nghệ phục vụ thực hiện pháp luật về an ninh mạng. Việc đầu tư hạ tầng kỹ thuật cần được thực hiện có trọng tâm, trọng điểm, tránh dàn trải, hình thức hoặc không phù hợp với năng lực vận hành thực tế. Nguồn lực thực hiện pháp luật về an ninh

mạng cũng cần được phân bổ theo mức độ rủi ro. Cần ưu tiên nguồn lực cho hệ thống thông tin quan trọng về ANQG, cơ sở dữ liệu quốc gia, hệ thống phục vụ dịch vụ công thiết yếu và các lĩnh vực có tác động lớn đến ANQG, TTATXH như tài chính, ngân hàng, năng lượng, y tế, giao thông, viễn thông, quốc phòng, an ninh. Cần xây dựng cơ chế thuê, huy động và sử dụng chuyên gia trong trường hợp cần thiết; tăng cường hợp tác công - tư trong bảo đảm nguồn lực thực hiện pháp luật về an ninh mạng. Bên cạnh việc bảo đảm nguồn lực, cần có cơ chế kiểm tra, đánh giá hiệu quả sử dụng nguồn lực trong thực hiện pháp luật về an ninh mạng. Việc đánh giá cần dựa trên các tiêu chí như mức độ giảm thiểu rủi ro, khả năng phát hiện và ứng phó sự cố, năng lực bảo vệ hệ thống thông tin quan trọng, hiệu quả phối hợp liên ngành, chất lượng nhân lực và mức độ bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức trong quá trình thực thi pháp luật.

#### **Tiểu kết chương 4**

Trên cơ sở việc nghiên cứu, đánh giá thực trạng an ninh mạng ở nước ta hiện nay, tại Chương 4, Luận án đã khái quát cơ bản những yêu cầu đặt ra với công tác hoàn thiện pháp luật về an ninh mạng ở nước ta hiện nay. Cụ thể như: phải đáp ứng yêu cầu phát triển kinh tế - xã hội bền vững, đẩy mạnh hội nhập quốc tế nhưng phải lấy bảo đảm quốc phòng, an ninh, an sinh xã hội, trật tự an toàn của đất nước là ưu tiên; phải bảo đảm phát huy và thể hiện sâu sắc nền dân chủ xã hội chủ nghĩa; phải bám sát thực tiễn đất nước và xu thế phát triển của thời đại; phải kế thừa và tiếp nối truyền thống văn hóa pháp lý của đất nước ta. Trước những yêu cầu đó cùng với hệ thống lý luận đã được làm rõ tại Chương 2, trong Chương này, nghiên cứu sinh đã khái quát một số quan điểm trong hoàn thiện pháp luật về an ninh mạng ở nước ta. Theo đó, những quan điểm này bao gồm: bảo đảm cân bằng giữa bảo vệ ANQG và bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức; phải dựa trên quản trị rủi ro, không chỉ dựa trên xử lý sau vi phạm; phải bảo đảm tính đồng bộ giữa QPPL và cơ chế thực thi; phải thích ứng với công nghệ nhưng không chạy theo từng hiện tượng kỹ

thuật đơn lẻ. Trong bối cảnh hiện nay, để hoàn thiện pháp luật về an ninh mạng, nghiên cứu sinh đã trình bày một số giải pháp mang tính trước mắt và một số giải pháp mang tính chiến lược lâu dài. Tuy nhiên, trước hết các quy định pháp luật về an ninh mạng ở Việt Nam cần bổ sung hoàn thiện quy định về nguyên tắc bảo vệ an ninh mạng; quy định hành vi vi phạm pháp luật về an ninh mạng; quy định về biện pháp bảo vệ an ninh mạng; quy định địa vị pháp lý của các chủ thể, thẩm quyền xử lý hành vi vi phạm pháp luật về an ninh mạng; quy định chế tài xử lý hành vi vi phạm pháp luật về an ninh mạng; quy định hợp tác quốc tế về an ninh mạng. Với nhóm giải pháp bảo đảm tính đồng bộ, minh bạch và chất lượng lập pháp trong lĩnh vực an ninh mạng cần rà soát, hệ thống hóa và xử lý chồng chéo giữa các văn bản pháp luật; nâng cao chất lượng đánh giá tác động chính sách; chuẩn hóa thuật ngữ và kỹ thuật lập pháp. Với nhóm giải pháp trong tổ chức thực hiện pháp luật về an ninh mạng cần: nâng cao năng lực của cơ quan thực thi pháp luật về an ninh mạng; thiết lập cơ chế phối hợp liên ngành rõ ràng; bảo đảm nguồn lực thực hiện pháp luật.

## KẾT LUẬN

Trong bối cảnh chuyển đổi số quốc gia, không gian mạng đã trở thành môi trường quan trọng đối với hoạt động của Nhà nước, nền kinh tế và đời sống xã hội. Cùng với những lợi ích do công nghệ số mang lại, các nguy cơ xâm phạm an ninh mạng ngày càng gia tăng về quy mô, tính chất, mức độ phức tạp và hậu quả. an ninh mạng vì vậy không còn là vấn đề kỹ thuật đơn thuần, mà đã trở thành vấn đề chính trị - pháp lý, gắn trực tiếp với bảo vệ ANQG, TTATXH, chủ quyền quốc gia trên không gian mạng, quyền con người, quyền công dân và sự phát triển bền vững của đất nước. Do đó, hoàn thiện pháp luật về an ninh mạng ở Việt Nam là yêu cầu khách quan, cấp thiết và có ý nghĩa chiến lược.

Về phương diện lý luận, luận án tiếp cận pháp luật về an ninh mạng như một lĩnh vực pháp luật có tính liên ngành, có tính độc lập tương đối, nằm ở giao điểm giữa bảo vệ ANQG, bảo đảm TTATXH, quản trị rủi ro công nghệ, bảo vệ dữ liệu, bảo vệ quyền con người, quyền công dân và quản lý hoạt động của các chủ thể trên không gian mạng. Trên cơ sở đó, luận án làm rõ khái niệm pháp luật về an ninh mạng và xác định cấu trúc lý luận của lĩnh vực pháp luật này gồm sáu nhóm chế định cơ bản: nguyên tắc bảo vệ an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng; chế tài xử lý hành vi vi phạm; địa vị pháp lý của các chủ thể; biện pháp bảo vệ an ninh mạng; hợp tác quốc tế trong lĩnh vực an ninh mạng.

Luận án đã xác lập hệ tiêu chí đánh giá mức độ hoàn thiện của pháp luật về an ninh mạng ở Việt Nam, gồm ba nhóm: nhóm tiêu chí về nội dung pháp luật, bao gồm tính đầy đủ, tính đồng bộ, khả năng thích ứng với công nghệ và mức độ bảo đảm quyền, lợi ích hợp pháp của cá nhân, tổ chức; nhóm tiêu chí về kỹ thuật pháp lý, bao gồm tính minh bạch và kỹ thuật lập pháp; nhóm tiêu chí về thực thi pháp luật, bao gồm tính khả thi và hiệu quả của cơ chế thực thi. Hệ tiêu chí này là cơ sở khoa học để đánh giá thực trạng pháp luật, thực tiễn thực hiện pháp luật và đề xuất giải pháp hoàn thiện pháp luật về an ninh mạng ở Việt Nam.

Về thực trạng, luận án cho thấy pháp luật về an ninh mạng ở Việt Nam đã từng bước hình thành, phát triển từ các quy định phân tán trong pháp luật về công nghệ thông tin, viễn thông, giao dịch điện tử, an toàn thông tin mạng và xử lý vi phạm đến giai đoạn chuyên biệt hóa với Luật An ninh mạng năm 2018 và các văn bản hướng dẫn thi hành. Việc Quốc hội thông qua Luật An ninh mạng số 116/2025/QH15 tiếp tục thể hiện xu hướng hoàn thiện pháp luật theo hướng thống nhất, đồng bộ và phù hợp hơn với yêu cầu quản trị không gian mạng trong bối cảnh chuyển đổi số.

Pháp luật về an ninh mạng ở Việt Nam hiện nay đã đạt được nhiều kết quả quan trọng. Hệ thống pháp luật đã bước đầu xác lập khung điều chỉnh tương đối toàn diện đối với sáu nhóm chế định cơ bản; tạo cơ sở pháp lý cho việc bảo vệ ANQG, TTATXH, hệ thống thông tin quan trọng, dữ liệu, quyền và lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng; từng bước nhận diện các hành vi vi phạm, thiết lập hệ thống chế tài, xác định trách nhiệm của các chủ thể, quy định các biện pháp bảo vệ an ninh mạng và ghi nhận hợp tác quốc tế trong lĩnh vực này.

Tuy nhiên, pháp luật về an ninh mạng ở Việt Nam vẫn còn một số hạn chế, bất cập. Một số nguyên tắc bảo vệ an ninh mạng chưa thể hiện đầy đủ yêu cầu quản trị rủi ro, trách nhiệm giải trình, kiểm soát quyền lực và bảo vệ quyền của chủ thể bị tác động. Quy định về hành vi vi phạm chưa theo kịp các hành vi mới phát sinh từ trí tuệ nhân tạo, deepfake, tài sản số, tiền mã hóa, nền tảng xuyên biên giới, tấn công chuỗi cung ứng và xâm phạm dữ liệu quy mô lớn. Một số chế tài xử lý chưa thật sự tương xứng với tính chất, mức độ và hậu quả của hành vi vi phạm. Địa vị pháp lý của một số chủ thể mới trong hệ sinh thái số chưa được xác định đầy đủ. Một số biện pháp bảo vệ an ninh mạng chưa được quy định thật rõ về căn cứ, điều kiện, thẩm quyền, trình tự, thủ tục, thời hạn, phạm vi áp dụng và cơ chế kiểm soát. Hợp tác quốc tế về an ninh mạng còn thiếu cơ chế chuyên biệt, nhất là trong thu thập, bảo quản, chuyển giao chứng cứ điện tử, xử lý tội phạm mạng xuyên biên giới và hợp

tác với nền tảng số nước ngoài. Thực tiễn thực hiện pháp luật, mặc dù có nhiều chuyển biến tích cực, tuy nhiên, tình trạng lộ, mất dữ liệu, mua bán dữ liệu cá nhân, lừa đảo trực tuyến, tấn công mạng, phát tán thông tin sai sự thật, sử dụng công nghệ cao để phạm tội vẫn diễn biến phức tạp; cơ chế phối hợp liên ngành, chia sẻ dữ liệu, báo cáo sự cố, thu thập chứng cứ điện tử và hợp tác với doanh nghiệp cung cấp dịch vụ xuyên biên giới còn chưa đáp ứng đầy đủ yêu cầu thực tiễn.

Trên cơ sở đó, luận án đề xuất các nhóm giải pháp hoàn thiện pháp luật về an ninh mạng. Về nội dung pháp luật, cần tiếp tục hoàn thiện sáu nhóm chế định cơ bản: bổ sung các nguyên tắc quản trị rủi ro, tương xứng, trách nhiệm giải trình, phối hợp đa chủ thể và kiểm soát quyền lực; thiết kế lại quy định về hành vi vi phạm theo hướng kết hợp giữa liệt kê hành vi điển hình và tiêu chí nhận diện mở; hoàn thiện chế tài xử lý theo hướng phân tầng, tương xứng và gắn với khắc phục hậu quả; xác định rõ địa vị pháp lý của các chủ thể trong hệ sinh thái số; cụ thể hóa các biện pháp bảo vệ an ninh mạng về căn cứ, điều kiện, thẩm quyền, trình tự, thủ tục và cơ chế kiểm soát; mở rộng hợp tác quốc tế trong lĩnh vực chứng cứ điện tử, dữ liệu xuyên biên giới, tội phạm mạng và nền tảng số xuyên biên giới. Về tổ chức thực thi, cần nâng cao năng lực của cơ quan có thẩm quyền, lực lượng chuyên trách bảo vệ an ninh mạng, chủ quản hệ thống thông tin và doanh nghiệp cung cấp dịch vụ trên không gian mạng; xây dựng cơ chế phối hợp liên ngành thống nhất, có đầu mối điều phối rõ ràng; phát triển nguồn nhân lực pháp lý - kỹ thuật chuyên sâu; đầu tư hạ tầng giám sát, cảnh báo, ứng cứu sự cố, giám định số và bảo toàn chứng cứ điện tử; tăng cường thanh tra, kiểm tra, xử lý vi phạm; đồng thời hoàn thiện cơ chế giám sát, trách nhiệm giải trình, khiếu nại, tố cáo, bồi thường thiệt hại và khắc phục hậu quả khi việc áp dụng biện pháp bảo vệ an ninh mạng xâm phạm quyền, lợi ích hợp pháp của cá nhân, tổ chức.

## **DANH MỤC CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ**

1. Bùi Thị Thùy Dung (2022), Sách chuyên khảo An ninh truyền thống và an ninh phi truyền thống trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư, Nhà xuất bản Công an nhân dân, Hà Nội.

2. Bùi Thị Thùy Dung (2023), Giá trị tác phẩm “Chủ quyền không gian mạng - yêu cầu thời đại và nghĩa vụ quốc gia” với tiến trình hoàn thiện pháp luật về an ninh mạng, Kỷ yếu Hội thảo khoa học “Bình luận khoa học cuốn sách “Chủ quyền không gian mạng yêu cầu thời đại và nghĩa vụ quốc gia”, Hà Nội.

3. Bùi Thị Thùy Dung (2025), Kiến nghị hoàn thiện pháp luật hình sự về an ninh mạng ở Việt Nam hiện nay, Tạp chí Quản lý Nhà nước, số 352 (5/2025), Hà Nội.

4. Bùi Thị Thùy Dung, Triệu Mạnh Tùng (2025), Đổi mới tư duy pháp lý về an ninh mạng trong kỷ nguyên mới, Tạp chí Cộng sản, Hà Nội.

5. Bùi Thị Thùy Dung (2025), Kinh nghiệm quốc tế về quản lý tiền điện tử và những gợi mở cho Việt Nam, Tạp chí Quản lý Nhà nước, số tháng 8/2025, Hà Nội.

6. Bùi Thị Thùy Dung (2025), Nhận diện âm mưu chuyển hóa vấn đề trật tự, an toàn xã hội thành vấn đề an ninh quốc gia của các thế lực thù địch hiện nay, Tạp chí Công an nhân dân số tháng 3/2025, Hà Nội.

7. Bùi Thị Thùy Dung (2025), Âm mưu, hoạt động lợi dụng tôn giáo để chuyển hóa vấn đề trật tự, an toàn xã hội thành an ninh quốc gia trên không gian mạng hiện nay, Tạp chí Lý luận Chính trị Công an nhân dân số tháng 10/2025, Hà Nội.

## **DANH MỤC TÀI LIỆU THAM KHẢO**

### **Tài liệu trong nước:**

1. Trần Xuân Thiên An (2022), Đấu tranh phòng, chống tội phạm công nghệ cao tại Nigeria và kinh nghiệm cho Việt Nam (Fighting against high-tech crimes in Nigeria and experience for Vietnam), Tạp chí Kiểm sát, Hà Nội.
2. GS.TS Nguyễn Ngọc Anh (2019), Pháp luật về an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao ở Việt Nam, Nxb Chính trị quốc gia Sự thật, Hà Nội.
3. Nguyễn Ngọc Anh (2022), Pháp luật về hoạt động môi giới thương mại điện tử, Luận án Tiến sĩ, Đại học Luật Hà Nội.
4. Nguyễn Mai Linh, Ngô Thị Hương Giang, Nguyễn Quý Cảnh, Nguyễn Phương Anh (2021), Pháp luật về điện toán đám mây trong thương mại điện tử ở một số quốc gia và Việt Nam, Tạp chí Nghiên cứu lập pháp, Hà Nội.
5. PGS.TS. Nguyễn Thị Quế Anh và PGS. TS. Ngô Huy Cương - Đồng chủ biên (2019), Cách mạng công nghiệp lần thứ Tư và những vấn đề đặt ra đối với cải cách pháp luật Việt Nam, Nxb. Chính trị quốc gia, Hà Nội.
6. Nguyễn Thị Quế Anh (2022), Hoàn thiện pháp luật sở hữu trí tuệ Việt Nam trong bối cảnh phát triển trí tuệ nhân tạo, Tạp chí Luật học (Đại học Quốc gia Hà Nội), số 3/2022
7. Ban Chấp hành Trung ương Đảng khóa XIII (2023), Nghị quyết số 44-NQ/TW, ngày 24/11/2023 về Chiến lược bảo vệ Tổ quốc trong tình hình mới, Hà Nội.
8. Phạm Thị Thanh Bình, Vũ Văn Hà (2022), Vấn đề an ninh mạng ở các nước Đông Nam Á (Cybersecurity Issues in Southeast Asian Countries, Tạp chí Nghiên cứu Đông Nam Á, Hà Nội.
9. Nguyễn Mai Bộ (2022), Vấn đề an toàn thông tin và an ninh mạng trong giao dịch điện tử (Issues of information safety and network security in electronic transactions), Tạp chí Nghiên cứu lập pháp, Hà Nội.

10. Ban Chỉ đạo An ninh mạng quốc gia - Văn phòng (2026), Báo cáo về kết quả hoạt động của Ban Chỉ đạo An ninh mạng quốc gia năm 2025, số 02/BC-VPBCĐ ngày 04/3/2026, Hà Nội.
11. Bộ Chính trị (2018), Nghị quyết số 23-NQ/TW, ngày 22-3-2018 về “Định hướng xây dựng chính sách phát triển công nghiệp quốc gia đến năm 2030, tầm nhìn đến năm 2045”, Hà Nội.
12. Bộ Chính trị (2019), Nghị quyết số 52-NQ/TW, ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư, Hà Nội.
13. Bộ Chính trị (2022), Nghị quyết số 27-NQ/TW, ngày 09-11-2022 về “Tiếp tục xây dựng và hoàn thiện Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam trong giai đoạn mới”, Hà Nội.
14. Bộ Chính trị (2024), Nghị quyết số 57-NQ/TW, ngày 22-12-2024 về “Đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia”, Hà Nội.
15. Bộ Chính trị (2025), Nghị quyết số 66-NQ/TW, ngày 30-4-2025 về “Đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới”, Hà Nội.
16. Bộ Chính trị (2024), Nghị quyết số 68-NQ/TW, ngày 04-5-2025 về “Phát triển kinh tế tư nhân”, Hà Nội.
17. Bộ Công an, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ (2017), Bảo đảm an ninh mạng, an ninh thông tin trong thời kỳ cách mạng công nghiệp lần thứ 4, Kỷ yếu Hội thảo - Triển lãm quốc gia về An toàn bảo mật năm 2017, Hà Nội.
18. Bộ Công an (2018), “Các loại tội phạm công nghệ cao ở Việt Nam, bao gồm tội phạm lạm dụng tình dục trực tuyến và tội phạm liên quan đến tiền mã hóa, các biện pháp phòng ngừa hoạt động tội phạm”, Tài liệu Hội thảo bàn tròn quốc gia về an ninh mạng và tội phạm sử dụng công nghệ cao, do UNODC và Bộ Công an tổ chức ngày 24, 25/9/2018 tại Thành phố Hồ Chí Minh, Thành phố Hồ Chí Minh.

19. Bộ Công an (2023), Tổng tập lý luận nghiệp vụ an ninh, tập I, II, Nxb Công an nhân dân, Hà Nội.
20. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (2018), Báo cáo tổng kết công tác năm 2018, 2019, 2020, 2021, 2022, 2023, 2024, Hà Nội.
21. Bộ Quốc phòng (2019), Sách Trắng Quốc phòng Việt Nam, Nxb Chính trị quốc gia Sự thật, Hà Nội.
22. Bộ Khoa học và Công nghệ (2021), Nghiên cứu, xây dựng phần mềm giám sát, cảnh báo, hỗ trợ công tác phòng, chống tấn công trên mạng cục bộ, bảo đảm an toàn thông tin trong các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh, Nhiệm vụ nghiên cứu cấp tỉnh/thành phố, Hà Tĩnh.
23. Bộ Thông tin và Truyền thông (2017), Nhiệm vụ nghiên cứu cấp Bộ Nghiên cứu đề xuất các biện pháp xử lý vi phạm hành chính trong lĩnh vực an toàn thông tin trên mạng, Hà Nội.
24. Bộ Thông tin và Truyền thông (2017), Nhiệm vụ nghiên cứu cấp Bộ Nghiên cứu kinh nghiệm xây dựng chiến lược quốc gia về an toàn không gian mạng và đề xuất cho Việt Nam, Hà Nội.
25. Bộ Thông tin và Truyền thông, Sách Trắng Công nghệ thông tin và Truyền thông Việt Nam các năm 2018, 2019, 2020, 2021, 2022, 2023, Nxb Thông tin và Truyền thông, Hà Nội.
26. Bộ Thông tin và Truyền thông (2020), An ninh mạng trong cuộc cách mạng công nghiệp 4.0, Nxb Thông tin và Truyền thông, Hà Nội.
27. Bộ Thông tin và Truyền thông (2020), Nhiệm vụ nghiên cứu cấp Bộ Nghiên cứu xây dựng bộ tiêu chuẩn về các kỹ thuật an toàn công nghệ thông tin (Lựa chọn, triển khai và vận hành các hệ thống phát hiện và ngăn chặn xâm nhập (IDPS) và các tiêu chuẩn ISO/IEC về an toàn thông tin), Hà Nội.
28. Bộ Tư pháp (2020), Nhiệm vụ khoa học cấp Bộ Nghiên cứu xây dựng những định hướng chính sách lớn hoàn thiện pháp luật về xử lý vi phạm hành chính, Hà Nội.

29. Bộ Tư pháp (2020), Nhiệm vụ khoa học cấp Bộ Hoàn thiện pháp luật về phòng, chống rửa tiền trong bối cảnh cách mạng công nghiệp 4.0, Hà Nội.
30. Bộ Tư pháp (2023), Nhiệm vụ khoa học cấp Bộ Hoàn thiện pháp luật hình sự Việt Nam đáp ứng yêu cầu phòng, chống tội phạm trong bối cảnh Cách mạng công nghiệp lần thứ tư, Hà Nội.
31. Mai Chi (2022), Tăng cường quản lý nhà nước về bảo đảm an toàn thông tin, an ninh mạng xã hội ở Việt Nam hiện nay, Tạp chí giáo dục lý luận, Hà Nội.
32. Chính phủ (1997), Nghị định số 21/NĐ-CP ngày 05/3/1997 về việc ban hành Quy chế tạm thời về quản lý, thiết lập, sử dụng mạng Internet ở Việt Nam, Hà Nội.
33. Chính phủ (2001), Nghị định số 55/NĐ-CP ngày 23/8/2001 về quản lý, cung cấp và sử dụng dịch vụ Internet, Hà Nội.
34. Chính phủ (2008), Nghị định số 97/NĐ-CP ngày 28/8/2008 về quản lý, cung cấp và sử dụng dịch vụ Internet và thông tin điện tử trên Internet, Hà Nội.
35. Chính phủ (2013), Nghị định 72/2013/NĐ-CQ ngày 15/7/2013 quy định về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng, Hà Nội.
36. Chính phủ (2014), Nghị định số 25/2014/NĐ-CP ngày 07/4/2014 quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao, Hà Nội.
37. Chính phủ (2016), Nghị định 142/2016/NĐ-CP ngày 14/10/2016 về ngăn chặn xung đột thông tin mạng, Hà Nội.
38. Chính phủ (2018), Nghị định số 27/2018/NĐ-CP ngày 01/3/2018 sửa đổi, bổ sung một số điều của Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng, Hà Nội.

39. Chính phủ (2018), Nghị định số 130/2018/NĐ-CP ngày 27/9/2018 quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số, Hà Nội.
40. Chính phủ (2019), CÔNG BÁO/Số 773+774, 775+776, 777+778, 779 + 780/ngày 17/10/2017, Văn bản hợp nhất Bộ luật Hình sự, Hà Nội.
41. Chính phủ (2019), CÔNG BÁO/Số 291+292/ngày 03/11/2019, Văn bản hợp nhất Luật An toàn thông tin mạng, Hà Nội.
42. Chính phủ (2020), Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử, Hà Nội.
43. Chính phủ (2020), Nghị định 91/2020/NĐ-CP ngày 14/8/2020 về chống tin nhắn rác, thư điện tử rác, cuộc gọi rác, Hà Nội.
44. Chính phủ (2020), 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, Hà Nội.
45. Chính phủ (2021), Nghị định số 144/2021/NĐ-CP ngày 31/12/2021 quy định về xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội, phòng, chống tệ nạn xã hội, phòng cháy, chữa cháy, cứu nạn, cứu hộ, phòng, chống bạo lực gia đình, Hà Nội.
46. Chính phủ (2022), CÔNG BÁO/Số 643+644/Ngày 03-8-2022, Văn bản hợp nhất Nghị định quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin, an toàn thông tin mạng và giao dịch điện tử, Hà Nội.
47. Chính phủ (2022), Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng, Hà Nội.
48. Chính phủ (2023), CÔNG BÁO/Số 485+486/Ngày 19-02-2023, Văn bản hợp nhất Luật Xử lý vi phạm hành chính, Hà Nội.
49. Chính phủ (2023), Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 quy định về bảo vệ dữ liệu cá nhân, Hà Nội.

50. Chính phủ (2023), CÔNG BÁO/Số 361+362/Ngày 13-02-2023, Văn bản hợp nhất Luật Sở hữu trí tuệ, Hà Nội.
51. Chính phủ (2023), CÔNG BÁO/Số 365+366/Ngày 13-02-2023, Văn bản hợp nhất Luật Khoa học và công nghệ, Hà Nội.
52. Chính phủ (2024), CÔNG BÁO/Số 385+386/Ngày 08-3-2024, Văn bản hợp nhất Luật Tàn số vô tuyến điện, Hà Nội.
53. Chính phủ (2024), CÔNG BÁO/Số 389+390/Ngày 09-3-2024, Văn bản hợp nhất Luật Công nghệ thông tin, Hà Nội.
54. Chính phủ (2024), CÔNG BÁO/Số 1151+1152/Ngày 27-10-2024, Văn bản hợp nhất Luật Công an nhân dân, Hà Nội.
55. Công an thành phố Hà Nội (2019), Phòng, chống tội phạm và vi phạm pháp luật liên quan đến hoạt động “Tín dụng đen” trên địa bàn thành phố Hà Nội, Nhiệm vụ khoa học cấp Bộ, năm 2019.
56. Phí Mạnh Cường (2022), Pháp luật về thương mại điện tử ở Việt Nam, Luận án Tiến sĩ, Đại học Luật Hà Nội.
57. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2019), Báo cáo số 5407/BC-A05-P1 ngày 26/11/2019 về tổng kết tình hình, kết quả công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2019, phương hướng nhiệm vụ trọng tâm năm 2020, Hà Nội.
58. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2020), Báo cáo số 6369/BC-A05-P1 ngày 30/11/2020 về tổng kết tình hình, kết quả công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2020, phương hướng nhiệm vụ trọng tâm năm 2021, Hà Nội.
59. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2022), Thông báo số 205/TB-A05-P1 ngày 14/01/2022 về tình hình, kết quả công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2021, Hà Nội.

60. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2022), Báo cáo số 6556/BC-A05-P1 ngày 21/12/2022 về tổng kết công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2022, Hà Nội.
61. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2023), Báo cáo số 6686/BC-A05-P1 ngày 07/12/2020 về tổng kết tình hình, kết quả công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2023, phương hướng nhiệm vụ trọng tâm năm 2024, Hà Nội.
62. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2024), Báo cáo số 7833/BC-A05-P1 ngày 06/12/2024 về tổng kết tình hình, kết quả công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2024, phương hướng nhiệm vụ trọng tâm năm 2025, Hà Nội.
63. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2025), Báo cáo số 10316/BC-A05-P1 ngày 05/12/2025 về tổng kết tình hình, kết quả công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao năm 2025, phương hướng nhiệm vụ trọng tâm năm 2026, Hà Nội.
64. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (2020), Kỷ yếu Hội thảo An ninh, an toàn thông tin mạng - Chìa khóa bảo đảm hoạt động ổn định và phát triển bền vững cho các cơ quan, tổ chức, doanh nghiệp, Hà Nội.
65. Nguyễn Ngọc Cương (2010), Tin học ứng dụng trong điều tra tội phạm, Nxb Công an nhân dân, Hà Nội.
66. Trần Đại Quang, Phạm Ngọc Lăng, Nguyễn Trường Thắng, Nguyễn Ngọc Cương (2016), Giáo trình An ninh không gian mạng, Nxb Công an nhân dân, Hà Nội.
67. Nguyễn Văn Công (2022), Tấn công mạng dưới góc độ pháp luật quốc tế và pháp luật Việt Nam (Cyber attack from the perspectives of international and Vietnamese law), Tạp chí Luật học, Hà Nội.

