

DOI: 10.62829/VNHN.373.135.140

AN NINH MẠNG VÀ LUẬT AN NINH MẠNG TRONG THỜI KỲ CÔNG NGHIỆP 4.0

✍ TS. Hoàng Văn Liêm

● **TÓM TẮT:** Trong bối cảnh cách mạng công nghiệp 4.0 phát triển mạnh mẽ, không gian mạng đã trở thành một phần không thể thiếu trong đời sống kinh tế, xã hội và chính trị của mỗi quốc gia. Tuy nhiên, cùng với sự phát triển đó, sự gia tăng của các mối đe dọa an ninh mạng như tội phạm công nghệ cao, tấn công mạng, phát tán thông tin xấu độc, gây phương hại đến lợi ích quốc gia, tổ chức và cá nhân cũng ngày một lớn hơn. Trước thực tiễn đó, Luật An ninh mạng (ban hành ngày 12/6/2018, có hiệu lực từ 1/1/2019) ra đời nhằm bảo vệ chủ quyền, an toàn quốc gia trên không gian mạng. Tuy nhiên, trong quá trình triển khai, Luật vẫn bộc lộ một số bất cập, đòi hỏi cần có những điều chỉnh, bổ sung để phù hợp hơn với tình hình thực tiễn. Để luật thật sự đi vào cuộc sống và phát huy hiệu quả, cần tiếp tục rà soát, điều chỉnh, bổ sung các quy định cho phù hợp với thực tế, đảm bảo cân bằng giữa bảo vệ an ninh và tôn trọng quyền công dân... Đó cũng là những nội dung được đề cập khá đầy đủ trong bài viết này.

● **Từ khóa:** Luật An ninh mạng; không gian mạng; quyền con người.

● **ABSTRACT:** In the context of the strong development of the Fourth Industrial Revolution, cyberspace has become an indispensable part of the economic, social, and political life of every nation. However, along with this advancement, the rise of cyber security threats such as high-tech crimes, cyberattacks, and the spread of harmful and hostile information that undermines national interests, organizations, and individuals has become increasingly serious. In response to this reality, the Law on Cybersecurity (promulgated on June 12, 2018, and effective from January 1, 2019) was introduced to safeguard national sovereignty and security in cyberspace. Nevertheless, during implementation, the Law has revealed certain limitations, requiring adjustments and supplements to better align with practical circumstances. To ensure the Law is effectively enforced and achieves its intended impact, continuous review, amendment, and refinement of relevant provisions are necessary in order to balance national security protection with the respect for citizens' rights. These are also the core issues discussed comprehensively in this article.

● **Keywords:** Cybersecurity Law; cyberspace; human rights.

Ngày nhận bài: 29/9/2025 Ngày bình duyệt: 24/10/2025 Ngày duyệt đăng: 28/10/2025

TỔNG QUAN VỀ AN NINH MẠNG VÀ LUẬT AN NINH MẠNG

Về mặt khái niệm, **An ninh mạng** là tập hợp các biện pháp kỹ thuật, quản lý và pháp lý nhằm bảo vệ hệ thống mạng, dữ liệu và thông tin trên không gian mạng khỏi các mối đe dọa như tấn công mạng, phần mềm độc hại, truy cập trái phép, rò rỉ dữ liệu, và các hành vi phá hoại khác.

Mục tiêu chính của an ninh mạng là: Bảo vệ chủ quyền, lợi ích quốc gia, an ninh trật tự trên không gian mạng; Phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi vi phạm pháp luật trên mạng; Bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân khi tham gia hoạt động trên mạng. Trong đó hàm chứa các yếu tố: Tính bảo mật (Confidentiality): Dữ liệu không bị truy cập trái phép; Tính toàn vẹn (Integrity): Dữ liệu không bị thay đổi hoặc phá hoại; Tính sẵn sàng (Availability): Hệ thống và dữ liệu sẵn sàng phục vụ khi cần.

