

KIẾN NGHỊ HOÀN THIÊN PHÁP LUẬT HÌNH SỰ VỀ AN NINH MẠNG Ở VIỆT NAM HIỆN NAY

BÙI THỊ THÙY DUNG*

Thời gian qua, Đảng, Nhà nước ta đã ban hành nhiều chủ trương, chính sách, pháp luật và các giải pháp để thúc đẩy ứng dụng, phát triển công nghệ thông tin trong các lĩnh vực gắn với bảo vệ vững chắc chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng. Trên cơ sở chỉ ra các hạn chế, bất cập của pháp luật hình sự về an ninh mạng ở Việt Nam hiện nay, bài viết đề xuất một số kiến nghị hoàn thiện pháp luật hình sự về lĩnh vực này

Từ khóa: Việt Nam; an ninh mạng; pháp luật hình sự; thực trạng; giải pháp.

In recent years, the Party and the State of Vietnam have issued numerous guidelines, policies, laws, and solutions to promote the application and development of information technology in various fields, closely associated with firmly safeguarding national sovereignty, interests, and security in cyberspace. This article proposes several recommendations for improving the legal framework in this field by analyzing the current limitations and inadequacies of Vietnam's criminal law on cybersecurity.

Keywords: Vietnam; cybersecurity; criminal law; current situation; solutions.

NGÀY NHẬN: 11/3/2025 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 23/4/2025 NGÀY DUYỆT: 16/5/2025

DOI: <https://doi.org/10.59394/qlnn.352.2025.1176>

1. Đặt vấn đề

An ninh mạng là một lĩnh vực then chốt trong kỷ nguyên số. Sự gia tăng các hành vi xâm phạm an ninh mạng đã và đang gây ra những hậu quả nghiêm trọng. Pháp luật hình sự Việt Nam hiện hành đã có những quy định nhất định để điều chỉnh các hành vi xâm phạm lĩnh vực này. Tuy nhiên, trước sự phát triển không ngừng của các mối đe dọa đến an ninh mạng, việc đánh giá thực trạng và kiến nghị các giải pháp nhằm hoàn thiện khung pháp lý và nâng cao hiệu quả bảo vệ an ninh quốc gia và trật tự an toàn xã hội trên không gian mạng là vô cùng cần thiết.

2. Thực trạng pháp luật hình sự về an ninh mạng ở Việt Nam hiện nay

Hiện nay, pháp luật hình sự về an ninh mạng ở Việt Nam được quy định tại nhiều văn bản quy phạm pháp luật, như: *Bộ luật Hình sự* năm 2015 (sửa đổi, bổ sung năm 2017); *Luật Công nghệ cao* năm 2008 (sửa đổi, bổ sung năm 2019); *Luật Tần số vô tuyến điện* năm 2009 (sửa đổi, bổ sung năm 2022); *Luật An toàn thông tin mạng* năm 2015 (sửa đổi, bổ sung năm 2018); *Luật Bảo vệ bí mật Nhà nước* năm 2018; *Luật An ninh mạng* năm

* *ThS, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*

2018; *Luật Giao dịch điện tử* năm 2023; *Luật Viễn thông* năm 2023; *Luật Căn cước* năm 2024... Những luật này là cơ sở pháp lý để triển khai các hoạt động bảo vệ an ninh mạng và điều tra, xử lý các hành vi vi phạm pháp luật về an ninh mạng, góp phần tích cực nâng cao hiệu quả công tác bảo vệ an ninh mạng, tạo nên một không gian mạng có tính an toàn hơn, lành mạnh hơn. Chẳng hạn:

(1) Tại mục 2 *Bộ luật Hình sự* năm 2015 (sửa đổi, bổ sung năm 2017) đã quy định các tội danh trong lĩnh vực công nghệ thông tin, mạng viễn thông: 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 (Điều 285); tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 286); tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287); tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288); tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289); tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290); tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291); 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 (Điều 293); tội cố ý gây nhiễu có hại (Điều 294).

(2) Điều 8 *Luật An ninh mạng* năm 2018 đã quy định các hành vi bị nghiêm cấm, như: thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; 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 quan trọng về an ninh quốc gia; sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của

mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác; chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng; lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi ...

(3) Điều 6 *Luật Giao dịch điện tử* năm 2023 đã quy định 8 hành vi bị nghiêm cấm, gồm: lợi dụng giao dịch điện tử xâm phạm đến lợi ích quốc gia, dân tộc, an ninh quốc gia, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cản trở hoặc ngăn chặn trái pháp luật quá trình tạo ra, gửi, nhận, lưu trữ thông điệp dữ liệu hoặc có hành vi khác nhằm phá hoại hệ thống thông tin phục vụ giao dịch điện tử; thu thập, cung cấp, sử dụng, tiết lộ, hiển thị, phát tán, kinh doanh trái pháp luật thông điệp dữ liệu; giả mạo, làm sai lệch hoặc xóa, hủy, sao chép, di chuyển trái pháp luật một phần hoặc toàn bộ thông điệp dữ liệu; tạo ra thông điệp dữ 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; cản trở việc lựa chọn thực hiện giao dịch điện tử; hành vi khác bị nghiêm cấm theo quy định của luật.