68. Hạ Thị Thiếu Dao, Lại Văn Tài (2021), Tội phạm sử dụng công nghệ cao và phòng chống tội phạm sử dụng công nghệ cao tại Việt Nam, Tạp chí Thị trường Tài chính tiền tệ, Hà Nội.
69. Trần Vi Dân (2016), Phương hướng hoàn thiện hệ thống văn bản pháp luật về bảo vệ an ninh quốc gia trong tình hình hiện nay, Đề tài nghiên cứu khoa học cấp Bộ.
70. Phạm Hồng Diên (2022), Hoàn thiện pháp luật về trung cầu ý dân ở Việt Nam hiện nay, Luận án Tiến sĩ, Đại học Luật Hà Nội.
71. Nguyễn Văn Phương, Trần Văn Diễn (2021), Rủi ro và thách thức an ninh mạng trong lĩnh vực ngân hàng tại Việt Nam (Risks and challenges for cybersecurity in the banking sector in Vietnam), Tạp chí Khoa học (Đại học Mở thành phố Hồ Chí Minh).
72. Trần Thị Hồng Minh, Nguyễn Anh Dương (2023), Hệ thống chính sách của chuyển đổi số trong thương mại: thực trạng và giải pháp, Tạp chí Khoa học & công nghệ Việt Nam, Hà Nội.
73. Trần Tuấn Duy, Phan Trần Mai Phương (2020), Giải pháp tăng cường bảo vệ không gian mạng theo quan điểm của Đảng và pháp luật của nhà nước của nhóm tác giả, Tạp chí Phát triển nhân lực, Hà Nội.
74. Đại học Luật Hà Nội (2020), Giáo trình Lý luận về nhà nước và pháp luật (tái bản lần thứ tư, có sửa chữa, bổ sung), Nxb Chính trị quốc gia Sự thật, Hà Nội.
75. Đại học Luật Hà Nội (2018), Các khía cạnh pháp lý của tiền ảo: Thực tiễn các nước và một số kinh nghiệm cho Việt Nam, Nhiệm vụ khoa học cấp Bộ, Đại học Luật Hà Nội.
76. Đại học Quốc gia Hà Nội (2019), Nhiệm vụ nghiên cứu cấp Quốc gia, Ứng dụng công nghệ bảo đảm an ninh, an toàn mạng và bí mật thông tin ở mức cao để phát triển bộ giải pháp an toàn an ninh mạng LAN cho cơ quan nhà nước và doanh nghiệp, Hà Nội.
77. Đại học Quốc gia Hà Nội (2017), Giáo trình Đại cương về Nhà nước và pháp luật, Nxb Đại học quốc gia Hà Nội, Hà Nội.

78. Đại học Quốc gia Hà Nội (2019), Nhiệm vụ nghiên cứu cấp Quốc gia Ứng dụng công nghệ bảo đảm an ninh, an toàn mạng và bí mật thông tin ở mức cao để phát triển bộ giải pháp an toàn an ninh mạng LAN cho cơ quan nhà nước và doanh nghiệp, Đại học Quốc gia, Hà Nội.
79. Đảng Cộng sản Việt Nam, Văn kiện Đại hội đại biểu toàn quốc lần thứ VI, VII, VIII, IX, X, XI, XII, XIII, Nxb Chính trị quốc gia, Hà Nội.
80. Đài Tiếng nói Việt Nam (2022), Nghiên cứu, đề xuất giải pháp bảo đảm an ninh mạng cho Đài Tiếng nói Việt Nam trong tình hình mới, Nhiệm vụ nghiên cứu cấp Bộ, Hà Nội.
81. Nguyễn Tân Đăng, Hoàng Sỹ Tương (2022), An ninh mạng - Thành tố quan trọng trong chuyển đổi số, Tạp chí Công nghệ thông tin và truyền thông, Hà Nội.
82. Nguyễn Minh Đoan, Nguyễn Minh Đức (2019), Xây dựng và hoàn thiện hệ thống pháp luật Việt Nam trong bối cảnh xây dựng nhà nước pháp quyền xã hội chủ nghĩa, Nxb CTQG Sự thật, Hà Nội.
83. Dương Hải Hà, Lê Minh Toàn (2022), Những điểm mới về quản lý giao dịch thương mại điện tử, Tạp chí Công nghệ thông tin và truyền thông, Hà Nội.
84. Đỗ Thị Hà (2020), Những khía cạnh pháp lý về cấm sử dụng vũ lực, đe dọa sử dụng vũ lực và quyền tự vệ của quốc gia trên không gian mạng trong luật quốc tế, Tạp chí Khoa học Kiểm sát, Hà Nội.
85. Trịnh Thu Hà (2023), Một số dự báo an ninh mạng trong năm 2023 (Some cybersecurity forecasts in 2023), Tạp chí Ngân hàng (Chuyên đề Công nghệ và Ngân hàng số), Hà Nội.
86. Đào Trí Úc, Trương Thị Hồng Hà (2018), Hoàn thiện hệ thống pháp luật đáp ứng yêu cầu xây dựng Nhà nước pháp quyền xã hội chủ nghĩa ở Việt Nam hiện nay, Nxb. Chính trị quốc gia Sự thật, Hà Nội.
87. Nguyễn Thị Hạnh (2013), Nghiên cứu sửa đổi, bổ sung chế định Chính phủ trong Hiến pháp năm 1992, Đề tài khoa học cấp Bộ, Hà Nội.

88. Trần Thị Hồng Hạnh (2021), Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam, Nhà xuất bản Đại học Quốc gia Hà Nội.
89. Trần Thị Hằng (2016), Nghiên cứu tìm hiểu thực trạng về an ninh mạng và biện pháp khắc phục, Luận văn Thạc sĩ, Hà Nội.
90. Chu Thị Hoa (2022), Hoàn thiện pháp luật điều chỉnh mô hình kinh tế chia sẻ ở Việt Nam hiện nay, Nhà xuất bản Tư pháp, Hà Nội.
91. Nguyễn Thị Thúy Hoa (2018), Bảo đảm an ninh mạng đối với hệ thống thông tin trong cơ quan nhà nước, Tạp chí Khoa học Nội vụ, Hà Nội.
92. PGS.TS Trần Văn Hòa (2015), An ninh mạng trong cuộc cách mạng công nghiệp 4.0, Nxb Thông tin và truyền thông, Hà Nội.
93. Học viện Chính trị quốc gia Hồ Chí Minh (1985), Nhà nước và pháp luật, Nxb Pháp lý, Hà Nội.
94. Trần Thế Hệ (2023), Pháp luật về bảo vệ quyền lợi người tiêu dùng sử dụng dịch vụ vay trực tuyến tại các công ty tài chính (Law on protecting the interests of consumers using online loan services at financial companies) , Tạp chí Luật sư Việt Nam, Hà Nội.
95. Lâm Thị Thu Hiền (2023), Hoàn thiện pháp luật bảo hiểm xã hội bắt buộc ở Việt Nam, Luận án Tiến sĩ, Đại học Luật Hà Nội.
96. Trần Mạnh Hùng (2020), Gián điệp mạng từ góc nhìn mối đe dọa an ninh toàn cầu, Nxb Công an nhân dân, Hà Nội.
97. Vũ Ngọc Hưng (2022), An toàn thông tin mạng cho người tiêu dùng trên không gian mạng trong tình hình mới, Tạp chí Công nghệ thông tin và truyền thông, Hà Nội.
98. Lâm Văn Minh, Phùng Thu Phương, Nguyễn Sỹ Huy (2022), Hoàn thiện pháp luật quản lý thuế đối với sàn giao dịch thương mại điện tử, Tạp chí Kiểm sát, Hà Nội.
99. Trần Đăng Khoa (2022), Chiến lược an toàn, an ninh mạng quốc gia: Chủ động, sẵn sàng cho một Việt Nam số, Tạp chí Công nghệ thông tin và truyền thông, Hà Nội.
100. Nguyễn Quý Khuyến (2022), Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông theo Luật hình sự Việt Nam, Luận án Tiến sĩ, Đại học Luật Hà Nội.

101. GS.TS Tô Lâm (2021), Chủ quyền không gian mạng yêu cầu thời đại và nghĩa vụ quốc gia, Nxb Công an nhân dân, Hà Nội.
102. Nguyễn Việt Lâm (2019), Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam, Nxb Chính trị quốc gia sự thật, Hà Nội.
103. Nguyễn Việt Lâm (2021), Trung Quốc với vấn đề chủ quyền không gian mạng, Tạp chí Lý luận Chính trị, Hà Nội.
104. Tùng Lâm (2022), Năm mục tiêu chiến lược trong bảo đảm an toàn không gian mạng thời kỳ chuyển đổi số, Tạp chí Công nghệ thông tin và truyền thông, Hà Nội.
105. Võ Thị Thanh Linh (2022), Pháp luật về quảng cáo thương mại trên mạng xã hội ở Việt Nam, Luận án Tiến sĩ, Đại học Luật thành phố Hồ Chí Minh.
106. Hoàng Thế Liên (2015), Đổi mới tổ chức và hoạt động của Chính phủ ở Việt Nam hiện nay, Tạp chí Nhà nước và Pháp luật, số 7/2015, Hà Nội.
107. Bùi Thị Long (2021), Thực hiện pháp luật về an ninh mạng ở Việt Nam, Luận án Tiến sĩ, Học viện Chính trị quốc gia Hồ Chí Minh, Hà Nội.
108. Nguyễn Khắc Vĩnh Lộc (2021), Quản trị an ninh thông tin mạng xã hội trong sinh viên ở Việt Nam hiện nay, Luận văn Thạc sĩ, Hà Nội.
109. Nguyễn Hương Ly (2022), Hoàn thiện pháp luật về đầu tư công ở Việt Nam, Luận án Tiến sĩ, Học viện Khoa học xã hội, Hà Nội.
110. Hảo Linh (2018), An ninh mạng hay an toàn dữ liệu cho Việt Nam, Tia sáng, Hà Nội.
111. Liên hợp quốc (2025), Công ước của Liên hợp quốc về chống tội phạm mạng, bản tiếng Việt, Hà Nội.
112. Nguyễn Hoàng Chi Mai (2022), Kinh nghiệm quốc tế về xử lý tội phạm công nghệ cao và một số khuyến nghị cho Việt Nam, Tạp chí Kiểm sát, Hà Nội.
113. Nguyễn Công Minh (2021), Nhận biết và ngăn chặn hành vi đánh cắp dữ liệu, Tạp chí Ngân hàng (Chuyên đề Công nghệ và Ngân hàng số), số 01/2021, Hà Nội.

114. Bạch Thị Nhã Nam (2022), Hướng tiếp cận và hoàn thiện pháp luật bảo vệ dữ liệu cá nhân tại Việt Nam trước tác động lập pháp của thế giới và khu vực, Tạp chí luật học, Hà Nội.
115. Hoàng Thành Nam (2017), Tăng cường công tác thông tin tuyên truyền phòng, ngừa, chống vi phạm trên mạng Internet, Nxb Thông tin và Truyền thông, Hà Nội.
116. Huỳnh Nhân Nghĩa (2023), Bảo đảm an ninh quốc gia trong không gian mạng của Mỹ (2000 - 2020), Luận văn Thạc sĩ, Thành phố Hồ Chí Minh.
117. Lê Thị Minh Thư; Phạm Thị Thu Thảo; Huỳnh Tuyết Ngân; Nguyễn Thị Thu Nga (2022), Một số ý kiến về trách nhiệm bồi thường thiệt hại đối với hành vi xâm phạm danh dự, nhân phẩm, uy tín của cá nhân, Tạp chí Công thương, Hà Nội.
118. Ngân hàng Nhà nước Việt Nam (2022), Quản lý Nhà nước về hoạt động ngân hàng số - thực tiễn, kinh nghiệm quốc tế và giải pháp đối với Việt Nam, Nhiệm vụ nghiên cứu cấp Bộ, Hà Nội.
119. Bảo Ngọc (2021), An toàn, an ninh mạng: Thực hiện sứ mệnh quan trọng trong chuyển đổi số quốc gia, Tạp chí Con số và sự kiện, Hà Nội.
120. Trần Phạm Sĩ Nguyên (2023), An ninh mạng tại Việt Nam từ năm 2011 đến nay: Thực trạng và chính sách, Tạp chí Nghiên cứu Ấn Độ và châu Á, Hà Nội.
121. Nguyễn Công Minh (2021), Nhận biết và ngăn chặn hành vi đánh cắp dữ liệu, Tạp chí Ngân hàng (Chuyên đề Công nghệ và Ngân hàng số), Hà Nội.
122. Nguyễn Thị Thu Trang (2020), Đổi mới phương thức quản lý tiền tệ trong kinh tế số Việt Nam, Tạp chí Kinh tế Tài chính Việt Nam, Hà Nội.
123. Trần Tuấn Duy, Phan Trần Mai Phương (2020), Giải pháp tăng cường bảo vệ không gian mạng theo quan điểm của Đảng và pháp luật của nhà nước, Tạp chí Phát triển nhân lực, Hà Nội.
124. Nguyễn Hoàng Chi Mai (2022), Kinh nghiệm quốc tế về xử lý tội phạm công nghệ cao và một số khuyến nghị cho Việt Nam, Tạp chí Kiểm sát, Hà Nội.

125. Lê Minh Mạnh (2019), Luật An ninh mạng - Nội dung cơ bản và một số vấn đề thu hút sự quan tâm của dư luận xã hội, Tham luận tại Hội nghị an toàn thông tin mạng ngành Bảo hiểm xã hội năm 2019, Đà Nẵng.
126. Nguyễn Văn Mạnh (2010), Thực hiện pháp luật - những vấn đề lý luận và thực tiễn, Nxb Chính trị quốc gia, Hà Nội.
127. Hoàng Thành Nam (2017), Tăng cường công tác thông tin tuyên truyền phòng, ngừa, chống vi phạm trên mạng Internet, Nxb Thông tin và Truyền thông, Hà Nội.
128. Đỗ Thị Thúy Nga (2012), Các quy định của pháp luật Việt Nam về dịch vụ Internet trong thời kỳ hội nhập quốc tế, Luận văn thạc sĩ, Đại học quốc gia Hà Nội, Hà Nội.
129. Ngân hàng Nhà nước Việt Nam (2015), Thông tư 31/2015/TT-NHNN ngày 28/12/2015 của Ngân hàng Nhà nước Việt Nam quy định về bảo đảm an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng, Hà Nội.
130. Hoàng Văn Nghĩa (2019), Quản lý nhà nước về mạng xã hội: tiếp cận từ quyền và nghĩa vụ của người sử dụng mạng xã hội ở Việt Nam hiện nay, bài đăng trong sách Mạng xã hội trong bối cảnh phát triển xã hội thông tin ở Việt Nam - Lý luận và thực tiễn, Nxb Lao động, Hà Nội.
131. Lưu Thị Phấn, Hoàng Thị Kim Nhung, Lê Thị Thúy Nga (2023), Pháp luật quản lý thuế trong bối cảnh cách mạng công nghiệp 4.0 và định hướng hoàn thiện, Tạp chí Giáo dục và Xã hội, Hà Nội.
132. Nguyễn Minh Phong, Nguyễn Trần Minh Trí (2018), Luật An ninh mạng - sự cần thiết và công tác tuyên truyền tạo đồng thuận xã hội, Tạp chí Ngân hàng, Hà Nội.
133. Đinh Hữu Phí (2022), Hoàn thiện pháp luật về sở hữu trí tuệ trong bối cảnh hội nhập quốc tế (Perfecting the law on intellectual property in the context of international integration), Tạp chí Cộng sản, Hà Nội.
134. Đặng Kim Phương (2021), Hoàn thiện pháp luật thuế môi trường nhằm nâng cao hiệu quả thực hiện ở Việt Nam, Luận án Tiến sĩ, Hà Nội.

135. Phạm Long Phương (2018), Quản lý thông tin mạng Internet ở một số khu vực trên thế giới và kinh nghiệm cho Việt Nam, Tạp chí Quản lý nhà nước, Hà Nội.
136. Trần Đại Quang (2015), Không gian mạng - Tương lai và hành động, Nxb Công an nhân dân, Hà Nội.
137. Nguyễn Kim Quang, Cao Minh Thắng (2017), Nghiên cứu kinh nghiệm xây dựng chiến lược quốc gia về an toàn không gian mạng và đề xuất cho Việt Nam, Đề tài khoa học cấp Bộ, Bộ Thông tin và truyền thông, Hà Nội.
138. Hồng Quân, Hà Trung (2023), Xây dựng khung pháp lý hoàn chỉnh cho thị trường dữ liệu và các dịch vụ số, Tạp chí Pháp lý, Hà Nội.
139. Hoàng Thị Kim Quế (2015), Các yếu tố tác động đến thực hiện pháp luật của công dân ở nước ta hiện nay, Tạp chí Khoa học, Đại học Quốc gia Hà Nội.
140. Quốc hội (2004), Luật An ninh quốc gia năm 2004, Hà Nội.
141. Quốc hội (2005), Luật Sở hữu trí tuệ năm 2005 sửa đổi, bổ sung năm 2022, Hà Nội.
142. Quốc hội (2006), Luật Công nghệ thông tin năm 2006 sửa đổi, bổ sung năm 2024, Hà Nội.
143. Quốc hội (2009), Luật Tần số vô tuyến điện năm 2009 sửa đổi, bổ sung năm 2024, Hà Nội.
144. Quốc hội (2010), Luật Bưu chính năm 2010, Hà Nội.
145. Quốc hội (2011), Luật Cơ yếu năm 2011, Hà Nội.
146. Quốc hội (2012), Luật quảng cáo năm 2012, Hà Nội.
147. Quốc hội (2012), Luật Xử lý vi phạm hành chính năm 2012 sửa đổi, bổ sung năm 2023, Hà Nội.
148. Quốc hội (2013), Hiến pháp năm 2013, Hà Nội.
149. Quốc hội (2013), Luật Khoa học công nghệ năm 2013 sửa đổi, bổ sung năm 2023, Hà Nội.

150. Quốc hội (2015), Luật An toàn thông tin mạng năm 2015 sửa đổi, bổ sung năm 2018, Hà Nội.
151. Quốc hội (2015), Bộ luật Dân sự năm 2015, Hà Nội.
152. Quốc hội (2015), Bộ luật Hình sự năm 2015 sửa đổi, bổ sung năm 2017, Hà Nội.
153. Quốc hội (2018), Luật An ninh mạng năm 2018, Hà Nội.
154. Quốc hội (2018), Luật Bảo vệ bí mật nhà nước năm 2018, Hà Nội.
155. Quốc hội (2018), Luật An ninh mạng năm 2018, Hà Nội.
156. Quốc hội (2018), Luật Bí mật nhà nước năm 2018, Hà Nội.
157. Quốc hội (2018), Luật Công an nhân dân năm 2018 sửa đổi, bổ sung năm 2024, Hà Nội
158. Quốc hội (2023), Luật Bảo vệ người tiêu dùng năm 2023, Hà Nội.
159. Quốc hội (2023), Luật Giao dịch điện tử năm 2023, Hà Nội.
160. Quốc hội (2023), Luật Viễn thông năm 2023, Hà Nội.
161. Quốc hội (2024), Luật Căn cước năm 2024, Hà Nội.
162. Quốc hội (2024), Luật Dữ liệu năm 2024, Hà Nội.
163. Quốc hội (2025), Luật Ban hành văn bản quy phạm pháp luật năm 2025, Hà Nội.
164. Quốc hội (2025), Luật sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật năm 2025, Hà Nội.
165. Quốc hội (2025), Luật Bảo vệ dữ liệu cá nhân năm 2025, Hà Nội.
166. Quốc hội (2025), Luật An ninh mạng năm 2025, Hà Nội.
167. Quốc hội (2025), Luật Bảo vệ bí mật nhà nước năm 2025, Hà Nội.
168. Quốc hội (2025), Luật Trí tuệ nhân tạo năm 2025, Hà Nội.
169. Tào Thị Quyên (2016), Hoàn thiện pháp luật về thương mại điện tử ở Việt Nam hiện nay, Nhà xuất bản Tư pháp, Hà Nội.
170. Hoàng Thị Quyên (2020), Bảo vệ chủ quyền quốc gia trên không gian mạng trong thời đại công nghệ số, Tạp chí Lý luận chính trị, Hà Nội.
171. Hoàng Phê (2003), Viện Ngôn ngữ học, Từ điển Tiếng Việt, Hà Nội.

172. Đặng Thanh Sơn (2018), Hoàn thiện pháp luật về xử lý vi phạm hành chính, Nhà xuất bản Tư pháp, Hà Nội.
173. Nguyễn Ngọc Quyền (2022), Pháp luật về bảo vệ quyền lợi người tiêu dùng trong thương mại điện tử ở Việt Nam, Luận án Tiến sĩ, Trường Đại học Luật Hà Nội.
174. Lê Minh Tâm (1992), Một số vấn đề lý luận và thực tiễn xây dựng và hoàn thiện hệ thống pháp luật Việt Nam, Luận án tiến sĩ Luật học.
175. Tạ Ngọc Tấn (2013), An ninh quốc gia, những vấn đề an ninh phi truyền thống, Nxb Chính trị - Hành chính, Hà Nội.
176. Nguyễn Thị Phương Thảo (2022), Hoàn thiện pháp luật Việt Nam về góp vốn bằng quyền sở hữu trí tuệ (Improving Vietnam's regulations on the capital contribution in terms of intellectual property rights), Tạp chí Công thương, Hà Nội.
177. Lê Thị Hoài Thu (2021), Hoàn thiện pháp luật kinh doanh tại Việt Nam nhằm đáp ứng các yêu cầu của hiệp định thương mại tự do FTA thế hệ mới, Nhà xuất bản Đại học Quốc gia, Hà Nội.
178. Nguyễn Thị Xuân Thu (2022), 5G và những vấn đề an ninh bảo mật mạng (5G and network security issues), Tạp chí Khoa học & công nghệ Việt Nam, Hà Nội.
179. Nguyễn Thị Thu Thủy (2018) Pháp luật về bảo đảm an ninh thông tin ở Việt Nam và phương hướng hoàn thiện, Kỷ yếu Hội thảo: “Những vấn đề lý luận và thực tiễn về an ninh thông tin và bảo đảm an ninh thông tin ở Việt Nam hiện nay”, Học viện An ninh nhân dân, Hà Nội.
180. Bùi Thị Thanh Thúy (2019), Hoàn thiện pháp luật về quyền con người trong quản lý hành chính nhà nước, Nxb Khoa học xã hội, Hà Nội.
181. Thủ tướng Chính phủ (2019), Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Hà Nội.
182. Thủ tướng Chính phủ (2022), Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ về Chiến lược An toàn, An ninh

mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030, Hà Nội.

183. Nguyễn Thị Thuận (2020), Hoàn thiện pháp luật về an ninh mạng đáp ứng yêu cầu chuyển đổi số quốc gia, Tạp chí Nghiên cứu Lập pháp, Hà Nội.
184. Trần Doãn Tiến (2010), Phê phán các quan điểm sai trái về tư tưởng chính trị trên mạng Internet góp phần bảo vệ chế độ xã hội chủ nghĩa ở nước ta hiện nay, Luận án tiến sĩ triết học, Học viện Chính trị quốc gia Hồ Chí Minh, Hà Nội.
185. Tòa án Nhân dân tối cao, Báo cáo tổng kết công tác năm 2018, 2019, 2020, 2021, 2022, 2023, 2024, Hà Nội.
186. Lê Minh Toàn (2022), Nhận diện hành vi tội phạm mạng trong lĩnh vực tài chính tín dụng, Tạp chí Công nghệ thông tin và truyền thông, Hà Nội
187. Trung tâm từ điển học (2010), Từ điển tiếng Việt 2010, Nxb Đà Nẵng, Hà Nội.
188. Vũ Văn Tư, (2023), Trách nhiệm hình sự của pháp nhân thương mại trong Luật Hình sự Việt Nam, Luận án Tiến sĩ, Học viện Khoa học xã hội Việt Nam.
189. Nguyễn Thị Thu Trang (2020), Đổi mới phương thức quản lý tiền tệ trong kinh tế số Việt Nam; Tạp chí Kinh tế Tài chính Việt Nam, Hà Nội.
190. Nguyễn Thị Thu Trang (2022), Bảo vệ dữ liệu cá nhân trong kỷ nguyên trí tuệ nhân tạo - Kinh nghiệm của châu Âu và kiến nghị hoàn thiện pháp luật Việt Nam (Personal data protection in the AI age - European experience and recommendations to improve the law of Vietnam), Tạp chí Luật học, Hà Nội.
191. Lâm Tô Trang (2023), Bảo đảm tính thống nhất của khái niệm quyền tài sản trong Bộ luật Dân sự và Luật Sở hữu trí tuệ Việt Nam hiện hành (Ensuring consistency of the right to property in the Civil Code and the existing Law on intellectual property rights), Tạp chí Nghề luật, Hà Nội.
192. Nguyễn Phú Trọng (2023), Một số vấn đề lý luận và thực tiễn về chủ nghĩa xã hội và con đường đi lên chủ nghĩa xã hội ở Việt Nam, Nxb Chính trị Quốc gia Sự thật, Hà Nội.

193. Đàm Trọng Tùng (2016), Bảo vệ độc lập dân tộc của Việt Nam trước mối đe dọa an ninh phi truyền thống từ năm 2001 đến năm 2015, Luận án tiến sĩ, Học viện Chính trị quốc gia Hồ Chí Minh, Hà Nội.
194. Trần Ngọc Tuấn (2022), Những ảnh hưởng của quảng cáo hành vi trực tuyến đến người tiêu dùng và một số kiến nghị, Tạp chí Nghiên cứu lập pháp, Hà Nội.
195. Nguyễn Văn Ty (2019), Nâng cao ý thức làm chủ và bảo vệ không gian mạng của cán bộ, đảng viên và nhân dân, Tạp chí Cộng sản, Hà Nội.
196. Viện Khoa học pháp lý (2006), Từ điển luật học, Nxb Từ điển Bách khoa và Nxb Tư pháp, Hà Nội.
197. Viện Khoa học pháp lý (2019), Kế hoạch ứng phó cuộc Cách mạng công nghiệp lần thứ tư của Hàn Quốc, tại Hội thảo khoa học quốc gia Cách mạng công nghiệp lần thứ Tư và những vấn đề pháp lý đặt ra cho việc xây dựng, hoàn thiện hệ thống pháp luật Việt Nam, Hà Nội.
198. Viện Kiểm sát nhân dân tối cao (2020), Báo cáo tổng kết công tác năm 2018, 2019, 2020, 2021, 2022, 2023, 2024, Hà Nội.
199. Viện Nhà nước và Pháp luật (2004), Giáo trình Lý luận chung về Nhà nước và pháp luật, Nxb Lý luận chính trị, Hà Nội.
200. Trịnh Tiến Việt (2019), Pháp luật hình sự Việt Nam trước thách thức an ninh phi truyền thống, Nxb Chính trị quốc gia Sự thật, Hà Nội.
201. Võ Khánh Vinh (2022), Chiến lược phát triển pháp luật Việt Nam đến năm 2030, tầm nhìn đến năm 2045: Những vấn đề lý luận và thực tiễn, Nxb Chính trị quốc gia Sự thật, Hà Nội.
202. Nguyễn Như Ý (1999), Đại từ điển Tiếng Việt, Nxb Văn hóa thông tin, Thành phố Hồ Chí Minh.
203. Hoàng Yến (2022), Chuyển biến nhận thức về an ninh mạng trong đại dịch Covid-19 của các doanh nghiệp vừa và nhỏ, Tạp chí Công nghệ thông tin và truyền thông, Hà Nội.

**Tài liệu tham khảo nước ngoài:**

204. A. Appazov, Legal Aspects of Cybersecurity, 2014
205. Asif H. Qureshi, Li Zhuangxu, Cecilia J. Flores Elizondo (2021), “Reforming Legal Systems: Global Perspectives”
206. Asif H. Qureshi (2024), Law Reforms Around the World: Perspectives from National and International Law, Routledge Press.
207. Adam Segal (2018), When China rule the web: Technology in service of the state, Foreign Affairs 97(5), p.10.
208. Anthony Reyes, Richard Britton, Kevin O’Shea, Jim Steel (2011), Crime investigation: bridging the gaps between security professional, law enforcement and prosecutors Syngress Press, Australia.
209. Barry Buzan, Ole Wæver, Jaap de Wilde Security (1998), A New Framework for Analysis, Boulder, CO: Lynne Rienner.
210. Bộ Đại học và Trung học chuyên nghiệp Liên Xô (1984), Lý luận về Nhà nước và pháp luật, (tái bản lần thứ 2 có bổ sung), Nxb Sách pháp lý, Mátxcova.
211. Ben Buchanan (2017), The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations, Oxford University Press.
212. Cộng hòa liên bang Đức (2015), Luật An ninh mạng, Berlin.
213. Cộng hòa nhân dân Trung Hoa (2017), Luật An ninh mạng, Bắc Kinh.
214. C.L. Montesquieu (1996), Tinh thần pháp luật, Nxb Giáo dục, Hà Nội.
215. Daniel J. Solove (2008), Understanding Privacy, Harvard university press.
216. Daniel Leslie Scherr, Cybersecurity Policy Development at the State Level: A Case Study of Middle Tennessee, Walden University, 2019.
217. Nguyen Huu Phuoc Dai, European (Visegrád countries) Cyber-security in Applying for Asian Countries: The Case of Vietnam, Óbuda University, 2019
218. Dorothea Czarnecki (2016), Báo cáo đánh giá năng lực bảo vệ trẻ em trên môi trường mạng tại Việt Nam, Bộ Lao động, Thương binh và Xã hội, UNICEF, Hà Nội.