Trên thực tế, những lợi ích mà mạng xã hội nói chung mang lại cho cuộc sống của con người là điều không thể phủ nhận. Tuy nhiên, mạng xã hội cũng đồng thời đặt ra nhiều thách thức đối với quốc gia, cũng như với cộng đồng xã hội; nhất là việc đánh giá tính chân thực của thông tin mạng trong hầu hết mọi lĩnh vực. Ở đó, thông tin đều khó xác định, khó kiểm chứng tính chân thực mà mình nhận được hoặc quan tâm. Điều này dẫn tới việc kẻ xấu có thể lợi dụng Internet, mạng xã hội vì những mục đích xấu, như: Đưa thông tin giật gân nhằm câu view, câu like; đưa thông tin về đời tư do hẹp hòi, ích kỷ; nhất là thông tin chống phá nhà nước... Thực tế đó cho thấy, trong thời đại ngày nay, vấn đề An ninh quốc gia, trật tự an toàn xã hội và quyền con người đang đứng trước những thách thức mới. Nếu như trước đây An ninh quốc gia là bảo vệ chủ quyền vùng đất, vùng biên, vùng trời, chế độ xã hội... thì ngày nay, đó còn là bảo vệ an ninh không gian mạng.

Luật An ninh mạng được Quốc hội thông qua ngày 12/6/2018, cũng là nhằm phát huy mặt tích cực, đồng thời hạn chế tới mức cao nhất những mặt tiêu cực của mạng xã hội, vì sự phát triển ổn định của đất nước và sự yên bình của người dân... Trong quá trình thực hiện, trên thực tế, Luật đã có những tác động tích cực như: Tăng cường kiểm soát, giảm thiểu hành vi vi phạm pháp luật trên mạng; Bảo vệ dữ liệu cá nhân và quyền riêng tư; Góp phần giữ vững an ninh quốc gia trong bối cảnh chiến tranh mạng ngày càng phổ biến.

Trong Luật An ninh mạng có đưa ra khái niệm về không gian mạng; cụ thể: Không gian mạng là khái niệm rộng hơn Internet. Nó là mạng lưới kết nối toàn cầu của các cơ sở hạ tầng công nghệ thông tin, bao gồm Internet, các mạng viễn thông, các hệ thống máy tính và các hệ thống xử lý và điều khiển trong các ngành công nghiệp trọng yếu, là môi trường đặc biệt “*môi trường ảo*”, nơi mà con người có thể trao đổi thông tin và tương tác với nhau, không bị giới hạn bởi không gian và thời gian.

Luật an ninh mạng liên quan đến việc bảo vệ quyền con người, cũng như đưa ra các ý kiến phản bác lại quan điểm của một số đối tượng thù địch, phản động, chống đối xuyên tạc cho rằng hoạt động xử lý tin giả, thông tin sai sự thật, thông tin xấu độc là vi phạm quyền con người, quyền tự do ngôn luận.

Luật An ninh mạng có một số nội dung chính sau đây:

Điều 8: Nghiêm cấm các hành vi sử dụng không gian mạng để tuyên truyền chống phá nhà nước, kích động bạo lực, gây rối trật tự công cộng, tung tin sai sự thật...

Trách nhiệm của doanh nghiệp (Điều 26): Doanh nghiệp trong và ngoài nước cung cấp dịch vụ tại Việt Nam phải lưu trữ dữ liệu cá nhân tại Việt Nam và phải có chi nhánh hoặc văn phòng đại diện. Doanh nghiệp cung cấp dịch vụ Internet có trách

nhiệm quản lý, phòng ngừa, phát hiện và ngăn chặn phần mềm độc hại. Doanh nghiệp cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại.

Điều 29: Bảo vệ thông tin cá nhân trên không gian mạng. Trong đó, biện pháp bảo vệ an ninh mạng bao gồm thẩm định, đánh giá, kiểm tra, giám sát, ứng phó sự cố, đấu tranh bảo vệ an ninh mạng, sử dụng mật mã, yêu cầu xóa bỏ thông tin trái pháp luật, thu thập dữ liệu điện tử, và phong tỏa, hạn chế hoạt động của hệ thống thông tin.

