Giáo dục an toàn thông tin và phòng chống vi phạm pháp luật trên không gian mạng cho sinh viên tại Trung tâm Giáo dục Quốc phòng và An ninh, Đại học Thái Nguyên

Nguyễn Quang Công*

**Trung tâm Giáo dục Quốc phòng và An ninh, Đại học Thái Nguyên*
Received: 7/12/2023; Accepted:15/12/2023; Published: 20/01/2024

***Abstract**: From the practice of developing information on the Internet, the situation of law violations and crimes on the Internet, inadequacies in the management of information content on the internet and the problems posed to content management information on the internet is necessary to deploy comprehensive solutions to promote the positive aspects and limit the negative aspects of the Internet, meeting the country's political tasks in the new situation.*

***Keywords:** Information, security measures and education*

1. Đặt Vấn đề

Internet bắt đầu xuất hiện từ những năm thập niên 60 của thế kỷ XX. Tuy nhiên, tại thời điểm đó nó chỉ được sử dụng nội bộ và phục vụ chủ yếu cho quân sự. Ngày 19/11/1997 là ngày đầu tiên Việt Nam chính thức hòa vào mạng Internet toàn cầu, sau hơn 20 năm hoạt động Internet trở thành một thuật ngữ hầu như ai cũng biết, một phương tiện truyền thông mà phần lớn con người đã và đang sử dụng phục vụ cho nhu cầu cuộc sống, sinh hoạt hàng ngày. Do bản chất công nghệ đã định hình, Internet là một môi trường mở hướng tới tự do truyền thông cho cộng đồng trên toàn thế giới, cho phép người sử dụng tự do cung cấp, tìm kiếm và sử dụng thông tin mà không có giới hạn về địa lý, lãnh thổ. Và trong đa số các trường hợp sử dụng dịch vụ thông tin trên Internet, thông tin về cá nhân của người dùng không cần xác thực. Điều đó một mặt tạo điều kiện thuận lợi một cách tối đa cho người muốn cung cấp, sử dụng thông tin trên Internet, loại bỏ tối đa những ràng buộc về pháp lý, những mặc cảm trong ý thức để tham gia vào môi trường thông tin trên Internet; mặt khác nó cũng là môi trường để một số tổ chức, cá nhân với động cơ xấu có thể che dấu danh tính để cung cấp thông tin sai trái, độc hại; thậm chí xóa bỏ dấu vết để thực hiện hành vi tội phạm, lừa đảo, trong đó phổ biến nhất là những hành vi tội phạm xuyên quốc gia.

Nhận thức được tính hai mặt của công nghệ Internet cũng như nội dung thông tin trên Internet giúp chúng ta có định hướng chính sách và giải pháp quản lý thông tin phù hợp với tính chất thông tin, bản chất công nghệ nhằm phát huy mặt tích cực và hạn chế những tác động tiêu cực của thông thông tin sai trái, độc hại. Ở Việt Nam, mặc dù công tác quản lý nhà nước về thông tin trên Internet trong thời gian qua đã tạo được môi trường thuận lợi cho Internet phát triển, đóng góp tích cực cho nền kinh tế, xã hội, tuy nhiên vẫn còn tồn tại một số vấn đề như: các thông tin có nội dung xuyên tạc và chống phá Đảng, Nhà nước, phá hoại khối đại đoàn kết dân tộc vẫn được tuyên truyền, khai thác khá rộng rãi trên mạng Internet và phát tán trong một bộ phận nhân dân, gây nên tâm lý hoài nghi vào sự lãnh đạo của Đảng, làm mất uy tín của lãnh tụ, gây chia rẽ trong một bộ phận tôn giáo. Các thông tin độc hại (bạo lực, khiêu dâm, ma túy...), các chương trình trò chơi điện tử trực tuyến (online games) có nội dung không phù hợp với thuần phong mỹ tục, văn hóa của Việt Nam vẫn thâm nhập, lây lan qua Internet đến người dùng trong nước, ảnh hưởng tiêu cực đến lối sống, sinh hoạt của một bộ phận cán bộ, thanh thiếu niên, học sinh, sinh viên nói chung cũng như SV Đại học Thái Nguyên nói riêng. Hoạt động sử dụng Internet để tấn công, truy cập bất hợp pháp, phát tán mã độc và các trang tin, báo mạng của cơ quan Đảng, Chính phủ, các tổ chức và doanh nghiệp do các tổ chức tội phạm thực hiện vẫn gia tăng. Các hành vi lợi dụng Internet để lừa đảo, đánh cắp mật mã, thông tin riêng của các tổ chức và cá nhân, các vụ lộ lọt thông tin bí mật quốc gia trên môi trường mạng xảy ra khá nghiêm trọng.