(4) Điều 9 *Luật Viễn thông* năm 2023 đã quy định 5 hành vi bị nghiêm cấm, gồm: lợi

dụng hoạt động viễn thông nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; xâm phạm an ninh quốc gia, trật tự, an toàn xã hội gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân; 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 khác; cản trở trái pháp luật việc thiết lập cơ sở hạ tầng viễn thông, gây rối, phá hoại việc thiết lập cơ sở hạ tầng viễn thông, việc cung cấp và sử dụng hợp pháp các dịch vụ viễn thông; thiết lập cơ sở hạ tầng viễn thông, cung cấp dịch vụ viễn thông khi chưa được phép thực hiện theo quy định của *Lược này*; sử dụng thiết bị, phần mềm gửi, truyền, nhận thông tin qua mạng viễn thông để thực hiện những hành vi vi phạm pháp luật.

3. Một số khó khăn, bất cập

Hiện nay, pháp luật hình sự về an ninh mạng nước ta vẫn còn một số khó khăn, bất cập, đó là:

(1) Chưa có quy định thống nhất về khách thể “an ninh không gian mạng”. Mặc dù tại Điều 6 *Lược An ninh mạng* năm 2018 đã xác định “nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng” và thông qua các biện pháp phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; trong đó có biện pháp phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội đã được quy định tại Điều 18 để bảo vệ an ninh mạng. Nhưng tại Điều 1 và Điều 8 của *Bộ luật Hình sự* năm 2015 (sửa đổi, bổ sung năm 2017) lại chưa đề cập đến khách thể này.

(2) Chưa có chế tài xử lý đối với hành vi vi phạm pháp luật hình sự về an ninh mạng liên quan đến hoạt động kinh doanh tiền ảo, tiền

kỹ thuật số, tài sản ảo. Trong những năm gần đây, hoạt động kinh doanh, giao dịch, khai thác tiền ảo, tiền mã hóa, tài sản ảo đã gây ra nhiều hệ lụy nghiêm trọng đặc biệt đến an ninh, trật tự và sự phát triển của kinh tế đất nước. Về vấn đề này, nhiều quốc gia trên thế giới đã chính thức tuyên bố giao dịch, khai thác tiền ảo, tiền mã hóa là bất hợp pháp và bị nghiêm cấm dưới mọi hình thức. Thực tế cho thấy, việc nghiên cứu, rà soát những quy định trong hệ thống pháp luật nói chung để quản lý hoạt động liên quan đến tiền ảo, tiền kỹ thuật số, tài sản ảo là hết sức cần thiết.

(3) Chưa có chế tài xử lý đối với hành vi vi phạm pháp luật hình sự về an ninh mạng liên quan đến hoạt động thu thập, sử dụng, khai thác, chuyển nhượng, xử lý dữ liệu cá nhân trái quy định của pháp luật. Thời gian qua, việc mua bán, lấy cắp, khai thác, sử dụng dữ liệu cá nhân đã trở nên phổ biến và gây ra những hậu quả rất nghiêm trọng đến quyền và lợi ích hợp pháp của nhiều cá nhân, đe dọa tới sự phát triển ổn định của xã hội. Thông tin cá nhân người sử dụng các ứng dụng, dịch vụ trên không gian mạng đang bị thu thập, khai thác, sử dụng công khai bởi các doanh nghiệp cung cấp dịch vụ nội dung số, thương mại điện tử, nhiều ứng dụng lưu trữ dữ liệu tại nước ngoài. Đối tượng xấu sử dụng những thông tin cá nhân mà chúng đánh cắp, mua bán được để thực hiện các hành vi phạm tội, như: làm giấy tờ giả, tống tiền, lừa đảo, chiếm đoạt tài sản, mua bán người, xâm hại tình dục, xúc phạm uy tín, danh dự của nạn nhân... Trong khi đó, liên quan đến dữ liệu cá nhân, *Bộ luật Hình sự* hiện nay mới quy định “tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác” (Điều 159); tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288); tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291). Cả 3 tội danh này đều không quy định để xử lý trực tiếp đối với hành

vi phạm về dữ liệu cá nhân như nêu trên. Chính vì thế, cần nghiên cứu để quy định là tội phạm đối với các hành vi xâm phạm đến dữ liệu cá nhân, đó là: hành vi thu thập (đánh cắp, mua bán, tặng cho...), sử dụng, khai thác, chuyển nhượng trái phép dữ liệu cá nhân và hành vi để lộ hoặc xử lý dữ liệu cá nhân trái quy định của pháp luật.