Điều 34-38: Quy định về xử lý vi phạm, kiểm tra và đánh giá an ninh mạng đối với các hệ thống thông tin quan trọng.

NHỮNG KẾT QUẢ ĐẠT ĐƯỢC

Sau gần 6 năm triển khai thực hiện, Luật An ninh mạng đã góp phần quan trọng trong việc bảo vệ an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng, đồng thời nâng cao nhận thức và trách nhiệm của các cơ quan, tổ chức, doanh nghiệp và người dân trong việc sử dụng Internet an toàn, hiệu quả. Luật đã có những tác động tích cực như: Tăng cường kiểm soát, giảm thiểu hành vi vi phạm pháp luật trên mạng; Bảo vệ dữ liệu cá nhân và quyền riêng tư; Góp phần giữ vững an ninh quốc gia trong bối cảnh chiến tranh mạng ngày càng phổ biến.

Một số kết quả cụ thể như sau:

1. Luật An ninh mạng đã tạo hành lang pháp lý rõ ràng, đồng bộ cho các cơ quan chức năng trong công tác phòng ngừa, phát hiện, xử lý các hành vi sử dụng không gian mạng xâm phạm đến an ninh quốc gia, trật tự an toàn xã hội. Nhiều vụ việc liên quan đến tuyên truyền chống phá Đảng, Nhà nước, kích động bạo lực, xuyên tạc lịch sử, bịa đặt thông tin sai sự thật... đã được xử lý kịp thời, qua đó góp phần giữ vững ổn định chính trị và trật tự xã hội.

2. Nâng cao hiệu quả quản lý nhà

nước trong lĩnh vực thông tin mạng: Các bộ, ngành đã phối hợp chặt chẽ trong công tác thanh tra, kiểm tra, xử lý vi phạm trên môi trường mạng. Việc yêu cầu các doanh nghiệp cung cấp dịch vụ xuyên biên giới như Google, Facebook, YouTube... tuân thủ pháp luật Việt Nam đã có những chuyển biến tích cực. Nhiều nội dung xấu, độc, vi phạm pháp luật đã bị gỡ bỏ theo yêu cầu của cơ quan chức năng.

3. Một trong những điểm nổi bật của Luật An ninh mạng là bảo vệ quyền riêng tư, thông tin cá nhân của người dân trên không gian mạng. Các quy định yêu cầu tổ chức, doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ tại Việt Nam phải lưu trữ dữ liệu người dùng và bảo đảm an toàn thông tin đã giúp người dùng Internet Việt Nam được bảo vệ tốt hơn trước các nguy cơ mất cắp, lộ lọt thông tin cá nhân.

4. Thông qua công tác tuyên truyền, phổ biến Luật An ninh mạng, nhận thức của người dân về việc sử dụng mạng xã hội một cách văn minh, có trách nhiệm đã được nâng lên. Nhiều chương trình, lớp tập huấn, hướng dẫn kỹ năng phòng tránh thông tin giả, tin xấu độc đã được triển khai rộng khắp trong học đường, cơ quan, doanh nghiệp và cộng đồng.

5. Thông qua các điều khoản về phòng chống khủng bố mạng, gián điệp mạng, xâm phạm bí mật cá nhân, bí mật doanh nghiệp; góp phần nâng cao ý thức chấp hành pháp luật của cá nhân, tổ chức hoạt động trên không gian mạng.

Có thể nói, Luật An ninh mạng là bước tiến quan trọng trong quá trình hoàn thiện hệ thống pháp luật nhằm bảo vệ chủ quyền, an ninh quốc gia trong kỷ nguyên số. Tuy nhiên, trước sự phát triển không ngừng của công nghệ và các chiêu trò mới trên không gian mạng, việc tiếp tục hoàn thiện các quy định pháp lý, tăng cường hợp tác quốc tế, nâng cao năng lực cán bộ và ý thức của người dân là điều cần thiết để Luật An ninh

mạng phát huy hiệu quả hơn nữa trong thời gian tới.