219. Edward Wilding (2018), Information risk and security: preventing and investigating workplace computer crime, Routledge/Taylor & Francis.
220. Eric D. Knapp (2011), Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.
221. Edward Wilding (2006), Information risk and security: preventing and investigating workplace computer crime, Gower Publishing Press, Ltd.
222. Google, Temasek và Bain (2024), Báo cáo kinh tế số ASEAN 2024, tài liệu báo cáo thường niên.
223. Georg Sven Lampe, Research on Information Security in Business Processes Related to Global Risks, Luận án tiến sĩ, Bucharest University of Economic Studies, 2024
224. Hellenic republic ministry of digital governance National Cybersecurity Strategy, “National cybersecurity strategy 2020 - 2025”, [https://mindigital.gr/wp-content/uploads/2022/11/e%ce%9d-national-cyber-security-strategy-2020\\_2025.pdf](https://mindigital.gr/wp-content/uploads/2022/11/e%ce%9d-national-cyber-security-strategy-2020_2025.pdf)
225. ITU (2015), Global Cybersecurity Challenges - Collaborating for effective enhancement of cybersecurity in developing countries, ITU Cybersecurity Workshop, Geneva, Switzerland, September 2015.
226. Jack Goldsmith, Tim Wu (2007), Who Controls the Internet? Illusions of a Borderless World. International Journal of Communication.
227. Jian Jiang, Vulnerabilities, Cybersecurity, and the Role of Law and Regulation, Erasmus University Rotterdam, 2021
228. Julien Nocetti (2019), Geopolitique de la Cyber - conflictualite.
229. Julien Nocetti (2018), Geopolitique de la Cyber- conflictualite, Politique etrangere, 2018/2 Ete, pp.15-27.
230. Joanna Lyn Grama (2022), Legal and Privacy Issues in Information Security, Jones & Bartlett Learning.
231. Kaushik, s. & Wang, Y. (2018), Data privacy: Demystifying the GDPR, [https://ischool.syr.edu/truy data-privacy-demystifying-gdpr/](https://ischool.syr.edu/truy-data-privacy-demystifying-gdpr/), 22/7/2024.

232. Kevin Mitnick (2019), *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*, Back Bay Books.
233. Lawrence Lessig (1999), *Code and Other Laws of Cyberspace*, Basic Books.
234. Lee Brotherston và Amanda Berlin (2017), *Defensive Security Handbook: Best Practices for Securing Infrastructure*, Defensive Security Handbook.
235. Lee A. Bygrave, *The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes*, *Computer Law & Security Review*, 2024/2025
236. Liên bang Nga (2016), *Học thuyết An ninh thông tin Liên bang Nga*, Mátxcova.
237. Liên bang Nga (2018), *Bộ luật Hình sự Liên bang Nga số 63-FZ ngày 13/6/1996, được sửa đổi, bổ sung ngày 27/12/2018*, Matxcova.
238. Liên minh Châu Âu (2001), *Công ước Budapest về tội phạm mạng*.
239. Li, H. & Yu, L. & He, w. (2019), *The Impact of GDPR on Global Technology Development*, *Journal of Global Information Technology Management*, Vol. 22(1), p. 1.
240. Marie-Helen Maras (2011), *Computer forensics: cybercriminal, laws and evidence*, Jones & Bartlett Publishers Press.
241. Martin Hilbert and Priscila López (2011), *The World's Technological Capacity to Store, Communicate, and Compute Information*, *Science*, 332(6025), pp. 60-65.
242. Marie-Helen Maras (2014), *Computer forensics: cybercriminal, laws and evidence*, Ph.D. Published by Jones & Bartlett Learning.
243. Michael Pittaro (2021), *Global Perspectives on Reforming the Criminal Justice System*.
244. Mireille Hildebrandt (2015), *Smart Technologies and the End(s) of Law*, Edward Elgar Publishing.

245. Nandan Nilekani (2018), Data to the People: India's inclusive Internet, Foreign Affairs, 97 (5), p.19.
246. Nhật Bản (2014), Đạo luật số 104 về an ninh mạng của Nhật Bản, Tokyo.
247. The World Book Encyclopedia 2016
248. Osula A. M. & Kaska K. (2013), National Cyber Security Strategy Guidelines, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.
249. Peter Townsendp (2017), The dark side of technology (Mặt trái của công nghệ).
250. Peter Townsendp (2018), Mặt trái của công nghệ, Nxb Chính trị quốc gia - Sự thật, Hà Nội.
251. Philip C. Aka và Joseph Abiodun Balogun (2022), Improving Disability Laws under Nigeria's Fourth Republic: Ten Measured Steps into the Future, Lexington Books.
252. Primavera De Filippi (2018), Blockchain and the Law: The Rule of Code, Harvard University Press.
253. Pomaza-Ponomarenko, Leonenko (2023), Legal Reform and Change: Research on Legal Reform Processes and Their Impact on Society, Journal of Law and Sustainable Development.
254. Richard A. Spinello (2020), Cyberethics: Morality and Law in Cyberspace: Morality and Law in Cyberspace, Jones & Bartlett Learning.
255. Uchenna Jerome Orji, Cybersecurity Law and Regulation, Wolf Legal Publishers, 2012
256. Ulrich Beck (1992), Risk Society: Towards a New Modernity,, SAGE Publications.
257. Stuart McClure, Joel Scambray, George Kurtz (2012), Hacking Exposed 7: Network Security Secrets and Solutions, McGraw Hill
258. Tim Lindsey (2004), Law Reform in Developing and Transitional States, Melbourne, Routledge.

259. Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried Spellar (2022), Cybercrime and Digital Forensics: An Introduction, Routledge
260. Technology (2008), Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America, Open Technology Institute - New America Foundation.
261. William Gauvin (2013), Applied Cyber and Network Security Labs, Amazon Digital Services LLC.

### **Trang Web**

262. <https://www.dataguidance.com/news/singaporecybersecurityamendment-bill-passed> 21h30 phút ngày 21/9/2024
263. <https://nhandan.vn/viet-nam-phai-doi-mat-voi-khoang-552000-cuoc-tan-cong-mang-trong-nam-2025-post936719.html> ngày 24/5/2026
264. <https://viettelsecurity.com/vi/resource-report/bao-cao-tinh-hinh-nguy-co-at-tt-tai-viet-nam-nam-2025/> ngày 24/5/2026
265. <https://www.xuanzhou.gov.cn/OpennessContent/show/2977729.html>
266. <https://dhannd.edu.vn/chu-quyen-quoc-gia-tren-khong-gian-mang-nhung-yeu-cau-dam-bao-cac-chi-so-an-ninh-an-toan-trong-boi-can-hien-nay-a-1503>
267. Council of Europe, Convention on Cybercrime, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

## PHỤ LỤC

### Phụ lục 1: DANH MỤC VĂN BẢN QUY PHẠM PHÁP LUẬT TRONG LĨNH VỰC AN NINH MẠNG TRƯỚC THỜI ĐIỂM BAN HÀNH LUẬT AN NINH MẠNG 2025

| STT              | THỜI GIAN  | NỘI DUNG                                                                                                                                                                                            |
|------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LUẬT</b>      |            |                                                                                                                                                                                                     |
| 1                | 19/11/2015 | Luật an toàn thông tin mạng                                                                                                                                                                         |
| 2                | 12/6/2018  | Luật An ninh mạng                                                                                                                                                                                   |
| <b>NGHỊ ĐỊNH</b> |            |                                                                                                                                                                                                     |
| 1                | 15/7/2013  | Nghị định số 72/2013/NĐ-CP về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng                                                                                                    |
| 1                | 01/7/2016  | Nghị định số 108/2016/NĐ-CP quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng                                                                                         |
| 2                | 01/7/2016  | Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ                                                                                                                        |
| 3                | 01/7/2016  | Nghị định số 58/2016/NĐ-CP quy định chi tiết về kinh doanh sản phẩm, dịch vụ mật mã dân sự và xuất khẩu, nhập khẩu sản phẩm mật mã dân sự                                                           |
| 4                | 01/7/2016  | Nghị định số 101/2016/NĐ-CP quy định chi tiết trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng không gian mạng để khủng bố.                                                       |
| 5                | 14/10/2016 | Nghị định số 142/2016/NĐ-CP về ngăn chặn xung đột thông tin trên mạng                                                                                                                               |
| 6                | 01/3/2018  | Nghị định số 27/2018/NĐ-CP sửa đổi, bổ sung một số Điều của Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng |
| 7                | 27/9/2018  | Nghị định số 130/2018/NĐ-CP quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số                                                                          |
| 8                | 27/12/2019 | Nghị định số 04/2019/NĐ-CP Quy định chi tiết trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng (Mật)                                                                                   |
| 9                | 03/02/2020 | Nghị định số 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử                                 |
| 10               | 14/8/2020  | Nghị định số 91/2020/NĐ-CP chống tin nhắn rác, thư điện tử rác, cuộc gọi rác                                                                                                                        |
| 11               | 15/8/2022  | Nghị định số 53/2022/NĐ-CP quy định chi tiết một số điều của Luật An ninh mạng                                                                                                                      |
| <b>THÔNG TƯ</b>  |            |                                                                                                                                                                                                     |
| 1                | 14/11/2016 | Thông tư số 269/2016/TT-BTC của Bộ Tài Chính quy định chế độ thu, nộp, quản lý và sử dụng phí và lệ phí thuộc lĩnh vực an toàn thông tin                                                            |

|                   |            |                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                 | 12/9/2017  | Thông tư số 19/2017/TT-BTTTT của Bộ Thông tin và Truyền thông quy định công tác bảo vệ bí mật nhà nước trong ngành thông tin và truyền thông                                                                                                                                                                                   |
| 2                 | 12/9/2017  | Thông tư số 20/2017/TT-BTTTT của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc                                                                                                                                                                                       |
| 3                 | 20/10/2017 | Thông tư số 27/2017/TT-BTTTT của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, nhà nước                                                                                                                 |
| 4                 | 15/11/2017 | Thông tư số 31/2017/TT-BTTTT của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin                                                                                                                                                                                                           |
| 5                 | 15/10/2018 | Thông tư số 13/2018/TT-BTTTT của Bộ Thông tin và Truyền thông quy định về danh mục sản phẩm an toàn thông tin mạng nhập khẩu theo giấy phép và trình tự, thủ tục, hồ sơ cấp Giấy phép nhập khẩu sản phẩm an toàn thông tin mạng                                                                                                |
| 6                 | 12/12/2018 | Thông tư số 121/2018/TT-BTC của Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng                                                                                                                                              |
| 7                 | 5/9/2019   | Thông tư số 12/2019/TT-BTTTT của Bộ Thông tin và Truyền thông về việc sửa đổi, bổ sung một số điều của Thông tư 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng                  |
| 8                 | 11/11/2021 | Thông tư số 95/2021/TT-BTC của Bộ Tài chính quy định việc lập dự toán, quản lý sử dụng và quyết toán kinh phí thực hiện Đề án “Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021-2025”                                                                                                                     |
| 9                 | 20/7/2022  | Thông tư số 10/2022/TT-BTTTT sửa đổi, bổ sung một số điều của Thông tư số 13/2018/TT-BTTTT ngày 15 tháng 10 năm 2018 của Bộ trưởng Bộ Thông tin và Truyền thông quy định Danh mục sản phẩm an toàn thông tin mạng nhập khẩu theo giấy phép và trình tự, thủ tục, hồ sơ cấp Giấy phép nhập khẩu sản phẩm an toàn thông tin mạng |
| 10                | 12/8/2022  | Thông tư số 12/2022/TT-BTTTT quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ                                                                                                                                              |
| <b>QUYẾT ĐỊNH</b> |            |                                                                                                                                                                                                                                                                                                                                |
| 1                 | 16/3/2017  | Quyết định số 05/2017/QĐ-TTg Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia                                                                                                                                                                                                  |
| 2                 | 12/3/2018  | Quyết định số 02/2018/QĐ-TTg về việc thí điểm một số chế độ ưu đãi và cơ chế tài chính đặc thù cho cán bộ kỹ thuật và lực lượng ứng cứu sự cố an toàn thông tin mạng của Bộ Thông tin và Truyền thông                                                                                                                          |

|                                                  |                |                                                                                                                                         |                                                                                                                                                                                                                                               |
|--------------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3                                                | 15/5/2020      | Quyết định số 02/2020/QĐ-TTg về việc kéo dài thời hạn thí điểm thực hiện Quyết định số 02/2018/QĐ-TTg                                   |                                                                                                                                                                                                                                               |
| 4                                                | 17/3/2021      | Quyết định số 11/2021/QĐ-TTg về việc kéo dài thời hạn thực hiện cơ chế tài chính đặc thù của một số cơ quan, đơn vị hành chính nhà nước |                                                                                                                                                                                                                                               |
| VĂN BẢN CHỈ ĐẠO, ĐIỀU HÀNH LĨNH VỰC AN NINH MẠNG |                |                                                                                                                                         |                                                                                                                                                                                                                                               |
| STT                                              | Số hiệu        | Ngày ban hành                                                                                                                           | Trích yếu nội dung                                                                                                                                                                                                                            |
| 1                                                | 63/2010/QĐ-TTg | 13/01/2010                                                                                                                              | Về phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020                                                                                                                                                                  |
| 1                                                | 897/CT-TTg     | 10/6/2011                                                                                                                               | Chỉ thị của Thủ tướng Chính phủ Về tăng cường các hoạt động bảo đảm an toàn thông tin số                                                                                                                                                      |
| 2                                                | 82/CT-BTTTT    | 24/12/2014                                                                                                                              | Chỉ thị của Bộ trưởng Bộ Thông tin và Truyền thông về ngăn chặn tin nhắn rác, tin nhắn lừa đảo và tăng cường quản lý thông tin trên mạng                                                                                                      |
| 3                                                | 11/CT-BTTTT    | 18/3/2016                                                                                                                               | Chỉ thị của Bộ trưởng Bộ Thông tin và Truyền thông về tăng cường bảo vệ bí mật thông tin cá nhân của người sử dụng dịch vụ và ngăn chặn việc mua bán, lưu thông SIM di động sai quy định                                                      |
| 4                                                | 898/QĐ-TTg     | 27/5/2016                                                                                                                               | Quyết định của Thủ tướng Chính phủ phê duyệt Phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020                                                                                                            |
| 5                                                | 632/QĐ-TTg     | 10/5/2017                                                                                                                               | Quyết định của Thủ tướng Chính phủ ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia                                                                                 |
| 6                                                | 1622/QĐ-TTg    | 25/10/2017                                                                                                                              | Quyết định của Thủ tướng Chính phủ phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025 |
| 7                                                | 14/CT-TTg      | 25/05/2018                                                                                                                              | Chỉ thị của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại                                                                                                                                                       |
| 8                                                | 29-NQ/TW       | 25/7/2018                                                                                                                               | Nghị quyết của Bộ Chính trị về Chiến lược bảo vệ Tổ quốc trên không gian mạng (Mật)                                                                                                                                                           |
| 9                                                | 30-NQ/CP       | 25/7/2018                                                                                                                               | Nghị quyết của Bộ Chính trị về Chiến lược An ninh mạng quốc gia (Mật)                                                                                                                                                                         |
| 10                                               | 1017/QĐ-TTg    | 14/8/2018                                                                                                                               | Quyết định của Thủ tướng Chính phủ Phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến 2025                                                  |

|    |             |            |                                                                                                                                                                                             |
|----|-------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11 | 04/CT-BTTTT | 11/01/2019 | Chỉ thị của Bộ trưởng Bộ Thông tin và Truyền thông về tăng cường phòng chống mã độc và bảo vệ thông tin cá nhân trên môi trường mạng                                                        |
| 12 | 14/CT-TTg   | 07/6/2019  | Chỉ thị của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam                                                                |
| 13 | 22/NQ-CP    | 18/10/2019 | Nghị quyết của Chính phủ Ban hành Chương trình hành động của Chính phủ thực hiện Nghị quyết số 30-NQ/TW ngày 25 tháng 7 năm 2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia (Mật) |
| 14 | 41-CT/TW    | 24/3/2020  | Chỉ thị của Ban Bí thư về tăng cường phối hợp và triển khai đồng bộ các biện pháp bảo đảm an toàn, an ninh mạng (Mật)                                                                       |
| 15 | 70/QĐ-TTg   | 29/7/2020  | Quyết định của Thủ tướng Chính phủ về việc thành lập Ban chỉ đạo An toàn, an ninh mạng quốc gia (Mật)                                                                                       |
| 16 | 1907/QĐ-TTg | 23/11/2020 | Quyết định của Thủ tướng Chính phủ phê duyệt Đề án “Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025”                                      |
| 17 | 21/QĐ-TTg   | 06/01/2021 | Quyết định của Thủ tướng Chính phủ Phê duyệt Đề án “Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025”                                                           |
| 18 | 01/CT-TTg   | 18/2/2021  | Chỉ thị của Thủ tướng Chính phủ Về việc tăng cường công tác bảo vệ an ninh mạng trong tình hình hiện nay                                                                                    |
| 19 | 830/QĐ-TTg  | 01/06/2021 | Quyết định của Thủ tướng Chính phủ phê duyệt Chương trình “Bảo vệ và hỗ trợ trẻ em tương tác lành mạnh, sáng tạo trên môi trường mạng giai đoạn 2021 - 2025”                                |
| 20 | 49/CT-BTTTT | 18/8/2021  | Chỉ thị của Bộ trưởng Bộ Thông tin và Truyền thông về thúc đẩy phát triển và sử dụng nền tảng số an toàn, lành mạnh                                                                         |
| 21 | 60/CT-BTTTT | 16/9/2021  | Chỉ thị của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai Diễn tập Thực chiến bảo đảm an toàn thông tin mạng                                                            |
| 22 | 49/QĐ-TTg   | 15/7/2022  | Quyết định của Thủ tướng Chính phủ phê duyệt Đề án “Đào tạo và phát triển nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030”                                                  |
| 23 | 964/QĐ-TTg  | 10/8/2022  | Quyết định của Thủ tướng Chính phủ Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030                  |
| 24 | 18/CT-TTg   | 13/10/2022 | Chỉ thị số 18/CT-TTg của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam                                                             |

| 25                                             | 23/CT-TTg          | 26/12/2022    | Chỉ thị của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát                   |
|------------------------------------------------|--------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26                                             | 09/CT-TTg          | 23/02/2024    | Về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ                                                             |
| 27                                             | 33/CĐ-TTg          | 07/4/2024     | Về tăng cường bảo đảm an toàn thông tin mạng                                                                                                            |
| <b>VĂN BẢN HƯỚNG DẪN LĨNH VỰC AN NINH MẠNG</b> |                    |               |                                                                                                                                                         |
| STT                                            | Số hiệu            | Ngày ban hành | Trích yếu nội dung                                                                                                                                      |
| 1                                              | 430/BTTTT-CATTT    | 09/02/2015    | V/v hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước                                                          |
| 1                                              | 2290/BTTTT-CATTT   | 17/7/2018     | V/v hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật                                                                           |
| 2                                              | 1694/BTTTT-CATTT   | 31/5/2019     | Hướng dẫn yêu cầu an toàn thông tin cơ bản đối với hệ thống thông tin kết nối vào mạng TSLCD                                                            |
| 3                                              | 3001/BTTTT-CATTT   | 06/9/2019     | V/v Hướng dẫn bảo đảm an toàn thông tin cho hệ thống quản lý văn bản và điều hành                                                                       |
| 4                                              | 2973/BTTTT-CATTT   | 04/9/2019     | V/v hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước                                                           |
| 5                                              | 2612/BTTTT-CATTT   | 17/7/2021     | V/v bổ sung bộ tiêu chí, chỉ tiêu để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử            |
| 6                                              | 1145/BTTTT-CATTT   | 03/04/2020    | V/v hướng dẫn bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử |
| 7                                              | 4258/BTTTT-CATTT   | 26/10/2021    | V/v hướng dẫn tổ chức, hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng                                                                           |
| 8                                              | 5179/BTTTT-CATTT   | 19/10/2022    | V/v đơn đốc hoàn thành phân loại, xác định và phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin                                                 |
| 9                                              | 1439/QĐ-BTTTT      | 26/7/2022     | Ban hành quy trình hướng dẫn thực hiện diễn tập thực chiến                                                                                              |
| 10                                             | 713/CATTT-TĐQLGS   | 25/7/2019     | V/v hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ                                                                                |
| 11                                             | 235/CATTT-ATHTTT   | 08/4/2020     | V/v Hướng dẫn mô hình bảo đảm an toàn thông tin cấp bộ, tỉnh                                                                                            |
| 12                                             | 486/CATTT-ATHTTT   | 19/6/2020     | V/v Hướng dẫn bảo đảm an toàn thông tin cho Trung tâm dữ liệu phục vụ Chính phủ điện tử.                                                                |
| 13                                             | 247/CATTT-ATHTTT   | 26/3/2021     | V/v đơn đốc xác định cấp độ an toàn hệ thống thông tin và ban hành tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ 1, 2 và 3        |
| 14                                             | 793/CATTT-VNCERTCC | 25/6/2021     | Vv hướng dẫn quy trình ứng cứu, xử lý sự cố tấn công mạng                                                                                               |

|    |                  |            |                                                                                                                        |
|----|------------------|------------|------------------------------------------------------------------------------------------------------------------------|
| 15 | 166/CATTT-ATHTTT | 10/02/2022 | V/v ban hành hướng dẫn “Khung phát triển phần mềm an toàn (phiên bản 1.0)”                                             |
| 16 | 01/HD-CATTT      | 24/2/2022  | Hướng dẫn Thực hiện hoạt động diễn tập thực chiến                                                                      |
| 17 | 964/BTTTT-CATTT  | 16/3/2022  | V/v hướng dẫn áp dụng tiêu chuẩn an toàn thông tin cho các cơ quan nhà nước và hệ thống thông tin quan trọng quốc gia. |
| 18 | 1598/BTTTT-CATTT | 28/4/2022  | V/v tăng cường bảo đảm an toàn thông tin theo cấp độ và nâng cao năng lực bảo đảm an toàn thông tin theo mô hình 4 lớp |
| 19 | 5099/BTTTT-CATTT | 06/10/2023 | Hướng dẫn phát triển Đội ứng cứu sự cố cho một số lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng       |
| 20 | 1552/BTTTT-THH   | 24/4/2022  | Về việc hướng dẫn triển khai Đề án 06 (phiên bản 1.0)                                                                  |
| 21 | 708/BTTTT-CATTT  | 02/03/2024 | Về sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH                                  |

## Phụ lục 2: DANH MỤC NHỮNG THUẬT NGỮ THƯỜNG GẶP TRONG PHÁP LUẬT VỀ AN NINH MẠNG

| 1.1. Cyberspace: Không gian mạng |                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hướng dẫn Tallinn                | The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks.<br><i>Source: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013</i>                                                                                                                                             | Môi trường hình thành bởi các thành phần vật lý và phi vật lý, có đặc điểm là sử dụng máy tính và phổ điện từ để lưu trữ, sửa và trao đổi dữ liệu sử dụng các mạng máy tính.<br><i>Nguồn: Hướng dẫn Tallinn về Luật quốc tế áp dụng đối với Chiến tranh mạng - 2013</i>                                                                                                                                         |
| Australia                        | Cyberspace is a term used generally to describe the different experiences available and generated via the global online world of computer networks. For example, one might describe sending an email to their friend as sending it ‘through cyberspace’.<br><i>Source: Australian Communications and Media Authority, Cybersmart Glossary</i>                                                                                             | Không gian mạng là thuật ngữ thường được sử dụng để chỉ các trải nghiệm khác nhau trên thế giới trực tuyến toàn cầu của các mạng máy tính. VD: một người có thể mô tả việc gửi một bức thư điện tử cho bạn bè của họ là gửi thư “qua không gian mạng”<br><i>Nguồn: Cơ quan Thông tin và Truyền thông Australia, Thuật ngữ mạng</i>                                                                              |
| Canada                           | Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.<br><i>Source: Canada’s Cyber Security Strategy (2010)</i>                                                                                                                | Không gian mạng là thế giới điện tử được tạo ra bởi các mạng công nghệ thông tin kết nối với nhau và thông tin lưu trữ trên các mạng này. Đó là địa điểm chung với trên 1.7 tỷ người kết nối nhằm trao đổi ý tưởng, dịch vụ và tình bạn.<br><i>Nguồn: Chiến lược An ninh mạng Canada (2010)</i>                                                                                                                 |
| Vương quốc Anh                   | An informal word first thought to have been used by novelist William Gibson to refer to the total data on all computers on all the networks in the world. The word has passed into common use as a way of referring to any large collection of network-accessible computer-based data.<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2008</i> | Là một từ không chính thức được tiêu thuyết gia William Gibson sử dụng để nói về tổng dữ liệu trên toàn bộ các hệ thống mạng trên thế giới. “Không gian mạng” đã được sử dụng thông dụng để chỉ bất kỳ tập hợp số lượng lớn dữ liệu máy tính có thể truy cập qua mạng.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2008</i> |
| Nga                              | Translation: A sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form human activity on them                                                                                                                                                                        | Phạm vi của hoạt động trong không gian thông tin, được hình thành bởi một loạt các kênh truyền dữ liệu của Internet và các mạng viễn thông khác, hạ tầng công nghệ nhằm bảo đảm chức năng của chúng và mọi hoạt động của con người trên đó (cá nhân, tổ chức, quốc gia).                                                                                                                                        |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | (individual, organizational, state).<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2014</i>                                                                                                                                                                                                                                                                                                                        | <i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2014</i>                                                                                                                                                                                                                                                                                                                                                                              |
| Nhật Bản                                | Cyberspace, a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities.<br><br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2013</i>                                                                                                                                                                        | Không gian mạng, lĩnh vực mạng bao gồm các hệ thống thông tin, mạng viễn thông và các hệ thống khác, cung cấp nền tảng cho các hoạt động quân sự, kinh tế, xã hội và các hoạt động khác.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2013</i>                                                                                                                                                                                  |
| Mỹ                                      | National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.<br><i>Source: Cyberspace Policy Review 2009</i> | Chỉ thị Tổng thống về an ninh quốc gia số 54/Chỉ thị Tổng thống về an ninh nội địa số 23 (NSPD-54/HSPD23) định nghĩa không gian mạng là hệ thống mạng phụ thuộc lẫn nhau của các hạ tầng công nghệ thông tin bao gồm: Internet, mạng viễn thông, hệ thống máy tính, bộ xử lý nhúng và các bộ điều khiển tại các ngành công nghiệp quan trọng. Thuật ngữ này cũng thường được dùng để chỉ môi trường thông tin ảo và tương tác giữa con người với con người.<br><i>Nguồn: Đánh giá Chính sách an ninh mạng 2009</i> |
| <b>1.2. Cybersecurity: An ninh mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Mỹ                                      | The ability to protect or defend the use of cyberspace from cyber attacks.<br><i>Source: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Department of Commerce, NISTIR 7298, Revision 2, - 2010</i>                                                                                                                                                                                                                                      | Khả năng bảo vệ hoặc phòng thủ việc sử dụng không gian mạng chống lại tấn công mạng<br><i>Nguồn: Chú giải các thuật ngữ an ninh mạng quan trọng, eds. Richard Kissel, Viện Tiêu chuẩn và Công nghệ quốc gia, Bộ Thương mại Mỹ, NISTIR 7298, Revision 2 - 2010</i>                                                                                                                                                                                                                                                  |
| Nga                                     | Translation: A set of conditions under which all components of cyberspace are protected from the maximum number of threats and impacts with undesirable consequences.<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2014</i>                                                                                                                                                                                       | Một tập hợp các điều kiện trong đó toàn bộ các thành phần của không gian mạng được bảo vệ trước số lượng tối đa các mối đe dọa và tác động với các hậu quả không mong muốn.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2014</i>                                                                                                                                                                                               |
| EU                                      | Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military                                                                                                                                                                                                                                                                                                                                                                   | An ninh mạng thường liên quan đến việc bảo vệ và các hành động có thể được sử dụng nhằm bảo vệ lĩnh vực mạng, cả quân sự và dân sự,                                                                                                                                                                                                                                                                                                                                                                                |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | <p>fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2013</i></p>                                                  | <p>chống lại các mối đe dọa kèm theo hoặc các mối đe dọa có thể gây thiệt hại cho hạ tầng thông tin và các hệ thống mạng phụ thuộc lẫn nhau. An ninh mạng bảo vệ tính sẵn có, toàn vẹn của hệ thống mạng và hạ tầng, tính bí mật của thông tin trên đó.</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2013</i></p>                                                                                                                   |
| Pháp                                       | <p>The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyber defence.</p> <p><i>Source: Information Systems and Defence - France's Strategy (2011)</i></p> | <p>Tình trạng mong muốn của một hệ thống thông tin mà trong đó nó có thể kháng cự các sự kiện trên không gian mạng nhằm tấn công tính sẵn có, toàn vẹn hoặc bí mật của dữ liệu được lưu trữ, xử lý hoặc truyền đưa và của các dịch vụ liên quan do các hệ thống này cung cấp hoặc cho phép truy cập. An ninh mạng sử dụng các kỹ thuật an ninh hệ thống thông tin và dựa trên cơ sở chống tội phạm mạng và thiết lập phòng thủ mạng.</p> <p><i>Nguồn: Hệ thống thông tin và Phòng thủ - Chiến lược của Pháp (2011)</i></p> |
| Từ điển Oxford                             | <p>[Cybersecurity] The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.</p>                                                                                                                                                                                                                                                                                                                                                           | <p>An ninh mạng là tình trạng được bảo vệ chống lại hoạt động tội phạm sử dụng hoặc việc sử dụng trái phép dữ liệu điện tử hoặc các biện pháp nhằm đạt được điều này.</p>                                                                                                                                                                                                                                                                                                                                                  |
| <b>1.3. Cyberwarfare: Chiến tranh mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Bi                                         | <p>(Translation) usage of cybercapacity of a sufficient scale, during a determined period in high speed, to reach certain objectives in or through cyberspace, these actions being considered as a menace for the targeted state.</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2012</i></p>                                                                                                                      | <p>Việc sử dụng các năng lực không gian mạng ở quy mô vừa đủ trong một thời gian nhất định với tốc độ cao nhằm đạt được mục đích hoặc tác động nhất định trên không gian mạng; hành động này được coi là mối đe dọa đối với lợi ích quốc gia.</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2012</i></p>                                                                                                                             |
| Áo                                         | <p>Cyber war refers to acts of war in and around virtual space with means which are predominantly associated with information technology. In a broader sense, this implies the support of military campaigns in traditional operational spaces - i.e. ground, sea, air and outer space - through measures taken in the virtual space. In general,</p>                                                                                                                                                             | <p>Chiến tranh mạng là hành động chiến tranh trên không gian ảo với các phương tiện chủ yếu liên quan đến công nghệ thông tin. Ở khía cạnh rộng hơn, điều này muốn đề cập đến việc hỗ trợ các chiến dịch quân sự trên các không gian truyền thống: trên bộ, trên biển, trên không và không gian vũ trụ - thông qua các biện pháp trên không gian mạng. Nói</p>                                                                                                                                                             |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | the term also refers to high-tech warfare in the information age based on the extensive computerisation, electronisation and networking of almost all military sectors and issues.<br><br><i>Source: Austrian Cyber Security Strategy (2013)</i>                                                                                                                                                                                                                                                                                    | chung, thuật ngữ còn đề cập đến chiến tranh công nghệ cao trong thời đại thông tin trên cơ sở vi tính hóa, điện tử hóa và sự kết nối sâu rộng hầu hết các vấn đề và lĩnh vực quân sự.<br><i>Nguồn: Chiến lược An ninh mạng Áo(2013)</i>                                                                                                                                                                                                                                                                            |
| Từ điển Oxford                             | [Cyberwar] The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of communication systems by another state or organization.                                                                                                                                                                                                                                                                                                                                      | Việc sử dụng công nghệ máy tính để làm gián đoạn hoạt động của một quốc gia hoặc tổ chức, đặc biệt là việc tấn công có chủ đích các hệ thống truyền dữ liệu do một quốc gia hoặc tổ chức khác thực hiện.                                                                                                                                                                                                                                                                                                           |
| Mỹ                                         | The use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems.<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2008</i>                                                                                                                                                                                                                                                | Việc sử dụng máy tính để làm gián đoạn hoạt động của một quốc gia thù địch, đặc biệt là việc tấn công có chủ đích các hệ thống truyền dữ liệu.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2008</i>                                                                                                                                                                                                                            |
| <b>1.4. Cyber Offensive: Tấn công mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Bi                                         | The offensive capacity includes the manipulation or disruption of networks and systems with the purpose of limiting or eliminating the adversary's operational capability. This capability can be required to guarantee one's freedom of action in the cyber domain. Cyber-attacks can be launched to repel an attack (active defence) or to support the operational action.<br><br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2014</i> | Năng lực tấn công bao gồm việc thao túng hoặc gây gián đoạn hệ thống mạng và máy tính nhằm mục đích hạn chế hoặc hủy diệt khả năng vận hành của đối phương. Khả năng này là cần thiết nhằm bảo đảm sự tự do hành động trong lĩnh vực mạng. Các cuộc tấn công mạng có thể được phát động nhằm đẩy lùi một cuộc tấn công (phòng thủ chủ động) hoặc để hỗ trợ kế hoạch khác.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2014</i> |
| Áo                                         | The term “cyber attack” refers to an attack through IT in cyber space, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally.<br><br><i>Source: Austrian Cyber Security Strategy (2013)</i>                                                                                                                                                                                                      | Thuật ngữ “tấn công mạng” để chỉ một cuộc tấn công bằng công nghệ thông tin (IT) trên không gian mạng, trực tiếp nhằm vào một hoặc một số hệ thống công nghệ thông tin, mục đích là để làm suy yếu một phần hoặc toàn bộ các mục tiêu hệ thống bảo vệ bảo mật ICT (tính bí mật, toàn vẹn và sẵn sàng).<br><i>Nguồn: Chiến lược An ninh mạng Áo (2013)</i>                                                                                                                                                          |
| Canada                                     | Cyber attacks include the unintentional or unauthorised access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical                                                                                                                                                                                                                                                                                                                                  | Các cuộc tấn công mạng bao gồm truy nhập, sử dụng, thao túng, làm gián đoạn hoặc phá hủy (bằng các phương tiện điện tử) thông tin điện tử và/hoặc hạ tầng vật lý và điện tử sử dụng để xử lý, truyền đưa và/hoặc                                                                                                                                                                                                                                                                                                   |