Từ thực tiễn phát triển thông tin trên Internet, tình hình vi phạm pháp luật và tội phạm trên mạng Internet, những bất cập trong công tác quản lý nội dung thông tin trên Internet và những vấn đề đặt ra cho công tác quản lý nội dung thông tin trên Internet cần thiết để triển khai các giải pháp tổng thể nhằm

phát huy mặt tích cực và hạn chế tính tiêu cực của Internet, đáp ứng yêu cầu nhiệm vụ chính trị của đất nước trong tình hình mới.

2.Một số biện pháp giáo dục an toàn thông tin và phòng chống vi phạm pháp luật trên không gian mạng cho sinh viên khi tham gia học tập tại Trung tâm GDQP&AN Đại học Thái Nguyên.

2.1. Giáo dục nâng cao nhận thức về bảo vệ chủ quyền quốc gia, các lợi ích và sự nguy hại đến từ không gian mạng cho SV.

Ngày nay, quan niệm về lãnh thổ, chủ quyền, biên giới của một quốc gia không chỉ là đất liền, hải đảo, vùng biển và vùng trời, mà cả lãnh thổ không gian mạng, chủ quyền không gian mạng. Theo đó, lãnh thổ không gian mạng là một bộ phận hợp thành lãnh thổ quốc gia, nơi xác định biên giới mạng và thực thi chủ quyền quốc gia trên không gian mạng.

Bảo vệ chủ quyền quốc gia còn là bảo vệ không gian mạng của quốc gia, bao gồm, bảo vệ các hệ thống thông tin; các chủ thể hoạt động trên không gian mạng; hệ thống dữ liệu, tài nguyên mạng; các quy tắc xử lý và truyền số liệu. Đảm bảo quyền bình đẳng trong tham dự quản lý mạng Internet quốc tế; độc lập trong vận hành hạ tầng cơ sở thông tin thuộc lãnh thổ quốc gia; bảo vệ không gian mạng quốc gia không bị xâm phạm và quyền quản trị truyền tải cũng như xử lý số liệu của quốc gia.

Cán bộ, đảng viên và các tầng lớp nhân dân mà nhất là SV cần nhận thức rõ các nguy cơ đến từ không gian mạng như: tấn công mạng, gián điệp mạng, khủng bố mạng, tội phạm mạng, đặc biệt là nguy cơ chiến tranh mạng đang là thách thức gay gắt về an ninh, và bảo đảm an ninh mạng đang trở thành trọng tâm ưu tiên của quốc gia. Vì vậy, cần quán triệt các quan điểm của Đảng về phát triển khoa học công nghệ và chiến lược bảo vệ Tổ quốc trong tình hình mới, các định hướng hành động của Việt Nam trong bảo vệ chủ quyền và lợi ích quốc gia trên không gian mạng và nhận thức rõ rằng, đe dọa trên không gian mạng là một trong những mối đe dọa thực tế và nguy hiểm nhất đối với an ninh quốc gia hiện nay cho các em hiểu biết được.

2.2.Tuyên truyền, phổ biến, giáo dục các quy định của pháp luật về quản lý không gian mạng cho SV.