MỘT SỐ TỒN TẠI, HẠN CHẾ

Bên cạnh những kết quả quan trọng đạt được, Luật An ninh mạng, qua quá trình thực hiện cũng bộc lộ một số tồn tại, hạn chế:

1. Một số quy định còn mang tính chung chung, chưa có hướng dẫn chi tiết thi hành, gây khó khăn cho việc áp dụng. Ví dụ như điều khoản yêu cầu doanh nghiệp nước ngoài đặt máy chủ tại Việt Nam chưa rõ ràng về cơ chế thực thi.

2. Còn mâu thuẫn, chồng chéo với các luật khác, như: Có sự giao thoa giữa Luật An ninh mạng và Luật An toàn thông tin mạng, Luật Công nghệ thông tin... gây khó khăn trong phối hợp thực hiện.

3. Một số quy định bị cho là có thể dẫn đến hạn chế quyền tự do biểu đạt, tạo cảm giác kiểm soát quá mức đối với người dùng mạng.

4. Việc đảm bảo thực thi các quy định về giám sát, kiểm soát và xử lý vi phạm trên mạng đòi hỏi hệ thống kỹ thuật hiện đại và đội ngũ cán bộ có chuyên môn cao. Nhưng hiện nay còn chưa đáp ứng đầy đủ được.

Sở dĩ còn có những hạn chế là do:

- Quá trình xây dựng luật chưa bao quát hết thực tiễn, một số nội dung mới chưa được quy định trong pháp luật Việt Nam nên khó tránh khỏi thiếu sót.

- Tốc độ phát triển công nghệ quá nhanh: Các hình thức tội phạm mạng ngày càng tinh vi, trong khi pháp luật thường có độ trễ.

- Thiếu sự tham gia của các bên liên quan: Doanh nghiệp, đặc biệt là doanh nghiệp công nghệ nước ngoài, còn thiếu tiếng nói trong việc góp ý, phản hồi chính sách.

- Cơ chế thực thi và phối hợp chưa hiệu

quả: Việc xử lý các vụ việc trên không gian mạng vẫn còn chậm, chưa có sự đồng bộ giữa các ngành, các cấp.

Có thể nói, An ninh mạng đang trở thành một trong những thách thức lớn nhất của thời đại số. Việc ban hành và thực thi luật An ninh mạng là cần thiết để bảo vệ lợi ích của quốc gia và công dân. Tuy nhiên, cần có sự điều chỉnh linh hoạt và minh bạch nhằm đảm bảo hài hòa giữa an ninh, phát triển công nghệ, và quyền con người.

GIẢI PHÁP HOÀN THIỆN VÀ NÂNG CAO HIỆU QUẢ THỰC THI LUẬT AN NINH MẠNG

Để nâng cao hiệu quả thực hiện Luật An ninh mạng, cần triển khai đồng bộ nhiều giải pháp từ hoàn thiện chính sách pháp luật đến tăng cường năng lực thực thi trên thực tế. Trước hết, cần tiếp tục rà soát, sửa đổi, bổ sung các quy định pháp luật liên quan nhằm bảo đảm sự thống nhất, đồng bộ giữa Luật An ninh mạng và các văn bản quy phạm pháp luật khác. Đồng thời, tăng cường đầu tư vào hạ tầng kỹ thuật, ứng dụng công nghệ hiện đại trong kiểm soát, phát hiện và xử lý các hành vi vi phạm trên không gian mạng. Bên cạnh đó, cần đẩy mạnh công tác phối hợp giữa các cơ quan chức năng, doanh nghiệp cung cấp dịch vụ mạng và các tổ chức xã hội để nâng cao hiệu quả giám sát, bảo mật thông tin. Song song với đó, việc nâng cao nhận thức, trách nhiệm của người dân trong sử dụng Internet an toàn, lành mạnh cũng là yếu tố then chốt để bảo vệ an ninh mạng quốc gia một cách bền vững. Dưới đây là những giải pháp chính:

1. Hoàn thiện hệ thống pháp luật và hướng dẫn thi hành:

- Hoàn thiện văn bản hướng dẫn chi tiết Luật An ninh mạng để đảm bảo tính khả thi trong thực tiễn. Xây dựng quy chuẩn, tiêu chuẩn kỹ thuật về an ninh mạng áp dụng cho hệ thống thông tin quan trọng quốc gia. Bổ sung chế tài xử phạt cụ thể, nghiêm minh đối với các hành vi vi phạm.

- *Ban hành các văn bản hướng dẫn chi tiết*: Chính phủ và các bộ, ngành liên quan cần sớm ban hành các nghị định, thông tư hướng dẫn thi hành để cụ thể hóa các điều khoản của Luật.

- *Sửa đổi, bổ sung luật cho phù hợp với thực tiễn*: Nghiên cứu cập nhật, điều chỉnh các quy định có nguy cơ xâm phạm quyền tự do cá nhân, bảo đảm hài hòa giữa an ninh và quyền con người.

2. *Tăng cường năng lực kỹ thuật và hạ tầng an ninh mạng*: Đầu tư nâng cấp hệ thống giám sát, phát hiện, ứng phó sự cố an ninh mạng tại các cơ quan, tổ chức nhà nước và doanh nghiệp lớn. Phát triển các sản phẩm công nghệ an ninh mạng nội địa để giảm phụ thuộc vào công nghệ nước ngoài. Triển khai hệ thống bảo vệ tự động, cảnh báo sớm các nguy cơ tấn công mạng. Xây dựng các trung tâm giám sát an toàn thông tin hiện đại, đồng bộ.

3. *Nâng cao nhận thức và đào tạo nguồn nhân lực*: Tổ chức các chương trình đào tạo, tuyên truyền về an ninh mạng cho cán bộ, công chức và người dân. Đưa nội dung an ninh mạng vào chương trình giáo dục ở các cấp học, nhất là đại học và cao đẳng kỹ thuật. Phát triển đội ngũ chuyên gia an ninh mạng, đặc biệt là trong các cơ quan nhà nước và lực lượng chuyên trách. Tăng cường đào tạo chuyên gia an ninh mạng trong cả khu vực công và tư.

4. *Tăng cường vai trò của các cơ quan chức năng*: Thường xuyên kiểm tra, đánh giá mức độ an toàn thông tin tại các cơ quan, tổ chức. Phát hiện và xử lý nghiêm các hành vi vi phạm Luật An ninh mạng, đặc biệt là các hành vi xuyên tạc, kích động, phá hoại trật tự xã hội trên không gian mạng. Tăng cường hợp tác với các nhà cung cấp dịch vụ xuyên biên giới (như Google, Facebook...) để kiểm soát nội dung vi phạm. Phát huy vai trò của Bộ Công an, Bộ Thông tin và Truyền thông, Bộ Quốc phòng trong thực thi pháp luật

và bảo vệ không gian mạng. Phân định rõ trách nhiệm giữa các cơ quan trong giám sát, xử lý sự cố và hỗ trợ người dùng. Thiết lập cơ chế phối hợp chặt chẽ giữa các bộ, ngành, địa phương và doanh nghiệp.

5. *Đẩy mạnh hợp tác quốc tế về an ninh mạng*: Tham gia các diễn đàn, tổ chức quốc tế về an ninh mạng để chia sẻ thông tin, kinh nghiệm và phối hợp ứng phó sự cố. Thiết lập cơ chế hợp tác song phương và đa phương trong phòng, chống tội phạm mạng. Học hỏi các mô hình quản lý không gian mạng hiệu quả từ các quốc gia tiên tiến. Đảm bảo rằng Luật An ninh mạng phù hợp với các cam kết quốc tế mà Việt Nam tham gia, tránh tạo rào cản với doanh nghiệp nước ngoài.