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                        | infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.<br><i>Source: Canada's Cyber Security Strategy (2010)</i>                                                                                                                    | lưu trữ thông tin đó không có ý hoặc trái phép. Mức độ nghiêm trọng của tấn công mạng xác định mức độ ứng cứu và hoặc các biện pháp giảm thiểu thiệt hại.<br><i>Nguồn: Chiến lược An ninh mạng Canada (2010)</i>                                                                                                                                                                                              |
| NATO                                                   | Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber attack.<br><br><i>Source: NATO AAP-06 Edition 2014</i>                                                                                                                 | Hành động nhằm gây gián đoạn, từ chối hoặc hủy diệt máy tính và/hoặc mạng máy tính, thông tin lưu trữ trên máy tính và/hoặc mạng máy tính. Ghi chú: Tấn công mạng máy tính là một kiểu tấn công mạng.<br><i>Nguồn: NATO AAP-06 Edition 2014</i>                                                                                                                                                               |
| Mỹ                                                     | An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information<br><br><i>Source: NIST US Department of Commerce: Glossary of Key Information Security Terms (June 2013)</i> | Một cuộc tấn công, thông qua không gian mạng, nhằm vào việc sử dụng không gian mạng của một doanh nghiệp nhằm mục đích gây gián đoạn, vô hiệu hoặc chiến quyền điều khiển hạ tầng/môi trường điện toán hoặc phá hoại tính toàn vẹn của dữ liệu hoặc đánh cắp thông tin bị kiểm soát.<br><i>Nguồn: Chủ giải các thuật ngữ an ninh mạng quan trọng, Viện Tiêu chuẩn và Công nghệ quốc gia, Bộ Thương mại Mỹ</i> |
| Từ điển Oxford                                         | [Cyberattack] An attempt by hackers to damage or destroy a computer network or system.                                                                                                                                                                                                                                                                                                  | Nỗ lực của tin tặc nhằm gây thiệt hại hoặc hủy diệt mạng máy tính.                                                                                                                                                                                                                                                                                                                                            |
| Hướng dẫn Tallinn                                      | A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.<br><br><i>Source: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013, Rule 30</i>                                                                                                     | Một cuộc tấn công mạng là một chiến dịch mạng, dù là tấn công hay phòng thủ, đều có lý do cho rằng sẽ gây thương vong hoặc chết người hoặc gây thiệt hại hoặc phá hủy các mục tiêu.<br><i>Nguồn: Hướng dẫn Tallinn về Luật quốc tế áp dụng đối với Chiến tranh mạng - 2013, Quy tắc 30</i>                                                                                                                    |
| <b>1.5. Cybercriminality/cybercrime: Tội phạm mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                               |
| Bỉ                                                     | (Translation) an offence of abusive usage of automation or automated given to threaten information systems or registered information<br><i>Source: Cyber Security Strategy. Securing Cyberspace - 2012</i>                                                                                                                                                                              | Tội phạm lợi dụng kỹ thuật tự động để đe dọa các hệ thống thông tin hoặc thông tin đăng ký.<br><i>Nguồn: Chiến lược An ninh mạng: Không gian mạng an toàn - 2012</i>                                                                                                                                                                                                                                          |
| Mỹ                                                     | Cybercrime is criminal activity conducted using computers and the Internet, often financially motivated. Cybercrime includes identity theft, fraud, and internet scams, among other activities. Cybercrime is                                                                                                                                                                           | Tội phạm mạng là hoạt động tội phạm được thực hiện bằng cách sử dụng máy tính và Internet, thường là vì động cơ tài chính. Tội phạm mạng bao gồm: đánh cắp danh tính, gian lận và lừa đảo qua mạng và                                                                                                                                                                                                         |

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <p>distinguished from other forms of malicious cyber activity, which have political, military, or espionage motivations.</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2015 July</i></p>                                                                                                                                                                                                                                                                                                                                                                                           | <p>các hoạt động khác. Tội phạm mạng khác với các loại hình xấu độc khác trên không gian mạng có động cơ chính trị, quân sự hoặc gián điệp.</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 07/2015</i></p>                                                                                                                                                                                                                                                                                                                                                                            |
| Vương quốc Anh | <p>For the purposes of this study, we are using the term “cyber crime” to mean the illegal activities undertaken by criminals for financial gain. Such activities exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the Government.</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2011</i></p>                                                                                                                                                                 | <p>Tại nghiên cứu này, chúng ta sử dụng thuật ngữ “tội phạm mạng” để chỉ các hoạt động bất hợp pháp thực hiện vì mục đích tài chính. Đó là các hoạt động khai thác lỗ hổng trong việc sử dụng internet và các hệ thống điện tử để truy cập trái phép hoặc tấn công thông tin và dịch vụ do công dân, doanh nghiệp và chính phủ sử dụng.</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2011</i></p>                                                                                                                                                                                   |
| Ba Lan         | <p>An offence committed in cyberspace</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2013</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>Một hành vi phạm tội trên không gian mạng</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2013</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| EU             | <p>Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2013</i></p> | <p>Tội phạm mạng thường để chỉ một phạm vi rộng các hoạt động tội phạm khác nhau có liên quan đến máy tính và hệ thống thông tin với vai trò hoặc là công cụ chính hoặc là mục tiêu chính. Tội phạm mạng bao gồm tội phạm truyền thống (VD: gian lận, giả mạo và đánh cắp danh tính), tội phạm liên quan đến nội dung (VD: truyền bá khiêu dâm trẻ em, kích động phân biệt chủng tộc) và các tội phạm riêng có của máy tính và hệ thống thông tin (VD: tấn công các hệ thống thông tin, tấn công từ chối dịch vụ, mã độc)</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2013</i></p> |
| Australia      | <p>The Australian Government defines cyber crime as those computer offences under the Commonwealth Criminal Code Act 1995 (Part</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>Chính phủ Australia định nghĩa tội phạm mạng là các vi phạm về máy tính theo Bộ luật hình sự của Khối Thịnh vượng chung (Phần 10.7) liên</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                           | 10.7) which involve the unauthorised access to, modification or impairment of electronic communications.<br><i>Source: Australian Government, Cyber Security Strategy (2009)</i>                                                                                                                                                                                                                                                                                                                                                                     | quan đến truy cập, thay đổi trái phép hoặc làm hư hỏng dữ liệu điện tử.<br><i>Nguồn: Chiến lược An ninh mạng (2009), Chính phủ Australia.</i>                                                                                                                                                                                                                                                                                                                                                                                            |
| Áo                                                        | Cyber crime comprises illegal attacks from cyber space on or through ICT systems, which are defined in penal or administrative laws. The term therefore covers all criminal offences committed with the aid of information technologies and communications networks and also encompasses Internet crime.<br><br><i>Source: Austrian Cyber Security Strategy (2013)</i>                                                                                                                                                                               | Tội phạm mạng bao gồm các cuộc tấn công trái pháp luật từ không gian mạng hoặc thông qua các hệ thống ICT, được định nghĩa trong luật hình sự và luật hành chính. Vì vậy, thuật ngữ này bao gồm toàn bộ các hành vi phạm tội sử dụng công nghệ thông tin và hệ thống mạng truyền dữ liệu, bao gồm cả tội phạm Internet.<br><i>Nguồn: Chiến lược An ninh mạng Áo (2013)</i>                                                                                                                                                               |
| Pháp                                                      | Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime.<br><br><i>Source: Information Systems and Defence - France's Strategy (2011)</i>                                                                                                                                                                                                                                                                                                                 | Hành vi vi phạm các hiệp ước quốc tế và luật pháp quốc gia, nhằm vào các hệ thống mạng hoặc hệ thống thông tin hoặc sử dụng các hệ thống này để thực hiện hành vi tội phạm.<br><i>Nguồn: Phòng thủ và Các hệ thống thông tin - Chiến lược của Pháp (2011)</i>                                                                                                                                                                                                                                                                            |
| Từ điển Oxford                                            | [Cybercrime] Crime conducted via the Internet or some other computer network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Tội phạm thực hiện qua mạng Internet hoặc một số mạng máy tính khác.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Mỹ/Nga                                                    | the use of cyberspace for criminal purposes as defined by national or international law<br><i>Source: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014</i>                                                                                                                                                                                                                          | Sử dụng không gian mạng nhằm mục đích phạm tội như định nghĩa tại luật quốc gia và quốc tế.<br><i>Nguồn: Viện Đông Tây, Cơ sở thuật ngữ quan trọng 2, Hiệp định song phương Nga - Mỹ về An ninh mạng, Eds. Habes B. Godwin III, Báo cáo chính sách 2/2014, - 2014</i>                                                                                                                                                                                                                                                                    |
| <b>1.6. Cyberspace Defense: Phòng thủ không gian mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Mỹ                                                        | - The passive, active and dynamic employment of capabilities to respond to imminent or on-going actions against AF or AF- protected networks, AF's portion of the Global Information Grid (GIG) or expeditionary communications assigned to the AF. (AFDD 3-12)<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2010</i><br>- Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific | - Việc sử dụng các năng lực nhằm đối phó với các hành động đang và sắp xảy ra chống lại hệ thống mạng của Không quân, phần của không quân trong Mạng lưới thông tin toàn cầu (GIG).<br><br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2010</i><br>- Hành động thường được tạo trong phạm vi không gian mạng của Bộ Quốc phòng nhằm mục đích bảo đảm an toàn, vận hành và bảo vệ các hệ thống mạng thông tin của BQP. Các hành động cụ thể bao gồm: bảo |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <p>actions include protect, detect, characterize, counter, and mitigate.</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2014</i></p> <p>- Combat operations in, through, and from cyberspace to achieve military objectives and influence the course and outcome of conflict by taking decisive actions against approved targets.</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2010</i></p> <p>- The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0).</p> <p><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2012</i></p> | <p>vệ, phát hiện, mô tả đặc điểm, phản công và giảm nhẹ tác hại</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2014</i></p> <p>- Hoạt động chiến đấu trên, thông qua hoặc từ không gian mạng nhằm đạt được các mục tiêu quân sự và tác động đến quá trình và kết quả xung đột bằng cách thực hiện các hành động quyết định chống lại các mục tiêu đã được phê duyệt.</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2010</i></p> <p>- Việc sử dụng các năng lực không gian mạng tại đó mục đích chính là đạt được các mục tiêu trên hoặc thông qua không gian mạng.</p> <p><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2012</i></p> |
| US/Russia | <p>organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack</p> <p><i>Source: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <p>Các năng lực được tổ chức nhằm bảo vệ, giảm nhẹ và nhanh chóng khôi phục hậu quả của tấn công mạng.</p> <p><i>Nguồn: Viện Đông Tây, Cơ sở thuật ngữ quan trọng 2, Hiệp định song phương Nga - Mỹ về An ninh mạng, Eds. Habes B. Godwin III, Báo cáo chính sách 2/2014, - 2014</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Pháp      | <p>The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical.</p> <p><i>Source: Information Systems and Defence - France's Strategy (2011)</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>Tập hợp các biện pháp kỹ thuật và phi kỹ thuật cho phép một quốc gia có bảo vệ các hệ thống thông tin không gian mạng trọng yếu của quốc gia</p> <p><i>Nguồn: Các hệ thống thông tin và Phòng thủ - Chiến lược của Pháp (2011)</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Bỉ        | <p>The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defence consists of following duties: Protect, Detect, Respond,</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p>Việc áp dụng các biện pháp bảo vệ hữu hiệu nhằm đạt được mức độ bảo mật không gian mạng phù hợp bảo đảm các chức năng và hoạt động phòng thủ. Điều này đạt được bằng cách áp dụng các biện pháp bảo vệ phù hợp nhằm giảm nguy cơ bảo mật xuống mức độ chấp nhận được. Phòng thủ mạng bao gồm các nhiệm vụ sau: Bảo vệ, Phát hiện, Ứng cứu</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               | and Recover<br><br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2014</i>                                                                                                                                                                                                                                                                                                                                       | và Khôi phục.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2014</i>                                                                                                                                                                                                                                                                                                                                     |
| Montenegro                                                    | Cyber defence is mainly used in military context, but it may be also related to criminal and espionage activities. NATO uses the following definition when referring to cyber defence the ability to safeguard the delivery and management of services in an operational Communications and Information Systems (CIS) in response to potential and imminent as well as actual malicious actions that originate in cyberspace.”<br><i>Source: Strategy on Cyber Security of Montenegro to 2017 (2013)</i> | Phòng thủ mạng chủ yếu sử dụng trong bối cảnh quân sự nhưng cũng có thể liên quan đến các hoạt động gián điệp và tội phạm. NATO sử dụng định nghĩa dưới đây khi đề cập đến phòng thủ mạng, khả năng bảo vệ việc phân phối và quản lý các dịch vụ tại một hệ thống CIS hoạt động (CIS - Các hệ thống thông tin và Truyền thông) nhằm đáp trả các hành động thù địch xảy ra có bắt nguồn từ không gian mạng.<br><br><i>Nguồn: Chiến lược An ninh mạng đến năm 2017 của Montenegro (2013)</i> |
| <b>1.7. Cyberspace Intelligence: Tình báo không gian mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Mỹ                                                            | Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.<br><br><i>Source: US Department of Defense Dictionary of Military and Associated Terms</i>                                                                                                                                             | Các biện pháp nhằm xác định, xâm nhập hoặc vô hiệu hóa các chiến dịch của nước ngoài sử dụng phương tiện mạng cũng như các nỗ lực thu thập thông tin tình báo nước ngoài sử dụng các phương pháp truyền thống để đánh giá ý đồ và năng lực không gian mạng.<br><i>Nguồn: Từ điển quân sự và các thuật ngữ liên quan của Bộ Quốc phòng Mỹ</i>                                                                                                                                               |
| Bi                                                            | Activities using all “intelligence” sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-attacks.<br><br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2014</i>                                                              | Các hoạt động sử dụng tất cả các nguồn “tình báo” nhằm hỗ trợ An ninh mạng chỉ ra mối đe dọa trên không gian mạng, thu thập các ý đồ, mục đích trên không gian mạng và khả năng của các đối thủ tiềm tàng, phân tích, truyền dữ liệu, xác minh, định vị nguồn phát sinh các cuộc tấn công mạng<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2014</i>                                                    |
| <b>1.8. Cyber Espionage: Tình báo/gián điệp mạng</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Hướng dẫn Tallinn                                             | Cyber Reconnaissance: The use of cyber capabilities to obtain information about activities, information resources, or system                                                                                                                                                                                                                                                                                                                                                                             | Việc sử dụng các khả năng không gian mạng nhằm thu thập thông tin về hoạt động, tài nguyên thông tin hoặc khả năng của hệ thống.                                                                                                                                                                                                                                                                                                                                                           |

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | capabilities.<br><br><i>Source: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <i>Nguồn: Hướng dẫn Tallinn về Luật quốc tế áp dụng đối với Chiến tranh mạng - 2013</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Đức            | A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage.<br><br><i>Source: Cyber Security Strategy for Germany (2011)</i> | Tấn công mạng là tấn công về CNTT trên không gian mạng nhằm vào một hoặc một số hệ thống CNTT khác và nhằm mục đích gây thiệt hại về bảo mật CNTT. Các mục tiêu của bảo mật CNTT, bao gồm tính bảo mật, toàn vẹn và sẵn có, bị xâm nhập (toàn bộ hoặc từng phần). Các cuộc tấn công nhằm vào tính bảo mật của một hệ thống CNTT, do các cơ quan tình báo nước ngoài phát động hoặc kiểm soát, được gọi là tình báo/gián điệp mạng. Các cuộc tấn công mạng nhằm vào tính toàn vẹn và sẵn có của một hệ thống CNTT được coi là tấn công phá hoại mạng.<br><i>Nguồn: Chiến lược An ninh mạng Đức (2011)</i> |
| Từ điển Oxford | [cyberespionage] The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.                                                                                                                                                                                                                                                                                                                                                                                                                 | Việc sử dụng mạng máy tính nhằm chiếm quyền truy cập trái phép các thông tin mật của chính phủ hoặc tổ chức.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Anh            | Cyber attacks have aimed to steal sensitive information and data from financial, government and utilities infrastructure targets. These attacks can target intellectual property or sensitive information about organisations or government<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2011</i>                                                                                                                                                                               | Các cuộc tấn công mạng nhằm đánh cắp thông tin và dữ liệu nhạy cảm từ các mục tiêu hạ tầng tài chính, chính phủ, điện, nước... Các cuộc tấn công có thể nhằm vào tài sản trí tuệ hoặc thông tin nhạy cảm về tổ chức hoặc chính phủ.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2011</i>                                                                                                                                                                                                                             |
| NATO CCD COE   | Cyber espionage is defined narrowly as any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party. The act must occur in territory controlled by a party to the conflict. “                                                                                                                                                                                                                                                            | Tình báo/gián điệp mạng được định nghĩa cụ thể là bất kỳ hành vi nào thực hiện bí mật hoặc bằng cách lừa dối sử dụng các năng lực không gian mạng nhằm thu thập hoặc tìm cách thu thập thông tin với mục đích chuyển cho đối phương. Hành vi phải xảy ra tại lãnh thổ do một bên tham gia xung đột kiểm soát.                                                                                                                                                                                                                                                                                            |
| Montenegro     | Cyber espionage is defined as the use of an agent in order to obtain information about plans or activities of foreign country or competitive company”.”                                                                                                                                                                                                                                                                                                                                                                                                                      | Tình báo/gián điệp mạng được định nghĩa là việc sử dụng một tác nhân nhằm thu thập thông tin về kế hoạch hoặc hoạt động của nước ngoài hoặc công ty cạnh tranh.                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | <p><i>Source: Strategy on Cyber Security of Montenegro to 2017 (2013)</i></p> <p>Cyber espionage is defined as the use of an agent in order to obtain information about plans or activities of foreign country or competitive company”. It is not uncommon that companies or governments are faced with attempts of unauthorised access to their computer systems via Internet. Many countries use espionage tools to encourage their economic development based on advanced technologies of other nations. ICT present foundation of development and implementation of most other technologies both in civilian and military sectors, and thereupon they have become primary target of espionage”</p> <p><i>Source: National Cyber Security Strategy for Montenegro 2013-2017 - 2013</i></p>                                                                                  | <p><i>Nguồn: Chiến lược An ninh mạng Montenegro đến năm 2017 (2013)</i></p> <p>Tình báo/gián điệp mạng được định nghĩa là việc sử dụng một tác nhân nhằm thu thập thông tin về kế hoạch hoặc hoạt động của nước ngoài hoặc công ty cạnh tranh. Thông thường các công ty hoặc chính phủ đang đương đầu với các nỗ lực chiếm quyền truy cập trái phép hệ thống máy tính của họ qua Internet. Nhiều nước sử dụng các công cụ tình báo/gián điệp nhằm thúc đẩy phát triển kinh tế đất nước trên cơ sở công nghệ tiên tiến của các nước khác. CNTT và VT cung cấp nền tảng cho phát triển và thực thi hầu hết các công nghệ khác cả trên lĩnh vực dân sự và quân sự, do vậy nó đã trở thành mục tiêu thu thập thông tin tình báo/gián điệp quan trọng nhất</p> <p><i>Nguồn: Chiến lược An ninh mạng Montenegro đến năm 2017 (2013)</i></p>   |
| <b>1.9. Cyber Terrorism: Khủng bố mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Áo                                         | <p>Cyber terrorism is defined as a politically motivated crime of state and / or non-state actors against computers, networks and the information stored therein. Its aim is to provoke a severe or long-term disruption of public life or to cause serious damage to economic activity with the intention of severely intimidating the population, of forcing public authorities or an international organisation to carry out, tolerate or omit an act or of profoundly unsettling or destroying the political, constitutional, economic or social foundations of a state or an international organisation. These acts constitute organised cyber sabotage (attacks) caused by political-fundamentalist groups or individual perpetrators; they are directed against states, organisations or enterprises.</p> <p><i>Source: Austrian Cyber Security Strategy (2013)</i></p> | <p>Khủng bố mạng được định nghĩa là hoạt động tội phạm có động cơ chính trị của các tác nhân nhà nước và/hoặc phi nhà nước chống lại hệ thống máy tính, mạng và thông tin lưu trữ trên đó. Mục đích của khủng bố mạng là gây gián đoạn nghiêm trọng hoặc lâu dài của đời sống công cộng hoặc gây thiệt hại nghiêm trọng đến hoạt động kinh tế với mục đích đe dọa dân chúng, buộc cơ quan có thẩm quyền hoặc một tổ chức quốc tế phải thực hiện hoặc không thực hiện một hành động, làm đảo lộn hoặc phá hủy nền tảng xã hội, kinh tế, chính trị của một quốc gia hoặc tổ chức quốc tế. Các hành động này cấu thành việc tấn công phá hoại không gian mạng có tổ chức do các nhóm, cá nhân có động cơ chính trị; trực tiếp nhằm vào các quốc gia, tổ chức hoặc doanh nghiệp;</p> <p><i>Nguồn: Chiến lược An ninh mạng Áo (2013)</i></p> |
| Từ điển Oxford                             | [Cyberterrorism] The politically motivated use of computers and information technology to cause severe disruption or widespread fear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Việc sử dụng hệ thống máy tính và công nghệ thông tin có động cơ chính trị nhằm gây gián đoạn nghiêm trọng hoặc gieo rắc nỗi sợ hãi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hàn Quốc                                                   | Various forms of cyber terrorism: Hacking, DDoS attacks, denials of service, logic bombs, Trojan horses, Worm viruses, HERF guns etc.<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2012</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Các hình thức khác nhau của khủng bố mạng: Tấn công xâm nhập (Hacking), tấn công từ chối dịch vụ, bom logic, virus Trojan, sâu máy tính...<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2012</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Mỹ                                                         | The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.<br><i>Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2008</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Việc sử dụng hệ thống máy tính và công nghệ thông tin có động cơ chính trị nhằm gây gián đoạn nghiêm trọng hoặc gieo rắc nỗi sợ hãi trong xã hội.<br><i>Nguồn: Tài liệu về các khái niệm liên quan đến An ninh mạng và An ninh thông tin, Open Technology Institute New America - 2008</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>1.10. Cyber Infrastructure: Hạ tầng không gian mạng</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Mỹ/Nga                                                     | The aggregation of people, processes and systems that constitute cyberspace<br><i>Source: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Không gian mạng cấu thành bởi tập hợp người dùng, các tiến trình và hệ thống.<br><i>Nguồn: Viện Đông Tây, Cơ sở thuật ngữ quan trọng 2, Hiệp định song phương Nga - Mỹ về An ninh mạng, Eds. Habes B. Godwin III, Báo cáo chính sách 2/2014, - 2014</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Mỹ                                                         | Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition-SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.<br><i>Source: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Department of Commerce, NISTIR 7298, Revision 2, - 2010</i> | Bao gồm thông tin điện tử, các dịch vụ và hệ thống truyền dữ liệu, thông tin lưu trữ trên các hệ thống và dịch vụ này. Thông tin, các dịch vụ và hệ thống truyền dữ liệu bao gồm toàn bộ phần cứng, phần mềm xử lý, lưu trữ và truyền thông tin hoặc kết hợp toàn bộ các yếu tố này. Xử lý bao gồm việc tạo, truy cập, sửa đổi và xóa thông tin. Lưu trữ bao gồm lưu trữ bằng giấy, từ tính, điện tử và toàn bộ các phương tiện lưu trữ khác. Truyền dữ liệu bao gồm chia sẻ và phân phối thông tin. VD: Hệ thống máy tính, hệ thống điều khiển (Hệ thống điều khiển giám sát và thu thập dữ liệu - SCADA), hệ thống mạng: Internet và các dịch vụ mạng (dịch vụ bảo mật) là bộ phận của hạ tầng không gian mạng.<br><i>Nguồn: Chủ giải các thuật ngữ an ninh mạng quan trọng, eds. Richard Kissel, Viện Tiêu chuẩn và Công nghệ quốc gia, Bộ Thương mại Mỹ, NISTIR 7298, Revision 2 - 2010</i> |