Phổ biến các điều khoản của Bộ luật Hình sự 2015 (Mục 2, Điều 285-294) liên quan đến lĩnh vực công nghệ thông tin, mạng viễn thông; Nghị định số 72/2013/NĐ-CP ngày 15-7-2013 của Chính phủ và Thông tư số 09/2014/BTTTT ngày 19-8-2014 của Bộ Thông tin và Truyền thông về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội, những hành vi bị nghiêm cấm trong sử dụng mạng xã hội.

Tuyên truyền, phổ biến, giáo dục Luật An ninh mạng năm 2018. Luật An ninh mạng được xây dựng nhằm bảo vệ người dùng hợp pháp trên không gian mạng; phòng ngừa, đấu tranh, làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống Nhà nước, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, kích động biểu tình, phá rối an ninh trên mạng của các thế lực phản động. Phòng ngừa, ngăn chặn, ứng phó, khắc phục hậu quả của các đợt tấn công mạng, khủng bố mạng và phòng, chống nguy cơ chiến tranh mạng.

Tuyên truyền sâu rộng về những hành vi bị cấm trong Luật An ninh mạng, nhất là các hành vi sử dụng không gian mạng để tuyên truyền chống Nhà nước; tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước; xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; thông tin sai sự thật; hoạt động mại dâm, tệ nạn xã hội; phá hoại thuần phong, mỹ tục; xúi giục, lôi kéo, kích động người khác phạm tội; thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm 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 tổ chức, cá nhân hoặc để trục lợi.

Các hình thức giáo dục cần được vận dụng đa dạng, phong phú và linh hoạt như: Thông qua các bài học lý thuyết tổ chức nói chuyện chuyên đề, phổ biến pháp luật; tuyên tuyền Luật An ninh mạng hoặc tổ chức các cuộc thi tìm hiểu về an toàn thông tin cho SV; Qua đó góp ý xây dựng chương trình giáo dục an toàn thông tin mạng của các cơ sở giáo dục hoặc tham gia biên soạn các tài liệu liên quan đến an toàn thông tin mạng.

2.3. Bồi dưỡng kỹ năng nhận diện các âm mưu, thủ đoạn tấn công mạng và các hình thái phát sinh trên không gian mạng cho SV.

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 gắm 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…

Ở mức độ cao hơn, các thế lực thù địch có thể thông qua block cá nhân lôi kéo, kích động các phần tử bất mãn, tập hợp lực lượng, thành lập các tổ chức chống đối như Việt Tân, Chính phủ quốc gia Việt Nam lâm thời, Thanh Niên Dân Chủ,… núp dưới vỏ bọc các tổ chức "xã hội dân sự", "diễn đàn dân chủ" để xuyên tạc cương lĩnh, đường lối, quan điểm, nền tảng tư tưởng của Đảng.

Các thế lực thù địch còn lợi dụng báo điện tử, các website, dịch vụ thư điện tử, mạng xã hội facebook, Zalo, Twitter, diễn đàn,... để phát tán các tài liệu, kêu gọi tuần hành, biểu tình, gây mất ổn định an ninh chính trị, trật tự an toàn xã hội, chống phá chính quyền, chia rẽ mối đoàn kết giữa Đảng và Nhân dân hoặc sử dụng "khoảng trống thông tin" để tấn công vào sự hiếu kỳ của công chúng; làm mới thông tin cũ, bịa đặt thông tin mới để chống phá. Các trang mạng có nhiều nội dung thông tin xấu, độc như Dân Làm Báo, Quan Làm Báo; Boxit, Dân Luận, Chân Dung Quyền Lực…

2.4.Nâng cao ý thức phòng tránh, tự vệ và sử biện pháp kỹ thuật để khắc phục hậu quả trong trường hợp bị tấn công trên không gian mạng cho SV.

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.