6. *Tuyên truyền và nâng cao nhận thức cộng đồng*: Nâng cao nhận thức của người dân, đặc biệt là giới trẻ, về an toàn thông tin cá nhân, trách nhiệm pháp lý khi sử dụng mạng. Phản ánh kịp thời các vấn đề an ninh mạng, góp phần tạo ra môi trường mạng lành mạnh. Tăng cường phổ biến, giáo dục các quy định của pháp luật về quản lý không gian mạng: Các hình thức giáo dục cần được vận dụng đa dạng, phong phú và linh hoạt như: phối hợp giữa cơ quan chức năng với các cơ quan, địa phương, đơn vị, doanh nghiệp, cơ sở giáo dục tổ chức nói chuyện chuyên đề, phổ biến pháp luật; tuyên truyền Luật An ninh mạng; các cuộc thi tìm hiểu về ATTT; góp ý xây dựng chương trình giáo dục ATTT mạng của các cơ sở giáo dục hoặc tham gia biên soạn các tài liệu liên quan đến ATTT mạng.

7. *Bồi dưỡng kỹ năng nhận diện các âm mưu, thủ đoạn tấn công mạng và các hình thái phát sinh trên không gian mạng*: Hoạt động tấn công không gian mạng rất đa dạng và tinh vi như: làm mất kết nối Internet, đánh sập các website của chính phủ, cơ quan, đơn vị, nhà trường, doanh nghiệp; giả mạo các website nhằm lừa đảo; cài găm vào máy tính cá nhân hoặc lấy tài khoản và mật

khẩu; đánh cắp dữ liệu cá nhân (hình ảnh, file, video); tấn công bằng mã độc (theo tệp đính kèm trong email hoặc ẩn trong quảng cáo Skype); tấn công ẩn danh bằng những phần mềm độc hại (phần mềm diệt virus, các trình duyệt); tấn công qua usb, đĩa CD, địa chỉ IP, server,...

8. *Nâng cao ý thức phòng tránh, tự vệ và sử dụng biện pháp kỹ thuật để khắc phục hậu quả trong trường hợp bị tấn công trên không gian mạng:* Nêu cao ý thức chính

trị, trách nhiệm, nghĩa vụ công dân đối với nhiệm vụ bảo vệ không gian mạng quốc gia. Tuân thủ quy định của pháp luật về bảo vệ an ninh mạng; kịp thời cung cấp thông tin liên quan đến an ninh mạng, nguy cơ đe dọa an ninh mạng và các hành vi xâm phạm khác, thực hiện yêu cầu và hướng dẫn của cơ quan quản lý nhà nước có thẩm quyền; giúp đỡ, tạo điều kiện cho người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng./.

TÀI LIỆU THAM KHẢO:

1. *Luật An ninh mạng 2018 (Luật số 24/2018/QH14) được Quốc hội Việt Nam thông qua ngày 12/6/2018.*
2. *Nghị định 53/2022/NĐCP (ban hành ngày 15/8/2022) - Nghị định hướng dẫn một số điều của Luật An ninh mạng.*
3. *Văn bản giới thiệu / tóm lược Luật An ninh mạng (giới thiệu pháp lý, phạm vi điều chỉnh.*
4. *Bài viết “Quản lý nhà nước về an toàn*

- thông tin mạng Internet của một số quốc gia trên thế giới và kinh nghiệm cho Việt Nam” (trên trang của Bộ Thông tin và Truyền thông).*
5. *Bài “Thách thức an ninh mạng khi Việt Nam bước vào thời đại 5G và IoT” (Báo Pháp Luật TP. Hồ Chí Minh).*
6. *Bài viết về việc Bộ Công an đề xuất hợp nhất Luật An ninh mạng với Luật An toàn thông tin mạng, xây dựng “Luật An ninh mạng năm 2025” – Báo điện tử Chính phủ 11/4/2025*