### Phụ lục 3: VĂN BẢN QUY PHẠM PHÁP LUẬT VỀ AN NINH MẠNG CỦA MỘT SỐ QUỐC GIA, TỔ CHỨC QUỐC TẾ TRÊN THẾ GIỚI

| QUỐC GIA,<br>TCQT | VĂN BẢN QPPL<br>VỀ AN NINH MẠNG                                                                 | THỜI GIAN<br>BAN HÀNH | NỘI DUNG QUY ĐỊNH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|-------------------------------------------------------------------------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hoa Kỳ</b>     | 1. Đạo luật về An ninh Mạng Quốc gia (National Cybersecurity Protection Act)                    | 2014                  | Đạo luật Bảo vệ An ninh mạng quốc gia (National Cybersecurity Protection Act) được Quốc hội Hoa Kỳ thông qua vào năm 2014 nhằm cải thiện khả năng bảo vệ an ninh mạng của quốc gia trước các mối đe dọa mạng ngày càng gia tăng. Đạo luật này tập trung vào việc nâng cao khả năng phòng thủ và phản ứng với các cuộc tấn công mạng, đồng thời tạo ra các cơ chế hợp tác mạnh mẽ giữa chính phủ và các tổ chức tư nhân trong lĩnh vực bảo mật mạng. Với sự ban hành của đạo luật này Trung tâm An ninh mạng Quốc gia (National Cybersecurity and Communications Integration Center - NCCIC) chính thức ra đời. |
|                   | 2. Đạo luật Bảo vệ An ninh Mạng Quốc gia (National Cybersecurity Protection Advancement Act)    | 2015                  | Đạo luật này được thông qua năm 2015. Mục đích của luật này là tăng cường khả năng bảo vệ an ninh mạng quốc gia bằng cách cải thiện cơ chế phối hợp và chia sẻ thông tin về các mối đe dọa an ninh mạng giữa các cơ quan chính phủ, các tổ chức tư nhân và các nhà cung cấp dịch vụ mạng. Luật này được xem là một phần quan trọng trong nỗ lực của chính phủ Mỹ nhằm bảo vệ cơ sở hạ tầng quan trọng và các hệ thống thông tin khỏi các mối đe dọa an ninh mạng ngày càng gia tăng.                                                                                                                           |
|                   | 3. Đạo luật An ninh Mạng (Cybersecurity Act)                                                    | 2015                  | Đạo luật là một phần của Đạo luật Quốc phòng Quốc gia (NDAA), đạo luật này bảo vệ cơ sở hạ tầng quan trọng của quốc gia và tăng cường các biện pháp bảo vệ an ninh mạng cho các cơ quan chính phủ và khu vực tư nhân. Điểm nổi bật của đạo luật là việc thành lập Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA), tạo điều kiện cho sự hợp tác giữa các cơ quan chính phủ và khu vực tư nhân trong bảo vệ an ninh mạng..                                                                                                                                                                                         |
|                   | 4. Đạo luật về Quyền Riêng Tư và Bảo vệ Dữ liệu Cá nhân (Privacy Act)                           | 1974                  | Đạo luật quy định việc thu thập, sử dụng và chia sẻ thông tin cá nhân trong các cơ quan chính phủ của Hoa Kỳ. Mặc dù không trực tiếp liên quan đến an ninh mạng, đạo luật này yêu cầu các cơ quan chính phủ phải bảo vệ quyền riêng tư khi xử lý dữ liệu cá nhân, một yếu tố quan trọng trong bảo vệ an ninh mạng.                                                                                                                                                                                                                                                                                             |
|                   | 5. Đạo luật Tăng cường An ninh Mạng (Cybersecurity Enhancement Act)                             | 2014                  | Đạo luật tập trung vào nghiên cứu và phát triển công nghệ an ninh mạng, đồng thời thúc đẩy đào tạo và phát triển nguồn lực trong lĩnh vực an ninh mạng. Đạo luật này hỗ trợ các sáng kiến nghiên cứu để cải thiện phương pháp bảo vệ an ninh mạng và đối phó với các mối đe dọa mới.                                                                                                                                                                                                                                                                                                                           |
|                   | 6. Đạo luật Tăng cường Bảo vệ Cơ sở Hạ tầng Quan trọng (Critical Infrastructure Protection Act) | 2001                  | Đạo luật này là một phần của Đạo luật An ninh Nội địa (Homeland Security Act), được thông qua sau sự kiện tấn công khủng bố ngày 11 tháng 9, 2001, nhằm bảo vệ các cơ sở hạ tầng quan trọng của Hoa Kỳ, đặc biệt là trước các mối đe dọa từ khủng bố và các cuộc tấn công mạng. Đạo luật này đặt nền móng cho việc tăng cường bảo vệ các cơ sở hạ tầng quan                                                                                                                                                                                                                                                    |

|                      |                                                                                                                                                    |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |                                                                                                                                                    |      | trọng, bao gồm các ngành công nghiệp thiết yếu như năng lượng, viễn thông, giao thông, tài chính và y tế, trước các mối đe dọa tiềm ẩn và yêu cầu sự hợp tác chặt chẽ giữa chính phủ và khu vực tư nhân.                                                                                                                                                                                                                                                                                                                               |
|                      | 7. Đạo luật về Bảo vệ Thông tin trong Thương mại Điện tử (Electronic Communications Privacy Act - ECPA)                                            | 1986 | Đạo luật quy định bảo vệ quyền riêng tư của các cá nhân trong các giao dịch trực tuyến và thông qua các dịch vụ truyền thông điện tử, bao gồm email, dữ liệu lưu trữ trên điện toán đám mây và các giao dịch kỹ thuật số. Đạo luật này bảo vệ dữ liệu và quyền riêng tư của người dùng khi sử dụng các dịch vụ điện tử và trực tuyến.                                                                                                                                                                                                  |
|                      | 8. Đạo luật về An ninh Mạng và Quyền Riêng Tư trong Thế giới Kỹ Thuật Số (Cybersecurity Privacy Act of 2015)                                       | 2015 | Bảo đảm việc chia sẻ thông tin về các mối đe dọa mạng không làm xâm phạm quyền riêng tư và bảo mật dữ liệu cá nhân, nhằm tạo thế cân bằng giữa bảo vệ an ninh mạng và bảo vệ quyền riêng tư của công dân, khi có sự chia sẻ thông tin về mối đe dọa an ninh mạng.                                                                                                                                                                                                                                                                      |
|                      | 9. Đạo luật về Bảo vệ Quyền Riêng Tư và An ninh Mạng cho Các Hệ thống Công nghệ Thông tin (Federal Information Security Modernization Act - FISMA) | 2002 | Đạo luật quy định các yêu cầu bảo mật cho các hệ thống công nghệ thông tin của các cơ quan liên bang. FISMA yêu cầu các cơ quan chính phủ liên bang phải thiết lập các biện pháp bảo vệ mạng và dữ liệu theo các tiêu chuẩn bảo mật nghiêm ngặt để ngăn ngừa các mối đe dọa an ninh mạng. FISMA được sửa đổi và cập nhật vào năm 2014 để phù hợp với môi trường công nghệ mới, bao gồm các yêu cầu về đánh giá và giám sát an ninh mạng thường xuyên.                                                                                  |
|                      | 10. Đạo luật Tăng cường Quyền Riêng Tư và Bảo Mật (Gramm-Leach-Bliley Act - GLBA)                                                                  | 1999 | Đạo luật quy định về bảo mật và quyền riêng tư trong ngành tài chính, bao gồm các yêu cầu bảo vệ dữ liệu cá nhân và thông tin tài chính của khách hàng. GLBA yêu cầu các tổ chức tài chính phải bảo vệ thông tin cá nhân và bảo mật dữ liệu của khách hàng. Đạo luật này áp dụng cho các tổ chức tài chính như ngân hàng, công ty bảo hiểm và các tổ chức cung cấp dịch vụ tài chính khác.                                                                                                                                             |
| <b>Liên bang Nga</b> | 1. Luật về An ninh Thông tin (Federal Law No. 149-FZ “On Information, Information Technologies and Protection of Information”)                     | 2006 | Đây là một trong những đạo luật cơ bản điều chỉnh an ninh thông tin tại Nga. Luật này quy định các nguyên tắc cơ bản về việc bảo vệ thông tin và an ninh mạng, bao gồm việc bảo vệ dữ liệu cá nhân, bảo mật thông tin trong các hệ thống thông tin và bảo đảm tính toàn vẹn của dữ liệu. Luật này yêu cầu các tổ chức phải áp dụng các biện pháp bảo mật và bảo vệ thông tin, đồng thời cung cấp các quy định về xử lý thông tin và bảo vệ quyền lợi của người sử dụng.                                                                |
|                      | 2. Luật về An ninh Mạng (Federal Law No. 187-FZ “On the Security of Critical Information Infrastructure of the Russian Federation”)                | 2017 | Luật này quy định các yêu cầu bảo mật cho cơ sở hạ tầng thông tin quan trọng (Critical Information Infrastructure - CII) của Nga. Nó yêu cầu các tổ chức sở hữu cơ sở hạ tầng quan trọng phải thực hiện các biện pháp bảo mật để ngăn ngừa các cuộc tấn công mạng và bảo vệ các hệ thống thông tin. Đạo luật yêu cầu các tổ chức phải bảo vệ cơ sở hạ tầng quan trọng, bao gồm các ngành công nghiệp như năng lượng, giao thông, tài chính và viễn thông, đồng thời triển khai các hệ thống phát hiện mối đe dọa và ứng phó với sự cố. |
|                      | 3. Luật về Quyền Riêng Tư và Bảo Vệ Dữ Liệu Cá Nhân (Federal Law                                                                                   | 2006 | Luật này quy định về việc thu thập, xử lý, lưu trữ và bảo vệ dữ liệu cá nhân. Nó yêu cầu các tổ chức phải tuân thủ các quy định bảo mật khi xử lý thông tin cá nhân của công dân                                                                                                                                                                                                                                                                                                                                                       |

|                          |                                                                                                                                                                               |      |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | No. 152-FZ “On Personal Data”)                                                                                                                                                |      | Nga. Các tổ chức phải có các biện pháp bảo mật để bảo đảm rằng thông tin cá nhân không bị lộ hoặc sử dụng sai mục đích. Đồng thời, luật này yêu cầu các cơ quan chính phủ và các công ty phải thông báo cho công dân về việc thu thập dữ liệu và cho phép họ kiểm soát việc sử dụng dữ liệu cá nhân của mình.                                                                                                                            |
|                          | 4. Luật về Phòng chống Tội phạm Mạng (Federal Law No. 3-FZ “On Amendments to the Criminal Code of the Russian Federation regarding Cybercrime”)                               | 2011 | Luật này sửa đổi Bộ Luật Hình sự Nga, đặc biệt đối với các tội phạm mạng. Đạo luật quy định các hình phạt đối với các hành vi như xâm nhập trái phép vào hệ thống thông tin, phát tán phần mềm độc hại và gian lận qua mạng. Luật này giúp tăng cường khả năng truy tố các tội phạm mạng và thiết lập các biện pháp xử lý nghiêm khắc đối với những kẻ phạm tội trong không gian mạng.                                                   |
|                          | 5. Luật về Quyền của Công dân trong Việc Sử Dụng Internet (Federal Law No. 394-FZ “On the Internet Sovereignty of the Russian Federation”)                                    | 2019 | Luật này quy định về “chủ quyền internet” của Nga, tập trung vào việc kiểm soát và giám sát không gian mạng nội bộ của quốc gia. Nó yêu cầu các nhà cung cấp dịch vụ internet phải tuân thủ các quy định bảo mật và quản lý các hoạt động trực tuyến để ngăn ngừa các mối đe dọa từ bên ngoài. Luật này cũng yêu cầu các tổ chức có cơ sở hạ tầng mạng quan trọng phải có khả năng hoạt động độc lập nếu internet toàn cầu bị gián đoạn. |
|                          | 6. Chỉ thị về Phát triển An ninh Mạng và Hạ tầng Kỹ thuật số (Decree No. 1837-r “On the Concept of the State Policy of the Russian Federation in the Field of Cybersecurity”) | 2017 | Chỉ thị này xác định các chính sách của nhà nước về an ninh mạng tại Nga, bao gồm các chiến lược và mục tiêu bảo vệ thông tin và hệ thống mạng quốc gia. Nó xác định các mục tiêu bảo mật mạng, bao gồm việc bảo vệ cơ sở hạ tầng quan trọng và bảo đảm sự độc lập của Nga trong không gian mạng.                                                                                                                                        |
|                          | 7. Luật về Kiểm soát và Giám sát 8. Hoạt động trên Internet (Federal Law No. 242-FZ “On the Protection of Rights of Consumers of Electronic Services”)                        | 2017 | Luật này quy định các tiêu chuẩn bảo vệ quyền lợi của người tiêu dùng dịch vụ điện tử, bao gồm các yêu cầu về bảo mật và quyền riêng tư khi sử dụng các dịch vụ trực tuyến. Các dịch vụ phải bảo đảm rằng người tiêu dùng có quyền kiểm soát thông tin cá nhân của mình và các công ty cung cấp dịch vụ phải có các biện pháp bảo mật cần thiết để bảo vệ dữ liệu người dùng.                                                            |
|                          | 9. Chỉ thị về Xử lý Dữ Liệu Cá Nhân và Giám sát An ninh Mạng (Government Regulation No. 835)                                                                                  | 2019 | Quy định này yêu cầu các tổ chức phải thực hiện các biện pháp bảo vệ an ninh mạng cho các hệ thống xử lý dữ liệu cá nhân. Nó yêu cầu các tổ chức xử lý dữ liệu phải có các biện pháp bảo mật đặc biệt để bảo vệ dữ liệu cá nhân khỏi các mối đe dọa mạng.                                                                                                                                                                                |
|                          | 10. Luật về Giám sát và Cấm Các Công Cụ Mạng Độc Hại (Federal Law No. 125-FZ “On the Control of Malicious Software”)                                                          | 2019 | Luật này quy định các biện pháp kiểm soát việc phát tán và sử dụng phần mềm độc hại, yêu cầu các nhà cung cấp dịch vụ internet và các tổ chức phải ngừng cung cấp phần mềm độc hại. Luật này giúp ngăn chặn sự lây lan của phần mềm độc hại và tấn công mạng nhằm vào các tổ chức và cá nhân tại Nga.                                                                                                                                    |
| <b>Liên minh châu Âu</b> | 1. Chỉ thị về An ninh Mạng (NIS Directive - Directive (EU) 2016/1148)                                                                                                         | 2016 | NIS Directive (Network and Information Systems Directive) là một trong những đạo luật quan trọng nhất của EU về an ninh mạng. Đạo luật yêu cầu các quốc gia thành viên EU phải thiết lập các quy định về an ninh mạng cho các cơ sở hạ tầng quan trọng (như năng lượng, giao thông, tài chính) và các dịch vụ kỹ thuật số (như các dịch vụ trực tuyến, dịch                                                                              |

|                   |                                                                                                                        |      |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                                                                                                                        |      | vụ đám mây). Chỉ thị yêu cầu các nhà cung cấp dịch vụ và các tổ chức có cơ sở hạ tầng quan trọng phải thực hiện các biện pháp bảo vệ an ninh mạng phù hợp và thông báo về các sự cố bảo mật nghiêm trọng.                                                                                                                                                                                                                    |
|                   | 2. Chỉ thị về Quyền Riêng Tư và Bảo Vệ Dữ Liệu (GDPR - General Data Protection Regulation)                             | 2016 | GDPR đặt ra các quy định nghiêm ngặt về việc bảo vệ quyền riêng tư và bảo mật dữ liệu cá nhân của người dân EU. Mặc dù không chỉ tập trung vào an ninh mạng, GDPR yêu cầu các tổ chức phải bảo đảm an toàn cho dữ liệu cá nhân và phải thực hiện các biện pháp bảo vệ chống lại các mối đe dọa mạng. Các tổ chức phải thông báo cho các cơ quan giám sát và người dân trong vòng 72 giờ khi xảy ra vi phạm dữ liệu cá nhân.  |
|                   | 3. Chỉ thị về An ninh Mạng trong Các Tổ chức Tài Chính (PSD2 - Revised Payment Services Directive)                     | 2015 | Chỉ thị PSD2 đặt ra các quy định về an ninh mạng đối với các dịch vụ thanh toán trực tuyến, yêu cầu các tổ chức tài chính phải bảo đảm tính bảo mật của các giao dịch trực tuyến và bảo vệ các dữ liệu nhạy cảm của khách hàng. Các nhà cung cấp dịch vụ thanh toán phải triển khai các biện pháp bảo vệ an ninh mạng như xác thực hai yếu tố để ngăn ngừa gian lận trong các giao dịch.                                     |
|                   | 4. Chỉ thị về Hệ thống và Dịch vụ Viễn thông (ePrivacy Directive)                                                      | 2002 | Chỉ thị ePrivacy yêu cầu các tổ chức cung cấp dịch vụ viễn thông và dịch vụ kỹ thuật số phải bảo vệ thông tin cá nhân và sự riêng tư của người dùng. Điều này bao gồm cả bảo mật dữ liệu liên quan đến các cuộc gọi, tin nhắn và dịch vụ truyền thông điện tử. Chỉ thị này yêu cầu sự đồng ý của người dùng trước khi thu thập hoặc chia sẻ thông tin cá nhân và các biện pháp bảo vệ thông tin khi truyền tải qua các mạng. |
|                   | 5. Chỉ thị về Phòng chống Vi phạm An ninh Mạng (Cybercrime Directive - Directive 2013/40/EU)                           | 2013 | Chỉ thị này thiết lập các biện pháp pháp lý để ngăn chặn và trừng phạt các hành vi phạm tội mạng trên toàn EU, bao gồm các tội phạm liên quan đến việc xâm nhập trái phép vào hệ thống máy tính, phát tán phần mềm độc hại và các hành vi gian lận mạng. Chỉ thị yêu cầu các quốc gia thành viên EU tăng cường hợp tác và đồng bộ hóa các biện pháp pháp lý để xử lý các vi phạm an ninh mạng.                               |
|                   | 6. Chỉ thị về Quản lý Tính Bảo mật trong Các Mạng và Hệ thống Thông tin (Cybersecurity Act - Regulation (EU) 2019/881) | 2019 | Quy định này nhằm thiết lập một khuôn khổ bảo mật mạng và chứng nhận an ninh mạng cho các sản phẩm và dịch vụ kỹ thuật số trong EU. Quy định tạo ra Chứng nhận An ninh Mạng EU (EU Cybersecurity Certification Framework), bảo đảm rằng các sản phẩm và dịch vụ kỹ thuật số được chứng nhận đáp ứng các tiêu chuẩn bảo mật cao nhất.                                                                                         |
|                   | 7. Đạo luật về Bảo mật Cơ sở Hạ tầng Kỹ thuật số (Digital Services Act - DSA)                                          | 2020 | Đạo luật này thiết lập các quy định về trách nhiệm của các nền tảng trực tuyến lớn (như mạng xã hội và các dịch vụ trực tuyến), yêu cầu các nền tảng phải có các biện pháp bảo mật mạng và bảo vệ người dùng. DSA yêu cầu các nền tảng trực tuyến lớn phải báo cáo các vi phạm an ninh mạng và có các biện pháp bảo vệ người dùng khỏi các nội dung độc hại và các cuộc tấn công mạng.                                       |
| <b>Trung Quốc</b> | 1. Luật An ninh Mạng (Cybersecurity Law of the People's Republic of China)                                             | 2016 | Đây là một trong những đạo luật quan trọng nhất của Trung Quốc về an ninh mạng. Nó thiết lập các nguyên tắc về bảo vệ an ninh mạng, bảo mật thông tin và bảo vệ quyền riêng tư của công dân. Đạo luật yêu cầu các nhà cung cấp dịch vụ mạng phải bảo vệ an ninh mạng và dữ liệu của người dùng; quy định về kiểm soát các thông tin và dữ liệu cá nhân                                                                       |

|                  |                                                                                                                               |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|-------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  |                                                                                                                               |      | của công dân Trung Quốc; đề cập đến bảo vệ cơ sở hạ tầng quan trọng và ngăn ngừa các cuộc tấn công mạng.                                                                                                                                                                                                                                                                                                                                                                                             |
|                  | 2. Luật về Bảo vệ Dữ Liệu Cá Nhân (Personal Information Protection Law - PIPL)                                                | 2021 | Đây được coi là một trong những đạo luật bảo vệ quyền riêng tư quan trọng nhất của Trung Quốc, Luật Bảo vệ Dữ liệu Cá Nhân điều chỉnh việc thu thập, lưu trữ và xử lý dữ liệu cá nhân của công dân. Đạo luật quy định về quyền kiểm soát và quyền truy cập của người dân đối với dữ liệu cá nhân; yêu cầu các tổ chức và công ty phải có sự đồng ý rõ ràng từ người dùng trước khi thu thập dữ liệu cá nhân; quy định xử phạt nghiêm khắc đối với các vi phạm liên quan đến bảo mật dữ liệu cá nhân. |
|                  | 3. Luật về Chống Tội Phạm Mạng (Criminal Law of the People's Republic of China - Amendment to the Criminal Law on Cybercrime) | 2020 | Luật này sửa đổi Bộ Luật Hình sự của Trung Quốc, đặc biệt là đối với các tội phạm mạng. Nó quy định các hành vi phạm tội liên quan đến an ninh mạng, chẳng hạn như xâm nhập hệ thống thông tin trái phép, phát tán virus máy tính và gian lận qua mạng. Theo quy định tại văn bản pháp lý này, tội phạm mạng như hacking và phát tán phần mềm độc hại sẽ bị xử lý nghiêm minh; các hành vi phá hoại các hệ thống mạng quan trọng của quốc gia sẽ chịu mức án cao.                                    |
|                  | 4. Luật về Quản lý An ninh Dữ liệu (Data Security Law)                                                                        | 2021 | Luật này thiết lập các quy định về bảo mật và quản lý dữ liệu tại Trung Quốc, với mục tiêu bảo vệ dữ liệu quốc gia và bảo đảm an ninh dữ liệu trong nước. Luật này quy định về bảo vệ các dữ liệu quan trọng của quốc gia; yêu cầu các tổ chức xử lý dữ liệu phải bảo đảm an ninh dữ liệu, tuân thủ các tiêu chuẩn bảo mật quốc gia và có kế hoạch ứng phó khi có sự cố.                                                                                                                             |
|                  | 5. Chỉ thị về Quản lý Nội dung Internet (Regulations on the Administration of Internet Information Services)                  | 2000 | Quy định này quản lý việc cung cấp dịch vụ thông tin trên internet, đặc biệt đối với các nền tảng trực tuyến và các công ty công nghệ. Theo đó, văn bản này đã yêu cầu các công ty phải giám sát nội dung trực tuyến và báo cáo các hành vi vi phạm; các nền tảng internet phải kiểm tra và kiểm soát nội dung để ngăn chặn các hoạt động phi pháp như phát tán thông tin sai lệch, khủng bố, hoặc vi phạm bản quyền.                                                                                |
|                  | 6. Chỉ thị về Bảo vệ Quyền và Lợi ích của Người Tiêu Dùng qua Internet (Regulations on Consumer Protection in E-Commerce)     | 2019 | Chỉ thị này được thiết kế để bảo vệ quyền lợi của người tiêu dùng khi tham gia vào các giao dịch trực tuyến, bao gồm các biện pháp bảo mật khi thu thập và xử lý dữ liệu cá nhân. Theo quy định tại Chỉ thị này việc bảo đảm các nền tảng e-commerce phải bảo vệ quyền riêng tư của người tiêu dùng và ngừng việc thu thập hoặc sử dụng thông tin cá nhân mà không có sự đồng ý của họ.                                                                                                              |
|                  | 7. Chỉ thị về Các Công Ty và Cơ sở Hạ tầng Quan trọng (Critical Information Infrastructure Protection - CIIP)                 |      | Chỉ thị này thường xuyên được điều chỉnh bởi các chỉ thị bảo vệ hạ tầng quan trọng. Với mục tiêu nhằm bảo vệ các cơ sở hạ tầng quan trọng của quốc gia khỏi các mối đe dọa an ninh mạng, bao gồm các cơ sở năng lượng, giao thông, viễn thông và các dịch vụ công. Bảo đảm rằng các tổ chức có cơ sở hạ tầng quan trọng phải thực hiện các biện pháp bảo mật và có kế hoạch ứng phó với các cuộc tấn công mạng.                                                                                      |
|                  | 8. Quy định về Giám sát An ninh Mạng (Cybersecurity Monitoring Regulations)                                                   | 2017 | Quy định này yêu cầu các tổ chức phải thiết lập các hệ thống giám sát an ninh mạng để phát hiện và ngăn ngừa các mối đe dọa mạng. Theo đó, các tổ chức phải giám sát các hoạt động trên mạng và báo cáo cho các cơ quan có thẩm quyền về bất kỳ sự cố bảo mật nào.                                                                                                                                                                                                                                   |
| <b>Singapore</b> | 1. Luật An ninh Mạng                                                                                                          | 2018 | Luật An ninh Mạng là đạo luật chính của Singapore về bảo vệ an ninh mạng quốc gia. Đạo                                                                                                                                                                                                                                                                                                                                                                                                               |

|  |                                                                                         |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--|-----------------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | (Cybersecurity Act)                                                                     |          | luật này thiết lập một khung pháp lý để bảo vệ các hệ thống thông tin quan trọng (Critical Information Infrastructure - CII) và cung cấp các quy định về giám sát và phản ứng đối với các sự cố an ninh mạng. Quy định việc bảo vệ các cơ sở hạ tầng quan trọng của quốc gia như năng lượng, giao thông, viễn thông và tài chính. Các tổ chức sở hữu cơ sở hạ tầng quan trọng phải thực hiện các biện pháp bảo vệ an ninh mạng và thông báo về các sự cố an ninh mạng. Tạo ra Cơ quan An ninh Mạng Singapore (CSA), cơ quan đầu mối về an ninh mạng, có trách nhiệm giám sát và phản ứng với các sự cố an ninh mạng. |
|  | 2. Luật Bảo vệ Dữ Liệu Cá Nhân (Personal Data Protection Act - PDPA)                    | 2020     | PDPA là đạo luật bảo vệ quyền riêng tư của người dân Singapore trong môi trường số. Đạo luật này quy định về cách thức thu thập, sử dụng và lưu trữ dữ liệu cá nhân, nhằm bảo đảm rằng các tổ chức có trách nhiệm bảo vệ dữ liệu cá nhân khỏi các mối đe dọa bảo mật. Yêu cầu các tổ chức phải có sự đồng ý của người dùng trước khi thu thập và xử lý dữ liệu cá nhân. Đạo luật yêu cầu các tổ chức phải bảo đảm an ninh dữ liệu cá nhân và thông báo về bất kỳ vi phạm bảo mật dữ liệu nào.                                                                                                                        |
|  | 3. Luật Về Tội Phạm Mạng (Computer Misuse Act - CMA)                                    | Cập nhật | CMA là đạo luật quy định về các hành vi tội phạm mạng tại Singapore, bao gồm việc xâm nhập trái phép vào các hệ thống máy tính, phát tán virus và gian lận qua mạng. Định nghĩa và hình sự hóa các hành vi như xâm nhập trái phép vào hệ thống máy tính, đánh cắp thông tin và phát tán phần mềm độc hại. Các tội phạm mạng nghiêm trọng có thể bị xử lý hình sự, bao gồm các hình phạt tiền và tù giam.                                                                                                                                                                                                             |
|  | 4. Chỉ thị về Quản lý An ninh Thông tin (Information Security Management Act)           | 2016     | Chỉ thị này quy định về việc thiết lập và duy trì các tiêu chuẩn bảo mật thông tin tại các cơ quan chính phủ và các tổ chức cung cấp dịch vụ quan trọng. Yêu cầu các cơ quan chính phủ và các tổ chức phải thực hiện các biện pháp bảo mật thông tin chặt chẽ. Đề ra các biện pháp phòng ngừa, phát hiện và ứng phó với các sự cố an ninh mạng.                                                                                                                                                                                                                                                                      |
|  | 5. Luật về Quản lý Thông tin và Giao dịch Điện tử (Electronic Transactions Act - ETA)   | 2010     | Luật này tạo ra khung pháp lý cho các giao dịch điện tử tại Singapore, đặc biệt là các giao dịch thương mại và tài chính trực tuyến. Quy định về việc ký kết và công nhận các giao dịch điện tử hợp pháp, bao gồm các hợp đồng điện tử và chữ ký điện tử. Bảo đảm rằng các giao dịch trực tuyến được thực hiện một cách an toàn và bảo mật.                                                                                                                                                                                                                                                                          |
|  | 6. Chỉ thị về Giám sát và Kiểm soát An ninh Mạng (Cybersecurity Strategy)               | 2016     | Đây là một chiến lược quốc gia dài hạn của Singapore để nâng cao năng lực bảo vệ an ninh mạng và bảo đảm sự ổn định của hạ tầng số. Chiến lược này nhằm xây dựng một môi trường an toàn và đáng tin cậy cho các dịch vụ trực tuyến và các giao dịch điện tử tại Singapore. Đề ra các biện pháp để đối phó với các mối đe dọa an ninh mạng và tăng cường hợp tác quốc tế trong việc bảo vệ không gian mạng.                                                                                                                                                                                                           |
|  | 7. Chỉ thị về Quản lý và Bảo vệ Hạ tầng Kỹ thuật số (Digital Infrastructure Protection) | Cập nhật | Quy định về bảo vệ các hạ tầng kỹ thuật số quan trọng của quốc gia, bao gồm mạng viễn thông, dịch vụ tài chính và các cơ sở hạ tầng công nghệ thông tin. Các tổ chức phải triển khai các biện pháp bảo mật mạnh mẽ để bảo vệ hệ thống mạng khỏi các tấn công mạng và bảo đảm sự ổn định của các dịch vụ kỹ thuật số.                                                                                                                                                                                                                                                                                                 |