Mỗi SV cần nghiên cứu và sử dụng tốt các biện pháp kỹ thuật bảo đảm an toàn thông tin như bảo vệ tài khoản cá nhân bằng xác thực mật khẩu đa lớp; tạo thói quen quét virus trước khi mở file; thực hiện sao lưu dự phòng trên ổ cứng ngoài, mạng nội bộ hoặc trên các dịch vụ lưu trữ đám mây (Google Drive, OneDrive); kiểm tra lộ lọt thông tin tài khoản cá nhân qua Trung tâm xử lý tấn công mạng Việt Nam.

Người dùng không nên vào những trang web lạ (hoặc trang web đen), những email chưa rõ danh tính và đường dẫn đáng nghi ngờ; cập nhật bản trình duyệt, hệ điều hành và các chương trình sử dụng; dùng những phần mềm diệt virus uy tín và được cập nhật thường xuyên, không tắt chương trình diệt virus trong mọi thời điểm. Khi phát hiện bị tấn công trên không gian mạng, nhanh chóng ngắt kết nối mạng; sử dụng các công cụ giải mã độc; báo cho người có trách nhiệm qua đường dây nóng.

3.Kết luận

Trên đây là các biện pháp có ý nghĩa rất lớn nhằm nâng cao dân trí một cách toàn diện, để mỗi người dân, đặc biệt là thế hệ trẻ, học sinh, sinh viên có ý thức tự bảo vệ mình và trở thành bộ lọc thông tin, hướng dẫn những người xung quanh nhận biết, sàng lọc các thông tin xấu, thông tin độc hại. Nhóm biện pháp này mang tính tuyên truyền và giáo dục, đòi hỏi phải xây dựng một đề án thông tin riêng, phù hợp với đặc điểm tâm sinh lý, đời sống, trình độ nhận thức và điều kiện thực tiễn của Việt Nam; đặc biệt tránh kiểu lý luận mang tính giáo điều, xa rời thực tiễn cuộc sống. Các cơ quan báo chí đẩy mạnh công tác tuyên truyền, giáo dục về nguyên nhân, sự nguy hiểm, tác hại và ảnh hưởng do vi phạm pháp luật và tội phạm trên mạng Internet gây ra đối với an ninh quốc gia, trật tự an toàn xã hội; nâng cao nhận thức, trách nhiệm trong phòng ngừa, chống vi phạm pháp luật và tội phạm trên mạng Internet cho toàn dân, nhất là SV để các em chủ động đấu tranh chống lại các thông tin xuyên tạc, chống phá từ các thế lực thù địch, phản động; thường xuyên cập nhật, đưa tin chính xác, phản ánh đầy đủ và kịp thời tình hình chính trị, quốc phòng, an ninh, kinh tế - xã hội; phản bác hiệu quả những luận điệu sai trái của các thế lực thù địch trong và ngoài nước; qua đó làm tốt vai trò cầu nối giữa Đảng, Nhà nước với nhân dân; nâng cao nhận thức, tăng cường sự thống nhất tư tưởng trong toàn Đảng, toàn quân, toàn dân. Làm tốt việc tuyên truyền trên các phương tiện truyền thông đại chúng như báo chí, kết hợp với truyền thông xã hội, với gia đình, nhà trường, các tổ chức đoàn thể nhằm hướng dẫn, nâng cao ý thức phòng ngừa, chống vi phạm pháp luật và tội phạm trên mạng Internet, ý thức sử dụng thông tin trên Internet của người dân, đặc biệt là thế hệ trẻ để tự mình sàng lọc những nội dung xấu, khai thác những thông tin có lợi phục vụ nhu cầu học tập, thông tin giải trí lành mạnh.

Tài liệu tham khảo

1. Chỉ thị số 46-CT/TW ngày 27/7/2010 của Ban Bí thư Trung ương Đảng (khóa X) về "Chống sự xâm nhập của các sản phẩm văn hóa độc hại gây hủy hoại đạo đức xã hội".

2. Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư ban hành về tăng cường công tác bảo đảm an toàn thông tin mạng.