(4) Chưa có chế tài xử lý đối với hành vi vi phạm pháp luật hình sự về an ninh mạng liên quan đến hoạt động lập trình và sử dụng phần mềm AI để thực hiện hành vi phạm tội.

4. Một số kiến nghị hoàn thiện pháp luật hình sự về an ninh mạng ở Việt Nam hiện nay

Thứ nhất, cần bổ sung và làm rõ khái niệm “an ninh không gian mạng” trong *Bộ luật Hình sự*. Theo đó, khái niệm này có thể bổ sung một khoản mới vào Điều 1 hoặc Điều 8: “an ninh không gian mạng” là sự ổn định, an toàn và khả năng phòng thủ của không gian mạng quốc gia, bảo đảm hoạt động bình thường, liên tục, an toàn của hệ thống thông tin quan trọng quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng. Việc xác định rõ khách thể “an ninh không gian mạng” trong *Bộ luật Hình sự* sẽ tạo cơ sở pháp lý vững chắc cho việc truy cứu trách nhiệm hình sự đối với các hành vi xâm phạm đến lĩnh vực này, bảo đảm tính thống nhất và đồng bộ của hệ thống pháp luật.

Thứ hai, cần nghiên cứu và bổ sung các điều, khoản cụ thể trong *Bộ luật Hình sự* để làm rõ các hành vi vi phạm liên quan đến hoạt động kinh doanh, giao dịch, khai thác tiền ảo, tiền kỹ thuật số, tài sản ảo gây ra hậu quả nghiêm trọng đến an ninh, trật tự và kinh tế. Xây dựng các tội danh mới phát sinh hoặc sửa đổi, bổ sung các tội danh hiện có (ví dụ: tội rửa tiền, tội lừa đảo chiếm đoạt tài sản, tội vi phạm quy định về hoạt động ngân hàng, hoạt động khác liên quan đến ngân hàng...) để bao quát các hành vi phạm tội sử dụng tiền ảo, tài sản ảo làm công cụ hoặc đối tượng.

Thứ ba, cần bổ sung các tội danh cụ thể trong *Bộ luật Hình sự* để xử lý nghiêm các hành vi xâm phạm dữ liệu cá nhân. Chẳng hạn: quy định chi tiết về các hành vi để lộ hoặc xử lý dữ liệu cá nhân trái với quy định của pháp luật gây hậu quả nghiêm trọng; quy định cụ thể về các hành vi thu thập (đánh cắp, mua bán, tặng cho...), sử dụng, khai thác, chuyển nhượng trái phép dữ liệu cá nhân gây hậu quả nghiêm trọng hoặc thu lợi bất chính lớn. Bên cạnh đó, cần xác định rõ các yếu tố cấu thành tội phạm để có hình phạt tương xứng, bởi bảo vệ dữ liệu cá nhân là một yêu cầu cấp thiết trong bối cảnh số hóa hiện nay. Vì vậy, việc cụ thể hóa các hành vi xâm phạm dữ liệu cá nhân sẽ giúp bảo vệ quyền và lợi ích hợp pháp của cá nhân và sự ổn định của xã hội.

Thứ tư, sự phát triển nhanh chóng của AI tạo ra những nguy cơ tiềm ẩn cho an ninh mạng. Việc có chế tài xử lý đối với các hành vi lợi dụng AI để phạm tội là cần thiết để bảo đảm an toàn cho không gian mạng và xã hội. Vì vậy, cần nghiên cứu và bổ sung các quy định để xử lý các hành vi lợi dụng AI để thực hiện tội phạm trên không gian mạng, như: (1) Tội sử dụng trái phép phần mềm AI để phạm tội: cần chi tiết hóa về hành vi cố ý lập trình, huấn luyện hoặc sử dụng phần mềm AI nhằm thực hiện các hành vi phạm tội đã được quy định trong *Bộ luật Hình sự* (ví dụ: lừa đảo, tấn công mạng, phát tán thông tin độc hại...); (2) Cần xem xét trách nhiệm hình sự của cả người tạo ra và người sử dụng AI trong trường hợp AI được sử dụng để thực hiện hành vi phạm tội □

Tài liệu tham khảo:

1. Tô Lâm (2021). *Chủ quyền không gian mạng - Yêu cầu thời đại và nghĩa vụ của quốc gia*. H. NXB Công an nhân dân.

2. Hoàn thiện pháp luật bảo vệ an ninh mạng hệ thống thông tin quan trọng về an ninh quốc gia. <https://lsvn.vn>, ngày 03/02/2025.