**Phụ lục 4. DANH MỤC CÁC LUẬT CHUYÊN NGÀNH CÓ ĐỀ CẬP ĐẾN NỘI DUNG VỀ  
AN NINH MẠNG Ở VIỆT NAM**

| TT | Tên gọi/ Thời gian ban hành    | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Luật an ninh quốc gia năm 2004 | <p>Luật an ninh Quốc gia 2004 số 32/2004/QH11 không sử dụng trực tiếp thuật ngữ “an ninh mạng”. Tuy nhiên, luật này bao gồm nhiều nội dung liên quan đến việc bảo vệ thông tin, hệ thống thông tin và các hoạt động trên không gian mạng, vốn là những khía cạnh quan trọng của an ninh mạng</p> <p>Dưới đây là các nội dung liên quan đến vấn đề an ninh mạng được quy định trong luật:</p> <p>1. Định nghĩa về hoạt động xâm phạm an ninh quốc gia: “Hoạt động xâm phạm an ninh quốc gia là những hành vi xâm phạm chế độ chính trị, chế độ kinh tế, nền văn hoá, an ninh, quốc phòng, đối ngoại, độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của nước Cộng hoà xã hội chủ nghĩa Việt Nam”. Các hành vi này có thể bao gồm cả những hoạt động được thực hiện qua không gian mạng.</p> <p>2. Các hành vi bị nghiêm cấm:</p> <ul style="list-style-type: none"> <li>- Thu thập, tàng trữ, vận chuyển, mua bán, sử dụng, tiết lộ, cung cấp, tán phát trái phép tin tức, tài liệu, vật phẩm thuộc bí mật nhà nước. Điều này liên quan trực tiếp đến bảo mật thông tin, bao gồm cả thông tin kỹ thuật số.</li> <li>- Tổ chức, hoạt động, câu kết, xúi giục, khống chế, kích động, mua chuộc, lừa gạt, lôi kéo người khác nhằm chống chính quyền nhân dân, xóa bỏ vai trò lãnh đạo của Đảng Cộng sản Việt Nam, chia cắt đất nước, phá hoại khối đại đoàn kết toàn dân tộc. Các hành vi này có thể được thực hiện thông qua các phương tiện truyền thông và mạng máy tính.</li> <li>- Tham gia, giúp sức, cung cấp tài chính, vũ khí, phương tiện cho các tổ chức, cá nhân hoạt động xâm phạm an ninh quốc gia. “Phương tiện” ở đây có thể bao gồm cả phương tiện điện tử, công nghệ thông tin.</li> </ul> <p>3. Nhiệm vụ bảo vệ an ninh quốc gia: Bao gồm việc bảo vệ bí mật nhà nước và các mục tiêu quan trọng về an ninh quốc gia. Điều này đòi hỏi các biện pháp bảo mật thông tin toàn diện, trong đó có an ninh mạng.</p> <p>4. Các biện pháp cơ bản bảo vệ an ninh quốc gia: Bao gồm biện pháp khoa học - kỹ thuật và nghiệp vụ, có thể được áp dụng trong lĩnh vực an ninh mạng để phòng ngừa, phát hiện và đấu tranh với các</p> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>hoạt động xâm phạm.</p> <p>Áp dụng một số biện pháp cần thiết khi có nguy cơ đe dọa an ninh quốc gia nhưng chưa đến mức ban bố tình trạng khẩn cấp: Thủ tướng Chính phủ có thể quyết định áp dụng các biện pháp như:</p> <p>Kiểm soát việc sử dụng các phương tiện thông tin liên lạc tại một địa phương hay khu vực nhất định. Đây là biện pháp trực tiếp liên quan đến kiểm soát hạ tầng và dịch vụ truyền thông, có vai trò quan trọng trong an ninh mạng.</p> <p>6. Quyền hạn của cơ quan chuyên trách bảo vệ an ninh quốc gia: Để thực hiện nhiệm vụ bảo vệ an ninh quốc gia, các cơ quan này được quyền:</p> <ul style="list-style-type: none"> <li>- Yêu cầu cơ quan, tổ chức, cá nhân cung cấp thông tin, tài liệu, đồ vật khi có căn cứ xác định liên quan đến hoạt động xâm phạm an ninh quốc gia.</li> <li>- Yêu cầu cơ quan, tổ chức bưu chính, viễn thông kiểm tra thư tín, điện tín, bưu phẩm, bưu kiện có thông tin, tài liệu, vật phẩm có nguy hại cho an ninh quốc gia.</li> <li>- Kiểm tra phương tiện thông tin, máy tính, mạng máy tính, đồ vật, tài liệu, hàng hoá, chỗ ở, nơi làm việc hoặc các cơ sở khác của cơ quan, tổ chức, cá nhân khi có căn cứ xác định liên quan đến hoạt động xâm phạm an ninh quốc gia. Đây là quy định trực tiếp nhất đề cập đến “máy tính” và “mạng máy tính”, cho phép cơ quan chuyên trách kiểm soát và can thiệp vào các hệ thống này để bảo vệ an ninh quốc gia.</li> <li>- Tạm đình chỉ hoặc đình chỉ việc sử dụng phương tiện thông tin liên lạc hoặc các hoạt động khác trên lãnh thổ Việt Nam khi có căn cứ xác định các hoạt động này gây nguy hại cho an ninh quốc gia. Quy định này cho phép kiểm soát và ngừng các hoạt động gây nguy hại được thực hiện qua các phương tiện thông tin liên lạc, bao gồm cả mạng internet.</li> </ul> <p>7. Chế độ quản lý thông tin, tài liệu, đồ vật về bảo vệ an ninh quốc gia: Thông tin, tài liệu, đồ vật liên quan đến cơ quan chuyên trách bảo vệ an ninh quốc gia hoặc do cơ quan này thu thập được thuộc bí mật nhà nước và được quản lý theo quy định của pháp luật về bảo vệ bí mật nhà nước. Điều này nhấn mạnh tầm quan trọng của việc bảo vệ dữ liệu và thông tin, một thành phần cốt lõi của an ninh mạng.</p> <p>8. Nội dung quản lý nhà nước về an ninh quốc gia: Bao gồm việc tổ chức, chỉ đạo, hướng dẫn hoạt động thu thập, phát hiện, điều tra, xử lý thông tin, tài liệu, hành vi liên quan đến hoạt động xâm phạm</p> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | an ninh quốc gia. Điều này cũng ngụ ý đến việc quản lý thông tin và các hành vi trên không gian số.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 2. | Luật Công nghệ cao năm 2008 | <p>1. Chính sách của Nhà nước đối với hoạt động công nghệ cao liên quan đến quốc phòng, an ninh:</p> <ul style="list-style-type: none"> <li>- Luật quy định Nhà nước huy động nguồn lực đầu tư, áp dụng cơ chế khuyến khích, ưu đãi để phát huy vai trò chủ đạo của công nghệ cao trong phát triển khoa học và công nghệ phục vụ phát triển kinh tế - xã hội, quốc phòng, an ninh, bảo vệ môi trường và nâng cao chất lượng cuộc sống của nhân dân.</li> <li>- Ngân sách nhà nước được dành và cơ chế tài chính đặc thù được áp dụng để thực hiện các nhiệm vụ, chương trình, dự án về công nghệ cao, cũng như nhập khẩu một số công nghệ cao có ý nghĩa quan trọng đối với phát triển kinh tế - xã hội, quốc phòng, an ninh.</li> <li>- Việc nghiên cứu và phát triển công nghệ cao được Nhà nước khuyến khích nhằm phục vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh và bảo vệ môi trường.</li> <li>- Các dự án nhập khẩu công nghệ cao, máy móc, thiết bị công nghệ cao trong nước chưa tạo ra được để thực hiện dự án quan trọng về kinh tế - xã hội, quốc phòng, an ninh cũng được Nhà nước dành kinh phí.</li> </ul> <p>2. Các lĩnh vực công nghệ cao được ưu tiên đầu tư phát triển liên quan trực tiếp đến an ninh mạng:</p> <ul style="list-style-type: none"> <li>- Luật quy định Nhà nước tập trung đầu tư phát triển công nghệ cao trong các lĩnh vực, trong đó có Công nghệ thông tin. Phát triển Công nghệ thông tin là nền tảng cốt lõi của an ninh mạng.</li> <li>- Chính phủ có thể điều chỉnh, bổ sung lĩnh vực công nghệ cần tập trung đầu tư phát triển công nghệ cao căn cứ vào nhu cầu phát triển kinh tế - xã hội, quốc phòng, an ninh.</li> <li>- Công nghệ cao được ưu tiên đầu tư phải có tác động mạnh và mang lại hiệu quả lớn đối với sự phát triển của các ngành, lĩnh vực kinh tế - xã hội, quốc phòng, an ninh.</li> </ul> <p>3. Các hành vi bị nghiêm cấm liên quan đến an ninh mạng:</p> <ul style="list-style-type: none"> <li>- Lợi dụng hoạt động công nghệ cao gây phương hại đến lợi ích quốc gia, quốc phòng, an ninh, quyền và lợi ích hợp pháp của tổ chức, cá nhân là hành vi bị nghiêm cấm. Điều này bao hàm các hành vi tấn công mạng, phá hoại hệ thống thông tin hoặc các hoạt động mạng khác gây hại đến an ninh quốc gia.</li> <li>- Tiết lộ, cung cấp trái pháp luật bí mật về công nghệ cao là một hành vi bị nghiêm cấm. Quy định này trực tiếp bảo vệ tính bảo mật của thông tin công nghệ cao, một khía cạnh quan trọng của an ninh mạng.</li> </ul> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>4. Phát triển hạ tầng thông tin và cơ sở dữ liệu công nghệ cao:<br/> Nhà nước khuyến khích đầu tư xây dựng cơ sở hạ tầng kỹ thuật công nghệ cao, bao gồm cả hạ tầng thông tin, để đáp ứng yêu cầu phát triển công nghệ cao.<br/> Bộ Khoa học và Công nghệ có trách nhiệm chủ trì phối hợp với các bộ, cơ quan ngang bộ xây dựng cơ sở dữ liệu, hạ tầng thông tin về công nghệ cao; tạo điều kiện thuận lợi cho tổ chức, cá nhân tiếp cận, sử dụng, trao đổi thông tin về công nghệ cao. Việc xây dựng và quản lý hạ tầng thông tin, cơ sở dữ liệu này đòi hỏi phải bảo đảm an toàn, an ninh.<br/> Nhà nước cũng hỗ trợ xây dựng hạ tầng thông tin trong khu công nghệ cao, khu nông nghiệp ứng dụng công nghệ cao.</p> <p>5. Phát triển nhân lực công nghệ cao:<br/> Phát triển nhân lực công nghệ cao được coi là một nhiệm vụ trọng tâm của hệ thống giáo dục và đào tạo quốc gia, nhằm đáp ứng yêu cầu phát triển công nghệ cao. Mặc dù không nêu cụ thể là nhân lực an ninh mạng, nhưng những người có trình độ và kỹ năng về công nghệ cao sẽ đóng vai trò quan trọng trong việc bảo đảm an ninh cho các hệ thống và hoạt động công nghệ.</p> |
| 3. | Luật Bưu chính năm 2010     | <p>1. Bảo đảm an ninh, an toàn là nguyên tắc cốt lõi: Hoạt động bưu chính phải luôn bảo đảm an ninh, an toàn trong cung ứng và sử dụng dịch vụ. Đặc biệt, bí mật thư phải được bảo đảm theo quy định của pháp luật. Ngành bưu chính được xây dựng và phát triển cũng nhằm mục đích bảo đảm quốc phòng, an ninh.</p> <p>2. Nghiêm cấm các hành vi gây mất an ninh, an toàn:<br/> - Cấm gửi, chấp nhận, vận chuyển, phát bưu gửi có nội dung kích động, gây mất an ninh, chống phá Nhà nước hoặc gây mất trật tự, an toàn xã hội (ví dụ: chứa vũ khí, chất nổ, ma túy, vi trùng dịch bệnh).<br/> - Cấm tiết lộ thông tin về sử dụng dịch vụ bưu chính, bóc mở, hủy bưu gửi trái pháp luật.<br/> - Cấm xâm hại công trình bưu chính công cộng và cản trở hoạt động bưu chính hợp pháp, cũng như các loại tem có nội dung chống phá Nhà nước.</p> <p>3. Cơ chế bảo đảm an ninh trong hoạt động bưu chính:<br/> - Bưu gửi được bảo đảm an toàn từ khi chấp nhận đến khi phát.</p>                                                                                                                                                                          |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <ul style="list-style-type: none"> <li>- Doanh nghiệp cung ứng dịch vụ bưu chính có trách nhiệm đình chỉ vận chuyển, phát bưu gửi nếu phát hiện vi phạm quy định cấm và thông báo cho cơ quan chức năng để xử lý.</li> <li>- Cơ quan nhà nước có thẩm quyền có quyền tạm đình chỉ, kiểm tra, xử lý bưu gửi hoặc yêu cầu cung cấp thông tin về sử dụng dịch vụ bưu chính khi có căn cứ liên quan đến an ninh quốc gia hoặc vụ án hình sự. Việc này phải có văn bản yêu cầu và lập biên bản rõ ràng.</li> <li>- Nghiêm cấm lợi dụng việc kiểm tra, xử lý bưu gửi để gây thiệt hại.</li> </ul> <p>4. Trách nhiệm của doanh nghiệp và người sử dụng:</p> <ul style="list-style-type: none"> <li>- Doanh nghiệp phải có biện pháp bảo đảm an ninh thông tin và an toàn đối với con người, bưu gửi, mạng bưu chính để được cấp phép.</li> <li>- Doanh nghiệp bị thu hồi giấy phép nếu hoạt động chống lại Nhà nước, gây phương hại đến an ninh quốc gia, trật tự và an toàn xã hội.</li> <li>- Doanh nghiệp không được tiết lộ thông tin về sử dụng dịch vụ bưu chính của khách hàng, trừ trường hợp phục vụ mục đích an ninh theo yêu cầu của cơ quan nhà nước.</li> <li>- Người sử dụng dịch vụ bưu chính được bảo đảm an toàn và an ninh thông tin và có nghĩa vụ thực hiện các quy định về an toàn, an ninh đối với bưu gửi của mình.</li> </ul> <p>5. Mạng bưu chính chuyên biệt: Có sự tồn tại của mạng bưu chính phục vụ cơ quan Đảng, Nhà nước, quốc phòng, an ninh hoạt động không vì mục đích kinh doanh và chỉ được kết nối với mạng bưu chính công cộng để bảo đảm tính biệt lập và an toàn.</p> <p>6. Trách nhiệm quản lý nhà nước: Bộ Thông tin và Truyền thông phối hợp chặt chẽ với Bộ Công an và Bộ Quốc phòng để quy định về nguyên tắc, điều kiện xử lý các vấn đề liên quan đến an ninh bưu chính và xây dựng mạng bưu chính phục vụ mục đích an ninh, quốc phòng.</p> |
| 4. | Luật Cơ yếu năm 2011        | <p>1. Bảo vệ thông tin bí mật nhà nước là mục tiêu tối thượng: Hoạt động cơ yếu là một hoạt động cơ mật đặc biệt, thuộc lĩnh vực an ninh quốc gia, nhằm bảo vệ thông tin bí mật nhà nước. Mọi hoạt động phải bảo đảm tính tuyệt đối bí mật, an toàn, chính xác và kịp thời.</p> <p>2. Mã hóa thông tin bí mật nhà nước là bắt buộc:</p> <ul style="list-style-type: none"> <li>- Tất cả thông tin bí mật nhà nước khi được truyền qua các phương tiện thông tin, viễn thông bắt buộc phải được mã hóa bằng mật mã của cơ yếu.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>- Thông tin bí mật nhà nước được lưu giữ trong các thiết bị điện tử, tin học và trên mạng viễn thông cũng phải được mã hóa bằng mật mã của cơ yếu. Đây là biện pháp nền tảng để bảo đảm tính bảo mật và toàn vẹn của dữ liệu trong môi trường số.</p> <p>3. Nhà nước độc quyền và kiểm soát chặt chẽ sản phẩm mật mã:</p> <p>- Nhà nước có độc quyền trong việc sản xuất và cung cấp sản phẩm mật mã để bảo vệ thông tin bí mật nhà nước.</p> <p>- Ban Cơ yếu Chính phủ là cơ quan mật mã quốc gia, chịu trách nhiệm xây dựng kế hoạch, tổ chức sản xuất, cung cấp và trực tiếp quản lý các cơ sở sản xuất mật mã.</p> <p>- Nghiêm cấm sử dụng bất kỳ sản phẩm mật mã nào không do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin bí mật nhà nước, nhằm bảo đảm tính tin cậy và kiểm soát tuyệt đối các công cụ bảo mật quốc gia.</p> <p>4. Nghiêm cấm các hành vi gây mất an toàn thông tin và lợi dụng mật mã:</p> <p>- Luật nghiêm cấm các hành vi như tiết lộ bí mật nhà nước hoặc bí mật công tác trong hoạt động cơ yếu.</p> <p>- Cấm truyền thông tin bí mật nhà nước qua các phương tiện mà không mã hóa.</p> <p>- Cấm nghiên cứu, sản xuất, sử dụng, thu thập hoặc tiêu hủy sản phẩm mật mã của cơ yếu trái pháp luật.</p> <p>- Cấm cố ý làm hư hỏng hoặc chiếm đoạt sản phẩm mật mã và cản trở hoạt động cơ yếu trái pháp luật.</p> <p>5. Quản lý chặt chẽ hạ tầng và nghiệp vụ mật mã:</p> <p>- Sản phẩm mật mã phải tuân thủ quy chuẩn kỹ thuật và được kiểm định, đánh giá kỹ lưỡng trước khi đưa vào sử dụng.</p> <p>- Việc quản lý và sử dụng sản phẩm mật mã phải được thực hiện một cách thống nhất, chặt chẽ, tuân thủ các quy định về nghiệp vụ và quy trình sử dụng.</p> <p>- Mạng liên lạc cơ yếu được triển khai dựa trên nhu cầu bảo vệ thông tin bí mật nhà nước và phải bảo đảm các điều kiện về nhân lực, kỹ thuật, cũng như an ninh và an toàn chặt chẽ.</p> <p>6. Vai trò và trách nhiệm của lực lượng cơ yếu:</p> <p>- Lực lượng cơ yếu là lực lượng chuyên trách bảo vệ bí mật nhà nước, có nhiệm vụ chủ động phòng</p> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>ngừa và tham gia đấu tranh với các hoạt động thám mã (giải mã trái phép) gây phương hại đến an ninh quốc gia.</p> <ul style="list-style-type: none"> <li>- Ban Cơ yếu Chính phủ có trách nhiệm thống nhất quản lý, xây dựng và bảo đảm tính sẵn sàng của hệ thống mạng liên lạc cơ yếu và lực lượng dự bị, nguồn dự trữ sản phẩm mật mã để ứng phó hiệu quả trong mọi tình huống.</li> <li>- Người làm công tác cơ yếu có nghĩa vụ giữ bí mật thông tin bí mật nhà nước và bí mật công tác cơ yếu, ngay cả khi đã thôi làm việc.</li> </ul> <p>7. Biện pháp ứng phó khẩn cấp: Trong trường hợp khẩn cấp, nguy hiểm mà không còn biện pháp nào khác để bảo đảm an toàn mật mã, các cơ quan, tổ chức, cá nhân sử dụng sản phẩm mật mã phải thực hiện ngay biện pháp tiêu hủy để ngăn chặn thông tin rơi vào tay kẻ xấu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 5. | Luật quảng cáo năm 2012     | <p>1. Nghiêm cấm quảng cáo làm phương hại đến an ninh quốc gia: Đây là quy định cốt lõi liên quan trực tiếp đến an ninh. Luật cấm tuyệt đối các hành vi quảng cáo làm tiết lộ bí mật nhà nước, gây phương hại đến độc lập, chủ quyền quốc gia, an ninh và quốc phòng. Quy định này áp dụng cho mọi hình thức quảng cáo, bao gồm cả quảng cáo trên các phương tiện điện tử và trang thông tin điện tử, qua đó gián tiếp bảo vệ an ninh thông tin ở cấp độ quốc gia.</p> <p>2. Kiểm soát nội dung và hình thức quảng cáo trên phương tiện điện tử: Luật có các quy định cụ thể để quản lý hoạt động quảng cáo trên báo điện tử, trang thông tin điện tử, thiết bị điện tử, thiết bị đầu cuối và các thiết bị viễn thông khác.</p> <ul style="list-style-type: none"> <li>- Minh bạch thông tin: Quảng cáo trên báo điện tử không được thiết kế, bố trí lẫn vào phần nội dung tin tức, giúp người đọc dễ dàng phân biệt và tránh nhầm lẫn.</li> <li>- Kiểm soát tin nhắn và thư điện tử quảng cáo: Tổ chức, cá nhân chỉ được gửi tin nhắn hoặc thư điện tử quảng cáo khi có sự đồng ý trước của người nhận. Có giới hạn về thời gian gửi (từ 7 giờ đến 22 giờ) và số lượng (không quá ba tin nhắn hoặc thư điện tử đến một số điện thoại/địa chỉ trong vòng 24 giờ, trừ khi có thỏa thuận khác). Quan trọng hơn, người quảng cáo phải bảo đảm người nhận có khả năng từ chối quảng cáo và phải chấm dứt ngay việc gửi nếu nhận được thông báo từ chối, không được thu phí dịch vụ cho việc từ chối này. Các quy định này nhằm bảo vệ người dùng khỏi sự phiền nhiễu và bảo đảm trải nghiệm thông tin lành mạnh trên không gian mạng.</li> </ul> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>3. Chống quảng cáo vi phạm pháp luật sở hữu trí tuệ: Luật nghiêm cấm hành vi quảng cáo vi phạm pháp luật về sở hữu trí tuệ. Điều này góp phần bảo vệ quyền tài sản và lợi ích hợp pháp của các tổ chức, cá nhân trên môi trường số, bao gồm cả các tài sản số.</p> <p>4. Bảo đảm trật tự, an toàn xã hội và thuần phong mỹ tục: Các hành vi quảng cáo thiếu thẩm mỹ, trái với truyền thống lịch sử, văn hóa, đạo đức, thuần phong mỹ tục Việt Nam hoặc làm ảnh hưởng đến mỹ quan đô thị, trật tự an toàn giao thông, an toàn xã hội đều bị cấm. Mặc dù không trực tiếp là các biện pháp kỹ thuật an ninh mạng, nhưng những quy định này giúp tạo dựng một không gian quảng cáo (bao gồm cả không gian số) lành mạnh, an toàn và có trật tự.</p> <p>5. Trách nhiệm quản lý nhà nước: Chính phủ, Bộ Văn hóa, Thể thao và Du lịch, cùng các Bộ, cơ quan ngang Bộ và Ủy ban nhân dân các cấp có trách nhiệm thống nhất quản lý nhà nước về hoạt động quảng cáo. Điều này bao gồm cả việc ban hành và tổ chức thực hiện các văn bản quy phạm pháp luật, thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm trong hoạt động quảng cáo, qua đó gián tiếp quản lý và giảm thiểu các rủi ro phát sinh từ quảng cáo trên môi trường số.</p>                                    |
| 6. | Bộ luật Dân sự năm 2015     | <p>1. Bảo vệ an ninh quốc gia và lợi ích công cộng: Bộ luật quy định rằng các quyền dân sự chỉ có thể bị hạn chế trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội và lợi ích công cộng. Việc xác lập, thực hiện các quyền và nghĩa vụ dân sự không được xâm phạm đến lợi ích quốc gia, dân tộc, lợi ích công cộng, cũng như quyền và lợi ích hợp pháp của người khác. Điều này tạo cơ sở pháp lý rộng để kiểm soát các hành vi trên không gian mạng nếu chúng gây tổn hại đến an ninh quốc gia hay lợi ích công cộng.</p> <p>2. Bảo vệ quyền riêng tư cá nhân và bí mật thông tin:</p> <ul style="list-style-type: none"> <li>- Đời sống riêng tư, bí mật cá nhân và bí mật gia đình được pháp luật bảo vệ và là bất khả xâm phạm.</li> <li>- Việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến đời sống riêng tư, bí mật cá nhân hoặc bí mật gia đình phải được sự đồng ý của cá nhân hoặc các thành viên gia đình, trừ trường hợp luật có quy định khác.</li> <li>- Thư tín, điện thoại, điện tín, cơ sở dữ liệu điện tử và các hình thức trao đổi thông tin riêng tư khác của cá nhân được bảo đảm an toàn và bí mật. Việc kiểm soát hay thu giữ các thông tin này chỉ được thực hiện khi có quy định của luật.</li> </ul> |

| TT | Tên gọi/ Thời gian ban hành                        | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                                    | <p>- Các bên trong hợp đồng không được tiết lộ thông tin bí mật mà họ biết được trong quá trình giao kết, thực hiện hợp đồng.</p> <p>3. Ghi nhận giá trị pháp lý của giao dịch dân sự điện tử: Bộ luật công nhận giao dịch dân sự được thực hiện thông qua phương tiện điện tử dưới hình thức thông điệp dữ liệu có giá trị tương đương giao dịch bằng văn bản. Điều này khẳng định tính hợp pháp của các giao dịch trong môi trường số, đồng thời đặt ra yêu cầu về tính toàn vẹn và xác thực của thông tin điện tử.</p> <p>4. Bảo vệ danh dự, nhân phẩm, uy tín cá nhân: Cá nhân có quyền yêu cầu Tòa án bác bỏ thông tin làm ảnh hưởng xấu đến danh dự, nhân phẩm, uy tín của mình. Thông tin ảnh hưởng xấu được đăng tải trên phương tiện thông tin đại chúng phải được gỡ bỏ, cải chính. Quy định này đặc biệt quan trọng trong bối cảnh thông tin lan truyền nhanh chóng trên không gian mạng, giúp chống lại các hành vi phỉ báng, vu khống trực tuyến.</p> <p>5. Bảo vệ quyền sở hữu trí tuệ: Bộ luật công nhận quyền tài sản bao gồm cả quyền tài sản đối với đối tượng quyền sở hữu trí tuệ. Người tiến hành hoạt động sáng tạo có quyền sở hữu đối với tài sản có được từ hoạt động sáng tạo theo quy định của Luật sở hữu trí tuệ. Việc bảo vệ quyền sở hữu trí tuệ, đặc biệt là đối với các tài sản số, là một yếu tố quan trọng của an ninh mạng.</p> <p>6. Trách nhiệm bồi thường thiệt hại do vi phạm nghĩa vụ và hành vi trái pháp luật: Người nào có hành vi xâm phạm quyền, lợi ích hợp pháp của người khác mà gây thiệt hại thì phải bồi thường. Thiệt hại có thể bao gồm thiệt hại về vật chất (tổn thất tài sản, chi phí khắc phục) và thiệt hại về tinh thần (do xâm phạm danh dự, nhân phẩm, uy tín). Điều này tạo cơ sở pháp lý để xử lý và yêu cầu bồi thường nếu có thiệt hại phát sinh từ các hành vi vi phạm an toàn thông tin hoặc xâm phạm dữ liệu trên không gian mạng.</p> |
| 7. | Bộ luật Hình sự năm 2015 sửa đổi, bổ sung năm 2017 | <p>1. Chống lại các hành vi tấn công, gây rối loạn và xâm nhập trái phép vào hệ thống mạng:</p> <ul style="list-style-type: none"> <li>- Tội phạm hóa việc sản xuất, mua bán, trao đổi hoặc tặng cho các công cụ, thiết bị, phần mềm được thiết kế để tấn công mạng máy tính, mạng viễn thông hoặc phương tiện điện tử với mục đích trái pháp luật.</li> <li>- Nghiêm cấm hành vi cố ý phát tán các chương trình tin học gây hại (như virus, mã độc) ảnh hưởng đến hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>- Quy định rõ các tội danh liên quan đến việc cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử, bao gồm việc tự ý xóa, làm tổn hại, thay đổi phần mềm, dữ liệu điện tử, hoặc ngăn chặn trái phép việc truyền tải dữ liệu.</p> <p>- Tội phạm xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử, bao gồm vượt qua các lớp bảo vệ, chiếm quyền điều khiển, can thiệp vào chức năng, lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép dịch vụ.</p> <p>2. Bảo vệ thông tin và dữ liệu cá nhân, tổ chức trên không gian mạng:</p> <p>- Hình sự hóa hành vi đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, đặc biệt là thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân mà không được phép của chủ sở hữu.</p> <p>- Quy định tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng của người khác.</p> <p>- Các hành vi xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín, bao gồm cả việc cố ý làm hư hỏng, thất lạc, lấy cắp thông tin trong cơ sở dữ liệu điện tử hoặc các hình thức trao đổi thông tin riêng tư khác qua mạng viễn thông, đều bị xử lý.</p> <p>3. Xử lý các tội phạm liên quan đến việc sử dụng công nghệ thông tin để thực hiện các hành vi phạm tội khác:</p> <p>- Luật có các điều khoản quy định tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử để thực hiện hành vi chiếm đoạt tài sản, như lừa đảo trong thương mại điện tử, thanh toán điện tử, kinh doanh đa cấp, hoặc truy cập bất hợp pháp tài khoản.</p> <p>- Nó cũng bao gồm các tội danh mà hành vi phạm tội được thực hiện thông qua việc sử dụng mạng máy tính hoặc mạng viễn thông, phương tiện điện tử để làm nhục, vu khống hoặc tổ chức đánh bạc.</p> <p>4. Chống khủng bố trên không gian mạng:</p> <p>Hành vi tấn công, xâm hại, cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử của cơ quan, tổ chức, cá nhân nếu nhằm chống chính quyền nhân dân hoặc gây ra tình trạng hoảng sợ trong công chúng, được coi là hành vi khủng bố và bị xử lý nghiêm khắc.</p> <p>5. Trách nhiệm hình sự của pháp nhân thương mại:</p> <p>Bộ luật quy định rõ trách nhiệm hình sự của các pháp nhân thương mại đối với một số tội danh, trong</p> |

| TT | Tên gọi/ Thời gian ban hành          | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                      | <p>đó có nhiều tội liên quan đến công nghệ thông tin và tài chính số, như cố ý công bố thông tin sai lệch hoặc che giấu thông tin trong hoạt động chứng khoán, sử dụng thông tin nội bộ để mua bán chứng khoán, thao túng thị trường chứng khoán, hoặc rửa tiền.</p> <p>6. Bảo vệ bí mật nhà nước và công tác trong môi trường số:<br/> Các hành vi cố ý hoặc vô ý làm lộ bí mật nhà nước, chiếm đoạt, mua bán, tiêu hủy vật hoặc tài liệu bí mật nhà nước hoặc bí mật công tác, có thể liên quan đến các tài liệu dưới dạng số hóa và các hệ thống lưu trữ điện tử.</p> <p>7. Kiểm soát việc sử dụng tần số vô tuyến điện:<br/> Quy định tội sử dụng trái phép tần số vô tuyến điện dành riêng cho các mục đích cấp cứu, an toàn, quốc phòng, an ninh và tội cố ý gây nhiễu có hại, cản trở hoạt động bình thường của hệ thống thông tin vô tuyến điện.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 8. | Luật Bảo vệ bí mật nhà nước năm 2018 | <p>1. Nghiêm cấm các hành vi sử dụng trái phép công nghệ thông tin để xử lý bí mật nhà nước: Luật nghiêm cấm việc soạn thảo, lưu giữ tài liệu có chứa bí mật nhà nước trên các máy tính hoặc thiết bị kết nối với Internet, mạng máy tính, mạng viễn thông, trừ các trường hợp được phép theo quy định về cơ yếu. Đồng thời, việc truyền đưa bí mật nhà nước qua các phương tiện thông tin, viễn thông trái với quy định về cơ yếu cũng bị cấm. Đặc biệt, Luật cũng cấm việc chuyển đổi mục đích sử dụng các thiết bị đã từng chứa bí mật nhà nước mà chưa xóa bỏ nội dung mật và nghiêm cấm việc đăng tải, phát tán bí mật nhà nước trên các phương tiện thông tin đại chúng, Internet, mạng máy tính và mạng viễn thông. Các hành vi sử dụng thiết bị thu, phát tín hiệu, ghi âm, ghi hình trong các cuộc họp có nội dung bí mật nhà nước mà không được phép cũng bị cấm.</p> <p>2. Xác định thông tin về an ninh mạng là bí mật nhà nước: Luật quy định rõ các thông tin trong lĩnh vực thông tin và truyền thông có thể được coi là bí mật nhà nước. Điều này bao gồm chiến lược, kế hoạch, đề án phát triển các hạ tầng và công nghệ liên quan đến an toàn thông tin mạng phục vụ quốc phòng, an ninh. Ngoài ra, thiết kế kỹ thuật, sơ đồ, số liệu về thiết bị của hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quan trọng quốc gia và hệ thống mạng thông tin dùng riêng của các cơ quan Đảng, Nhà nước cũng được xem là bí mật nhà nước.</p> <p>3. Yêu cầu bảo vệ dữ liệu mật trên thiết bị số: Bí mật nhà nước được chứa trong các thiết bị có tính</p> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>năng lưu giữ, sao, chụp phải được bảo vệ bằng các biện pháp thích hợp nhằm bảo đảm an toàn. Các tài liệu, vật chứa bí mật nhà nước phải được lưu giữ, bảo quản tại nơi an toàn và có phương án bảo vệ rõ ràng.</p> <p>4. Trách nhiệm của các cơ quan trong bảo vệ bí mật nhà nước trên không gian mạng:</p> <ul style="list-style-type: none"> <li>- Bộ Công an chịu trách nhiệm chính trong quản lý nhà nước về bảo vệ bí mật nhà nước, bao gồm cả việc phòng, chống vi phạm pháp luật trong lĩnh vực này.</li> <li>- Ban Cơ yếu Chính phủ có vai trò quan trọng trong việc tham mưu xây dựng và phát triển hệ thống thông tin mật mã quốc gia, quản lý các hoạt động nghiên cứu, sản xuất, cung cấp và sử dụng sản phẩm mật mã để bảo vệ thông tin bí mật nhà nước. Điều này trực tiếp liên quan đến việc bảo mật thông tin trong môi trường kỹ thuật số thông qua các biện pháp mã hóa và an toàn thông tin.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 9. | Luật Chứng khoán năm 2019   | <p>1. Nguyên tắc và Chính sách Chung về An toàn Thị trường: Nhà nước có chính sách quản lý và giám sát để bảo đảm thị trường chứng khoán hoạt động công bằng, công khai, minh bạch, an toàn và hiệu quả. Các hoạt động về chứng khoán phải tuân thủ nguyên tắc tôn trọng quyền sở hữu, quyền tự do giao dịch, đầu tư, kinh doanh nhưng đồng thời phải công bằng, công khai, minh bạch và bảo vệ quyền, lợi ích hợp pháp của nhà đầu tư. Nhà nước cũng có chính sách đầu tư hiện đại hóa cơ sở hạ tầng, công nghệ thông tin cho hoạt động của thị trường chứng khoán.</p> <p>2. Biện pháp bảo đảm an ninh, An toàn Thị trường Chứng khoán:</p> <ul style="list-style-type: none"> <li>- Luật quy định các biện pháp cụ thể bao gồm giám sát an ninh, an toàn thị trường chứng khoán [30a, 363a].</li> <li>- Ứng phó, khắc phục sự cố, sự kiện, biến động ảnh hưởng đến an toàn, ổn định và tính toàn vẹn của thị trường chứng khoán [30b, 363b].</li> <li>- Ủy ban Chứng khoán Nhà nước (SSC) có quyền tạm ngừng, đình chỉ giao dịch đối với một hoặc một số chứng khoán hoặc toàn bộ hoạt động giao dịch của Sở Giao dịch Chứng khoán Việt Nam (VSE) và Tổng công ty Lưu ký và Bù trừ Chứng khoán Việt Nam (VSDCC) khi có biến động bất thường hoặc để bảo vệ quyền lợi nhà đầu tư và bảo đảm ổn định, an toàn, tính toàn vẹn của thị trường [30c, 30d, 30đ, 152, 363c, 363d, 363dd, 470, 471].</li> <li>- Bên cạnh đó, còn có biện pháp phong tỏa tài khoản chứng khoán, yêu cầu người có thẩm quyền</li> </ul> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>phong tỏa tài khoản tiền liên quan đến vi phạm pháp luật về chứng khoán và thị trường chứng khoán [31g, 364g].</p> <p>3. Trách nhiệm của các Cơ quan Quản lý và Tổ chức Hoạt động Thị trường:</p> <ul style="list-style-type: none"> <li>- Ủy ban Chứng khoán Nhà nước (SSC) có nhiệm vụ hiện đại hóa công nghệ thông tin trong lĩnh vực chứng khoán và thị trường chứng khoán [38k, 370k]. Cán bộ, công chức, viên chức của SSC có trách nhiệm bảo đảm trung thực, bảo mật thông tin trong quá trình thực hiện nhiệm vụ.</li> <li>- Sở Giao dịch Chứng khoán Việt Nam (VSE) có nghĩa vụ bảo đảm hoạt động giao dịch chứng khoán trên thị trường được tiến hành công khai, công bằng, trật tự, an toàn và hiệu quả [143a, 464a]. VSE cũng phải báo cáo, kiến nghị SSC các biện pháp ứng phó, khắc phục sự cố, sự kiện, biến động ảnh hưởng đến an toàn, ổn định và tính toàn vẹn của thị trường giao dịch chứng khoán [144đ, 465dd]. Nhân viên của VSE phải tuân thủ quy định về bảo mật thông tin.</li> <li>- Tổng công ty Lưu ký và Bù trừ Chứng khoán Việt Nam (VSDCC) có nghĩa vụ bảo đảm cơ sở vật chất, kỹ thuật phục vụ cho các hoạt động đăng ký, lưu ký, bù trừ và thanh toán chứng khoán [164a, 480a], xây dựng quy trình hoạt động và quản lý rủi ro cho từng nghiệp vụ [165d, 481d] và có biện pháp bảo vệ cơ sở dữ liệu và lưu giữ các chứng từ gốc về đăng ký, lưu ký, bù trừ và thanh toán chứng khoán [165đ, 481dd]. VSDCC cũng phải bảo mật thông tin liên quan đến sở hữu của khách hàng [165g, 481g] và cán bộ, nhân viên phải tuân thủ quy định về bảo mật thông tin. VSDCC quản lý riêng biệt tài sản của khách hàng với tài sản của mình và tài sản của các quỹ hỗ trợ thanh toán, quỹ bù trừ, quỹ phòng ngừa rủi ro nghiệp vụ [166k, 482k].</li> <li>- Ngân hàng thanh toán được lựa chọn phải có hệ thống cơ sở vật chất, kỹ thuật bảo đảm thực hiện thanh toán giao dịch và kết nối với hệ thống của VSDCC [190đ, 502d], cũng như có hệ thống cơ sở vật chất, kỹ thuật để lưu giữ số liệu thông tin thanh toán giao dịch trong thời hạn ít nhất 10 năm và cung cấp cho SSC hoặc VSDCC trong 48 giờ khi có yêu cầu [190g, 502g].</li> </ul> <p>4. Nghĩa vụ của Công ty Chứng khoán và Công ty Quản lý Quỹ: Các công ty này phải thiết lập hệ thống kiểm soát nội bộ, quản trị rủi ro và giám sát, ngăn ngừa những xung đột lợi ích<sup>1112</sup>, xây dựng hệ thống công nghệ thông tin, cơ sở dữ liệu dự phòng để bảo đảm hoạt động an toàn và liên tục và không được tiết lộ thông tin về khách hàng trừ khi được khách hàng đồng ý hoặc theo yêu cầu của cơ</p> |

| TT  | Tên gọi/ Thời gian ban hành                            | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                        | quan có thẩm quyền.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 10. | Luật Sở hữu trí tuệ năm 2005 sửa đổi, bổ sung năm 2022 | <p>1. Chính sách của Nhà nước về bảo hộ quyền sở hữu trí tuệ: Nhà nước không bảo hộ các đối tượng sở hữu trí tuệ trái với đạo đức xã hội, trật tự công cộng, hoặc có hại cho quốc phòng, an ninh. Ngoài ra, Nhà nước có thể cấm hoặc hạn chế chủ thể quyền sở hữu trí tuệ thực hiện quyền của mình trong trường hợp nhằm bảo đảm mục tiêu quốc phòng, an ninh, dân sinh và các lợi ích khác của Nhà nước, xã hội.</p> <p>2. Biện pháp công nghệ bảo vệ quyền và thông tin quản lý quyền:</p> <ul style="list-style-type: none"> <li>- Luật quy định về việc sử dụng biện pháp công nghệ bảo vệ quyền (các kỹ thuật, công nghệ, thiết bị, linh kiện) nhằm ngăn chặn hành vi xâm phạm quyền tác giả, quyền liên quan.</li> <li>- Luật cũng định nghĩa thông tin quản lý quyền (thông tin xác định tác phẩm, tác giả, điều kiện sử dụng, mã số...) phải gắn liền với bản sao hoặc xuất hiện đồng thời khi tác phẩm được truyền đến công chúng.</li> </ul> <p>3. Các hành vi xâm phạm liên quan đến công nghệ và thông tin:</p> <ul style="list-style-type: none"> <li>- Bao gồm việc cố ý hủy bỏ hoặc làm vô hiệu biện pháp công nghệ hữu hiệu được thiết lập để bảo vệ quyền tác giả, quyền liên quan.</li> <li>- Sản xuất, phân phối, nhập khẩu, chào bán các thiết bị, sản phẩm hoặc linh kiện, hoặc cung cấp dịch vụ nhằm mục đích vô hiệu hóa biện pháp công nghệ hữu hiệu bảo vệ quyền sở hữu trí tuệ.</li> <li>- Cố ý xóa, gỡ bỏ hoặc thay đổi thông tin quản lý quyền mà không được phép, hoặc phân phối bản sao tác phẩm khi biết thông tin quản lý quyền đã bị xóa/thay đổi.</li> <li>- Đối với quyền liên quan, còn có hành vi giải mã trái phép hoặc giúp giải mã trái phép tín hiệu vệ tinh mang chương trình được mã hóa.</li> </ul> <p>4. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trung gian:</p> <ul style="list-style-type: none"> <li>- Các doanh nghiệp này (cung cấp phương tiện kỹ thuật để đưa nội dung thông tin số lên mạng viễn thông và Internet, cung cấp kết nối trực tuyến) có trách nhiệm triển khai các biện pháp kỹ thuật, phối hợp với cơ quan nhà nước và chủ thể quyền để bảo vệ quyền tác giả, quyền liên quan trên môi trường mạng.</li> </ul> |

| TT  | Tên gọi/ Thời gian ban hành                                      | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                                  | <p>- Họ có thể được miễn trừ trách nhiệm pháp lý trong một số trường hợp nhất định, ví dụ như chỉ thực hiện truyền dẫn, lưu trữ tạm thời (cache), hoặc lưu trữ theo yêu cầu người dùng mà không biết nội dung đó vi phạm và đã hành động nhanh chóng để gỡ bỏ khi biết. Họ không phải tự giám sát dịch vụ của mình.</p> <p>5. Bảo vệ bí mật kinh doanh và dữ liệu thử nghiệm:</p> <p>- Luật bảo hộ bí mật kinh doanh và các hành vi xâm phạm bao gồm tiếp cận thông tin bằng cách chống lại các biện pháp bảo mật, bộc lộ, sử dụng bí mật kinh doanh bất hợp pháp.</p> <p>- Cơ quan có thẩm quyền cấp phép lưu hành dược phẩm, nông hóa phẩm có nghĩa vụ bảo mật dữ liệu thử nghiệm do các nhà sản xuất cung cấp, không được sử dụng cho mục đích thương mại không lành mạnh hoặc bộc lộ (trừ trường hợp cần thiết để bảo vệ công chúng).</p> <p>6. Kiểm soát an ninh đối với sáng chế trước khi nộp đơn đăng ký ở nước ngoài:</p> <p>Sáng chế trong các lĩnh vực kỹ thuật có tác động đến quốc phòng, an ninh được tạo ra tại Việt Nam bởi cá nhân/tổ chức Việt Nam chỉ được nộp đơn đăng ký ở nước ngoài sau khi đã nộp đơn đăng ký tại Việt Nam để thực hiện thủ tục kiểm soát an ninh. Đơn đăng ký sáng chế vi phạm quy định này sẽ bị hủy bỏ hiệu lực.</p> <p>7. Quyền của Nhà nước đối với tài sản trí tuệ từ nhiệm vụ khoa học và công nghệ sử dụng ngân sách nhà nước: Nhà nước có quyền cho phép các tổ chức, cá nhân khác sử dụng sáng chế, kiểu dáng công nghiệp, thiết kế bố trí, giống cây trồng là kết quả của nhiệm vụ khoa học và công nghệ sử dụng ngân sách nhà nước mà không cần sự đồng ý của người nắm độc quyền sử dụng, đặc biệt trong các trường hợp phục vụ quốc phòng, an ninh, phòng bệnh, chữa bệnh, dinh dưỡng cho Nhân dân hoặc đáp ứng các nhu cầu cấp thiết khác của xã hội.</p> <p>8. Hành vi cạnh tranh không lành mạnh liên quan đến tên miền: Luật xem việc chiếm hữu, sử dụng tên miền trùng hoặc tương tự gây nhầm lẫn với nhãn hiệu, tên thương mại được bảo hộ hoặc chỉ dẫn địa lý với dụng ý xấu để thu lợi bất chính là hành vi cạnh tranh không lành mạnh.</p> |
| 11. | Luật Xử lý vi phạm hành chính năm 2012 sửa đổi, bổ sung năm 2023 | 1. Mức phạt tiền tối đa cho vi phạm: Luật quy định mức phạt tiền tối đa đối với các hành vi vi phạm hành chính trong lĩnh vực an ninh mạng và an toàn thông tin mạng. Đối với cá nhân, mức phạt này có thể lên đến một trăm triệu đồng.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| TT  | Tên gọi/ Thời gian ban hành                                 | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                             | <p>2. Thẩm quyền xử phạt của lực lượng chuyên trách: Các chức danh trong lực lượng Công an nhân dân, đặc biệt là Trưởng phòng nghiệp vụ và Cục trưởng thuộc Cục an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, có thẩm quyền xử phạt vi phạm hành chính liên quan đến lĩnh vực này, bao gồm cả việc phạt tiền và áp dụng các hình thức xử phạt bổ sung.</p> <p>3. Biện pháp ngăn chặn và bảo đảm xử lý: Các cán bộ và thủ trưởng thuộc Cục an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao cũng có thẩm quyền áp dụng các biện pháp ngăn chặn hành chính như tạm giữ người để kịp thời ngăn chặn hoặc bảo đảm việc xử lý vi phạm hành chính trong lĩnh vực này.</p> <p>4. Sử dụng phương tiện kỹ thuật phát hiện vi phạm: Luật cho phép các cơ quan có thẩm quyền sử dụng phương tiện, thiết bị kỹ thuật nghiệp vụ để phát hiện các hành vi vi phạm hành chính, trong đó có nhắc đến lĩnh vực tần số vô tuyến điện, một yếu tố nền tảng của hoạt động mạng và các lĩnh vực khác liên quan đến an ninh trật tự, an toàn xã hội mà Chính phủ có thể quy định.</p>                                                                                                                                                                                                                                                                     |
| 12. | Luật Công nghệ thông tin năm 2006 sửa đổi, bổ sung năm 2024 | <p>1. Quản lý nhà nước về an toàn và an ninh thông tin: Nhà nước có trách nhiệm quản lý an toàn và an ninh thông tin trong các hoạt động ứng dụng công nghệ thông tin.</p> <p>2. Các hành vi bị nghiêm cấm:</p> <ul style="list-style-type: none"> <li>- Cản trở hoặc phá hoại hoạt động, cơ sở hạ tầng và thông tin trên môi trường mạng: Bao gồm việc phá hoại cơ sở hạ tầng thông tin quốc gia, hệ thống máy chủ tên miền, hoặc thông tin số.</li> <li>- Sử dụng thông tin số với mục đích xấu: Cấm cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số nhằm chống phá Nhà nước, kích động bạo lực, tuyên truyền chiến tranh, gây hận thù, kích động dân ô, đòi truy, tội ác, mê tín dị đoan, phá hoại thuần phong mỹ tục.</li> <li>- Tiết lộ bí mật: Nghiêm cấm tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và các bí mật khác đã được pháp luật quy định.</li> <li>- Xuyên tạc, vu khống, xúc phạm: Cấm các hành vi xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của công dân.</li> <li>- Xâm phạm sở hữu trí tuệ và giả mạo: Cấm xâm phạm quyền sở hữu trí tuệ trong công nghệ thông tin, sản xuất hoặc lưu hành sản phẩm công nghệ thông tin trái pháp luật, giả mạo trang thông tin điện tử của tổ chức, cá nhân khác và tạo đường dẫn trái phép đến tên miền hợp pháp.</li> </ul> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>3. Trách nhiệm bảo đảm an toàn thông tin:</p> <ul style="list-style-type: none"> <li>- Trách nhiệm chung: Các tổ chức, cá nhân tham gia hoạt động ứng dụng công nghệ thông tin phải chịu trách nhiệm về nội dung thông tin số của mình.</li> <li>- bảo đảm độ tin cậy và bí mật: Cơ quan nhà nước và các tổ chức, cá nhân phải bảo đảm độ tin cậy và bí mật của thông tin khi gửi, nhận văn bản trên môi trường mạng.</li> <li>- Ngăn chặn thông tin trái pháp luật: Tổ chức, cá nhân truyền đưa hoặc cho thuê chỗ lưu trữ thông tin số có trách nhiệm ngăn chặn truy nhập hoặc loại bỏ thông tin trái pháp luật khi phát hiện hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền.</li> <li>- Bảo vệ dữ liệu cá nhân: Việc thu thập, xử lý và sử dụng thông tin cá nhân trên môi trường mạng phải có sự đồng ý của chủ thể thông tin (trừ một số trường hợp cụ thể) và phải có biện pháp quản lý, kỹ thuật để bảo đảm thông tin không bị mất, đánh cắp, tiết lộ, thay đổi hoặc phá hủy. Không được cung cấp thông tin cá nhân cho bên thứ ba nếu không có sự đồng ý hoặc quy định của pháp luật.</li> <li>- Quản lý trang thông tin điện tử: Các tổ chức, cá nhân thiết lập trang thông tin điện tử phải chịu trách nhiệm quản lý nội dung và hoạt động của trang, đồng thời phải tuân thủ quy định về bảo vệ bí mật nhà nước.</li> </ul> <p>4. Bảo vệ cơ sở hạ tầng thông tin: Cơ sở hạ tầng thông tin quốc gia phải được bảo vệ và các tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng này phải bảo đảm an toàn, an ninh thông tin dưới sự quản lý, thanh tra, kiểm tra của cơ quan nhà nước có thẩm quyền.</p> <p>5. Bảo vệ tên miền quốc gia Việt Nam “.vn”: Tên miền quốc gia “.vn” được coi là tài nguyên thông tin quốc gia và cần được bảo vệ, đặc biệt đối với các tổ chức Đảng, cơ quan nhà nước.</p> <p>6. Chống thư rác và vi rút máy tính:</p> <ul style="list-style-type: none"> <li>- Quy định về thư rác: Cấm che giấu hoặc giả mạo danh tính khi gửi thông tin và yêu cầu phải cung cấp khả năng từ chối nhận thông tin quảng cáo.</li> <li>- Quy định về vi rút và phần mềm gây hại: Cấm tạo ra, cài đặt, phát tán vi rút máy tính và các phần mềm gây hại khác nhằm thay đổi thiết lập thiết bị, thu thập thông tin, vô hiệu hóa phần mềm bảo mật, chiếm đoạt quyền điều khiển, hoặc thay đổi/xóa bỏ thông tin.</li> </ul> <p>7. Bảo vệ trẻ em: Nhà nước, xã hội, nhà trường và gia đình có trách nhiệm bảo vệ trẻ em khỏi những</p> |

| TT  | Tên gọi/ Thời gian ban hành                                  | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                              | <p>tác động tiêu cực của thông tin trên môi trường mạng, bao gồm việc ngăn chặn nội dung bạo lực và khiêu dâm và phát triển các công cụ lọc nội dung.</p> <p>8. Xử lý vi phạm: Mọi hành vi vi phạm pháp luật về công nghệ thông tin sẽ bị xử lý kỷ luật, xử phạt hành chính hoặc truy cứu trách nhiệm hình sự và phải bồi thường thiệt hại nếu có.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 13. | Luật Tần số vô tuyến điện năm 2009 sửa đổi, bổ sung năm 2024 | <p>1. Các hành vi bị nghiêm cấm để bảo đảm an ninh quốc gia và TTATXH: Luật nghiêm cấm việc sử dụng tần số và thiết bị vô tuyến điện để chống lại Nhà nước, gây phương hại đến quốc phòng, an ninh, trật tự, an toàn xã hội, hoặc làm thiệt hại đến lợi ích của Nhà nước, tổ chức, cá nhân. Đặc biệt, việc cố ý gây nhiễu có hại hoặc cản trở trái pháp luật hoạt động của hệ thống thông tin vô tuyến điện là hành vi bị cấm.</p> <p>2. Quản lý và xử lý nhiễu có hại: Một trong những trọng tâm cốt lõi của Luật là việc kiểm soát chất lượng phát xạ vô tuyến điện và tương thích điện từ để hạn chế, phát hiện và xử lý nhiễu có hại. Các quy định về xử lý nhiễu có hại nhằm bảo đảm tính khả dụng và toàn vẹn của các hệ thống thông tin vô tuyến, đặc biệt ưu tiên các nghiệp vụ quan trọng như dẫn đường, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng và an ninh. Khi có nhiễu gây hại cho các mục đích này, có thể yêu cầu ngừng sử dụng thiết bị gây nhiễu.</p> <p>3. Yêu cầu về an toàn bức xạ và tương thích điện từ: Tổ chức, cá nhân sản xuất, nhập khẩu và sử dụng thiết bị vô tuyến điện phải tuân thủ các quy định về an toàn bức xạ vô tuyến điện và tương thích điện từ để ngăn ngừa tác hại đến con người, môi trường và tránh gây nhiễu cho các thiết bị, hệ thống khác.</p> <p>4. Điều kiện cấp phép sử dụng tần số vô tuyến điện: Khi được cấp giấy phép sử dụng tần số và thiết bị vô tuyến điện, các tổ chức, cá nhân phải có cam kết thực hiện quy định của pháp luật về bảo đảm an toàn, an ninh thông tin, cũng như các biện pháp kiểm tra, giải quyết nhiễu có hại và an toàn bức xạ vô tuyến điện.</p> <p>5. Quản lý tần số vô tuyến điện phục vụ quốc phòng, an ninh: Luật có chương riêng quy định về việc phân bổ, quản lý và sử dụng tần số vô tuyến điện cho mục đích quốc phòng, an ninh. Các cơ quan quản lý chuyên trách thuộc Bộ Quốc phòng, Bộ Công an có trách nhiệm quy định việc quản lý, cấp phép, kiểm tra, kiểm soát và xử lý nhiễu có hại trong lĩnh vực này. Trong các tình huống ảnh hưởng trực tiếp đến chủ quyền, an ninh quốc gia, Bộ Quốc phòng và Bộ Công an có quyền quyết định sử</p> |

| TT  | Tên gọi/ Thời gian ban hành                                | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                            | <p>dụng tần số và thiết bị vô tuyến điện ngoài các tần số đã được phân bổ riêng, đồng thời có thể yêu cầu các tổ chức, cá nhân khác ngừng sử dụng tần số nếu gây nhiễu.</p> <p>6. Sử dụng thiết bị gây nhiễu: Bộ Quốc phòng và Bộ Công an được phép sử dụng thiết bị gây nhiễu để thực hiện nhiệm vụ bảo vệ Tổ quốc, phòng ngừa, ngăn chặn, đấu tranh làm thất bại hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội. Đây là một công cụ mạnh mẽ để bảo vệ an ninh thông tin và an ninh quốc gia trên phổ tần số.</p> <p>7. Thu hồi giấy phép vì lý do an ninh: Giấy phép sử dụng tần số vô tuyến điện có thể bị thu hồi nếu tổ chức, cá nhân sử dụng tần số nhằm chống lại Nhà nước, làm phương hại đến quốc phòng, an ninh, trật tự, an toàn xã hội, hoặc cố ý gây nhiễu có hại trái phép gây hậu quả nghiêm trọng.</p> <p>8. Hợp tác quốc tế về tần số vô tuyến điện: Việt Nam tham gia vào các hoạt động đăng ký, phối hợp quốc tế về tần số vô tuyến điện và quỹ đạo vệ tinh để bảo vệ lợi ích quốc gia, đặc biệt là trong việc ngăn chặn và xử lý nhiễu có hại từ các quốc gia khác, cũng như sử dụng tần số cho hệ thống thông tin quốc tế.</p> |
| 14. | Luật Khoa học công nghệ năm 2013 sửa đổi, bổ sung năm 2022 | <p>1. Gắn kết với nhiệm vụ quốc phòng, an ninh: Hoạt động khoa học và công nghệ có nhiệm vụ và nguyên tắc phục vụ trực tiếp việc bảo đảm quốc phòng, an ninh, bên cạnh phát triển kinh tế - xã hội. Chính sách của Nhà nước cũng nhấn mạnh việc gắn phát triển khoa học và công nghệ với nhiệm vụ quốc phòng, an ninh.</p> <p>2. Bảo vệ bí mật nhà nước và thông tin nhạy cảm:</p> <ul style="list-style-type: none"> <li>- Luật nghiêm cấm hành vi tiết lộ tài liệu, kết quả khoa học và công nghệ thuộc danh mục bí mật nhà nước.</li> <li>- Tổ chức và cá nhân hoạt động khoa học và công nghệ có nghĩa vụ giữ bí mật nhà nước về khoa học và công nghệ.</li> <li>- Các nhiệm vụ khoa học và công nghệ thuộc bí mật quốc gia, đặc thù phục vụ an ninh, quốc phòng được giao trực tiếp và kết quả của chúng phải được đăng ký, lưu giữ theo chế độ mật.</li> <li>- Bên nhận đặt hàng thực hiện hợp đồng nghiên cứu khoa học và phát triển công nghệ có nghĩa vụ giữ bí mật về kết quả nghiên cứu theo thỏa thuận.</li> </ul> <p>3. Bảo hộ quyền sở hữu trí tuệ: Luật nghiêm cấm các hành vi xâm phạm quyền sở hữu trí tuệ, chiếm</p>                            |

| TT  | Tên gọi/ Thời gian ban hành          | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                      | <p>đoạt, chuyển nhượng, chuyển giao bất hợp pháp kết quả khoa học và công nghệ. Các tổ chức, cá nhân hoạt động khoa học và công nghệ có quyền được bảo hộ quyền sở hữu trí tuệ đối với các kết quả của mình.</p> <p>4. Nâng cao năng lực và làm chủ công nghệ: Nhà nước có chính sách đẩy mạnh nghiên cứu ứng dụng, nghiên cứu làm chủ và tạo ra công nghệ mới, đặc biệt là công nghệ tiên tiến, công nghệ cao, nhằm nâng cao năng lực khoa học và công nghệ quốc gia và năng lực cạnh tranh của sản phẩm. Việc này gián tiếp góp phần vào an ninh công nghệ.</p> <p>5. Xây dựng và bảo đảm hạ tầng thông tin: Nhà nước đầu tư xây dựng, khuyến khích tài trợ cho việc xây dựng hạ tầng thông tin, cơ sở dữ liệu quốc gia và thống kê về khoa học và công nghệ hiện đại để bảo đảm thông tin đầy đủ, chính xác, kịp thời. Điều này tạo nền tảng vững chắc cho việc quản lý và bảo vệ thông tin trong lĩnh vực S&amp;T.</p> <p>6. Ngăn chặn lợi dụng và vi phạm: Cấm lợi dụng hoạt động khoa học và công nghệ để xâm phạm lợi ích của Nhà nước, cá nhân, tổ chức. Các hành vi vi phạm pháp luật về khoa học và công nghệ sẽ bị xử lý theo quy định, bao gồm các hành vi có thể gây ảnh hưởng đến an ninh.</p> <p>7. an ninh trong hội nhập quốc tế: Hoạt động hội nhập quốc tế về khoa học và công nghệ phải tuân thủ nguyên tắc bảo đảm độc lập, chủ quyền, an ninh quốc gia.</p> |
| 15. | Luật Bảo vệ người tiêu dùng năm 2023 | <p>1. Bảo vệ thông tin người tiêu dùng là quyền cơ bản và trách nhiệm của tổ chức, cá nhân kinh doanh: Người tiêu dùng có quyền được bảo vệ thông tin khi tham gia giao dịch. Tổ chức, cá nhân kinh doanh có trách nhiệm bảo đảm an toàn, an ninh thông tin của người tiêu dùng khi thu thập, lưu trữ, sử dụng, chỉnh sửa, cập nhật hoặc hủy bỏ thông tin, kể cả khi ủy quyền cho bên thứ ba.</p> <p>2. Xây dựng và công khai quy tắc bảo vệ thông tin: Các tổ chức, cá nhân kinh doanh phải xây dựng và công khai các quy tắc về mục đích, phạm vi sử dụng, thời hạn lưu trữ thông tin và biện pháp bảo vệ, bảo đảm an toàn thông tin của người tiêu dùng.</p> <p>3. Sự đồng ý của người tiêu dùng và quyền kiểm soát thông tin: Việc thu thập, sử dụng thông tin của người tiêu dùng phải được thông báo rõ ràng về mục đích, phạm vi và được người tiêu dùng đồng ý. Người tiêu dùng có quyền kiểm tra, chỉnh sửa, cập nhật, hủy bỏ, chuyển giao hoặc ngừng chuyển giao thông tin của mình. Tổ chức, cá nhân kinh doanh phải tạo cơ chế để người tiêu dùng lựa chọn việc cho</p>                                                                                                                                                                                                                                                                                               |

| TT  | Tên gọi/ Thời gian ban hành     | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                 | <p>phép hoặc không cho phép chia sẻ, tiết lộ, chuyển giao thông tin cho bên thứ ba hoặc sử dụng thông tin cho mục đích quảng cáo.</p> <p>4. Trách nhiệm xử lý sự cố an ninh thông tin: Trong trường hợp hệ thống thông tin bị tấn công gây nguy cơ mất an toàn, an ninh thông tin của người tiêu dùng, tổ chức, cá nhân kinh doanh hoặc bên lưu trữ thông tin phải thông báo cho cơ quan quản lý nhà nước có thẩm quyền trong vòng 24 giờ và thực hiện các biện pháp cần thiết để bảo đảm an toàn, an ninh thông tin theo quy định của pháp luật về an ninh mạng, an toàn thông tin mạng và giao dịch điện tử.</p> <p>5. Các hành vi bị nghiêm cấm liên quan đến thông tin: Luật nghiêm cấm các hành vi của tổ chức, cá nhân kinh doanh như thu thập, lưu trữ, sử dụng, chỉnh sửa, cập nhật, hủy bỏ thông tin của người tiêu dùng trái quy định của pháp luật.</p> <p>6. Trách nhiệm đặc thù đối với giao dịch trên không gian mạng và nền tảng số: Các tổ chức thiết lập, vận hành nền tảng số trung gian có trách nhiệm cụ thể như xác thực danh tính tổ chức, cá nhân kinh doanh trên nền tảng của mình, lưu trữ thông tin về sản phẩm, giao dịch và cho phép người tiêu dùng truy cập, truy vết, tải, lưu trữ các tài liệu liên quan. Đồng thời, họ phải bảo đảm hiển thị đầy đủ, chính xác phản hồi, đánh giá của người tiêu dùng và có biện pháp ngăn chặn hiển thị không trung thực. Các nền tảng số lớn còn có trách nhiệm đánh giá định kỳ việc kiểm duyệt nội dung, sử dụng thuật toán, quảng cáo hướng đối tượng và xử lý tài khoản giả, sử dụng trí tuệ nhân tạo/giải pháp tự động.</p> |
| 16. | Luật Giao dịch điện tử năm 2023 | <p>1. Yêu cầu tuân thủ pháp luật về an toàn, an ninh mạng: Mọi cơ quan, tổ chức, cá nhân khi tham gia giao dịch điện tử phải tuân thủ chặt chẽ các quy định của pháp luật về an toàn thông tin mạng và an ninh mạng, bên cạnh các quy định khác về giao dịch điện tử. Các thông tin thuộc bí mật nhà nước trong thông điệp dữ liệu cũng phải tuân thủ quy định về bảo vệ bí mật nhà nước và pháp luật về cơ yếu.</p> <p>2. Các hành vi bị nghiêm cấm để bảo vệ an ninh: Luật quy định rõ các hành vi bị cấm nhằm ngăn chặn việc lợi dụng giao dịch điện tử để xâm phạm lợi ích quốc gia, an ninh quốc gia, trật tự, an toàn xã hội, hoặc quyền và lợi ích hợp pháp của tổ chức, cá nhân. Cụ thể bao gồm việc cản trở, ngăn chặn, hoặc phá hoại hệ thống thông tin phục vụ giao dịch điện tử; thu thập, cung cấp, sử dụng, tiết lộ thông điệp dữ liệu một cách trái pháp luật; giả mạo, làm sai lệch, xóa, hủy thông điệp dữ liệu; tạo thông điệp dữ</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>liệu nhằm thực hiện hành vi trái pháp luật; gian lận, giả mạo, chiếm đoạt, hoặc sử dụng trái pháp luật tài khoản giao dịch điện tử, chứng thư điện tử, chứng thư chữ ký điện tử, chữ ký điện tử.</p> <p>3. bảo đảm tính toàn vẹn và xác thực của thông điệp dữ liệu và chứng thư điện tử:</p> <ul style="list-style-type: none"> <li>- Thông điệp dữ liệu và các văn bản chuyển đổi giữa định dạng giấy và điện tử phải bảo đảm tính toàn vẹn (chưa bị thay đổi) và có thể truy cập, sử dụng được để tham chiếu.</li> <li>- Việc chuyển đổi các văn bản quan trọng như giấy phép, chứng chỉ sang thông điệp dữ liệu cần có chữ ký số của cơ quan thực hiện chuyển đổi để bảo đảm giá trị pháp lý.</li> <li>- Hệ thống thông tin phục vụ chuyển giao, lưu trữ, xử lý chứng thư điện tử phải đáp ứng yêu cầu bảo đảm an toàn thông tin mạng tối thiểu cấp độ 3.</li> </ul> <p>4. Yêu cầu kỹ thuật và pháp lý đối với chữ ký điện tử và chữ ký số: Chữ ký điện tử, đặc biệt là chữ ký số, phải bảo đảm khả năng xác nhận duy nhất chủ thể ký, kiểm soát dữ liệu tạo chữ ký tại thời điểm ký, phát hiện mọi thay đổi đối với thông điệp dữ liệu sau thời điểm ký và được bảo đảm bởi chứng thư chữ ký số để chống chối bỏ và bảo toàn tính toàn vẹn. Phương tiện tạo chữ ký số phải bảo đảm dữ liệu không bị tiết lộ, thu thập, giả mạo.</p> <p>5. Trách nhiệm của các chủ quản hệ thống thông tin và dịch vụ tin cậy:</p> <ul style="list-style-type: none"> <li>- Chủ quản hệ thống thông tin phục vụ giao dịch điện tử có trách nhiệm tuân thủ pháp luật về an toàn thông tin mạng, an ninh mạng, bảo vệ thông tin cá nhân, dữ liệu cá nhân và giám sát an toàn hệ thống.</li> <li>- Đối với các nền tảng số trung gian quy mô lớn và rất lớn, có trách nhiệm bổ sung như công bố cơ chế phản ánh và xử lý nội dung vi phạm pháp luật, báo cáo định kỳ về các vụ việc lợi dụng hệ thống và công khai nguyên tắc hiển thị nội dung, quảng cáo cho người dùng.</li> <li>- Các tổ chức cung cấp dịch vụ tin cậy (như dịch vụ chứng thực chữ ký số) phải đáp ứng điều kiện kinh doanh nghiêm ngặt về an toàn thông tin mạng (tối thiểu cấp độ 3) và có trách nhiệm bảo đảm an toàn cho hệ thống của mình.</li> </ul> <p>6. An toàn dữ liệu trong hoạt động của cơ quan nhà nước:</p> <ul style="list-style-type: none"> <li>- Các cơ quan nhà nước phải áp dụng biện pháp bảo đảm an toàn thông tin mạng, an ninh mạng và bảo mật dữ liệu trong quá trình kết nối, chia sẻ dữ liệu.</li> <li>- Việc chia sẻ dữ liệu trực tuyến là ưu tiên, trừ các trường hợp thông tin liên quan đến bí mật nhà nước</li> </ul> |

| TT  | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                             | <p>hoặc yêu cầu quốc phòng, an ninh.</p> <ul style="list-style-type: none"> <li>- Hệ thống thông tin và tài khoản giao dịch điện tử của cơ quan nhà nước phải được bảo đảm an toàn.</li> </ul> <p>7. Vai trò quản lý nhà nước: Chính phủ thống nhất quản lý nhà nước về giao dịch điện tử, với Bộ Thông tin và Truyền thông là cơ quan đầu mối chủ trì, phối hợp quản lý. Các nội dung quản lý bao gồm giám sát an toàn hệ thống thông tin, quản lý dịch vụ tin cậy và phát triển hạ tầng chứng thực điện tử quốc gia. Bộ Quốc phòng có trách nhiệm quản lý trong lĩnh vực cơ yếu và chữ ký số chuyên dùng công vụ.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 17. | Luật Viễn thông năm 2023    | <p>1. Trách nhiệm chung về bảo đảm an toàn, an ninh thông tin: Luật quy định rõ trách nhiệm của mọi cơ quan, tổ chức, cá nhân tham gia hoạt động viễn thông trong việc bảo đảm an toàn cơ sở hạ tầng viễn thông, an toàn thông tin mạng và an ninh thông tin. Các hành vi gây nhiễu có hại, làm hư hỏng thiết bị, công trình, mạng viễn thông hoặc gây hại đến hoạt động hợp pháp của cơ sở hạ tầng viễn thông đều bị nghiêm cấm.</p> <p>2. Bảo mật thông tin riêng tư và bí mật nhà nước:</p> <ul style="list-style-type: none"> <li>- Thông tin riêng của mọi tổ chức, cá nhân chuyển qua mạng viễn thông công cộng được bảo đảm bí mật. Việc kiểm soát thông tin trên mạng viễn thông chỉ được thực hiện bởi cơ quan nhà nước có thẩm quyền theo quy định của pháp luật.</li> <li>- Doanh nghiệp viễn thông không được tiết lộ thông tin riêng liên quan đến người sử dụng dịch vụ (bao gồm thông tin thuê bao và thông tin về việc sử dụng dịch vụ), trừ các trường hợp được pháp luật cho phép như có sự đồng ý của người dùng, thỏa thuận giữa các doanh nghiệp để tính cước, hoặc khi có yêu cầu hợp pháp từ cơ quan nhà nước có thẩm quyền.</li> <li>- Tổ chức, cá nhân khi gửi, truyền hoặc lưu giữ thông tin thuộc danh mục bí mật nhà nước trên mạng viễn thông có trách nhiệm mã hóa thông tin.</li> </ul> <p>3. Các hành vi bị nghiêm cấm liên quan đến an ninh mạng: Luật liệt kê cụ thể các hành vi bị cấm nhằm bảo vệ an ninh và trật tự, bao gồm:</p> <ul style="list-style-type: none"> <li>- Lợi dụng hoạt động viễn thông để chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.</li> <li>- Thu trộm, nghe trộm, xem trộm thông tin trên mạng viễn thông; trộm cắp, sử dụng trái phép tài</li> </ul> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>nguyên viễn thông, mật khẩu, khóa mật mã và thông tin riêng của tổ chức, cá nhân khác.</p> <ul style="list-style-type: none"> <li>- Cản trở trái pháp luật, gây rối, phá hoại việc thiết lập cơ sở hạ tầng viễn thông hoặc việc cung cấp và sử dụng dịch vụ hợp pháp.</li> <li>- Sử dụng thiết bị, phần mềm để gửi, truyền, nhận thông tin qua mạng viễn thông nhằm thực hiện hành vi vi phạm pháp luật.</li> </ul> <p>4. Trách nhiệm của doanh nghiệp viễn thông trong việc bảo đảm an ninh mạng:</p> <ul style="list-style-type: none"> <li>- Doanh nghiệp phải chịu sự quản lý, thanh tra, kiểm tra của cơ quan nhà nước có thẩm quyền về an toàn cơ sở hạ tầng viễn thông và an ninh thông tin.</li> <li>- Có nghĩa vụ thực hiện các biện pháp ngăn chặn kết nối, địa chỉ Internet, tên miền và các biện pháp khác đối với hệ thống, dịch vụ được sử dụng để thực hiện hành vi vi phạm pháp luật.</li> <li>- Phải ngừng khẩn cấp việc cung cấp dịch vụ trong trường hợp có bạo loạn, hoặc sử dụng dịch vụ viễn thông nhằm chống lại Nhà nước, xâm phạm an ninh quốc gia theo yêu cầu của cơ quan nhà nước có thẩm quyền.</li> <li>- Khi có yêu cầu của cơ quan nhà nước có thẩm quyền theo Luật an ninh mạng, doanh nghiệp phải cung cấp điểm truy nhập mạng viễn thông và các điều kiện kỹ thuật, nghiệp vụ cần thiết để cơ quan đó thực hiện nhiệm vụ kiểm soát và bảo đảm an ninh thông tin.</li> <li>- Có trách nhiệm phòng, chống, ngăn chặn tin nhắn, cuộc gọi vi phạm pháp luật và ngừng cung cấp dịch vụ đối với thuê bao viễn thông vi phạm pháp luật.</li> </ul> <p>5. Yêu cầu đối với dịch vụ trung tâm dữ liệu, điện toán đám mây và dịch vụ cơ bản trên Internet:</p> <ul style="list-style-type: none"> <li>- Các doanh nghiệp cung cấp những dịch vụ này phải tuân thủ pháp luật về an toàn thông tin mạng, an ninh mạng, bảo vệ dữ liệu cá nhân.</li> <li>- Không được truy nhập, khai thác, sử dụng dữ liệu của người dùng nếu chưa được sự đồng ý và không được theo dõi, giám sát thông tin của người dùng trừ trường hợp có yêu cầu hợp pháp.</li> <li>- Có trách nhiệm lưu trữ, quản lý thông tin người sử dụng dịch vụ.</li> </ul> <p>6. Quản lý tài nguyên viễn thông và hạ tầng: Việc quy hoạch phát triển viễn thông quốc gia và quản lý tài nguyên viễn thông (như kho số, tài nguyên Internet) phải bảo đảm an toàn cơ sở hạ tầng viễn thông và an ninh thông tin. Mã, số viễn thông, tài nguyên Internet có thể bị thu hồi nếu được sử dụng để</p> |

| TT  | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                             | <p>thực hiện các hành vi bị cấm.</p> <p>7. Trách nhiệm của người sử dụng và thuê bao: Người sử dụng dịch vụ viễn thông có quyền được bảo đảm bí mật thông tin riêng và phải chịu trách nhiệm trước pháp luật về nội dung thông tin mà mình gửi, lưu giữ trên mạng. Thuê bao có nghĩa vụ bảo vệ mật khẩu, khóa mật mã và thiết bị đầu cuối của mình.</p> <p>8. Hợp tác quốc tế và vai trò của Nhà nước: Luật khuyến khích hợp tác quốc tế về viễn thông trên cơ sở tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ, đồng thời quy định các Bộ Quốc phòng, Bộ Công an có trách nhiệm quản lý mạng viễn thông dùng riêng phục vụ quốc phòng, an ninh và cơ yếu. Việc cung cấp dịch vụ viễn thông qua biên giới phải bảo đảm yêu cầu về quốc phòng, an ninh và an toàn thông tin mạng.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 18. | Luật Căn cước năm 2024      | <p>1. Nguyên tắc và trách nhiệm chung về an ninh, an toàn thông tin mạng và Bảo vệ dữ liệu cá nhân:</p> <ul style="list-style-type: none"> <li>- Luật đặt ra nguyên tắc cơ bản là phải bảo đảm an ninh, an toàn thông tin và bảo vệ dữ liệu cá nhân trong mọi hoạt động quản lý căn cước, Cơ sở dữ liệu quốc gia về dân cư và Cơ sở dữ liệu căn cước.</li> <li>- Công dân và người gốc Việt Nam chưa xác định được quốc tịch đều có quyền được bảo vệ dữ liệu cá nhân của mình trong các cơ sở dữ liệu này.</li> <li>- Các cơ quan quản lý căn cước có trách nhiệm chính yếu trong việc bảo đảm an ninh, an toàn thông tin và bảo vệ dữ liệu cá nhân trong các cơ sở dữ liệu và hệ thống định danh, xác thực điện tử.</li> </ul> <p>2. Các Hành vi Bị nghiêm cấm nhằm bảo đảm an ninh mạng và An toàn Dữ liệu:</p> <ul style="list-style-type: none"> <li>- Nghiêm cấm các hành vi gây cản trở, rối loạn hoạt động của cơ sở hạ tầng thông tin, cơ sở dữ liệu căn cước và hệ thống định danh, xác thực điện tử.</li> <li>- Cấm làm giả, sửa chữa, cố ý làm sai lệch nội dung thẻ căn cước, căn cước điện tử, giấy chứng nhận căn cước; chiếm đoạt, sử dụng trái phép các giấy tờ này hoặc thông tin của người khác.</li> <li>- Cấm truy nhập, thay đổi, xóa, hủy, phát tán hoặc thực hiện các hoạt động xử lý dữ liệu cá nhân trong các cơ sở dữ liệu và hệ thống định danh, xác thực điện tử một cách trái phép.</li> <li>- Cấm khai thác, chia sẻ, mua, bán, trao đổi, chiếm đoạt, sử dụng trái phép thông tin, dữ liệu trong Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu căn cước, hệ thống định danh và xác thực điện tử.</li> </ul> <p>3. Yêu cầu Bảo vệ Hạ tầng thông tin và Cơ sở dữ liệu:</p> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <ul style="list-style-type: none"> <li>- Cơ sở hạ tầng thông tin của Cơ sở dữ liệu quốc gia về dân cư và Cơ sở dữ liệu căn cước phải được Nhà nước bảo vệ theo quy định của pháp luật về an ninh mạng và an toàn thông tin mạng, cũng như pháp luật về bảo vệ công trình quan trọng liên quan đến an ninh quốc gia.</li> <li>- Việc xây dựng và quản lý các cơ sở dữ liệu phải bảo đảm an ninh, an toàn thông tin, bảo vệ dữ liệu cá nhân và hoạt động ổn định, liên tục.</li> <li>- Các cơ sở dữ liệu phải được lưu trữ trên thiết bị có biện pháp chống truy nhập trái phép thông qua hệ thống bảo mật.</li> <li>- Có quy định về việc khóa và mở khóa căn cước điện tử trong các trường hợp cần thiết để bảo đảm an ninh, an toàn.</li> </ul> <p>4. Trách nhiệm của Cơ quan, Tổ chức và Cá nhân trong bảo đảm An toàn Dữ liệu:</p> <ul style="list-style-type: none"> <li>- Các cơ quan, tổ chức, cá nhân liên quan phải tuân thủ quy trình và bảo đảm việc cung cấp, thu thập, cập nhật thông tin đầy đủ, chính xác, kịp thời.</li> <li>- Người làm công tác quản lý căn cước có trách nhiệm bảo đảm an ninh, an toàn và tính đầy đủ, chính xác của thông tin.</li> <li>- Khi khai thác thông tin cá nhân trong cơ sở dữ liệu bởi các tổ chức, cá nhân không thuộc cơ quan nhà nước, cần phải được sự đồng ý của cơ quan quản lý căn cước và chủ thể của thông tin.</li> <li>- Việc kết nối, chia sẻ thông tin giữa các cơ sở dữ liệu quốc gia và chuyên ngành phải bảo đảm hiệu quả và an toàn.</li> </ul> <p>5. Vai trò của Bộ Công an và các Bộ ngành trong an ninh mạng và Hệ thống Định danh:</p> <ul style="list-style-type: none"> <li>- Bộ Công an là cơ quan đầu mối giúp Chính phủ thống nhất quản lý nhà nước về căn cước, các cơ sở dữ liệu và hệ thống định danh, xác thực điện tử.</li> <li>- Bộ Công an chịu trách nhiệm xây dựng, quản lý, bảo vệ và vận hành hệ thống định danh và xác thực điện tử, ứng dụng tài khoản định danh điện tử vào công tác quản lý nhà nước và cải cách hành chính, cũng như phòng, chống thiên tai, dịch bệnh.</li> <li>- Các Bộ, cơ quan ngang Bộ và Ủy ban nhân dân cấp tỉnh có trách nhiệm phối hợp với Bộ Công an trong việc quản lý nhà nước, phát triển, ứng dụng và kiểm tra, xử lý vi phạm liên quan đến an ninh mạng và an toàn thông tin của các hệ thống này.</li> </ul> |

| TT  | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19. | Luật Dữ liệu năm 2024       | <p>1. Nguyên tắc và Trách nhiệm Chung về an ninh Dữ liệu: Luật quy định rõ phải bảo đảm an ninh, an toàn, toàn vẹn, tin cậy và bảo mật dữ liệu trong suốt quá trình xây dựng, phát triển, quản trị, xử lý và sử dụng. Việc bảo vệ dữ liệu phải được thực hiện đồng bộ với các hoạt động phát triển dữ liệu.</p> <p>2. Các Hành vi Bị Nghiêm cấm: Luật nghiêm cấm các hành vi lợi dụng dữ liệu để xâm phạm lợi ích quốc gia, quốc phòng, an ninh, TTATXH; cản trở, tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu hoặc hệ thống thông tin; làm giả, làm sai lệch, làm mất hoặc làm hư hỏng dữ liệu trong các cơ sở dữ liệu nhà nước.</p> <p>3. Vai trò và Trách nhiệm của Cơ quan Nhà nước:</p> <ul style="list-style-type: none"> <li>- Chính phủ thống nhất quản lý nhà nước về dữ liệu.</li> <li>- Bộ Công an là cơ quan đầu mối chịu trách nhiệm chính về quản lý nhà nước về dữ liệu, bao gồm việc bảo đảm an ninh, an toàn dữ liệu, trừ dữ liệu thuộc phạm vi Bộ Quốc phòng quản lý.</li> <li>- Các cơ quan nhà nước có trách nhiệm bảo vệ dữ liệu trong ngành, lĩnh vực mình quản lý, xây dựng hệ thống bảo vệ dữ liệu thống nhất, đánh giá rủi ro an ninh dữ liệu và cảnh báo sớm.</li> <li>- Phải cung cấp công cụ và phân quyền truy cập, truy xuất dữ liệu để bảo đảm an ninh, an toàn và bảo vệ dữ liệu.</li> </ul> <p>4. Biện pháp Bảo vệ Dữ liệu và Hạ tầng:</p> <ul style="list-style-type: none"> <li>- Dữ liệu mật phải được mã hóa khi lưu trữ, truyền nhận trên mạng máy tính. Cơ quan có thẩm quyền có thể giải mã dữ liệu trong các trường hợp khẩn cấp hoặc đe dọa an ninh quốc gia.</li> <li>- Cơ sở hạ tầng của Trung tâm dữ liệu quốc gia phải được thiết kế, xây dựng với các giải pháp an ninh, bảo mật cao để kiểm soát, phát hiện, ngăn chặn tấn công, đột nhập, phá hoại, đồng thời bảo đảm chống khủng bố và thiên tai.</li> <li>- Các cơ sở dữ liệu quốc gia phải được lưu trữ trên hạ tầng của Trung tâm dữ liệu quốc gia, bảo đảm an ninh, an toàn thông tin và bảo vệ dữ liệu cá nhân.</li> </ul> <p>5. Quản lý Rủi ro an ninh mạng: Luật yêu cầu xác định, thiết lập cơ chế cảnh báo sớm về các rủi ro phát sinh trong xử lý dữ liệu, bao gồm rủi ro an ninh mạng, rủi ro quyền riêng tư và rủi ro quản lý truy cập. Chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải định kỳ đánh giá rủi ro và phối hợp với các đơn vị chuyên trách về an ninh mạng.</p> |

| TT | Tên gọi/ Thời gian ban hành | Quy định liên quan đến lĩnh vực an ninh mạng                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                             | <p>6. Quy định về Dịch vụ Dữ liệu: Các tổ chức cung cấp sản phẩm, dịch vụ trung gian dữ liệu, phân tích, tổng hợp dữ liệu, sản dữ liệu phải tuân thủ quy định pháp luật về an toàn thông tin mạng, an ninh mạng và giao dịch điện tử. Một số loại dữ liệu gây nguy hại đến quốc phòng, an ninh, đối ngoại bị cấm giao dịch trên sàn dữ liệu.</p> <p>7. Chuyển, xử lý Dữ liệu Xuyên Biên giới: Việc chuyển và xử lý dữ liệu cốt lõi, dữ liệu quan trọng xuyên biên giới phải bảo đảm quốc phòng, an ninh và lợi ích quốc gia.</p> <p>8. Tiêu chuẩn và Quy chuẩn Kỹ thuật: Quy định việc ban hành và áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu, bao gồm tiêu chuẩn cho hệ thống thông tin, phần cứng, phần mềm, quản lý, vận hành, xử lý và bảo vệ dữ liệu.</p> |